117-202

TEST KING

LEADING THE WAY IN IT
TESTING AND CERTIFICATION TOOLS!

LPI 202

Linux Networking Administration

Version 1.0

Important Note
Please Read Carefully

This product will provide you questions and answers along with detailed explanations carefully compiled and written by our experts. Try to understand the concepts behind the questions instead of just cramming the questions. Go through the entire document at least twice so that you make sure that you are not missing anything.

You are constantly adding and updating our products with new questions and making the previous versions better so email us once before your exam and you will send you the latest version of the product.

Each pdf file contains a unique serial number associated with your particular name and contact information for security purposes. So if you find out that particular pdf file being distributed by you. Testking will reserve the right to take legal action against you according to the International Copyright Law. So don't distribute this PDF file.

QUESTION NO: 1
What is the minimum number of partitions you need to install Linux?

Answer: 2

QUESTION NO: 2
What file contains the default environment variables when using the bash shell?

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

Answer: C

QUESTION NO: 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

QUESTION NO: 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

QUESTION NO: 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

QUESTION NO: 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

QUESTION NO: 7
Which field is used to define the user's default shell?

Answer: command

QUESTION NO: 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, GID, home directory, command, comment
B. username, UID, GID, comment, home directory, command
C. UID, username, GID, home directory, comment, command
D. username, UID, group name, GID, home directory, comment

Answer: B

QUESTION NO: 9
What file defines the levels of messages written to system log files?

Answer: kernel.h

QUESTION NO: 10
Which utility can you use to automate rotation of logs?

Answer: logrotate

QUESTION NO: 11
What is the name and path of the main system log?

Answer: /var/log/messages

QUESTION NO: 12
What is the name and path of the default configuration file used by the syslogd daemon?

Answer: /etc/syslog.conf

QUESTION NO: 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

QUESTION NO: 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

QUESTION NO: 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

QUESTION NO: 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

QUESTION NO: 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

QUESTION NO: 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 tem 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

QUESTION NO: 19
What is the usual mode for the /tmp directory?

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

Answer: D

QUESTION NO: 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/shh/sshd_config file?

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

Answer: B

QUESTION NO: 21
You have an extensive collection of icons in /usr/local/lib/icons/*.gif, which you want to make available as htt://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

QUESTION NO: 22
IP address resolution should be handled by DNS, NIS, and the local /etc host file (in that order). If any of the services returns an address not found message the search should

halt. Which of the following entries in /ect/nsswitch.conf would achieve this configuration?

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

Answer: D

QUESTION NO: 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

QUESTION NO: 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 reobert@newdomain.cnm.

Answer: C

QUESTION NO: 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

QUESTION NO: 26
When running INN, how do you force an update of the news groups are you 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

QUESTION NO: 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

QUESTION NO: 28
You are creating a new partition in preparation for installing Linux. You want to have five different partitions. You have successfully created four partitions, but are unable to create the fifth one. What is the problem?

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

Answer: C

QUESTION NO: 29
When looking at the /etc/passwd file, you notice that all the password files 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

QUESTION NO: 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

QUESTION NO: 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

QUESTION NO: 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 command?

Answer: passwd boba

QUESTION NO: 33
Which file defines all users on your system?

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

Answer: A

QUESTION NO: 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

QUESTION NO: 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

QUESTION NO: 36
What daemon is responsible for tracking events on your system?

Answer: syslogd

QUESTION NO: 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

QUESTION NO: 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, 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: A

QUESTION NO: 39

You system is the primary nameserver for example.com. Due to network growth you must delete 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: C

QUESTION NO: 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

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

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

Answer: A

QUESTION NO: 42
All of the following commands can be used to determine open TCP ports an localhost EXCEPT:

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

Answer: E

QUESTION NO: 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

QUESTION NO: 44
You've installed a PAM-aware restricted service and installed the appropriate /etc/pam.d/<service> file, but you cant 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

QUESTION NO: 45
Several users complain that when checking their email of 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 serve 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

QUESTION NO: 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. You client requests a list of originating IP addresses connecting to that port. Using a Linux workstation as traffic analyzer, which of the following commands would gather the data requested by the client?

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

Answer: A

QUESTION NO: 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

QUESTION NO: 48

The maximum size of the swap partition is _____ MB?

Answer: 128

QUESTION NO: 49
In order to improve your system's security you decide to implement shadow passwords. What command should you use?

Answer: pwconv

QUESTION NO: 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

QUESTION NO: 51
Which of the following tasks in not necessary when creating a new user by editing the /etc/passwd file?

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

Answer: A

QUESTION NO: 52
In order to prevent a user form logging in, you can add a (n) _____ at the beginning of the password file.

Answer: asterick

QUESTION NO: 53
What command you use to review boot messages?

Answer: dmseg

QUESTION NO: 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/syslogd.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

QUESTION NO: 55
You notice that your server load is exceptionally high during the hours of 10 am to 2 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

QUESTION NO: 56
Some networks attacks use IP packets with the SYN, ACK, PSH, URG, FIN and RST options set. (This is sometimes called a "Chernobyl1 packet" or "xmas tree packet", and crashes some operating systems.) To log all such packets received, you would use:

A. iptables –1 INPUT –s 0.0.0.0/0 –d 192.168.0.44/33 --protocol tcp --xmas-pkt –j LOG

B. iptables –1 INPUT –s 0.0.0.0/0 –d 192.168.0.44/32 --protocol tcp --cher-pkt –j LOG
C. iptables –1 INPUT –s 0.0.0.0/0 –d 192.168.0.44/32 --protocol tcp --cher-pkt –log
D. iptables –1 INPUT –s 0.0.0.0/0 –d 192.168.0.44/32 --protocol tcp --tcp-flags SYN, ACK, HSK, PSH, URG, FIN –log
E. iptables –1 INPUT –s 0.0.0.0/0 –d 192.168.44/32 --protocol tcp --tcp-flags ALL, SYN, ACK, PSH, URG, RST, FIN, -j LOG

Answer: E

QUESTION NO: 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

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

_____
/dev/null

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

Answer: E

QUESTION NO: 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	Geteway	Genmask	Flags	Metric	Ref	Use lface
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

QUESTION NO: 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: E

QUESTION NO: 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

QUESTION NO: 62
You can cause named to reload a zone file by:

Answer: ndc reload

QUESTION NO: 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/ .sss/authorized_keys
D. $HOME/ .ssh/trusted_keys

C

QUESTION NO: 64
The recommended minimum size of the swap partition is _____ MB?

Answer: 16

QUESTION NO: 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

QUESTION NO: 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

QUESTION NO: 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 asterick.

Answer: C

QUESTION NO: 68
Which of the following user names is valid?

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

Answer: A

QUESTION NO: 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

QUESTION NO: 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

QUESTION NO: 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

QUESTION NO: 72
Given the CIDR mask /29, the equivalent subnet mask in dotted quad format would be 255.255.255.___.

Answer: 248

QUESTION NO: 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

QUESTION NO: 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

QUESTION NO: 75
What would you use to generate an RSA key for named to sign zone transfer with?

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

Answer: B

QUESTION NO: 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

QUESTION NO: 77
Using wu-ftpd, you have setup an anonymous FTP server to allow access only to files under /var/ftp. You want to share out your current /etc/mtab file so users can see what filesystems are mounted on your system at any given time. You make a symbolic link from /etc/mtab to /var/ftp/pub/mounted_filesystems. During testing, you find that when logged in as a normal user. The file is accessible but when logged in anonymously, the file can NOT be read. Why might this happen?

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

Answer: E

QUESTION NO: 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 NO: 79
What command is used to remove the password assigned to a group?

Answer: gpasswd -r

QUESTION NO: 80
What account is created when you install Linux?

Answer: root

QUESTION NO: 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

QUESTION NO: 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: unknown

QUESTION NO: 83
You 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

QUESTION NO: 84
Given a CIDR mask of /25 and a netmask of 255.255.255.128 how many host IP addresses are available?

Answer: 128

QUESTION NO: 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

QUESTION NO: 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

QUESTION NO: 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

QUESTION NO: 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

QUESTION NO: 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

QUESTION NO: 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

QUESTION NO: 91
The beginning user identifier is defined in the _____ file.

Answer: /etc/login/defs

QUESTION NO: 92
While logged on as a regular user, your boss calls up and wants you to create a new user account immediately. How can you do this without first having to close your work, log odd and logon as root?

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

Answer: B

QUESTION NO: 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

QUESTION NO: 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: A

QUESTION NO: 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

QUESTION NO: 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

QUESTION NO: 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

QUESTION NO: 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

QUESTION NO: 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: A

QUESTION NO: 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

QUESTION NO: 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: D

QUESTION NO: 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

QUESTION NO: 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

QUESTION NO: 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

QUESTION NO: 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. allows-transfer { IP_ADDRESS; };
B. allow-update { IP_ADDRESS; };
C. allow-access { IP_ADDRESS; };
D. allow-access { IP_ADDRESS };

Answer:

QUESTION NO: 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

QUESTION NO: 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