# Total Question 107

**QUESTION** 1
What is the minimum number of partitions you need to install Linux?

Answer: 1.

Explanation: At a bare minimum, Linux requires just one partition to install and boot. This is the root partition, which is known as the / partition. However, a minimum of two partitions is recommended: one for the root partition and one for the swap partition.
Reference: Roderick W. Smith. Sybex Linux + Study Guide: page 37.

**QUESTION** 2
What file contains the default environment variables when using the bash shell?

A. ~/.profile
B. /bash
C. /etc/profile
D. ~/bash

Answer: C

Explanation: The file /etc/profile contains shell commands that are executed at login time for any user whose entry in /etc/passwd has a shell specified in the shell field whose name ends in sh.
Reference: http://docsrv.caldera.com/cgi-bin/man/man?profile+4
Incorrect Answers
A: The ~/.profile is the profile file stored in each user's home directory. This file contains settings that apply to that user only.
B: The default environment variables are stored in the /etc/profile file, not the /bash file.
D: The default environment variables are stored in the /etc/profile file, not the ~/bash file.

**QUESTION** 3
You need to delete the group dataproject. Which two of the following tasks should you do first before deleting the group?

A. Check the /etc/passwd file to make sure no one has this group as his default group.
B. Change the members of the dataproject group to another group besides users.
C. Make sure that members listed in the /etc/group file are given new login names.
D. Verify that no file or directory has this group listed as its owner.

A. A and C
B. A and D
C. B and C
D. B and D

Answer: B.

Explanation: You can delete a group by editing the /etc/group file and removing the relevant line for the group. It's generally better to use groupdel, though, because groupdel checks to see if the group is any user's primary group. If it is, groupdel refuses to remove the group; you must change the user's primary group or delete the user account first. As with deleting users, deleting groups can leave "orphaned" files on the computer. It's usually best to delete the files or assign them other group ownership using the chown or chgrp commands.
Reference: Roderick W. Smith. Sybex Linux + Study Guide: page 274.
Incorrect Answers
A: It is not necessary to assign new login names to the members listed in the /etc/group file.
C: It is not necessary to assign new login names to the members listed in the /etc/group file.
D: It is only necessary to change the users' default group if the default group is the dataproject group.

---

**QUESTION** 4
All groups are defined in the /etc/group file. Each entry contains four fields in the following order.

A. groupname, password, GID, member list
B. GID, groupname, password, member list
C. groupname, GID, password, member list
D. GID, member list, groupname, password

Answer: A

Explanation: A typical line in the /etc/group file looks like the following:
project1:x:501:sally,sam,ellen,george
Each field is separated from the others by a colon. The meanings of the four fields are as follows:
Group name The first field (project1 in the preceding example) is the name of the group.
Password The second field (x in the preceding example) is the group password. Distributions that use shadow passwords typically place an x in this field; others place the encrypted password directly in this field.
GID The group ID number goes in this field.
User list The final field is a comma-separated list of group members.
Reference: Roderick W. Smith. Sybex Linux + Study Guide: page 273.
Incorrect Answers
B: This is the incorrect order of fields.
C: This is the incorrect order of fields.
D: This is the incorrect order of fields.

---

**QUESTION** 5
You issue the following command
useradd -m bobm
But the user cannot logon. What is the problem?

A. You need to assign a password to bobm's account using the passwd command.
B. You need to create bobm's home directory and set the appropriate permissions.
C. You need to edit the /etc/passwd file and assign a shell of bobm's account.
D. The username must be at least five characters long.

Answer: A

Explanation: When you add a user, the account is disabled until you specify a password for the account. You can use the -p option with the useradd command, but that requires you to enter an encrypted password. For this reason it is easier to use the passwd command. This enables you to enter a plain text password which will then be automatically encrypted.
Reference: Roderick W. Smith. Sybex Linux + Study Guide: page 262.
Incorrect Answers
B: The home directory will be created automatically with the useradd command.
C: The user will use the default shell.
D: The username does not have to be five characters long.

---

**QUESTION** 6
You create a new user account by adding the following line to your /etc/passwd file.
Bobm:baddog:501:501:Bob Morris:/home/bobm:/bin/bash
Bob calls you and tells you that he cannot logon. You verify that he is using the correct username and password. What is the problem?

A. The UID and GID cannot be identical.
B. You cannot have spaces in the line unless they are surrounded with double quotes.
C. You cannot directly enter the password; rather you have to use the passwd command to assign a password to the user.
D. The username is too short, it must be at least six characters long.

Answer: C

Explanation: The password saved in the /etc/passwd file is encrypted. For this reason, you cannot directly enter the password in this file. Rather, you must use the passwd command. The passwd command will take the plain text password and save it in encrypted form in the /etc/passwd file.
Reference: Roderick W. Smith. Sybex Linux + Study Guide: page 262.
Incorrect Answers
A: The UID and the GID can be the same.
B: You can have spaces because each field is separated by a colon (:).
D: The username does not have to be at least six characters long.

---

**QUESTION** 7
Which field in the passwd file is used to define the user's default shell?

Answer: command

Explanation: The last field, known as the command field or login command, is used to specify what shell the user will use when he/she logs in.

---

**QUESTION** 8
There are seven fields in the /etc/passwd file. Which of the following lists all the fields in the correct order?

A. username, UID, password, GID, home directory, command, comment
B. username, password, UID, GID, comment, home directory, command
C. UID, username, GID, home directory, password, comment, command
D. username, password, UID, group name, GID, home directory, comment

Answer: B

Explanation: The first field contains the username. The second field contains the encrypted password or an 'x' if a shadow password file is used. The third field is the User ID number. The fourth field is the primary Group ID number. The fifth field is the comments field. The sixth field is the home directory field. The seventh field is the command field which specifies the user's default shell.
Reference: http://www.unet.univie.ac.at/aix/files/aixfiles/passwd_etc.htm
Incorrect Answers
A: The order of these fields is not correct.
C: The order of these fields is not correct.
D: The order of these fields is not correct.

---

**QUESTION** 9
What file defines the levels of messages written to system log files?

Answer: syslog.conf

Explanation: The file /etc/syslog.conf contains information used by the system log daemon, syslogd to forward a system message to appropriate log files and/or users.
Reference: http://www.unidata.ucar.edu/cgi-bin/man-cgi?syslog.conf+4

---

**QUESTION** 10
Which utility can you use to automate rotation of logs?

Answer: logrotate

Explanation: The logrotate utility is used to manipulate log files. This includes the rotation of log files and the creation of new log files.
Reference: http://www.oreillynet.com/linux/cmd/l/logrotate.html

---

**QUESTION** 11
What is the name and path of the main system log?

Answer: /var/log/messages

Explanation: Most system log files are stored in subdirectories of the /var/log directory. The main system log is /var/log/messages. An example /var/log/messages file can be found here: http://wwwoss.fnal.gov/projects/fermilinux/611/adminclass/examples/messages.html
Reference: Roderick W. Smith. Sybex Linux + Study Guide: Page 293/613.

---

**QUESTION** 12
What is the name and path of the default configuration file used by the syslogd daemon?

Answer: /etc/syslog.conf

Explanation: The file /etc/syslog.conf contains information used by the system log daemon, syslogd to forward a system message to appropriate log files and/or users.
Reference: http://www.unidata.ucar.edu/cgi-bin/man-cgi?syslog.conf+4

---

**QUESTION** 13
You want to ensure that your system is not overloaded with users running multiple scheduled jobs. A policy has been established that only the system administrators can create any scheduled jobs. It is your job to implement this policy. How are you going to do this?

A. Create an empty file called /etc/cron.deny.
B. Create a file called /etc/cron.allow which contains the names of those allowed to schedule jobs.
C. Create a file called /etc/cron.deny containing all regular usernames.
D. Create two empty files called /etc/cron.allow and /etc/cron.deny.

Answer: B

Explanation: Cron has a built in feature of allowing you to specify who may, and who may not use it. It does this by the use of /etc/cron.allow and /etc/cron.deny files. These files work the same way as the allow/deny files for other daemons do. To stop a user using cron, just put their name in cron.deny, to allow a user put their name in the cron.allow.
Reference: http://sharedhosting.net/support/crontab/man.html
Incorrect Answers
A: An empty cron.deny file will not prevent users creating scheduled (cron) jobs.
C: Creating a file called /etc/cron.deny containing all regular usernames is a long way of doing it. It would be much quicker to use a cron.allow file.
D: An empty cron.allow file would not allow anyone (including the administrators) to create cron jobs.

---

**QUESTION** 14
When defining a cronjob, there are five fields used to specify when the job will run. What are these fields and what is the correct order?

A. minute, hour, day of week, day of month, month.

B. minute, hour, month, day of month, day of week.
C. minute, hour, day of month, month, day of week.
D. hour, minute, day of month, month, day of week.

Answer: C

Explanation: The correct order for the five fields are:
minute (0-59),
hour (0-23),
day of the month (1-31),
month of the year (1-12),
day of the week (0-6 with 0=Sunday).
There is a sixth field. This is used to specify the job that will run at the specified time.
Reference: http://sharedhosting.net/support/crontab/man.html
Incorrect Answers
A: These fields are not in the correct order.
B: These fields are not in the correct order.
D: These fields are not in the correct order.

---

**QUESTION** 15
You company does not want to start a mailing list for each of its departments and would rather have an alias for each department. What would you put in the /etc/aliases file to make this work?

A. alias_name: read:/ect/mail/alias-list
B. alias_name: :include:/etc/mail/alias-list
C. alias_name: read-from:/etc/mail/alias-list
D. alias_name: include-from:/etc/mail/alias-list

Answer: B

Explanation: The /etc/aliases file is used to redirect mail when the mail is sent to an alias. For example, you could have an alias named 'accounts'. When mail is sent to 'accounts', it gets redirected to each member of the accounts department. You can list the recipients on the same line as the alias or you can 'include' the names listed in another file.
Reference: http://nscp.upenn.edu/aix4.3html/aixbman/commadmn/ml_alias.htm
Incorrect Answers
A: To redirect mail to the names listed in a file, you would enter ':include: <filename>', not 'read <filename>'.
C: To redirect mail to the names listed in a file, you would enter ':include: <filename>', not 'readfrom <filename>'.
D: To redirect mail to the names listed in a file, you would enter ':include: <filename>', not 'include-from <filename>'.

---

**QUESTION** 16
How would you specify in your zone file that the zone is maintained by hostmaster@foo.com?

A. You specify this when you register the domain.
B. Put "hostmaster.foo.com" as the second field in the SOA record.
C. Create a " MAIL TO hostmaster@foo.com" record for the zone.
D. Put "hostmaster@foo.com" as the second field in the SOA record.

Answer: B

Explanation: The SOA (Start of Authority) records contains a field that specifies who the zone is maintained by. The email address is listed with a '.' instead of '@' as required by DNS standards.
Reference: http://docsrv.caldera.com/NET_tcpip/dnsT.servconf.html
Incorrect Answers
A: You don't specify this when you register the domain.
C: You don't create a 'MAIL TO <email address>'.
D: The email address is listed with a '.' instead of '@' as required by DNS standards.

---

**QUESTION** 17
Internal users of your company's website complain that at peak time they can connect to your server only with extreme difficulty and often receive a timeout error. You find however that the system load is negligible, plenty of extra memory and bandwidth are available, no hardware or line problem is involved and that no errors are logged. What is the most likely cause of this issue?

A. The value of the "MinSpareServers" parameter is too low.
B. The value of the "MaxClients" parameter is too low.
C. The value of the "MaxRequestPerChild" parameter is too low.
D. The value of the "MaxKeepAliveRequest" parameter is too low
E. The value of the "StartServers" parameter is too low.

Answer: B

Explanation: The MaxClients parameter configures the maximum number of authenticated clients which may be logged into a server or anonymous account. Once this limit is reached, additional clients attempting to authenticate will be disconnected. Increasing the MaxClients parameter will allow more connections, thus eliminating the timeouts.
Reference: http://proftpd.linux.co.uk/docs/directives/linked/config_ref_MaxClients.html
Incorrect Answers
A: This parameter is not the cause of the timeout errors.
C: This parameter is not the cause of the timeout errors.
D: This parameter is not the cause of the timeout errors.

---

**QUESTION** 18
You have implemented your firewall rules, and the firewall can connect to the outside, but no one behind the firewall can connect to the Internet. What might be the problem?

A. The users are clueless, show them how it's done.

B. The OUTPUT chain policy is DENY, it must be ACCEPT or no outgoing traffic will leave the host.
C. IP forwarding is turned off in /proc/sys/net/ipv4.
D. The firewall can connect to the Internet, so systems behind it are OK.
The problem must be elsewhere.

Answer: A

Explanation: IP forwarding is disabled by default.

---

**QUESTION** 19
What is the usual mode for the /tmp directory?

A. 0777
B. 0755
C. 7777
D. 1777
E. 0222

Answer: D.

Explanation: The usual mode (permissions) for the /tmp directory is read, write and execute for everybody. Read has a value of 4, write has a value of 2 and execute has a value of 1. When you add these values together you get 7. In this answer (1777), the first 7 means rwx permissions for the file owner. The second 7 means rwx permission for the user's group and the third 7 means rwx permission for everyone else. The 1 means 'sticky'. This means that although everyone has full permissions on the directory, a user cannot delete files that the user doesn't own.
Reference: http://www.comptechdoc.org/os/linux/usersguide/linux_ugfilesp.html
http://lightfocus.com/ebook/m020312.htm
Incorrect Answers
A: This sticky bit (1) is set by default on the /tmp directory.
B: Everyone has rwx (7) permission on the /tmp directory.
C: The first 7 is invalid.

---

**QUESTION** 20
You have just finished setting up your sshd server. Now you need to state which hosts are allowed access to the system. Which is the correct option to enable this in the /etc/ssh/sshd_config file?

A. AllowIP IP_ADDRESS IP_ADDRESS
B. AllowHost IP_ADDRESS IP_ADDRESS
C. EnableIP IP_ADDRESS IP_ADDRESS
D. EnableHosts HOSTNAME HOSTNAME

Answer: B

Explanation: You can specify which hosts are allowed access to system by using the AllowHost parameter in the /etc/ssh/sshd_config file. AllowHost is followed by the hostnames or IP addresses of the systems which are allowed access.
Reference: http://www.linuxchix.org/pipermail/techtalk/2000-July/007737.html
Incorrect Answers
A: The correct option is AllowHost, not Allow IP.
C: The correct option is AllowHost, not EnableIP.
D: The correct option is AllowHost, not EnableHosts.

---

**QUESTION** 21
You have an extensive collection of icons in /usr/local/lib/icons/*.gif, which you want to make available as http://your.server.com/image/*.gif. What is the easiest way to do this?

A. Use a Symlink directive in httpd.conf.
B. Add "Alias /image /usr/local/lib/icons" to httpd.conf.
C. Use a Redirect directive in httpd.conf.
D. Create $DOCUMENT_ROOT/image and copy the files.

Answer: B

Explanation: When configuring a web server, you can use an alias to point to a directory. You would specify the alias in the httpd.conf file which is the configuration file for the http daemon. The line "Alias /image /usr/local/lib/icons" would make the /usr/local/lib/icons directory available using the 'image' alias so <servername>/image would point to <servername>/usr/local/lib/icons.
Reference: http://www.oreilly.com/catalog/debian/chapter/ch12_02.html
Incorrect Answers
A: There is no Symlink directive in httpd.conf. Instead, aliases are used.
C: A redirect would make a request for one file return a different file.
D: It is not necessary to copy the files to the document root folder. The files can stay at their original path and an alias used to point to the path.

---

**QUESTION** 22
IP address resolution should be handled by DNS, NIS, and the local /etc/host file (in that order). If any of the services returns an address not found message the search should halt. Which of the following entries in /ect/nsswitch.conf would achieve this configuration?

A. hosts: dns nis files
B. hosts: dns [NOTFOUND=continue] nis [NOTFOUND=continue] files
C. hosts: dns [RETURN] nis [RETURN] files
D. hosts: dns [NOTFOUND=return] nis [NOTFOUND=return] files
E. hosts: dns [CONTINUE] nis [CONTINUE] files

Answer: D

Explanation: The entry, "hosts: dns [NOTFOUND=return] nis [NOTFOUND=return] files" specifies that DNS should be used first, then NIS then 'files' which means files such as /etc/hosts.

The "[NOTFOUND=return]" option means that if the service cannot resolve the query, a file not found error is returned. The next service is only tried if the preceding service is unavailable. For example, NIS would only be tried if the DNS server was down.
Reference: http://w3.pppl.gov/cgi-bin/man?page=nsswitch.conf&section=4
Incorrect Answers
A: To halt the search if any of the search services return a file not found message, you need the "[NOTFOUND=return]" option.
B: To halt the search if any of the search services return a file not found message, you need the "[NOTFOUND=return]" option.
C: To halt the search if any of the search services return a file not found message, you need the "[NOTFOUND=return]" option.
E: To halt the search if any of the search services return a file not found message, you need the "[NOTFOUND=return]" option.

---

**QUESTION** 23
In a PAM configuration file, a sufficient control allows access:

A. Immediately on success, if no previous required or requisite control failed.
B. Immediately on success, regardless of other controls.
C. After waiting if all other controls return success.
D. Immediately, but only if the user is root.

Answer: D
Reference: http://www.kernel.org/pub/linux/libs/pam/Linux-PAM-html/pam-4.html

---

**QUESTION** 24
When setting up an alias in Sendmail that forwards mail messages to a host in a different domain, what is the syntax of the /etc/aliases entry?

A. bob@domain.com : robert@newdomain.com
B. bob: domain.com : robert@newdomain.com
C. bob: robert@newdomain.com
D. bob:redirect:robert@newdomain.com
E. bob robert@newdomain.com.

Answer: C

Explanation: To forward email to a host in a different domain, you simply specify the alias (in this case 'bob') followed by a colon (:) followed by a space then the address to be forwarded to (in this case robert@newdomain.com).
Reference: http://nscp.upenn.edu/aix4.3html/aixbman/commadmn/ml_alias.htm
Incorrect Answers
A: You are creating an alias called bob so you don't need to specify a full email address as the alias.
B: In this answer, the mail would be forwarded to domain.com and robert@newdomain.com.
D: You don't need to enter the word 'redirect'.
E: The alias must be followed by a colon.

---

**QUESTION** 25
Which line in the aliases file will cause the program msgfilter to filter on mail arriving for the user called msg?

A. msg: "/usr/local/msgfilter"
B. msg: "|/usr/local/msgfilter"
C. msg: "exec /usr/local/msgfilter"
D. msg: "filter /usr/local/msgfilter"
E. msg: "F /usr/local/msgfilter"

Answer: B

Explanation: The pipe symbol ( | ) is a command redirector. It is used to take the output of one command and use it as input for another command. In this case, email sent to 'msg' is the output which is piped (redirected) to /usr/local/msgfilter.
Reference: http://www.netti.hu/doc/LinuxShellScript/rpf.htm
Incorrect Answers
A: You need the pipe symbol to make the msgfilter program take the email as its input.
C: You need the pipe symbol to make the msgfilter program take the email as its input.
D: You need the pipe symbol to make the msgfilter program take the email as its input.
E: You need the pipe symbol to make the msgfilter program take the email as its input.

---

**QUESTION** 26
When running INN, how do you force an update of the news groups you are monitoring?

A. Stop and restart innd.
B. /usr/bin/newsfeed
C. /usr/bin/innfeed
D. /usr/bin/dlnews
E. /usr/bin/innd -dl -news

Answer: C

Explanation:
Reference: http://linuxcommand.org/man_pages/innfeed1.html
Incorrect Answers
A:
B:
C:
D:

---

**QUESTION** 27
You have a computer with Windows 95 installed and want to install Linux on it.
However, there is no free space available. How could you manage to install Linux on this computer with the least amount of effort?

A. Use fips to resize the partition containing Windows 95.
B. Repartition the hard drive; reinstall Windows 95 and then install Linux.
C. You cannot run Windows 95 and Linux on the same computer.
D. Create a directory under Windows 95 and install Linux in that directory.

Answer: A

Explanation: FIPS is a partition resizing tool. It can reduce the size of the Windows 95 partition without losing any data, thus freeing up enough space to create a Linux partition.
Reference: Roderick W. Smith. Sybex Linux + Study Guide: Page 43.
Incorrect Answers:
B. It is not necessary to reinstall Windows 95.
C. You can run Windows 95 and Linux on the same computer.
D. You cannot install Linux into a subdirectory in Windows 95.

---

**QUESTION** 28
You are creating a new partition in preparation for installing Linux. You want to have five different partitions. You have successfully created four partitions, but are unable to create the fifth one. What is the problem?

A. Your hard drive is not large enough for more than four partitions.
B. You need to create the swap partition last.
C. You created four primary partitions.
D. Linux cannot be installed on more then four partitions.

Answer: C

Explanation: A hard disk can only contain up to four primary partitions. If you want more than four partitions on your hard disk, you'll need to create up to three primary partitions and one 'extended' partition. The extended partition can contain multiple logical partitions thus enabling you to have more than four partitions on the disk.
Reference: http://www.tldp.org/HOWTO/mini/Install-Strategies/x72.html
Incorrect Answers
A: Assuming you know what you're doing, you would know if your disk had any free space on it and would only attempt to create another partition if you knew the disk had free space.
B: You don't need to create the swap partition last.
D: Linux can be installed on more than four partitions.

---

**QUESTION** 29
When looking at the /etc/passwd file, you notice that all the password fields contain 'x'. What does this mean?

A. The password is encrypted.
B. That you are using shadow password.
C. That all passwords are blank.

D. That all passwords have expired.

Answer: B

Explanation: Linux distributions that use shadow password files typically place an 'x' in the password field in the /etc/passwd file.
Reference: Roderick W. Smith. Sybex Linux + Study Guide: Page 273.
Incorrect Answers
A: If the password is encrypted, you can see the encrypted password.
C: An x does not indicate a blank password.
D: An x does not indicate that a password has expired.

---

**QUESTION** 30
After Bob leaves the company you issue the command userdel bob. Although his entry in the /etc/passwd file has been deleted, his home directory is still there. What command could you have used to make sure that his home directory was also deleted?

A. userdel -m bob
B. userdel -u bob
C. userdel -l bob
D. userdel -r bob

Answer: D

Explanation: The -r option used with the userdel command is used to delete the users home directory and any files in the directory.
Reference: http://www.oreillynet.com/linux/cmd/u/userdel.html
Incorrect Answers
A: The -m option is invalid.
B: The -u option is invalid.
C: The -l option is invalid.

---

**QUESTION** 31
You create a new user by adding the following line to the /etc/passwd file
bobm::501:501:Bob Morris:/home/bobm:/bin/bash
You then create the user's home directory and use the passwd command to set his password. However, the user calls you and says that he cannot log on. What is the problem?

A. The user did not change his password.
B. bobm does not have permission to /home/bobm.
C. The user did not type his username in all caps.
D. You cannot leave the password field blank when creating a new user.

Answer: B

Explanation: You should use the useradd utility to create a new user. This will create the home

directory and apply the necessary permissions to it. As you didn't use useradd, you would have to have manually created the home directory (/home/bobm). The most likely reason for the login failure is that you didn't give the user account the necessary permissions on the home directory.
Incorrect Answers
A: The user should be able to log on with the password that you set.
C: The username is bobm which is lowercase.
D: You can leave the password field blank. Furthermore, you set the password with the passwd command, so it is no longer blank.

---

**QUESTION** 32
Bob Armstrong, who has a user name of boba, calls to tell you he forgot his password. What command should you use to reset his password?

Answer: passwd boba

Explanation: The command to change a password for a user account is "password <username>". You will then be prompted for a new password for the account. You must be a privileged user to change the password for another users account.
Reference: http://www.oreillynet.com/linux/cmd/p/passwd.html

---

**QUESTION** 33
Which file defines all users on your system?

A. /etc/passwd
B. /etc/users
C. /etc/password
D. /etc/user.conf

Answer: A

Explanation: The user accounts on a Linux system are listed in the /etc/passwd file. Each user account is listed on one line of the /etc/passwd file. A typical entry would look like:
sally:x:529:100:Sally Jones:/home/sally:/bin/bash
Reference: Roderick W. Smith. Sybex Linux + Study Guide: Page 266.
Incorrect Answers
B: The user accounts are not listed in the /etc/users file.
C: The user accounts are not listed in the /etc/password file.
D: The user accounts are not listed in the /etc/user.conf file.

---

**QUESTION** 34
You have configured logrotate to rotate your logs weekly and keep them for eight weeks. You are running out of disk space. What should you do?

A. Quit using logrotate and manually save old logs to another location.
B. Reconfigure logrotate to only save logs for four weeks.
C. Configure logrotate to save old files to another location.

D. Use the prerotate command to run a script to move the older logs to another location.

Answer: D

Explanation: The default setting for the logrotate utility is to run the prerotate script for every log that is rotated. You could edit the prerotate script to move the older logs to another location to free up some disk space.
Reference: http://misc.eecs.umich.edu/cgi-bin/man2html?logrotate+8
Incorrect Answers
A: It is not necessary to stop using logrotate.
B: It is not necessary to reconfigure logrotate to only save logs for four weeks.
C: You cannot directly configure logrotate to old and new logs in different locations. This is why logrotate runs the prerotate script for every rotated log.

---

**QUESTION** 35
Which log contains information on currently logged in users?

A. /var/log/utmp
B. /var/log/wtmp
C. /var/log/lastlog
D. /var/log/messages

Answer: A

Explanation: The /var/log/utmp file contains information about users that are currently logged in to the system.
Reference: http://www.unixreview.com/documents/s=1236/urm0104b/0104b.htm
Incorrect Answers
B: The /var/log/wtmp file contains information about people who have logged in to the system previously. The users listed in this file may not be currently logged in.
C: The currently logged in users are not listed in the /var/log/lastlog file.
D: The /var/log/messages file contains system messages and messages generated by applications. It does not record logons.

---

**QUESTION** 36
What daemon is responsible for tracking events on your system?

Answer: syslogd

Explanation: Syslogd (system log deamon) is responsible for tracking and logging system events.
Reference: http://docsrv.caldera.com:8457/cgi-bin/man?mansearchword=syslogd&mansection=8

---

**QUESTION** 37
In order to schedule a cronjob, the first task is to create a text file containing the jobs to be run along with the time they are run. Which of the following commands will run the script MyScript every day at 11:45 pm?

A. * 23 45 * * MyScript
B. 23 45 * * * MyScript
C. 45 23 * * * MyScript
D. * * * 23 45 MyScript

Answer: C

Explanation: The order of the time fields is:
minute (0-59),
hour (0-23),
day of the month (1-31),
month of the year (1-12),
day of the week (0-6 with 0=Sunday).
11:45 pm is 45 minutes past the 23 hour. Therefore, the first two fields should be 45 23. The next three fields contain wildcards to run the job every day. The time fields are followed by the script name, "MyScript".
Reference: http://sharedhosting.net/support/crontab/man.html
Incorrect Answers
A: This answer is invalid. It has 45 in the day of the month field.
B: This answer is invalid. It has 45 in the hour field.
D: This answer is invalid. It has 23 in the month field and 45 in the day of the week field.

---

**QUESTION** 38
The netstat -r command produces the following output:
192.168.10.0 * 255.255.255.0 U 40 0 0 eth1
Which of the following best describes this line?

A. 192.168.10.0 is a Gateway (G) to all external (*) networks.
B. The host, 192.168.10.0, is currently up (U).
C. There are currently 40 packets waiting for transmission over this route.
D. The network, 192.168.10.0, is accessible through the local NIC configured as eth1.
E. The router at 192.168.10.0, which is up (U), is sending and receiving Routing Information Protocol packets.

Answer: D.

Explanation: The netstat -r command displays the routing table. The first field is the destination field. The second field in the routing table entry is the gateway field. When an address matches an entry in the table, the Gateway field tells the system how to reach the specified destination. If the Gateway field contains the IP address of a router, then that router is used. If the Gateway field contains all zeros (0.0.0.0) or an asterisk (*), the destination is a directly connected network, and the "gateway" is the computer's network interface.
Reference: http://www.linux-mag.com/2001-05/routing_02.html
Incorrect Answers
A: The asterisk is in the gateway field, not the destination field.

B: The address 192.168.10.0 with a network mask of 255.255.255.0 is a network address, not a host address.
C: The number 40 is the metric (cost of the route), not the number of packets waiting to be sent.

---

**QUESTION** 39
Your system is the primary nameserver for example.com. Due to network growth you must delegate authority for engr.example.com to the host server.engr.example.com. Which of the following lines should be added to your zone file?

A. engr ID IN PTR server.engr.example.com
B. server ID IN NS server.engr.example.com
C. server ID IN NIS server.engr.example.com
D. server ID IN PTR engr.example.com
E. server ID IN A engr.example.com

Answer: B.

Explanation: The NS record is used to list the name server responsible for a zone. To delegate authority for a subdomain, you need to create an NS record in the zone file of the parent domain.
For example: To delegate "subname.yourname.com", create NS-records for "subname.yourname.com" in the "yourname.com" zone.
These NS-records must point to the DNS server responsible for "subname.yourname.com" for example "ns1.subname.yourname.com" - or a DNS server somewhere else like "ns1.othername.net".
Reference: http://www.jhsoft.com/help/rec_NS.htm
Incorrect Answers
A: A PTR record is used for reverse DNS lookups.
C: NIS is an invalid option.
D: An A record is used for a standard DNS lookup.

---

**QUESTION** 40
You need to reconfigure Sendmail on a client's email server that has been recently abused by third parties as a relay machine for unsolicited commercial email. Assuming a default set of configuration files, which one should be modified?

A. sendmail.cf
B. relay.cf
C. access
D. domaintable
E. mailertable

Answer: C

Explanation: The access database (/etc/mail/access) defines what host(s) or IP addresses have access to the local mail server and what kind of access they have. Hosts can be listed as OK, REJECT, RELAY or simply passed to sendmail's error handling routine with a given mailer error. Hosts that are listed as OK, which is the default, are allowed to send mail to this host as long as the mail's final

destination is the local machine. Hosts that are listed as REJECT are rejected for all mail connections. Hosts that have the RELAY option for their hostname are allowed to send mail for any destination through this mail server.
Reference: http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/sendmail.html
Incorrect Answers
A: The sendmail.cf file is not used to restrict email access.
B: The relay.cf file is not used to restrict email access.
D: The domaintable file is not used to restrict email access.
E: The mailertable file is not used to restrict email access.

---

**QUESTION** 41
You are trying to secure Apache. After successfully setting up Apache to run inside a chroot jail, you try to run it as a non-root user, and find that httpd no longer starts. What is the most probable cause?

A. Apache needs to start as root to bind to port 80.
B. Apache can't read the main index.html file because it wasn't moved into the chroot environment.
C. A LoadModule line for mod_chroot needs to be added to httpd.conf.
D. Apache requires a VirtualHost directive when running form a chroot environment.
E. The mod_chroot configuration needs the absolute path to the chroot environment.

Answer: A

Explanation:
Reference: http://www.openna.com/community/articles/security/v1.3-xml/chap29sec254.html
Incorrect Answers
A:
B:
C:
D:

---

**QUESTION** 42
All of the following commands can be used to determine open TCP ports a local host EXCEPT:

A. lsof
B. netstat
C. nmap
D. fuser
E. ifconfig

Answer: E

Explanation: The ifconfig command is used to assign an address to a network interface and/or configure network interface parameters. It is also used to display information about the network interface(s). It does not display information about open TCP ports on the computer.

Reference: http://www.oreillynet.com/linux/cmd/i/ifconfig.html
Incorrect Answers
A: This command can be used to display the open TCP ports on the computer.
B: This command can be used to display the open TCP ports on the computer.
C: This command can be used to display the open TCP ports on the computer.
D: This command can be used to display the open TCP ports on the computer.

---

**QUESTION** 43
How would you display your system's current ARP cache?

A. arp -a
B. netstat -a
C. netstat -arp
D. cat /ect/arp

Answer: A

Explanation: The arp -a command is used to display the current ARP cache. This is a TCP/IP command that works across various operating systems.
Reference: http://www.oreillynet.com/linux/cmd/a/arp.html
Incorrect Answers
B: Netstat is used to display port information, not the ARP cache.
C: Netstat is used to display port information, not the ARP cache.
D: The ARP cache is not written to a file; it is stored in RAM.

---

**QUESTION** 44
You've installed a PAM-aware restricted service and installed the appropriate /etc/pam.d/<service> file, but you can't authenticate. What is the best place to look for problems?

A. Reinstall libpam and reboot; the library isn't being seen.
B. Remove /etc/pam.d/<service>, change the /etc/pam.d/other modules entries from pam_deny.o to pam_accept.0 and try again.
C. Change all controls to optional and try again.
D. Look for clues in the log file where auth and authpriv messages are logged.

Answer: D

Explanation: When troubleshooting a problem, the first step is always to look at the log files. The log files often indicate the source of a problem.
Incorrect Answers
A: The question is asking where to look for problems. You should look in the log files.
B: The question is asking where to look for problems. You should look in the log files.
C: The question is asking where to look for problems. You should look in the log files.

---

**QUESTION** 45
Several users complain that when checking their email or telnetting to your server they have to wait up to 60 seconds before getting their email or being presented with a login screen. However, immediately successive attempts at the same operation succeed normally - only to suffer again from the same problem after some time. What is causing this behavior?

A. The DNS server used by the clients is not properly resolving the server name to an ip address.
B. The routing table on the server contains multiple routes to the client's machines.
C. The server is timing-out while trying to resolve the client's IP addresses to names.
D. A router along the way is dropping packets in transit.
E. Another machine on the server's network is using the same IP address.

Answer: C

Explanation: When you connect to a Linux server to collect email or via Telnet, the server looks at your IP address and then tries to resolve it to a hostname to check whether the hostname is allowed to connect. This is known as a reverse DNS lookup. The cause of the problem is that the server is timing out while performing the IP address to hostname resolution.
Incorrect Answers
A: If the DNS server used by the clients is not properly resolving the server name to an IP address, the clients would never be able to connect using the server hostname.
B: The server would use the route with the lowest cost if multiple routes existed.
D: This is possible, but it is not the most likely cause of the problem. You would get an error message is the packets were being dropped.
E: An IP conflict is unlikely to be the cause of the problem.

---

**QUESTION** 46
You find that a host (192.168.1.4) being used on one of your client's networks has been compromised with a backdoor program listening on port 31337. Your client requests a list of originating IP addresses connecting to that port. Using a Linux workstation as traffic analyzer, which of the following commands would gather the data requested by the client?

A. tcpdump host 192.168.1.4 and port 31337 -w out
B. nmap host 192.168.1.4:31337
C. arpwatch -n 192.168.1.4/32 -p 31337> capture
D. pcap -d 192.168.1.4:31337
E. ipwatch --syn 192.168.1.4 -p 31337 --log=out

Answer: A

Explanation: Tcpdump is a traffic analyzer package from Ethereal. The "tcpdump host 192.168.1.4 and port 31337 -w out" command will give the required information. The -w option will write the information to a file rather than display it on screen.
Reference: http://www.ethereal.com/tcpdump.8.html
Incorrect Answers
B: This command will not give the required information.

C: This command will not give the required information.
D: This command will not give the required information.
E: This command will not give the required information.

---

**QUESTION** 47
How would you tell named that the nameserver with ip 1.2.3.4 is unreliable and should not be queried?

A. server 1.2.3.4. { bogus yes; };
B. blackhole { 1.2.3.4; };
C. ignore 1,2,3,4;
D. disallow-query 1,2,3,4;

Answer: A

Explanation: If a name server is giving out false information, you can configure your name server to ignore it using the 'bogus yes' option.
Reference: http://softwaredev.earthweb.com/sdopen/article/0,,12077_625181_4,00.html
Incorrect Answers
B: The blackhole is used to list a server known to be abusive, not unreliable.
C: Ignore is not a valid option.
D: Disallow-query is not a valid option.

---

**QUESTION** 48
The maximum size of the swap partition is _____ MB?

Answer: 128

Explanation: The maximum size of a Linux swap partition is 128MB, although Linux supports up to 16 swap partitions.
Reference: Michael J. Tobler. New Riders, Inside Linux: Page 17.

---

**QUESTION** 49
In order to improve your system's security you decide to implement shadow passwords. What command should you use?

Answer: pwconv

Explanation: The pwconv command is used to convert unshadowed entries in /etc/passwd into shadowed entries in the /etc/shadow file, and to replace the encrypted password in /etc/password with an x.
Reference: http://www.oreillynet.com/linux/cmd/p/pwconv.html

---

**QUESTION** 50
You need to create a new group called sales with Bob, May and Joe as members. Which of the following would accomplish this?

A. Add the following line to the /etc/group file: sales:44:bob,mary,joe
B. Issue the command groupadd sales
C. Issue the command groupadd -a sales bob,mary,joe
D. Add the following line to the /etc/group file: sales::44:bob,mary,joe

Answer: D

Explanation: The correct entry in the /etc/group file is: sales::44:bob,mary,joe. Note the two colons after the group name 'sales'. This is because the second field (the password field) should be empty. 44 is the group ID. The members of the group are separated by commas.
Reference: http://www.unet.univie.ac.at/aix/files/aixfiles/group_security.htm
Incorrect Answers
A: There should be two colons after 'sales', for the empty password field.
B: This command would create the group but it doesn't add the group members.
C: The -a option is invalid.

---

**QUESTION** 51
Which of the following tasks in not necessary when creating a new user by editing the /etc/passwd file?

A. Create a link from the user's home directory to the shell the user will use.
B. Create the user's home directory.
C. Use the passwd command to assign a password to the account.
D. Add the user to the specified group.

Answer: A

Explanation: A typical entry in the passwd file would look like:
sally:x:529:100:Sally Jones:/home/sally:/bin/bash
The /bin/bash entry is the default shell for the user account. There is no need to create a link from the users home directory to the shell that the user will use.
Reference: Roderick W. Smith. Sybex Linux + Study Guide: Page 266.
Incorrect Answers
B: When you create a user by directly editing the /etc/passwd file, you need to manually create the home directory.
C: You must assign a password to the account before the account can be used.
D: Every user account must be assigned to a group.

---

**QUESTION** 52
In order to prevent a user from logging in, you can add a (n) _____ at the beginning of the password file.

Answer: asterisk

Explanation: When you create a user account, the password field contains an asterisk (*). To enable

the account, you must assign a password to the account. To disable a user account, you can enter an asterisk in the password field of the account.
Reference: http://www.unet.univie.ac.at/aix/files/aixfiles/passwd_etc.htm

---

**QUESTION** 53
What command you use to review boot messages?

Answer: dmesg

Explanation: Immediately after you start the computer, you will see the messages in the kernel ring buffer scroll past on the screen at high speed as the computer boots. The dmesg command is used to display the kernel ring buffer.
Reference: http://www.oreillynet.com/linux/cmd/d/dmesg.html

---

**QUESTION** 54
You wish to have all mail messages except those of type info to the /var/log/mailmessages file. Which of the following lines in your /etc/syslog.conf file would accomplish this?

A. mail.*;mail!=info /var/log/mailmessages
B. mail.*;mail.=info /var/log/mailmessages
C. mail.*;mail.info /var/log/mailmessages
D. mail.*;mail.!=info /var/log/mailmessages

Answer: D

Explanation: The first part of the answer, "mail.*" instructs syslogd to log all types of mail messages, which is not what we want (the syntax is mail.type). However, the second part of the answer, "mail.!=info" overrules that and instructs syslogd to ignore mail messages of the type 'info'. 'Info' is a 'serverity level' for the message. Examples of other levels are err and crit.
Reference: http://nodevice.com/sections/ManIndex/man1597.html
Incorrect Answers
A: There must be a dot (period) separating mail and !=info.
B: The exclamation mark (!) means to ignore this type. This answer will only log the info type. We want to ignore the info type.
C: This answer will log all mail messages of type 'info' or above. We want to exclude the 'info' type.

---

**QUESTION** 55
You notice that your server load is exceptionally high during the hours of 10 am to 12 noon. When investigating the cause, you suspect that it may be a cron job scheduled by one of your users. What command can you use to determine if your suspicions are correct?

A. crontab -u
B. crond -u
C. crontab -l
D. crond -l

Answer: C

Explanation: The -l option used with the crontab command is used to list the users crontab file. This command must be run as root to list all users' crontab files.
Reference: http://www.oreillynet.com/linux/cmd/c/crontab.html
Incorrect Answers
A: The -u option is used to specify which users crontab file will be acted upon.
B: Crond is the cron daemon responsible for running the cron jobs.
D: Crond is the cron daemon responsible for running the cron jobs.

---

**QUESTION** 56
Some network attacks use IP packets with the SYN, ACK, PSH, URG, FIN and RST options set. (This is sometimes called a "Chernobyl1 packet" or "xmas tree packet", and crashes some operating systems.) To log all such packets received, you would use:

A. iptables -1 INPUT -s 0.0.0.0/0 -d 192.168.0.44/33 --protocol tcp --xmas-pkt -j LOG
B. iptables -1 INPUT -s 0.0.0.0/0 -d 192.168.0.44/32 --protocol tcp --cher-pkt -j LOG
C. iptables -1 INPUT -s 0.0.0.0/0 -d 192.168.0.44/32 --protocol tcp --cher-pkt -log
D. iptables -1 INPUT -s 0.0.0.0/0 -d 192.168.0.44/32 --protocol tcp --tcp-flags SYN, ACK, HSK, PSH, URG, FIN -log
E. iptables -1 INPUT -s 0.0.0.0/0 -d 192.168.0.44/32 --protocol tcp --tcp-flags ALL, SYN, ACK, PSH, URG, RST, FIN, -j LOG

Answer: E

Explanation: When using the tcp-flags option, the first argument is the flags which we should examine, written as a comma-separated list, and the second argument is a comma-separated list of flags which must be set. In this answer, we should examing 'ALL' flags, and the SYN, ACK, PSH, URG, RST, FIN must be set.
Reference: http://www.linuxguruz.org/iptables/howto/maniptables.html
Incorrect Answers
A: 'Xmas-pkt' is an invalid option.
B: "Cher-pkt' is an invalid option.
C: "Cher-pkt' is an invalid option.
D: This answer has the 'ALL' statement missing. This answer will examine the SYN, ACK, HSK, PSH, URG, FIN flags, but it doesn't specify which flags should be set.

---

**QUESTION** 57
Which of the following options can be passed to a DHCP client machine using configuration options on the DHCP server?

A. The iptables security settings.
B. The routing table.
C. The subnet netmask.
D. The NIS server maps.

E. The IP address resolution order.

Answer: C.

Explanation: DHCP is used to assign client computers TCP/IP configurations. The only option from the answers given that can be passed to a DHCP client is the subnet mask.
Incorrect Answers
A: This is not a TCP/IP configuration option.
B: The routing table is not given out by DHCP. The client computer will have its own routing table.
D: The NIS server maps are not given out by DHCP.
E: The client will have its own default IP resolution order. This is not given out by DHCP.

---

**QUESTION** 58
A specific mail archive application, which prefilters with procmail, must support a custom header. If a user has a "X-No-Archive: yes" line in this header, the message should be sent to /dev/null. Complete the following rule to implement this feature.
:o

_____
/dev/null

A. MATCH="X-NO-ARCHIVE:*YES"
B. /X-No-Archived:\ yes/
C. ^x-no-archive: yes
D. X-No-Archived:\ yes
E. * ^x-no-archive: yes

Answer: E

Explanation:

---

**QUESTION** 59
You have just completed booting the system but you are unable to connect to the Internet. Looking at the following route -n route, what is the problem?
Kernel IP routing table

| Destination | Gateway | Genmask | Flags | Metric | Ref | Use Iface |
|---|---|---|---|---|---|---|
| 207.122.247.33 | 0.0.0.0 | 255.255.255.240 | U | 0 | 0 | 0 eth0 |
| 207.122.247.36 | 0.0.0.0 | 255.255.255.240 | U | 0 | 0 | 0 eth1 |
| 127.0.0.0 | 0.0.0.0 | 255.0.0.0 | U | 0 | 0 | 0 lo |

A. The subnet mask is incorrect for the stated network.
B. The local machine does not have any declared hosts.
C. There are too many default routes declared within the same subnet.
D. There is no default route.

Answer: D

Explanation: The routing table must have a default route, if you want to connect to the internet. A default route means that if the destination of a packet does not match a specific route in the table, the packet is sent to the default gateway. From there, it will be forwarded to the appropriate destination.
Reference: http://www.linux-mag.com/2001-05/routing_02.html
Incorrect Answers
A: The subnet mask is not incorrect.
B: This is not required for internet access.
C: You can have as many routes as you like.

---

**QUESTION** 60
Your organization has opened a new office on a different floor, and the computers that will be installed there will be on a new network, 192.168.1.0/24. A Linux gateway having the address 192.168.0.2 on your local network will route traffic between the two subnets. Which invocation of the 'route' command will properly reconfigure your firewall (address 192.168.0.1) so that it can communicate with the new subnet?

A. route add 192.168.1.0/24 192.168.0.2
B. route add -net 192.168.1.0 netmask 255.255.255.0 gw 192.168.0.2
C. route add 192.168.1.0 netmask 24 gw 192.168.0.2
D. route add -net 192.168.1.0/24 192.168.0.2/32
E. route add 192.168.1.0/255.255.255.0 gw 192.168.0.2

Answer: B

Explanation: To add a route to the routing table, you use the route add command. The syntax is: route add [-net] <destination> netmask <netmask> gw <gateway>. In this case, we are using the -net option to specify that the destination is a network address. The network address is followed by the 'netmask' option with the netmask written in decimal notation (x.x.x.x). The gw option specifies the gateway of 192.168.0.2.
Reference: http://www.linux-mag.com/2001-05/routing_03.html
Incorrect Answers
A: You cannot use CIDR notation (/24) with the route add command.
C: The network mask must be written in decimal notation. In this case 255.255.255.0.
D: You cannot use CIDR notation (/24) with the route add command.
E: You must use the 'netmask' option if you are going to specify the network mask (which isn't always necessary).

---

**QUESTION** 61
Users of a newly-installed Squid caching proxy server complain that after logging to an interactive web site that requires them to use individual names and passwords, the remote system mistakes them for other users. Everything works well if the users turn off the proxy in the browser settings. What is the most likely cause of this malfunction?

A. The browser's proxy settings are incorrect.
B. The proxy is caching cookies.
C. The proxy is not compatible with this web site.
D. The proxy cache is stale and should be purged.
E. The proxy is caching dynamically-generated pages.

Answer: E

Explanation: The web pages are generated dynamically according to the input entered by the users. The problem here is that the proxy server is caching these dynamically generated pages.
Incorrect Answers
A: The browser's proxy settings are correct because they are receiving cached pages.
B: The problem is not caused by cached cookies.
C: This is not a compatibility issue.
D: Clearing the cache won't prevent the problem occurring in the future.

---

**QUESTION** 62
You can cause named to reload a zone file by:

Answer: ndc reload

Explanation: You can force a running named process to reload a zone file by issuing the 'ndc reload' command.
Reference: http://www.apnic.net/db/revdel.html

---

**QUESTION** 63
What is the name of the file that contains the key (s) for logging in without a password?

A. $HOME/.ssh/known_keys
B. $HOME/.ssh/allowed_keys
C. $HOME/.ssh/authorized_keys
D. $HOME/.ssh/trusted_keys

Answer: C

Explanation: You can login to a Linux system of SSH without entering a password by using the SSH keys for authentication. The keys are kept in the $ HOME/.ssh/authorized_keys directory.
Reference: http://www-unix.mcs.anl.gov/mpi/mpich/docs/mpichman-chp4/node46.htm
Incorrect Answers
A: The keys are not kept in this directory.
B: The keys are not kept in this directory.
D: The keys are not kept in this directory.

---

**QUESTION** 64
The recommended minimum size of the swap partition is _____ MB?

Answer: 16

Explanation: The swap partition should ideally be twice the amount of physical RAM, although a minimum of 16 MB is recommended.
Reference: Michael J. Tobler. New Riders, Inside Linux: Page 13.

---

**QUESTION** 65
When you look at the /etc/group file you see the group kmem listed. Since it does not own any files and no one is using it as a default group, can you delete this group?

Answer: no

Explanation: The kmem group is used to provide direct access to the system memory. This group is used by programs that need to directly access memory and therefore should not be deleted.
Reference: http://www.gsp.com/cgi-bin/man.cgi?section=5&topic=linprocfs

---

**QUESTION** 66
Mary has recently gotten married and wants to change her username from mstone to mknight. Which of the following commands should you run to accomplish this?

A. usermod -l mknight mstone
B. usermod -l mstone mknight
C. usermod -u mknight mstone
D. usermod -u mstone mknight

Answer: A

Explanation: The syntax of the usermod command is 'usermod [options] user'. The -l <name> option enables you to change the username name of an account.
Reference: http://www.oreillynet.com/linux/cmd/u/usermod.html
Incorrect Answers:
B: This answer would change the name mknight to mstone (if the name existed).
C: The -u option is used to change the user ID number.
D: The -u option is used to change the user ID number.

---

**QUESTION** 67
You attempt to use shadow passwords but are unsuccessful. What characteristic of the /etc/passwd file may cause this?

A. The login command is missing.
B. The username is too long.
C. The password field is blank.
D. The password field is prefaced by an asterisk.

Answer: C

Explanation: Linux distributions that use shadow password files typically place an 'x' in the password field in the /etc/passwd file. If the password field is blank, the shadow password file won't be used.
Reference: Roderick W. Smith. Sybex Linux + Study Guide: Page 273.
Incorrect Answers
A: There is no login command in the passwd file. There is however a 'command' field. This is used to specify the login shell. If this field was missing, the default shell would be used.
B: There is no maximum length for a username.
D: The username field comes before the password field. It is unlikely that the username field would contain an asterisk.

---

**QUESTION** 68
Which of the following user names is valid?

A. Theresa Hadden
B. thadden
C. Theresa H
D. T.H.

Answer: B.

Explanation: A Linux username is case sensitive and can not contain spaces or dots. 'thadden' is the only valid username of the answers given. If you try to create an account containing invalid character, you will get an error saying "invalid username".
Incorrect Answers
A: The username cannot contain spaces.
C: The username cannot contain spaces.
D: The username cannot contain dots.

---

**QUESTION** 69
You wish to rotate all your logs weekly except for the /var/log/wtmp log which you wish to rotate monthly. How could you accomplish this?

A. Assign a global option to rotate all logs weekly and a local option to rotate the /var/log/wtmp log monthly.
B. Assign a local option to rotate all logs weekly and a global option to rotate the /var/log/wtmp log monthly.
C. Move the /var/log/wtmp log to a different directory.
Run logrotate against the new location.
D. Configure logrotate to not rotate the /var/log/wtmp log.
Rotate it manually every month.

Answer: A

Explanation: Logrotate reads everything about the log files it should be handling from the series of configuration files specified on the command line. Each configuration file can set global options

(local definitions override global ones, and later definitions override earlier ones) and specify some logfiles to rotate. Therefore, we can set a global option to rotate all logfiles weekly and set a local option to rotate the /var/log/wtmp file monthly.
Reference: http://www.fifi.org/cgi-bin/man2html/usr/share/man/man8/logrotate.8.gz
Incorrect Answers
B: The local option overrides the global option, not the other way round.
C: It is not necessary to move the file to a different directory.
D: It is not necessary to manually rotate the log.

---

**QUESTION** 70
Which of the following lines in your /etc/syslog.conf file will cause all critical messages to be logged to the file /var/log/critmessages?

A. *.=crit /var/log/critmessages
B. *crit /var/log/critmessages
C. *=crit /var/log/critmessages
D. *.crit /var/log/critmessages

Answer: A

Explanation: The syntax is <message>.<type>. The <message> is the type of system message (mail, kernel etc.) and the <type> is the severity level. The = character is used to specify that level only (in this case, only messages with the severity level of 'critical'). So here we have * (all) messages of the type 'critical' will be logged at /var/log/critmessages.
Reference: http://nodevice.com/sections/ManIndex/man1597.html
Incorrect Answers
B: There must be a dot (.) between the message type and the severity level.
C: There must be a dot (.) between the message type and the severity level.
D: This answer is nearly correct. However with the '=' character, all messages with a level of critical and above will be logged.

---

**QUESTION** 71
Which daemon must be running in order to have any scheduled jobs run as scheduled?

A. crond
B. atd
C. atrun
D. crontab

Answer: A

Explanation: A cron job is a job scheduled to run regularly at the specified time. The daemon that provides this service is the cron daemon known as crond. An job scheduled to run with the 'at' command will run at the scheduled time but it will only run once.
Reference: http://ddart.net/linux/man/html/crond.8.html
Incorrect Answers

B: The at daemon (atd) is used to run a job scheduled with the at command. However, these jobs will only run once, which is why A is a better answer.
C: Atrun required the cron daemon to run 'at' jobs.
D: A crontab is a file listing the cron jobs and the times when they should run.

---

**QUESTION** 72
Given the CIDR mask /29, the equivalent subnet mask in dotted quad format would be 255.255.255.___.

Answer: 248

Explanation: Dotted quad format divides a 32 bit number into four 8 bit sections. 8 bits in decimal = 255. Therefore, the first 24 bits can be represented as 255.255.255. This leaves us with 5 bits. 2 ^ 5 = 248.

---

**QUESTION** 73
What would you add to the options section of named.conf to tell named not to perform recursive resolution for any clients?

A. disable-recursion
B. recurse: no
C. disallow-recursion {*; };
D. recursion no; fetch-glue no;

Answer: D

Explanation: Normally a name server returning NS records for which it does not have A records will attempt to retrieve them. This is called glue fetching. This can be disabled with the fetch-glue no option. To disable recursion, you would use the recursion no option.
Reference: http://www.acmebw.com/resources/papers/securing.pdf
Incorrect Answers
A: This is an invalid option.
B: This is an invalid option.
C: This is an invalid option.

---

**QUESTION** 74
While performing a security audit, you discover that a machine is accepting connections to TCP port 184, but is not obvious which process has the port open. Which of the following programs would you use to find out?

A. traceroute
B. strace
C. debug
D. nessus
E. lsof

Answer: E

Explanation: The lsof (list set of files) can be used to display what files are opened by a specified process. It can also be used to display what ports are opened by the specified processs.
Reference: http://helix.nih.gov/talks/basicsecurity/#ISlsof
Incorrect Answers
A: This command does not display the ports opened by a process.
B: This command does not display the ports opened by a process.
C: This command does not display the ports opened by a process.
D: This command does not display the ports opened by a process.

---

**QUESTION** 75
What would you use to generate an RSA key for named to sign zone transfers with?

A. You can use the keys created by shh-keygen.
B. dnskeygen
C. named --keygen
D. You can use PGP-generated keys.

Answer: B

Explanation: Dnskeygen (DNS Key Generator) is a tool to generate and maintain keys for DNS Security within the DNS (Domain Name System). Dnskeygen can generate public and private keys to authenticate zone data, and shared secret keys to be used for Request/Transaction signatures.
Reference: http://www.rt.com/man/dnskeygen.1.html
Incorrect Answers
A: You wouldn't use SSH keys for DNS.
C: There is no 'named --keygen' command.
D: You wouldn't use PGP keys for DNS.

---

**QUESTION** 76
A server detects a number of connection attempts that you believe to be an attempted attack. Where do you go to find out about recent exploits?

A. http://www.cert.org/
B. http://www.slashdot.org/
C. http://www.nsa.gov/
D. http://www.ciac.org/

Answer: A

Explanation: This is taken from their homepage: The CERT(r) Coordination Center (CERT/CC) is a center of Internet security expertise, located at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University. Our information ranges from protecting your system against potential problems to reacting to current problems to predicting future problems. Our work involves handling computer security incidents and vulnerabilities,

publishing security alerts, researching long-term changes in networked systems, and developing information and training to help you improve security at your site.
Reference: http://www.cert.org/
Incorrect Answers
B: This is not the correct website.
C: This is not the correct website.
D: This is not the correct website.

---

**QUESTION** 77
Using wu-ftpd, you have setup an anonymous FTP server to allow access only to files under /var/ftp. You want to share out your current /etc/mtab file so users can see what filesystems are mounted on your system at any given time. You make a symbolic link from /etc/mtab to /var/ftp/pub/mounted_filesystems. During testing, you find that when logged in as a normal user, the file is accessible but when logged in anonymously, the file can NOT be read. Why might this happen?

A. The symbolic link points to an absolute path.
B. The permissions on the symbolic link are wrong.
C. The FTP server will not allow files owned by root to be accessed.
D. The FTP server needs write access to the /etc directory to it can update the access time on the file.
E. The timestamp on /etc mtab is wrong.

Answer: E

---

**QUESTION** 78
Given a CIDR mask of 2/3 and a netmask of 255.255.255.0 how many usable host IP addresses are available?

Answer: unknown

---

**QUESTION** 79
What command is used to remove the password assigned to a group?

Answer: gpasswd -r

Explanation: The gpasswd command is used to administer the /etc/group file. The -r option is used to remove a password from a group.
Reference: http://ddart.net/linux/man/html/gpasswd.1.html

---

**QUESTION** 80
What account is created when you install Linux?

Answer: root

Explanation: When you install Linux, the root account is created. The root account is the Linux

version of a Windows Administrator account. The account has full access permissions to the entire filesystem and all the processes running on the system.

---

**QUESTION** 81
You have been assigned the task of determining if there are any user accounts defined on your system that have not been used during the last three months. Which log file should you examine to determine this information?

A. /var/log/wtmp
B. /var/log/lastlog
C. /var/log/utmp
D. /var/log/messages

Answer: B

Explanation: The lastlog command can be used to display the contents of /var/log/lastlog file. This file contains a list of all user accounts on the system and the time of their last login. If a user has never logged in to the system, they will be listed as 'Never logged in'.
Reference: http://www.fifi.org/cgi-bin/man2html/usr/share/man/man8/lastlog.8.gz
Incorrect Answers
A: The /var/log/wtmp file does contain information about previous logins. However, this file is typically rotated. The lastlog file contains the specific information required in the question.
C: The /var/log/utmp file contains a list of the currently logged on users.
D: The /var/log/messages file contains system messages.

---

**QUESTION** 82
Complete the following ipchains invocation so that "ICMP unreachable" messages will be sent back to anyone trying to connect to the telnet service listening on port 23
ipchains -A input --dbport 23 -p tcp -j _____

Answer: REJECT

Explanation: The -j option is used to specify a 'target'. Examples of targets are ACCEPT, DENY, REJECT, RIDIRECT, RETURN and MASQThe REJECT option is the same as the DENY option, except that the REJECT option will send an ICMP message back to the user saying that the destination is unreachable.
Reference: http://olympus.het.brown.edu/cgi-bin/man2html?ipchains+8

---

**QUESTION** 83
Your users request that you process their incoming mail so that duplicate forwarded messages are deleted, which if the following could be used to accomplish this task?

A. fetchmail
B. mqueue
C. procmail
D. elm

E. rmail

Answer: C

Explanation: The procmail utility can be used to filter email messages when they arrive. It can be configured delete messages according to specified rules such as duplicate forwarded messages.
Reference: http://nlsn.free.fr/lin-docs/procmail/man/procmail.html
Incorrect Answers
A: This cannot be used to filter email at the email server.
B: This cannot be used to filter email at the email server.
D: This cannot be used to filter email at the email server.
E: This cannot be used to filter email at the email server.

---

**QUESTION** 84
Given a CIDR mask of /25 and a netmask of 255.255.255.128 how many host IP addresses are available?

Answer: 126

Explanation: An IP address is 32 bits long. A 25 bit subnet mask means that 25 bits of the IP address are used for the network address. This leaves 7 bits for the host address. The formula for working out the number of host addresses is 2 ^ n - 2 (where n is the number of bits used for the host addresses). 2 ^ 7 - 2 = 126.

---

**QUESTION** 85
You are installing Linux into a computer with two IDE hard drives. You plan on dividing each hard drive into two partitions. What are the names of the partitions?

A. hda1, hda2, hda3, hda4
B. hda1, hda2, hdb1, hdb2
C. sda1, sda2, sda1, sdb2
D. sda1, sda2, sda3, sda4

Answer: B

Explanation: IDE hard drives can be recognized by the letters 'hd'. SCSI hard drives use the letters 'sd'. Hard drives use letters a, b, c etc... with 'a' being the first hard drive (hda) and 'b' being the second hard drive (hdb). The partitions use numbers 1, 2, 3 etc.. with 1 being the first partition and 2 being the second partition. Therefore the first 2 partitions on the first disk will be hda1 and hda2 and the first 2 partitions on the second disk will be hdb1 and hdb2.
Incorrect Answers
A: hda3 and hda4 are the 3rd and 4th partitions on the first disk.
C: The letters sd are used for SCSI disks.
D: The letters sd are used for SCSI disks.

---

**QUESTION** 86
You have created a subdirectory of your home directory containing your scripts. Since you use the bash shell, what file would you edit to put this directory on your path?

A. ~/.profile
B. /etc/profile
C. /etc/bash
D. ~/.bash

Answer: A

Explanation: As a normal login shell, bash 'sources' the system-wide file /etc/profile, where the system environment and path can be set for bash users. The user can overwrite values set in /etc/profile by creating a file ~/.bash_profile, ~/.bash_login or ~/.profile.
Reference: http://www.tldp.org/HOWTO/mini/Path-6.html
Incorrect Answers
B: The /etc/profile file is for system-wide settings, not user specific settings.
C: This is the incorrect file to set the path variable.
D: This is the incorrect file to set the path variable.

---

**QUESTION** 87
You changed the GID of the sales group by editing the /etc/group file. All of the members can change to the group without any problem except Joe. He cannot even login to the system. What is the problem?

A. Joe forgot his password for the group.
B. You need to add Joe to the group again.
C. Joe had the original GID specified as his default group in the /etc/passwd file.
D. You need to delete Joe's account and recreate it.

Answer: C

Explanation: Every user account has an entry in the /etc/passwd file. The third field of each entry is the user's primary group identifier (GID). This number must be the number of an existing group otherwise the user will not be able to log on. In this question, you have changed the GID number of the group, so therefore the GID entry for Joe is invalid.
Reference: http://www.unet.univie.ac.at/aix/files/aixfiles/passwd_etc.htm
Incorrect Answers
A: You log on with the user account password, not the group account password.
B: You don't need to re-add the users to a group if you change the group ID.
D: It is unnecessary to delete and recreate Joe's account.

---

**QUESTION** 88
You have created special configuration files that you want copied to each user's home directories when creating a new user accounts. You copy the files to /etc/skel.
Which of the following commands will make this happen?

A. useradd -m username
B. useradd -mk username
C. useradd -k username
D. useradd -Dk username

Answer: B

Explanation: The '-m' option used with the useradd command is used to create the user's home directory if it doesn't already exist. The 'k' option is used to copy default files to the user's home directory. Meaningful only when used with the -m option. The default files are copied from /etc/skel/ unless an alternate dir is specified.
Reference: http://www.oreillynet.com/linux/cmd/u/useradd.html
Incorrect Answers
A: The '-m' option used with the useradd command is used to create the user's home directory if it doesn't already exist. However, you need the 'k' option to copy the files.
C: The 'k' option can only be used with the '-m' option.
D: The -D option is used to set or display default settings.

---

**QUESTION** 89
When using useradd to create a new user account, which of the following tasks is not done automatically?

A. Assign a UID.
B. Assign a default shell.
C. Create the user's home directory.
D. Define the user's home directory.

Answer: C

Explanation: When creating a user account with the useradd command, the home directory is not created automatically. To create the home directory, you need to use the -m option with the useradd command.
Reference: http://www.oreillynet.com/linux/cmd/u/useradd.html
Incorrect Answers
A: The UID is created automatically. The default value is the smallest ID value greater than 99 and greater than every other UID.
B: The default shell is taken from the /etc/login.defs file.
D: The default home directory is /home/<username>.

---

**QUESTION** 90
Your company has implemented a policy that users' passwords must be reset every ninety days. Since you have over 100 users you created a file with each username and the new password. How are you going to change the old passwords to the new ones?

A. Use the chpasswd command along with the name of the file containing the new passwords.

B. Use the passwd command with the -f option and the name of the file containing the new passwords.
C. Open the /etc/passwd file in a text editor and manually change each password.
D. Use the passwd command with the u- option.

Answer: A

Explanation: The chpasswd command is used to change passwords by using a file as it's input. Chpasswd reads a file of user name and password pairs from standard input and uses this information to update a group of existing users. The file must contain one username and password per line in the form: username:password.
Reference: http://www.fifi.org/cgi-bin/man2html/usr/share/man/man8/chpasswd.8.gz
Incorrect Answers
B: There is no -f option for the passwd command.
C: This would be a long way of doing it. Also, you would have to manually enter encrypted passwords into the file.
D: There is no 'u' option with the passwd command.

---

**QUESTION** 91
The beginning user identifier is defined in the _____ file.

Answer: /etc/login.defs

Explanation: The system-wide user and group account settings are defined in the /etc/login.defs file. These settings include the minimum UID number.
Reference: http://www.fifi.org/cgi-bin/man2html/usr/share/man/man5/login.defs.5.gz

---

**QUESTION** 92
While logged on as a regular user, your boss calls up and wants you to create a new user account immediately. How can you do this without first having to close your work, log odd and logon as root?

A. Issue the command rootlog.
B. Issue the command su and type exit when finished.
C. Issue the command su and type logoff when finished.
D. Issue the command logon root and type exit when finished.

Answer: B

Explanation: The su (switch user) command is used to open a shell as another user without closing your existing shell. You can switch to any user account using the 'su <username>' command. If you don't specify a username, the root account is assumed and you will be prompted for the root password. You can close the shell by issuing the exit command.
Reference: http://www.oreillynet.com/linux/cmd/s/su.html
Incorrect Answers
A: Rootlog is the incorrect command to switch user accounts.

C: Logoff is the incorrect command to exit from 'su'.
D: Logon is an invalid command.

---

**QUESTION** 93
You have been told to configure a method of rotating log files on your system.
Which of the following factors do you need to consider?

A. Date and time of messages.
B. Log size.
C. Frequency of rotation.
D. Amount of available disk space.

Answer: A

Explanation: Your log file rotation system will depend on the date and the time of the logged messages. This will vary according to what you are logging. All other considerations such as the frequency of the rotation will be based on the date and time of the logged messages.
Incorrect Answers
B: The log size should be considered but it is not the most important consideration.
C: The frequency of rotation will depend on the date and time of the logged information, and other factors such as log size and disk space.
D: This is a minor consideration. The date and time of the messages is more important. If you want for example, one month of data in a log but don't have enough disk space, you would add more disk space.

---

**QUESTION** 94
You have made changes to the /etc/syslog.conf file. Which of the following commands will cause these changes to be implemented without having to reboot your computer?

A. kill SIGHINT 'cat /var/run/syslogd.pid'
B. kill SIGHUP 'cat /var/run/syslogd.pid'
C. kill SIGHUP syslogd
D. kill SIGHINT syslogd

Answer: B.

Explanation: 'Kill SIGHUP' instructs syslogd to perform a re-initialization. All open files are closed, the configuration file (default is /etc/syslog.conf) will be reread and the syslogd facility is started again. 'cat /var/run/syslogd.pid' will give the kill SIGHUP command the exact process ID of the syslogd process.
Reference: http://www.uwm.edu/cgi-bin/Dept/IMT/wwwman?topic=syslogd(8)&msection=1
Incorrect Answers
A: SIGHINT is the incorrect 'kill' argument.
C: You should give the kill SIGHUP command the exact process ID of the syslogd process with the 'cat /var/run/syslogd.pid' statement.
D: SIGHINT is the incorrect 'kill' argument.

---

**QUESTION** 95
One of your users, Bob, has created a script to reindex his database. Now he has it scheduled to run every day at 10:30 am. What command should you use to delete this job?

A. crontab -ru bob
B. crontab -u bob
C. crontab -du bob
D. crontab -lu bob

Answer: A

Explanation: The -r option used with the crontab command is used to delete a cron job. The 'u' option is used to specify which user's crontab file, the command will be acted upon.
Reference: http://www.oreillynet.com/linux/cmd/c/crontab.html
Incorrect Answers
B: This command will give an error because you have specified no actions to be taken.
C: There is no -d option with crontab.
D: The -l option will display the user's crontab file as.

---

**QUESTION** 96
As the system administrator you need to review Bob's cronjobs. What command would you use?

A. crontab -lu bob
B. crontab- u bob
C. crontab -l
D. cronq -lu bob

Answer: A

Explanation: The -l option used with the crontab command is used to display a crontab file. The 'u' option is used to specify which user's crontab file, the command will be acted upon.
Reference: http://www.oreillynet.com/linux/cmd/c/crontab.html
Incorrect Answers
B: This command will give an error because you have specified no actions to be taken.
C: This command will display your crontab file because you haven't specified another user.
D: Cronq is an invalid command.

---

**QUESTION** 97
You have entered the following cronjob. When will it run?
15 * * * 1. 3. 5 myscript

A. At 15 minutes after every hour on the 1st, 3rd and 5th of each month.
B. At 1:15 am, 3:15 am, and 5:15 am every day.
C. At 3:pm on the 1st, 3rd, and 5th of each month.

D. At 15 minutes after every hour every Monday, Wednesday, and Friday.

Answer: D

Explanation: The order of the time fields is:
minute (0-59),
hour (0-23),
day of the month (1-31),
month of the year (1-12),
day of the week (0-6 with 0=Sunday).
The 15 means 15 minutes past. The first asterisk means every hour. The third asterisk means every month. The second asterisk means every day but the job won't run every day. This is because the 1.3.5 in the 'day of the week' field means Monday, Wednesday and Friday. Therefore, the job will run on every Monday, Wednesday and Friday at 15 minutes past every hour. Myscript is the name of the script that will run at the specified times.
Reference: http://sharedhosting.net/support/crontab/man.html
Incorrect Answers
A: This is the wrong time.
B: This is the wrong time.
C: This is the wrong time.

---

**QUESTION** 98
What is the role of the file /etc/ftpusers?

A. Stores FTP usernames and passwords.
B. Lists users NOT allowed to use the ftp server.
C. Configures permission to transfer files to and from the system.
D. Lists users NOT allowed to use the ftp client.

Answer: B

Explanation: The ftpusers file is used to deny FTP access to specific users. The format is a simple text file listing the restricted users one per line.
Reference: http://www.qnx.com/developer/docs/qnx_6.1_docs/neutrino/utilities/f/ftpusers.html
Incorrect Answers
A: The /etc/ftpusers file does not store FTP usernames and passwords.
C: The /etc/ftpusers file is not used to configure permission to transfer files to and from the system.
D: The /etc/ftpusers is not used to list users NOT allowed to use the ftp client.

---

**QUESTION** 99
In a PAM configuration file, the difference between a required control and a requisite control is:

A. Nothing, they both permit or deny access based on the outcome of the test.
B. A required control failure is acted upon immediately.
C. A requisite control failure is acted upon immediately, while the failure of a required control is

ignored until other modules are evaluated.
D. Only requisite controls log failure messages to syslog.

Answer: C.

Explanation: A required control indicates that the success of the module is required for the moduletype facility to succeed. Failure of this module will not be apparent to the user until all of the remaining modules (of the same module-type) have been executed.
A requisite control is similar to a required control, however, in the case that such a module returns a failure, control is directly returned to the application. The return value is that associated with the first required or requisite module to fail.
Reference: http://www.kernel.org/pub/linux/libs/pam/Linux-PAM-html/pam-4.html
Incorrect Answers
A: They are similar but slightly different. A requisite control failure is acted upon immediately whilst a required control failure is not acted upon until all other required controls have been tested.
B: A requisite control, not a required control failure is acted upon immediately.
D: All controls log their failures.

---

**QUESTION** 100
You are the primary nameserver for an international corporation. You have found that your DNS cache is utilizing 1GB of total system memory and is severely affecting system performance. What is the correct directive to limit the amount of memory to 256MB?

A. memlimit { 256M };
B. datasize { 256M };
C. cache-limit { (256* 1024) };
D. cachesize { 256; };

Answer: B

Explanation: The 'datasize' option is used to set the maximum amount of system memory the server may use. This is a hard limit on server memory usage. If the server attempts to allocate memory in excess of this limit, the allocation will fail, which may in turn leave the server unable to perform DNS service.
Reference: http://www.csd.uwo.ca/staff/magi/doc/bind9/Bv9ARM.ch06.html
Incorrect Answers
A: This is the incorrect option to set the maximum amount of system memory to be used.
C: This is the incorrect option to set the maximum amount of system memory to be used.
D: This is the incorrect option to set the maximum amount of system memory to be used.

---

**QUESTION** 101
You have a static external IP of 10.0.0.10 on your firewall. You want to masquerade all internal hosts on the network 192.168.0.0/24 behind this static IP. Your iptables rule is:

A. iptables -t nat -A POSTROUTING -s 192.168.0.0/24 -d 0/0 -j MASQUERADE

B. iptables -t nat -A POSTROUTING -s 192.168.0.0/24 -d/0/0 -j SNAT --to -source 10.0.0.10
C. iptables -t nat A FORWARD -s 192.168.0.0/24 -d 0/0 -j SNAT --to -source 10.0.0.10
D. iptables -t filter -A FORWARD -s 192.168.0.0/24 -d 0/0 -j MASQUERADE

Answer: B.

Explanation: The SNAT option used in a POSTROUTING chain is used to specify that the source address of the packet should be modified. The 'SNAT --to -source 10.0.0.10' option specifies that the source address of all outgoing packets will be changed to 10.0.0.10.
Reference: http://www.linuxguruz.org/iptables/howto/maniptables.html
Incorrect Answers
A: MASQUERADE should only be used with dynamically assigned IP (dialup) connections: if you have a static IP address, you should use the SNAT option.
C: SNAT can only be used in a POSTROUTING chain.
D: MASQUERADE can only be used in a POSTROUTING chain.

---

**QUESTION** 102
What is wrong with the following zone records?
domain.org. IN MX 7 mail.domain.org
mail.domain.org IN CNAME server.domain.org
server.domain.org IN A 192.168.1.1

A. Hostnames on the left half of the record must not be fully qualified.
B. MX record priorities must be in multiples of 10.
C. CNAME should be CANON for BIND and above.
D. BIND requires matching IN6 records.
E. MX records should not point to a CNAME.

Answer: E

Explanation: In the zone file, we can see that mail.domain.org is a CNAME (alias) for server.domain.org and that the MX record points to mail.domain.org.
Section 10.3 of RFC 2181 (Standards Track) specifies that the domain name used as the value of a NS resource record, or part of the value of a MX resource record must not be an alias (CNAME).
Reference: http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc2181.html#sec-10
Incorrect Answers
A: The hostnames can be fully qualified.
B: MX record priorities are usually multiples of 10 but this is not a requirement.
C: CNAME should not be CANON for any version of BIND.
D: BIND does not require matching IN6 records.

---

**QUESTION** 103
You want to assign IP addresses from a Class C network to your numerous bootp clients. What would you add to the dhcpd.conf?

A. bootp-dynamic 192.168.0.0/24;

B. range dynamic bootp 192.168.0.2 192.168.0.255;
C. range dynamic-bootp 192.168.0.2 192.168.0.255;
D. assign range 192.168.0.0/24 bootp;
E. bootp { range: 192.168.0.0/24; }

Answer: C

Explanation: For any subnet on which addresses will be assigned dynamically, there must be at least one range statement. The range statement gives the lowest and highest IP addresses in a range. All IP addresses in the range should be in the subnet in which the range statement is declared. The dynamic-bootp flag may be specified if addresses in the specified range may be dynamically assigned to BOOTP clients as well as DHCP clients.
Reference: http://www.fifi.org/cgi-bin/man2html/usr/share/man/man5/dhcpd.conf.5.gz
Incorrect Answers
A: The syntax of this answer is incorrect.
B: There should be a hyphen between dynamic and bootp (dynamic-bootp).
D: The syntax of this answer is incorrect.

---

**QUESTION** 104
Which of the following tools can forward user ports on a remote host to ports local to the system where it is used?

A. ssh
B. ipfwadm
C. ipchains
D. nmap
E. ipmasqadm

Answer: A

Explanation: Ssh2 (Secure Shell) is a program for logging into a remote machine and executing commands in a remote machine. The -R listen-port:host:port option is used to forward a remote port to a local address. This causes ssh to listen for connections on a port, and forward them to the other side by connecting to host:port.
Reference: http://www.alladmin.com/security/ssh_details.html
Incorrect Answers
B: This is the incorrect tool.
C: This is the incorrect tool.
D: This is the incorrect tool.
E: This is the incorrect tool.

---

**QUESTION** 105
You have been asked to set up a DNS server for your department. You are to allow the company's main DNS server to update yours. What is the correct entry in the named.conf?

A. allow-transfer { IP_ADDRESS; };

B. allow-update { IP_ADDRESS; };
C. allow-access { IP_ADDRESS; };
D. allow-access { IP_ADDRESS };

Answer: A.

Explanation: A zone transfer occurs when a slave server asks the primary server for the zone information. Allow-transfer specifies which hosts are allowed to receive zone transfers from the server. This must be configured in the zone file on the primary DNS server.
Reference: http://www.freebsddiary.org/secondary.php
Incorrect Answers
B: Allow-update specifies which hosts are allowed to submit Dynamic DNS updates to the server.
C: This is an invalid option.
D: This is an invalid option.

---

**QUESTION** 106
You investigate a complaint and find that a malicious user has sent out a 20MB attachment to hundreds of recipients. You also find that it is the only job present in the outbound queue.
Which command should be used to purge the queue?

A. sendmail -q
B. sendmail --flush -outbound
C. rm /var/spool/mqueue/*
D. sendmail --purge=all
E. sendmail -dq

Answer: C

Explanation: The mail queue can be found at /var/spool/mqueue/. You can delete the mail queue using the rm //var/spool/mqueue/* command. As there is only one mail in the queue, other users will not be affected.
Incorrect Answers
A: The -q option is used to send the queued mail, not delete it.
B: This option is invalid.
D: This option is invalid.
E: This option is invalid.

---

**QUESTION** 107
What is the most important reason why an administrator should not enable telnet on a secured system?

A. Telnet is inherently insecure due to the number of known exploits against it.
B. It is possible to get passwords by sniffing traffic.
C. Telnet is insecure and does no security checking of users allowed to login or password expiry checks.
D. Telnet exposes the secured system to port scanning attempts.

Answer: B

Explanation: Telnet sends the user's password across the network as plain text. This would enable someone to discover your password by sniffing network traffic. This is why a more secure method such as SSH is recommended because SSH encrypts the traffic sent across the network.
Incorrect Answers
A: The main reason why telnet is insecure is that the password is sent as plain text.
C: This is not the most important reason why Telnet should not be used.
D: This is not the most important reason why Telnet should not be used.

---

**QUESTION** 108
What are the names of the two files that are not combined directly into httpd.conf?

A. src.conf and mod.conf
B. srm.conf and access.conf
C. source.conf and security.conf
D. users.conf and sconfig.conf
E. htaccess.conf and src.conf

Answer: