

Actualtests.com

The Power of Knowing



Exam : 117-202

Title : Linux Networking Administration



Ver : 04-17-06

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. *Sybox 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 `dataport` 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. *Sybox 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://www-oss.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 'read-from <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_ugfiles.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 /etc/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§ion=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

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 than 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 daemon) 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 from 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>

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 if 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. arpswatch -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/passwd 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 is 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 'severity 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 "Chernobyl packet" or "xmas tree packet", and crashes some operating systems.) To log all such packets received, you would use:

- A. iptables -I INPUT -s 0.0.0.0/0 -d 192.168.0.44/33 --protocol tcp --xmas-pkt -j LOG
- B. iptables -I INPUT -s 0.0.0.0/0 -d 192.168.0.44/32 --protocol tcp --cher-pkt -j LOG
- C. iptables -I INPUT -s 0.0.0.0/0 -d 192.168.0.44/32 --protocol tcp --cher-pkt -log
- D. iptables -I 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 -I 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 examine '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.

:0

/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 GatewayGenmask 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 ssh-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-ftp, 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 MASQ. The 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 off and log on 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](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 module-type 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.freebsdidiary.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: B

QUESTION 109:

You are asked to set up a host with specified MAC and IP addresses in DHCP to use a particular DNS server with a specified IP. Which of the following lines would you add to the host entry of dhcpd.conf?

A. hardware use-mac-addr FF:FF:FF:FF:FF:FF; fixed-dns IP_ADDRESS; option domain-nameserver DNS_IP;

B. hardware ethernet FF:FF:FF:FF:FF:FF; fixed-address IP_ADDRESS; option domain-nameserver DNS_IP;

C. hardware ethernet FF:FF:FF:FF:FF:FF; dns-server IP_ADDRESS; option domain-nameserver DNS_IP;

D. hardware use-mac-addr FF:FF:FF:FF:FF:FF; default-dns IP_ADDRESS; option domainname-server DNS_IP;

Answer: B

QUESTION 110:

Convert the following BIND 4.9 named.boot entry to the equivalent BIND 8 named.conf entry.

secondary mysite.com 192.168.14.5 mysite.zone

A. zone "mysite.com" in {
type secondary;
file "mysite.zone";
masters {192.168.14.5};}

```
};  
B. zone "mysite.com" in {  
type secondary;  
zone "mysite.zone";  
masters {192.168.14.5;};  
};  
C. zone "mysite.com" in {  
type slave;  
zone "mysite.zone";  
masters {192.168.14.5;};  
};  
D. zone "mysite.com" {  
type slave;  
file "mysite.zone";  
masters {192.168.14.5;};  
};  
E. zone "mysite.com" in {  
type slave;  
file "mysite.zone";  
masters {192.168.14.5;};  
};
```

Answer: E

QUESTION 111:

You need to obtain a list of TCP ports that are currently listening for connections. How would you use netstat to list only those?

- A. netstat -l -t
- B. netstat -C --TCP
- C. netstat -n -X
- D. netstat -w -l

Answer: A

QUESTION 112:

You suspect that you are receiving messages with a forged From: address. What could help you find out where the mail is originating?

- install TCP wrappers, and log all connections on port 25
- add the command 'FR-strlog' to the sendmail.cf file
- add the command 'define('LOG_REAL_FROM')dnl' to the sendmail.mc file
- run a filter in the aliases file that checks the originating address when mail arrives
- look in the Received: and Message-ID: parts of the mail header

Answer: E

QUESTION 113:

You need to debug an outbound email address rewrite. What command would you pass to Sendmail to verify that it is working? Assume that Sendmail is already in test mode.

- A. /try smtp user@domain.com
- B. /try rewrite user@domain.com
- C. /try generics user@domain.com
- D. /try rewrite

Answer: B

QUESTION 114:

You are about to run ypinit on your system to build the NIS map file. Which file controls what files are to be made available via NIS?

- A. /var/yo/buildlist
- B. /var/yp/Makefile
- C. /etc/ypmake
- D. /etc/ypinit.conf
- E. /usr/yp/etc/conf

Answer: B

QUESTION 115:

You have decided to make the default FORWARD policy on your firewall REJECT. The rule you need is:

- A. iptables -t mangle -A FORWARD -j REJECT
- B. iptables -A FORWARD -j REJECT
- C. iptables -A FORWARD REJECT
- D. REJECT is not a valid policy

Answer:

QUESTION 116:

Which ONE of the following authentication activities has a significant risk of password sniffing?

- A. Logging onto an http website

- B. Logging onto a remote host using rsh and .rhosts files
- C. Logging onto an https website
- D. Logging onto a remote host using ssh

Answer: A

QUESTION 117:

You need to retrieve mail on a remote mailserver and distribute it to users on your local system. Which of the following could be used to accomplish this task? (Please make TWO selections.)

- A. elm
- B. pine
- C. fetchmail
- D. rmail
- E. procmail

Answer: C, D

QUESTION 118:

A coworker sets up an experimental MySQL server inside your office network. She wishes to test the server from home where she uses an ISP dialup to connect to the internet. You transparently forward port 3306 on your firewall to port 3306 on the internal server, but to improve security you wish to allow only connections from the ISP IP pool, which is in range 1.1.1.1 to 1.1.1.26. Please complete the following invocation of ipchains so that this requirement is met.

ipchains -A input -s ! _____/25 (- -dport) 3306 -j DENY
(Please type your answer in the text field below.)

Answer: 1.1.1.0

QUESTION 119:

How would you view the routing table on a host?

- A. route or netstat -r
- B. cat /proc/routes
- C. cat /etc/routes
- D. ifconfig -route

Answer: A

QUESTION 120:

You want a machine to look for a host in NIS and NIS+ and then stop if its not found. However, if NIS and NIS+ are not running, you want the machine to use DNS. If DNS fails, then it should try the /etc/hosts fle. Which of the following lines would you add to nsswitch.conf to accomplish this?

- A. hosts : nis nisplus dns /etc/hosts
- B. hosts : nis nisplus dns files
- C. hosts : nis nisplus [NOTFOUND=return] dns files
- D. hosts : nis nisplus [NOTFOUND=return] dns /etc/hosts
- E. hosts : nis nisplus dns [NOTFOUND=return] dns files

Answer: C

QUESTION 121:

What steps are required to activate changes to Sendmail's aliases file?

- A. run newaliases or sendmail -bi
- B. restart the sendmail daemon
- C. kill sendmail with SIGHUP
- D. invoke sendmail with hoststat
- E. run mkbd -f aliases

Answer: A

QUESTION 122:

When setting up an NFS server, you can use NIS groups to export the file systems. What file on the NIS master would you change to add or remove hosts from certain groups?

- A. The NIS group file.
- B. The NIS securenets file.
- C. The NIS hosts file.
- D. The NIS netgroups file.
- E. The NIS networks file.

Answer: D

QUESTION 123:

What is the role of the file /etc/ftpusers?

- A. Lists users allowed to use the ftp client
- B. Lists users allowed to use the ftp server
- C. Lists users NOT allowed to use the ftp client
- D. Lists users allowed to upload files via FTP

- E. Lists users NOT allowed to use the ftp server
- F. Lists users NOT allowed to upload files via FTP

Answer: E

QUESTION 124:

You are using a PAM aware sshd and you want to enable null password logins. What option would you add to the /etc/pam.d/sshd file to allow this?

- A. auth required /lib/security/pam_unix.so shadow nodelay passwd-no-req
- B. auth required /lib/security/pam_unix.so shadow nodelay no-passwd
- C. auth required /lib/security/pam_unix.so shadow nodelay nullpass
- D. auth required /lib/security/pam_unix.so shadow nodelay nullok
- E. auth required /lib/security/pam_unix.so shadow nodelay null-allowed

Answer: D

QUESTION 125:

Which line in the aliases file will cause emails to user devgroup to be sent to all users listed in /etc/aliases/devgroup?

- A. devgroup: ":list:/etc/aliases/devgroup"
- B. devgroup: ":file:/etc/aliases/devgroup"
- C. devgroup: ":include:/etc/aliases/devgroup"
- D. devgroup: ":read:/etc/aliases/devgroup"
- E. devgroup: "[:/etc/aliases/devgroup"

Answer: C

QUESTION 126:

You manage a network which receives password information from a NIS database. After a user changes his password, he finds that about half the system on the network use the new password and the rest do not. After waiting for a few hours, the rest of the systems start using the new password. What is the most likely cause of this?

- A. The master NIS server is not pushing changes to some of the slave servers.
- B. The system which take a few hours to update are in a different NIS domain.
- C. The permissions on /var/nis/ are not set correctly.
- D. PAM is caching password lookups.
- E. Some of the systems are using NIS+ and some are using NIS.

Answer: A

QUESTION 127:

This is a line from the file /etc/nsswitch.conf

hosts: files nis [NOTFOUND=return] dns

What does it mean?

- A. IP address resolution is handled by the local /etc/hosts file, NIS and DNS, in that order. If NIS returns a service not available message the search should halt.
- B. IP address resolution is handled by DNS, NIS and the local /etc/hosts file, in that order. If NIS returns a service not available message the search should halt
- C. IP address resolution is handled by the local /etc/hosts file, NIS and DNS, in that order. If NIS returns an address not found message the search should halt
- D. IP address resolution is handled by DNS, NIS and the local /etc/hosts file, in that order. If NIS returns an address not found message the search should halt
- E. IP address resolution is handled by the local /etc/hosts file, NIS and DNS, order not defined in this file. If NIS does NOT return a success message the search should halt

Answer: C

QUESTION 128:

You have just added a Linux machine named Linus to your network with an IP address of 192.168.1.11. You have a Linux firewall with an IP address of 192.168.1.1 which acts as a gateway to the Internet. You want all traffic that is destined for the Internet to go through the firewall. What invocation of the route command on the host named Linus will properly set this up?

- A. route add -net 255.255.255.255 gw 192.168.1.1
- B. route add default gw 192.168.1.1
- C. route add 192.168.1.0 gw 192.168.1.1
- D. route add -net 192.168.1.0 192.168.0.11
- E. route add 192.168.1.0 mask 255.255.255.0 gw 192.168.0.1

Answer: B

QUESTION 129:

Your website logs are showing a large number of file not found, or 404, errors. You would really like to have a way to catch these visitors and send them to a sitemap page. The Apache directive you need to use is:

- A. ErrorBounce
- B. Redirect
- C. MissingPage
- D. ErrorDocument

E. BounceUser

Answer: D

QUESTION 130:

Users have complained that their files in /tmp are being deleted by other users. You have investigated permissions on /tmp. Which of the following is the most likely explanation?

- A. Because /tmp must have permissions of 0777, there is no way to stop users from deleting anyone's files in /tmp.
- B. You should change permissions on /tmp to 0707, since group permissions of rwx allow users to delete other users files.
- C. You must change permission on /tmp to 4777 as this ensures that users can only delete their own files in /tmp
- D. Users are confused and can only delete their own files from /tmp even when its permissions are 0777
- E. You must set the sticky bit on /tmp with the 1777 permission mode to ensure that users can only delete their own temporary files.

Answer: E

QUESTION 131:

You believe your system has been compromised, and a trojan version of ls may have been installed. Your ad hoc method of listing files until you fix the problem is:

- A. /ls
- B. /bin/ls
- C. /sbin/ls
- D. echo *
- E. echo \$CWD

Answer: D

QUESTION 132:

You have been asked to set up a nameserver which blocks any DNS requests from a specific host or hosts. What is the appropriate entry in named.conf?

- A. forget {IP_ADDRESS; IP_ADDRESS};
- B. block {IP_ADDRESS; IP_ADDRESS};
- C. deny-req {IP_ADDRESS; IP_ADDRESS };
- D. blackhole {IP_ADDRESS; IP_ADDRESS};

Answer: D

QUESTION 133:

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

- A. NIS domain name
- B. The resolving order in the /etc/resolv.conf
- C. The priority order in the /net/nsswitch.conf
- D. The security settings of ipchains/iptables
- E. The content of the hosts.allow and hosts.deny

Answer: A

QUESTION 134:

You want to set up your system to accept e-mail aliases for domains other than your host system's actual domain. What file do you need to edit after editing sendmail.cf file?

- A. aliases
- B. passwd
- C. virtusertable
- D. mailusers
- E. maildomains

Answer: D

QUESTION 135:

In the zone file for foo.com, what is wrong with the following record?
MX 3 mail.foo.com

- A. MX priorities must be multiples of 10.
- B. It should be "MX mail.foo.com 3".
- C. The primary MX is mail.foo.com by default, and need not be specified.
- D. "mail.foo.com" is missing a period at the end.

Answer: D

Explanation: Fully Qualify Domain Name (FQDN) should end with period .

QUESTION 136:

How should you configure an internal nameserver to forward all queries to the firewall at 192.168.0.1?

- A. forward-only { 192.168.0.1; };
- B. forwarder { 192.168.0.1; }
- C. forward { 192.168.0.1;};
- D. forward only, forwarders { 192.168.0.1; };

Answer: D

Explanation: forwarders global options in /etc/named.conf forward the queries to another DNS server if that server doesn't have answer. forward only means caching only name server means answer from the cache. So, it will forward the queries to firewall server if this server doesn't have answer and reply to client from the cache.

QUESTION 137:

You have just installed a second NIC in your Linux system. Both eth0 and eth1 are configured and connectivity has been confirmed on each port. However, the routing of traffic between the two networks is not currently working. Which of the following will likely fix the problem?

- A. Manually updating your system's routing table
- B. `echo 1 > /proc/sys/net/ipv4/ip_forward`
- C. Running `ifconfig-route` on
- D. Running `route-enable eth0 eth1`
- E. Setting `/proc/sys/net/route/redirect_coount`

Answer: B

Explanation: We can modify the Running Kernel Parameter through the Virtual Filesystem /proc. In the question scenario, System as going use as Router for two different network. If IP forwarding is disabled then it can't forward the packets from one network to another network.

By default IP Forwarding Feature is disabled.

To enable for current session.

`echo "1" > /proc/sys/net/ipv4/ip_forward`

where 1 means enable the IP Forwarding and 0 means disable the IP Forwarding.

For Permanent use the file /etc/sysctl.conf

`Net.ipv4.IP_Forward=1 | 0`

QUESTION 138:

What would you add to /etc/aliases to cause all mail sent to foo to be piped through /usr/local/bin/fooread?

- A. `foo: ":run:usr/local/bin/fooread"`
- B. `foo: "|include:/usr/local/bin/fooread"`
- C. `foo: "include:/usr/local/bin/fooread"`

D. foo: ":/usr/local/bin/fooread"

Answer: B

QUESTION 139:

What is the name of the Apache tool used to create and maintain user authentication files?

Answer: htpasswd

Explanation: htpasswd command manager user files for basic authentication.

Example: htpasswd -c /etc/httpd/conf/mypasswd user1 à Which creates the user1 as a http user and add the username and password into /etc/httpd/conf/mypasswd file.

QUESTION 140:

Which of the following directives instructs Apache to respond to request on port 8080?
(Please make TWO selections.)

- A. Active 8080
- B. Port 8080
- C. Blind 8080
- D. Listen 8080
- E. Remap 80 8080

Answer: B, D

Explanation: port or listen directive instructs the apache to respond on specified port. By default http runs on 80 port If you want to run on different port: change the value of Listen portnumber

Example: Listen 8080 will run on 8080 port.

QUESTION 141:

You have a web server running behind the firewall on IP 192.168.0.5 and you want to allow public access. The firewall's external IP is 10.0.0.10. Determine which rule(s) is/are required to make this work (your default policy is ACCEPT for all chains):

- A. iptables -t nat -A PREROUTING -p tcp --dport 80 -j REDIRECT --to-destination 192.168.0.5:80
- B. iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT --to-destination 192.168.0.5:80
- C. iptables -t nat -A POSTROUTING -m multiport 80,443 -s 10.0.0.10 DNAT --to-destination 192.168.0.5:80
- D. iptables cannot do port forwarding, you need ipmasqadm

Answer: B

Explanation: DNAT -> set in the PREROUTING chain where filtering uses translated address.

```
iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT --to-destination 192.168.0.5:80
```

à When we apply this rule on Firewall server, when request comes on 80 port on server it redirects the request to 192.168.0.5 host on same port 80.

-p means protocol

--dport means destination port.

QUESTION 142:

You use pam_lastlog.so modules to make sure that an entry is made in lastlog during login. Under which authentication management type should this module be listed?

- A. auth
- B. account
- C. password
- D. session

Answer: D

Explanation: To identify the session of users, session control flags should use by pam_lastlog.so modules.

QUESTION 143:

You have configured Apache to forward requests to the company proxy, but you want it to serve some internal domains directly. How would you do this?

- A. NoProxy .some.example-domain.com, .some.other-example-domain.com
- B. IgnoreProxy .some.example-domain.com, .some.other-example-domain.com
- C. Run it on a different port.
- D. ProxyIgnore .some.example-domain.com, .some.other-example-domain.com

Answer: A

QUESTION 144:

Given a CIDR mask of /24 and a netmask of 255.255.255.0, how many usable host IP addresses are available?

_____ IP Addresses

(Please type your answer in the text field below.)

Answer: 254

Explanation: In /24 CIDR mask 24 bits is used for Network and 8 bits for Host.

You can calculate by converting in binary:

11111111.11111111.11111111.00000000

Total Number of Network=224-2=2622

Total Number of Host per Network= 28-2 = 254

QUESTION 145:

To use Kerberos services, you must first obtain a valid _____.

- A. domain-certificate
- B. primary-credential-packet
- C. ticket-key
- D. service-certificate
- E. ticket-granting-ticket

Answer: E

QUESTION 146:

How can you manually add an entry to your system's ARP cache?

- A. directly edit /etc/arp-cache
- B. add-arp hostname FF:FF:FF:FF:FF:FF
- C. ping -a hostname
- D. arp -s hostname FF:FF:FF:FF:FF:FF
- E. edit arp.conf and restart arpd

Answer: D

Explanation: arp -a àDisplays the all arp table

arp -s hostname MAC address àManually create an ARP address mapping entry for host hostname with MAC address.

QUESTION 147:

You need to view the complete kernel routing tables with IP addresses instead of hostnames. How would you use netstat to specify this?

- A. netstat -r -n
- B. netstat -e
- C. netstat --r -l
- D. netstat -i -l

Answer: A

Explanation: netstat is the multiple purpose command, which prints the network

connections, routing tables, interface statistics, masquerade connections and multicast memberships.

-r or --route àDisplay the kernel routing table with hostname.

--numeric or -n àShow numerical addresses instead of trying to determine symbolic host, port or use names.

QUESTION 148:

You are running a local DNS and HTTP server. While booting the system you see messages complaining about Apache not being able to resolve any VirtualHost entries. What may be the cause(s) of this?

(Please make TWO selections)

- A. The network is not yet configured, thus Apache is unable to run a DNS check of the virtual hosts.
- B. The network is up but named is not yet running, thus Apache is unable to run a DNS check of the virtual hosts.
- C. The VirtualHost directives for the hosts are incorrect in the httpd.conf file.
- D. The Apache process died before the virtual hosts were properly configured.

Answer: A, B

Explanation: Probably the cause is either network is not configure properly or named service is not running.

QUESTION 149:

You are writing a new IP packet sniffer. Of these libraries, which one would you have to link to your program?

- A. libtcpdump
- B. libnet
- C. libpcap
- D. libether
- E. libip

Answer: C

QUESTION 150:

You receive complaints that a user sends large attachments to hundreds of users. What command do you use to investigate the mail message queued for delivery?

- A. mailq
- B. sendmail -q
- C. mqueue

- D. qm
- E. lpq

Answer: A

Explanation: mailq command prints for each message shows the internal identifier used on this host for the message with a possible status character, the size of the message in bytes, the date and time the message was accepted into the queue, and the envelope sender of the message.

Syntax: mailq [-options]

-Ac àShow the mail submission queue specified in the /etc/mail/submit.cf instead of the MTA queue specified in /etc/mail/sendmail.cf.

-qL àshow the lost item in the mail queue.

QUESTION 151:

Your server is running Sendmail. The file /etc/mail/access contains the following line:

Somedomain.com 550

What does it mean?

- A. Your server relays mail from all servers on domain somedomain.com
- B. Your server relays mail from any server to domain somedomain.com
- C. Your server accepts mail from servers on domain somedomain.com, but will not relay it.
- D. Your server does not accept mail from servers on domain somedomain.com

Answer: D

Explanation: /etc/mail/access file is used to accept or deny the incoming mail.

somedomain.com RELAY àRelay all message from somedomain.com

somedomain.com OK àAccept the mail but don't relay from somedomain.com

somedomain.com REJECT àReject the mail from somedomain.com

somedomain.com 550 message àLike reject but returns with your message.

QUESTION 152:

The netstat -r command produces the following output:

```
192.168.1.0 * 255.255.255.0 U 40 0 0 eth1
```

Which of the following describes this line?

- A. 192.168.1.0 is the default gateway.
- B. The host 192.168.1.0 can be reached via the local NIC configured at /dev/eth1.
- C. The 255.255.255.0 network can be reached via the router at 192.168.1.0 out the NIC configured as eth1.
- D. The network, 192.168.1.0/24, is accessible through the local NIC configured as eth1.
- E. The router at 192.168.1.0, which is up (U), is sending and receiving Routing Information Protocol packets.

Answer: D

Explanation: netstat is the multi purpose command. netstat -r command displays the routing table. By default locally connected Network add on routing table.

Output is in this format:

Destination Gateway Netmask Flags MSS Window irtt Iface

Gateway * means all packets regarding this network will forward using the connected interface eth1

QUESTION 153:

What is the correct way to keep the root.hints file up-to-date?

- A. FTP the file from ds.internic.net
- B. It is updated automatically by named
- C. mail -s root.hints hostmaster@internic.net
- D. dig @m.root-servers.net . ns > root.hints

Answer: D

QUESTION 154:

After adding a new host to a zone, what should you do before restarting BIND?

- A. Update the DNS Secondaries.
- B. Increment the serial number for the zone.
- C. Make sure the new hostname and IP are in /etc/hosts on the primary nameserver.
- D. Make sure the new hostname and IP are in /etc/named.conf on the primary nameserver.
- E. Update the TTL in the zone files on the primary nameserver.

Answer: B

Explanation: Every Slave Name server points to the Master Name server. Slave Name server Synchronize to Master Name Server as specified time of refresh in Master Name Server. Either Modifying the Master Name Server or Adding new host to Master Name server, one mandatory things is update the serial number because slave name server check to master name server if serial name server is updated then slave name server copy from the master name server.

QUESTION 155:

You have created a user account that you wish to use for authenticated ftp access but you do not want the user to be able to login interactively. In order to achieve this, you have created a zero byte file named /bin/no-user-login and set the user's login shell to this file. Testing via ssh shows that the user can not login as expected but ftp logins are also failing.

In order to enable ftp logins using this setup, you will need to edit the _____ file.
(Please type your answer in the text field below.)

Answer: /etc/shells

Explanation: /etc/shells is a text file which contains the full pathnames of valid login shells. This file is consulted by chsh and available to be queried by other programs.

QUESTION 156:

You have found evidence that leads you to believe that your RPM-based Linux system may have been cracked; a number of strange directories have been found and there are unknown processes listening to port 6667. Using the standard RPM tools, how would you verify the integrity of your binaries as originally installed by your package management tool? (Type a single command with only necessary command line options.)
(Please type your answer in the text field below.)

Answer: rpm -a --verify
OR: rpm -aV

Explanation: rpm -a --verify verifying a package compares information about the installed files in the package with information about the files taken from then package metadata stored in the rpm database(/var/lib/rpm). Among other things, verifying compares the size, MD5 sum, permissions, type, owner and group of each file. Any discrepancies are displayed.

QUESTION 157:

You can cause named to reload its zone file by:
(Please make TWO selections.)

- A. named --reload-config
- B. killall -HUP named
- C. bind-server --restart
- D. ndc reload

Answer: B, D

Explanation: killall sends a signal to all processes running any of the specified commands. If no signal name is specified, SIGTERM is sent. Signals can be specified either by name eg. -HUP or by number).
ndc or rndc is a name server control utility, which control the operation of a name server.

QUESTION 158:

What would you use to display all ICMP packets on eth0?

- A. `iplog eth0`
- B. `tcpdump -i eth0 icmp`
- C. `icmpdump -i eth0`
- D. Put "`net.icmp /var/log/icmp`" into `/etc/syslog.conf` and `grep` for ICMP

Answer: B

Explanation: `tcpdump` prints out the headers of packets on a network interface that match the boolean expression.

Syntax: `tcpdump interface protocol`

Example: `tcpdump -i eth0 icmp` It shows all icmp packets traveling through eth0 interface.

QUESTION 159:

To avoid unnecessary downtime, you wish to check that your modified `httpd.conf` is syntactically valid without restarting the server. Which of the following commands would you use?

- A. `httpd -check`
- B. `apachectl verify`
- C. Run a non-production `httpd` with the same configuration file first.
- D. `httpd -reload`
- E. `apachectl configtest`

Answer: E

Explanation: `apachectl` is a HTTP server control interface .

Syntax: `apachectl [httpd-argument]`

`Configtest` à Run a Configuration file syntax test. It parses the configuration files and either reports Syntax OK or detailed information about the particular error. This is equivalent to `apachectl -t` .

QUESTION 160:

On a new DNS server configured to be secondary for a number of domains, a series of "lame server" warning messages are found in the local system log. These messages always include the IP address of the primary server but in reference to a few different and apparently unrelated domains. No other problems are reported and all DNS queries for all domains return the correct answers. Which configuration error is causing these warnings to be produced for those domains?

- A. The primary does not have the local server listed as a secondary.
- B. The local server is pointing to the wrong primary address.
- C. The primary is denying zone transfers to the secondary.

- D. The upper-level servers are not pointing to the primary as authoritative.
- E. The primary does not have an NS record pointing to itself.

Answer: E

QUESTION 161:

You are on a multi-user system with many people belonging to your groups. What is the LEAST restrictive permission your ~/.ssh/identity file may have while not compromising security?

- A. 0660
- B. 0644
- C. 0664
- D. 0600
- E. 0400

Answer: D

Explanation: Answer D is correct and Most correct permission value, which sets the read and write to owner user only and no permission to other users.
You can set this permission to ~/.ssh/authorized_keys file.

QUESTION 162:

You would like remote access to a Linux workstation via SSH. The system is on a network that is behind a firewall which blocks incoming connections to TCP ports below 1024. Which option in your sshd_config could you use to work around the firewall?

- A. GatewayPorts
- B. ListenAddress
- C. UseHighPorts
- D. PrivPort
- E. Port

Answer: E

Explanation: Port option in /etc/ssh/sshd_config should enable to use around the firewall. By default it runs on port 22.

QUESTION 163:

How would you run named inside a chroot jail as user nobody and group nogroup?

- A. Add "user nobody, group nogroup; chroot /var/named/root" to named.conf
- B. Named runs as nobody/nogroup by default, so just invoke it as "named -- chroot

/var/named/root"

- C. Use /usr/bin/chroot after running "chown nobody.nogroup named"
- D. Invoke named as "named -t /var/named/root -u nobody -g nogroup"

Answer: D

QUESTION 164:

Given the following configuration excerpt from the my.com zone file, BIND will refuse to load the zone because:

```
NS ns.my.com.  
NS ns1.my.com.  
MX 10 mail.my.com  
my.com. A 192.168.0.20  
Server A 192.168.0.20  
ns CNAME server  
www CNAME server  
mx A 192.168.0.20
```

- A. The NS records are in different zones.
- B. There are two records pointing to server as a CNAME.
- C. The MX host mail.my.com does not exist.
- D. The NS record is pointing to a CNAME entry.
- E. The CNAME for server does not have an origin tag.

Answer: D

Explanation: Name server for my.com is ns.my.com but NS Record pointing the CNAME entry to server so giving error.

QUESTION 165:

When setting up a Squid proxy server, what would be a reason to limit the incoming reply_body_max_size?

- A. Prevent overloading the cache_mem.
- B. Prevent user's from streaming large video or audio files.
- C. Prevent attacks on your proxy server's access port.
- D. Prevent users from downloading files over a certain size.
- E. Set a limit on the number of requests made to a single site by a single user.

Answer: D

Explanation: reply_body_max_size parameter is used prevent users from downloading very large files.

Example: reply_body_max_size size allow all

QUESTION 166:

Which port must be open on a firewall, to allow a DNS server to receive queries? (Enter only the port number).

Answer: 53

Explanation:

DNS Server uses the 53 port of UDP and TCP protocol. To allow DNS server to receive the queries 53 port number should open on firewall.

QUESTION 167:

According to the configuration below, what is the e-mail address of the administrator for this domain?

```
STTL 86400
$ORIGIN certkiller.com
@ IN SOA mars.certkiller.com hostmaster.certkiller.com/
      2005020801
      10800
      3600
      604800
      86400)
```

Answer: hostmaster@ Certkiller .com

Explanation:

Hostmaster. Certkiller .com specifies the contact person for the domain. Conventionally, the responsible party's email address is used, replacing the @ with dot.

QUESTION 168:

Which of these ways can be used to only allow access to a DNS server from specified networks/hosts?

- A. Using the limit{...;}statement in the named configuration file.
- B. Using the allow-query{...;}statement in the named configuration file.
- C. Using the answer only{...;}statement in the named configuration file.
- D. Using the answer{...;}statement in the named configuration file.
- E. Using the query access{...;}statement in the named configuration file.

Answer: B

Explanation: allow-query { list } à Specifies an address match list of hosts allowed to query this server. If this option is not set, any host can query the server.

Example

allow-query {192.168.0.0/24;}; à Only hosts from 192.168.0.0 network can query to DNS server.

QUESTION 169:

According to the BIND configuration file below, which of the following sentences is true?

```
options {
    directory "/var/named";
    allow-query { any; };
    allow-recursion { 127.0.0.1; 10.0.0.0/24; };
    forwarders { 192.168.0.4; };
    forward first;
};

zone "." {
    type hint;
    file "named.ca";
};
```

- A. Any host, from any network, may use this server as its main DNS server.
- B. If the server doesn't know the answer to a query, it sends a recursive query to 192.168.0.4.
- C. If the server doesn't know the answer to a query, it sends a query to a root DNS server.
- D. Hosts in the network 10.0.0.0/24 will be able to ask for zone transfers.
- E. If the server doesn't know the answer to a query, it sends a recursive query to 192.168.0.4 and, if this fails, it returns a failure.

Answer: B

Explanation: B is correct answer because forwarding the query to 192.168.0.4 if it doesn't have the answer.

forwarders -> Server forwards queries it can't answer to name servers at the IP Address in this list.

QUESTION 170:

Which of these would be the simplest way to configure BIND to return a different version number to queries?

- A. Compile BIND with the option -blur-version=my version.
- B. Set version-string "my version" in BIND's configuration file.
- C. Set version "my version" in BIND's configuration file.
- D. Set version=my version in BIND's configuration file.
- E. Set version-bind "my version" in BIND's configuration file.

Answer: C

QUESTION 171:

Performing a DNS lookup with dig results in this answer:

```
;; QUESTION SECTION:
;5.123.168.192.in-addr.arpa.    IN      PTR

;; ANSWER SECTION:
5.123.168.192.in-addr.arpa. 600 IN PTR    linuxerv.example.net.123.168.192.in-addr.arpa.

;; AUTHORITY SECTION:
123.168.192.in-addr.arpa. 600 IN NS      linuxerv.example.net

;; ADDITIONAL SECTION:
linuxerv.example.net.      600 IN A      192.168.123.5
```

What might be wrong in the zone definition?

- A. Nothing. All seems to be good.
- B. There's no "." after linuxerv.example.net in the PTR record in the forward lookup zone file.
- C. There's no "." after linuxerv in the PTR record in the forward lookup zone file.
- D. There's no "." after linuxerv.example.net in the PTR record in the reverse lookup zone file.
- E. The "." in the NS definition in reverse lookup zone has to be removed.

Answer: D

Explanation: Answer D is wrong because linuxerv.example.net is end with dot.

QUESTION 172:

What is the purpose of a PTR record?

- A. To provide name to IP resolution.
- B. To provide IP to name resolution.
- C. To direct email to a specific host.
- D. To provide additional host information.
- E. To direct clients to another nameserver.

Answer: B

Explanation:

PRT (Pointer) For reverse lookup that is PTR records specify the octets of the domain in the reverse order. For example if the zone were defined as 100.100.192.in-addr.arpa, then the name server would expand the PTR reference in the side into 3.100.100.192.in-addr-arpa.

QUESTION 173:

Some users are unable to connect to specific local hosts by name, while accessing hosts in other zones works as expected. Given that the hosts are reachable by their IP addresses, which is the default log file that could provide hints about the problem?

- A. /var/named/log
- B. /var/lib/named/dev/log
- C. /var/log/bind_errors
- D. /var/log/bind/errors

E. /var/log/messages

Answer: E

Explanation: /var/log/messages log file contains the standard log messages i.e user's session open, closed, service start, stop etc.

QUESTION 174:

DNSSEC is used for?

- A. Encrypted DNS queries between nameservers.
- B. Cryptographic authentication of DNS zones.
- C. Secondary DNS queries for local zones.
- D. Defining a secure DNS section.
- E. Querying a secure DNS section.

Answer: B

Explanation: dnssec-keygen command is used to generate the public and private keys used to secure communicate.

QUESTION 175:

Which is the preferred mail server for the domain example.com, according to the BIND configuration below? (Type the fully-qualified domain name.)

[..]

```
@ IN MX 10 mx-ny.certkiller.com
```

```
@ IN MX 50 mx-ca.certkiller.com
```

[..]

Answer: mx-ny. Certkiller .com

Explanation: mx-ny. Certkiller .com is the primary (preferred) mail server because check the MX value, lower server will get the preference.

QUESTION 176:

Which type of DNS record defines which server(s) email for a domain should be sent to?

Answer: MX

Explanation: DNS define the mail exchanger for the domain. To define the primary and secondary mail exchanger for domain should use MX record.

Example:

@ IN MX 5 mail.example.com

@ IN MX 10 mail1.example.com

Here mail.example.com is the primary mail exchanger for example.com domain and

mail1.example.com is the secondary mail exchanger for example.com.

QUESTION 177:

What is a significant difference between host and zone keys generated by dnssec-keygen?

- A. There is no difference.
- B. Both zone key files (.key/.private) contain a public and private key.
- C. Both host keys files (.key/. private) contain a public and private key.
- D.Host Keys must always be generated if DNSSEC is used; zone keys are optional
- E.Zone Keys must always be generated if is used; host keys are optional

Answer: B

Explanation: dnssec-keygen command is used to generate the public and private keys used to secure communicate.

QUESTION 178:

In which configuration file can a key-file be defined to enable secure DNS zone transfers?
(Please enter the file name without the path)

Answer: named.conf

Explanation: /etc/named.conf file is used to register zone, to set global options as well as key-file for rndc or ndc.

See the sample configuration of /etc/named.conf

```
//  
// named.conf for Red Hat caching-nameserver  
//  
acl "mynet" {192.168.3.0/24;192.168.4.0/24;192.168.2.0/24;};  
options {  
    directory "/var/named";  
    dump-file "/var/named/data/cache_dump.db";  
    statistics-file "/var/named/data/named_stats.txt";  
    /*  
    * If there is a firewall between you and nameservers you want  
    * to talk to, you might need to uncomment the query-source  
    * directive below. Previous versions of BIND always asked  
    * questions using port 53, but BIND 8.1 uses an unprivileged  
    * port by default.  
    */
```

```
// query-source address * port 53;
// forwarders {202.79.33.50; 202.79.33.35; };
};
//
// a caching only nameserver config
//
controls{
inet 127.0.0.1 allow { localhost; } keys {rndckey; };
};
zone"." IN {
type hint;
file "named.ca";
};
zone"localdomain" IN {
type master;
file "localdomain.zone";
allow-update { none; |l
};
zone"localhost" IN {
type master;
file "localhost.zone";
allow-update { none; |l
};
zone"0.0.127.in-addr.arpa" IN {
type master;
file "named.local";
allow-update { none; |l
};
zone"0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa
IN {
type master;
file "named.ip6.local";
allow-update { none; |l
};
zone"255.in-addr.arpa" IN {
type master;
file "named.broadcast";
allow-update { none; |l
};
zone"0.in-addr.arpa" IN {
type master;
file "named.zero";
allow-update { none; |l
};
zone"rhce.com" IN {
type master;
```

```
file "rhce.com.zone";  
};  
zone "example.com" IN {  
type master;  
file "example.com.zone";  
};  
zone "0.168.192.in-addr.arpa" IN {  
type master;  
file "0.168.192.zone";  
};  
include "/etc/rndc.key"; It is the Key file used to make secure  
the DNS communication.
```

QUESTION 179:

Which of these tools can provide the most information about DNS queries?

- A. dig
- B. nslookup
- C. host
- D. named - checkconf
- E. named - checkzone

Answer: A

Explanation: dig, nslookup and host commands send the request to DNS server specified in /etc/resolv.conf.

Among them dig command is the most useful and provides the most information of DNS queries.

QUESTION 180:

The mailserver is currently called fred, while the primary MX record points to mailhost.example.org. What must be done to direct example.org email towards fred?

- A. Add an A record for mailhost to fred's IP address.
- B. Add a CNAME record from mailhost to fred
- C. Add another MX record pointing to fred's IP address.
- D. Add a PTR record from mailhost to fred.

Answer: A

Explanation:

mailhost IN A IP Address

@ IN MX 5 mailhost.example.org

mailhost's Associated IP Address is fred's IP Address and primary Mail Exchanger of

example.org is mailhost.example.org, every mail to example.org send the mailhost.example.org host.

QUESTION 181:

As of Linux kernel 2.4, which software is used to configure a VPN?

- A. IPSec
- B. SSH
- C. net - tools
- D. FreeS/WAN
- E. iproute2

Answer: D

QUESTION 182:

Which option must be used with ifconfig, to also see interfaces that are down?

- A. - d
- B. -a
- C. --all
- D. --down
- E. None.

Answer: B

Explanation: ifconfig command is used to configure the network as well as to display the information of connected interfaces. By default it displays the information of interfaces, which is up.

Use the -a option to display the information of interface even interface is down.

QUESTION 183:

A server with 2 network interfaces, eth0 and eth1, should act as a router. eth0 has the IP address 192.168.0.1 in the subnet 192.168.0.1/24 and eth1 has the IP address 10.0.0.1 in the subnet 10.0.0.0/16. The routing table looks fine, but no data is traversing the networks. Which TWO of the following need to be done?

- A. Enable IP forwarding with echo "1" > /proc/sys/net/ipv4/ip_forward
- B. Add new firewall chains to handle inbound & outbound traffic on both interfaces.
- C. Reconfigure the firewall rules to allow traffic to traverse the networks.
- D. The routing table needs to be restarted, for the changes to take effect.
- E. The server needs to be restarted, for the changes to take effect.

Answer: A, C

Explanation: To act Linux system as a router, IP Forwarding should enable. If 0 value is set then disable the IP forwarding and 1 set the IP forwarding enable.

To change the value of running kernel

echo "1" >/proc/sys/net/ipv4/ip_forward à Which enable the ip forwarding for current session. To set permanently IP forwarding

net.ipv4.ip_forward=1 in /etc/sysctl.conf file.

As well as to forward the packets from one network to another network rule should be allow to forward.

QUESTION 184:

What file should be edited to make the route command show human-readable names for networks? (Please enter the full path)

Answer: /etc/networks

QUESTION 185:

Running tcpdump -nli eth1 'icmp' shows the following output:

11:56:35.599063 IP 192.168.123.5 > 194.25.2.129: icmp 64: echo request seq 1

11:56:35.670910 IP 194.25.2.129 > 192.168.123.5: icmp 64: echo reply seq 1

What command was used on the host 192.168.123.5, to generate this output?

Answer: ping

Explanation: icmp (Internet Control Message Protocol) is used by ping command.

QUESTION 186:

If the command arp -f is run, which file will be read by default?

- A. /etc/hosts
- B. /etc/ethers
- C. /etc/arp.conf
- D. /etc/networks
- E. /var/cache/arp

Answer: B

Explanation: arp command manipulates the system ARP (Address Resolution Protocol) cache.

arp -a à To display all ARP entry from the system.

arp -f

à Similar to -s manually creates an ARP address mapping entry for host hostname with

hardware address set to hw_addr class. If you use the -f option address information is taken from the file. Default filename is /etc/ethers.

QUESTION 187:

Which of the following tools, on its own, can provide dial-in access to a server?

- A. mingetty
- B. pppd
- C. dip
- D. chat
- E. mgetty

Answer: E

Explanation: mgetty is a smart getty replacement, designed to be used with Hayes compatible data and data/fax modems.
You should write in /etc/inittab file to provide the response by init to dialup users.

QUESTION 188:

Which TWO of the following commands could be used to add a second IP address to eth0?

- A. ifconfig eth0 - add ip 192.168.123.10
- B. ifconfig eth0:1 192.168.123.10
- C. ifconfig eth0 1 192.168.123.10
- D. ifconfig eth0 +192.168.123.10
- E. ifconfig eth0:sub1 192.168.123.10

Answer: B, E

Explanation: ifconfig command is used to configure and display the network information. To display the information use ifconfig command. As well as to set the IP Address for current session: ifconfig eth0 ip address
If you want to add more than one IP address
ifconfig eth0:0 IP address where :0 is called clone number
Another way :
ifconfig eth0:sub1 IP address
If you want to set the IP address permanently
vi /etc/sysconfig/network-scripts/ifcfg-eth0:0
IPADDR=X.X.X.X
NETMASK=X.X.X.X

QUESTION 189:

What is the command to add another IP address to an interface that already has (at least)

one IP address?

- A. ifconfig eth0:1 192.168.1.2
- B. ifconfig eth0 192.168.1.2
- C. ipconfig eth0:1 192.168.1.2
- D. ipconfig eth0 192.168.1.2

Answer: A

Explanation: ifconfig command is used to configure and display the network information.

To display the information use ifconfig command. As well as to set the IP Address for

current session: ifconfig eth0 ip address

If you want to add more then one IP address

ifconfig eth0:0 IP address à where :0 is called clone number

If you want to set the IP address permanently

vi/etc/sysconfig/network-scripts/ifcfg-eth0:0

IPADDR=X.X.X.X

NETMASK=X.X.X.X

QUESTION 190:

When configuring a PPP dial-in server, which option is used (in the pppd configuration file) to enable user authentication against the system password database?

- A. login
- B. auth
- C. local
- D. password
- E. user

Answer: A

Explanation: To enable user authentication using the ppp is enable using login option on pppd configuration file.

QUESTION 191:

Considering the following kernel IP routing table below, which of the following commands must be used to remove the route to the network 10.10.1.0/24?

Kernel IP routing table							
Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
200.207.199.162	0.0.0.0	255.255.255.255	UH	0	0	0	ppp0
172.16.87.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0
192.168.246.0	0.0.0.0	255.255.255.0	U	0	0	0	eth1
10.10.1.0	192.168.246.11	255.255.255.0	UG	0	0	0	eth1
127.0.0.0	0.0.0.0	255.0.0.0	U	0	0	0	lo
0.0.0.0	200.207.199.162	0.0.0.0	UG	0	0	0	ppp0

- A. route del 10.10.1.0
- B. route del 10.10.1.0/24

- C. route del - net 10.10.1.0/24
- D. route del 10.10.1.0/24 gw 192.168.246.11
- E. route del -net 10.10.1.0

Answer: C

Explanation:

route add | del -net | -host netaddress|host address netmask gw next hop

Example:

route add -net 192.168.4.0 netmask 255.255.255.0 gw 192.168.0.2

where 192.168.4.0 is the remote network 255.255.255.0 is the netmask of remote network

192.168.0.2 is the gateway for remote network.

route add -host 192.168.0.1 255.255.255.0 gw 192.168.1.1

It is a route to 192.168.0.1 host

Similarly to remove the route from routing table: route del -net network address netmask

QUESTION 192:

According to the tcpdump output below, what is the IP address of the client host?

```
02:12:40.511381 IP 192.168.246.11.1045 > 192.168.246.1.22: S 3838532429:3838532429(0) win 5840 <seq 1460,ackOK,timestamp 31325740,nop,wscale 2>  
02:12:40.511540 IP 192.168.246.1.22 > 192.168.246.11.1045: S 1209330085:1209330085(0) ack 383853 2430 win 5792 <seq 1460,ackOK,timestamp 11553457 3132574,nop,wscale 0>  
02:12:40.511755 IP 192.168.246.11.1045 > 192.168.246.1.22: . ack 1 win 1460 <nop,nop,timestamp 3 132574 11553457>  
02:12:40.515122 IP 192.168.246.1.22 > 192.168.246.11.1045: F 1:26(25) ack 1 win 5792 <nop,nop,timestamp 11553460 3132574>  
02:12:40.515511 IP 192.168.246.11.1045 > 192.168.246.1.22: . ack 26 win 1460 <nop,nop,timestamp 3132578 11553460>  
02:12:40.515952 IP 192.168.246.11.1045 > 192.168.246.1.22: F 1:23(22) ack 26 win 1460 <nop,nop,timestamp 3132578 11553460>
```

Answer: 192.168.246.11

Explanation: See on the last output, 192.168.246.11.1045 where 1045 is the port number.

Sending packets to 192.168.246.1.22 where 22 is the port number.

Output Syntax is:

Time.packetssize IP client Address > Server IP Address protocol

QUESTION 193:

What command must be used to print the kernel's routing table?

- A. route print
- B. route enumerate
- C. route show
- D. route list
- E. route

Answer: E

Explanation: route command shows or manipulate the IP routing table.

QUESTION 194:

The following is an excerpt from the output of `tcpdump -nli eth1 'udp'`:

13:03:17.277327 IP 192.168.123.5.1065 > 192.168.5.112.53: 43653+ A? lpi.org. (25)

13:03:17.598624 IP 192.168.5.112.53 > 192.168.123.5.1065: 43653 1/0/0 A 24.215.7.109 (41)

Which network service or protocol was used?

- A. FTP
- B. HTTP
- C. SSH
- D. DNS
- E. DHCP

Answer: D

Explain: `tcpdump` prints out the headers of packets on a network interface that match the Boolean expression.

Output is to display the packets using UDP protocol

See the output that port is 53. DNS uses the 53 UDP port.

QUESTION 195:

A network client has an ethernet interface (eth0) configured with an IP address in the subnet 192.168.0.0/24. This subnet has a router, with the IP address 192.168.0.1, that connects this subnet to the Internet. What needs to be done on the client to enable it to use the router as its default gateway?

- A. Run `route add default gw 192.168.0.1 eth1`.
- B. `route add gw 192.168.0.1 eth1`
- C. `ifconfig eth0 defaultroute 192.168.0.1`.
- D. Add "`defaultroute 192.168.0.1`" to `/etc/resolv.conf`.
- E. `route add defaultgw=192.168.0.1 if=eth0`.

Answer: A

Explanation:

In the Network there is a router having 192.168.0.1 IP Address. So we should set the gateway to 192.168.0.1 to all clients.

`route add default gw 192.168.0.1`

QUESTION 196:

What command is used to add a route to the 192.168.4.0/24 network via 192.168.0.2?

- A. `route add - network 192.168.4.0 netmask 255.255.255.0 gw 192.168.0.2`
- B. `route add - net 192.168.4.0/24 gw 192.168.0.2`
- C. `route add - network 192.168.4.0/24 192.168.0.2`
- D. `route add - net 192.168.4.0 netmask 255.255.255.0 192.168.0.2`
- E. `route add - net 192.168.4.0 netmask 255.255.255.0 gw 192.168.0.2`

Answer: E

Explanation:

route add | del -net | -host netaddress|host address netmask gw next hop

Example:

route add -net 192.168.4.0 netmask 255.255.255.0 gw 192.168.0.2

where 192.168.4.0 is the remote network 255.255.255.0 is the netmask of remote network

192.168.0.2 is the gateway for remote network.

route add -host 192.168.0.1 255.255.255.0 gw 192.168.1.1

It is a route to 192.168.0.1 host

QUESTION 197:

The users of the local network complain that name resolution is not fast enough. Enter the command, without the path or any options, that shows the time taken to resolve a DNS query.

Answer: dig

Explanation: dig command displays the Query time to DNS Server

dig www.example.com

Query Time: 2 msec

SERVER 192.168.0.254#53

WHEN date

MSG SIZE rcvd: 77

QUESTION 198:

Which Apache directive allows the use of external configuration files defined by the directive AccessFileName?

A. AllowExternalConfig

B. AllowAccessFile

C. AllowConfig

D. IncludeAccessFile

E. AllowOverride

Answer: E

Explanation: AccessFileName directive is used to look file for each directory for additional configuration directives. By default it looks .htaccess file.

To use the .htaccess file on each virtual host for use authentication we should call using AllowOverride

See the sample Configuration:

<VirtualHost 192.168.0.100>

```
ServerName www.abc.com
DocumentRoot /var/www/abc
DirectoryIndex index.html
<Directory /var/www/abc/>BR> AllowOverride Authconfig
</Directory>BR> ErrorLog logs/abc.error
</VirtualHost>
```

QUESTION 199:

A web server is expected to handle approximately 200 simultaneous requests during normal use with an occasional spike in activity and is performing slowly. Which directives in httpd.conf need to be adjusted?

- A. MinSpareServers & MaxSpareServers.
- B. MinSpareServers, MaxSpareServers, StartServers & MaxClients.
- C. MinServers, MaxServers & MaxClients.
- D. MinSpareServers, MaxSpareServers, StartServers, MaxClients & KeepAlive.

Answer: B

Explanation:

StartServers à Number of Server Processes to start by default 8

MinSpareServers à Minimum Number of server processes which are kept spare by default 5

MaxSpareServers à Maximum number of server processes which are kept spare by default

ServerLimit à Maximum Value for MaxClients for the lifetime of the server by default 256

MaxClients à Maximum number of server processes allowed to start by default 256

QUESTION 200:

Enter one of the Apache configuration file directives that defines where log files are stored.

Answer: ErrorLog

Explanation: ErrorLog directive define the path of error log file. You can create different error log file as per virtualhost.

See the sample Configuration

```
<VirtualHost 192.168.0.100>
```

```
ServerName www.abc.com
```

```
DocumentRoot /var/www/abc
```

```
DirectoryIndex index.html
```

```
ErrorLog logs/abc.error
```

```
</VirtualHost>
```

QUESTION 201:

Which file, in the local file-system, is presented when the client requests `http://server/~joe/index.html` and the following directive is present in server's Apache configuration file?

UserDir site/html

Given that all users have their home directory in `/home`, please type in the FULL file name including the path.

Answer: `/home/joe/site/html/index.html`

Explanation:

The UserDir directive allows users to have a separate space for their own web documents. If `/home/joe/site/index.html` existed and UserDir was set to `site/index.html` then a request to `http://server/~joe` would read documentation from `/home/joe/site/`.

QUESTION 202:

The listing below is an excerpt from a Squid configuration file:
Which of the following is true?

```
[...]
acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl to_localhost dst 127.0.0.0/8
acl SSL_ports port 443
acl Safe_ports port 80 443 1025-65535
acl CONNECT method CONNECT
acl localhost src 10.0.0.0/24

http_access allow manager localhost
http_access deny manager
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localnet
[...]
```

- A. Users connecting from localhost will be able to access web sites through this proxy.
- B. It's necessary to include a `http_access` rule denying access to all , at the end of the rules.
- C. It's possible to use this proxy to access SSL enabled web sites listening on any port.
- D. This proxy can't be used to access FTP servers listening on the default port.
- E. This proxy is misconfigured and no user will be able to access web sites through it.

Answer: D

Explanation: On output connection only to certain ports are allowed. i.e 80 443 1025-65535
All other ports except then `safe_ports` are denied so ftp is not included on `safe_ports` acl.

QUESTION 203:

The Internet gateway connects the clients with the Internet by using a Squid proxy. Only the clients from the network `192.168.1.0/24` should be able to use the proxy. Which of the following configuration sections is correct?

- A. `acl local src 192.168.1.0/24 http_allow local`

- B. `acl local src 192.168.1.0/24 http_access allow local`
- C. `acl local src 192.168.1.0/24 http access allow local`
- D. `acl local src 192.168.1.0/24 http_access_allow=local`
- E. `acl local src 192.168.1.0/24 httpd local allow`

Answer: B

Explanation:

To allow or deny to access the Internet , we should create the acl. Then allow or deny to acl.

Example:

```
acl mynet src 192.168.0.0/24
```

```
http_access mynet allow
```

QUESTION 204:

Which Squid configuration directive defines the authentication method to use?

- A. `auth_param`
- B. `auth_method`
- C. `auth_program`
- D. `auth_mechanism`
- E. `proxy_auth`

Answer: A

Explanation:

Edit `squid.conf`; specifically, you need to define the authentication program in `squid.conf`, which

is in this case `ncsa_auth`. Next, create an ACL named `ncsa_users` with the `REQUIRED` keyword that forces Squid to use the NCSA `auth_param` method you defined previously. Finally, create an `http_access` entry that allows traffic that matches the `ncsa_users` ACL entry. Here's a simple user authentication example; the order of the statements is important

```
#
```

```
# Add this to the auth_param section of squid.conf
```

```
#
```

```
auth_param basic program /usr/lib/squid/ncsa_auth /etc/squid/squid_passwd
```

```
#
```

```
# Add this to the bottom of the ACL section of squid.conf
```

```
#
```

```
aclncsa_users proxy_auth REQUIRED
```

```
#
```

```
# Add this at the top of the http_access section of squid.conf
```

```
#
```

```
http_access allow ncsa_users
```

QUESTION 205:

Which Apache directive is used to configure the main directory for the site, out of which it will serve documents?

- A. ServerRoot
- B. UserDir
- C. DirectoryIndex
- D. Location
- E. DocumentRoot

Answer: E

Explanation:

To specify the Main directory for the documents of website we should use the DocumentRoot directive.

See the sample Configuration

```
<VirtualHost 192.168.0.100>
```

```
ServerName www.example.com
```

```
DocumentRoot /var/www/example à The Directory contains the main documents of  
www.example.com
```

```
</VirtualHost>
```

QUESTION 206:

Users in the acl named 'sales_net' must only be allowed to access to the Internet at times specified in the time_acl named 'sales_time'. Which is the correct http_access directive, to configure this?

- A. http_access deny sales_time sales_net
- B. http_access allow sales_net sales_time
- C. http_access allow sales_net and sales_time
- D. allow http_access sales_net sales_time
- E. http_access sales_net sales_time

Answer: B

Explanation:

aclhome_network src 192.168.1.0/24 à Create the ACL for 192.168.1.0/24 Network

aclbusiness_hours time M T W H F 9:00-17:00 à Create the ACL for Allowed time

```
#
```

```
# Add this at the top of the http_access section of squid.conf
```

```
#
```

```
http_access allow home_network business_hours à Allow to home network on allowed hour.
```

QUESTION 207:

Which of the following is recommended to reduce Squid's consumption of disk resources?

- A. Disable the use of access lists.
- B. Reduce the size of cache_dir in the configuration file.
- C. Rotate log files regularly.
- D. Disable logging of fully qualified domain names.
- E. Reduce the number of child processes to be started in the configuration file.

Answer: B

Explanation: In Squid configuration file /etc/squid/squid.conf file cache directory and size of cache directory is specified. If you want to consume the disk space reduce the size of cache directory.

QUESTION 208:

When Apache is configured to use name-based virtual hosts:

- A. it's also necessary to configure a different IP address for each virtual host.
- B. the Listen directive is ignored by the server.
- C. it starts multiple daemons (one for each virtual host).
- D. it's also necessary to create a VirtualHost block for the main host.
- E. only the directives ServerName and DocumentRoot may be used inside a block.

Answer: D

Explanation: See the Sample Configuration of Name Based Virtual Host

NameVirtualHost 192.168.0.1

<VirtualHost www.abc.com>

Servername www.abc.com

DocumentRoot /var/www/abc

DirectoryIndex index.html index.htm index.php

ServerAdmin webmaster@abc.com

</VirtualHost>

<VirtualHost www.example.com>

Servername www.example.com

DocumentRoot /var/www/example

DirectoryIndex index.html index.htm index.php

ServerAdmin webmaster@example.com

</VirtualHost>

So, First You should specified the IP Address in which you are going to create multiple Name Based Virtual Host. As well as you should create the multiple virtual host directive

QUESTION 209:

There is a restricted area in an Apache site, which requires users to authenticate against the file /srv/www/security/site-passwd. Which command is used to CHANGE the password of existing users, without losing data, when Basic authentication is being used.

- A. htpasswd -c /srv/www/security/site passwd user
- B. htpasswd /srv/www/security/site -passwd user
- C. htpasswd -n /srv/www/security/site -passwd user
- D. htpasswd -D /srv/www/security/site -passwd user
- E. None of the above.

Answer: B

Explanation:

For User based Authentication, you should create the htpasswd user.

First Time To create the user:

htpasswd -c filename username

From Second Time either to change the password of httpuser or to append other http user

htpasswd -m filename username

QUESTION 210:

In the file /var/squid/url_blacklist is a list of URLs that users should not be allowed to access. What is the correct entry in Squid's configuration file to create an acl named blacklist based on this file?

- A. acl blacklist urlpath_regex /var/squid/url_blacklist
- B. acl blacklist file /var/squid/url_blacklist
- C. acl blacklist "/var/squid/url_blacklist"
- D. acl blacklist urlpath_regex "/var/squid/url_blacklist"
- E. acl urlpath_regex blacklist /var/squid/url_blacklist

Answer: D

Explanation: In Squid proxy Server, either we can block the URL by creating individual ACL i.e

acl deny site dstdomain .yahoo.com

http_access deny dstdomain

And it is very difficult to declare the individual ACL name to individual URL. So we can create the File contains all URL to be blocked and we can set

acl blacklist urlpath_regex "File with path"

http_access deny blacklist

QUESTION 211:

Which of the following sentences is true about ISC DHCP?

- A. It can't be configured to assign addresses to BOOTP clients.
- B. Its default behavior is to send DHCPNAK to clients that request inappropriate addresses.
- C. It can't be used to assign addresses to X - terminals.
- D. It can be configured to only assign addresses to known clients.
- E. None of the above.

Answer: D

Explanation: ISC DHCP can be configured to assign the IP address only to known clients.

QUESTION 212:

Which command can be used to change the password for an LDAP entry?

Answer: `ldappasswd`

Explanation: `ldappasswd` is a tool to set the password of an LDAP user.

QUESTION 213:

Which `dhcpd.conf` option defines the DNS server address(es) to be sent to the DHCP clients?

- A. `Domainname`
- B. `domain - name servers`
- C. `domain -nameserver`
- D. `domain - server`

Answer: B

Explanation:

Domain Name Server is specified in `dhcpd.conf` file using `domain-name-servers` option.

See the sample Configuration

See the sample Configuration:

```
1. vi /etc/dhcpd.conf
ddns-update-style none;
options routers 192.168.0.1;
option domain-name "example.com";
option domain-name-servers 192.168.0.254;
default-lease-time 1234;
max-lease-time 12345;
subnet 192.168.0.0 netmask 255.255.255.0
range 192.168.0.2 192.168.0.100;
range 192.168.0.150 192.168.0.250;
```

```
{
host server2
{
hardware Ethernet 12:12:12:34:34:e3;
fixed-address 192.168.0.2;
}
}
```

In this sample configuration: domain name is example.com

Gateway is 192.168.0.1

DNS server is 192.168.0.254

That host having MAC address 12:12:12:34:34:e3 assign always fixed address 192.168.0.2.

QUESTION 214:

To configure an LDAP service in the company " Certkiller Ltd", which of the following entries should be added to slapd.conf, in the Database Directives section, to set the rootdn so that the common name is Manager and the company's domain is Certkiller .com ?

- A: rootdn cn=Manager dc= Certkiller dc=com
- B: rootdn "cn=Manager,dc= Certkiller ,dc=com"
- C: rootdn cn= Certkiller ,dc=com,dc=Manager
- D: rootdn "cn= Certkiller ,dc=com,dc=Manager"
- E: rootdn "cn=Manager dc= Certkiller dc=com"

Answer: B

Explanation:

/etc/opeldap/slapd.conf file is used to specify the rootdn as well as domain controller.

Under database section:

rootdn "cn=Manager, dc=" Certkiller dc=com"

As well as you should specify the password either in plain text format or in encrypted format.

rootpw plaintextpassword

rootpw encrypted password

QUESTION 215:

In which directory are the PAM modules stored?

Answer: /lib/security

Explanation: All PAM modules are stored in /lib/security directory, PAM based application /etc/pam.d/ and PAM configuration file in /etc/security/

QUESTION 216:

LDAP-based authentication against a newly-installed LDAP server does not work as

expected. The file /etc/pam.d/login includes the following configuration parameters. Which of them is NOT correct?

- A. password required /lib/security/pam_ldap.so
- B. auth sufficient /lib/security/pam_ldap.so use_first_pass
- C. account sufficient /lib/security/pam_ldap.so
- D. password required /lib/security/pam_pwdb.so
- E. auth required /lib/security/pam_ldap.so

Answer: E

Explanation: To control the ldap based authentication through the PAM, Auth is not a required test.

QUESTION 217:

Which of the following is true, when a server uses PAM authentication and both /etc/pam.conf & /etc/pam.d/ exist?

- A. It causes error messages.
- B. /etc /pam.conf will be ignored.
- C. /etc / pam.d/ will be ignored.
- D. Both are used, but /etc/pam.d/ has a higher priority.
- E. Both are used. but /etc/pam.conf has a higher priority.

Answer: B

Explanation: All PAM (Pluggable Authentication Modules) Stores in /etc/pam.d/. If both /etc/pam.conf as well as /etc/pam.d/ exists then it will ignore the /etc/pam.conf (deprecated file).

QUESTION 218:

The host, called " Certkiller ", with the MAC address "08:00:2b:4c:59:23", should always be given the IP address of 192.168.1.2 by the DHCP server. Which of the following configurations will achieve this?

- A. host Certkiller {
hardware-ethernet08:00:2b.4c.:59:23;
fixed-address 192.168.1.2;
}
- B. host Certkiller {
mac=08:00:2b.4c.:59:23;
ip= 192.168.1.2;
}
- C. host Certkiller = 08:00:2b.4c:59:23 192.168.1.2

```
D. host Certkiller {  
hardware-ethernet08:00:2b.4c.:59:23;  
fixed-address 192.168.1.2;  
}  
E. host Certkiller {  
hardware-address08:00:2b.4c.:59:23;  
fixed-ip 192.168.1.2;  
}
```

Answer: D

Explanation:

To assign the Fixed IP address to host by examining the MAC address we should use the host hostname {

hardware ethernet MAC address à It is a MAC address of host
fixed-address IP Address à To assign the fixed IP address to host.
}

By default DHCP server assigns the IP address to host by random basis. If you want to assign static IP through DHCP server you should write this.

See the sample Configuration:

```
1. vi /etc/dhcpd.conf  
ddns-update-style none;  
options routers 192.168.0.1;  
option domain-name "example.com";  
option domain-name-servers 192.168.0.254;  
default-lease-time 1234;  
max-lease-time 12345;  
subnet 192.168.0.0 netmask 255.255.255.0  
{  
range 192.168.0.2 192.168.0.100;  
range 192.168.0.150 192.168.0.250;  
host server2  
{  
hardware Ethernet 12:12:12:34:34:e3; fixed-address 192.168.0.2; }  
}
```

In this sample configuration: domain name is example.com

Gateway is 192.168.0.1

DNS server is 192.168.0.254

That host having MAC address 12:12:12:34:34:e3 assign always fixed address 192.168.0.2.

QUESTION 219:

What is the advantage of using SASL authentication with OpenLDAP?

- A. It can prevent the transmission of plain text passwords over the network.
- B. It disables anonymous access to the LDAP server.

- C. It enables the use of Access Control Lists.
- D. It allows the use of LDAP to authenticate system users over the network.
- E. All of the above.

Answer: A

Explanation: SASL authentication is used to send the encrypted password then plain text password over the network.

QUESTION 220:

According to the dhcpd.conf file below, which domain name will clients in the 172.16.87.0/24 network get?

```
default-lease-time 1800;
max-lease-time 7200;
option domain-name "certkiller.com"

subnet 172.16.87.0 netmask 255.255.255.0 {
    range 172.16.87.128 172.16.87.254;
    option broadcast-address 172.16.87.255;
    option domain-name-servers 172.16.87.1;
    option domain-name "lab.certkiller.com";
}

subnet 172.16.88.0 netmask 255.255.255.0 {
    range 172.16.88.128 172.16.88.254;
    option broadcast-address 172.16.88.255;
    option domain-name-servers 172.16.88.1;
}
```

Answer: lab. Certkiller .com

Explanation:

Correct is lab. Certkiller .com, in /etc/dhcpd.conf file domain name is specified using domain-name option. As well as Domain Name Server is specified using domain-name-servers option.

See the sample Configuration:

```
1. vi /etc/dhcpd.conf
ddns-update-style none;
options routers 192.168.0.1;
option domain-name "example.com";
option domain-name-servers 192.168.0.254;
default-lease-time 1234;
max-lease-time 12345;
subnet 192.168.0.0 netmask 255.255.255.0
{
    range 192.168.0.2 192.168.0.100;
    range 192.168.0.150 192.168.0.250;
    host server2
    {
        hardware Ethernet 12:12:12:34:34:e3;
```

```
fixed-address 192.168.0.2;  
}  
}
```

In this sample configuration: domain name is example.com

Gateway is 192.168.0.1

DNS server is 192.168.0.254

That host having MAC address 12:12:12:34:34:e3 assign always fixed address 192.168.0.2.

QUESTION 221:

What is the correct format for an ftpusers file entry?

- A. Use only one username on each line.
- B. Add a colon after each username.
- C. Add a semicolon after each username.
- D. Add ALLOW after each username.
- E. Add DENY after each username.

Answer: A

Explanation: Either to deny or allow the users login through FTP service you should write the one username at each line.

See the sample of /etc/vsftpd.ftpusers

```
root  
bin  
daemon  
adm  
lp  
shutdown
```

QUESTION 222:

The command route shows the following output:

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
194.168.123.5	-	255.255.255.255	!H	0	-	0	-
192.168.123.0	0.0.0.0	255.255.255.0	U	0	-	0	eth2
169.254.0.0	0.0.0.0	255.255.0.0		0	-	0	eth0
127.0.0.0	0.0.0.0	255.0.0.0		0	-	0	lo
0.0.0.0	192.168.123.254	0.0.0.0	UG	0	0	0	eth0

Which of the following statements is correct?

- A. The network 169.254.0.0 is not a valid route.
- B. The host 194.168.123.5 is temporarily down.
- C. The host route 194.168.123.5 is rejected by the kernel.
- D. The "!H" signals that traffic to the host 194.168.123.5 is dropped.
- E. The network path to the host 194.168.123.5 is not available.

Answer: C

Explanation: Using route -n or netstat -rn command can display the routing table. By default, Linux system add the Local connected network on routing table. For each allowed entry it shows the gateway, netmask as well as interface. If There is - in the place of gateway or interface that route is rejected by system kernel.

QUESTION 223:

Which TWO of the following statements about xinetd and inetd are correct?

- A. xinetd supports access control by time.
- B. xinetd only supports TCP connections.
- C. xinetd is faster than inetd and should be preferred for this reason.
- D. xinetd includes support for X connections.
- E. xinetd and inetd are used to reduce the number of listening daemons.

Answer: A, E

Explanation: Before xinetd transient daemon are controlled by inetd super daemon. xinetd daemon supports the time based authentication (ALC)

If you write in /etc/xinetd.conf

access_times = 09:30-17:30

All transient daemons are allow to access between 9:30 to 17

Other options are:

instances = 60

How many instances should listen ?

per_source = ?

How many connection can get by one dedicate connection ?

If you set these options on /etc/xinetd.conf (the global configuration file for transient daemon) it applies to all xinetd based services. If you want to modify on individual service can you edit the individual service file in /etc/xinetd.d/

QUESTION 224:

What security precautions must be taken when creating a directory into which files can be uploaded anonymously using FTP?

- A. The directory must not have the execute permission set.
- B. The directory must not have the read permission set.
- C. The directory must not have the read or execute permission set.
- D. The directory must not have the write permission set.
- E. The directory must not contain other directories.

Answer: B

QUESTION 225:

When the default policy for the iptables INPUT chain is set to DROP, why should a rule allowing traffic to localhost exist?

- A: All traffic to localhost must always be allowed.
- B: It doesn't matter; iptables never affects packets addressed to localhost
- C: Sendmail delivers emails to localhost
- D: Some applications use the localhost interface to communicate with other applications.
- E: syslogd receives messages on localhost

Answer: D

Explanation:

Some application communicate to localhost ie gdm, xdm etc so Rule to INPUT chain should ACCEPT to localhost. Otherwise all packets from localhost will drop then can't communicate with other application so can't run.

QUESTION 226:

What command must be used to create an SSH key-pair? Please enter the command without the path or any options or parameters.

Answer: ssh-keygen

Explanation:

ssh-keygen command is used to generate, manages and convert the authentication keys for ssh. We can create either RSA or DSA key by using -t option.

Example: ssh-keygen -t dsa

It will ask the file name to store the private and public key to store. By default it creates the key file on \$HOME/.ssh/id_dsa or \$HOME/.ssh/id_rsa is the private key file and \$HOME/.ssh/id_dsa.pub or \$HOME/.ssh/id_rsa.pub file which stores the public key.

QUESTION 227:

What is the appropriate configuration file entry to allow SSH to run from inetd ?

- A. ssh stream tcp nowait root /usr/sbin/tcpd sshd
- B. ssh stream tcp nowait root /usr/sbin/tcpd tcpd
- C. ssh stream tcpd nowait root /usr/sbin/tcpd sshd
- D. ssh data tcpd nowait root /usr/sbin/tcpd sshd
- E. ssh data tcp nowait root /usr/sbin/tcpd sshd

Answer: A

QUESTION 228:

Which keys are stored in the authorized_keys file?

Answer: public

ssh-keygen command is used to generate, manage and convert the authentication keys for ssh. We can create either RSA or DSA key by using -t option.

Example: ssh-keygen -t dsa

It will ask for the file name to store the private and public key. By default it creates the key file on \$HOME/.ssh/id_dsa or \$HOME/.ssh/id_rsa is the private key file and \$HOME/.ssh/id_dsa.pub or \$HOME/.ssh/id_rsa.pub file which stores the public key.

For secure communication between hosts we should write the public key (id_dsa.pub or id_rsa.pub) into \$HOME/.ssh/authorized_keys file.

QUESTION 229:

A server is being used as a smurf amplifier, whereby it is responding to ICMP Echo-Request packets sent to its broadcast address. To disable this, which command needs to be run?

- A. ifconfig eth0 nobroadcast
- B. echo "0" > /proc/sys/net/ipv4/icmp_echo_accept_broadcasts
- C. iptables A INPUT p icmp j REJECT
- D. echo "1" > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts
- E. echo "1" > /proc/sys/net/ipv4/icmp_echo_nosmurf

Answer: D

Explanation:

To modify the value of running kernel, we should use the /proc file system. If the value of icmp_echo_ignore_broadcasts is 0 then it means enable and 1 means disable.

QUESTION 230:

All machines outside the network are able to send emails through the server to addresses not served by that server. If the server accepts and delivers the email, then it is a(n) _____.

Answer: open email relay

Explanation:

Mail relay means sending the mail from one MTA (Mail Transport Agent) to another MT

- A. MTA Transport the mail on the basis of MX Record.

QUESTION 231:

A program, called vsftpd, running in a chroot jail, is giving the following error:
/bin/vsftpd: error while loading shared libraries: libc.so.6: cannot open shared object file:
No such file or directory.

Which TWO of the following are possible solutions?

- A. Get the vsftpd source code and compile it statically.
- B. The file /etc/ld.so.conf must contain the path to the appropriate lib directory in the chroot jail
- C. Create a symbolic link that points to the required library outside the chroot jail
- D. Copy the required library to the appropriate lib directory in the chroot jail.
- E. Run the program using the command chroot and the option --static_libs

Answer: A, D

QUESTION 232:

On a newly-installed mail server with the IP address 10.10.10.1, ONLY local networks should be able to send email. How can the configuration be tested, using telnet, from outside the local network?

- A. telnet 10.10.10.1 25
MAIL FROM:<admin@example.com>
RECEIPT TO:<someone@example.org>
- B. telnet 10.10.10.1 25
RCPT FROM:<admin@example.com>
MAIL TO:<someone@example.org>
- C. telnet 10.10.10.1 25
HELLO bogus.example.com
MAIL FROM:<anyone@example.org>
RCPT TO:<someone@example.net>
- D. telnet 10.10.10.1 25
HELO bogus.example.com
MAIL FROM:<anyone@example.org>
RCPT TO:<someone@example.net>
- E. telnet 10.10.10.1 25
HELO: bogus.example.com
RCPT FROM:<anyone@example.org>
MAIL TO:<someone@example.net>

Answer: D

Explanation: We can test the mail server either working or not by logging on SMTP or POP port using telnet program.

telnet 10.10.10.1 25 à Login on 10.10.10.1 on 25 port

helo bogus.example.com à Checking either Server Responding or not

mail from: anyone@example.com à Sender Address

rcpt to: someone@example.com à Receptient Address

data àSection to type message should end with .

QUESTION 233:

To be able to access the server with the IP address 10.12.34.56 using HTTPS, a rule for iptables has to be written. Given that the client host's IP address is 192.168.43.12, which of the following commands is correct?

- A. iptables - A FORWARD -p tcp -s 0/0 -d 10.12.34.56 --dport 80 -j ACCEPT
- B. iptables - A FORWARD -p tcp -s 192.168.43.12 d 10.12.34.56:443 -j ACCEPT.
- C. iptables - A FORWARD -p tcp -s 192.168.43.12 -d 10.12.34.56 --dport 443 -j ACCEPT.
- D. iptables - A INPUT -p tcp -s 192.168.43.12 - d 10.12.34.56:80 -j ACCEPT.
- E. iptables - A FORWARD -p tcp -s 0/0 -d 10.12.34.56 --dport 443 -j ACCEPT.

Answer: C

Explanation: It is a rule applied for FORWARD chain, in this rule source from 192.168.43.12 to destination 10.12.34.56 on destination port 443 (For https) is accept.

-A à Chain can be either INPUT or OUTPUT or FORWARD for filter table and PREROUTING or POSTROUTING for NAT

-p à Layer 4 Protocols

-s à Source Address

-d à Destination Address

--sport à Source Port

--dport à Destination Port

-i à Incoming interface

-o à Outgoing Interface

QUESTION 234:

To allow X connections to be forwarded from or through an SSH server, what line must exist in the sshd configuration file?

Answer: X11Forwarding yes

Explanation: To allow the X connection to be forwarded from ssh you should set the yes in /etc/sshd_config file

X11Forwarding no or yes

QUESTION 235:

A security-conscious administrator would change which TWO of the following lines found in an SSH configuration file?

- A. Protocol 2,1
- B. PermitEmptyPasswords no
- C. Port 22
- D. PermitRootLogin yes

E. IgnoreRhosts yes

Answer: A, D

Explanation: In sshd configuration file /etc/ssh/sshd_config file you can layers protocol as well as permit to root to login or not.

QUESTION 236:

A correctly-formatted entry has been added to /etc/hosts.allow to allow certain clients to connect to a service, but this is having no effect. What would be the cause of this?

- A. tcpd needs to be sent the HUP signal.
- B. The service needs to be restarted.
- C. The machine needs to be restarted.
- D. There is a conflicting entry in /etc/hosts.deny .
- E. The service does not support tcpwrappers

Answer: E

Explanation:

Many daemons provides their own set of security mechanism to identify the host or user. Ie. httpd or smb etc. These mechanism are more advanced then the simple functionality that tcp_wrappers provides. On the other hand, it is much easier to use one central location for your service security policy. The libwrap.so library, more commonly referred to as tcp_wrappers, provides host based access control lists for various network services. tcp_wrappers can't provides the access control lists to that services not liked with libwrap.so.

Some services compiled with libwrap.so are

1. sendmail
2. slapd
3. sshd
4. stunnel
5. xinetd
6. gdm
7. gonme-session
8. portmap

QUESTION 237:

Which of the following can the program tripwire NOT check?

- A. File size.
- B. File signature.
- C. Permissions.
- D. File existence.

E. Boot sectors.

Answer: E

Explanation:

tripwire can be configured to detect changes in file/directory size, access time, inode timestamp, user/group, owner and a number of file/directory attributes.

Tripwire is a policy based program that monitors file system changes as specified in a policy file. An encrypted database is used to keep track of modifications that have occurred in a system.

But tripwire can't check the boot sector.

QUESTION 238:

The following is an excerpt from a procmail configuration file:

```
:0 c
```

```
* ! ^To: backup
```

```
! backup
```

Which of the following is correct?

- A. All mails will be backed up to the path defined by \$MAILDIR .
- B. All mails to the local email address backup will be stored in the directory backup.
- C. A copy of all mails will be stored in file backup.
- D. A copy of all mails will be send to the local email address backup.
- E. Mails not addressed to backup are passed through a filter program named backup.

Answer: D

Explanation:

Flags starts from :0

Condition from * i.e

```
*^From
```

And Action;

Example

```
:0
```

```
*^From.*user1
```

```
*^Subject.*Payment
```

```
{
```

```
:0 c à this line forward the mail to another address
```

```
! user2@abc.com à Email address to forward condition matched mail address
```

```
:0:
```

```
paymentmail
```

```
}
```

To forward the mail from user1 regarding the payment to user2 as well as append the mail to paymentmail file.

QUESTION 239:

The internal network (192.168.1.0/24) needs to be able to relay email through the site's sendmail server. What line must be added to /etc/mail/access to allow this?

- A. 192.168.1.0/24 RELAY
- B. 192.168.1 RELAY
- C. 192.168.1.0/24 OK
- D. 192.168.1 OK

Answer: B

Explanation:

Answer B is correct because to specify the Network, we just use the Network portion only.
i.e 192.168.0 .

See the sample Configuration:

user1@ Certkiller .com OK

192.168.0 RELAY

nobody@ DISCARD

info@xyz.com ERROR:550 non-trusted mail address

QUESTION 240:

A user is on holiday for two weeks. Anyone sending an email to that account should receive an auto-response. Which of the following procmailrules should be used, so that all incoming emails are processed by vacation?

- A. :0c:
|/usr/bin/vacation nobody
- B. :w
|/usr/bin/vacation nobod
- C. :0fc:
|/usr/bin/vacation nobod
- D. | /usr/bin/vacation nobod
- E. :> |/usr/bin/vacation nobody

Answer: A

Explanation: Procmail is a very powerful delivery tool, different uses included:

- Sorting incoming email into different folders or files
 - Preprocessing email
 - Starting an event or program when email is received
 - Automatically forwarding email to others
 - Remember additional MTA (mail transport Agent) must configured
- Once your MTA has been configured to use procmail you may implement a system - wide configuration (/etc/procmailrc) or by individual user \$HOME/.procmailrc to sort mail or

forward the mail by checking header information.

To process all condition matched mails by certain program should begin by | and program path with name,

QUESTION 241:

The syntax of the procmail configuration file is?

- A. :0[flags][:[lockfile]]
[* condition]
action
- B. [* condition]
action
:0[flags][:[lockfile]]
- C. :0[flags][:[lockfile]]
[* condition] action
- D. :0[flags][:[lockfile]]:[* condition]
action
- E. :0[flags][:[lockfile]]:[* condition]:action

Answer: A

Explanation:

Flags starts from :0

Condition from * i.e

*^From

And Action;

Example

:0

*^From.*user1

*^Subject.*Payment

{

:0 c à this line forward the mail to another address

! user2@abc.com à Email address to forward condition matched mail address

:0:

paymentmail

}

To forward the mail from user1 regarding the payment to user2 as well as append the mail to paymentmail file.

QUESTION 242:

Please enter the name of the main majordomo configuration file without the path.

Answer: majordomo.cf

QUESTION 243:

Which of the following recipes will append emails from "root" to the "rootmails" mailbox?

A. :0c:
rootmails
* ^From.*root

B. :0c:
* ^From.*root
rootmails

C. :0c:
* ^From=root
rootmails

D. :0c:
* ^From=*root
rootmails

E. :0c:
\$From=\$root
rootmails

Answer: B

Explanation:

```
:0
*^From.*user1
*^Subject.*Payment
{
:0 c à this line forward the mail to another address
! user2@abc.com à Email address to forward condition matched mail address
:0:
paymentmail à File name to append the mail
}
To forward the mail from user1 regarding the payment to user2 as well as append the mail
to pymentmail file
```

QUESTION 244:

Which of the following defines the maximum allowed article size in the configuration file for INN?

- A. limitartsize
- B. artsizelimit
- C. maxartlimit
- D. maxartsize
- E. setartlimit

Answer: D

QUESTION 245:

Which entry in the .procmailrc file will send a copy of an email to another mail address?

- A. :0 c
- B. :0 copy
- C. :c
- D. :copy
- E. :s

Answer: A

Explanation: See the sample procmailrc configuration

```
:0
*^From.*user1
*^Subject.*Payment
{
:0 c à this line forward the mail to another address
! user2@abc.com à Email address to forward condition matched mail address
:0:
paymentmail
}
To forward the mail from user1 regarding the payment to user2 as well as append the mail
to pymmentmail file.
```

QUESTION 246:

Which file, on a majordomo server, will contain a list of all members' email addresses for the mailing list "linux-users"? (Enter only the file name).

Answer: linux-users

QUESTION 247:

In which file, on an INN news server, can access to the news server be configured? (Enter only the file name).

Answer: readers.conf

QUESTION 248:

What does the following procmail configuration section do?

```
:0fw
```

* < 256000
| /usr/bin/foo

- A. procmail sends all email older than 256000 seconds to the external program foo .
- B. If an email contains a value less than 256000 anywhere within it, will process the email with the program foo.
- C. procmail sends mail containing less than 256000 words to program foo.
- D. The program is used instead of for all emails larger than 256000 Bytes.
- E. If the email smaller than 256000 Bytes, will process it with the program foo.

Answer: E

Explanation: See the sample procmailrc configuration

```
:0
*^From.*user1
*^Subject.*Payment
{ :0 c
! user2@abc.com
:0:
paymentmail
}
```

To forward the mail from user1 regarding the payment to user2 as well as append the mail to pymmentmail file. Similarly you can check different header information ie. Size, domain etc

QUESTION 249:

The innd configuration file has been changed and it should be used as soon as possible. What is the fastest way to accomplish that?

- A. ctlinnd kill hup
- B. kill - HUP process id
- C. ctlinnd xexec innd
- D. ctlinnd reload innd
- E. /usr/sbin/innd reload

Answer: C

QUESTION 250:

Which network service or protocol is used by sendmail for RBLs (Realtime Blackhole Lists)?

- A. RBLP
- B. SMTP
- C. FTP

- D. HTTP
- E. DNS

Answer: E

Explanation:

DNS is used by sendmail server for RBLs (Realtime Blackhome Lists)

See the sample line configuration

FEATURE(`dnsbl') à Checks a DNS implemented blackhole list to block email spammers

QUESTION 251:

A procmail recipe is required to delete all emails marked as spam. Please complete the recipe.

:0:

* X-Spam-Status: Yes

Answer: /dev/null

Explanation: After identifying the spam message, either you can forward all spam mail into different folder or you can remove.

See the sample configuration

SPAMFOLDER=spam

:0 wf

| /usr/bin/spamassassin

:0 w : \$SPAMFOLDER/.lock

* ^X-spam-status: Yes

\$SPAMFOLDER/.

QUESTION 252:

Where is the user foo's procmail configuration stored, if home directories are stored in /home? Please enter the complete path to the file.

Answer: /home/foo/procmailrc

Explanation: Procmail is a very powerful delivery tool, different uses included:

- Sorting incoming email into different folders or files
 - Preprocessing email
 - Starting an event or program when email is received
 - Automatically forwarding email to others
 - Remember additional MTA (mail transport Agent) must configured
- Once your MTA has been configured to use procmail you may implement a system - wide configuration (/etc/procmailrc) or by individual user \$HOME/.procmailrc to sort mail or forward the mail by checking header information.

QUESTION 253:

Which file can be used to make sure that procmail is used to filter a user's incoming email?

- A. \${HOME}/.procmail
- B. \${HOME}/.forward
- C. \${HOME}/.bashrc
- D. /etc/procmailrc
- E. /etc/aliases

Answer: B

Explanation: When mail come first it checks the file \$HOME/.forward file to filter the all incoming mails.

QUESTION 254:

What command can be used to add a new newsgroup called Certkiller that allows posting?

- A. ctlinnd newgroup Certkiller n news
- B. ctlinnd newgroup Certkiller y news
- C. ctlinnd addgroup Certkiller y news
- D. ctlinnd newgroup Certkiller +rw news
- E. ctlinnd addgroup Certkiller +rw news

Answer: B