



# I N D E X

## Symbols

---

- “ ” (double quotes) in chat scripts, 112, 133
- ! (exclamation point)
  - procmon.cmd files, 69
  - telnet command, 44
  - UUCP addresses, 99-100
- # (pound) symbol in network configuration files, 18
- \* (asterisk)
  - traceroute command, 37
  - terminal write status, 31
- ? (question mark)
  - process tables, 51
  - telnet command, 44
- \ (backslash)
  - bang addressing, 100
  - UUCP Dialer file special characters, 107
  - UUCP Permissions file, 118
- 8lgm mailing list (network security holes), 444, 848

## A

---

- a command option
  - arp, 38
  - netstat, 33
  - ruptime, 30
- ac command, 147

- accessing
  - TCP services with netcat, 329
  - TCP/IP connection sequence numbers, 312
- accounting user accounts with Kerberos, 539
- accounts, *see* user accounts
- accton command, 154
- ACK flags (TCP), 311
- ACM SigSAC (Special Interest Group on Security, Audit, and Controls), 208
- active DNS spoofing attacks, 306
- aculog file (Unix audit log), 151
- add-on utilities (PGP), 686-689
- adding user accounts to authentication server database (TIS Firewall Toolkit), 364-368
- additional-tickets field (KRB\_KDC\_REQ message), 589
- Address Resolution Protocol (ARP), 16-18, 38-39
- addresses
  - bang addressing, 99
  - broadcast, 9, 259
  - classes, 7-10
  - destinations, specifying, 16
  - dotted decimal address, 9
  - e-mail (online directories), 461
  - Ethernet, 18
  - hardware, spoofing, 279-281
  - hostname to IP address resolution, 24-25

- Internet assignments, 7
- Internet-to-Ethernet address translation table, 38
- IP addresses, 7-9
  - hacker access to*, 445-447
  - spoofing*, 492-495
- multicast, 8
- netmasks, 10
- networks, pinging with netscan utility (TIS Firewall Toolkit), 379
- octets, 8-9
- reserved, 9
- subnets, 9-12
- translating hostnames into IP addresses, 12
- UUCP (Unix to Unix CoPy) commands, compatibility with Internet addressing, 99
- addresses field (KRB\_KDC\_REQ message), 589
- administration (system policies), 182
  - see also* system security, policies
- alert (syslog file severity level), 149
- ALLOW-POSTDATE field (Kerberos tickets), 585
- anonymous FTP, 45, 478
- anonymous login (UUCP), 123-124
- antivirus utilities, 814-827
  - behavior blockers, 829-830
  - heuristic scanners, 830-832
  - integrity checkers, 824-825
  - memory scanners, 823-825
  - virus scanners, 815-820
- ap-options field (KRB\_AP\_REQ message), 595
- APOLLO mailing list, 207
- APOLLO-L mailing list, 207
- appending COM file viruses, 785
- Applet Host security mode (Java applets), 727
- applets (Java)
  - security modes, 727-728
  - testing, 703, 725-727
  - viewing with Netscape, 728
- Appletviewer (Java), 725-727
- Application Log (Windows NT), 161
- applications
  - TIS Firewall Toolkit
    - authmgr client*, 394-395
    - authsrv*, 360-372, 395-402
    - clauses*, 328
    - comments, inserting*, 328
    - ftp-gw*, 343-348, 402-406
    - http-gw*, 354-359, 406-412
    - login-sh*, 412-413
    - netacl*, 329-333, 414-415
    - plug-gw*, 372-378, 416-417
    - rlogin-gw*, 339-343, 418-419
    - rules*, 328, 339
    - smap client*, 349, 420-421
    - smapd*, 351, 421-423
    - tn-gw*, 333-339, 423-426
    - x-gw*, 359-360, 426-427
  - Argus network management program, 472
  - ARMOR configuration keyword (PGP), 678
  - armor mode (PGP), 667
  - ARMORLINES configuration keyword (PGP), 678
  - arp command (ifconfig), 16
  - ARP (Address Resolution Protocol), 18
    - caches
      - deleting entries*, 286
      - displaying entries*, 285
      - inserting multiple static entries*, 286
      - inserting static entries*, 286
      - permanent entries*, 285
    - servers, 286
  - spoofing, 281-284
    - case study*, 287-288
    - detecting*, 288-292
    - host-level active detection*, 289
    - host-level passive detection*, 289
    - network-level active detection*, 290-292
    - preventing*, 284-287
    - rlogin protocol vulnerability*, 276
    - server-level active detection*, 289-290
- arp program, 16, 38-39, 443
- ARPANET, 6-7, 45
- arpmon network monitoring software, 292

- ARPWatCh 1.7 network monitoring
  - software, 292
- asax (audit trail analyzer), 158
- ASSERT ERROR (UUCP log file error message), 125
- asterisk (\*)
  - terminal write status, 31
  - traceroute command, 38
- asymmetric cryptography, 277
  - see also* public key cryptosystems
- attaching digital signatures to e-mail messages
  - with PGP, 665, 668-671
- attacks on network security, 431-444
  - acquiring login accounts, 436-437
  - acquiring root access, 437-438
  - characterizing, 435-438
  - extend access by hackers, 438-439
  - modem-based, 467-476
- audit trails, 145, 209
  - analyzing
    - asax program*, 158
    - chklastlog program*, 158
    - chkwtmp program*, 158
  - auditing utilities, 155-158
  - DOS utilities, 164-165
  - drills, 214
  - Ethernet sniffers, 157-158
  - open files reports (lsof program), 158
  - procedure testing, 214-215
  - process accounting, 153-155
  - system monitoring/logging utilities, 158-159
  - Unix audit logs, 146-153
  - Windows NT, 160-164
  - see also* logging; messages; reports
- auth host access rule (tn-gw application), TIS Firewall Toolkit, 338
- auth (syslog file facility), 149
- AUTH\_UNIX authentication, 480
- authdump command, 368-370
- authenticating
  - clients
    - in Kerberos networks*, 591-595
    - to network services via Kerberos tickets*, 571-573
    - tickets (Kerberos), 570
    - user accounts with Kerberos, 538-542
    - workstations in Kerberos, 609-610
  - authenticating login shell, *see* login-sh application
  - authentication server, *see* authsrv
  - Authentication Service Exchange (Kerberos), 575-578, 584-591
  - authentication systems, 202
  - authenticator field (KRB\_AP\_REQ message), 596
  - authenticator-vno field (Kerberos ticket authenticators), 574
  - authenticators (Kerberos tickets), 573-574
  - authload command, 368-370
  - authmgr client application (TIS Firewall Toolkit), 368, 394-395
  - authorization data (Kerberos messages), 606
  - authorization-data field
    - Kerberos ticket authenticators, 574
    - Kerberos tickets, 573
  - authorizing user accounts with Kerberos, 539
  - authpriv (syslog file facility), 149
  - authsrv (authentication server), TIS Firewall Toolkit, 360-372, 395-402
    - adding users to database, 364-368
    - administrative commands, 364-366
    - commands, 398-401
    - compiling, 361
    - configurations, 361
    - database management, 368-370
    - group configurations, 397
    - installation, 401-402
    - operations, 370-372
    - reports, 382-383
    - rules, 362-363
    - user configurations, 397
  - authtime field
    - Kerberos tickets, 572
    - KRB\_CRED message, 604
    - KRB\_KDC\_REP message, 591
- autonomous network systems, 295

**B**

- b (finger command option), 32
- B1 virus, 783
- backslash (\)
  - bang addressing, 100
  - UUCP Dialer file special characters, 107
  - UUCP Permissions file, 118
- backups (system security), 196
- BAD LOGIN/MACHINE COMBINATION (UUCP log file error message), 125
- BAKRING configuration keyword (PGP), 678
- bang addressing, 99
- Basic Input/Output System (BIOS), 756
- BATCHMODE command-line option (PGP), 681
- baud rates, configuring in UUCP networks, 110, 132
- bdflush daemon, 55
- behavior blockers (antivirus utilities), 829-830
- Bellman-Ford protocols, 296
- Berkeley r-commands, 40-43
- bibliographies
  - computer law, 238-239
  - computer security, 239-244
  - ethics, 244-246
  - Internet Worm, 246-248
  - miscellaneous publications, 251-253
  - National Computer Security Center, 248-251
  - security checklists, 251
- big endian coding, 721
- bin directory (SATAN), 502-503
- binary files
  - integrity, verifying to prevent hacker attacks, 497-498
  - PGP, vulnerability to hackers, 685
  - processing with PGP, 666-667
- BIND
  - DNS name server software, 308
  - resolver library, 39
- BIOS (Basic Input/Output System), 756
- BIOS parameter blocks (floppy disks), 755
- bits (subnet addresses), determining fixed, 11
- BNU (Basic Networking Utilities), 96
  - Devices file, 103-105
  - Dialers file, 106-108
  - Systems file, 108-111
  - see also* UUCP
- Bolt, Beranek, and Newman, Inc. (BBN), 6
- Bones Kerberos distribution, 556-557
- boot (run level action field), 72
- boot protocols, implementing, 24
- boot record viruses, 767-768, 805
  - Internet transmission, 805
  - methods of infection, 837-839
  - peer-to-peer network infection, 805
  - preventing, 831
  - repairing, 831
  - server infection, 805
- boot records (floppy disks), 755
- booting, *see* system boot
- BOOTP daemon, 24
- bootpd servers, exploitation by/vulnerability to hackers, 455-457
- bootwait (run level action field), 73
- bounce to program hole (sendmail program), 439
- Bourne shell daemons, creating, 61-65
- BREAK signals (UUCP chat scripts), 111, 132
- bridges
  - networks, 265, 274
  - vulnerability to spoofing, 280
- broadcast addresses, 9, 259
- broadcast command (ifconfig), 16
- broadcast storms, debugging, 157
- brouters, 291
- browsers, *see* Web browsers
- brute force hacker attacks against PGP, 682-683
- BSD (Berkeley Software Distribution) code, 52
- BSD Unix (University of California at Berkeley), 6
- BTNG RMON agent, 292

buffers  
     fingerd program, vulnerability to  
         hackers, 440  
     overruns, CGI programming in C/C++, 746  
 bugtraq mailing list (network security holes),  
     444, 848  
 building SATAN, 513-534  
 bypassing CGI scripts to ensure security,  
     741-742  
 bytetimes (Java), 699, 707, 717

## C

-C options (endmail program), vulnerability to  
     hackers, 443  
 -c count (ping command option), 27  
 C programming language  
     CGI libraries, 735  
     CGI programming, 746  
 C++ Programming Language  
     CGI programming, 746  
     versus Java, 703-706  
 caches  
     ARP  
         *deleting entries*, 286  
         *displaying entries*, 285  
         *inserting multiple static entries*, 286  
         *inserting static entries*, 286  
         *permanent entries*, 285  
     DNS name servers, 303, 496  
 caddr field  
     Kerberos tickets, 573  
     KRB\_CRED message, 604  
     KRB\_KDC\_REP message, 591  
 Caesar cipher encryption, 621-623  
 Call-unit (L-devices file field), 130  
 CALLBACK (Permissions file keyword), 120  
 CALLBACK REQUIRED (UUCP log file error  
     message), 125  
 calling costs, controlling for UUCP systems,  
     108, 122, 131  
 \$canonical field (SATAN database facts  
     records), 527  
 CAN'T ACCESS FILE (UUCP log file error  
     message), 125  
 cast statements (Java), 705  
 CBC (Cipher Block Chaining) encryption, 546  
 CERT (Computer Emergency Response Team),  
     204-205, 846-847  
 CERT- ADVISORY mailing list, 204  
 CERT-TOOLS mailing list, 205  
 CERT\_DEPTH configuration keyword  
     (PGP), 678  
 CFB (Cipher Feedback) encryption, 546  
 CGI (Common Gateway Interface) scripts,  
     732-736  
     access restriction, 739  
     access restriction with HTTP, 736  
     bypassing to ensure security, 741-742  
     dangers of, 733  
     data protection, 747-748  
     decoding, 734-735  
     encoding, 734-735  
     environment variables, 737  
     GET method of data input, vulnerability to  
         hackers, 737-738  
     libraries, 735-736  
     nobody UIDs, 739  
     operations, 733-734  
     passing data to  
         *via command-line arguments*, 733  
         *via environment variables*, 734  
         *via standard input streams*, 734  
     POST method of data input, vulnerability to  
         hackers, 737-738  
     programming  
         *in C*, 746  
         *in C++*, 746  
         *in PERL*, 743-746  
         *in safe languages*, 746-747  
     request logins, 749  
     running  
         *from controlled file system Web servers*, 740  
         *under program owner UIDs*, 740-741  
         *with minimum privileges*, 739-740

- SSI (Server Side Includes), 742-743
  - vulnerability to hackers, 733, 736-740
  - Web server trust relationships, 736
- CGIWrap utility, 741
- characterizing attacks on network security, 435-438
- CHARSET configuration keyword (PGP), 678
- chat scripts (UUCP), 107-108, 111-114, 132-133
  - "" (double quotes), 112, 133
  - defining, 111-114, 132
  - special characters, 112-113, 133
  - with TCP/IP, 114
- Chat-script (L.sys file field), 132
- checking accounts, vulnerability to network sniffers, 261
- checksums, 200
  - collision-proof, 553
  - CRC checksums, 200
  - crc32, 553
  - cryptographic, 200-201
  - des-mac, 554
  - des-mac-k, 555
  - Kerberos support for, 552-555
  - keyed, 553
  - rsa-md4, 554
  - rsa-md4-des, 554
  - rsa-md4-des-k, 554
  - rsa-md5, 554
  - rsa-md5-des, 554
- chklastlog (Web site), 158
- chklastlog (audit trail analyzer), 158
- chkwtmp (audit trail analyzer), 158
- chmod command (UUCP), 124
- CIAC (Computer Incident Advisory Capability) group, 846
- CIAC archives Web site, 463
- Cipher Block Chaining (CBC) encryption, 546
- cipher fields (encrypted messages), 549
- ciiphertext, 543
- CISC (Complex Instruction Set Computing) CPUs, 719
- cksum field
  - Kerberos ticket authenticators, 574
  - KRB\_SAFE message, 599
- class A addresses, 8
- class B addresses, 8
- class C addresses, 9
- class loader (Java), 716-717
- classes
  - addresses, 7-9
  - downloading with Java, 715
  - fragile superclasses (C++), 705
  - Internet Threat Levels, 433
  - Java, 705
  - methods, calling with Java, 714
  - viruses, 806-814
- clauses (TIS Firewall Toolkit applications), 328
  - netacl, 330
  - plug-gw, 372-373
  - rlogin-gw application, 340
  - smap, 420-421
  - tn-gw, 334-335
- CLEARSIG configuration keyword (PGP), 678
- clearsigning e-mail messages with PGP, 674-675
- clients (HTTP)
  - non-proxy aware, 355-356
  - proxy aware, 356
- client requests (Kerberos Key Distribution Center), 584
- client/server authentication exchange (Kerberos), 591-597
- clients
  - authenticating
    - in Kerberos networks, 591-595
    - to network services via Kerberos tickets, 571-573
  - Authentication Service exchange with Kerberos, 575-578
  - Ticket Granting Service exchange with Kerberos, 578-584
- Clone command (Java Appletviewer), 726
- close (telnet command), 44
- CLOSE\_WAIT (socket state), 36
- CLOSED (socket state), 36
- CLOSING (socket state), 36
- clusters (floppy disk sectors), 754

- cname field
  - Kerberos tickets, 572
  - KRB\_KDC\_REP message, 591
  - KRB\_KDC\_REQ message, 588
- COAST (Computer Operations, Audit, and Security Technology) project, 309, 846
- code listings
  - dfmon daemon, 74-78
  - dfmon.cfg configuration file, 78-82
  - procmon command, 82
- collision-proof checksums, 553
- COM files
  - appending viruses, 785
  - improved overwriting viruses, 787
  - overwriting viruses, 786
  - prepending viruses, 785
  - virus infection, 762
- commands
  - ac, 147
  - accton, 154
  - administrative, 27-40
  - arp, 38-39
  - authdump, 368-370
  - authentication server (TIS Firewall Toolkit), 364-366
  - authload, 368-370
  - authmgr, 368
  - Berkeley r-commands, 40-43
  - chmod (UUCP), 124
  - cu (UUCP), 106, 111, 130, 132
  - dig, 39-40
  - executing on remote systems, 42-48
  - finger, 31-33
  - history, 153
  - hostname, 13
  - ICMP ECHO\_REQUEST, 27
  - ifconfig, 15-17, 30-31
  - inetd, 20
  - Java Appletviewer, 726
  - kill, 62
  - last, 147
  - lastcomm, 154
  - logging, 153-155
  - ls (UUCP), 105
  - make install (TIS Firewall Toolkit), 321
  - man, 64
  - mesg, 491
  - netstat, 24, 33-36, 156-157, 325
  - nslookup, 25
  - ping, 27-29
  - print, 66-67
  - processing, changing delay between, 69
  - procmon, 82-83
  - ps, 50, 155
  - r-commands (rlogin protocol), 276
  - rcmd, 43
  - rcp, 41, 276
  - remote command execution, 137
  - require, 69
  - rlogin, 40, 43
  - rsh, 42, 276
  - ruptime, 29-30
  - rwho, 30
  - sa, 155
  - showmount, 60
  - sudo, 150
  - switch user, 150
  - TCP/IP categories, 26
  - telnet, 43-48
  - tn-gw application (TIS Firewall Toolkit), 336
  - traceroute, 36-37
  - uname (UUCP), 100
  - user commands, 40
  - uucico (UUCP), 114
  - uuclean, 138
  - uustat, 127
  - uutry (UUCP), 114
  - who, 74
- COMMANDS (Permissions file keyword), 120
- COMMENT configuration keyword (PGP), 678
- comments, inserting in TIS Firewall Toolkit applications, 328
- Common Gateway Interfaces, *see* CGI scripts
- companion viruses (DOS program files), 797-798

- compilers (Java), 703, 712-715
- compiling
  - authentication servers (TIS Firewall Toolkit), 361
  - TIS Firewall Toolkit
    - under BSDI*, 320
    - under SunOS*, 320
  - with Java, 709, 712-715
- complete trust relationships (PGP keys), 649-650, 658
- COMPLETES\_NEEDED configuration keyword (PGP), 678
- COMPRESS configuration keyword (PGP), 679
- compressing e-mail messages with PGP, 666
- Computer Emergency Response Team, *see* CERT
- Computer Incident Advisory Capability group, *see* CIAC group
- Computer Operations, Audit, and Security Technology project, *see* COAST project
- The Computer Underground Digest, 203
- Computers and Security (journal), 208
- config directory (SATAN), 501
- configuration files
  - dfmon.cfg, 78-82
  - /etc/ethers, 18
  - /etc/exports, 60
  - /etc/ftpusers, 46
  - /etc/hosts, 17-18
  - /etc/hosts.equiv, 21
  - /etc/hosts.lpd, 23
  - /etc/inetd.conf, 20
  - /etc/inittab, 55
  - /etc/networks, 18-19
  - /etc/passwd, 22
  - /etc/pcnfsd.conf, 60
  - /etc/printcap, 23
  - /etc/procmon.cfg, 68
  - /etc/protocols, 19
  - /etc/rc, 53
  - /etc/sendmail.cf, 58
  - /etc/service, 19-20
  - /etc/sockcf, 23
  - /etc/strcf, 23
  - /etc/syslog.conf, 26, 57
  - .netrc, 47
  - pound (#) symbol, 18
  - procmon.cfg, 68
  - procmon.cmd, 68
  - .rhosts, 21
  - syslog.conf, 148
  - /usr/mmdf/mmdftailor, 59
- configurations
  - firewalls for NTP server time updates, 325
  - interfaces for networks, 15-17
  - modems (UUCP Devices file), 103-105
  - non-standard (firewalls), 218
  - PGP, 677-682
  - procedures for system security, 195-196
  - SATAN, 520-522
  - TCP/IP for TIS Firewall Toolkit, 326-327
  - TIS Firewall Toolkit, 322-326
    - authentication server*, 361
    - DNS for smap client application*, 353-355
    - ftp-gw application*, 343-348
    - http-gw application*, 354-359, 409-411
    - netacl application*, 329-333
    - plug-gw application*, 372-373
    - rlogin-gw application*, 339-343
    - smap client application*, 349-351
    - smapd application*, 351-353
    - tn-gw application*, 333-339
    - x-gw application*, 359-360
  - TLIS connections (UUCP systems), 139-140
  - UUCP, 103, 129, 139-140
  - verifying software, 209
- confounders (encryption), 549
- connecting
  - to FTP sites
    - anonymous FTP, 45, 478
    - with ftp-gw application (TIS Firewall Toolkit)*, 347
    - with netacl*, 331-333, 348
  - to Gopher sites with http-gw application (TIS Firewall Toolkit), 354-359



- to newsgroups with plug-gw application (TIS Firewall Toolkit), 373-376
  - to remote hosts with rlogin-gw application (TIS Firewall Toolkit), 342
  - to telnet sites with tn-gw application (TIS Firewall Toolkit), 336-337
  - to WWW sites with http-gw application (TIS Firewall Toolkit), 354-359
  - connections
    - NNTP, with plug-gw application (TIS Firewall Toolkit), 373-376
    - POP, with plug-gw application (TIS Firewall Toolkit), 376-378
    - TCP
      - preventing remote access to local services*, 454
      - setup*, 310
      - via modems*, 488
      - via proxy servers*, 476
      - vulnerability to hackers*, 440-441
    - TCP/IP
      - sequence numbers, accessing*, 312
      - vulnerability to sniffing/forging attacks*, 312
    - UDP, preventing remote access to local services, 454
  - constant pool memory area (JVM stacks), 724-730
  - Control Panel (SATAN), 515
  - conventional encryption (e-mail messages with PGP), 668
  - conventional memory (DOS storage methods), 790
  - converting
    - PCs to network bridges, 274
    - Web servers from root to controlled file systems, 740
  - COPS security utility, 209-210, 437
  - copy protection, 23
  - copyrighted software, system policies, 180
  - corruption (DNS caches), 496
  - council, *see* legal considerations
  - Courtney (SATAN scan detection program), 471
  - cpd daemon, 23, 56
  - CPUs (central processing units)
    - daemon requirements, 51
    - integrating with JVMs, 719
    - logging time consumption, 155
  - cracking user account passwords, 436
  - CRC checksums, 200
  - crc32 checksums, 553
  - crealm and cname field (Kerberos ticket authenticators), 574
  - crealm field
    - Kerberos tickets, 572
    - KRB\_KDC\_REP message, 591
  - credit card accounts, vulnerability to network sniffers, 261
  - crit (syslog file severity level), 149
  - cron (syslog file facility), 149-151
  - cron daemon, 56
  - crontab files (UUPC), 56, 126-127, 151
  - cross-checking DNS name servers, 303
  - crypt (data encryption), 199
  - cryptographic checksums, 200-201
  - ctime field
    - Kerberos ticket authenticators, 574
    - KRB\_AP\_REP message, 597
  - cu command (UUCP), 106, 111, 130-132
  - cusec field
    - Kerberos ticket authenticators, 574
    - KRB\_AP\_REP message, 597
  - Customer Warning System (Sun Microsystems), 212
  - Cygnus Corporation Web site, 473, 848
- 
- ## D
- 
- d (ping command) option, 27
  - d debug hole (sendmail program), 439
  - d host (arp command) options, 38
  - daemons, 7, 50-55
    - bdflush, 55
    - BOOTP, 24
    - compared to programs, 50
    - cpd, 23, 56
    - CPU requirements, 51

- creating
  - Bourne shell*, 61-65
  - devices*, 62
  - input/output files*, 61, 66-67
  - PERL programming language*, 65-70
  - trapping signals*, 62-64, 67
- cron, 56
- deliver, 59
- dfmon, 64
- file descriptors, 61
- getty, 59
- inetd, 20, 26, 59, 324, 333
- init, 55
- ldsocket, 23
- lockd, 60
- lpd, 23, 56
- lpsched, 56
- mountd, 60, 477
- named, 25
- networks, exploitation by hackers, 453
- NFS server, 60
- nfsd, 60
- pcnfsd, 60
- preventing shutdowns, 65-66
- procmon, 67-70
- RARP, 24
- required during system boot
  - HP-UX*, 52-53
  - SCO Unix*, 53-54
  - SunOS*, 51
- Reverse Address Resolution Protocol, 18
- rlogind, 59
- routed, 24-25, 59
- rpc.statd, 60
- RWHO, 26
- sco\_cpd, 56
- sendmail, *see* sendmail daemon
- slink, 23
- SNMP, 24
- starting from Internet super-server, 20
- statd, 60
- swapper, 55
- syslog, 26, 57-58, 148-149
- update, 55
- uudemon.cleanup (UUCP), 127
- uudemon.poll (UUCP), 127
- DARPA (Defense Advanced Research Projects Agency), 6-7, 19
- Data Encryption Standard, *see* DES
- data exchange (TCP), 311
- The Data Security Letter, 208
- databases
  - authentication server (TIS Firewall Toolkit), 368-370
  - SATAN, 516
    - facts records*, 525-528
    - host records*, 528-529
    - records*, 525-529
    - todo records*, 529
- datagrams (TCP/IP), forged, 311-313
- DDN Management Bulletin, 207
- DDN Network Information Center, 19
- DDN Security Bulletin, 205, 207
- debug command (ifconfig), 16
- debug (syslog file severity level), 150
- debug command (ifconfig), 16
- debugging
  - broadcast storms, 157
  - enabling, 16
  - networks, 38, 157
  - permission files (UUCP version 2), 135
  - UUCP network connections, 114-115
    - checking file ownership*, 115
    - displaying error messages*, 114, 133
    - log files*, 124-126
- DEC Ultrix Kerberos, 556, 558
- deciphering transposition encryption, 619-620
- decoding CGI scripts, 734-735
- decrypting e-mail messages
  - with PGP, 644-645, 671-673
  - without saving to files, 676
- defaults
  - netmask addresses, 10
  - permissions, 118-119
- deleting ARP cache entries, 286
- deliver daemon, 59

- Department of Energy, 206
- DES (Data Encryption Standard), 198, 545-547
- des-cbc-crc encryption systems, 551
- des-cbc-md4 encryption systems, 552
- des-cbc-md5 encryption systems, 552
- des-mac checksums, 554
- des-mac-k checksums, 555
- DESlogin 1.3 zero-knowledge authentication software, 278
- dest pattern host access rule (tn-gw application), TIS Firewall Toolkit, 338
- dest-address command (ifconfig), 16
- detached signatures (PGP), 675-676
- detecting
  - ARP spoofing, 288-292
  - DNS spoofing, 303
  - network security holes, 445-476
  - SATAN scans, 471-472
- Device (BNU Devices file field name), 104
- Device (L-devices file field), 130
- DEVICE FAILED (UUCP log file error message), 125
- DEVICE LOCKED (UUCP log file error message), 125
- devices
  - creating, 62
  - defining for local networks, 105
  - UUCP
    - devices allowed*, 132
    - file ownership*, 105
- Devices (Basic Networking Utilities file), 96
- Devices file (UUCP), 103-105
- dfmon daemon, 64
  - code listings, 74-78
  - installing, 74
- dfmon.cfg configuration file, code listings, 78-82
- dial-out facilities, logging usage, 151
- Dialcodes (Basic Networking Utilities file), 97
- Dialcodes file (UUCP), 110-111
- DIALER SCRIPT FAILED (UUCP log file error message), 125
- dialer-token pairs (BNU Devices file field name), 104
- Dialers (Basic Networking Utilities file), 97
- Dialers file (UUCP), 106-108
- dig command, 39-40
- digital signatures
  - e-mail messages, 641-642, 665, 668-671
  - removing from PGP keys, 661-662
- direct action viruses (DOS program files), 789, 793-796
- directories
  - e-mail (world-writeable), vulnerability to hackers, 442
  - SATAN
    - bin*, 502-503
    - config*, 501
    - html*, 503
    - html/admin*, 508
    - html/data*, 508
    - html/docs*, 503-504
    - html/dots*, 504-505
    - html/images*, 505
    - html/reporting*, 505-506
    - html/running*, 506-507
    - html/tutorials*, 507
    - html/tutorials/vulnerability*, 507
    - include*, 501
    - perl*, 512-513
    - perllib*, 502
    - rules*, 501
    - src*, 508
    - src/boot*, 508
    - src/ftp*, 510-511
    - src/misc*, 509
    - src/nfs-chk*, 509
    - src/port\_scan*, 510
    - src/rpcgen*, 511
    - src/yp-chk*, 511-512
    - top-level*, 500
- disabling inetd services, 324
- disk buffers, flushing, 55
- disk monitor daemons, creating with Bourne shell, 61-65

disks, file maintenance, 126-127, 138-139

display (telnet command), 44

displaying ARP cache entries, 285

distributing PGP keys, 640-641

DNS (Domain Name Service), 12

- cached, corruption, 496
- configuring for smap client application (TIS Firewall Toolkit), 353-355
- name servers, 302
  - BIND software*, 308
  - caches*, 303
  - cross-checking*, 303
  - security weaknesses*, 304-305
- record types, 302
- SATAN scans, 477
- searchlists (security issues), 492
- spoofing, 301-309
  - active attacks*, 306
  - detecting*, 303
  - passive attacks*, 306-309
  - preventing*, 303, 306-309
  - preventing in TIS Firewall Toolkit configuration*, 329
  - rlogin protocol vulnerability*, 276

documentation (SATAN), 522-523

Domain Information Groper, 39-40

Domain Name Service, *see* DNS

domain names, 13, 17

DOS

- audit trail utilities, 164-165
- program files
  - companion viruses*, 797-798
  - potential damage by viruses*, 798-799
  - preventing viruses*, 833-834
  - repairing viruses*, 833-834
  - viruses*, 784-797
  - viruses under Windows NT DOS boxes*, 840
  - vulnerability to viruses*, 762-764

DOS Protected Mode Interface (DPMI),  
Windows 3.1 viruses, 841

dotted decimal address, 9

double quotes (“”) in chat scripts, 112, 133

down command (ifconfig), 16

downloading
 

- classes with Java, 715
- SATAN, 499-500
- TIS Firewall Toolkit, 319

DPMI (DOS Protected Mode Interface),  
Windows 3.1 viruses, 841

Drawbridge software, converting PCs to  
network brides, 274

drop files (SATAN scan rulesets), 530

dynamic loading (Java capabilities), 708-709

---

## E

e-data field (KRB\_ERROR message), 608

e-mail

- addresses, online directories, 461
- delivery, 59
- interaction with Java, 730
- messages
  - clearsigning with PGP*, 674-675
  - compressing with PGP*, 666
  - conventional encryption with PGP*, 668
  - decrypting with PGP*, 644-645, 671-673
  - decrypting without saving to files*, 676
  - detached signatures with PGP*, 675-676
  - digital signatures*, 641-642, 665
  - encrypting with PGP*, 643-644, 665, 670-671
  - filtering with PGP*, 665-666
  - non-repudiation*, 641
  - public key encryption*, 669-670
  - sending with PGP*, 667
  - signing with PGP*, 668-671
  - verifying with PGP*, 644-645, 671-673
  - vulnerability to network sniffers*, 261
- origin authentication, 199
- privacy enhanced mail, 199
- reports with TIS Firewall Toolkit, 387-388
- sendmail daemon, *see* sendmail daemon
- system security policies, 183
- TIS Firewall Toolkit applications, 348-354
- world-writable directories, vulnerability to  
hackers, 442

- e-text field (KRB\_ERROR message), 608
- ECB (Electronic Codebook) encryption, 546
- editing makefiles for TIS Firewall Toolkit under BSDI, 320
- Electronic Mail Association, 183
- emerg (syslog file severity level), 149
- enc-authorization-data field (KRB\_KDC\_REQ message), 588
- enc-part field
  - Kerberos tickets, 572
  - KRB\_AP\_REP message, 596
  - KRB\_CRED message, 604
  - KRB\_KDC\_REP message, 591
  - KRB\_PRIV message, 601
- ENC-TKT-IN-SKEY field (Kerberos tickets), 570, 585
- encapsulation (trailer), 16
- encoding
  - CGI scripts, 734-735
  - transited fields in Kerberos Ticket Granting Service exchange, 583
- ENCRYPT utility, 622
- encryption, 198, 616-617
  - Caesar cipher, 621-623
  - CBC (Cipher Block Chaining), 546
  - CFB (Cipher Feedback), 546
  - confounders, 549
  - conventional encryption, e-mail messages via PGP, 668
  - crypt, 199
  - DES, 198, 545-547
  - des-cbc-crc systems, 551
  - des-cbc-md4 systems, 552
  - des-cbc-md5 systems, 552
  - ECB (Electronic Codebook), 546
  - exporting programs for, 547-548
  - IDEA cryptosystem, 635, 668
  - IP addresses, 315
  - Java protection, 715
  - Kerberos, 543-555
    - client/server authentication exchange*, 594-595
    - keys*, 550-551
    - specifications*, 549-550
  - monoalphabetic substitutions, 624-627
  - national security issues, 543
  - NULL systems, 551
  - OFB (Output Feedback Mode), 546
  - passwords, 277-278
  - PGP program, 633-634
    - armor mode*, 667
    - binary distribution*, 637-639
    - binary files, vulnerability to hackers*, 685
    - clearsigning e-mail messages*, 674-675
    - compressing e-mail messages*, 666
    - configurations*, 677-682
    - conventional encryption*, 668
    - decrypting e-mail messages*, 644-645, 671-673
    - detached signatures*, 675-676
    - encrypting e-mail messages*, 643-644, 665 670-671
    - filtering e-mail messages*, 665-666
    - For Her Eyes Only messages*, 676
    - history of*, 634-636
    - keys, adding to public key rings*, 642-643, 654-656
    - keys, distributing*, 640-641
    - keys, extracting from public key rings*, 656-657
    - keys, fingerprints*, 663-664
    - keys, generating*, 639-640, 651-654
    - keys, management*, 650-665
    - keys, naming*, 646-647
    - keys, pass phrases*, 652
    - keys, removing from key rings*, 661-662
    - keys, removing signatures from*, 661-662
    - keys, revoking*, 664-665
    - keys, signing*, 657-660
    - keys, trust relationships*, 648-650, 658
    - keys, userids*, 652-654
    - keys, verifying*, 663-664
    - pass phrases*, 638
    - practical applications*, 635-636
    - processing binary files*, 666-667
    - processing text files*, 666-667

- public key rings*, 647, 660-685
- public key servers*, 686-687
- secret key rings*, 648, 660-661, 683-684
- security*, 682-685
- sending e-mail messages*, 667
- signing e-mail messages*, 668-671
- verifying e-mail messages*, 644-645, 671-673
- Windows front-end applications*, 688
- wiping files*, 676-677
- public key cryptosystems, 199, 277, 544, 636, 669-670
- secret key encryption, 544-545, 636
- substitution, 621-631
- symmetric encryption, 279
- transposition, 617-620
- Vigenere encryption, 628-631
- vulnerability to hackers, 496-497
- ENCRYPTTOSELF configuration keyword (PGP), 679
- endtime field
  - Kerberos tickets, 572
  - KRB\_CRED message, 604
- environ (telnet command), 44
- environment variables (CGI scripts), 737
- equivalency, 21-23
- err (syslog file severity level), 150
- error messages
  - displaying, 114, 133
  - UUCP log files, 125-126
- error-code field (KRB\_ERROR message), 608
- Esniff.c sniffing software, 260
- ESTABLISHED (socket state), 36
- /etc/ethers network configuration files, 18
- /etc/exports configuration files, 60
- /etc/ftpusers network configuration files, 46
- /etc/hosts network configuration files, 17-18
- /etc/hosts.equiv network configuration files, 21
- /etc/hosts.lpd network configuration files, 23
- /etc/inetd.conf network configuration files, 20
- /etc/inittab configuration files, 55
- /etc/networks network configuration files, 18-19
- /etc/passwd network configuration files, 22
- /etc/pcnfsd.conf configuration files, 60
- /etc/printcap network configuration files, 23
- /etc/procmon.cfg configuration files, 68
- /etc/protocols network configuration files, 19
- /etc/rc configuration files, 53
- /etc/sendmail.cf configuration files, 58
- /etc/service network configuration files, 19-20
- /etc/sockcf network configuration files, 23
- /etc/strcf network configuration files, 23
- /etc/syslog.conf configuration files, 57
- /etc/syslog.conf network configuration files, 26
- EthDump sniffing software, 260
- Ethernet, 6
  - addresses, 18
  - sniffers, 157-158
- etype field
  - encrypted messages, 549
  - KRB\_KDC\_REQ message, 589
- eval statement (PERL CGI programming), 745
- Event Viewer application (Windows NT), 161-162
- exclamation point (!)
  - procmon.cmd files, 69
  - telnet command, 44
  - UUCP addresses, 99-100
- EXE file viruses, 762-764, 787-788
- executing code with Java, 718
- execution environment (JVM stacks), 723
- expect-send pairs, 111-114, 132-133
- expiration (Kerberos tickets), 577
- exporting encryption programs, 547-548
- extend access (networks), illegal, 438-439
- extensions (SATAN scans), adding, 532-534
- external routing protocols, 296, 300
- extracting PGP keys from public key rings, 656-657

---

**F**

- f command option
  - finger, 32
  - ping, 27
  - netstat, 33
  - arp, 38
- facts files (SATAN scan rulesets), 530-531
- facts records (SATAN databases), 525-526, 528
- FAQs (Frequently Asked Questions), Secure Shell program, 474
- Farmer, Dan (co-creator of SATAN), 469
- FAT (File Allocation Tables), floppy disks, 755
- FBRs (Floppy Boot Records), 756-757
  - preventing viruses, 831
  - repairing, 831
  - viruses, 768-776
- fields
  - Kerberos ticket authenticators, 574
  - KRB\_AP\_REP message, 596-597
  - KRB\_AP\_REQ message, 595-596
  - KRB\_CRED message, 604
  - KRB\_ERROR message, 607
  - KRB\_KDC\_REP message, 591
  - KRB\_KDC\_REQ message, 587-589
  - KRB\_PRIV message, 601-602
  - KRB\_SAFE message, 599
  - tickets (Kerberos), 572-573
  - transited, encoding in Kerberos Ticket Granting Service excha, 583
- File Allocation Tables, *see* FAT
- file systems
  - unprivileged access scans by SATAN, 480-481
  - unrestricted exports, scanning with SATAN, 481
  - vulnerability to hackers, 459-460
- File Transfer Protocol, *see* FTP
- files
  - copying from remote terminals, 41
  - crontab (UUCP), 56, 126-127
  - deleting (UUCP file maintenance), 127
  - descriptors, 61
    - closing*, 66
    - opening*, 66
  - file system requests, 60
  - information integrity, 200
  - listing open, 158
  - logging access to httpd service (Windows NT), 163
  - logging file system changes, 159
  - ownership (UUCP devices), 105
  - permission (UUCP version 2), 134-137
  - status (UUCP), 117, 133
  - stealth virus-infected, repairing, 834
  - syslog.conf, 57-58
  - transfer statistics logs, 152
  - transferring, 45-48
    - system security*, 122
    - UUCP (Unix to Unix CoPy)*, 99-101
    - see also FTP; TCP/IP*
  - Unix audit logs, 146-153
  - USERFILE (UUCP version 2), transfer entries, 136
  - UUCP
    - Devices*, 103-105
    - Dialers*, 106-108
    - Systems*, 108-111
    - wiping with PGP, 676-677
  - filtering e-mail messages with PGP, 665-666
  - FIN\_WAIT\_1 (socket state), 36
  - FIN\_WAIT\_2 (socket state), 36
  - financial accounts, vulnerability to network sniffers, 261
  - finger utility, 31-33
    - vulnerability to hackers, 440
    - exploitation by hackers, 457
  - fingerprints (PGP keys), 663-664
  - firewalls, 197, 201
    - configuring for NTP server time updates, 325
    - impact of Java, 729
    - TIS Firewall Toolkit, 318-322
      - authentication server*, 360-372
      - authmgr client application*, 394-395
      - authsrv*, 395-402
      - compiling under BSDI*, 320
      - compiling under SunOS*, 320

- disabling IP address forwarding*, 326-327
- disabling inetd services*, 324
- downloading*, 319
- FTP site regarding*, 466
- FTP site availability*, 319
- ftp-gw application*, 343-348, 402-406
- Help*, 389-390
- http-gw application*, 354-359, 406-412
- installation*, 321-322
- login-sh application*, 412-413
- mailing lists regarding*, 390
- netacl application*, 329-333, 414-415
- netperm table*, 328-329, 390-394
- netscan utility*, 379
- newsgroups regarding*, 389
- plug-gw application*, 372-378, 416-417
- preparing for configuration*, 322-326
- preventing DNS spoofing*, 329
- report utilities*, 380-394
- rlogin-gw application*, 339-343, 418-419
- smap client application*, 349, 420-421
- smapd application*, 351, 421-423
- TCP/IP configurations*, 326-327
- tn-gw application*, 333-339, 423-426
- Web site*, 848
- x-gw application*, 359-360, 426-427
- vulnerability to SATAN, 475-476
- FIRST (Forum of Incident and Response Security Teams), 847
- flags (Kerberos tickets), 567-570
- flags field
  - Kerberos tickets, 572
  - KRB\_KDC\_REP message, 591
- Floppy Boot Records (FBRs), 756-757
  - viruses, 768-776
- floppy disks
  - BIOS parameter blocks, 755
  - boot records, 755
  - components, 754
  - File Allocation Tables, 755
  - formatting, 754
  - logical formats, 755
  - repairing (virus infections), 831
  - root directories, 755
- For Her Eyes Only messages (PGP), 676
- FORCE command-line option (PGP), 681
- forged datagrams (TCP/IP), 311-313
- Form virus, 780
- formatting floppy disks, 754
- Forum of Incident and Response Security Teams, *see* FIRST
- forums
  - The Computer Underground Digest, 203
  - SUN-NETS, 204
  - TCP-IP mailing list, 204
  - Unix security mailing list, 203
  - Usenet, 204
  - VIRUS-L security mailing list, 203
  - see also* mailing lists; newsgroups
- FORWARDABLE flag (Kerberos tickets), 567, 569-570, 584
- forwardable tickets (Kerberos), 569-570
- FORWARDED flag (Kerberos tickets), 567, 569-570, 584
- forwarding IP addresses
  - disabling for TIS Firewall Toolkit, 326-327
  - exploitation by hackers, 463
- fping command, exploitation by hackers, 447
- FQDN (fully qualified domain name), 17
- fragile superclasses (C++), 705
- Fremont network security evaluation system, 470
- from field (KRB\_KDC\_REQ message), 589
- FTP (File Transfer Protocol), 45-48, 149
  - access records (WTMP file), 147
  - anonymous mode, 45, 478
  - connections, logging (Windows NT), 162
  - daemon (Unix audit logs), 152
  - sites
    - Argus network management program*, 472
    - arpmon network monitoring software*, 292
    - ARPWatch 1.7 network monitoring software*, 292
    - binary files, integrity of*, 497-498
    - Bones*, 557



- CERT*, 846-847
  - CIAC group*, 846
  - COAST project*, 846
  - connecting to with TIS Firewall Toolkit applications*, 331-333, 347-348
  - DESlogin 1.3 zero-knowledge authentication software*, 278
  - EthDump sniffing software*, 260
  - FIRST*, 847
  - Fremont network security evaluation system*, 470
  - GateD route spoofing prevention software*, 299
  - Internet security-related*, 850-853
  - ISS network security evaluation program*, 470
  - netlog network monitoring software*, 292
  - netlog program*, 472
  - Netman sniffing software*, 260
  - network security-related*, 444
  - SATAN*, 499-500
  - Secure Shell program*, 474
  - socks IP encapsulation program*, 476
  - TCP wrappers (SATAN scan detection program)*, 472
  - TIS Firewall Toolkit*, 319
  - usage reports (TIS Firewall Toolkit)*, 386
  - Wietse Venema (co-creator of SATAN)*, 469
  - Xinetd SATAN scan detection program*, 472
  - versus rcp command*, 276
  - FTP proxy application, *see* ftp-gw application
  - ftp-gw application (TIS Firewall Toolkit), 343-348, 402
    - authentication, 405-406
    - configurations, 343-348
    - host access rules, 345-346
    - installation, 406
    - options, 403-405
    - rules, 344
    - verifying operation of, 346-347
  - ftpd
    - Kerberos, 610
    - password files, 489
    - scanning with SATAN, 478-480
    - servers, vulnerability to hackers, 449-451
    - vulnerability to hackers, 441-442
  - fully qualified domain name (FQDN), 17
  - functions
    - http-gw application (TIS Firewall Toolkit), 358
    - PGP key management, 650
- 
- ## G
- 
- Gabriel, SATAN scan detection program, 471
  - garbage collected heap (JVM stacks), 723
  - garbage collector (Java), 697, 706
  - GateD route spoofing prevention software, 299
  - gateways, 25
    - filtering packets, 201
    - routing tables, removing networks, 201
  - genUSER program, 142-143
  - GET method (CGI data input), vulnerability to hackers, 737-738
  - getty daemon, 59
  - Gopher
    - http-gw application functions (TIS Firewall Toolkit), 411
    - sites, connecting to with http-gw application (TIS Firewall Toolkit), 354-359
  - gtimes program, 140-142
- 
- ## H
- 
- hacking system security policies, 180-181
  - hard drives
    - MBR viruses, 757-758, 832
    - PBR viruses, 758-760, 833
    - partitioning, 757
  - hardware
    - address spoofing, 279-281
    - ARP spoofing prevention, 287
    - barriers for network segment security, 266-274

- Power-On Self Tests, 756
  - virus targets, 754
- hash functions, 200
- heads (floppy disks), 754
- Help (TIS Firewall Toolkit), 389-390
- heuristic scanners (antivirus utilities), 830-832
- history command, 153
- history logs (Unix audit logs), 153
- holes in network security, 438-443
  - detecting, 445-467
  - mailing lists regarding, 444
  - newsgroups regarding, 444
- HoneyDanBer (HDB) UUCP, 96
- hop counts (routers), 296
- host access rules (TIS Firewall Toolkit applications)
  - ftp-gw, 345-346
  - http-gw, 357
  - rlogin-gw, 342-343
  - tn-gw, 337-338
- host addresses (Kerberos), 605-606
- host equivalence files (password protection with rlogin), 275
- Host Equivalency, 21-22
- host records (SATAN databases), 528-529
- host tables, 12
- host-level active detection (ARP spoofing), 289
- host-level passive detection (ARP spoofing), 289
- hostname command, 13, 100
- hostnames
  - aliases, 17-18
  - assigning, 17-18
  - domain names, 13
  - guidelines, 13
  - hacker access to, 445-447
  - host tables, 12
  - hostname command, 13, 100
  - networks, 12-13
  - translating into IP addresses, 12
  - validating via UUCP Permissions file, 122
- hosts
  - addresses, 7-9
  - name resolution, 301
  - networks
    - services*, 19-20
    - traffic logs*, 156-157
  - hosts.equiv files (user accounts), vulnerability to hackers, 440
  - hosttype files (SATAN scan rulesets), 531
  - html directory (SATAN), 503
  - HTML interface (SATAN), 514-523
  - html/admin directory (SATAN), 508
  - html/data directory (SATAN), 508
  - html/docs directory (SATAN), 503-504
  - html/dots directory (SATAN), 504-505
  - html/images directory (SATAN), 505
  - html/reporting directory (SATAN), 505-506
  - html/running directory (SATAN), 506-507
  - html/tutorials directory (SATAN), 507
  - html/tutorials/vulnerability directory (SATAN), 507
- HTTP (Hypertext Transfer Protocol)
  - client applications
    - non-proxy aware*, 355-356
    - proxy aware*, 356
  - integration with Java, 729
  - restricting access to CGI scripts with, 736
- http-gw (HTTP proxy) application, TIS Firewall Toolkit, 354-359, 406-412
  - configurations, 354-359, 409-411
  - functions, 358
  - Gopher functions, 411
  - host access rules, 357
  - installation, 412
  - interaction with non-proxy aware HTTP clients, 355-356
  - interaction with proxy aware HTTP clients, 356
  - operations, 407-408
  - options, 407
  - reports, 386
  - rules, 355
  - security, 411-412
- httpd
  - Web site, 466
  - randomization (SSL), vulnerability to hackers, 440

servers (Unix audit logs), 153  
 Windows NT services, 163  
 https, vulnerability to hackers, 496  
 hubs, 281  
 HW-AUTHENT flag (Kerberos tickets),  
 568-570

## I

---

-i command option  
 finger, 32  
 netstat, 33  
 -I interface (netstat command options), 33  
 -i seconds (ping command option), 28  
 I/O (input/output) file descriptors for daemons,  
 61-62, 66-67  
 IBM PC viruses, 767-803  
 ICMP (Internet Control Message Protocol),  
 27, 294  
 ICMP ECHO\_REPLY, 27  
 ICMP ECHO\_REQUEST command, 27  
 ICMP PORT UNREACHABLE, 37  
 ICMP TIME\_EXCEEDED, 36  
 ICMP-based route spoofing, 294-296  
 IDEA cryptosystem, 635, 668, 683  
 identd servers, vulnerability to/exploitation by  
 hackers, 462  
 IEEE Technical Committee on Security &  
 Privacy, 208  
 ifconfig command, 15-17  
 -debug, 16  
 -arp, 16  
 arp, 16  
 broadcast, 16  
 configurable parameters, 15-16  
 debug, 16  
 dest-address, 16  
 down, 16  
 metric N, 16  
 netmask MASK, 16  
 querying interface configuration, 30-31  
 syntax, 15  
 -trailers, 16  
 trailers, 16  
 up, 16  
 illegal root access (networks), preventing, 437  
 improved overwriting COM file viruses, 787  
 include directory (SATAN), 501  
 inetd services, 20, 59  
 disabling, 324  
 restarting after configurations, 333  
 super-server, 26  
 info (syslog file severity level), 150  
 Info command (Java Appletviewer), 726  
 Information Systems Security Association, 208  
 init daemon, 55  
 initdefault (run level action field), 73  
 INITIAL flag (Kerberos tickets), 568, 570  
 initial tickets (Kerberos), 568  
 initialization, *see* system boot  
 insecure network segments, 270-271  
 inserting  
 comments in TIS Firewall Toolkit applica-  
 tions, 328  
 multiple static ARP cache entries, 286  
 static ARP cache entries, 286  
 installation  
 authmgr client application, 395  
 authsrv application (TIS Firewall Toolkit),  
 401-402  
 dfmon daemon, 74  
 ftp-gw application (TIS Firewall  
 Toolkit), 406  
 http-gw application (TIS Firewall  
 Toolkit), 412  
 login-sh application (TIS Firewall  
 Toolkit), 413  
 netacl application (TIS Firewall  
 Toolkit), 415  
 plug-gw application (TIS Firewall  
 Toolkit), 417  
 rlogin-gw application (TIS Firewall Toolkit),  
 420-421

- smap client application (TIS Firewall Toolkit), 349, 421
  - smapd application (TIS Firewall Toolkit), 351, 422-423
  - system security (configuration management), 195-196
  - TIS Firewall Toolkit, 321-322
  - tn-gw application (TIS Firewall Toolkit), 425-426
  - x-gw applications (TIS Firewall Toolkit), 427
  - installation files (virus infections), 839
  - instruction sets (JVMs), 720-721
  - integrity checkers (antivirus utilities), 824-825
  - INTERACTIVE configuration keyword (PGP), 679
  - interfaces
    - CGI, 732-736
    - Java, 705
    - localhost loopback, 17
    - networks, 14-15
      - configuring*, 15-17
      - names*, 14
      - PPP (Point-to-Point Protocol)*, 15
      - promiscuous mode*, 259
      - SLIP (Serial Line Internet Protocol)*, 15
      - sniffing*, 258-260
    - PGP for Unix, 687
    - querrying configuration, 30-31
    - SATAN, 514-523
    - system security (ethernet promiscuous mode), 158
  - International Traffic in Arms Regulation (ITAR), 547, 635
  - Internet, 7, 171
    - addresses, 7
    - boot record virus transmission, 805
    - Domain Name Server, 25
    - file virus transmission, 805
    - macro virus transmission, 806
    - RFC 950, 10
    - security
      - FTP sites regarding*, 850-853
      - newsgroups regarding*, 853-854
      - Web sites regarding*, 850-853
    - super-servers, starting daemons, 20
  - Internet Control Message Protocol, *see* ICMP
  - Internet Protocol, *see* IP
  - Internet Request for Comments (RFC), 13
  - Internet Threat Levels, *see* ITLs
  - Internet-to-Ethernet address translation table, 38
  - interpreters (Java), 715-718
  - INVALID flag (Kerberos tickets), 568
  - invalid tickets (Kerberos), 568
  - IP (Internet Protocol)
    - addresses, 7-9, 315
      - forwarding, disabling for TIS Firewall Toolkit*, 326-327
      - hacker access to*, 445-447
    - aliases, 19
    - forwarding, exploitation by hackers, 463
    - routing systems, spoofing, 293
    - source routing, exploitation by hackers, 463
    - spoofing (SATAN scans), 492-495
  - ISS (network security evaluation program), 470
  - ITAR (International Traffic and Arms Regulation), 547, 635
  - iterative replies (DNS servers), 302
  - ITLs (Internet Threat Levels) to network security, 432-435
- 
- ## J
- 
- Java, 693-695
    - applets
      - security modes*, 727-728
      - testing*, 703, 725-727
      - viewing with Netscape*, 728
    - Appletviewer, 725-727
    - architecture, 707-712
    - bytecodes, 699, 707, 717
    - calling class methods, 714

- cast statements, 705
  - class loader, 716-717
  - classes, 705
  - compiler, 703, 712-715
  - compiling with, 709, 712-715
  - components, 699
  - downloading classes, 715
  - dynamic loading capabilities, 708-709
  - e-mail interaction, 730
  - encryption protection, 715
  - environment features, 701-712
  - executing code, 718
  - garbage collector for memory, 697, 706
  - history of, 699-701
  - impact on firewalls, 729
  - integration with HTTP, 729
  - interfaces, 705
  - interpreter, 715-718
  - loading code, 716
  - memory layout, 714-715
  - memory management, 697, 706-707
  - multithreading capabilities, 699, 706, 710
  - Netscape runtime engine, 728
  - object-orientation, 698
  - opcodes, 713-714
  - operands, 713-714
  - performance levels, 695, 698
  - portability, 695-696
  - programming language features, 703-707
  - robustness, 695, 697, 709-710
  - running code, 715-718
  - runtime
    - checking*, 709
    - environment*, 702
    - memory layout*, 697
    - reference resolution*, 708
  - security, 694-698, 711-712, 724-730
  - socket interaction, 729
  - software support, 696
  - thread synchronization, 706
  - versus C++, 703-706
  - Web site, 730
- Java Virtual Machines, *see* JVMs
- JDK (Java Development Kit), 703
  - JVMs (Java Virtual Machines), 696, 707, 718-724
    - instruction set, 720-721
    - integrating with CPUs, 719
    - registers, 722
    - stacks, 722-724
      - constant pool memory area*, 724-730
      - execution environment*, 723
      - garabage collected heap*, 723
      - local variables*, 722-723
      - method memory area*, 724-730
      - operand stacks*, 723
- 
- ## K
- 
- kdc-options field (KRB\_KDC\_REQ message), 588
  - KDC\_ERR\_CANNOT\_POSTDATE message (Kerberos Authentication Services exchange), 576
  - KDC\_ERR\_ETYPE\_NOSUPP message (Kerberos Authentication Services exchange), 576
  - KDC\_ERR\_PREAUTH\_FAILED message (Kerberos Authentication Services exchange), 576
  - KDC\_ERR\_TRTYPE\_NOSUPP error message (Kerberos Ticket Granting Service exchange), 581
  - KEEPBINARY configuration keyword (PGP), 679
  - Kerberos network authentication system, 472-473, 536
    - accounting user accounts, 539
    - authenticating user accounts, 538-542
    - Authentication Service Exchange, 575-578, 584-591
    - authorizing user accounts, 539
    - Bones distribution, 556-557
    - checksums, 552-555
    - client detection of modified messages, 597-598

- client message encryption, 600-601
- client/server authentication exchange, 591-597
- clients, authenticating, 591-595
- DEC Ultrix distribution, 556-558
- encryption, 543-555
  - keys*, 550-551, 594-595
  - specifications*, 549-550
  - systems*, 551-552
- ftpd, 610
- host addresses, 605-606
- Key Distribution Center (client requests), 584
- KRB\_CRED message, 602-604
- KRB\_ERROR messages, 607-609
- KRB\_KDC\_REP message, 590-592
- KRB\_KDC\_REQ message, 586-590
- KRB\_PRIV message, 600-602
- KRB\_SAFE message, 597-600
- messages (authorization data), 606
- MIT version 4 distribution, 555
- MIT version 5 distribution, 556
- naming schemes, 605
- network realms, 537-538
  - intercommunication*, 565
  - naming*, 562-563
- newsgroups regarding, 611
- operations, 536-537
- OSF DCE security distribution, 556, 559
- port assignments, 609-610
- RFCs, 538
- sending credentials between hosts by clients, 602-603
- servers, 537, 563-564
- Telnet Authentication, 610
- Ticket Granting Service exchange, 578-591
- tickets, 536, 571-573
  - authentication*, 570
  - authenticators*, 573-574
  - expiration*, 577
  - fields*, 572-573
  - flags*, 567-570
  - forwardable*, 569-570
  - initial*, 568
  - invalid*, 568
  - postdated*, 569
  - preauthenticated*, 568
  - proxiable*, 569
  - proxied*, 569
  - renewable*, 568-569
  - requests via Authentication Service exchange*, 575-578
  - requests via Ticket Granting Service exchange*, 578-584
- time stamps, 605
- Transarc distribution, 556-559
- user authentication, 202
- vendors
  - interoperability issues*, 558-561
  - selecting*, 557
- version 4, 555-556
- version 5, 556, 559-561
- vulnerability to hackers, 542
- vulnerability to SATAN, 473
- Web site, 473, 848
- workstation authentication, 609-610
- kern (syslog file facility), 149
- Key Distribution Center (Kerberos client requests), 584
- key field
  - Kerberos tickets, 572
  - KRB\_CRED message, 604
  - KRB\_KDC\_REP message, 591
- key-expiration field (KRB\_KDC\_REP message), 591
- keyed checksums, 553
- keys (PGP)
  - adding to public key rings, 642-643, 654-656
  - distributing, 640-641
  - extracting from public key rings, 656-657
  - fingerprints, 663-664
  - generating, 639-640, 651-654
  - management, 650-665
  - naming, 646-647
  - pass phrases, 652, 683

- public key rings, 647
  - public key rings,
    - viewing contents*, 660-682
  - public key rings,
    - vulnerability to hackers*, 684-685
  - removing from key rings, 661-662
  - removing signatures from, 661-662
  - revoking, 664-665
  - secret key rings, 648
  - secret key rings,
    - viewing contents*, 660-661
  - secret key rings,
    - vulnerability to hackers*, 683-684
  - signing, 657-660
  - trust relationships, 648-650, 658
  - userids, creating, 652-654
  - verifying, 663-664
  - keytype fields (encryption keys), 551
  - keyvalue fields (encryption keys), 551
  - keywords (netacld application), TIS Firewall Toolkit, 330
  - kill command, 62
  - KRB\_AP\_REP message (Kerberos client/server authentication exchange), 594-597
  - KRB\_AP\_REQ message (Kerberos client/server authentication exchange), 592-596
  - KRB\_AS\_REP message (Kerberos Authentication Services exchange), 575
    - generation, 576-577
    - receipt, 577-578
  - KRB\_AS\_REQ message (Kerberos Authentication Services exchange)
    - generation, 576
    - receipt, 576
  - KRB\_CRED message (Kerberos), 602-604
  - KRB\_ERROR message
    - Kerberos Authentication Services exchange, 575
      - generation*, 578
      - receipt*, 578
    - Kerberos client/server authentication exchange, 597
      - Kerberos Ticket Granting Service exchange, 579
    - KRB\_ERROR messages (Kerberos), 607-609
    - KRB\_KDC\_REP message (Kerberos), 590-592
    - KRB\_KDC\_REQ message (Kerberos), 586-590
    - KRB\_PRIV message (Kerberos), 600-602
    - KRB\_SAFE message (Kerberos), 597-600
    - KRB\_TGS\_REP message (Kerberos Ticket Granting Service exchange), 579
      - generation, 581-583
      - receipt, 584
    - KRB\_TGS\_REQ message (Kerberos Ticket Granting Service exchange), 579
      - generation, 579-580
      - receipt, 580-581
    - kvno fields (encrypted messages), 549
- 
- L**
- 
- l command option
    - finger, 32
    - ruptime, 30
    - rsh, 42
  - L-devices (UUCP version 2 file), 96, 129-130
  - L-dialcodes (UUCP version 2 file), 97
  - L.cmds file (UUCP version 2), 137
  - L.sys (UUCP), 97, 131-133
  - L\_stat (UUCP version 2 file), 98
  - L\_sub (UUCP version 2 file), 98
  - lags field (KRB\_CRED message), 604
  - LANGUAGE configuration keyword (PGP), 679
  - last command, 147
  - last request fields (Kerberos Authentication Server exchange), 606-607
  - last-req field (KRB\_KDC\_REP message), 591
  - LAST\_ACK (socket state), 36
  - lastcomm command, 154
  - lastlog file (Unix audit log), 146
  - ldsocket daemon, 23
  - legal considerations
    - conflicts between law enforcement and sites, 231

- law enforcement contacts, 229-230
  - legal council, 230
  - log books, 232
    - procedures, 230-231
  - libpcap program, 463
  - libraries (CGI scripts), 735-736
  - license managers, 56
  - licensed software system policies, 180
  - link-state routing protocols, 296
  - LISTEN (socket state), 36
  - little endian coding, 721
  - loading code with Java, 716
  - local variables (JVM stacks), 722-723
  - local0-7 (syslog file facility), 149
  - localhost loopback interface, 17
  - LOCK (DOS audit trail utility), 165
  - lockd daemon, 60
  - log files
    - analyzing
      - asax program*, 158
      - chklastlog program*, 158
      - chkwtmp program*, 158
      - programs (code listings)*, 140-143
    - security problems, 166-167
    - system logs
      - evidence of tampering*, 166
      - fake entries*, 166
    - system security, 192
    - UUCP, 124-126
      - error messages*, 125-126
      - troubleshooting network connections*, 124
    - UUCP version 2, 137-138
    - Windows NT
      - Application Log*, 161
      - Security Log*, 162
      - System Log*, 162
      - TCP/IP applications*, 163-164
      - viewing*, 161-162
  - LOGFILE (UUCP version 2), 137
  - logging
    - access to specific files (Windows NT httpd service), 163
    - commands, 154-155
      - CPU time consumption, 155
      - crontab file usage, 151
      - dial-out facilities usage, 151
      - DOS utilities, 164
      - file system changes, 159
      - ftp connections (Windows NT), 162
      - logins, 146-148
        - messages, 148-150
        - netlog system sniffer, 159
        - system resource allocation, 155
        - user activity, 156
        - users, 150-151
        - utilities, tampering, 167
      - logical formats (floppy disks), 755
      - LOGIN FAILED (UUCP log file error message), 125
      - login-sh (authenticating login shell), TIS Firewall Toolkit, 412-413
      - logins, 59
        - anonymous (UUCP), 123-124
        - chat scripts (UUCP), 111-114, 132-133
        - CGI requests, 749
        - lastlog file, 146
        - prompts, 59
        - remote, 59
        - tracking, 146-148
        - UTMP file, 146-148
      - LOGNAME (Permissions file keyword), 119
      - logout (telnet command), 44
      - lpd daemon, 23, 56
      - LPD protocol, 56
      - lpd-errs file (Unix audit logs), 152
      - lpr (syslog file facility), 149
      - lpsched daemon, 56
      - ls command (UUCP Device file ownership), 105
      - lsdf program (open file listing), 158
- 
- M**
- m (netstat command options), 33
  - MACHINE (Permissions file keyword), 119
  - MacPGP, 689



- macro viruses, 765-767, 800-802, 806
  - Internet transmission, 806
  - peer-to-peer network infection, 806
  - preventing, 835-841
  - repairing, 835-841
  - server infection, 806
  - under Windows NT, 841
- mail (syslog file facility), 149
- Mail Transport Agent, 58
- mailing lists
  - 8lgm (networks security holes), 444, 848
  - bugtraq (network security holes), 444, 848
  - ftp sites, 207
  - network security hole-related, 444
  - system security, 203, 204, 207
  - TIS Firewall Toolkit-related, 390
- make install command (TIS Firewall Toolkit), 321
- makefiles (TIS Firewall Toolkit), editing under BSDI, 320
- MAKERANDOM command-line option (PGP), 681
- man command, 64
- marginal trust relationships (PGP keys), 649-650, 658
- MARGINALS\_NEEDED configuration keyword (PGP), 679
- mark (syslog file facility), 149
- Master Boot Records (MBRs), hard drives, 757-758
  - repairing virus infection, 832
  - viruses, 780-784
- Maxuuscheds (Basic Networking Utilities file), 97
- Maxuuxqts (Basic Networking Utilities file), 97
- MAY-POSTDATE flag (Kerberos tickets), 567-569
- MBRs (Master Boot Records), hard drives, 757-758
  - methods of virus infection, 835-837
  - preventing virus infection, 831
  - repairing virus infection, 831-832
  - viruses, 780-784
- MCBs (Memory Control Blocks), conventional memory storage, 790
- memory
  - conventional memory (DOS storage methods), 790
  - failures, troubleshooting, 35
  - Java garbage collector, 697, 706
  - layout with Java, 714-715
  - managing with Java, 697, 706-707
  - printing usage, 33-36
  - runtime layout with Java, 697
  - swapper daemons, 55
- Memory Control Blocks (MCBs), conventional memory storage, 790
- memory scanners (antivirus utilities), 820-821
- memory-resident viruses (DOS program files), 789, 796-797
- mesg command, 491
- messages
  - displaying error messages (UUCP), 114, 133
  - e-mail
    - clearsigning with PGP*, 674-675
    - compressing with PGP*, 666
    - conventional encryption with PGP*, 668
    - decrypting with PGP*, 644-645, 671-673
    - decrypting without saving to file*, 676
    - detached signatures with PGP*, 675-676
    - digital signatures*, 641-642, 665
    - encrypting with PGP*, 643-644, 665, 670-671
    - filtering with PGP*, 665-666
    - non-repudiation*, 641
    - public key encryption*, 669-670
    - sending with PGP*, 667
    - signing with PGP*, 668-671
    - verifying with PGP*, 644-645, 671-673
    - vulnerability to network sniffers*, 261
- Kerberos authorization data, 606
- logging, 148-150
- syslog (fake), 166
- system, logging, 26
- system monitoring, 69-70
- UUCP log file error messages, 125-126
- see also* audit trails; logging; reports

method memory area (JVM stacks), 724-730

methods (classes), calling with Java, 714

metric N command (ifconfig), 16

MIT Kerberos version 5, 556

MITSign Kerberos key signer for PGP, 687-688

MMDF mail system (deliver daemon), 59

mode (telnet command), 44

modems

- calling time scheduling
  - UUCP L.sys file*, 131
  - UUCP Systems file*, 109
- configuring
  - baud rates (UUCP systems)*, 110, 132
  - UUCP Devices file*, 103-105
- initiating calls, 106-108
- network security attacks, 467-476
- TCP connections, 488
- UUCP networks, specifying phone numbers, 110
  - UUCP Systems file (retry numbers), 109

modules (STREAMS), linking, 23

monitoring networks to detect ARP spoofing, 291-292

monoalphabetic substitutions (encryption), 624-627

mountd daemon, 60, 477

msg-type field

- KRB\_AP\_REQ message, 595
- KRB\_KDC\_REP message, 591
- KRB\_KDC\_REQ message, 587
- KRB\_PRIV message, 601
- KRB\_SAFE message, 599

msg-typeq field (KRB\_AP\_REP message), 596

multicast addresses, 8

multipartite viruses, 814

multitasking, 710

multithreading (Java capabilities), 699, 706, 710

mutual trust relationships (network segments), 269-270

MYNAME (Permissions file keyword), 121

MYNAME configuration keyword (PGP), 679

---

## N

-n command option

- netstat, 33
- ping, 28
- rsh, 42

Name (BNU Devices file field name), 103

name resolution (hosts), 301

named daemons, 25

names

- domains, 13
- network interfaces, 14
- UUCP system names, 100-102

naming

- PGP keys, 646-647
- realms (Kerberos), 562-563

National Computer Security Center (NCSC), 210-211

National Institute of Standards and Technology (NIST), 205

National Science Foundation, 6

National Security Act of 1947, 543

netacl (network access control) application, TIS Firewall Toolkit, 329-333, 414-415

- clauses, 330
- configurations, 329-333
- FTP connections, establishing, 331-333
- installation, 415
- options, 414-415
- reports, 386-387
- rules, 330
- starting, 329

netlog sniffer utility, 159, 292, 472

NetMan sniffing software, 260

netmask MASK command (ifconfig), 16

netmasks (addresses)

- defaults, 10
- determining for subnets, 12

netperm table (TIS Firewall Toolkit), 328-329, 390-394

.netrc network configuration file, 47

netscan utility (TIS Firewall Toolkit), 379

Netscape Java runtime engine, 728

- netstat command, 24, 33-36, 156-157, 325
- Network News Transport Protocol, *see* NNTP
- network-level active detection (ARP spoofing), 290
  - via continuous monitoring, 291-292
  - via periodic polling, 290-291
- networks
  - access points, 189
  - addresses, 7
    - octets*, 8-9
    - pinging with nescan utility (TIS Firewall Toolkit)*, 379
    - subnets*, 9-12
  - analyzers, 258
  - arpmon monitoring software, 292
  - ARPWatch 1.7 monitoring software, 292
  - autonomous systems, 295
  - bridges, 265, 274, 280
  - broadcast addresses, 259
  - brouters, 291
  - configuration files
    - /etc/ethers*, 18
    - /etc/fipusers*, 46
    - /etc/hosts*, 17-18
    - /etc/hosts.equiv*, 21
    - /etc/hosts.lpd*, 23
    - /etc/inetd.conf*, 20
    - /etc/networks*, 18-19
    - /etc/passwd*, 22
    - /etc/printcap*, 23
    - /etc/protocols*, 19
    - /etc/service*, 19-20
    - /etc/sockcf*, 23
    - /etc/strcf*, 23
    - /etc/syslog.conf*, 26
    - .netrc*, 47
    - .rhosts*, 21
  - connections
    - configuring (UUCP)*, 103-105
    - debugging*, 38
    - testing*, 106, 130-131
  - daemons, exploitation by hackers, 453
  - debugging, 106, 157
  - Ethernet sniffers, 157-158
  - extend access (illegal), 438-439
  - file systems
    - unprivileged access scans by SATAN*, 480-481
    - unrestricted exports, scanning with SATAN*, 481
    - vulnerability to hackers*, 459-460
  - gateway filtering packets, 201
  - hostnames, 12-13
  - hosts
    - name resolution*, 301
    - services*, 19-20
    - traffic logs*, 156-157
  - hubs, 281
  - inetd services, disabling, 324
  - interfaces, 14-15
    - configuring*, 15-17
    - names*, 14
    - PPP*, 15
    - promiscuous mode*, 259
    - SLIP*, 15
    - sniffing*, 258-260
  - IP routing systems, spoofing, 293
  - limiting access, 201
  - local machine status displays, 29-30
  - mailing lists, 204
  - memory, printing usage, 33-36
  - monitoring to detect ARP spoofing, 291-292
  - netlog monitoring software, 292
  - operating systems, hacker determination of
    - via telnetd information, 447-449
  - peer-to-peer networks
    - boot record viruses*, 805
    - file viruses*, 804
    - macro viruses*, 806
  - realms (Kerberos), 537-538
    - intercommunication*, 565
    - naming*, 562-563
  - remote shell access (SATAN scans), 483-485

- root access
  - hacker acquisition of, 437-438*
  - illegal, preventing, 437*
- routers, 266
  - hop counts, 296*
  - preventing ARP spoofing, 287*
- routing programs (exploitation by hackers), 461
- SATAN scans, detecting, 471-472
- secure links, 198
- security
  - attacks on, 431-444*
  - attacks on, acquiring login accounts, 436-437*
  - attacks on, acquiring root access, 437-438*
  - attacks on, characterizing, 435-438*
  - attacks on, extend access by hackers, 438-439*
  - attacks on, modem-based, 467-476*
  - classifications, 435*
  - detecting vulnerabilities via public documentation, 465-476*
  - evaluating for weaknesses, 466-476*
  - FTP sites regarding, 444*
  - hacker-generated patches, 466*
  - holes, 438-443*
  - holes, detecting, 445-467*
  - holes, mailing lists regarding, 444*
  - holes, newsgroups regarding, 444*
  - improving with firewalls, 475-476*
  - improving with Kerberos, 472-473*
  - improving with Secure Shell program, 474*
  - improving with SSL, 474-475*
  - Internet Threat Levels, 432-435*
  - low-cost solutions, 272*
  - SATAN searches for breaches, 434*
  - scanning with SATAN, 477-478*
  - testing with SATAN, 430-431*
  - Web sites regarding, 444*
- segmenting to prevent sniffing, 265-266
- segments
  - insecure, 270-271*
  - mutual trust relationships, 269-270*
  - one-way trust relationships, 270-271*
  - secure, 268-269*
  - trust relationships, 266-274*
- services
  - denial reports (TIS Firewall Toolkit), 385*
  - reducing active processes, 323*
  - SATAN scans, 478*
  - status displays, 322*
  - vulnerability to hackers, 498*
- shared media, 259
- sniffing, 257-279
  - as an administration tool, 259*
  - e-mail vulnerability, 261*
  - exploitation by hackers, 462-463*
  - financial account vulnerability, 261*
  - operations, 258-260*
  - password protection from, 274-279*
  - password vulnerability, 261*
  - preventing, 265-274*
  - protocol vulnerability, 262-265*
  - software, 259*
  - threats to security, 260-262*
- SNMP (Windows NT), logging local activity, 163
- spoofing, 258, 279-316
  - ARP spoofing, 281-292*
  - bridge vulnerability, 280*
  - DNS spoofing, 301-309*
  - hardware addresses, 279-281*
  - ICMP-based route spoofing, 294-296*
  - RIP-based, 297-298*
  - TCP-based spoofing, 309-316*
  - tracing, 280*
- statistic displays, 325
- subnetting to prevent ARP spoofing, 287
- subsystems, querying, 33-36
- Sun Microsystems addresses, 9
- switches, 265
- trust-based, vulnerability to hackers, 485
- types, 14
- user accounts
  - hacker acquisition of, 436-437*
  - password cracking, 436*

- vulnerability to viruses, 803-805
  - workstations
    - password protection*, 269
    - security*, 269
    - see also* octets; subnets
  - news (syslog file facility), 149
  - newsgroups
    - connecting to with plug-gw application (TIS Firewall Toolkit), 373-376
    - Internet security-related, 853-854
    - Kerberos-related, 611
    - network security hole-related, 444
    - TIS Firewall Toolkit-related, 389
  - NFS (Network File System)
    - servers
      - daemons*, 60
      - vulnerability to hackers*, 442
    - unprivileged access (SATAN scans), 480-481
    - unrestricted exports, scanning with SATAN, 481-482
  - NFS watch utility, 159
  - nfsbug program (hacking network file systems), 459
  - nfsd daemon, 60
  - nfsmenu program (hacking network file systems), 459
  - nfsshell program (hacking network file systems), 459
  - NIS servers
    - exploitation by hackers, 460
    - passwd files, SATAN scans, 482
    - password protection, 489
    - SATAN scans, 482
    - vulnerability to hackers, 460
  - NNTP (Network News Transport Protocol), 373-376
    - connections with plug-gw application (TIS Firewall Toolkit), 373-376
    - vulnerability to/exploitation by hackers, 461
  - No Access security mode (Java applets), 727
  - NO CALL (RETRY TIME NOT REACHED), UUCP log file error message, 125
  - NO DEVICES AVAILABLE (UUCP log file error message), 126
  - no trust relationships (PGP keys), 649-650, 658
  - nobody UIDs (CGI scripts), 739
  - nodename, 100
  - non-proxy aware HTTP clients, interaction with http-gw, 355-356
  - non-repudiation (e-mail messages), 641
  - nonce field
    - KRB\_CRED message, 604
    - KRB\_KDC\_REP message, 591
    - KRB\_KDC\_REQ message, 589
  - NOREAD (Permissions file keyword), 120
  - notice (syslog file severity level), 150
  - NSFNet, 6
  - nslookup program, 25, 446
  - NULL encryption systems, 551
  - NWRITE (Permissions file keyword), 120
  - NYB virus, 783
- 
- ## O
- 
- object-oriented programming with Java, 698
  - octets (addresses), 8-9
  - OFB (Output Feedback Mode) encryption, 546
  - off (run level action field), 73
  - OK (UUCP log file error message), 126
  - ONC clients (RPC server support), 60
  - once (run level action field), 73
  - ondemand (run level action field), 73
  - one-time password programs, 490
  - one-way trust relationships (network segments), 270-271
  - online documentation (SATAN), 522-523
  - OOP (object-oriented programming) with Java, 698
  - opcodes (Java), 713-714
  - open (telnet command), 44
  - operand stacks (JVMs), 723
  - operands (Java), 713-714
  - operating systems
    - networks, hacker determination of via telnetd information, 447-449

obtaining bug fixes, 211-212  
 secure, 210-211  
 Orange Book (Department of Defense system classification), 435  
 OSF DCE Kerberos-based security, 556, 559  
 overwriting COM file viruses, 786

## P

---

-p command option  
 finger, 32  
 rcp, 41  
 -p pattern (ping command option), 28  
 -p protocol-name (netstat command options), 33  
 packet sniffer programs, 496  
 packets  
 RIP security issues, 491  
 sniffing, exploitation by hackers, 462-463  
 padata field  
 KRB\_KDC\_REP message, 591  
 KRB\_KDC\_REQ message, 587  
 padata-type field (KRB\_KDC\_REQ message), 588  
 PAGER configuration keyword (PGP), 679  
 Partition Boot Records (PBRs), hard drives, 758-760  
 repairing virus infection, 833  
 viruses, 776-780  
 partitioning hard drives, 757  
 pass phrases (PGP keys), 638, 652, 683  
 passive DNS spoofing attacks, 306  
 -passok host access rule (tn-gw application), TIS Firewall Toolkit, 338  
 password files (genUSER program), 142-143  
 password protected workstations, 269  
 passwords  
 backdoor, 167  
 equivalency, 21-23  
 FTP access, 46-48  
 ftpd, 489  
 NIS servers  
*protecting*, 489  
*SATAN scans*, 482  
 one-time, 490  
 policies, changing passwords, 217  
 protecting from sniffing, 274-279  
*with encryption*, 277-278  
*with rlogin*, 275-277  
*with Secure RPC*, 278  
*with symmetric encryption*, 279  
*with zero-knowledge authentication*, 278  
 protection, 488-490  
 rlogin protocol (sniffer protection), 275-277  
 selecting, 182, 215-217  
 selection enforcement programs, 490  
 shadow files, 489  
 smart card security programs, 202, 490  
 standard, 195  
 system management, 215  
 system security, 157, 175, 178  
 user accounts, cracking, 436  
 vulnerability  
*to hackers*, 217  
*to network sniffers*, 261  
 patches (network security), hacker-generated, 466  
 patimestamp field (KRB\_KDC\_REQ message), 588  
 pausec field (KRB\_KDC\_REQ message), 588  
 PBRs (Partition Boot Records), hard drives, 758-760  
 preventing virus infection, 831  
 repairing virus infection, 831-833  
 viruses, 776-780  
 PC/DACS (DOS audit trail utility), 164-165  
 pcnfsd daemon, 60  
 PCs  
 converting to network bridges, 274  
 viruses, 767-803  
 peer-to-peer networks  
 boot record viruses, 805  
 file viruses, 804  
 macro viruses, 806

- periodic polling, network-level ARP spoofing detection, 290-291
- PERL programming language
  - CGI libraries, 735
  - CGI programming, 743-746
  - daemons, creating, 65-70
- perl directory (SATAN), 512-513
- perllib directory (SATAN), 502
- permission files (UUCP version 2), 134-137
- permissions (special access), UUCP version 2, 136
- Permissions files (Basic Networking Utilities file), UUCP, 97, 118-119
  - anonymous login, 123-124
  - defaults, 118-119
  - entry rules, 121
  - keywords, 119-121
  - validating hostnames, 122
- PGP (Pretty Good Privacy) encryption program, 633-634
  - add-on utilities, 686-689
  - armor mode, 667
  - binary files
    - distribution*, 637-639
    - vulnerability to hackers*, 685
  - brute force hacker attacks, 682-683
  - clearsigning e-mail messages, 674-675
  - compressing e-mail messages, 666
  - configurations, 677-682
  - conventional encryption, 668
  - decrypting e-mail messages, 644-645, 671-673, 676
  - detached signatures, 675-676
  - encrypting e-mail messages, 643-644, 670-671
  - filtering e-mail messages, 665-666
  - For Her Eyes Only messages, 676
  - history of, 634-636
  - integration with Unix mailers, 688
  - keys
    - adding to public key rings*, 642-643, 654-656
    - distributing*, 640-641
    - extracting from public key rings*, 656-657
    - fingerprints*, 663-664
    - generating*, 639-640, 651-654
    - management*, 650-665
    - naming*, 646-647
    - pass phrases*, 652, 683
    - public key rings*, 647, 661-682
    - public key rings, viewing contents*, 660-682
    - public key rings, vulnerability to hackers*, 684-685
    - removing from key rings*, 661-662
    - removing signatures from*, 661-662
    - revoking*, 664-665
    - secret key rings*, 648
    - secret key rings, viewing contents*, 660-661
    - secret key rings, vulnerability to hackers*, 683-684
    - signing*, 657-660
    - trust relationships*, 648-650, 658
    - userid*, creating, 652-654
    - verifying*, 663-664
- Macintosh compatible, 689
- MITSign (Kerberos key signer), 687-688
- pass phrases, 638
- practical applications, 635-636
- processing binary files, 666-667
- processing text files, 666-667
- public key servers, 686-687
- security, 682-685
- sending e-mail messages, 667
- signing e-mail messages, 668-671
- Unix interface, 687
- verifying e-mail messages, 644-645, 671-673
- Windows front-end applications, 688
- wiping files, 676-677
- PGPMenu Unix interface for PGP, 687
- Phone (BNU Systems file field name), 110
- PIDs (process identifiers), procuring, 324
- ping command, 27-29
  - BSD Unix, 29
  - fault isolation, 29
  - options, 27-28

- pinging
    - network addresses with netscan utility (TIS Firewall Toolkit), 379
    - servers to determine firewall/Internet connections, 447
  - PKE (public key encryption), 636
  - plug-gw (plugboard connectivity) application, TIS Firewall Toolkit, 372-378, 416-417
    - bugs, 417
    - clauses, 372-373
    - configurations, 372-373
    - installation, 417
    - NNTP connections, 373-376
    - POP connections, 376-378
    - rules, 372-373
  - pname field (KRB\_CRED message), 604
  - point-of-contact persons (system security), 228-229
  - point-to-point leased lines, 6
  - Point-to-Point Protocol (PPP), 15
  - policies, *see* system security, policies
  - Poll (Basic Networking Utilities file), 97
  - polling (periodic), network-level ARP spoofing detection, 290-291
  - polymorphic viruses, 807
  - POP (Post Office Protocol), 376-378
  - portability (Java), 695
  - portmap program
    - exploitation by hackers, 454-455
    - forwarding (SATAN scans), 482-483
    - rexed services, vulnerability to hackers, 463
    - secure, 455
    - vulnerability to hackers, 442
  - ports
    - connecting to TCP ports, 45
    - Kerberos assignments, 609-610
    - scanning by SATAN, 465
    - TCP, scanning by hackers, 453-454
    - UDP, scanning by hackers, 453-454
  - portscan utility (TIS Firewall Toolkit), 325, 378
  - POST method (CGI data input), vulnerability to hackers, 737-738
  - Post Office Protocol, 376-378
  - POSTDATED flag (Kerberos tickets), 585, 568-569
  - postdated tickets (Kerberos), 569
  - POSTs (Power-On Self Tests), hardware, 756
  - PostScript files, viewing to prevent hacker attacks, 498
  - pound symbol (#) in network configuration files, 18
  - powerfail (run level action field), 73
  - powerwait (run level action field), 73
  - PPP (Point-to-Point Protocol), 15
  - PRE-AUTHENT flag (Kerberos tickets), 568-570
  - prealm field (KRB\_CRED )message, 604
  - preauthenticated tickets (Kerberos), 568
  - prepending COM file viruses, 785
  - Pretty Good Privacy, *see* PGP encryption
  - program
    - preventing
      - ARP spoofing, 284-287
        - with ARP servers*, 286
        - with hardware barriers*, 287
        - with permanent cache entries*, 285-286
      - boot record viruses, 831
      - DNS spoofing, 303, 306-309
      - DOS program file viruses, 833-834
      - ICMP-based route spoofing, 294
      - illegal root access, 437
      - macro viruses, 835-841
      - RIP-based spoofing, 298-300
    - sniffing
      - with hardware barriers*, 266-274
      - with network segmentation*, 265-266
      - with trust relationships*, 266
  - TCP connections to local services from remote systems, 454
  - TCP/IP spoofing, 314-315
  - UDP connections to local services from remote systems, 454
- principal names (Kerberos servers), 564
- print command, 66-67



- print spoolers, 56
- printer error logs, 152
- printing
  - lpd daemon, 56
  - network memory usage, 33-36
  - print spoolers, 56
  - spool area handler, 23
- private key encryption, 545
- probes, 37
- process accounting
  - enabling, 154
  - files (disk space consumption), 154
  - reports, 154-155
  - Unix audit logs, 153
- process identifiers (PIDs), procuring, 324
- process table, 50-51
- processes
  - listing files in use, 158
  - logging daemons, 68
  - monitoring daemons, 67-70
  - network services, reducing activity, 323
  - reports, 156
- processing
  - binary files with PGP, 666-667
  - text files with PGP, 666-667
- procmon command, 82
- procmon daemon, 67-70
- procmon.cfg configuration file, 68-69
- procmon.cmd configuration file, 68
- procuring PIDs, 324
- professional societies/journals related to system security, 208-214
- Program Segment Prefixes (PSP), 790
- programming CGI scripts
  - in C, 746
  - in C++, 746
  - in PERL, 743-746
  - in safe languages, 746-747
- programs
  - compared to daemons, 50
  - daemons, 7
- promiscuous mode (network interfaces), 259
- Properties command (Java Appletviewer), 726
- “Protect and Proceed” policy, 186-187
- protecting
  - IP addresses from spoofing, 494-495
  - passwords, 488-490
    - from sniffing*, 274-279
    - from sniffing with encryption*, 277-278
    - from sniffing with rlogin*, 275-277
    - from sniffing with Secure RPC*, 278
    - from sniffing with symmetric encryption*, 279
    - from sniffing with zero-knowledge authentication*, 278
- protocols
  - address resolution protocol, 38
  - ARP
    - caches, deleting entries*, 286
    - caches, displaying entries*, 285
    - caches, inserting multiple static entries*, 286
    - caches, inserting static entries*, 286
    - caches, permanent entries*, 285
    - servers*, 286
    - spoofing*, 281-284
    - spoofing, detecting*, 288-292
    - spoofing, preventing*, 284-287
  - boot, implementing, 24
  - DARPA, 19
  - embedding Kerberos tickets, 536
  - external routing protocols, 296, 300
  - File Transfer Protocol, 45-48
  - HTTP
    - integration with Java*, 729
    - restricting access to CGI scripts with*, 736
  - ICMP, 27, 294
  - IP, encryption, 315
  - link-state routing protocols, 296
  - LPD, 56
  - NNTP
    - connections with plug-gw application (TIS Firewall Toolkit)*, 373-376
    - vulnerability to exploitation by hackers*, 461

- POP, 376-378
- PPP, 15
- privacy enhanced mail, 199
- RIP, 296
  - security issues*, 491
  - spoofing*, 297-298
- rlogin
  - drawbacks*, 276-277
  - protecting passwords from sniffers*, 275-277
- RMON, 292
- routing protocols, 295-296
- SNMP, 24
- SPF, 296
- SSL, 440
- TCP
  - ACK flags*, 311
  - connection setup*, 310
  - data exchange*, 311
  - SATAN scans*, 477
  - spoofing*, 309-316
  - SYN flags*, 310
- TCP/IP, 7, 311
  - configuring for TIS Firewall Toolkit*, 326-327
  - forged datagrams*, 312-313
  - terminal hijacking*, 313-314
- TELNET, 43
- UDP (SATAN scans), 477
- vector-distance routing protocols, 296
- vulnerability to network security
  - attacks, 432
- vulnerability to network sniffers, 262-265
- Xerox NS Routing Information Protocol, 24, 59
- PROXIABLE flag (Kerberos tickets), 567, 569, 584
- proxiable tickets (Kerberos), 569
- proxied tickets (Kerberos), 569
- proximity settings (SATAN scans), 522
- proxy aware HTTP clients, interaction with
  - http-gw, 356
- PROXY flag (Kerberos tickets), 567-569, 585
- ps command, 50, 155
- PSP (Program Segment Prefixes), conventional
  - memory storage, 790
- pty files (security issues), 490-491
- PUBDIR (Permissions file keyword), 121
- public key cryptosystems, 199, 277, 544, 636, 669-670
- public key rings (PGP), 647
  - adding keys to, 654-656
  - extracting keys from, 656-657
  - viewing contents, 660-682
  - vulnerability to hackers, 684-685
- public keyservers (PGP), 686-687
- public relations (security breaches), 225-226
- PUBRING configuration keyword (PGP), 680
- “Pursue and Prosecute” policy, 186-187
- pvno field
  - KRB\_AP\_REP message, 596
  - KRB\_AP\_REQ message, 595
  - KRB\_KDC\_REP message, 591
  - KRB\_KDC\_REQ message, 587
  - KRB\_PRIV message, 601
  - KRB\_SAFE message, 599
- Python CGI programming language, 747

---

## Q-R

- q command option
  - finger, 32
  - ping, 28
- question mark (?)
  - process tables, 51
  - telnet command, 44
- quit (telnet command), 44
- r command option
  - netstat, 33
  - ping, 28
  - rcp, 41
  - ruptime, 30
- r-address field
  - KRB\_CRED message, 604
  - KRB\_SAFE message, 600
- r-commands (rlogin protocol), 276

- R\_stat (UUCP version 2 file), 98
- R\_sub (UUCP version 2 file), 98
- RANDSEED configuration keyword (PGP), 680
- RARP (Reverse Address Resolution Protocol), 24
- RARP daemon, 24
- rcmd command, 43
- rcp command, 41, 276
- READ (Permissions file keyword), 120
- realm field
  - Kerberos tickets, 572
  - KRB\_KDC\_REQ message, 589
- realms (Kerberos), 537-538
  - intercommunication, 565
  - naming, 562-563
- records
  - log books, 222-223
  - SATAN databases, 525-529
- recursive replies (DNS servers), 302
- registers (JVMs), 722
- Registry Editor (Windows NT), 162
- Reload command (Java Appletviewer), 726
- remote command execution, 137
- REMOTE DOES NOT KNOW ME (UUCP log file error message), 126
- REMOTE HAS A LCK FILE FOR ME (UUCP log file error message), 126
- remote hosts, connecting to with rlogin-gw application (TIS Firewall Toolkit), 342
- remote login, 59
- Remote Procedure Calls, *see* RPCs
- REMOTE REJECT AFTER LOGIN (UUCP log file error message), 126
- REMOTE REJECT, UNKNOWN MESSAGE (UUCP log file error message), 126
- remote shell access (SATAN scans), 483-485
- remote.unknown file (UUCP), anonymous login, 123
- removing
  - PGP keys from key rings, 661-662
  - signatures from PGP keys, 661-662
- RENEW field (Kerberos tickets), 586
- renew-till field
  - Kerberos tickets, 572
  - KRB\_CRED message, 604
  - KRB\_KDC\_REQ message, 591
- RENEWABLE flag (Kerberos tickets), 568-570, 585
- renewable tickets (Kerberos), 568-569
- RENEWABLE-OK field (Kerberos tickets), 585
- repairing
  - boot record viruses, 831
  - DOS program file viruses, 833-834
  - infected floppy disks, 831
  - infected MBRs, 832
  - macro viruses, 835-841
  - stealth virus-infected files, 834
- report utilities (TIS Firewall Toolkit), 380-394
- reports
  - network connections, 156-157
  - open files (lsop program), 158
  - post-incident, 234
  - process accounting, 154-155
  - processes, 156
  - SATAN scans, 518-520
  - security breaches, follow up analysis, 228
  - system access, sorting, 148
  - system activity, 147-148
  - system resource allocation, 155
  - system security
    - procedures*, 195-197
    - tools*, 209-210
- TIS Firewall Toolkit applications
  - authentication server*, 384-385
  - FTP site usage*, 386
  - http-gw*, 386
  - netacl*, 386-387
  - network service denials*, 385
  - rlogin-gw*, 388-389
  - smap*, 387-388
  - tn-gw*, 388-389
  - see also* audit trails; logging; messages
- req-body field (KRB\_KDC\_REQ message), 588

- REQUEST (Permissions file keyword), 119
- requests (tickets)
  - via Authentication Service exchange, 575-578
  - via Ticket Granting Service exchange, 578-584
- require command, 69
- reserved addresses, 9
- RESERVED flag (Kerberos tickets), 567-568, 585-586
- respawn (run level action field), 73
- response tactics
  - containment, 227
  - damage assessment, 234
  - eliminating causes, 227, 233
  - follow up analysis, 227, 234
  - log books, 234
  - system cleanup, 234
  - system recovery, 227
- response teams (system security), 204-205, 226
- Restart command (Java Appletviewer), 726
- restarting inetd after configurations, 333
- restricting
  - CGI access, 736, 739
  - SSI access, 742
- retro viruses, 813-814
- Reverse Address Resolution Protocol (RARP), 18
- revoking PGP keys, 664-665
- rexd services (portmap programs)
  - SATAN scans, 485
  - vulnerability to hackers, 463
- RFCs (request for comments), 538
  - Kerberos, 538
  - RFC 1244 (Site Security Handbook), 169-253
  - RFC 950 (Internet), 10
- .rhosts network configuration file, 21
- rhosts files, password protection with rlogin, 275
- RIP (Routing Information Protocol), 296
  - RIP-based spoofing, 297-300
  - security issues, 491
- RISC (Reduced Instruction Set Computing) CPUs, 719
- rlogin command, 40, 43
  - drawbacks, 276-277
  - protecting passwords from sniffers, 275-277
- rlogin-gw application (TIS Firewall Toolkit), 418-419
  - clauses, 340
  - configurations, 339-343
  - connecting to remote hosts, 342
  - host access rules, 342-343
  - installation, 420-421
  - options, 418-419
  - reports, 388-389
  - rules, 340
  - verifying operations, 343
- rlogind daemon, 59
- RMON protocol, 292
- ROM-based software (virus infection), 760-762
- root access (networks)
  - hacker acquisition of, 437-438
  - illegal, preventing, 437
- root directories (floppy disks), 755
- rootkit program (hacker coverup), 438
- routed daemon, 24-25, 59
- routers (addresses), 10, 266
  - hop counts, 296
  - preventing ARP spoofing, 287
- routes
  - dynamic, 25
  - probes, 37
  - static, 25
  - tracing, 36-37
- Routing Information Protocol, *see* RIP
- routing metric, 16
- routing programs, exploitation by hackers, 461
- routing protocols, 295-296
- routing systems (IP), spoofing, 293
- routing tables, 24-25, 59
  - querying, 33
  - removing networks, 201
- rpc.statd daemon, 60
- rpcbind programs, 455
- RPCs (Remote Procedure Calls)
  - SATAN scans, 477
  - Secure RPC, 278

- RSA cryptography
    - hacking, 682-683
    - Web site, 848
    - see also* PGP, keys
  - rsa-md4 checksums, 554
  - rsa-md4-des checksums, 554
  - rsa-md4-des-k checksums, 554
  - rsa-md5 checksums, 554
  - rsa-md5-des checksums, 554
  - rsh command, 42, 276
  - rtime field (KRB\_KDC\_REQ message), 589
  - rules (TIS Firewall Toolkit applications), 328
    - authsrv, 362-363
    - ftp-gw, 344
    - http-gw, 355
    - netacl, 330
    - plug-gw, 372-373
    - rlogin-gw application, 340
    - smap client, 350
    - smapd, 352
    - tn-gw, 334-335
    - writing, 339
  - rules directory (SATAN), 501
  - rulesets (SATAN scans), 529-532
  - run levels, 55, 71-74
    - action fields, 72-74
    - adjusting, 71
    - SCO OpenServer 5.0, 71-72
    - viewing current, 74
  - running
    - CGI scripts
      - from controlled file system Web servers, 740*
      - under program owner UIDs, 740-741*
      - with minimum privileges, 739-740*
    - code with Java, 715-718
    - SATAN from Web browsers, 487-488
    - SATAN scans, 524-525
  - runtime (Java)
    - checking, 709
    - environment, 702
    - memory layout, 697
    - reference resolution, 708
  - ruptime command, 29-30
  - rusers program, exploitation by hackers, 457-459
  - rwall program
    - RPC services, 491
    - vulnerability to hackers, 443
  - rwho command
  - RWHO daemon, 26
  - rwho program, 30, 457-459
- 
- ## S
- 
- s command option
    - finger, 32
    - netstat, 33
  - s packetize (ping command option), 28
  - s host address (arp command options), 38
  - s-address field
    - KRB\_CRED message, 604
    - KRB\_SAFE message, 600
  - S/KEY zero-knowledge authentication
    - software, 278
  - sa command, 155
  - safe languages (CGI programming), 746-747
  - safe-body field (KRB\_SAFE message), 599
  - safecgiperl CGI programming language, 747
  - SATAN (network security program), 430-431, 468
    - Admin Guide to Cracking documentation, 523
    - benefits of, 534
    - building, 513-534
    - CIAC Web site, 470
    - components, 468
    - configurations, 520-522
    - Control Panel, 515
    - databases, 516
      - facts records, 525-528*
      - host records, 528-529*
      - records, 525-529*
      - todo records, 529*
    - detecting scans by, 471-472

## directories

- bin*, 502-503
- config*, 501
- html*, 503
- html/admin*, 508
- html/data*, 508
- html/docs*, 503-504
- html/dots*, 504-505
- html/images*, 505
- html/reporting*, 505-506
- html/running*, 506-507
- html/tutorials*, 507
- html/tutorials/vulnerability*, 507
- include*, 501
- perl*, 512-513
- perllib*, 502
- rules*, 501
- src*, 508
- src/boot*, 508
- src/ftping*, 510-511
- src/misc*, 509
- src/nfs-chk*, 509
- src/port\_scan*, 510
- src/rpcgen*, 511
- src/typ-chk*, 511-512
- top-level*, 500

## downloading, 499-500

FTP sites, 499-500

history of, 468-469

HTML interface, 514-523

impact on network security, 470-471

online documentation, 522-523

Reference documentation, 523

running from Web browsers, 487-488

## scans

*extensions, adding*, 532-534*ftpd*, 478-480*heavy*, 478*IP spoofing*, 492-495*light*, 477*NIS servers*, 482*normal*, 477-478*portmap program forwarding*, 455, 482-483*ports*, 465*proximity settings*, 522*remote shell access*, 483-485*result reports*, 518*rexid services*, 485*rulesets*, 529-532*running*, 524-525*selecting targets*, 517-518*sendmail program*, 485-486*servers for remote access services*, 454*ftpd file access*, 483*unprivileged NFS access*, 480-481*unrestricted NFS exports*, 481-482*X servers*, 486-487

searching for potential network security

breaches, 434

vendor reaction to, 470-476

versus other network security evaluation

programs, 470

Vulnerabilities Tutorials docu-

mentation, 523

## scanning

*ftpd with SATAN*, 478-480

network security with SATAN, 477-478

ports with SATAN, 465

TCP ports by hackers, 453-454

TCP services with portscan, 325, 378

UDP ports by hackers, 453-454

Web servers for vulnerability, 460

## scans (SATAN)

*extensions, adding*, 532-534*ftpd*, 478-480*heavy*, 478*IP spoofing*, 492-495*light*, 477*NIS servers*, 482*normal*, 477-478*portmap program forwarding*, 455, 482-483*ports*, 465*proximity settings*, 522*remote shell access*, 483-485*result reports*, 518*rexid services*, 485

- rulesets, 529-532
- running, 524-525
- selecting targets, 517-518
- sendmail program, 485-486
- servers for remote access services, 454
- tftpd file access, 483
- unprivileged NFS access, 480-481
- unrestricted NFS exports, 481-482
- X servers, 486-487
- SCO OpenServer 5.0 run levels, 71-72
- SCO Unix operating system
  - dialer programs, 106
  - /etc/inetd.config file, 20
- sco\_cpd daemon, 56
- scripts (chat), 107-108
- searchlists (DNS), security issues, 492
- secret key encryption, 544-545, 636
- secret key rings (PGP), 648, 661
  - viewing contents, 660-661
  - vulnerability to hackers, 683-684
- SECRING configuration keyword (PGP), 680
- sectors (floppy disks), 754
- secure links, 198
- secure network segments, 268-269
- secure portmap programs, 455
- Secure RPC, 278
- secure rpcbind programs, 455
- Secure Shell program (network security), 474
- Secure Sockets Layer, *see* SSL protocol
- Security Coordination Center (SCC), 205
- Security Log (Windows NT), 162
- segmenting networks to prevent sniffing, 265-266
- segments (networks)
  - insecure, 270-271
  - mutual trust relationships, 269-270
  - one-way trust relationships, 270-271
  - secure, 268-269
  - trust relationships, 266-274
- send (telnet command), 44
- SENDFILES (Permissions file keyword), 119
- sending e-mail messages with PGP, 667
- sendmail daemon, 7, 45, 58
  - bounce to program hole, 439
  - C option, vulnerability to hackers, 443
  - d debug hole, 439
  - exploitation by hackers, 451-453
  - SATAN scans, 485-486
  - syslog buffer, vulnerability to hackers, 439
  - Unix audit logs, 151
  - vulnerability to hackers, 58, 451-453
  - Web site, 466
- sendmail proxy application, *see* smap client application; smapd application
- seq-number field
  - Kerberos ticket authenticators, 574
  - KRB\_SAFE message, 599
- SEQF (UUCP version 2 file), 98
- Serial Line Internet Protocol, *see* SLIP
- Server Side Includes (SSI)
  - access restrictions, 742
  - alternatives to, 742-743
  - CGI scripts, 742-743
- server-level active detection (ARP spoofing), 289-290
- servers
  - ARP servers, 286
  - authentication server (TIS Firewall Toolkit), 360-372
  - boot record viruses, 805
  - bootpd servers, vulnerability to hackers, 455-457
  - DNS name servers, 302
    - BIND software*, 308
    - caches*, 303
    - cross-checking*, 303
    - security weaknesses*, 305
  - exploitation by hackers, 455-457
  - file viruses, 803-804
  - ftpd servers, vulnerability to hackers, 449-451
  - hostnames, vulnerability to hackers, 445-447
  - identd servers, vulnerability to/exploitation by hackers, 462

- inetd super-server, 26
- Kerberos
  - authentication servers*, 537
  - principal names*, 564
  - protection*, 472-473
- macro viruses, 806
- NFS servers, vulnerability to hackers, 442
- NIS servers
  - exploitation by hackers*, 460
  - password protection*, 489
  - SATAN scans*, 482
  - vulnerability to hackers*, 460
- pinging to determine firewall/Internet connections, 447
- remote, updating remote server database, 26
- SNMP servers, vulnerability to/exploitation by hackers, 464-465
- starting, 59
- Web servers
  - CGI request logins*, 749
  - CGI security issues*, 740
  - CGI trust relationships*, 736
  - converting from root to controlled file systems*, 740
  - SSL protection*, 474
  - vulnerability to hackers*, 460
- X Windows servers
  - SATAN scans*, 486-487
  - vulnerability to hackers*, 463
- \$service field (SATAN database facts records), 526
- services
  - networks, 19-20
    - denial reports (TIS Firewall Toolkit)*, 385
    - reducing active processes*, 323
    - status displays*, 322
    - vulnerability to hackers*, 498
  - TCP
    - accessing with netacl*, 329
    - scanning with portscan*, 325, 378
- services files (SATAN scan rulesets), 531
- SESAME network authentication program, 536, 557
  - see also* Kerberos network authentication program
- set (telnet command), 44
- setup
  - Java security, 724-730
  - TCP connections, 310
- \$severity field (SATAN database facts records), 526-527
- shadow password files, 489
- shared media networks, 259
- shell histories (history logs), 153
- Shortest Path First (SPF) protocols, 296
- showmount command, 60
- showmount scans (SATAN), 477
- SHOWPASS configuration keyword (PGP), 680
- SIGABRT (signal), 63
- SIGALRM (signal), 63
- SIGBUS (signal), 63
- SIGCHLD (signal), 63
- SIGCONT (signal), 63
- SIGEMT (signal), 63
- SIGFPE (signal), 63
- SIGHUP (signal), 63
- SIGILL (signal), 63
- SIGINT (signal), 63
- SIGIO (signal), 63
- SIGKILL (signal), 63
- SIGLOST (signal), 63
- signal library functions, 64
- signals, 62-63
  - BREAK (UUCP chat scripts), 111, 132
  - trapping, 62-64, 67
- signing
  - e-mail messages with PGP, 668-671
  - PGP keys, 657-660
- SIGPIPE (signal), 63, 67
- SIGPROF (signal), 63
- SIGQUIT (signal), 63
- SIGSEGV (signal), 63
- SIGSTOP (signal), 63
- SIGSYS (signal), 63
- SIGTERM (signal), 63



- SIGTRAP (signal), 63
- SIGTSTP (signal), 63
- SIGTTIN (signal), 63
- SIGTTOU (signal), 63
- SIGURG (signal), 63
- SIGUSR1 (signal), 63
- SIGUSR2 (signal), 63
- SIGVTALRM (signal), 63
- SIGWINCH (signal), 63
- SIGXCPU (signal), 63
- SIGXFSZ (signal), 63
- Simple Network Management Protocol, *see* SNMP
- Site Security Policy Handbook Working Group
  - Web site, 170
- sites
  - FTP sites
    - Argus network management program*, 472
    - arpmon network monitoring software*, 292
    - ARPCWatch 1.7 network monitoring software*, 292
    - binary files, integrity of*, 497-498
    - Bones*, 557
    - CERT*, 846-847
    - CIAC group*, 846
    - COAST project*, 846
    - connecting to with fip-gw application*, 347
    - connecting to with netacl*, 331-333, 348
    - DESlogin 1.3 zero-knowledge authentication software*, 278
    - EthDump sniffing software*, 260
    - FIRST*, 847
    - Fremont network security evaluation system*, 470
    - GateD route spoofing prevention software*, 299
    - Internet security-related*, 850-853
    - ISS network security evaluation program*, 470
    - netlog network monitoring software*, 292
    - netlog program*, 472
    - Netman sniffing software*, 260
    - network security-related*, 444
    - SATAN*, 499-500
    - Secure Shell program*, 474
    - socks IP encapsulation program*, 476
    - TCP wrappers (SATAN scan detection program)*, 472
    - TCPDump 3.0.2 sniffing software*, 260
    - TIS Firewall Toolkit*, 319
    - usage reports (TIS Firewall Toolkit)*, 386
    - Wietse Venema (co-creator of SATAN)*, 469
    - Xinetd SATAN scan detection program*, 472
  - Gopher sites, connecting to with http-gw, 354-359
  - Telnet sites
    - connecting to with tn-gw application*, 336-337
    - verifying connections with tn-gw application*, 338-339
  - WWW sites
    - BIND DNS name server software*, 308
    - CGI libraries*, 735
    - CGI specifications*, 732
    - CIAC*, 463, 470, 846
    - COAST security lab*, 309, 846
    - connecting to with http-gw*, 354-359
    - Courtney, SATAN scan detection program*, 471
    - Cygnus Corporation*, 473, 848
    - Farmer, Dan (co-creator of SATAN)*, 469
    - FIRST*, 847
    - Gabriel, SATAN scan detection program*, 471
    - GateD route spoofing prevention software*, 299
    - httpd*, 466
    - international law dealing with encryption*, 548
    - Internet security-related*, 850-853
    - ISS network security evaluation program*, 470
    - Java*, 730

- Kerberos*, 848, 473
- MacPGP*, 689
- MITSign*, 688
- network security-related*, 444
- PGP add-on utilities*, 688
- Python CGI programming language*, 747
- RSA cryptography*, 848
- sendmail program*, 466
- SESAME*, 557
- socks IP encapsulation program*, 476
- SSL*, 475
- Tcl CGI programming language*, 747
- TIS Firewall Toolkit*, 848
- X Windows security*, 487
- SKE (secret key encryption), 636
  - see also* secret key rings
- slc (telnet command), 44
- slink daemon, 23
- SLIP (Serial Line Internet Protocol), 15
- slow viruses, 812
- smap (sendmail proxy) client application, TIS
  - Firewall Toolkit, 349, 420-421
  - configurations, 349-351
  - DNS configurations, 353-355
  - installation, 349, 421
  - reports, 387-388
- smapd (sendmail proxy daemon) application,
  - TIS Firewall Toolkit, 351, 421-423
  - configurations, 351-353
  - installation, 351, 422-423
  - options, 421-422
- smart card password security programs,
  - 202, 490
- SMTP ports (system security), 151
- sname field
  - Kerberos tickets, 572
  - KRB\_CRED message, 604
  - KRB\_KDC\_REP message, 591
  - KRB\_KDC\_REQ message, 588
- sniffing networks, 257-279
  - as an administration tool, 259
  - e-mail vulnerability, 261
  - exploitation by hackers, 462-463
  - financial account vulnerability, 261
  - implementing, 258-260
  - password protection, 274-279
    - with encryption*, 277-278
    - with rlogin protocol*, 275-277
    - with Secure RPC*, 278
    - with symmetric encryption*, 279
    - with zero-knowledge authentication*, 278
  - password vulnerability, 261
  - preventing
    - with hardware barriers*, 266-274
    - with network segmentation*, 265-266
    - with trust relationships*, 266
  - protocol vulnerability, 262-265
  - software, 259
  - threats to security, 260-262
- SNMP (Simple Network Management Protocol), 24
  - network-level detection of ARP spoofing servers, vulnerability to/exploitation by hackers, 464-465
  - Windows NT, logging local network activity, 163
- SNMP daemon, 24
- snmpget utility, 464
- snmpnetstat utility, 464
- snmpwalk utility, 464
- sockets
  - interaction with Java, 729
  - querying status, 33-36
  - states, 36
- socks (IP encapsulation), 476
  - Internet sites, 476
  - vulnerability to SATAN, 476
- software
  - bugs, 190
  - copyrighted/licensed, 180
  - Drawbridge, converting PCs to network brides, 274
  - network sniffing, 259
  - repositories, 213
  - ROM-based, virus infection, 760-762
  - system monitoring, 192

- verifying configuration, 209
- virus targets, 755
- source routing (IP), exploitation by
  - hackers, 463
- special characters
  - UUCP chat scripts, 112-113, 133
  - UUCP Dialer file, 107
- speed (BNU Devices file field name), 104
- Speed (BNU Systems file field name), 110
- Speed (L-devices file field), 130
- Speed (L.sys file field), 132
- SPF (Shortest Path First) protocols, 296
- spoofing networks, 258, 279-316
  - ARP spoofing, 281-284, 287-288
    - case study*, 287-288
    - detecting*, 288-292
    - host-level active detection*, 289
    - host-level passive detection*, 289
    - network-level active detection*, 290-292
    - preventing*, 284-287
    - rlogin protocol vulnerability*, 276
    - server-level active detection*, 289-290
- bridge vulnerability, 280
- DNS spoofing, 301-309
  - active attacks*, 306
  - detecting*, 303
  - passive attacks*, 306-309
  - preventing*, 303, 306-309
  - preventing in TIS Firewall Toolkit configuration*, 329
  - rlogin protocol vulnerability*, 276
- hardware addresses, 279-281
- ICMP-based route spoofing, 294-296
- IP address spoofing, 315-316, 492-495
- IP routing systems, 293
- RIP-based, 297-300
- TCP-based spoofing, 309-316
- TCP/IP spoofing, 314-315
- tracing, 280
- SQFILE file (UUCP version 2), 137
- SQL Server (Windows NT), transaction logging, 164
- src directory (SATAN), 508
  - src/boot directory (SATAN), 508
  - src/fping directory (SATAN), 510-511
  - src/misc directory (SATAN), 509
  - src/nfs-chk directory (SATAN), 509
  - src/port\_scan directory (SATAN), 510
  - src/rpcgen directory (SATAN), 511
  - src/yp-chk directory (SATAN), 511-512
- srealm field
  - KRB\_CRED message, 604
  - KRB\_KDC\_REP message, 591
- SSI (Server Side Includes)
  - access restrictions, 742
  - alternatives to, 742-743
  - CGI scripts, 742-743
- SSL (Secure Sockets Layer) protocol, 440, 474-475
  - httpd randomization, vulnerability to hackers, 440
  - RSA public key encryption, 279
  - vulnerability to SATAN, 474-475
  - Web sites, 475
- stacks (JVMs), 722-724
  - constant pool memory area, 724-730
  - execution environment, 723
  - garbage collected heap, 723
  - local variables, 722-723
  - method memory area, 724-730
  - operand stacks, 723
- starting netacl application (TIS Firewall Toolkit), 329
- starttime field
  - Kerberos tickets, 572
  - KRB\_CRED message, 604
- statd daemon, 60
- \$status field (SATAN database facts records), 526
- status (telnet command), 44
- status files (UUCP), 117, 133
- STDERR (standard error files), 66
- STDIN (standard input files), 66
- STDOUT (standard output files), 66
- stealth viruses, 808-811
- stime field (KRB\_ERROR message), 608

- Stoned.Monkey virus, 809
- streams, querying, 33
- STREAMS modules, linking, 23
- subexpect-subsend pairs, 111-114, 132-133
- subkey field
  - Kerberos ticket authenticators, 574
  - KRB\_AP\_REP message, 597
- subnets, 9-12
  - address interpretation, 10
  - determining fixed bits, 11
  - dividing addresses into, 10-12
  - netmasks, determining, 12
  - reserved divisions, 10
  - types, selecting, 11
- subnetting networks to prevent ARP spoofing, 287
- substitution encryption, 621-631
- SUCCEEDDED (UUCP log file error message), 126
- sudo command, 150
- sulog file (Unix audit log), 150-151
- Sun Microsystems
  - bug fixes, 212
  - network addresses, 9
- SUN-MANAGERS mailing list, 207
- SUN-SPOTS mailing list, 207
- superuser access programs, 438
- superusers, 269
- susec field (KRB\_ERROR message), 608
- swapper daemon, 55
- switch user command, 150
- switches (networks), 265
- symmetric encryption (password protection), 279
- SYN flags (TCP), 310
- SYN\_RECIEVED (socket state), 36
- SYN\_SENT (socket state), 36
- synchronizing threads with Java, 706
- SYS file viruses, 764, 788-789
- SYSADM-LIST mailing lists, 207
- Sysfiles (Basic Networking Utilities file), 97
- sysinit (run level action field), 73
- SYSLOG (UUCP version 2), 137
- syslog (syslog file facility), 149
  - facilities, 149
  - fake messages, 166
  - severity levels, 149-150
  - Unix audit log, 148-150
  - vulnerability to hackers, 439
- syslog.conf file, 57-58, 148
- syslogd daemon, 26, 57-58, 148-149
- System (L.sys file field), 131
- system administrators
  - education, 195-197
  - RFC 1244, 171
- system boot
  - init daemon, 55
  - required files
    - HP-UX*, 52-53
    - SCO Unix*, 53-54
    - SunOS*, 51
  - run levels, 72
- system log files
  - evidence of tampering, 166
  - Windows NT, 162
- system messages, logging, 26
- SYSTEM NOT IN Systems (UUCP log file error message), 126
- system policies, *see* system security, policies
- system resources (allocation log files), 155
- system security
  - access points, 189
  - accounts
    - detecting misuse*, 194
    - management procedures*, 215
  - administrator education, 195-197
  - advanced planning, 219
  - audit trails (Windows NT), 160-164
  - audits, 214
  - authentication systems, 202
  - backups, 196
  - benefits, 219
  - bibliography
    - ethics*, 244-246
    - Internet Worm*, 246-248
    - law*, 237, 253

- miscellaneous publications, 251-252*
- National Computer Security Center (NCSC), 248-251*
- security, 239-244*
- security checklists, 251*
- break-ins (elements), 166
- command log files, 155
- configuration management, 217-218
- crontab file (logging usage), 151
- detecting unauthorized use, 191-193
- dial-out facilities (logging usage), 151
- DOS utilities, 164-165
- e-mail
  - origin authentication, 199*
  - privacy enhanced mail, 199*
- encryption, 198
- Ethernet sniffers, 157
- file transfer logs, 152
- generating access reports, 147-148
- goals, 220-221
- history, 172
- history logs (shell histories), 153
- Host Equivalency, 21-22
- information integrity, 199-201
- information resources, 203-208
- insider threats, 190
- intruder indicators, 165
- legal considerations, 219, 229-231
- log files, 192
  - security problems, 166-167*
  - utilities, recommendations, 165-167*
  - utilities, tampering, 167*
- logins (UTMP file unreliability), 146
- lpd bugs, 152
- misconfigured systems, 189
- networks
  - connections log files, 156-157*
  - limiting access, 201*
- obtaining bug fixes, 211-212
- passwords, 46-48, 175, 195, 215-217
- permission files (UUCP version 2), 134
- physical security, 191
- planning, 174
- point-of-contact persons, 228-229
- policies, 179
  - accountability, 182*
  - administrative privileges, 182*
  - assisting other Internet sites, 185*
  - authority for, 176*
  - configuration management, 217-218*
  - contacting outside organizations, 185*
  - e-mail, 183*
  - enforcement responsibilities, 176*
  - ethical issues, 179*
  - general considerations, 175-176*
  - granting system access, 181-182*
  - hacking, 180-181*
  - interpreting, 187*
  - local, 221-222*
  - passwords, 182*
  - "Protect and Proceed," 186-187*
  - publicizing, 188*
  - "Pursue and Prosecute," 186-187*
  - restricting use, 179-181*
  - sensitivity of data, 184*
  - software, 180*
  - system administrator responsibilities, 183*
  - system uses, 179-181*
  - user education, 194-195*
  - user responsibilities, 179-183*
  - users, 179*
  - violations, 184*
- priorities, 220-221
- procedures, 188-189
  - configuration management, 195-196*
  - cost control, 190*
  - general outline, 174-175*
  - incident handling, 193*
  - post-incident, 232-235*
  - risk assessment, 189-190*
  - testing, 214*
- process accounting, 153
- process activity logs, 156
- procmon.cfg configuration file, 69
- professional societies/journals, 208
- protection controls, 190

- public relations guidelines, 226
  - rationale, 172-174
  - remote command execution, 137
  - reporting procedures, 195, 197
  - reporting tools, 209-210
  - resources, 197-214, 235
  - response tactics, 226-229
  - response teams, 204-205, 226
  - risk assessment, 177
    - determining system assets, 177-178*
    - sensitivity of data, 178*
    - system down time, 178-192*
    - unauthorized access, 178*
  - secure operating systems, 210-211
  - security breaches
    - evaluation, 222-224*
    - notification methods, 224-226*
    - notifying authorities, 225*
    - post-incident responses, 233-234*
    - public relations, 225*
  - sendmail log files, 151
  - software bugs, 190
  - strategies, 191
  - summary of threats, 172-174
  - system log files, evidence of tampering, 166
  - system monitoring, 191-193
  - TCP wrapper log files, 166
  - Trusted Host Access, 21-22
  - trusted hosts list, 21
  - UCCP, debugging network connections, 117-118
  - Unix
    - reporting utilities, 158-159*
    - Security mailing list, 203*
  - upgrading methods, 235
  - upgrading operating systems, 196
  - user privileges, 151
  - USERFILE (UUCP version 2), 135-136
  - usernames, recording switched, 150
  - UUCP
    - anonymous login, 123-124*
    - CALLBACK Permissions file option, 122*
    - command sequence, 116*
    - open connections, 115-118*
    - Permissions file, 118-123*
    - SENDFILES Permissions file option, 122*
    - validating hostnames, 122*
  - workstation management, 194
  - system service providers (virus infection), 760-762
  - System\_Name (BNU Systems file field name), 108
  - systems
    - activity, generating reports, 147-148
    - configuring on the fly, 69
    - conversations, tracking, 137
    - information logs, 57-58
    - misconfigured, 189
    - monitoring, 191-193
    - names (UUCP systems), 100-101
    - remote
      - accessing with chat scripts, 111-114, 132-133*
      - validating identity, 135*
    - run levels, 71-74
    - shutdown records, 147
    - subsystems, querying, 33-36
    - system monitoring messages, 69-70
    - troubleshooting, log files, 124
    - UUCP
      - defining, 108-111*
      - system statistics, 127*
      - see also system security*
  - Systems (Basic Networking Utilities file), 97
  - Systems file (UUCP), 108-111, 123
  - Systems Management Server (Windows NT), monitoring TCP/IP traffic, 164
- 
- ## T
- 
- t command option
    - netstat, 33
    - ruptime, 30
  - tables
    - address resolution protocol, 38-39

- host, 12
- Internet-to-Ethernet address translation, 38
- process, 50-51
- routing, 24, 59
- Tag command (Java Appletviewer), 726
- talk program, vulnerability to hackers, 465
- TALKING (UUCP log file error message), 126
- \$target field (SATAN database facts records), 526
- task scheduling, 56
- Tcl CGI programming language, 747
- TCP (Transfer Control Protocol)
  - ACK flags, 311
  - connections
    - preventing remote access to local services, 454*
    - setup, 310*
    - via modems, 488*
    - via proxy servers, 476*
    - vulnerability to hackers, 440-441*
  - data exchange, 311
  - ports, scanning by hackers, 453-454
  - SATAN scans, 477
  - services
    - accessing with netacl, 329*
    - scanning with portscan, 325, 378*
  - spoofing, 309-316
  - SYN flags, 310
- TCP wrapper utility, 159, 454, 471-472
- TCP-IP mailing list, 204
- TCP/IP (Transmission Control Protocol/Internet Protocol), 311
  - access files, 21-23
  - addresses, 8-9
  - command categories, 26
  - configuration files, 17-20
  - configuring for TIS Firewall Toolkit, 326-327
  - connections
    - sequence numbers, accessing, 312*
    - vulnerability to sniffing/forging attacks, 312*
  - daemons, 23-26
  - forged datagrams, 311-313
  - history, 6-7
  - hostnames, 12-13
  - network interfaces, 14-17
  - spoofing, preventing, 314-315
  - subnets, 9-12
  - Systems Management Server
    - monitoring traffic, 164*
  - terminal hijacking, 313-314
  - utilities, 26-48
- TCPDump 3.0.2 sniffing software, 260
- tcpdump program, 463
- Telnet, 43-48
  - Kerberos Authentication, 610
  - sites
    - connecting to with tn-gw application (TIS Firewall Toolkit), 336-337*
    - verifying connections with tn-gw application (TIS Firewall Toolkit), 338-339*
- telnet proxy application, *see* tn-gw application
- telnetd, hacker exploitation of to determine
  - network operating systems, 447-449
- terminal hijacking (TCP/IP), 313-314
- terminals
  - \* (asterisk) terminal write status, 31
  - idle time, 31
  - remote terminal sessions, 40
  - terminal emulation, 43-45
- testing
  - applets, 703, 725-727
  - network security with SATAN, 430-431
  - procedures, 214
  - system policies, 214
- \$text field (SATAN database facts records), 528
- text files, processing with PGP, 666-667
- TEXTMODE configuration keyword (PGP), 680
- tftpd file access (SATAN scans), 483
- threads, synchronizing with Java, 706
- ticket field
  - KRB\_AP\_REQ message, 596

- KRB\_KDC\_REP message, 591
- Ticket Granting Service exchange (Kerberos), 578-591
- tickets (Kerberos), 536, 571-573
  - authentication, 570
  - authenticators, 573-574
  - expiration, 577
  - fields, 572-573
  - flags, 567-570
  - forwardable, 569-570
  - initial, 568
  - invalid, 568
  - postdated, 569
  - preauthenticated, 568
  - proxiable, 569
  - proxied, 569
  - renewable, 568-569
  - requests
    - via *Authentication Service exchange*, 575-578
    - via *Ticket Granting Service exchange*, 578-584
- tickets field (KRB\_CRED message), 604
- till field (KRB\_KDC\_REQ message), 589
- time stamps (Kerberos support), 605
- Time\_to\_Call (BNU Systems file field name), 108
- TIME\_WAIT (socket state), 36
- timestamp field
  - KRB\_CRED message, 604
  - KRB\_SAFE message, 599
- TIS (Trusted Information Systems) Firewall Toolkit, 318-322
  - applications
    - authentication server*, 360-372
    - authmgr client*, 394-395
    - authsrv*, 395-402
    - clauses*, 328
    - comments, inserting*, 328
    - ftp-gw*, 343-348, 402-406
    - http-gw*, 354-359, 406-412
    - login-sh*, 412-413
    - netacl*, 329-333, 414-415
    - plug-gw*, 372-378, 416-417
    - rlogin-gw*, 339-343, 418-419
    - rules*, 328, 339
    - smap client*, 349, 420-421
    - smapd*, 351, 421-423
    - tn-gw*, 333-339, 423-426
    - x-gw*, 359-360, 426-427
  - compiling
    - under BSDI, 320
    - under SunOS, 320
  - disabling IP address forwarding, 326-327
  - disabling inetd services, 324
  - downloading, 319
  - FTP sites regarding, 466
  - FTP site availability, 319
  - Help, 389-390
  - installation, 321-322
  - mailing lists regarding, 390
  - makefiles, editing under BSDI, 320
  - netperm table, 328-329, 390-394
  - netscan utility, 379
  - newsgroups regarding, 389
  - portscan utility, 378
  - preparing for configuration, 322-326
  - preventing DNS spoofing, 329
  - report utilities, 380-394
  - TCP/IP configurations, 326-327
  - Web site, 848
- tkt-vno field (Kerberos tickets), 572
- TLIS connections, configuring for UUCP systems, 139-140
- TMP configuration keyword (PGP), 680
- tn-gw (telnet gateway) application, TIS Firewall Toolkit, 333-339, 423-426
  - clauses, 334-335
  - commands, 336
  - configurations, 333-339
  - host access rules, 337-338
  - installation, 425-426
  - options, 424-425
  - reports, 388-389
  - rules, 334-335
  - Telnet connections
    - establishing*, 336-337
    - verifying*, 338-339



todo files (SATAN scan rulesets), 532  
 todo records (SATAN databases), 529  
 toggle (telnet command), 44  
 token ring, 6  
 top-level directories (SATAN), 500  
 traceroute program, 36-37  
   \* (asterisk), 38  
   finding IP layer information, 463  
 tracing network spoofing, 280  
 tracks (floppy disks), 754  
 trailer encapsulation, 16  
 -trailers command (ifconfig), 16  
 trailers command (ifconfig)rs, 16  
 Transarc Kerberos distribution, 556-559  
 Transfer Control Protocol, *see* TCP  
 Transfer Control Protocol/Internet Protocol,  
   *see* TCP/IP  
 transited fields (Kerberos tickets), 572  
   encoding, 583  
 Transmission Control Protocol/Internet  
   Protocol, *see* TCP/IP  
 transposition encryption, 617-620  
 Trickle SNMP management software, 292  
 tripwire Unix file system utility, 159  
 Trojan Horses, 209  
 troubleshooting  
   memory failures, 35  
   system log files, 124  
 trust files (SATAN scan rulesets), 532  
 trust relationships  
   network segments, 266-274  
   PGP keys, 648-650, 658  
 trust-based networks, vulnerability to  
   hackers, 485  
 \$trusted field (SATAN database facts  
   records), 527  
 Trusted Host Access, 21-22  
 Trusted Information Systems, *see* TIS Firewall  
   Toolkit  
 \$trustee field (SATAN database facts  
   records), 527

TSRs (terminate-and-stay resident) programs,  
   virus infection, 761  
 tty files (security issues), 490-491  
 Type (BNU Dialers file field name), 107  
 Type (BNU Systems file field name), 109  
 Type (L-devices file field), 129  
 TZFIX configuration keyword (PGP), 681

---

## U

-u (runtime command option), 30  
 UDP (User Datagram Protocol)  
   connections, preventing remote access to  
     local services, 454  
   ports, scanning by hackers, 453-454  
   SATAN scans, 477  
 uname command (UUCP), 100  
 University of California at Berkeley, 6  
   Berkeley r-commands, 40-43  
   bug fixes, 212-213  
 Unix  
   audit logs, 146-155  
   mailers, integration with PGP, 688  
   network sniffer software, 260  
   operating systems, 20  
   PGP interface, 687  
 Unix Security mailing list, 203  
 Unix to Unix CoPy, *see* UUCP  
 unknown trust relationships (PGP keys),  
   649-650, 658  
 Unrestricted security mode (Java applets), 727  
 unset (telnet command), 44  
 UNUSED field (Kerberos tickets), 585  
 up command (ifconfig), 16  
 update daemon, 55  
 upgrading operating systems, system  
   security, 196  
 usec field  
   KRB\_CRED message, 604  
   KRB\_SAFE message, 599  
 Usenet newsgroups  
   Internet security-related, 853-854  
   Kerberos-related, 611  
   network security hole-related, 444

- TIS Firewall Toolkit-related, 389
- UUCP names, 101
- user (syslog file facility), 149
- user accounts
  - accounting with Kerberos, 539
  - adding to authentication server database (TIS Firewall Toolkit), 364-368
  - authenticating with Kerberos, 202, 538-542
  - authorizing with Kerberos, 539
  - currently logged in reports, 30
  - detecting misuse, 194
  - hacker acquisition of, 436-437
  - hosts.equiv files, vulnerability to hackers, 440
  - information
    - distributing*, 33
    - querying*, 31-33
  - logging activity, 156
  - management procedures, 195, 215
  - passwords, cracking, 436
  - policies, 181-183
  - requesting credentials from Kerberos authentication servers, 541
  - system policies (education), 194-195
  - UUCP, anonymous login, 123-124
- user commands, 40
- user-data field (KRB\_SAFE message), 599
- USERFILE (UUCP version 2 permission file), 97, 134
  - file transfer entries, 136
  - system security, 135-136
- userid (PGP keys), creating, 652-654
- usernames
  - logging, 150-151
  - system security, ethernet sniffers, 157
- users, *see* user accounts
- /usr/mmdf/mmdftailor configuration file, 59
- UTMP files (Unix audit log), 146-147, 443
- uuclean (Basic Networking Utilities file), 97
- uucico (Basic Networking Utilities file), 97
- uucico command (UUCP), 97, 114
- uuclean command (UUCP), 97, 138
- uucleanup (Basic Networking Utilities file), 97
- UUCP (Unix to Unix CoPy), 96, 149
  - addresses
    - bang addressing*, 99-100
    - Internet compatibility*, 99-100
  - cancelling jobs, 127
  - chat scripts, 111-114, 132-133
    - defining*, 111-114, 132
    - special characters*, 112-113, 133
    - with TCP/IP*, 114
  - configuring, 103, 129
    - devices*, 103-105
    - over TCP/IP*, 139-140
  - debugging
    - device connections*, 106
    - network connections*, 114-115, 133
  - devices
    - defining for local networks*, 105
    - defining for TCP/IP connections*, 105
    - file ownership*, 105
    - testing connections*, 106, 130-131
  - Devices file (field names), 103-105
  - Dialer file (special characters), 107
  - directories, file layout, 102-111
  - files
    - maintenance*, 126-127, 138-139
    - status*, 117, 133
    - transferring*, 99-100
  - history, 96-98
  - log files, 124-126
    - error messages*, 125-126
    - troubleshooting network connections*, 124
  - modem connections, defining phone numbers, 110-111
  - networks, 98-99, 108-111
  - Permissions file, 118-119
    - anonymous login*, 123-124
    - defaults*, 118-119
    - validating hostnames*, 122
  - system names, 100-101
    - choosing*, 101-102

*length limitations*, 100  
*setting*, 101  
 system security  
     *anonymous login*, 123-124  
     *CALLBACK Permissions file option*, 122  
     *command sequence*, 116  
     *debugging network connections*, 117-118  
     *open connections*, 115-118  
     *Permissions file*, 118-123  
     *SENDFILES Permissions file option*, 122  
 Systems file  
     *calling time scheduling*, 109  
     *retry numbers*, 109  
 utilities, 152  
 version 2  
     *debugging permission files*, 135  
     *file layout*, 128-129  
     *permission files*, 134-137  
 versions, 96  
     *file listings*, 96-98  
     *verification*, 101-102  
 uudemmon.admin (Basic Networking Utilities file), 97  
 uudemmon.cleantu (Basic Networking Utilities file), 97  
 uudemmon.cleanup (UUCP daemon), 127  
 uudemmon.day (UUCP version 2 file), 97  
 uudemmon.hour (Basic Networking Utilities file), 97  
 uudemmon.kr (UUCP version 2 file), 98  
 uudemmon.poll (UUCP daemon), 97, 127  
 uudemmon.wk (UUCP version 2 file), 98  
 uugetty (Basic Networking Utilities file), 98  
 UUNET Communications Services, Inc, 213  
 uusched (Basic Networking Utilities file), 98  
 uustat command, 127  
 uusub (UUCP version 2 file), 98  
 uutry command (UUCP), 97-98, 114  
 uuxqt (Basic Networking Utilities file), 98  
 uuxqt (UUCP version 2 file), 98

---

## V

-v (ping command option), 28  
 VALIDATE (Permissions file keyword), 121  
 VALIDATE field (Kerberos tickets), 586  
 variables (JVM stacks), 722-723  
 vector-distance routing protocols, 296  
 vendors (security software), 848  
 Venema, Wietse (co-creator of SATAN), 469  
 VERBOSE configuration keyword (PGP), 681  
 verifying  
     binary file integrity to prevent hacker attacks, 497, 498  
     e-mail messages with PGP, 644-645, 671-673  
     ftp-gw application operations, 346-347  
     Java bytecodes, 717  
     PGP keys, 663-664  
     rlogin-gw application operations, 343  
     Telnet connections with tn-gw application (TIS Firewall Toolkit), 338-339  
 viewing  
     applets with Netscape, 728  
     PostScript files to prevent hacker attacks, 498  
     public key ring contents, 660-661  
     secret key ring contents, 660-661  
 Vigenere encryption, 628-631  
 virus scanners, 815-820  
 VIRUS-L security mailing list, 203  
 viruses, 751-753  
     antivirus utilities, 814-827  
         *behavior blockers*, 829-830  
         *heuristic scanners*, 830-832  
         *integrity checkers*, 824-825  
         *memory scanners*, 823-825  
         *virus scanners*, 815-820  
     appending COM file viruses, 785  
     B1, 783  
     boot record viruses, 767-768, 805  
         *Internet transmission*, 805  
         *methods of infection*, 837-839

- peer-to-peer network infection*, 805
- preventing*, 831
- repairing*, 831
- server infection*, 805
- classes, 806-814
- COM files, 762, 785
- companion viruses (DOS program files), 797-798
- DOS program files, 784-797
  - potential damage*, 798-799
  - preventing*, 833-834
  - repairing*, 833-834
  - targets*, 762-764
  - under Windows NT DOS boxes*, 840
- EXE files, 762-764, 787-788
- FBR viruses, 756, 768-776
- Form, 780
- hardware targets, 754
- improved overwriting COM file viruses, 787
- installation file infections, 839
- Internet transmission, 805
- macro viruses, 765-767, 800-802, 806
  - Internet transmission*, 806
  - peer-to-peer network infection*, 806
  - preventing*, 835-841
  - repairing*, 835-841
  - server infection*, 806
  - under Windows NT*, 841
- MBR viruses, 758, 780-784, 835-837
- multipartite viruses, 814
- network vulnerability, 803-805
- NYB, 783
- overwriting COM file viruses, 786
- PBR viruses, 760, 76-780
- polymorphic viruses, 807
- prepending COM file viruses, 785
- retro viruses, 813-814
- servers, 803-804
- slow viruses, 812
- software targets, 755
- stealth viruses, 808-811
- Stoned.Monkey virus, 809

- SYS files, 764, 788-789
- system service provider targets, 760-762
- Windows 3.1 under Windows NT, 841
- Windows NT native viruses, 841

---

## W

- w (finger command option), 32
- wait (run level action field), 73
- warning (syslog file severity level), 150
- Watchdog (DOS audit trail utility), 165
- Web browsers
  - Netscape Java runtime engine, 728
  - non-proxy aware, 355-356
  - proxy aware, 356
  - running SATAN from, 487-488
- Web servers
  - CGI request logins, 749
  - CGI security issues, 740
  - CGI trust relationships, 736
  - converting from root to controlled file systems, 740
  - SSL protection, 474
  - vulnerability to hackers, 460
- Web sites, *see* WWW sites
- who command, 74
- whois program, hacker exploitation of, 445
- Windows front-end applications for PGP, 688
- Windows 3.1 viruses under Windows NT, 841
- Windows NT
  - Application Log, 161
  - audit trails, 160-164
  - crashing (Registry Editor), 162
  - Directory Auditing dialog box, 160
  - enabling auditing, 160
  - Event Viewer application, 161-162
  - httpd service, 163
  - log files
    - TCP/IP applications*, 163-164
    - viewing*, 161-162
  - logging ftp connections, 162
  - native viruses, 841
  - Security Log, 162

- SNMP, logging local network activity, 163
- SQL Server, transaction logging, 164
- System Log, 162
- Systems Management Server, monitoring
  - TCP/IP traffic, 164
  - virus concerns, 835-841
- wiping files with PGP, 676-677
- workstations
  - authentication in Kerberos, 609-610
  - managing (system security), 194
  - password protection, 269
  - security, 269
  - see also* segments, networks
- World Wide Web, *see* WWW
- world-writeable e-mail directories, vulnerability
  - to hackers, 442
- worms, 802-803
- WRITE (Permissions file keyword), 120
- WRONG MACHINE NAME (UUCP log file
  - error message), 126
- WRONG TIME TO CALL (UUCP log file
  - error message), 126
- WTMP files (Unix audit log), 147-148
- WWW (World Wide Web)
  - browsers
    - Netscape, Java support*, 728
    - non-proxy aware*, 355-356
    - proxy aware*, 356
    - running SATAN*, 487-488
  - servers
    - CGI request logins*, 749
    - CGI security issues*, 740
    - CGI trust relationships*, 736
    - converting from root to controlled file systems*, 740
    - SSL protection*, 474
    - vulnerability to hackers*, 460
  - sites
    - asax*, 158
    - BIND DNS name server software*, 308
    - CGI libraries*, 735
    - CGI specifications*, 732
    - chklastlog*, 158
    - chkwtmp*, 158
    - CIAC*, 463, 470, 846
    - COAST security lab*, 309, 846
    - connecting to with http-gw application (TIS Firewall Toolkit)*, 354-359
    - Courtney, SATAN scan detection program*, 471
    - Cygnus Corporation*, 473, 848
    - Farmer, Dan (co-creator of SATAN)*, 469
    - FIRST*, 847
    - Gabriel, SATAN scan detection program*, 471
    - GateD route spoofing prevention software*, 299
    - htpfd*, 466
    - international law dealing with encryption*, 548
    - Internet security-related*, 850-853
    - ISS network security evaluation program*, 470
    - Java*, 730
    - Kerberos*, 473, 848
    - LOCK*, 165
    - lsof*, 158
    - MacPGP*, 689
    - MITSign*, 688
    - netlog*, 159
    - network security-related*, 444
    - NFS watch utility*, 159
    - PGP add-on utilities*, 688
    - Python CGI programming language*, 747
    - RSA cryptography*, 848
    - sendmail program*, 466
    - SESAME*, 557
    - Site Security Policy Handbook*, 170
    - socks IP encapsulation program*, 476
    - SSL*, 475
    - Tcl CGI programming language*, 747
    - TCP wrapper utility*, 159
    - tripwire*, 159
    - TIS Firewall Toolkit*, 848
    - X Windows security*, 487

## X-Y-Z

---

- .xray file transfer entry (UUCP version 2 USERFILE), 136
- nuucp file transfer entry (UUCP version 2 USERFILE), 136
- X Window System Athena Widget set, compiling X-gw proxies for TIS Firewall Toolkit, 319
- X Windows proxy application, *see* x-gw application
- X Windows security Web site, 487
- X Windows servers
  - SATAN scans, 486-487
  - vulnerability to hackers, 463
- x-gw (X Windows proxy) application, TIS Firewall Toolkit, 359-360, 426-427
  - configurations, 359-360
  - installation, 427
  - options, 427
- Xerox NS Routing Information Protocol, 24, 59
- xfer program, hacker exploitation of, 446
- Xinetd (SATAN scan detection program), 472
  
- z (telnet command), 44
- zero-knowledge authentication (password protection), 278