LPI_Prepking_117-102_v2011-12-13_286q_KenCom

Number: 117-102
Passing Score: 625
Time Limit: 120 min
File Version: 2011-12-13

Exam - LPI_Prepking_117-102

Version - 2011-12-13

Questions - 286

Combined from altin and neotokyo without double questions.

You dont need any more the altin and the neotokyo tests.

You need 500 points of 800 to pass also you need 62,5%.
In this test you have to make 625 of 1000 to pass.

By KenCom

Sections

1. 105.1 Customize and use the shell environment
2. 105.2 Customize or write simple scripts
3. 105.3 SQL data management
4. 106.1 Install and configure X11
5. 106.2 Setup a display manager
6. 106.3 Accessibility
7. 107.1 Manage user and group accounts and related system files
8. 107.2 Automate system administration tasks by scheduling jobs
9. 107.3 Localisation and internationalisation
10. 108.1 Maintain system time
11. 108.2 System logging
12. 108.3 Mail Tranfer Agent (MTA) basics
13. 108.4 Manage printers and printing
14. 109.1 Fundamentals of internet protocols
15. 109.2 Basic network configuration
16. 109.3 Basic network troubleshooting
17. 109.4 Configure client side DNS
18. 110.1 Perform security administration tasks
19. 110.2 Setup host security
20. 110.3 Securing data with encryption

Exam A

QUESTION 1
Which of the following is NOT a Mail Transport Agent?

A. exim
B. postfix
C. sendmail
D. qmail
E. mail

Correct Answer: E
Section: 108.3 Mail Tranfer Agent (MTA) basics
Explanation

Explanation/Reference:
From wikipedia:
postfix is a free and open-source mail transfer agent (MTA) that routes and delivers electronic mail. It is intended as a fast, easier-to-administer, and secure alternative to the widely-used sendmail MTA.
sendmail is the [...] standard MTA under most variants of the Unix.
exim is a message transfer agent (MTA) developed at the University of Cambridge for use on Unix systems.
qmail is a mail transfer agent (MTA) that runs on Unix. It was written, [...] as a more secure replacement for the popular sendmail program.

mail is a command line e-mail client to send/create mails.

QUESTION 2
The legacy program for sending files to the printer queues from the command line is:

A. lpd
B. lpr
C. lpq
D. lpp

Correct Answer: B
Section: 108.4 Manage printers and printing
Explanation

Explanation/Reference:
From the man pages:
lpr submits files for printing. Files named on the command line are sent to the named printer (or the default destination if no destination is specified). If no files are listed on the command-line, lpr reads the print file from the standard input.

lpq - show printer queue status
lpd - the equivalent of the printserver
lpp - there is no command lpp

QUESTION 3
What is pool.ntp.org?

A. A deprecated feature for maintaining system time in the Linux kernel
B. A website which provides binary and source packages for the OpenNTPD project
C. A virtual cluster of various timeservers
D. A community website used to discuss the localization of Linux

Correct Answer: C
Section: 108.1 Maintain system time
Explanation

Explanation/Reference:
From http://www.pool.ntp.org/en:
The pool.ntp.org project is a big virtual cluster of timeservers providing reliable easy to use NTP service for millions of clients.

QUESTION 4
Which file, when using Sendmail or a similar MTA system, will allow a user to redirect all their mail to another address and is configurable by the user themselves?

A. /etc/alias
B. /etc/mail/forwarders
C. ~/.alias
D. ~/.forward

Correct Answer: D
Section: 108.3 Mail Tranfer Agent (MTA) basics
Explanation

Explanation/Reference:
From wikipedia:

~/.forward files
sendmail, the reference SMTP implementation in the early 1980s, provided for ~/.forward files, which can store the target email-addresses for given users. One can configure some email-program filters to automatically perform forwarding or replying actions immediately after receiving. Forward files can also contain shell scripts, which have become a source of many security problems.

Email predates the formalization of client–server architectures in the 1990s.[11] Therefore, the distinction between client and server seems necessarily forced. The original distinction contrasted daemons and user-controlled programs which run on the same machine. The sendmail daemon used to run with root privileges so it could impersonate any user whose mail it had to manage. On the other hand, users can access their own individual mail-files and configuration files, including ~/.forward. Client programs may assist in editing the server configuration-files of a given user, thereby causing some confusion as to what role each program plays.

QUESTION 5
What entry can you add to syslog.conf file to have all syslog messages generated by your system go to virtual console 12?

A. *.* /dev/tty12
B. /var/log/messages | /dev/tty12
C. | /dev/tty12
D. syslog tty12
E. mail.* /dev/tty12

Correct Answer: A
Section: 108.2 System logging
Explanation

Explanation/Reference:
The syntax of the syslogd.conf is basically
selector action

where selector specifies what log messages and action can be programs, files, or an email address.

B,C,D miss the selector, and E only sends mail logs to console 12

QUESTION 6
Which configuration file does sudo read when determining if a user is permitted to run applications with root privileges?

A. /etc/groups
B. /etc/passwd
C. /etc/sudoers
D. /etc/sudo.conf

Correct Answer: C
Section: 110.1 Perform security administration tasks
Explanation

Explanation/Reference:
From the man pages:
sudo determines who is an authorized user by consulting the file @sysconfdir@/sudoers. (typically /etc/sudoers)

QUESTION 7
What is the purpose of the Sticky Keys feature in x?

A. To assist users who have difficulty holding down multiple keys at once
B. To prevent repeated input of a single character if the key is held down
C. To ignore brief keystrokes according to a specified time limit
D. To repeat the input of a single character

Correct Answer: A
Section: 106.3 Accessibility
Explanation

Explanation/Reference:
From wikipedia:
StickyKeys is an accessibility feature to aid users who have physical disabilities. It essentially serializes keystrokes instead of pressing multiple keys at a time: StickyKeys allows the user to press a modifier key, such as Shift, Ctrl, Alt, or the Windows key, and have it remain active until another key is pressed.

QUESTION 8
On a system running the K Display Manager, when is the /etc/kde4/kdm/Xreset script automatically executed?

A. When KDM starts
B. When a users x session exits
C. When KDM crashes
D. When x is restarted
E. When x crashes

Correct Answer: B
Section: 106.2 Setup a display manager
Explanation

Explanation/Reference:
From the man pages:

/etc/kde4/kdm/Xreset script to run as root after session exits

QUESTION 9
For accessibility assistance, which of the following programs is an on-screen keyboard?

A. xkb
B. atkb
C. GOK
D. xOSK

Correct Answer: C
Section: 106.3 Accessibility
Explanation

Explanation/Reference:
From the GOK homepage:
GOK is an on-screen keyboard that provides access to the GNOME desktop via dynamically generated keyboards, and text entry via one of the provided alphanumeric keyboards, or a dynamic keyboard created based on the users current system keyboard driver, or even a user made keyboard.

xOSK = seems to be nothing
atkb = seems to be nothing
xkb = In the X Window System, the X keyboard extension or XKB extends the ability to control the keyboard over what is offered by the X Window System core protocol.

QUESTION 10
What output will the command `$ seq 1 5 20` produce?

A. 1 6 11 16
B. 1 5 10 15
C. 1 2 3 4
D. 2 3 4 5
E. 5 10 15 20

Correct Answer: A
Section: 105.2 Customize or write simple scripts
Explanation

Explanation/Reference:
From the man pages:
seq - seq [OPTION]... FIRST INCREMENT LAST
Print numbers from FIRST to LAST, in steps of INCREMENT.

QUESTION 11
Which of the following words is used to restrict the records that are returned from a SELECT query based on a supplied criteria for the values in the records?

A. LIMIT
B. FROM
C. WHERE
D. IF

Correct Answer: C
Section: 105.3 SQL data management
Explanation

Explanation/Reference:
The WHERE clause is used to extract only those records that fulfill a specified criterion.

Limit is used to limit your query results to those that fall *within a specified range*. You can use it to show the first X number of results, or to show a range from X - Y results. It is phrased as Limit X, Y and included at the end of your query. X is the starting point (remember the first record is 0) and Y is the duration (how many records to display).

QUESTION 12
Which of the following SQL statements will select the fields name and address from the contacts table?

A. SELECT (name, address) FROM contacts;
B. SELECT (name address) FROM contacts;
C. SELECT name, address FROM contacts;
D. SELECT name address FROM contacts;

Correct Answer: C
Section: 105.3 SQL data management
Explanation

Explanation/Reference:
see http://www.sqlite.org/syntaxdiagrams.html#select-stmt for a detailed description of the SQL select syntax.

QUESTION 13
What output will the following command `$ seq 10` produce?

A. A continuous stream of numbers increasing in increments of 10 until stopped
B. The numbers 1 through 10 with one number per line
C. The numbers 0 though 9 with one number per line
D. The number 10 to standard output

Correct Answer: B
Section: 105.2 Customize or write simple scripts
Explanation

Explanation/Reference:
if only one number is specified the following synopsis is used
seq [OPTION]... LAST

QUESTION 14
Which command will print the exit value of the previous command to the screen in bash?

A. echo $?
B. echo $#
C. echo $exit
D. echo $status
E. echo $&

Correct Answer: A
Section: 105.2 Customize or write simple scripts
Explanation

Explanation/Reference:
There are quite a few internal variables used in bash: see http://tldp.org/LDP/abs/html/internalvariables.html

Some of them are:
$! PID of last job run in background
$? Exit status of a command, function, or the script itself (see Example 24-7)
$$ PID of the script/process itself.

QUESTION 15
Which of the following is the command used to deactivate a network interface?

A. ifdown
B. ipdown
C. net
D. netdown

Correct Answer: A
Section: 109.2 Basic network configuration
Explanation

Explanation/Reference:
From the man pages:
ifup - bring a network interface up
ifdown - take a network interface down
net - used for samba configuration

also correct would be `ifconfig <interface> down`

QUESTION 16
Identify the statement that would create a default route using a gateway of 192.168.1.1.

A. netstat -add default gw
B. route default 192.168.1.1
C. ip route default 192.168.1.1
D. route add default gw 192.168.1.1
E. ifconfig default gw 192.168.1.1eth0

Correct Answer: D
Section: 109.2 Basic network configuration
Explanation

Explanation/Reference:
From the man pages:
route - show / manipulate the IP routing table
[-v] [-A family] **add** [-net|-host] **target** [netmask Nm] [**gw Gw**] [metric N] [mss M] [window W] [irtt I] [reject] [mod] [dyn] [reinstate] [[dev] If]

where target is default and Gw is the IP address of the Gateway.

QUESTION 17
Which statement is true regarding the following /etc/resolv.conf file?

```
search example.com
127.0.0.1
208.77.188.166
```

A. There is a syntax error

B. If DNS queries to the localhost fail, the server 208.77.188.166 will be queried
C. example.com will be appended to all host lookups
D. The DNS servers at 127.0.0.1 and 208.77.188.166 will be queried in a round robin fashion
E. The DNS server with the shortest ping time will be queried first. If the lookup fails, the second server will be queried

Correct Answer: A
Section: 109.2 Basic network configuration
Explanation

Explanation/Reference:
From the man pages:
The resolver configuration file contains information that is read by the resolver routines the first time they are invoked by a process. The file is designed to be human readable and contains a list of keywords with values that provide various types of resolver information.

Keywords must be at the start of the line, IP addresses are not allowed as keywords.

Example:
```
domain server.com
search server.com
nameserver 10.0.0.1
nameserver 192.168.0.1
```

QUESTION 18
Suppose that the command netstat -a hangs for a long time without producing output. You might suspect:

A. a problem with NFS
B. a problem with DNS
C. a problem with NIS
D. a problem with routing
E. that the netstat daemon has crashed

Correct Answer: B
Section: 109.3 Basic network troubleshooting
Explanation

Explanation/Reference:
If the -n, --numeric option is not specified netstat tries to resolve all ip addresses into hostnames; hostnames are provided by a nameserver (or locally using /etc/hosts). The default timeout for a nameserver query is 5 seconds, so a long waiting time would indicate the DNS is not responding (or configured incorrectly).

QUESTION 19
Which of the following lines would you find in the file /etc/resolv.conf?

A. order hosts,bind
B. 192.168.168.4 dns-server
C. hosts: files,dns
D. domain mycompany.com

Correct Answer: D
Section: 109.2 Basic network configuration
Explanation

Explanation/Reference:

From the man pages:
The resolver configuration file contains information that is read by the resolver routines the first time they are invoked by a process. The file is designed to be human readable and **contains a list of keywords with values** that provide various types of resolver information.

The following keywords are allowed in /etc/resolv.conf:
nameserver
domain
search
sortlist
options

QUESTION 20
You are working on a server that has multiple ethernet network interfaces, and you wish to find out the IP address assigned to the eth1 interface.

Which of the following commands will print the necessary information?

A. ipconfig /dev/eth1
B. ethconfig -d eth1
C. ifconfig eth1
D. prntconf eth1

Correct Answer: C
Section: 109.2 Basic network configuration
Explanation

Explanation/Reference:
From the man pages:
ifconfig - configure a network interface
ifconfig [-v] [-a] [-s] [interface]

QUESTION 21
What is the purpose of the dig command?

A. To adjust a directory's hidden permissions
B. To search for files on the filesystem
C. To adjust a file's hidden permissions
D. To perform hostname lookups
E. To ping all known hosts on the current subnet

Correct Answer: D
Section: 109.3 Basic network troubleshooting
Explanation

Explanation/Reference:
From the man pages:
dig (domain information groper) is a flexible tool for interrogating DNS name servers. It performs DNS lookups and displays the answers that are returned from the name server(s) that were queried. Most DNS administrators use dig to troubleshoot DNS problems because of its flexibility, ease of use and clarity of output.

QUESTION 22
Which of the following looks like a correct entry in the /etc/hosts file:

A. localhost 127.0.0.1 localhost.localdomain

B. localhost.localdomain localhost 127.0.0.1
C. localhost localhost.localdomain 127.0.0.1
D. 127.0.0.1 localhost.localdomain localhost
E. localhost.localdomain 127.0.0.1 localhost

Correct Answer: D
Section: 109.2 Basic network configuration
Explanation

Explanation/Reference:
From the man pages:
/etc/hosts is a simple text file that associates IP addresses with hostnames, one line per IP address. For each host a single line should be present with the following information:
IP_address canonical_hostname [aliases...]

Example:
```
127.0.0.1     localhost
:1            localhost ip6-localhost ip6-loopback
```

QUESTION 23
Which of the following describes the Linux ping packet or datagram?

A. IP packet with a packet type
B. ICMP packet with a message type
C. ICMP packet with a payload
D. UDP datagram with a protocol type
E. UDP datagram with a payload

Correct Answer: B
Section: 109.1 Fundamentals of internet protocols
Explanation

Explanation/Reference:
From the man pages:
ping uses the ICMP protocol's mandatory ECHO_REQUEST datagram to elicit an ICMP ECHO_RESPONSE from a host or gateway. ECHO_REQUEST datagrams (``pings'') have an IP and ICMP header, followed by a struct timeval and then an arbitrary number of ``pad'' bytes used to fill out the packet.

QUESTION 24
When attempting to send a file to another user securely with GPG, which of the following actions must be done?

A. Encrypt the file using your public key
B. Encrypt the file using their public key
C. Encrypt the file using your private key
D. Encrypt the file using their private key
E. Sign the file with your public key

Correct Answer: B
Section: 110.3 Securing data with encryption
Explanation

Explanation/Reference:
You always use the Public key of the person you want to send the data to to encrypt it, because the data can only be decrypted with the private key.

To authenticate messages you do the opposite, encrypt a hash of the message with your private key, and every one can decrypt it with the public key, thus proving that you signed the message.

QUESTION 25
Which of the following commands can be used to activate a specific network interface?

A. ipup
B. net
C. ifup
D. netup

Correct Answer: C
Section: 109.2 Basic network configuration
Explanation

Explanation/Reference:
From the man pages:
ifup - bring a network interface up
ifdown - take a network interface down

QUESTION 26
What is the highest numbered TCP/IP port?

A. 2047
B. 32767
C. 65535
D. 131071

Correct Answer: C
Section: 109.1 Fundamentals of internet protocols
Explanation

Explanation/Reference:
Port addresses are 16 bit long, allowing all numbers from [1-65535]

QUESTION 27
You need to pause the CUPS printer HPLaserjet4, and you want to cancel all print jobs with a message, "hello".

Which command will do this?

A. cupsreject -c -r hello HPLaserjet4
B. cupsreject -p -m hello HPLaserjet4
C. cupsdisable -c -r hello HPLaserjet4
D. cupsdisable -p -m hello HPLaserjet4

Correct Answer: C
Section: 108.4 Manage printers and printing
Explanation

Explanation/Reference:
From the man pages:
cupsdisable, cupsenable - stop/start printers and classes

cupsdisable [-E] [-U username] [-c] [-h server[:port]] [-r reason] [--hold] destination(s)

The following options may be used:
-c Cancels all jobs on the named destination.
-r "reason" Sets the message associated with the stopped state. If no reason is specified then the message is set to "Reason Unknown".

QUESTION 28
Which of the following are commonly used Mail Tranfer Agent (MTA) applications?

(Please select THREE correct answers)

A. postfix
B. procmail
C. sendmail
D. exim
E. smtpd

Correct Answer: ACD
Section: 108.3 Mail Tranfer Agent (MTA) basics
Explanation

Explanation/Reference:
smtpd is a mail proxy for firewalls with anti-spam and anti-relay features Smtpd uses two programs, smtpd which listens for incoming mail and places it in a private queue, and smtpfwdd, which invokes sendmail to deliver messages from the queue.
procmail is a mail delivery agent (MDA) capable of sorting incoming mail into various directories and filtering out spam messages. Procmail is widely used on Unix-based systems and stable, but no longer maintained; users who wish a maintained program are advised to use an alternative MDA, such as maildrop.

QUESTION 29
On a dual boot system, every time the system is booted back into Linux the time has been set backward by two hours.

Which of the following commands will correct the problem so it will not occur again?

A. ntpdate pool.ntp.org
B. date -d 'two hours'
C. hwclock --hctosys --localtime
D. time hwclock

Correct Answer: C
Section: 108.1 Maintain system time
Explanation

Explanation/Reference:
From the man pages:
hwclock sets the kernel timezone to the value indicated by TZ and/or /usr/share/zoneinfo when you set the System Time using the --hctosys option.

QUESTION 30
What is NOT contained in the locale setting of the operating system?

A. currency symbol
B. language
C. timezone

D. thousands separator

Correct Answer: C
Section: 107.3 Localisation and internationalisation
Explanation

Explanation/Reference:
From the man pages:
These environment variables affect each locale categories for all locale-aware programs:
LC_CTYPE Character classification and case conversion.
LC_COLLATE Collation order.
LC_TIME Date and time formats.
LC_NUMERIC Non-monetary numeric formats.
LC_MONETARY Monetary formats.
LC_MESSAGES Formats of informative and diagnostic messages and interactive responses.
LC_PAPER Paper size.
LC_NAME Name formats.
LC_ADDRESS Address formats and location information.
LC_TELEPHONE Telephone number formats.
LC_MEASUREMENT Measurement units (Metric or Other).
LC_IDENTIFICATION Metadata about the locale information.

Timezone is not handled by locale.

QUESTION 31
A French user has installed the French language pack, but currencies are still being displayed with a leading '$' sign in his spread sheets.

What must be done to fix this?

A. Alter the locale
B. Set the timezone correctly
C. Edit /etc/currency
D. Reinstall the French language pack

Correct Answer: A
Section: 107.3 Localisation and internationalisation
Explanation

Explanation/Reference:
try changing the value in /etc/default/locale.
Locale files are stored in LOCPATH or /usr/lib/locale

QUESTION 32
Each entry in a crontab must end with what character?

A. tab
B. space
C. backslash
D. newline

Correct Answer: D
Section: 107.2 Automate system administration tasks by scheduling jobs
Explanation

Explanation/Reference:

From the man pages:
The format of a cron command is very much the V7 standard, with a number of upward-compatible extensions. Each line has five time and date fields, followed by a command, followed by a newline character ('\n').

QUESTION 33
X is running okay but you're concerned that you may not have the right color depth set. What single command will show you the running color depth while in X?

A. xcd
B. xcdepth
C. xwininfo
D. xcolordepth
E. cat /etc/X11

Correct Answer: C
Section: 106.1 Install and configure X11
Explanation

Explanation/Reference:
Example:
xwininfo: Window id: 0x3800005 "Terminal"

Absolute upper-left X: 374
Absolute upper-left Y: 159
Relative upper-left X: 374
Relative upper-left Y: 159
Width: 1311
Height: 740
Depth: 32
[...]

QUESTION 34
What output will the following command sequence produce?

```
echo '1 2 3 4 5 6' | while read a b c; do
echo result: $c $b $a;
done
```

A. result: 3 4 5 6 2 1
B. result: 1 2 3 4 5 6
C. result: 6 5 4
D. result: 6 5 4 3 2 1
E. result: 3 2 1

Correct Answer: A
Section: 105.2 Customize or write simple scripts
Explanation

Explanation/Reference:
This command sequence read "1" into a, "2" into b and "3 4 5 6" into c, then outputs first c, then b then a ("3 4 5 6" "2" "1")

QUESTION 35
What benefit does an alias provide?

A. It provides faster lookups for commands
B. It prevents having to type long commands
C. It hides what command you are running from others
D. It creates a local copy of a file from another directory

Correct Answer: B
Section: 105.1 Customize and use the shell environment
Explanation

Explanation/Reference:
aliases substitute long commands (including options!) with shorter commands.

QUESTION 36
While checking your security, you discover that you can connect to one of the machines on the network via port 23.

What should you do to the network service on this machine?

A. Deactivate it, you don't need a SMTP server there
B. Deactivate it, you should not use TELNET
C. Leave active, SSH is safe.
D. Deactivate it, you don't need a FTP server there.

Correct Answer: B
Section: 109.3 Basic network troubleshooting
Explanation

Explanation/Reference:
/etc/services defines port 23 as
```
telnet    23/tcp
```

QUESTION 37
What file should be edited to make the system aware of newly added library files?

A. /etc/modules.conf
B. /etc/conf.modules
C. /etc/ld.so.conf
D. /etc/ld.so.cache
E. /etc/LD_LIBRARY_PATH.conf

Correct Answer: C
Section: 105.1 Customize and use the shell environment
Explanation

Explanation/Reference:
Explanation:
ldconfig creates the necessary links and cache to the most recent shared libraries found in the directories specified on the command line, in the file /etc/ld.so.conf, and in the trusted directories (/lib and /usr/lib). The cache is used by the run-time linker, ld.so or ld-linux.so. ldconfig checks the header and file names of the libraries it encounters when determining which versions should have their links updated.

Some files:
/lib/ld.so run-time linker/loader
/etc/ld.so.conf File containing a list of colon, space, tab, newline, or comma spearated directories in which to search for libraries.

/etc/ld.so.cache File containing an ordered list of libraries found in the directories specified in /etc/ld.so.conf

QUESTION 38
What is the binary conversion of the IP address 192.168.1.10?

A. 11000000.10101000.00000001.00001010
B. 01101010.11000100.10101000.00000001
C. 00000001.00001010.11000000.10101000
D. 10101000.00000001.00001010.11000000
E. None of the choices

Correct Answer: A
Section: 109.1 Fundamentals of internet protocols
Explanation

Explanation/Reference:
00000001 = 1
00000010 = 2
00000100 = 4
00001000 = 8
00010000 = 16
00100000 = 32
01000000 = 64
10000000 = 128

QUESTION 39
Your investigation of a system turns up a file that contains the line below:
`find /home -iname .rhosts -exec rm -f {} \;`
What is the purpose of this script?

A. To enhance system security
B. To remove all program error dumps
C. To remove all temporary files in the user's home directories
D. To reset the configuration for the rsh and rexec utilities

Correct Answer: A
Section: 110.2 Setup host security
Explanation

Explanation/Reference:
.rhosts is used to control which machines trust other machines for access to your account. If a machine trusts another machines then it will allow a specified user (usually yourself) to access your account without having to enter a password.

From the man pages:
-iname pattern Like -name, but the match is case insensitive.
-exec command {} ; Execute command; All following arguments to find are taken to be arguments to the command until an argument consisting of `;' is encountered. The command line is built by appending each selected file name at the end.

QUESTION 40
Which of the following commands will provide locale-specific information about your system and its environment?

A. loconfig

B. getlocale
C. locale
D. tzconfig
E. tzselect

Correct Answer: C
Section: 107.3 Localisation and internationalisation
Explanation

Explanation/Reference:
loconfig, getlocale do not exist
tzconfig (deprecated on Debian) and tzselect are used to set time zone information

```
$ locale
LANG=en_US.utf8
LC_CTYPE="en_US.utf8"
LC_NUMERIC="en_US.utf8"
LC_TIME="en_US.utf8"
LC_COLLATE="en_US.utf8"
LC_MONETARY="en_US.utf8"
LC_MESSAGES="en_US.utf8"
LC_PAPER="en_US.utf8"
LC_NAME="en_US.utf8"
LC_ADDRESS="en_US.utf8"
LC_TELEPHONE="en_US.utf8"
LC_MEASUREMENT="en_US.utf8"
LC_IDENTIFICATION="en_US.utf8"
LC_ALL=
```

Exam B

QUESTION 1
Which of the following lines would you expect to see in the file /etc/services?

A. in.tftpd: LOCAL
B. tftp dgram udp wait root /usr/sbin/tcpd in.tftpd
C. tftp 69/udp
D. udp 17 UDP

Correct Answer: C
Section: 109.2 Basic network configuration
Explanation

Explanation/Reference:
services is a plain ASCII file providing a mapping between human-friendly textual names for internet services, and their underlying assigned port numbers and protocol types. Every networking program should look into this file to get the port number (and protocol) for its service.

A) /etc/hosts.allow
B) /etc/inetd.conf
D) /etc/protocols

QUESTION 2
Which commands will set a regular users password so it forces them to change it every 60 days?

(Choose all that apply)

A. passwd -x 60 user
B. chage -M 60 user
C. passwd +x 60 user
D. usermod -f 60 user

Correct Answer: AB
Section: 107.1 Manage user and group accounts and related system files
Explanation

Explanation/Reference:
from the man pages:
chage - change user password expiry information
-M, --maxdays MAX_DAYS Set the maximum number of days during which a password is valid. When MAX_DAYS plus LAST_DAY is less than the current day, the user will be required to change his/her password before being able to use his/her account. This occurrence can be planned for in advance by use of the -W option, which provides the user with advance warning.
passwd - change user password
-x, --maxdays MAX_DAYS Set the maximum number of days a password remains valid. After MAX_DAYS, the password is required to be changed.

QUESTION 3
Rate this comment: The "root" account has no security restrictions imposed upon them

A. True
B. False

Correct Answer: A

Section: 107.1 Manage user and group accounts and related system files
Explanation

Explanation/Reference:
From http://en.wikipedia.org/wiki/Superuser:
In Unix-style computer operating systems, root is the conventional name of the user who has all rights or permissions (to all files and programs) in all modes (single- or multi-user).

QUESTION 4
Which of the following lines would you expect to see in the file /etc/services?

A. in.tftpd: LOCAL
B. tftp dgram udp wait root /usr/sbin/tcpd in.tftpd
C. tftp 69/udp
D. udp 17 UDP

Correct Answer: C
Section: 109.2 Basic network configuration
Explanation

Explanation/Reference:
services is a plain ASCII file providing a mapping between human-friendly textual names for internet services, and their underlying assigned port numbers and protocol types. Every networking program should look into this file to get the port number (and protocol) for its service.

A) /etc/hosts.allow
B) /etc/inetd.conf
D) /etc/protocols

QUESTION 5
You need to print 12 copies of the document foo.txt.

Which of the following commands would you use?

A. cat foo.txt | lpr -#12
B. cat foo.txt > lpr -#12
C. cat foo.txt | lpr -12
D. cat foo.text > lpr -12

Correct Answer: A
Section: 108.4 Manage printers and printing
Explanation

Explanation/Reference:
From the man pages:
-# copies sets the number of copies to print from 1 to 100.

QUESTION 6
What BASH environment variable will prevent you from overwriting a file with a ">" or ">>"?

A. set -o safe
B. set -o noglob
C. set -o noclobber
D. set -o append
E. set -o nooverwrite

Correct Answer: C
Section: 105.1 Customize and use the shell environment
Explanation

Explanation/Reference:
From the man pages:
-o noclobber, -C If set, bash does not overwrite an existing file with the >, >&, and <> redirection operators. This may be overridden when creating output files by using the redirection operator >| instead of >

QUESTION 7
In the following command and its output

```
$ echo $$
12942
```

What is 12942?

A. the process ID of the echo command
B. the process ID of the current shell
C. the process ID of the last command executed
D. the process ID of the last backgrounded command

Correct Answer: B
Section: 105.2 Customize or write simple scripts
Explanation

Explanation/Reference:
see http://tldp.org/LDP/abs/html/internalvariables.html
$? Exit status of a command, function, or the script itself
$$ Process ID (PID) of the script/process itself
$_ Special variable set to final argument of previous command executed.
$! PID (process ID) of last job run in background

QUESTION 8
We have bash script ~/myscript shown below:
`shift echo $2`
We call this script:
`~/myscript alpha beta gamma delta`
What will we see?

A. alpha
B. beta
C. gamma
D. delta

Correct Answer: C
Section: 105.2 Customize or write simple scripts
Explanation

Explanation/Reference:
shift shifts all arguments to the left (meaning arg1 becomes arg2, arg2 becomes arg3, ...), so after the shift the 2nd argument becomes gamma.

QUESTION 9
To test a shell script called myscript, the environment variable FOOBAR must be removed temporarily.

How can this be done?

A. unset -v FOOBAR
B. set -a FOOBAR=""
C. env -u FOOBAR myscript
D. env -i FOOBAR myscript

Correct Answer: C
Section: 105.2 Customize or write simple scripts
Explanation

Explanation/Reference:
From the man pages:
env - run a program in a modified environment
-u, --unset=NAME remove variable from the environment

QUESTION 10
Which of the following is the best way to list all defined shell variables?

A. env
B. set
C. env -a
D. echo $ENV

Correct Answer: B
Section: 105.1 Customize and use the shell environment
Explanation

Explanation/Reference:
A) env - run a program in a modified environment (-a does not exist)
C) option -a does not exist
D) `echo $ENV` prints the shell variable $ENV if it exists

QUESTION 11
Which of the following commands shows ONLY the user id of Bob?

(Select TWO)

A. cat /etc/passwd | grep Bob | cut -d: -f3
B. cat /etc/passwd | grep Bob | cut -f: -d3
C. grep Bob /etc/passwd | awk -F: '{ print $3 }'
D. grep Bob /etc/passwd | awk -f: '{ print $3 }'
E. grep Bob /etc/passwd | cut -F: -d3

Correct Answer: AC
Section: 105.2 Customize or write simple scripts
Explanation

Explanation/Reference:
UID is in the 3rd column of /etc/passwd, the columns are separated by ":"
`cut` option -d lets us specify the separator, as does `awk` option -F

QUESTION 12
Which command allows you to make a shell variable visible to subshells?

A. export $VARIABLE
B. export VARIABLE
C. set $VARIABLE
D. set VARIABLE
E. env variable

Correct Answer: B
Section: 105.1 Customize and use the shell environment
Explanation

Explanation/Reference:
From the man pages:
export [-fn] [name[=word]] ...
export -p
The supplied names are marked for automatic export to the environment of subsequently executed commands. If the -f option is given, the names refer to functions. If no names are given, or if the -p option is supplied, a list of all names that are exported in this shell is printed. The -n option causes the export property to be removed from each name. If a variable name is followed by =word, the value of the variable is set to word. export returns an exit status of 0 unless an invalid option is encountered, one of the names is not a valid shell variable name, or -f is supplied with a name that is not a function.

You can not use export $VARIABLE, because the shell would expand $VARIABLE to its content before calling export.

QUESTION 13
Which of the following commands will lock the user foobar's account?

A. userdel -r foobar
B. moduser -l foobar
C. usermod -L foobar
D. userconf -l foobar

Correct Answer: C
Section: 107.1 Manage user and group accounts and related system files
Explanation

Explanation/Reference:
From the man pages:
usermod - modify a user account
-L, --lock Lock a users password. This puts a ! in front of the encrypted password, effectively disabling the password. You cant use this option with -p or -U.

QUESTION 14
Which of the following are elements of good password practice for users?

(Choose THREE)

A. Do not use words from a dictionary
B. Use upper- and lower-case letters
C. Use only alpha-numeric characters
D. A password should be easy to remember
E. Passwords should be 10 to 12 characters long

Correct Answer: ABE

Section: 107.1 Manage user and group accounts and related system files
Explanation

Explanation/Reference:
Safeguard against Dictionary attacks
Safeguard against brute force attacks using upper, lower case characters, digits and special characters
Safeguard against hash attacks by using 15+ chars when using MD5 hashes, or 8+ chars when using DES hashes.

(see http://www.redhat.com/docs/manuals/linux/RHL-8.0-Manual/security-guide/s1-wstation-pass.html)

QUESTION 15
Which crontab entry could be used to set the system time at regular intervals?

A. 1 0 * * * date dt$24
B. 1 0 * * * settime dt$24
C. 1 0 * * * /usr/sbin/runcron date <ntpl.digex.net
D. 1 0 * * * /usr/sbin/ntpdate ntp1.digex.net> /dev/null 2>&1
E. 1 0 * * * date<ntpl.digex.net

Correct Answer: D
Section: 107.2 Automate system administration tasks by scheduling jobs
Explanation

Explanation/Reference:
ntpdate - set the date and time via NTP

A) invalid option for date
B) settime is not a valid command
C,E) date does not get a NTP server via stdin

QUESTION 16
The system utility that automatically creates new log files and moves old ones is called what?

A. newlog
B. mvlog
C. rotatelog
D. logrotate

Correct Answer: D
Section: 108.2 System logging
Explanation

Explanation/Reference:
From the man pages:
logrotate - rotates, compresses, and mails system logs

A,B,C) commands do not exist

QUESTION 17
You have a script called logout-users which will log out inactive users every hour between the hours of 6 p.m and 7 a.m., Monday through Friday.

Choose the best option for a crontab entry:

A. 00 18-07 * * 1-5 logout-users
B. 00 6PM-7AM * * Mon-Friday logout-users
C. * 6-7 * * 1-5 logout-users
D. * 18,19,20,21,22,23,0,1,2,3,4,5,6,7 * * 1-5 logout-users

Correct Answer: A
Section: 107.2 Automate system administration tasks by scheduling jobs
Explanation

Explanation/Reference:
Crontab job format: minute hour day month day/week command in numeric format (if not prefixed with @)

B) not correct
C) would only run every minute from 6AM to 7AM
D) would run every minute from 6PM to 7AM

QUESTION 18
You have modified user bob's login information. In the passwd file, you changed /bin/bash to /bin/false. What effect will this have on user bob?

A. Bob's account will run the false utility
B. This will not effect Bob's account
C. This will change the user's UID
D. This will suspend Bob's interactive login

Correct Answer: D
Section: 107.1 Manage user and group accounts and related system files
Explanation

Explanation/Reference:
This has the effect of rejecting shell login attempts over ssh, telnet, or other shell-requesting protocols. It may have other side effects too, but those are beyond the scope of this article.

CAUTION: Simply using /bin/false as someone's shell does not keep them from using said account to authenticate over ssh and using non-shell tools such as port forwarding. A default configuration in sshd will often allow tunneling and other non-shell activity.

QUESTION 19
Which of the statements is the result of the following command?

```
$ export PS2="[\u\w]\\$ "
```

A. The primary bash prompt uses underlining and white background (black foreground)
B. The primary bash prompt includes the username and working path
C. The secondary bash prompt uses underlining and white background (black foreground)
D. The secondary bash prompt includes the username and working path
E. The bash prompt maps mouse button one as Ctrl-U (undo) and mouse two as Ctrl-W (write line to file)

Correct Answer: D
Section: 105.1 Customize and use the shell environment
Explanation

Explanation/Reference:
PS2 specifies the secondary bash prompt (used when expanding input over several lines).
\u = username

\w = working dir

Others:
\d = the date
\h = the hostname
\j = the number of jobs currently managed by the shell
\$ = if the effective UID is 0, a #, otherwise a $

QUESTION 20
On a system using shadowed passwords, the correct permissions for **/etc/passwd** are _____ and the correct permission for **/etc/shadow** are _____.

A. -rw-r-----, -r--------
B. -rw-r--r--, -r--r--r--
C. -rw-r--r--, -r--------
D. -rw-r--rw-, -r-----r--
E. -rw--------, -r-------

Correct Answer: C
Section: 107.1 Manage user and group accounts and related system files
Explanation

Explanation/Reference:
/etc/passwd must be readable by all, while /etc/shadow should be readable only by the superuser.

QUESTION 21
You discover a pending job for the at command.

Which of the following do you have to use to remove it?

A. atrm
B. atq -r
C. at -r
D. rmat

Correct Answer: A
Section: 107.2 Automate system administration tasks by scheduling jobs
Explanation

Explanation/Reference:
From the man pages:
atrm deletes jobs, identified by their job number.

QUESTION 22
Which two of the following Class B IPv4 networks are reserved by IANA for private address assignment and private routing?

(Choose two)

A. 128.0.0.0
B. 169.16.0.0
C. 169.254.0.0
D. 172.16.0.0
E. 172.20.0.0

Correct Answer: DE
Section: 109.1 Fundamentals of internet protocols
Explanation

Explanation/Reference:
172.16.0.0/16 172.31.0.0/16 Class B addresses are reserved for both private assignment and routing.

169.254.0.0/16 is an APIPA address, and used only locally (see http://tools.ietf.org/html/rfc3927)
169.16/16 and 128.0/16 are public IPv4 addresses and should not be used for internal routing.

QUESTION 23
The following output shows an excerpt from a standard network configuration file:

```
time  37/udp timeserver
rlp   39/udp
name  42/udp nameserver
whois 43/tcp nickname
```

Which file could this be from?

A. /etc/hosts
B. /etc/inetd.conf
C. /etc/named.conf
D. /etc/services
E. /etc/syslog.conf

Correct Answer: D
Section: 109.2 Basic network configuration
Explanation

Explanation/Reference:
/etc/services is a plain ASCII file providing a mapping between human-friendly textual names for internet services, and their underlying assigned port numbers and protocol types.

QUESTION 24
A new department's local area network has to be connected to the existing LAN using a router. This new department's LAN uses IP addresses from 192.168.112.64/26 and the first free IP address there was reserved for the router.

How many IP addresses were left for other hosts to be connected?

A. 63
B. 24
C. 61
D. 42

Correct Answer: C
Section: 109.1 Fundamentals of internet protocols
Explanation

Explanation/Reference:
Subnetmask /26 defines 6 Bits for the Subnetaddresses. 6 Bit = 64 Addresses (2^6 = 64). Subtract 2 for Broadcast- and Net-Addresses and 1 for the router, leaves 61 addresses for hosts.

QUESTION 25
Which of the following lines would you find in the file /etc/nsswitch.conf?

A. order hosts, bind
B. 192.168.168.4 dns-server
C. hosts: files,dns
D. domain mycompany.com

Correct Answer: C
Section: 109.2 Basic network configuration
Explanation

Explanation/Reference:
nsswitch.conf - System Databases and Name Service Switch configuration file
This file specifies how services look for specific data like Mail aliases, Groups of users, hosts, protocols or services. For each "database" the lookup paths are specified. In this example for hosts the system would look first in /etc/hosts before asking a dns server for the information.

A) would indicate /etc/host.conf
B) would indicate /etc/hosts
D) would indicate /etc/resolv.conf

QUESTION 26
Which of the following lines would you find in the file /etc/host.conf?

A. order hosts, bind
B. 192.168.168.4 dns-server
C. hosts: files, dns
D. domain mycompany.com

Correct Answer: A
Section: 109.2 Basic network configuration
Explanation

Explanation/Reference:
The file /etc/host.conf contains configuration information specific to the resolver library. It should contain one configuration keyword per line, followed by appropriate configuration information. The keywords recognized are **order, trim, multi, nospoof, spoof,** and **reorder**.

B) would indicate /etc/hosts
C) would indicate /etc/nsswitch.conf
D) would indicate /etc/resolv.conf

QUESTION 27
Which of the following protocols uses two different network ports?

A. NTP
B. FTP
C. Rsh
D. HTTP
E. Telnet

Correct Answer: B
Section: 109.1 Fundamentals of internet protocols
Explanation

Explanation/Reference:

FTP is odd in the fact that it uses two ports to accomplish its task. It typically uses port 20 (active, or dynamic ports for passive FTP) for data transfer and port 21 to listen to commands.

QUESTION 28
If you suspect that a gateway machine on your network has failed but you are unsure which machine, which command will help locate the problem?

A. ps
B. netstat
C. nslookup
D. ifconfig
E. traceroute

Correct Answer: E
Section: 109.3 Basic network troubleshooting
Explanation

Explanation/Reference:
A) lists processes
B) lists open ports
C) lists DNS entries
D) lists information about ethernet adaptors

traceroute has to be installed separately (at least in ubuntu)

QUESTION 29
You have a file /etc/resolv.conf, but the computer does not use the configured DNS servers to look up host names.

What is most likely the problem?

A. The hosts entry in your /etc/nsswitch.conf does not list dns.
B. You do not have a /etc/named.conf file.
C. The localhost hostname is not properly configured in /etc/hosts.
D. The named daemon is not running on your computer.

Correct Answer: A
Section: 109.4 Configure client side DNS
Explanation

Explanation/Reference:
nsswitch.conf is used to specify what resources a service has to use, check if the hosts entry contains files and dns as possible lookup methods.

QUESTION 30
Which two services resolve Netbios names to IP addresses?

A. WINS
B. NetbiosSVC
C. smbd
D. nmbd
E. DNS

Correct Answer: AD
Section: 109.1 Fundamentals of internet protocols

Explanation

Explanation/Reference:
A) Windows Internet Name Service (WINS) is Microsoft's implementation of NetBIOS Name Service (NBNS), a name server and service for NetBIOS computer names. Effectively WINS is to NetBIOS names, what DNS is to domain names
D) This program is part of the samba suite. nmbd is a server that understands and can reply to NetBIOS over IP name service requests, like those produced by SMB/CIFS clients such as Windows 95/98/ME, Windows NT, Windows 2000, Windows XP and LanManager clients. It also participates in the browsing protocols which make up the Windows "Network Neighborhood" view.

QUESTION 31
Which of the following will run a file named /myscript every 23 minutes past midnight every two hours?

A. 23 0-23/2 * * * /myscript
B. 23 */0-23 * * * /myscript
C. 23 @2 * * * /myscript
D. 11 2/0-23 * * * /myscript

Correct Answer: A
Section: 107.2 Automate system administration tasks by scheduling jobs
Explanation

Explanation/Reference:
crontab job syntax: minutes hours days months day/week command
also correct would be 23 */2 * * * /myscript

QUESTION 32
Which file is responsible for configuring the inet daemon?

A. /etc/inetd.conf
B. /etc/xinetd.conf
C. /etc/tcpd.conf
D. /etc/inet.conf

Correct Answer: A
Section: 110.2 Setup host security
Explanation

Explanation/Reference:
From http://www.freebsd.org/doc/handbook/network-inetd.html:

Configuration of inetd is done via the file /etc/inetd.conf. Each line of the configuration file specifies an individual daemon. Comments in the file are preceded by a "#". The format of each entry in /etc/inetd.conf is as follows:

```
service-name
socket-type
protocol
{wait|nowait}[/max-child[/max-connections-per-ip-per-minute[/max-child-per-ip]]]
user[:group][/login-class]
server-program
server-program-arguments
```

An example entry for the ftpd(8) daemon using IPv4 might read:

```
ftp     stream  tcp     nowait  root    /usr/libexec/ftpd       ftpd -l
```

QUESTION 33
Which of the following lines would you expect to see in the file /etc/protocols?

A. in.tftpd: LOCAL
B. tftp dgram udp wait root /usr/sbin/tcpd in.tftpd
C. tftp 69/udp
D. udp 17 UDP

Correct Answer: D
Section: 109.2 Basic network configuration
Explanation

Explanation/Reference:
This file is a plain ASCII file, describing the various DARPA internet protocols that are available from the TCP/IP subsystem. It should be consulted instead of using the numbers in the ARPA include files, or, even worse, just guessing them. These numbers will occur in the protocol field of any IP header.

A) /etc/hosts.allow
B) /etc/inetd.conf
C) /etc/services

QUESTION 34
The following excerpt is from what standard network configuration file?

```
ftp         21/tcp
fsp         21/udp         fspd
ssh         22/tcp                      # SSH Remote Login Protocol
ssh         22/udp
telnet      23/tcp
smtp        25/tcp         mail
time        37/tcp         timserver
time        37/udp         timserver
rlp         39/udp         resource    # resource location
nameserver  42/tcp         name        # IEN 116
whois       43/tcp         nicname
```

A. /etc/hosts
B. /etc/inetd.conf
C. /etc/services
D. /etc/syslog.conf

Correct Answer: C
Section: 109.2 Basic network configuration
Explanation

Explanation/Reference:
From the man pages:
services is a plain ASCII file providing a mapping between human-friendly textual names for internet services, and their underlying assigned port numbers and protocol types.

QUESTION 35
The user space log daemon is called ...?

A. klog
B. klogd
C. syslog

D. syslogd

Correct Answer: D
Section: 108.2 System logging
Explanation

Explanation/Reference:
From the man pages:
System logging is provided by a version of syslogd(8) derived from the stock BSD sources. Support for kernel logging is provided by the klogd(8) utility which allows kernel logging to be conducted in either a standalone fashion or as a client of syslogd.

QUESTION 36
How can you verify the integrity of the /etc/passwd file?

A. pwchk
B. pwck
C. chkpw
D. ckpw

Correct Answer: B
Section: 107.1 Manage user and group accounts and related system files
Explanation

Explanation/Reference:
From the man pages:
The pwck command verifies the integrity of the users and authentication information. It checks that all entries in /etc/passwd and /etc/shadow have the proper format and contain valid data. The user is prompted to delete entries that are improperly formatted or which have other uncorrectable errors.
Checks are made to verify that each entry has:

- the correct number of fields
- a unique and valid user name
- a valid user and group identifier
- a valid primary group
- a valid home directory
- a valid login shell

QUESTION 37
The user bob complains that he cannot access his email. In which directory would you look to see if there is any deliverable email for him?

A. /var/spool/mail
B. /var/mail/mqueue
C. /var/spool/mqueue
D. /home/bob/.mail

Correct Answer: A
Section: 108.3 Mail Tranfer Agent (MTA) basics
Explanation

Explanation/Reference:
A) in /var/spool/mail/ (or /var/mail in newer distributions) exists one file per user, this file contains all (undelivered) mails for that user. If the user is unable to read his/her mails, check the permissions on the file.
B) ???
C) The mail queue, /var/spool/mqueue, is the directory in which the mail queue and temporary files reside. The messages are stored in various queue files that exist under the /var/spool/mqueue directory. Queue files

take the following forms:
qf*—control (queue) files for messages
df*—data files
tf*—temporary files
nf*—a file used when a unique ID is created
xf*—transcript file of the current session
Normally, a sendmail subdaemon processes the messages in this queue periodically, attempting to deliver each message. Each time sendmail processes the queue, it reads and sorts the queue, then attempts to run all jobs in order.
D) ???

QUESTION 38
To avoid spammers using your mail server to relay their messages, you need to _____.

A. Disable the relay control in /etc/aliases
B. Set up a ruleset for this in /etc/sendmail.cf
C. Set up relay control in your DNS's MX record.
D. Recompile sendmail with the -NORELAY flag.

Correct Answer: B
Section: 108.3 Mail Tranfer Agent (MTA) basics
Explanation

Explanation/Reference:
For an overly complicated example see http://www.sendmail.org/m4/anti_spam.html#header_checks

QUESTION 39
One of your users has installed a commercial publishing program that works under X on a variety of UNIX and Linux platforms. The user made a series of configuration changes regarding the initial window size, location and color. Now he is having difficulties undoing these changes and is asking for your help. In which file would you think you would most likely find the configuration settings you are seeking to change?

A. ~/.Xdefaults
B. ~/.xinitrc
C. ~/.xconfig
D. /etc/X11/XF86Config

Correct Answer: A
Section: 106.1 Install and configure X11
Explanation

Explanation/Reference:
From http://wiki.archlinux.org/index.php/Xdefaults#Xdefaults_syntax:

To see the default settings for your installed X11 apps, look in /usr/share/X11/app-defaults/.
The syntax of an Xdefaults file is as follows:
```
name.Class.resource: value
```

Here is a real world example:
```
xscreensaver.Dialog.headingFont: -*-fixed-bold-r-*-*-*-100-*-*-*-*-iso8859-1
```

QUESTION 40
Which of the following answers regarding user account configuration are true?

(Choose two)

A. Username is case-sensitive
B. Password is case-sensitive
C. Username is case-insensitive
D. Password is case-insensitive

Correct Answer: AB
Section: 107.1 Manage user and group accounts and related system files
Explanation

Explanation/Reference:
see http://tldp.org/LDP/lame/LAME/linux-admin-made-easy/creating-user-accounts.html

Exam C

QUESTION 1
Which commands can you use to change a user's password expiry information?

(Choose THREE correct answers)

A. usermod
B. passwd
C. chattr
D. chage
E. chsh

Correct Answer: ABD
Section: 107.1 Manage user and group accounts and related system files
Explanation

Explanation/Reference:
chattr - change file attributes on a Linux file system
chsh - change login shell

usermod - modify a user account
-f, --inactive INACTIVE The number of days after a password expires until the account is permanently disabled. A value of 0 disables the account as soon as the password has expired, and a value of -1 disables the feature.

chage - change user password expiry information
-M, --maxdays MAX_DAYS Set the maximum number of days during which a password is valid. When MAX_DAYS plus LAST_DAY is less than the current day, the user will be required to change his/her password before being able to use his/her account. This occurrence can be planned for in advance by use of the -W option, which provides the user with advance warning. Passing the number -1 as MAX_DAYS will remove checking a passwords validity.

passwd - change user password
-x, --maxdays MAX_DAYS Set the maximum number of days a password remains valid. After MAX_DAYS, the password is required to be changed.

QUESTION 2
Your machine's IP address used to function, but it's only got the localhost "lo" entry now. What three client-mode commands could you possibly use to get a new DHCP address?

A. dhcpd
B. ipconfig
C. dhclient
D. pump
E. dhcpcd

Correct Answer: CDE
Section: 109.3 Basic network troubleshooting
Explanation

Explanation/Reference:
From http://www.faqs.org/docs/Linux-mini/DHCP.html:
Currently there are three different DHCP client programs for Linux: **dhcpcd**, **pump** and **dhclient**.

From the man pages:

dhclient - Dynamic Host Configuration Protocol Client
dhcpcd is an implementation of the DHCP client specified in RFC2131 (when -r option is not specified) and RFC1541 (when -r option is specified). It gets the host information (IP address, netmask, broadcast address, etc.) from a DHCP server and configures the network interface of the machine on which it is running. It also tries to renew the lease time according to RFC2131 or RFC1541 (obsolete).
pump - configure network interface via BOOTP or DHCP protocol

QUESTION 3
Which of the following lines would you expect to see in the file /etc/services?

A. in.tftpd: LOCAL
B. tftp dgram udp wait root /usr/sbin/tcpd in.tftpd
C. tftp 69/udp
D. udp 17 UDP

Correct Answer: C
Section: 109.2 Basic network configuration
Explanation

Explanation/Reference:
services is a plain ASCII file providing a mapping between human-friendly textual names for internet services, and their underlying assigned port numbers and protocol types. Every networking program should look into this file to get the port number (and protocol) for its service.

A) /etc/hosts.allow
B) /etc/inetd.conf
D) /etc/protocols

QUESTION 4
For accessibility assistance, which of the following programs is an on-screen keyboard?

A. xkb
B. atkb
C. GOK
D. xOSK

Correct Answer: C
Section: 106.3 Accessibility
Explanation

Explanation/Reference:
From the GOK homepage:
GOK is an on-screen keyboard that provides access to the GNOME desktop via dynamically generated keyboards, and text entry via one of the provided alphanumeric keyboards, or a dynamic keyboard created based on the users current system keyboard driver, or even a user made keyboard.

xOSK = seems to be nothing
atkb = seems to be nothing
xkb = In the X Window System, the X keyboard extension or XKB extends the ability to control the keyboard over what is offered by the X Window System core protocol.

QUESTION 5
You have replaced inetd with xinetd.What must be done after installing to ensure that your machine will work correctly?

A. You must add a symbolic link from inetd.conf to xinetd.conf.

B. You don't have to do anything because they are compatible.
C. You must create a new configuration file for xinetd.
D. You must run xinetd-configure first.

Correct Answer: C
Section: 109.3 Basic network troubleshooting
Explanation

Explanation/Reference:
From http://www.xinetd.org/faq.html:
Q. Is it compatible with inetd ?
A. No, its configuration file has a different format than inetd's one and it understands different signals. However the signal-to-action assignment can be changed and a program has been included to convert inetd. conf to xinetd.conf. [the programs are called itox and xconv.pl]

QUESTION 6
Which configuration option can you use to prevent the root user from logging directly onto a machine using ssh?

A. NoRootLogon
B. PermitRootLogin No
C. NoRootLogon Yes
D. RootLogin = No
E. ProhibitRootLogon No

Correct Answer: B
Section: 110.2 Setup host security
Explanation

Explanation/Reference:
Fom the man pages:
sshd(8) reads configuration data from /etc/ssh/sshd_config (or the file specified with -f on the command line). The file contains keyword-argument pairs, one per line. Lines starting with '#' and empty lines are interpreted as comments. Arguments may optionally be enclosed in double quotes (") in order to represent arguments containing spaces.

PermitRootLogin Specifies whether root can log in using ssh(1). The argument must be "yes", "without-password", "forced-commands-only", or "no". The default is "yes".

QUESTION 7
What are the addresses falling into the range of 224.0.0.0 through 254.0.0.0?

A. Class C network
B. Class B network
C. This is an experimental address range
D. This is a broadcast range

Correct Answer: C
Section: 109.1 Fundamentals of internet protocols
Explanation

Explanation/Reference:
see http://en.wikipedia.org/wiki/IP_address, http://en.wikipedia.org/wiki/Multicast_address

224/4 actually is multicast and 240/4 is reserved

QUESTION 8
Which of the following IP networks does RFC1918 reserve for use on private intranets?

(Choose two)

A. 10.0.0.0
B. 224.0.0.0
C. 199.14.0.0
D. 172.152.0.0
E. 192.168.0.0

Correct Answer: AE
Section: 109.1 Fundamentals of internet protocols
Explanation

Explanation/Reference:
B) Multicast
C,D) public ClassC address range
do not confuse D) with the 172.16.0.0/12 address range

QUESTION 9
A remote logging computer with a host name of foobar is being installed on the local network.

What line in the system message configuration file will send all system messages to the remote computer?

A. *.* foobar. *
B. *.* @foobar
C. *=foobar
D. * .foobar
E. =foobar

Correct Answer: B
Section: 108.2 System logging
Explanation

Explanation/Reference:
From the man pages:
Remote Machine This syslogd(8) provides full remote logging, i.e. is able to send messages to a remote host running syslogd(8) and to receive messages from remote hosts. The remote host won't forward the message again, it will just log them locally. To forward messages to another host, prepend the hostname with the at sign (``@'').

QUESTION 10
You are writing a script and want to test the exit status of a process.

Which of the following is true?

A. The normal exit value differs.
B. You can't test the normal exit value.
C. The normal exit value is $EXIT.
D. The normal exit value is 0.

Correct Answer: D
Section: 105.2 Customize or write simple scripts

Explanation

Explanation/Reference:
Unix standards define 0 (zero) to indicate process finished without errors, and uses values other than 0 for error codes.

QUESTION 11
You are looking into a new script you received from your senior administrator. In the very first line you notice a #! followed by a path to a binary.

The shell will ...

A. ignore the script
B. use that binary to interpret the script
C. use that binary to compile the script
D. be replaced by that binary

Correct Answer: B
Section: 105.2 Customize or write simple scripts
Explanation

Explanation/Reference:
put `#! /bin/bash` in the first line of a shell script to execute it in a bash environment.

QUESTION 12
A user complained that programs started from his shell won't use his favorite editor.

Which of the following files should you edit to change this?

A. .editor
B. .bashrc
C. .bash_rc
D. ~/bash.conf

Correct Answer: B
Section: 105.1 Customize and use the shell environment
Explanation

Explanation/Reference:
When an interactive shell that is not a login shell is started, bash reads and executes commands from /etc/bash.bashrc and ~/.bashrc, if these files exist.

QUESTION 13
In what file do you change default shell variables for all users?

A. /etc/bashrc
B. /etc/profile
C. ~/.bash_profile
D. /etc/skel/.bashrc
E. /etc/skel/.bash_profile

Correct Answer: B
Section: 105.1 Customize and use the shell environment
Explanation

Explanation/Reference:
When invoked interactively with the --login option or when invoked as sh, Bash reads the /etc/profile instructions. These usually set the shell variables PATH, USER, MAIL, HOSTNAME and HISTSIZE. All settings that you want to apply to all your users' environments should be in this file.

QUESTION 14
The correct command to view "verbose" line printer queue information is

A. lpq -l
B. lpq -all
C. lpq --verbose
D. lpq -a

Correct Answer: A
Section: 108.4 Manage printers and printing
Explanation

Explanation/Reference:
From the man pages:
lpq - show printer queue status
-l Requests a more verbose (long) reporting format

QUESTION 15
Ghostscript can be used as:

A. A Line Printer Daemon
B. A print filter to convert PostScript data for non-PostScript printers
C. A print filter to allow correct printing on PostScript printers
D. A print filter to remove "ghosting" and "staircase" effect problems
E. A graphical viewer for PostScript files

Correct Answer: B
Section: 108.4 Manage printers and printing
Explanation

Explanation/Reference:
From http://www.ghostscript.com/Ghostscript.html:
Ghostscript is a package of software that provides:
* An interpreter for the PostScript (TM) language, with the ability to convert PostScript language files to many raster formats, view them on displays, and print them on printers that don't have PostScript language capability built in;

QUESTION 16
Which of the following tools is used to configure CUPS?

A. lpc
B. lpadmin
C. lpr
D. lpd
E. lpctrl

Correct Answer: B
Section: 108.4 Manage printers and printing
Explanation

Explanation/Reference:
From http://www.cups.org/doc-1.1/sam.html#4_2:
The lpadmin command allows you to perform most printer administration tasks from the command-line and is located in /usr/sbin.

A) lpc was used to configure systems without CUPS.
C) lpr submits files for printing. Files named on the command line are sent to the named printer (or the default destination if nodestination is specified). If no files are listed on the command-line, lpr reads the print file from the standard input.
D,E) does not exist

QUESTION 17
What command should be entered to print and then delete the file, foobar.txt?

A. lpr -0 delete foobar.txt
B. lpr -d foobar.txt
C. lpr -r foobar.txt
D. lpr -0 remove foobar.txt

Correct Answer: C
Section: 108.4 Manage printers and printing
Explanation

Explanation/Reference:
From the man pages:
lpr - print files
-r Specifies that the named print files should be deleted after printing them.

QUESTION 18
Which of these are name resolution related files?

(Select TWO that apply)

A. /etc/hosts
B. /etc/nsswitch.conf
C. /etc/lmhosts
D. /etc/man
E. /etc/dns.conf

Correct Answer: AB
Section: 109.2 Basic network configuration
Explanation

Explanation/Reference:
/etc/hosts is the local name resolution "database" and /etc/nsswitch.conf tells the lookup programs if they have to look into /etc/hosts to find hostnames

C) is used for WINS name resolution (Lan Manager Hosts)
D) does not exist
E) does not exist (DNS server configuration file is called named.conf)

QUESTION 19
If you want to print a listing of your computer's mail queues, what command would you use?

A. sendmail -l

B. lpq
C. mailq
D. mlq

Correct Answer: C
Section: 108.3 Mail Tranfer Agent (MTA) basics
Explanation

Explanation/Reference:
From the man pages:
mailq List the mail queue. Each entry shows the queue file ID, message size, arrival time, sender, and the recipients that still need to be delivered. If mail could not be delivered upon the last attempt, the reason for failure is shown. This mode of operation is implemented by executing the postqueue(1) command.

A) there is no -l option in sendmail
B) print queue status
D) does not exist

QUESTION 20
The correct crontab entry to execute the script chklog once per hour between 3 p.m. and 5 p.m. on Monday and Thursday each week is:

A. 0 3,4,5 * * 2,5 chklog
B. 0 3,4,5 * * 1,4 chklog
C. 0 15,16,17 * * 1,4 chklog
D. 0 15,16,17 1,4 * * chklog
E. * 15,16,17 * * 1,4 chklog

Correct Answer: C
Section: 107.2 Automate system administration tasks by scheduling jobs
Explanation

Explanation/Reference:
also correct would be 0 15-17 * * 1,4 chklog

A) would run chklog at 3AM,4AM and 5AM on Tuesdays and Fridays
B) same as A, but Monday, Thursday
D) would run chklog at 3PM, 4PM, 5PM, on the 1st and 4th of each month
E) same as C, but would run chklog once every minute

QUESTION 21
Of the ways listed, which is the best way to temporarily suspend a user's ability to interactively login?

A. Changing the user's UID.
B. Changing the user's password.
C. Changing the user's shell to /bin/false.
D. Removing the user's entry in /etc/passwd.
E. Placing the command logout in the user's profile.

Correct Answer: C
Section: 107.1 Manage user and group accounts and related system files
Explanation

Explanation/Reference:
CAUTION: Simply using /bin/false as someone's shell does not keep them from using said account to

authenticate over ssh and using non-shell tools such as port forwarding. A default configuration in sshd will often allow tunneling and other non-shell activity.

QUESTION 22
What file is typically used to display messages at the login prompt when remote users telnet in to the machine?

A. /etc/issue
B. /etc/motd
C. /etc/net.banner
D. /etc/issue.net

Correct Answer: D
Section: 105.1 Customize and use the shell environment
Explanation

Explanation/Reference:
see http://www.wapopia.com/linux/etcissue.htm
/etc/issue and /etc/issue.net files can be used to print any logon messages to users logging on to a Linux machine, the message appears BEFORE the login prompt of the login console.

QUESTION 23
Which of the following information is not provided by the command netstat?

A. broadcast services
B. interface services
C. masquerading connections
D. network connections
E. routing information

Correct Answer: A
Section: 109.3 Basic network troubleshooting
Explanation

Explanation/Reference:
From the man pages:
netstat - Print network connections, routing tables, interface statistics, masquerade connections, and multicast memberships

QUESTION 24
Which of the following is an example of an ICMP packet with a message type?

A. HTTP traffic packet
B. DNS traffic packet
C. Ping packet
D. Ethernet frame
E. SSH packet

Correct Answer: C
Section: 109.1 Fundamentals of internet protocols
Explanation

Explanation/Reference:
From the man pages:

ping, ping6 - send ICMP ECHO_REQUEST to network hosts

QUESTION 25
Which of the following find command will print out a list of suid root files in /usr?

A. find /usr -uid 0 -perm +4000
B. find -user root +mode +s /usr
C. find -type suid -username root -d /usr
D. find /usr -ls *s* -u root
E. find /usr -suid -perm +4000

Correct Answer: A
Section: 105.2 Customize or write simple scripts
Explanation

Explanation/Reference:
find needs the starting directory as first parameter, eliminating B and C as the right answers.

From the man pages:
find - search for files in a directory hierarchy
-uid n
File's numeric user ID is n.
-perm mode
File's permission bits are exactly mode (octal or symbolic). Since an exact match is required, if you want to use this form for symbolic modes, you may have to specify a rather complex mode string. For example -perm g=w will only match files which have mode 0020 (that is, ones for which group write permission is the only permission set). It is more likely that you will want to use the `/' or `-' forms, for example -perm -g=w, which matches any file with group write permission.

QUESTION 26
Man pages cover what topics?

(Select THREE)

A. superuser commands
B. configuration commands
C. system policies
D. programming libraries
E. kernel version information

Correct Answer: ABD
Section: 105.1 Customize and use the shell environment
Explanation

Explanation/Reference:
There are twelve sections of the reference manuals. They are:

Section	Description
1	Commands and Application Programs
2	System Calls (used in programming languages)
3	Subroutines (used in programming languages)
4	File Formats
5	Miscellaneous
6	Games
7	Special Files
8	System Maintenance Procedures
local	Locally written man pages (third party software man pages.)

public Public domain software man pages.
new New software man pages.
old Old/obsolete software man pages.

QUESTION 27
Which of the following lines would you find in the file /etc/hosts?

A. order hosts, bind
B. 192.168.168.4 dns-server
C. hosts: files,dns
D. domain mycompany.com

Correct Answer: B
Section: 109.2 Basic network configuration
Explanation

Explanation/Reference:
This file is a simple text file that associates IP addresses with hostnames, one line per IP address. For each host a single line should be present with the following information: IP_address canonical_hostname [aliases...]

A) /etc/host.conf
C) /etc/nsswitch.conf
D) /etc/resolv.conf

QUESTION 28
Which of the following lines from /etc/X11/XF86Config indicates that fonts can be found on a font server?

A. FontPath= server
B. Fonts "unix/:7100"
C. FontPath "unix/:7100"
D. Fonts= server
E. Fontserver = "servername"

Correct Answer: C
Section: 106.1 Install and configure X11
Explanation

Explanation/Reference:
From http://www.xfree86.org/4.3.0/XF86Config.5.html#sect2

FontPath "path"
sets the search path for fonts. This path is a comma separated list of font path elements which the X server searches for font databases. Multiple FontPath entries may be specified, and they will be concatenated to build up the fontpath used by the server. Font path elements may be either absolute directory paths, or a font server identifier. Font server identifiers have the form:

<trans>/<hostname>:<port-number>

where <trans> is the transport type to use to connect to the font server (e.g., unix for UNIX-domain sockets or tcp for a TCP/IP connection), <hostname> is the hostname of the machine running the font server, and <port-number> is the port number that the font server is listening on (usually 7100).

QUESTION 29
When you start XWindows, which series of programs and/or scripts would most closely describe the start-up process?

A. xdm --> xinit --> xinitrc --> Xclients
B. kde --> xinitrc --> xinit --> Xclients
C. startx --> xinitrc --> Xclients --> kde
D. startx --> xinit --> xinitrc --> Xclients
E. startx-->xinit-->Xclients-->xinitrc

Correct Answer: D
Section: 106.1 Install and configure X11
Explanation

Explanation/Reference:
From http://tldp.org/HOWTO/XWindow-User-HOWTO/runningx.html:

typically when switching to runlevel >= 2 (depending on inittab) init starts xdm (the display manager), and thus X.
If the xdm dies, or needs to be restarted a user can call **startx** from console, which invokes **xinit** using the config scripts ~/.xserverrc and **~./xinitrc** (or /etc/X11/xinit/ if the local files are not found) and finally the config script **~/.Xclients**

QUESTION 30
Your senior administrator asked you to change the default background of his machine, which uses XDM.

Which file would you edit to achieve this?

A. /etc/X11/xdm/Xsetup
B. /etc/X11/xdm.conf
C. /etc/X11/xdm/Defaults
D. /etc/X11/defaults.conf

Correct Answer: A
Section: 106.2 Setup a display manager
Explanation

Explanation/Reference:
After resetting the X server, xdm runs the Xsetup script to assist in setting up the screen the user sees along with the xlogin widget.
For example, an entry in Xsetup to change the background could be:
/usr/X11R6/bin/xsetroot -solid steelblue

QUESTION 31
You are using an application that you want to appear on the screen of another machine.

What environment variable would you have to set or edit to achieve this?

A. DISPLAY
B. REMOTE
C. REMOTE_XWINDOW
D. SCREEN

Correct Answer: A
Section: 106.1 Install and configure X11
Explanation

Explanation/Reference:
From http://www.xfree86.org/current/X.7.html#sect4:

On POSIX systems, the default display name is stored in your DISPLAY environment variable. This variable is set automatically by the xterm terminal emulator. However, when you log into another machine on a network, you will need to set DISPLAY by hand to point to your display.

QUESTION 32
In XF86Config which section is concerned with fonts?

A. the Fonts section
B. The Files section
C. The xfsCodes section
D. The Graphics section
E. The modeline section

Correct Answer: B
Section: 106.1 Install and configure X11
Explanation

Explanation/Reference:
see http://www.xfree86.org/4.3.0/XF86Config.5.html#sect2

http://www.xfree86.org/4.3.0/XF86Config.5.html#sect4
The module section would be correct also, since it defines the modules used to display fonts

QUESTION 33
The files in the /etc/skel directory are used by the...

A. pwconv command
B. pwunconv command
C. useradd command
D. passwd command

Correct Answer: C
Section: 107.1 Manage user and group accounts and related system files
Explanation

Explanation/Reference:
useradd uses the config-file /etc/default/useradd which contains the shell variable $SKEL, that points to /etc/skel (if uncommented). useradd copies all files and directories in $SKEL to the new home directory.

QUESTION 34
Which of the following can the chage command NOT change?

A. The number of days since January 1, 1970 on which the use's account will no longer be accessible
B. The number of days since January 1, 1970 when the password can change
C. The number of days since January 1st, 1970 when the password was last changed
D. The maximum number of days during which a password is valid
E. The number of days of inactivity after a password has expired before the account is locked

Correct Answer: B
Section: 107.1 Manage user and group accounts and related system files
Explanation

Explanation/Reference:
From the man pages:

The chage command changes the number of days between password changes and the date of the last password change. This information is used by the system to determine when a user must change his/her password.

The answer refers to the minimum password age, but this is a value calculated from the last password change, not 1970-01-01. You can set the minimum age with option -m, --mindays.

QUESTION 35
Which command will set the local machine's timezone to UTC?

A. cat UTC > /etc/timezone
B. ln -s /usr/share/zoneinfo/UTC /etc/localtime
C. date --timezone=UTC
D. mv /usr/timezone/UTC /etc

Correct Answer: B
Section: 107.3 Localisation and internationalisation
Explanation

Explanation/Reference:
The symlink practice was stopped some time ago, probably because a /usr is not necessarily mounted all the time.
But technically B) is correct

use tzconfig to change the timezone on recent distributions.

QUESTION 36
Users cannot submit jobs to an attached printer. Choose the correct file that must be edited to fix this problem.

A. /etc/hosts
B. /etc/hosts.allow
C. /etc/host.deny
D. /etc/hosts.lpd
E. /var/spool/hosts.lpd

Correct Answer: D
Section: 108.4 Manage printers and printing
Explanation

Explanation/Reference:
From http://www.redhat.com/docs/manuals/linux/RHL-8.0-Manual/admin-primer/s1-printers-sharing.html:

For pure Linux or Linux/UNIX environments, printer sharing can be controlled using the /etc/hosts.lpd file. This file is not created by default; as root, create the file /etc/hosts.lpd on the machine to which the printer is attached. On separate lines in the file, add the IP address or hostname of each machine which should have printing privileges:

falcon.example.com
pinky.example.com
samiam.example.com
pigdog.example.com
yeti.example.com

To have LPRng use /etc/hosts.lpd for access control, you must add the following line to /etc/lpd.perms:
ACCEPT SERVICE=X REMOTEHOST=</etc/hosts.lpd

This line must be added to /etc/lpd.perms before the line containing "REJECT SERVICE=X NOT SERVER". Failure to do so will prevent /etc/hosts.lpd from being recognized. Finally, restart the lpd printer daemon by issuing the command /sbin/service lpd restart (as root).

QUESTION 37
In the following output, which answer is representative of the host performing gateway functions?

```
Destination     Gateway         Genmask          Flags  Metric  Ref  Use  Iface
10.3.3.0        192.168.1.1     255.255.255.255  UGH    0       0    0    eth0
192.168.1.0     *               255.255.255.0    U      0       0    0    eth0
192.168.77.0    *               255.255.255.0    U      0       0    0    vmnet1
127.0.0.0       *               255.0.0.0        U      0       0    0    lo
default         192.168.1.1     0.0.0.0          UG     0       0    0    eth0
```

A. The default gateway is on 192.168.77.0 network
B. The current host is the also the default gateway
C. Its eth0 interface is incorrectly configured
D. 192.168.1.1 is the default gateway

Correct Answer: D
Section: 109.1 Fundamentals of internet protocols
Explanation

Explanation/Reference:
A) with a probable netmask of 255.255.255.0 this address can never be a host
B) routes do not show the current host, so no conclusion about the host being the default gateway is possible
C) nothing indicates misconfiguration

QUESTION 38
Select the files that are associated with TCP Wrappers. Choose all that apply.

A. /etc/hosts
B. /etc/hosts.allow
C. /etc/hosts.deny
D. /etc/allow.hosts
E. /etc/allow.deny

Correct Answer: BC
Section: 109.2 Basic network configuration
Explanation

Explanation/Reference:
The example permits tftp requests from hosts in the local domain (notice the leading dot). Requests from any other hosts are denied. Instead of the requested file, a finger probe is sent to the offending host. The result is mailed to the superuser.

/etc/hosts.allow:
in.tftpd: LOCAL, .my.domain

/etc/hosts.deny:
in.tftpd: ALL: (/usr/sbin/safe_finger -l @%h | /usr/bin/mail -s %d-%h root) &

QUESTION 39
Which one of the following lines would you expect to see on the file /etc/hosts.allow?

A. in.tftpd: LOCAL

B. tftp dgram udp wait root /usr/sbin/tcpd in tdtpd
C. tftp 69/udp
D. udp 17 UDP

Correct Answer: A
Section: 109.2 Basic network configuration
Explanation

Explanation/Reference:
B) /etc/inetd.conf
C) /etc/services
D) /etc/protocols

QUESTION 40
What are the first two characters of an MD5 hashed password?

A. $1
B. $5
C. $6
D. 2a

Correct Answer: A
Section: 107.1 Manage user and group accounts and related system files
Explanation

Explanation/Reference:
From the man pages:
idsalt$encrypted
The following values of id are supported:

ID	Method
1	MD5
2a	Blowfish (not in mainline glibc; added in some Linux distributions)
5	SHA-256 (since glibc 2.7)
6	SHA-512 (since glibc 2.7)

Exam D

QUESTION 1
Which of the following commands can be used to view kernel messages?

A. less dmesg
B. less /var/log/boot.log
C. cat /proc/kernel |less
D. cat /proc/dmesg

Correct Answer: B
Section: 108.2 System logging
Explanation

Explanation/Reference:
A) this command would only work when executing it from /var/log
C) file does not exist
D) there is a dmesg file, but it's located in /var/log/dmesg

QUESTION 2
Which of the following commands will print the file putty on the printer hplaserj?

(Choose all that apply)

A. lpr -P hplaserj -F putty
B. lpr -Phplaserj putty
C. lpc printer=hplaserj file=putty
D. lpr -p hplaserj -f putty
E. lpr -P hplaserj putty

Correct Answer: BE
Section: 108.4 Manage printers and printing
Explanation

Explanation/Reference:
From the man pages:
lpr submits files for printing. Files named on the command line are sent to the named printer
-P destination[/instance] Prints files to the named printer.

-P expects, but does not require a space between printer name and option.
There is no -f or -F option.

QUESTION 3
Your server has two fully functional NICs with correct IP configuration. The server is not forwarding traffic between the NICs. Which command will enable forwarding properly?

A. setparam 1 > /proc/sys/net/ipv4/ip_autoconfig
B. echo 1 > /proc/sys/net/ipv4/ip_forward
C. cat $1 > /proc/sys/net/ethernet
D. set $=1 /proc/sys/net/ipv4/route

Correct Answer: B
Section: 109.2 Basic network configuration
Explanation

Explanation/Reference:
See http://www.ibm.com/developerworks/linux/library/l-proc.html

```
# cat /proc/sys/net/ipv4/ip_forward
0
# echo "1" > /proc/sys/net/ipv4/ip_forward
```

Remember that this solution is working only until reboot, use sysctl to set ip_forwarding permanently.

QUESTION 4
Which port is used for DNS?

A. 110
B. 21
C. 52
D. 53

Correct Answer: D
Section: 109.1 Fundamentals of internet protocols
Explanation

Explanation/Reference:
From /etc/services:

```
domain      53/tcp          # name-domain server
domain      53/udp
```

QUESTION 5
Which parameters should appear in a valid /etc/printcap file to allow a local printer queue to point to another machines print queue?

(Choose Two)

A. rm
B. rp
C. remoteip
D. netprinter
E. netip

Correct Answer: AB
Section: 108.4 Manage printers and printing
Explanation

Explanation/Reference:
see http://sunsite.ualberta.ca/Documentation/Misc/LPRng-3.5.2/LPRng-HOWTO-5.html#rm

The rm (remote machine or host) and rp or lp printer printcap options are used to specify the remote host and printer to be used.

QUESTION 6
While performing a security audit, you discover that a machine is accepting connections on TCP port 184, but it 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

Correct Answer: E
Section: 109.3 Basic network troubleshooting
Explanation

Explanation/Reference:
From the man pages:
lsof - list open files
-i This option selects the listing of files any of whose Internet address matches the address specified in i. If no address is specified, this option selects the listing of all Internet and x.25 (HP-UX) network files.
-n This option inhibits the conversion of network numbers to host names for network files. Inhibiting conversion may make lsof run faster. It is also useful when host name lookup is not working properly.
-P This option inhibits the conversion of port numbers to port names for network files. Inhibiting the conversion may make lsof run a little faster. It is also useful when port name lookup is not working properly.

`netstat -nap` would get the same information.

QUESTION 7
Which of the following lines would you expect to see in the file /etc/services?

A. in.tftpd: LOCAL
B. tftp dgram udp wait root /usr/sbin/tcpd in.tftpd
C. tftp 69/udp
D. udp 17 UDP

Correct Answer: C
Section: 109.2 Basic network configuration
Explanation

Explanation/Reference:
services is a plain ASCII file providing a mapping between human-friendly textual names for internet services, and their underlying assigned port numbers and protocol types. Every networking program should look into this file to get the port number (and protocol) for its service.

A) /etc/hosts.allow
B) /etc/inetd.conf
D) /etc/protocols

QUESTION 8
The following output shows an excerpt from a standard network configuration file:

```
time  37/udp timeserver
rlp   39/udp
name  42/udp nameserver
whois 43/tcp nickname
```

Which file could this be from?

A. /etc/hosts
B. /etc/inetd.conf
C. /etc/named.conf
D. /etc/services

E. /etc/syslog.conf

Correct Answer: D
Section: 109.2 Basic network configuration
Explanation

Explanation/Reference:
/etc/services is a plain ASCII file providing a mapping between human-friendly textual names for internet services, and their underlying assigned port numbers and protocol types.

QUESTION 9
Your server logfile shows repeated connections to TCP port 143. What service is being accessed?

A. smtp
B. imap
C. pop3
D. pop2
E. nmbd

Correct Answer: B
Section: 109.3 Basic network troubleshooting
Explanation

Explanation/Reference:
From /etc/services:

```
imap2           143/tcp         imap            # Interim Mail Access P 2 and 4
imap2           143/udp         imap
```

QUESTION 10
To learn more about the management or ownership of a website, what's the best utility to use?

A. tracert
B. traceroute
C. whois
D. ping
E. telnet

Correct Answer: C
Section: 109.4 Configure client side DNS
Explanation

Explanation/Reference:
A) Windows traceroute Befehl, lists all hosts on the way to target
B) Unix traceroute
D) ICMP echo request to target, lists average response time
E) opens a connection to a host to issue commands

whois is an undocumented program in /usr/bin, that reads the entries from the NIC database. see http://www.nic.com/nic/whois/

QUESTION 11
What command would cause a print job to be printed next regardless of its current position in the queue.

A. lpc topq
B. lpc -t

C. lpq -t
D. lpc move
E. lpq --next

Correct Answer: A
Section: 108.4 Manage printers and printing
Explanation

Explanation/Reference:
The lpc topq command can be used to put a job (or jobs) at the head of the spool queue. This command is very useful when some job requires priority service. You can select the job by using the job number or the job ID.

Example:

```
h4: {152} % lpc topq lp 17970
Printer: lp@h4
lp: selected 'papowell@h4+17970'
lp@h4.private: started
h4: {153} % lpq
Printer: lp@h4
 Queue: 3 printable jobs
 Server: pid 17999 active
 Rank   Owner/ID          Class Job Files      Size Time
active papowell@h4+17970    A 17970 (stdin)      5 18:23:35
1      papowell@h4+17959    A 17959 (stdin)      3 18:23:24
2      papowell@h4+17962    A 17962 (stdin)      6 18:23:30
```

This is valid for non-CUPS systems only!

QUESTION 12
Which two files are responsible for allowing users to execute cron jobs?

A. /etc/cron.allow
B. /var/spool/cron.allow
C. /var/spool/cron.allow
D. /etc/cron.deny

Correct Answer: AD
Section: 107.2 Automate system administration tasks by scheduling jobs
Explanation

Explanation/Reference:
From http://docs.sun.com/app/docs/doc/805-7229/6j6q8svfu?a=view:

You can control access to crontab by using two files in the /etc/cron.d directory: cron.deny and cron.allow. These files permit only specified users to perform crontab tasks such as creating, editing, displaying, or removing their own crontab files. The cron.deny and cron.allow files consist of a list of user names, one per line. These access control files work together like this:

* If cron.allow exists, only the users listed in this file can create, edit, display, or remove crontab files.
* If cron.allow doesn't exist, all users may submit crontab files, except for users listed in cron.deny.
* If neither cron.allow nor cron.deny exists, superuser privileges are required to run crontab.

Superuser privileges are required to edit or create the cron.deny and cron.allow files.

QUESTION 13
What file must you create in your home directory in order to enable mail forwarding?

A. .redirect

B. .forward
C. .plan
D. .mail
E. None of the choices

Correct Answer: B
Section: 108.3 Mail Tranfer Agent (MTA) basics
Explanation

Explanation/Reference:
From http://www.faqs.org/docs/Linux-HOWTO/Mail-User-HOWTO.html:

MTA aliases usually require administrator privileges to set up. But it is desirable for mail users to be able to set up forwarding of their own mail without administrator intervention. To support this, most MTAs follow sendmail's lead and look for a file called **.forward** in your home directory. The contents of this file is interpreted like the target of an alias which should receive all your mail. The most common use for this facility is to redirect your mail to an account on another machine.

QUESTION 14
The _____ is used by the local host to determine which hosts are on the local subnet, and which hosts are on remote networks.

A. DNS
B. ARP
C. gateway
D. netmask
E. routing protocol

Correct Answer: D
Section: 109.1 Fundamentals of internet protocols
Explanation

Explanation/Reference:
From http://en.wikipedia.org/wiki/Subnetwork
All computers belonging to a particular network must follow a simple rule for assigning addresses to their interfaces. This involves dividing the set of bits of an address into two parts:
1. The first part is the network prefix. It is a contiguous group of high-order bits whose value is common among all hosts within a network.
2. The remaining, least-significant bits of the address designate the host or interface identifier. This part is unique on the network and specifies the device or often just one specific network interface connected to the local network.
With this rule, IP packets may be selectively routed across multiple networks via routers to a destination host if the network prefixes of origination and destination hosts differ, or sent directly to a target host on the local network if they are the same.
The network prefix may be written in a form identical to that of the address itself. This is called the network mask, or netmask, of the address.

QUESTION 15
To disable telnet service on a system, which action should you take?

A. Put NONE in /etc/telnet.allow
B. Remove the appropriatetelnet init script.
C. Put a line 'ALL:ALL' in /etc/hosts.deny
D. Comment the telnet entry in /etc/inittab
E. Comment the telnet entry in /etc/inetd.conf

Correct Answer: E
Section: 109.2 Basic network configuration
Explanation

Explanation/Reference:
inetd, called also the super server, will load a network program based upon a request from the network. The inetd.conf file tells inetd which ports to listen to and what server to start for each port.

The first thing to look at as soon as you put your Linux system on ANY network is what services you need to offer. Services that you do not need to offer should be disabled and uninstalled so that you have one less thing to worry about, and attackers have one less place to look for a hole. Look at your /etc/inetd.conf file to see what services are being offered by your inetd program. Disable what you do not need by commenting them out by adding a # at the beginning of the line, and then sending your inetd process a SIGHUP command to update it to the current inetd.conf file.

Example from /etc/inetd.conf:
telnet stream tcp nowait root /usr/sbin/tcpd in.telnetd

Hints:
use this command to signal inetd to reload its config file:
killall -HUP inetd
use this command to make inetd.conf immune to accidental, or otherwise, changes:
chattr +i /etc/inetd.conf

QUESTION 16
In what file are the mail aliases kept for Sendmail? (Provide the complete path)

A. /etc/aliases
B. /etc/mailaliases
C. /etc/sendmail.aliases
D. /etc/sendmail/aliases
E. /var/spool/mail/aliases

Correct Answer: A
Section: 108.3 Mail Tranfer Agent (MTA) basics
Explanation

Explanation/Reference:
From http://linux.die.net/man/5/aliases.sendmail:

This file describes user ID aliases used by sendmail. The file resides in /etc and is formatted as a series of lines of the form
`name: addr{, addr}`
The name is the name to alias, and the addr are the aliases for that name. addr can be another alias, a local username, a local filename, a command, an include file, or an external address.

QUESTION 17
What are reverse DNS entries used for?

A. Reverse DNS enable diagnostic commands like traceroute to work.
B. Reverse DNS gives you information about the owner of the DNS entry.
C. Reverse DNS provides the hostname for a particular numeric IP address.
D. Reverse DNS provides geographical information about the DNS net location.

Correct Answer: C
Section: 109.1 Fundamentals of internet protocols
Explanation

Explanation/Reference:
Since normal DNS resolves hostnames into IP adresses, RDNS resolves IP addresses into hostnames.

QUESTION 18
What file determines the DNS servers used by your computer?

A. /etc/hosts
B. /etc/named.conf
C. /etc/nsswitch.conf
D. /etc/resolv.conf

Correct Answer: D
Section: 109.4 Configure client side DNS
Explanation

Explanation/Reference:
From http://en.wikipedia.org/wiki/Resolv.conf:
resolv.conf is the name of a computer file used in various operating systems to configure the Domain Name System (DNS) resolver library. The file is a plain-text file usually created by the network administrator or by applications that manage the configuration tasks of the system.

A) contains DNS entries
B) is the configuration file for the DNS server
C) is the file telling the lookup service where to look

QUESTION 19
To create a user account, keep in mind that the username is at most __ characters long.

A. 6
B. 8
C. 12
D. 18

Correct Answer: B
Section: 107.1 Manage user and group accounts and related system files
Explanation

Explanation/Reference:
From the Linux Admin FAQ:

6.17 What is the maximum username length, and is there way to extend it?
No. Username length is not configurable. Under libc-5, the utmp and wtmp files only allow 8 characters for a username. Under libc-6, this is increased to 32 characters. You can use usernames longer than this limit. However, the utmp/wtmp entries will be truncated, and so won't correspond to a valid username. This doesn't matter for most things.

QUESTION 20
When you use DNS to find a hostname using a particular IP address, which kind of DNS entry is involved?

A. Reverse DNS entries
B. IP DNS entries

C. Address DNS entries
D. Network DNS entries

Correct Answer: A
Section: 109.1 Fundamentals of internet protocols
Explanation

Explanation/Reference:
Normally DNS resolves hostnames to IP addresses, if you use an IP address to find a hostname use RDNS.

QUESTION 21
Your senior system administrator asked you to edit the /etc/inetd.conf file in order to disable the time service.

After doing so, what would be the next thing to do?

A. Reboot the machine
B. Restart the inetd
C. Find the PID of inetd and kill it with kill -15
D. Find the PID of inetd and send it a SIGHUP

Correct Answer: D
Section: 109.3 Basic network troubleshooting
Explanation

Explanation/Reference:
From the man pages:
inetd reads the configuration-file and the default settings in /etc/default/inetd once when it starts up and rereads them again whenever it receives a hangup signal, SIGHUP. New services can be activated and existing services can be deleted or modified by editing the configuration-file and then sending inetd a SIGHUP signal.

QUESTION 22
You have a Linux system routing 3 networks through 3 separate NICs and are having trouble with your IP forwarding. What file would you check to ensure that IP forwarding is enabled?

A. /etc/defaultrouter
B. /proc/net/tcp
C. /proc/sys/net/ipv4/ip_forward
D. /var/log/messages

Correct Answer: C
Section: 109.3 Basic network troubleshooting
Explanation

Explanation/Reference:
From http://techgurulive.com/2008/09/15/how-to-enable-ip-forwarding-in-linux-2:

To check for current status of IP forwarding on IPv4 IP class
```
# cat /proc/sys/net/ipv4/ip_forward
```
If IP forwarding is disabled, a value of 0 would be displayed and if IP forwarding is enabled, linux should be displaying a numerical value of 1.

QUESTION 23
Which command will delete the environment variable FOOBAR?

A. unset FOOBAR
B. del $FOOBAR
C. export FOOBAR
D. export FOOBAR=

Correct Answer: A
Section: 105.1 Customize and use the shell environment
Explanation

Explanation/Reference:
From http://www.slackbook.org/html/shell-bash.html:
`$ unset VARIABLE`
unset will remove any variables that you give it, wiping out both the variable and its value; bash will forget that variable ever existed.

QUESTION 24
Your network email server's address has changed. Which DNS record do you have to edit?

A. MX
B. ML
C. MS
D. DN

Correct Answer: A
Section: 109.4 Configure client side DNS
Explanation

Explanation/Reference:
from http://en.wikipedia.org/wiki/MX_record:
A mail exchanger record (MX record) is a type of resource record in the Domain Name System that specifies a mail server responsible for accepting email messages.

QUESTION 25
You want to add an alias for an existing DNS record. What type of DNS record could you use?

A. CNAME
B. MX
C. SOA
D. NS

Correct Answer: A
Section: 109.4 Configure client side DNS
Explanation

Explanation/Reference:

QUESTION 26
Consider the following command and an abbreviated version of its output:

```
$ netstat -nr
Kernel IP routing table
Destination        Gateway           Genmask             Flags     Iface
192.168.165.0      0.0.0.0           255.255.255.0       U         eth0
127.0.0.0          0.0.0.0           255.0.0.0           U         lo
0.0.0.0            192.168.165.1     0.0.0.0             UG        eth0
```

What is the default Gateway?

A. 192.168.165.1
B. 255.0.0.0
C. 255.255.255.0
D. 0.0.0.0
E. 192.168.165.0

Correct Answer: A
Section: 109.1 Fundamentals of internet protocols
Explanation

Explanation/Reference:
From http://www.freebsd.org/doc/handbook/network-routing.html:
For one machine to be able to find another over a network, there must be a mechanism in place to describe how to get from one to the other. This is called routing. A “route” is a defined pair of addresses: a “destination” and a “gateway”. The pair indicates that if you are trying to get to this destination, communicate through this gateway. There are three types of destinations: individual hosts, subnets, and “default”. The “default route” is used if none of the other routes apply.

Consider this output of netstat

```
# netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
192.168.165.0   *               255.255.255.0   U         0 0          0 eth0
link-local      *               255.255.0.0     U         0 0          0 eth0
default         192.168.165.1   0.0.0.0         UG        0 0          0 eth0
```

When you call netstat without the -n option you can see that 0.0.0.0 becomes "default", indicating the default route, and thus the default gateway.

QUESTION 27
In the LPD system, a print queue is defined in what file?

A. /etc/lprconf
B. /etc/printer
C. /etc/printqueue
D. /etc/printcap

Correct Answer: D
Section: 108.4 Manage printers and printing
Explanation

Explanation/Reference:
A,B,C) files do not exist
D) print queue definition

QUESTION 28
Which of the following provides a non-graphical, text based interface for users who are visually impaired that can be used as a screen reader?

A. easyspeech
B. textconvert
C. xscreen
D. emacspeak

Correct Answer: D
Section: 106.3 Accessibility
Explanation

Explanation/Reference:
Emacspeak (code.google.com/p/emacspeak/) is a speech interface that allows visually impaired users to interact independently and efficiently with the computer. Emacspeak speech-enables local and remote information via a consistent and well-integrated user interface. Available free of cost, Emacspeak has dramatically changed how the author and hundreds of blind and visually impaired users around the world interact with the personal computer and the Internet by providing efficient speech-enabled access to the audio desktop. Emacspeak/Linux provides a reliable, stable speech-friendly solution that opens up the Internet to visually impaired users around the world.

EasySpeech is a development utility that helps you speech-enable Windows programs.

xscreen = ???
textconvert = ???

QUESTION 29
What can you do to recover a lost passphrase for a DSA or RSA authentication key?

A. Run the ssh-keygen Command
B. Run the ssh --recover command
C. A lost passphrase cannot be recovered
D. Decrypt the authentication key with gpg
E. Decrypt the authentication key with ssh --decrypt

Correct Answer: C
Section: 110.3 Securing data with encryption
Explanation

Explanation/Reference:
From the man pages (ssh-keygen):
There is no way to recover a lost passphrase. If the passphrase is lost or forgotten, a new key must be generated and copied to the corresponding public key to other machines.

QUESTION 30
Which command should be added to ~/.bash_profile to change the language of messages from an internationalised program to Portuguese (pt)?

(Select TWO correct answers)

A. export LANGUAGE="pt"
B. export MESSAGE="pt"
C. export LANG="pt"
D. export LC_MESSAGES="pt"
E. export ALL_MESSAGES="pt"

Correct Answer: CD
Section: 107.3 Localisation and internationalisation
Explanation

Explanation/Reference:
From the man pages:
LANG Used to determine the locale category for any category not specifically selected with a variable

starting with LC_.
LC_MESSAGES This variable determines the locale used to translate double-quoted strings preceded by a $.

A,B,E) are not valid internal bash variables.

QUESTION 31
You have a user whose account you want to disable but not remove.

What should you do?

A. Edit /etc/gshadow and just remove his name
B. Edit /etc/passwd and change all numbers to 0
C. Edit /etc/shadow and remove the last field
D. Edit /etc/passwd and insert an * after the first :
E. Edit /etc/group file and put a # sign in front of his name

Correct Answer: D
Section: 107.1 Manage user and group accounts and related system files
Explanation

Explanation/Reference:
A,C would remove parts of the user data,
B would do something strange
E would probably result in a syntax error, you would comment only whole lines
D) does not really disable the accout, but temporarily change the password, so the user is not able to log in.

So D would be the least wrong answer.

From the man pages:
The encrypted password field may be blank, in which case no password is required to authenticate as the specified login name. However, some applications which read the /etc/passwd file may decide not to permit any access at all if the password field is blank. If the password field is a lower-case “x”, then the encrypted password is actually stored in the shadow(5) file instead; there must be a corresponding line in the /etc/shadow file, or else the user account is invalid. If the password field is any other string, then it will be treated as an encrypted password, as specified by crypt(3).

QUESTION 32
What two files acting together make up the login environment for a user on a default installation of Linux?

A. /etc/profile
B. /etc/bashrc
C. /etc/.login
D. ~/.bash_profile
E. /etc/.profile

Correct Answer: AD
Section: 105.1 Customize and use the shell environment
Explanation

Explanation/Reference:
From the man pages:
When bash is invoked as an interactive login shell it first reads and executes commands from the file /etc/profile, if that file exists. After reading that file, it looks for ~/.bash_profile, ~/.bash_login, and ~/.profile, in that order, and reads and executes commands from the first one that exists and is readable.

QUESTION 33
Which of the following options will speed up traceroute for distant network queries?

A. -n
B. -p
C. -t
D. -O

Correct Answer: A
Section: 109.3 Basic network troubleshooting
Explanation

Explanation/Reference:
A) -n Do not try to map IP addresses to host names when displaying them.
B) -p port For UDP tracing, specifies the destination port base traceroute will use (the destination port number will be incremented by each probe). For ICMP tracing, specifies the initial icmp sequence value (incremented by each probe too). For TCP specifies just the (constant) destination port to connect.
C) -t tos For IPv4, set the Type of Service (TOS) and Precedence value. Useful values are 16 (low delay) and 8 (high throughput). Note that in order to use some TOS precendence values, you have to be super user. For IPv6, set the Traffic Control value.
D) -O option Specifies some method-specific option. Several options are separated by comma (or use several -O on cmdline). Each method may have its own specific options, or many not have them at all. To print information about available options, use -O help.

QUESTION 34
Which ports are used for FTP data and control?

(Choose Two)

A. 20
B. 21
C. 22
D. 23

Correct Answer: AB
Section: 109.1 Fundamentals of internet protocols
Explanation

Explanation/Reference:
From http://www.windowsnetworking.com/articles_tutorials/Understanding-FTP-Protocol.html:
FTP typically uses port 20 for data transfer and port 21 to listen to commands.

QUESTION 35
Your IP address is 170.35.13.28 and your netmask is 255.255.255.192. What host address is NOT part of your local subnet?

A. 170.35.13.33
B. 170.35.13.88
C. 170.35.13.62
D. 170.35.13.55

Correct Answer: B
Section: 109.1 Fundamentals of internet protocols
Explanation

Explanation/Reference:
netmask 255.255.255.192 = 11111111.11111111.11111111.11000000, which means /26 is the CIDR notation, which means that 170.35.13.1 is the first valid address in the local subnet, and 170.35.13.62 is the last (170.35.13.63 is Broadcast).

QUESTION 36
You have just set up the Gnome Display Manager as your default display manager. What file should you edit to change the default greeting for it?

A. /etc/X11/prefdm
B. /etc/X11/XF86Config
C. /etc/X11/gdm.conf
D. /etc/X11/gdm/Init/Default

Correct Answer: D
Section: 106.2 Setup a display manager
Explanation

Explanation/Reference:
see http://library.gnome.org/admin/gdm/stable/configuration.html.en and http://library.gnome.org/admin/gdm/stable/configuration.html.en#greetersection

QUESTION 37
Which command will verify the syntax of the hosts.allow and host.deny files?

A. tcpdchk
B. tcpdmatch
C. verify --tcp
D. ipswitch

Correct Answer: A
Section: 110.2 Setup host security
Explanation

Explanation/Reference:
From the man pages:
tcpdchk examines your tcp wrapper configuration and reports all potential and real problems it can find. The program examines the tcpd access control files (by default, these are /etc/hosts.allow and /etc/hosts.deny), and compares the entries in these files against entries in the inetd network configuration file.
tcpdchk reports problems such as non-existent pathnames; services that appear in tcpd access control rules, but are not controlled by tcpd; services that should not be wrapped; non-existent host names or non-internet address forms; occurrences of host aliases instead of official host names; hosts with a name/address conflict; inappropriate use of wildcard patterns; inappropriate use of NIS netgroups or references to non-existent NIS netgroups; references to non-existent options; invalid arguments to options; and so on.

QUESTION 38
Which commands will print two copies of the file to the default printer?

(Choose all that apply)

A. cat hosts | lpr -#2
B. lpr -K2 hosts
C. lpr -P -count 2 hosts
D. for 1 in 2 lpr hosts

Correct Answer: AB
Section: 108.4 Manage printers and printing
Explanation

Explanation/Reference:
From the man pages:
lpr - off line print
SYNOPSIS
lpr [-A] [-B] [-b,l] [-C class] [-D debugopt] [-F filterformat] [-G] [-h] [-i indentcols] [-k] [-J job] **[-K, # copies]**
[-m mailTo] [-o options] [-P printer] [-Q] [-r] [-R remoteAccount] [-s] [-T title] [-U user]
[-V] [-w width] [-X userfile] [-Y] [-Z options] [-1,2,3,4 font] [filename ...]

CAUTION: -K does not work on CUPS systems

QUESTION 39
You have generated a DSA authentication key on host linux1.

In order to log into host linux2 with the new key, what do you need to do?

A. Copy the new authentication key into /etc/ssh/sshd_config on linux2.
B. Copy the new authentication key into $HOME/.ssh/authorized_keys on linux2.
C. Copy the new authentication key into $HOME/.ssh/id_dsa on linux2.
D. Copy the new authentication key into $HOME/.ssh/id_dsa on linux1.
E. Log into linux2 using the command ssh --key.

Correct Answer: B
Section: 110.3 Securing data with encryption
Explanation

Explanation/Reference:
From the man pages:
~/.ssh/authorized_keys Lists the public keys (RSA/DSA) that can be used for logging in as this user. The format of this file is described above. The content of the file is not highly sensitive, but the recommended permissions are read/write for the user, and not accessible by others. If this file, the ~/.ssh directory, or the user's home directory are writable by other users, then the file could be modified or replaced by unauthorized users. In this case, sshd will not allow it to be used unless the StrictModes option has been set to “no”.

QUESTION 40
Which configuration file would you edit to change default options for outbound ssh sessions?

A. /etc/ssh/sshd_config
B. /etc/ssh/ssh
C. /etc/ssh/client
D. /etc/ssh/ssh_config
E. /etc/ssh/sshclient

Correct Answer: D
Section: 110.3 Securing data with encryption
Explanation

Explanation/Reference:
From the man pages:
ssh_config — OpenSSH SSH client configuration files
the Debian openssh-client package sets several options as standard in /etc/ssh/**ssh_config.**

Exam E

QUESTION 1
User Bob Swanson (bswanson) has left Company.com. His data has already been removed from his directory. How do you remove his account and directory?

A. rm -rf /home/bswanson
B. deluser /home/bswanson
C. userdel -r bswanson
D. rm -user bswanson

Correct Answer: C
Section: 107.1 Manage user and group accounts and related system files
Explanation

Explanation/Reference:
From the man pages:
userdel is a low level utility for removing users. On Debian, administrators should usually use deluser(8) instead.
-r, --remove Files in the users home directory will be removed along with the home directory itself and the users mail spool. Files located in other file systems will have to be searched for and deleted manually.

QUESTION 2
Which of the following represents a class C netmask?

A. 255.0.0.0
B. 255.255.0.0
C. 255.255.255.0
D. 255.255.255.255

Correct Answer: C
Section: 109.1 Fundamentals of internet protocols
Explanation

Explanation/Reference:
A) A class
B) B class
D) Broadcast ID

QUESTION 3
When you run the command newaliases, it will:

A. ask for input on stdin to create new mail aliases.
B. restart sendmail.
C. remove the aliases currently configured.
D. rebuild the aliases database for the file /etc/aliases.

Correct Answer: D
Section: 108.3 Mail Tranfer Agent (MTA) basics
Explanation

Explanation/Reference:
From the man pages:
newaliases rebuilds the random access data base for the mail aliases file /etc/aliases. It must be run each time this file is changed in order for the change to take effect.

QUESTION 4
The file /etc/ssh_known_hosts typically contains hosts keys for _____.

A. all hosts that have logged into this server via ssh
B. all hosts that users have logged into from this server via ssh
C. clients allowed to connect to this host via ssh
D. machines the system administrator trusts users to connect to using ssh

Correct Answer: D
Section: 110.3 Securing data with encryption
Explanation

Explanation/Reference:
From the man pages:
/etc/ssh/ssh_known_hosts Systemwide list of known host keys. This file should be prepared by the system administrator to contain the public host keys of all machines in the organization. It should be world-readable.

QUESTION 5
Your FTP server has been under attack, and the ISP of the attacker has been less than helpful in mitigating the attacks. So you decide that all connections from that ISP (badguy.example.org) to your FTP server will be denied and sent a message. Which line in your /etc/hosts.allow will have the desired effect?

A. in.ftpd : .badguy.example.org : twist echo "450 denied due to numerous attacks from this domain"
B. ftp : badguy.example.org : DENIED message "450 denied due to numerous attacks from this domain"
C. in.ftpd : badguy.example.org : spawn "echo 450 denied due to numerous attacks from this domain"
D. ftp : .badguy.example.org : DENIED due to numerous attacks from this domain

Correct Answer: A
Section: 110.2 Setup host security
Explanation

Explanation/Reference:
twist replaces the requested service with the specified command. It can be used to send messages to connecting clients. The twist command must occur at the end of the rule line.

In the following example, clients attempting to access FTP services from the example.com domain are sent a message via the echo command:
```
vsftpd : .example.com : twist /bin/echo "421 Bad hacker, go away!"
```

QUESTION 6
What command prints available functions?

A. declare -f
B. set
C. typeset
D. function()

Correct Answer: A
Section: 105.1 Customize and use the shell environment
Explanation

Explanation/Reference:
From the man pages:
declare [-aAfFilrtux] [-p] [name[=value] ...] Declare variables and/or give them attributes. If no names are

given then display the values of variables. The -f option will restrict the display to shell functions.

QUESTION 7
Which of the following configuration files should be modified to set default shell variables for all users?

A. /etc/bashrc
B. /etc/profile
C. ~default/.bash_profile
D. /etc/skel/.bashrc
E. /etc/skel/.bash_profile

Correct Answer: B
Section: 105.1 Customize and use the shell environment
Explanation

Explanation/Reference:
From the man pages:
When bash is invoked as an interactive login shell, or as a non-interactive shell with the --login option, it first reads and executes commands from the file /etc/profile, if that file exists. After reading that file, it looks for ~/.bash_profile, ~/.bash_login, and ~/.profile, in that order, and reads and executes commands from the first one that exists and is readable. The --noprofile option may be used when the shell is started to inhibit this behavior.

When a login shell exits, bash reads and executes commands from the file ~/.bash_logout, if it exists.

When an interactive shell that is not a login shell is started, bash reads and executes commands from /etc/bash.bashrc and ~/.bashrc, if these files exist. This may be inhibited by using the --norc option. The --rcfile file option will force bash to read and execute commands from file instead of /etc/bash.bashrc and ~/.bashrc.

QUESTION 8
What should the permission settings be for /etc/passwd and /etc/shadow?

A. /etc/passwd: -rw-r--r-- /etc/shadow: -r-------
B. /etc/passwd: -r------- /etc/shadow: -rw-r--r--
C. /etc/passwd: -rw-r-r- /etc/shadow: -rw-r--r--
D. /etc/passwd: -r------- /etc/shadow: -r-------

Correct Answer: A
Section: 110.2 Setup host security
Explanation

Explanation/Reference:
shadow is a file which contains the password information for the systems accounts and optional aging information. This file must not be readable by regular users if password security is to be maintained. The passwd file should be world-readable.

QUESTION 9
To prevent a specific user from scheduling tasks with at, what should the administrator do?

A. Add the specific user to /etc/at.allow file.
B. Add the specific user to [deny] section in the /etc/atd.conf file.
C. Add the specific user to /etc/at.deny file.
D. Add the specific user to nojobs group.
E. Run the following: atd -deny [user].

Correct Answer: C
Section: 107.2 Automate system administration tasks by scheduling jobs
Explanation

Explanation/Reference:
From the man pages:
The /etc/at.allow and /etc/at.deny files determine which user can submit commands for later execution via at (1) or batch(1).
If the file /etc/at.allow exists, only usernames mentioned in it are allowed to use at.
If /etc/at.allow does not exist, /etc/at.deny is checked.

QUESTION 10
The legacy program for listing files in the printer queues from the command line is:

A. lpd
B. lpr
C. lpstat
D. lpq

Correct Answer: D
Section: 108.4 Manage printers and printing
Explanation

Explanation/Reference:
From the man pages:
lpq shows the current print queue status on the named printer. Jobs queued on the default destination will be shown if no printer or class is specified on the command-line.

A) does not exist
B) sends a file (or stdin) to the printer
C) prints cups status information

QUESTION 11
The files /etc/hosts.allow, /etc/hosts.deny and /etc/nologin all exist on your computer and the sshd daemon is running. What will happen when users try to connect with ssh?

A. Only connections from computers specified in /etc/hosts.allow will be allowed to log in.
B. Only root will be allowed to log in.
C. All users not specified in /etc/hosts.deny will be allowed to log in.
D. No user will be allowed to log in.

Correct Answer: B
Section: 110.2 Setup host security
Explanation

Explanation/Reference:
From http://docstore.mik.ua/orelly/networking_2ndEd/ssh/ch05_06.htm#ch05-42-fm2xml:
If the file /etc/nologin exists, sshd allows only root to log in; no other accounts are allowed access. Thus, `touch /etc/nologin` is a quick way to restrict access to the system administrator only, without having to reconfigure or shut down SSH.

QUESTION 12
You want to change the aging information in the /etc/shadow file. What is the best utility to use to do this?

A. vi

B. emacs
C. usermod
D. modinfo
E. chage

Correct Answer: E
Section: 107.1 Manage user and group accounts and related system files
Explanation

Explanation/Reference:
From the man pages:
The chage command changes the number of days between password changes and the date of the last password change. This information is used by the system to determine when a user must change his/her password.

QUESTION 13
You've been reviewing your security checklist and one of the items calls for reviewing the /etc/passwd file. You cat the file and notice that, while most users have an x in the second column, a few have a 14 character string in the second column.

What action, if any, should you take?

A. No action. The users with an x have their accounts locked.
B. Run pwconv to convert the unix passwords to shadow passwords.
C. Use the passwd program to give the users with the hashed passwords new passwords.
D. Use the passwd program to give the users with the x new passwords.
E. No action. Linux knows how to handle the situation and allow user logins.

Correct Answer: B
Section: 107.1 Manage user and group accounts and related system files
Explanation

Explanation/Reference:
From the man pages:
The pwconv command creates shadow from passwd and an optionally existing shadow.

QUESTION 14
What is a well-known service that binds port 25 and is it required on all hosts?

A. SNMP and it should be turned off if not needed.
B. SMTP and it is a required service.
C. SMTP and it is only required on MX hosts.
D. SLPD and it is required if you run LDAP services.
E. SSHD and it is required for secure logins.

Correct Answer: C
Section: 109.2 Basic network configuration
Explanation

Explanation/Reference:
From /etc/services:

```
smtp        25/tcp        mail
```

smtp is needed only on mail exchange servers.

QUESTION 15
How many cron fields are there for specifying the time to execute a cron job?

A. 1
B. 3
C. 4
D. 5
E. 6

Correct Answer: D
Section: 107.2 Automate system administration tasks by scheduling jobs
Explanation

Explanation/Reference:
minute hour day month day/week

Example:
0 22 * * * /usr/local/bin/somecommand

QUESTION 16
What program do you use to suspend a printer queue?

A. lpr
B. lpq
C. lpc
D. lpd
E. lprm

Correct Answer: C
Section: 108.4 Manage printers and printing
Explanation

Explanation/Reference:
The lpc utility is provided to manage printer queues and requires root privilege to perform most of its functions. lpc reports on all print queues and their attending lpd daemons.

This does not work with CUPS. Use lpadmin in CUPS systems to configure printer queues.

QUESTION 17
What would the following command do?
```
$ cat hosts | lpr -#2
```

A. Print the file hosts on the default printer two times.
B. Categorize hosts and print the categorization as job #2.
C. Output the file hosts to the line printer and assign it to the second printer queue.
D. Print the hosts file to STDOUT and assign the current print job to printer tray number 2.

Correct Answer: A
Section: 108.4 Manage printers and printing
Explanation

Explanation/Reference:
From the man pages:
lpr - print files

-# copies Sets the number of copies to print from 1 to 100.

QUESTION 18
The hosts.lpd file provides:

A. A list of network printer IP addresses.
B. A list of printers available on the local network.
C. A list of computers that have printer (lpd) daemons running.
D. A list of hosts allowed to use printers on the local machine.
E. A list of hosts on the local network that are not allowed access to printers attached to the local machine.

Correct Answer: D
Section: 108.4 Manage printers and printing
Explanation

Explanation/Reference:
From http://www.regatta.cmc.msu.ru/doc/usr/share/man/info/ru_RU/a_doc_lib/files/aixfiles/hosts.lpd.htm:
The /etc/hosts.lpd file defines which remote systems are permitted to print on the local system.

QUESTION 19
What file is displayed BEFORE users log in to the machine locally?

A. /etc/issue
B. /etc/issue.net
C. /etc/motd
D. /etc/local.banner

Correct Answer: A
Section: 107.1 Manage user and group accounts and related system files
Explanation

Explanation/Reference:
From the man pages:
The file /etc/issue is a text file which contains a message or system identification to be printed before the login prompt. It may contain various @char and \char sequences, if supported by the getty-type program employed on the system.

B) is used to display messages for users who log in to the machine remotely.
C) The contents of /etc/motd are displayed by login(1) after a successful login but just before it executes the login shell.
D) does not exist

QUESTION 20
Which two files in a user's home directory are used to customize the bash environment?

A. bash and .bashrc
B. bashrc and bash_conf
C. bashrc and bashprofile
D. .bashrc and .bash_profile
E. bash.conf and .bash_profile

Correct Answer: D
Section: 105.1 Customize and use the shell environment
Explanation

Explanation/Reference:
From the man pages:
When bash is invoked as an interactive login shell, it first reads and executes commands from the file /etc/profile, if that file exists. After reading that file, it looks for **~/.bash_profile**, ~/.bash_login, and ~/.profile, in that order, and reads and executes commands from the first one that exists and is readable.

When an interactive shell that is not a login shell is started, bash reads and executes commands from /etc/bash.bashrc and **~/.bashrc**.

QUESTION 21
Which of the following files has the correct permissions?

A. -rw--w--w- 1 root root 369 Dec 22 22:38 /etc/shadow
B. -rwxrw-rw- 1 root root 369 Dec 22 22:38 /etc/shadow
C. -rw-r--r-- 1 root root 369 Dec 22 22:38 /etc/shadow
D. -rw------- 1 root root 369 Dec 22 22:38 /etc/shadow

Correct Answer: D
Section: 107.1 Manage user and group accounts and related system files
Explanation

Explanation/Reference:
From the man pages:
shadow is a file which contains the password information for the systems accounts and optional aging information. This file must not be readable by regular users if password security is to be maintained.

QUESTION 22
You are working in a graphical environment and trying to configure PPP, but you are having problems. You know that PPP uses the local2 facility for logging. To better watch what's going on, you decide to open an Xconsole session and send all local2 messages there. How should you configure /etc/syslog.conf to show you all messages sent from PPP?

A. local2.* /dev/console
B. local2.* /dev/xconsole
C. *.local2 /dev/xconsole
D. *.local2 *

Correct Answer: B
Section: 108.2 System logging
Explanation

Explanation/Reference:
Every rule consists of two fields, a selector field and an action field. These two fields are separated by one or more spaces or tabs. The selector field specifies a pattern of facilities and priorities belonging to the specified action. The selector field consists of two parts, a facility and a priority, separated by a period (``.'').

QUESTION 23
What command do you use to create an OpenSSH authentication key?

A. sshd
B. ssh-agent
C. ssh-keygen
D. ssh-add

Correct Answer: C
Section: 110.3 Securing data with encryption
Explanation

Explanation/Reference:
From the man pages:
ssh-keygen generates, manages and converts authentication keys for ssh(1). ssh-keygen can create RSA keys for use by SSH protocol version 1 and RSA or DSA keys for use by SSH protocol version 2. The type of key to be generated is specified with the -t option. If invoked without any arguments, ssh-keygen will generate an RSA key for use in SSH protocol 2 connections.

A) sshd (OpenSSH Daemon) is the daemon program for ssh(1). Together these programs replace rlogin(1) and rsh(1), and provide secure encrypted communications between two untrusted hosts over an insecure network. sshd listens for connections from clients. It is normally started at boot from /etc/init/ssh.conf. It forks a new daemon for each incoming connection. The forked daemons handle key exchange, encryption, authentication, command execution, and data exchange.
B) ssh-agent is a program to hold private keys used for public key authentication (RSA, DSA). The idea is that ssh-agent is started in the beginning of an X-session or a login session, and all other windows or programs are started as clients to the ssh-agent program.
D) ssh-add adds RSA or DSA identities to the authentication agent, ssh-agent(1). When run without arguments, it adds the files ~/.ssh/id_rsa, ~/.ssh/id_dsa and ~/.ssh/identity.

QUESTION 24
Which of the following will flush all print jobs on all configured queues of the system?

A. lprm -a all
B. lprm -all
C. lprm -a *
D. lpflush -all

Correct Answer: A
Section: 108.4 Manage printers and printing
Explanation

Explanation/Reference:
from the man pages:
lprm - remove jobs from the line printer spooling queue
SYNOPSIS
lprm [-a] [-A] [-Ddebugopt] [-Pprinter] [-V] [-Uuser] [jobid...] [all]
-a Remove files from all spool queues available to the user.

QUESTION 25
What is the purpose of the bash built-in export command

A. To allow disks to be mounted remotely
B. To run a command as a process in a sub-shell
C. To make the command history available to sub-shells
D. To setup environment variables for applications
E. To share NFS partitions for use by other systems on the network

Correct Answer: D
Section: 105.1 Customize and use the shell environment
Explanation

Explanation/Reference:
From the man pages:

export -p The supplied names are marked for automatic export to the environment of subsequently executed commands. If the -f option is given, the names refer to functions. If no names are given, or if the -p option is supplied, a list of all names that are exported in this shell is printed. The -n option causes the export property to be removed from each name. If a variable name is followed by =word, the value of the variable is set to word.

QUESTION 26
Your /etc/passwd file appears to have approximately half shadow passwords and half standard unix excrypted passwords. What utility would you most likely run to fix this?

A. pwconv
B. passconvert
C. useradd -conv
D. pwhash
E. passwd -fix

Correct Answer: A
Section: 107.1 Manage user and group accounts and related system files
Explanation

Explanation/Reference:
From the man pages:
The pwconv command creates shadow from passwd and an optionally existing shadow.

QUESTION 27
Where are the default settings for the useradd command kept?

A. /etc/default/useradd
B. /etc/.useradd
C. /etc/defauls/useradd
D. /etc/sysconfig/useradd.cfg

Correct Answer: A
Section: 107.1 Manage user and group accounts and related system files
Explanation

Explanation/Reference:
From the man pages:
useradd will use the base directory specified by the HOME variable in /etc/default/useradd, or /home by default.

QUESTION 28
You find you execute a series of commands on a recurring basis. You want this series of commands available from your login to run in the current shell. Choose the best solution:

A. create a shell program
B. create a function
C. use the up arrow in BASH to find the command
D. use BASH's built-in ! function to run the last iteration of the command by the same name

Correct Answer: B
Section: 105.1 Customize and use the shell environment
Explanation

Explanation/Reference:

A) you could create a shell script, but not really a shell program easily
C) you would need to do that for each of the series of commands
D) in bash "!" is the negation operator (! expression => True if expression is false).

QUESTION 29
Which of the following programs uses the hosts.allow file to perform its main task of checking for access control restrictions to system services?

A. tcpd
B. inetd
C. fingerd
D. mountd
E. xinetd

Correct Answer: A
Section: 109.2 Basic network configuration
Explanation

Explanation/Reference:
From the man pages:
The tcpd program can be set up to monitor incoming requests for telnet, finger, ftp, exec, rsh, rlogin, tftp, talk, comsat and other services that have a one-to-one mapping onto executable files. [..] There are two possible modes of operation: execution of tcpd before a service started by inetd, or linking a daemon with the libwrap shared library as documented in the hosts_access(3) manual page. Operation when started by inetd is as follows: whenever a request for service arrives, the inetd daemon is tricked into running the tcpd program instead of the desired server. tcpd logs the request and does some additional checks. When all is well, tcpd runs the appropriate server program and goes away.

QUESTION 30
Which of the following services would least be likely to be governed over by the Internet Super Server?

A. ftp
B. telnet
C. ssh
D. finger

Correct Answer: C
Section: 109.2 Basic network configuration
Explanation

Explanation/Reference:
One of the reasons why one wouldn't start sshd through inetd is because it needs to generate the server key everytime it starts through inetd.
On the other hand *finger* can not be started as standalone daemon, like some implementations of *ftp* and *telnet* (but not all).

QUESTION 31
You are running an email server configured with the default settings. In which directory will you find the delivered mail for the user foo?

A. /var/spool/mail
B. /home/foo/mail
C. /var/mail/spool
D. /var/users/mail

Correct Answer: A
Section: 108.3 Mail Tranfer Agent (MTA) basics
Explanation

Explanation/Reference:
Defined in the FHS. see http://www.pathname.com/fhs/pub/fhs-2.3.html#VARMAILUSERMAILBOXFILES

In newer distributions /var/spool/mail is a link to /var/mail. This directory contains all delivered (but unread) mails for each user.

QUESTION 32
Which directory in a user's home contains configuration files and key rings for GPG?

A. ~/gpg.d/
B. ~/.gpg/
C. ~/.gnupg/
D. ~/gnupg/
E. ~/.gpg.d/

Correct Answer: C
Section: 110.3 Securing data with encryption
Explanation

Explanation/Reference:
From the man pages:
The GnuPG home directory [is] "~/.gnupg" if --homedir or $GNUPGHOME is not used

QUESTION 33
What command would be used to check the gpgp signature on a downloaded source file?

(Provide the name of the command only)

Correct Answer: gpg
Section: 110.3 Securing data with encryption
Explanation

Explanation/Reference:
From the man pages:
gpg --verify pgpfile
gpg --verify sigfile

Verify the signature of the file but do not output the data. The second form is used for detached signatures, where sigfile is the detached signature (either ASCII armored or binary) and are the signed data; if this is not given, the name of the file holding the signed data is constructed by cutting off the extension (".asc" or ". sig") of sigfile or by asking the user for the filename.

QUESTION 34
In the LPD system, a print queue is defined in what file?

A. /etc/lprconf
B. /etc/printer
C. /etc/printqueue
D. /etc/printcap

Correct Answer: D
Section: 108.4 Manage printers and printing

Explanation

Explanation/Reference:
A,B,C) files do not exist
D) print queue definition

QUESTION 35
Which of the following services is NOT usually protected via TCP wrappers?

A. ftp
B. finger
C. auth
D. http

Correct Answer: D
Section: 109.2 Basic network configuration
Explanation

Explanation/Reference:
From the man pages:
tcpd - access control facility for internet services
The tcpd program can be set up to monitor incoming requests for telnet, finger, ftp, exec, rsh, rlogin, tftp, talk, comsat and other services that have a one-to-one mapping onto executable files.
auth is an older protocol similiar to finger.

QUESTION 36
Your server was rebooted. Users have complained that the server refuses secured connections. What is the mostly likely cause?

A. The public keys have been corrupted on the server.
B. The clients are not resolving the server name properly.
C. sshd is not configured to start in the default runlevel.
D. The users need to ssh-keygen.

Correct Answer: C
Section: 110.1 Perform security administration tasks
Explanation

Explanation/Reference:
Check if sshd is running
Upstart: check the file /etc/init/ssh.conf and contains these 2 lines:
```
start on filesystem
stop on runlevel S
```
SystemV: check if the file /etc/rc?.d/S??ssh exists for your default runlevel.

QUESTION 37
A cronjob must run at least every 11 minutes. The job may take up to 7 minutes to complete, and there mustn't be two jobs at the same time. Which crontab line solves the problem?

A. */8 * * * * myjob
B. */9 * * * * myjob
C. */10 * * * * myjob
D. */11 * * * * myjob
E. */12 * * * * myjob

Correct Answer: C
Section: 107.2 Automate system administration tasks by scheduling jobs
Explanation

Explanation/Reference:
A) 0,8,16, ... 48,56,0,8 ... there are only 4 minutes between 56 and 0
B) 0,9,18,... 45,54,0,9 ... there are only 6 minutes between 54 and 0
D) 11,22, ... 44,55,0 ... there are only 5 minutes between 55 and 0
E) 12 is already too much

QUESTION 38
To see the current time set by a NTP clock, you use the command:

A. ntpd -clock
B. ndtime
C. hwdate
D. ntpdate

Correct Answer: D
Section: 108.1 Maintain system time
Explanation

Explanation/Reference:
From the man pages:
ntpdate - set the date and time via NTP
-q Query only - don't set the clock.

QUESTION 39
The file /etc/ssh/ssh_host_key should be:

A. world-readable
B. readable to group sys
C. readable to root only
D. readable by all SSH users

Correct Answer: C
Section: 110.2 Setup host security
Explanation

Explanation/Reference:
From the man pages:
the host key files are normally not readable by anyone but root. The default is /etc/ssh/ssh_host_key for protocol version 1, and /etc/ssh/ssh_host_rsa_key and /etc/ssh/ssh_host_dsa_key for protocol version 2.

QUESTION 40
You've decided to convert from standard shadow passwords to MD5 passwords. You make the appropriate changes to the /etc/pam.d/ files. What do you do next?

A. Nothing, the passwords will be changed as users login and out.
B. Nothing, users will be automatically prompted to change their passwords at the next login.
C. You need to manually change all the passwords using the passwd program.
D. Delete and recreate all the users.
E. Change the /etc/pam.d files back because shadow passwords and MD5 passwords are incompatible.

Correct Answer: C

Section: 107.1 Manage user and group accounts and related system files
Explanation

Explanation/Reference:
The reasoning behind password hashing is that NO ONE can calculate the password from the hash, that means that if you change the hash algorithm from, say, MD5 to SHA512 every user has to manually reset her password.

Exam F

QUESTION 1
Your machine has two working NICs with proper addresses. You want to split your network into two new subnets. What single command will accomplish this?

A. ifconfig
B. route
C. netstat
D. None of the choices

Correct Answer: A
Section: 109.2 Basic network configuration
Explanation

Explanation/Reference:
Since the question does not specify that the subnets have to talk to each other, you can skip ip forwarding and routing. That leaves configuring the interfaces using ifconfig.

QUESTION 2
Which of the following lines would you find in the file /etc/hosts?

A. order hosts, bind
B. 192.168.168.4 dns-server
C. hosts: files,dns
D. domain mycompany.com

Correct Answer: B
Section: 109.2 Basic network configuration
Explanation

Explanation/Reference:
This file is a simple text file that associates IP addresses with hostnames, one line per IP address. For each host a single line should be present with the following information: IP_address canonical_hostname [aliases...]

A) /etc/host.conf
C) /etc/nsswitch.conf
D) /etc/resolv.conf

QUESTION 3
In which sendmail configuration file are the domains listed that the machine is responsible for serving?

(Specify **only the filename**, without the path.)

Correct Answer: local-host-names
Section: 108.3 Mail Tranfer Agent (MTA) basics
Explanation

Explanation/Reference:
From http://www.faqs.org/docs/securing/chap22sec180.html:
The /etc/mail/local-host-names file is read to obtain alternative names for the local host. One use for such a file might be to declare a list of hosts in your network for which the local host is acting as the MX recipient.

QUESTION 4
The normal filesystem location for the LPD queue directory is:

Correct Answer: /var/spool/lpd
Section: 108.4 Manage printers and printing
Explanation

Explanation/Reference:
From http://www.pathname.com/fhs/pub/fhs-2.3.html#VARSPOOLAPPLICATIONSPOOLDATA:

/var/spool/lpd : Line-printer daemon print queues (optional)
The lock file for lpd, lpd.lock, must be placed in /var/spool/lpd. It is suggested that the lock file for each printer be placed in the spool directory for that specific printer and named lock.

QUESTION 5
The very first line of a shell script should always contain what two characters at the beginning of the line?

Correct Answer: #!
Section: 105.2 Customize or write simple scripts
Explanation

Explanation/Reference:
From http://en.wikipedia.org/wiki/Shebang_%28Unix%29:
In computing, a shebang (also called a hashbang, ...) refers to the characters "#!" when they are the first two characters in an interpreter directive as the first line of a text file. In a Unix-like operating system, the program loader takes the presence of these two characters as an indication that the file is a script, and tries to execute that script using the interpreter specified by the rest of the first line in the file.

QUESTION 6
You want to temporarily prevent users from logging in. Please complete the following command:

```
touch /etc/________
```

Correct Answer: nologin
Section: 110.2 Setup host security
Explanation

Explanation/Reference:
If the file /etc/nologin exists, login(1) will allow access only to root. Other users will be shown the contents of this file and their logins will be refused.

QUESTION 7
For security reasons, the system administrator is setting up a log server.

What file does the system administrator have to edit in order to have each machine send log entries to the new log server?

Correct Answer: /etc/syslog.conf
Section: 108.2 System logging
Explanation

Explanation/Reference:
From the man pages:
The syslog.conf file is the main configuration file for syslogd(8) which logs system messages on *nix systems. This file specifies rules for logging.

QUESTION 8
Which command prints or adjusts the current limits on resources available to the shell and to processes started by it, such as the maximum size of a core file or the maximum number of processes running?

(Enter only the command, without path or options)

Correct Answer: ulimit
Section: 105.1 Customize and use the shell environment
Explanation

Explanation/Reference:
From the man pages:
ulimit [-HSTabcdefilmnpqrstuvx [limit]]
Provides control over the resources available to the shell and to processes started by it, on systems that allow such control. The -H and -S options specify that the hard or soft limit is set for the given resource. A hard limit cannot be increased by a non-root user once it is set; a soft limit may be increased up to the value of the hard limit. If neither -H nor -S is specified, both the soft and hard limits are set. The value of limit can be a number in the unit specified for the resource or one of the special values hard, soft, or unlimited, which stand for the current hard limit, the current soft limit, and no limit, respectively. If limit is omitted, the current value of the soft limit of the resource is printed, unless the -H option is given. When more than one resource is specified, the limit name and unit are printed before the value.

QUESTION 9
You wish to notify all users that you have to take down a service on which they rely. What command will allow you to send a message to all currently logged on users?

(Enter only the command, without path or options)

Correct Answer: wall
Section: 107.1 Manage user and group accounts and related system files
Explanation

Explanation/Reference:
From the man pages:
Wall displays the contents of file or, by default, its standard input, on the terminals of all currently logged in users. Only the super-user can write on the terminals of users who have chosen to deny messages or are using a program which automatically denies messages. Reading from a file is refused when the invoker is not superuser and the program is suid or sgid.

QUESTION 10
The _____ command is used to modify or set the password expiration for a user.

(Enter only the command, without path or options)

Correct Answer: chage
Section: 107.1 Manage user and group accounts and related system files
Explanation

Explanation/Reference:
From the man pages:
The chage command changes the number of days between password changes and the date of the last password change. This information is used by the system to determine when a user must change his/her password.

QUESTION 11
To exclude all log messages of a given logging facility, you should use a logging priority of:

Correct Answer: none
Section: 108.2 System logging
Explanation

Explanation/Reference:
From the man pages:

An asterisk (``*'') stands for all facilities or all priorities, depending on where it is used (before or after the period). The keyword **none** stands for no priority of the given facility.

QUESTION 12
You just installed a new system, but before you create any new users you want to ensure they have a subdirectory bin/ in their home directory. To ensure this directory is automatically created each time you add a new user, in what subdirectory should you create the directory?

Correct Answer: /etc/skel
Section: 107.1 Manage user and group accounts and related system files
Explanation

Explanation/Reference:
From the man pages:
The skeleton directory is defined by the SKEL variable in /etc/default/useradd or, by default, /etc/skel.

QUESTION 13
The _____ file controls the system logging daemon.

Correct Answer: /etc/syslog.conf
Section: 108.2 System logging
Explanation

Explanation/Reference:
From the man pages:
The syslog.conf file is the main configuration file for syslogd(8) which logs system messages on *nix systems. This file specifies rules for logging.

QUESTION 14
You want to display a list of all last logged in users. The file /var/log/wtmp exists. Which command would you use?

(Enter only the command, without path or options)

Correct Answer: last
Section: 107.1 Manage user and group accounts and related system files
Explanation

Explanation/Reference:
From the man pages:
last searches back through the file /var/log/wtmp (or the file designated by the -f flag) and displays a list of all users logged in (and out) since that file was created. Names of users and tty's can be given, in which case last will show only those entries matching the arguments. Names of ttys can be abbreviated, thus `last 0` is the same as `last tty0`.

QUESTION 15
When adding a new user to the system using standard Linux commands, which directory contains the initial files copied to the new user's home directory?

Correct Answer: /etc/skel
Section: 107.1 Manage user and group accounts and related system files
Explanation

Explanation/Reference:
From the man pages:
The skeleton directory is defined by the SKEL variable in /etc/default/useradd or, by default, /etc/skel.

QUESTION 16

A user cannot access the cron scheduling system. What file needs to be modified to provide that access?

(Specify full path and filename)

Correct Answer: /etc/cron.allow
Section: 107.2 Automate system administration tasks by scheduling jobs
Explanation

Explanation/Reference:
From the man pages:
If the /etc/cron.allow file exists, then you must be listed therein in order to be allowed to use this command. If the /etc/cron.allow file does not exist but the /etc/cron.deny file does exist, then you must not be listed in the /etc/cron.deny file in order to use this command.

QUESTION 17
You are working an evening shift and want to look at which jobs are pending for the at command. What command would you use?

(Enter only the command, without path or options)

Correct Answer: atq
Section: 107.2 Automate system administration tasks by scheduling jobs
Explanation

Explanation/Reference:
From the man pages:
atq lists the user's pending jobs, unless the user is the superuser; in that case, everybody's jobs are listed. The format of the output lines (one for each job) is: Job number, date, hour, queue, and username.

QUESTION 18
The _____ command is used to print out the current date and time on the system.

Correct Answer: date
Section: 105.2 Customize or write simple scripts
Explanation

Explanation/Reference:
From the man pages:
date - print or set the system date and time

QUESTION 19
You want to change the file that contains the message which is used at the login prompt when users log in locally.

(Please enter the file including the path)

Correct Answer: /etc/issue
Section: 107.1 Manage user and group accounts and related system files
Explanation

Explanation/Reference:
From the man pages:
The file /etc/issue is a text file which contains a message or system identification to be printed before the login prompt.

QUESTION 20
How to invoke restricted mode in Bash?

(command only without path)

Correct Answer: bash -r -or- rbash
Section: 105.1 Customize and use the shell environment
Explanation

Explanation/Reference:
If bash is started with the name rbash, or the -r option is supplied at invocation, the shell becomes restricted. A restricted shell is used to set up an environment more controlled than the standard shell. It behaves identically to bash with the exception that the following are disallowed or not performed:

- changing directories with cd
- setting or unsetting the values of SHELL, PATH, ENV, or BASH_ENV
- specifying command names containing /
- specifying a file name containing a / as an argument to the . builtin command
- Specifying a filename containing a slash as an argument to the -p option to the hash builtin command
- importing function definitions from the shell environment at startup
- parsing the value of SHELLOPTS from the shell environment at startup
- redirecting output using the >, >|, <>, >&, &>, and >> redirection operators
- using the exec builtin command to replace the shell with another command
- adding or deleting builtin commands with the -f and -d options to the enable builtin command
- Using the enable builtin command to enable disabled shell builtins
- specifying the -p option to the command builtin command
- turning off restricted mode with set +r or set +o restricted.

These restrictions are enforced after any startup files are read. When a command that is found to be a shell script is executed (see COMMAND EXECUTION above), rbash turns off any restrictions in the shell spawned to execute the script.

QUESTION 21
In /etc/nsswitch.conf, which directive specifies which databases to search for host name lookups?

Correct Answer: hosts
Section: 109.4 Configure client side DNS
Explanation

Explanation/Reference:
hosts defines where namelookup commands like `hostname`, will look for the information. The line in /etc/nsswitch.conf typically reads
`hosts: files dns`
which would indicate that first /etc/hosts would be searched for the hostname, and only then would a DNS-Server be contacted.

QUESTION 22
Which command can allow you to run a process in a modified environment without changing the environment of the current shell?

Correct Answer: env
Section: 105.2 Customize or write simple scripts
Explanation

Explanation/Reference:
From the man pages:
env - run a program in a modified environment

QUESTION 23
For xinetd service definition, which config option will disable the service?

Correct Answer: disable
Section: 110.2 Setup host security
Explanation

Explanation/Reference:
From the man pages:
xinetd.conf is the configuration file that determines the services provided by xinetd.
disable this is boolean "yes" or "no". This will result in the service being disabled and not starting.

Example:
```
service myorg_server
{
  disable=no
  type=INTERNAL
  socket_type=stream
  protocol=tcp
  wait=no
  user=root
  server=/usr/etc/my_server_exec
}
```

QUESTION 24
Which IP protocol is connectionless and unreliable?

Correct Answer: udp -or- UDP
Section: 109.1 Fundamentals of internet protocols
Explanation

Explanation/Reference:
From http://en.wikipedia.org/wiki/User_Datagram_Protocol:
UDP uses a simple transmission model **without** implicit hand-shaking dialogues for providing reliability, ordering, or data integrity. Thus, UDP provides an unreliable service and datagrams may arrive out of order, appear duplicated, or go missing without notice. UDP assumes that error checking and correction is either not necessary or performed in the application, avoiding the overhead of such processing at the network interface level.

QUESTION 25
The _____ command is used to add a group to the system.

(Enter only the command, without path or options)

Correct Answer: groupadd
Section: 107.1 Manage user and group accounts and related system files
Explanation

Explanation/Reference:
From the man pages:
The groupadd command creates a new group account using the values specified on the command line plus the default values from the system. The new group will be entered into the system files as needed.

QUESTION 26
The system's timezone may be set by linking /etc/localtime to an appropriate file in which directory?

(Provide the **full path** to the directory, **without any country information**)

Correct Answer: /usr/share/zoneinfo
Section: 107.3 Localisation and internationalisation
Explanation

Explanation/Reference:
see http://www.pathname.com/fhs/pub/fhs-2.3.html#USRSHAREARCHITECTUREINDEPENDENTDATA

QUESTION 27
Which file specifies the user accounts can NOT submit jobs via at or batch?

(Provide the full path and filename)

Correct Answer: /etc/at.deny
Section: 107.2 Automate system administration tasks by scheduling jobs
Explanation

Explanation/Reference:
The /etc/at.allow and /etc/at.deny files determine which user can submit commands for later execution via at(1) or batch(1). The format of the files is a list of usernames, one on each line. The superuser may always use at. If the file /etc/at.allow exists, only usernames mentioned in it are allowed to use at. If /etc/at.allow does not exist, /etc/at.deny is checked.

QUESTION 28
After configuring printing on a Linux server, the administrator sends a test file to one of the printers and it fails to print. What command can be used to print the status of the printer's queue?

(Provide only the command, without any options or parameters)

Correct Answer: lpq
Section: 108.4 Manage printers and printing
Explanation

Explanation/Reference:
From the man pages:
lpq shows the current print queue status on the named printer. Jobs queued on the default destination will be shown if no printer or class is specified on the command-line.

QUESTION 29
Which file lists which users can execute commands using sudo?

(Provide the full path and filename)

Correct Answer: /etc/sudoers
Section: 107.1 Manage user and group accounts and related system files
Explanation

Explanation/Reference:
From the man pages:
The sudoers file is composed of two types of entries: aliases (basically variables) and user specifications (which specify who may run what). When multiple entries match for a user, they are applied in order. Where there are multiple matches, the last match is used (which is not necessarily the most specific match).

QUESTION 30
An administrator wants to determine the geometry of a particular window in X, so she issues the _____ -metric command and then clicks on the window.

Correct Answer: xwininfo
Section: 106.1 Install and configure X11
Explanation

Explanation/Reference:

From the man pages:
xwininfo is a utility for displaying information about windows. Various information is displayed depending on which options are selected. If no options are chosen, -stats is assumed. The user has the option of selecting the target window with the mouse (by clicking any mouse button in the desired window) or by specifying its window id on the command line with the -id option. Or instead of specifying the window by its id number, the -name option may be used to specify which window is desired by name. There is also a special -root option to quickly obtain information on the screen's root window.

QUESTION 31
What word is missing from the following SQL statement?

update tablename _____ fieldname='value' where id=909;

Correct Answer: set
Section: 105.3 SQL data management
Explanation

Explanation/Reference:
see http://www.sqlite.org/syntaxdiagrams.html#update-stmt

QUESTION 32
By default, which directories contents will be copied to a new user's home directory when the account is created, passing the -m option to the useradd command?

Correct Answer: /etc/skel
Section: 107.1 Manage user and group accounts and related system files
Explanation

Explanation/Reference:
From the man pages:
The skeleton directory, which contains files and directories to be copied in the users home directory, when the home directory is created by useradd. The skeleton directory is defined by the SKEL variable in /etc/default/useradd or, by default, /etc/skel.

QUESTION 33
What word will complete an if statement in bash such as the following:

```
if [-x "$file"]; then
echo $file
_____
```

(Please provide the missing word only)

Correct Answer: fi
Section: 105.2 Customize or write simple scripts
Explanation

Explanation/Reference:
From the man pages:
if list; then list; [elif list; then list;] ... [else list;] fi

The if list is executed. If its exit status is zero, the then list is executed. Otherwise, each elif list is executed in turn, and if its exit status is zero, the corresponding then list is executed and the command completes. Otherwise, the else list is executed, if present. The exit status is the exit status of the last command executed, or zero if no condition tested true.

QUESTION 34
What is the command to delete the default gateway from the system IP routing table?

(Please specify the complete command with arguments)

Correct Answer: route del default
Section: 109.2 Basic network configuration
Explanation

Explanation/Reference:
From the man pages:
route - show / manipulate the IP routing table
Synopsis
route [-v] [-A family] **del** [-net|-host] **target** [gw Gw] [netmask Nm] [metric N] [[dev] If]

QUESTION 35
Given the following line from /etc/nsswitch.conf:
`hosts: files mdns4_minimal [NOTFOUND=return] dns mdns4`
By default, which file will be queried first for hostname lookups ?

(Provide the full path and filename)

Correct Answer: /etc/hosts
Section: 109.4 Configure client side DNS
Explanation

Explanation/Reference:
Database "hosts" defines the lookup sequence for DNS related services, and the entries are done in order of "files", "mdns4_minimal", "dns", "mdns4". "files" specifies the local DNS resolver file, which is /etc/hosts.

QUESTION 36
In an xinetd config file, which attribute specifies the network address that will be used to offer the service?

Correct Answer: bind
Section: 110.2 Setup host security
Explanation

Explanation/Reference:
From the man pages:
bind Allows a service to be bound to a specific interface on the machine. This means you can have a telnet server listening on a local, secured interface, and not on the external interface. Or one port on one interface can do something, while the same port on a different interface can do something completely different.
Syntax: bind = (ip address of interface).

QUESTION 37
The _____ command is used to assign an IP address to a device

(Please specify the command without path information)

Correct Answer: ifconfig
Section: 109.2 Basic network configuration
Explanation

Explanation/Reference:
From the man pages:
Ifconfig is used to configure the kernel-resident network interfaces. It is used at boot time to set up interfaces as necessary. After that, it is usually only needed when debugging or when system tuning is needed. **If no arguments are given, ifconfig displays the status of the currently active interfaces.** If a single interface argument is given, it displays the status of the given interface only; if a single -a argument is given, it displays the status of all interfaces, even those that are down. Otherwise, it configures an interface.

QUESTION 38
The _____ command is used to print the network connections, routing tables, and interface statistics.

Correct Answer: netstat
Section: 109.3 Basic network troubleshooting
Explanation

Explanation/Reference:
Netstat prints information about the Linux networking subsystem. The type of information printed is controlled by the first argument, as follows:

(none) By default, netstat displays a list of open sockets. If you don't specify any address families, then the active sockets of all configured address families will be printed.
--route , -r Display the kernel routing tables. See the description in route(8) for details. netstat -r and route -e produce the same output.
--groups , -g Display multicast group membership information for IPv4 and IPv6.
--interfaces, -i Display a table of all network interfaces.
--masquerade , -M Display a list of masqueraded connections.
--statistics , -s Display summary statistics for each protocol.

QUESTION 39
What command can be used to generate log entries of any facility and priority?

(supply just the command name without a path)

Correct Answer: logger
Section: 108.2 System logging
Explanation

Explanation/Reference:
From the man pages:
Logger makes entries in the system log. It provides a shell command interface to the syslog(3) system log module.

CAUTION: In most cases anyone can log to any facility, so we rely on convention for the correct facility to be chosen. However, generally only the kernel can log to the "kern" facility. This is because the implementation of openlog() and syslog() in glibc does not allow logging to the "kern" facility. Klogd circumvents this restriction when logging to syslogd by reimplementing those functions itself.

QUESTION 40
What word is missing from the following SQL statement?

select count(*) _____ tablename;

Correct Answer: from
Section: 105.3 SQL data management
Explanation

Explanation/Reference:
See http://www.sqlite.org/syntaxdiagrams.html#select-core

Exam G

QUESTION 1
You need to sync your hardware clock, which is on GMT, with your system clock, which you just updated with NTP.

To do this, complete the following command: _____ -u --systohc

Correct Answer: hwclock
Section: 108.1 Maintain system time
Explanation

Explanation/Reference:
From the man pages:
hwclock is a tool for accessing the Hardware Clock. You can display the current time, set the Hardware Clock to a specified time, set the Hardware Clock to the System Time, and set the System Time from the Hardware Clock.
You can also run hwclock periodically to insert or remove time from the Hardware Clock to compensate for systematic drift (where the clock consistently gains or loses time at a certain rate if left to run).
-w, --systohc Set the Hardware Clock to the current System Time.
-s, --hctosys Set the System Time from the Hardware Clock.
-u, --utc
--localtime Indicates that the Hardware Clock is kept in Coordinated Universal Time or local time, respectively. It is your choice whether to keep your clock in UTC or local time, but nothing in the clock tells which you've chosen. So this option is how you give that information to hwclock.

QUESTION 2
For the `last` command to work, what file must exist?

Correct Answer: /var/log/wtmp
Section: 105.1 Customize and use the shell environment
Explanation

Explanation/Reference:
From the man pages:
last searches back through the file /var/log/wtmp (or the file designated by the -f flag) and displays a list of all users logged in (and out) since that file was created.

QUESTION 3
You are logged in as root. How to check user brown's group?

Correct Answer: groups brown
Section: 107.1 Manage user and group accounts and related system files
Explanation

Explanation/Reference:
Print group memberships for each USERNAME or, if no USERNAME is specified, for the current process (which may differ if the groups database has changed).

QUESTION 4
You can run the _____ command to see active network and UNIX domain socket connection.

Correct Answer: netstat
Section: 109.3 Basic network troubleshooting
Explanation

Explanation/Reference:
From the man pages:

Netstat prints information about the Linux networking subsystem.
OUTPUT
Active Internet connections (TCP, UDP, raw)
Active UNIX domain Sockets (unix)

QUESTION 5
The _____ command is used to send ICMP ECHO_REQUEST packets to other hosts over the network

Correct Answer: ping
Section: 109.1 Fundamentals of internet protocols
Explanation

Explanation/Reference:
From the man pages:
ping uses the ICMP protocol's mandatory ECHO_REQUEST datagram to elicit an ICMP ECHO_RESPONSE from a host or gateway. ECHO_REQUEST datagrams (``pings'') have an IP and ICMP header, followed by a struct timeval and then an arbitrary number of ``pad'' bytes used to fill out the packet.

QUESTION 6
Which file contains a list of services and hosts that will be denied by a TCP Wrapper such as tcpd?

Correct Answer: /etc/hosts.deny
Section: 110.2 Setup host security
Explanation

Explanation/Reference:
From the man pages:
The access control software consults two files. The search stops at the first match:
· Access will be granted when a (daemon,client) pair matches an entry in the /etc/hosts.allow file.
· Otherwise, access will be denied when a (daemon,client) pair matches an entry in the /etc/hosts.deny file.
· Otherwise, access will be granted.
A non-existing access control file is treated as if it were an empty file. Thus, access control can be turned off by providing no access control files.

QUESTION 7
The _____ command prints a list of email that is currently in the queue waiting for delivery.

Correct Answer: mailq
Section: 108.3 Mail Tranfer Agent (MTA) basics
Explanation

Explanation/Reference:
From the man pages:
mailq List the mail queue. Each entry shows the queue file ID, message size, arrival time, sender, and the recipients that still need to be delivered. If mail could not be delivered upon the last attempt, the reason for failure is shown. The queue ID string is followed by an optional status character:
* The message is in the active queue, i.e. the message is selected for delivery.
! The message is in the hold queue, i.e. no further delivery attempt will be made until the mail is taken off hold.
This mode of operation is implemented by executing the postqueue(1) command.

This is identical to `sendmail -bp`.

QUESTION 8
What is the name of the file whose global read bit would control the ability of normal users to get useful information from the who and w commands?

(Provide full name and path)

Correct Answer: /var/run/utmp
Section: 107.1 Manage user and group accounts and related system files
Explanation

Explanation/Reference:
From the man pages:
The utmp file allows one to discover information about who is currently using the system. There may be more users currently using the system, because not all programs use utmp logging.

QUESTION 9
You need an additional email address for a user in your department. You decide to add just an alias on your sendmail email server. What command must be executed to make the changes take effect?

Correct Answer: newaliases
Section: 108.3 Mail Tranfer Agent (MTA) basics
Explanation

Explanation/Reference:
From the man pages:
newaliases Initialize the alias database. If no input file is specified, the program processes the file(s) specified with the alias_database configuration parameter. If no alias database type is specified, the program uses the type specified with the default_database_type configuration parameter. This mode of operation is implemented by running the postalias(1) command.

QUESTION 10
The _____ file maps TCP and UDP ports to common resources.

Correct Answer: /etc/services
Section: 109.2 Basic network configuration
Explanation

Explanation/Reference:
From the man pages:
/etc/services is a plain ASCII file providing a mapping between human-friendly textual names for internet services, and their underlying assigned port numbers and protocol types. Every networking program should look into this file to get the port number (and protocol) for its service. The C library routines getservent(3), getservbyname(3), getservbyport(3), setservent(3), and endservent(3) support querying this file from programs.

QUESTION 11
Your ISP has given you an IP block for your use. The block is 192.168.112.64/26.

If your network administrator uses the first usable IP for the router he's installed on your network, how many usable IPs do you have left?

Correct Answer: 61
Section: 109.1 Fundamentals of internet protocols
Explanation

Explanation/Reference:
CIDR notation /26 means you have 6 bits left as Host-IDs (32-26=6). The maximum number consisting of 6 Bits is 63 (00111111b) giving you 64 Hosts (including 0). You have to remove 2 IPs for Net-ID and Broadcast-ID and 1 for the Router. 64 - 3 = 61.

QUESTION 12
You decide to use xinetd instead of inetd. Now, you need to transfer information from /etc/inetd.conf to

another file. What file?

Correct Answer: /etc/xinetd.conf
Section: 110.2 Setup host security
Explanation

Explanation/Reference:
From the man pages:
/etc/xinetd.conf - Extended Internet Services Daemon configuration file

QUESTION 13
Where do you change the GNOME display greeting?

(Provide filename and full path)

Correct Answer: /etc/gdm/custom.conf
Section: 106.2 Setup a display manager
Explanation

Explanation/Reference:
From http://www.cyberciti.biz/tips/howto-unix-linux-change-gnome-login-banner.html:

You can use the following options in the [greeter] section:

```
DefaultWelcome=false
Welcome=Message for local users
RemoteWelcome=Message for remote login users
```

QUESTION 14
To slave your NTP daemon to an external source, you need to modify the _____ variable (alt: value or record) in your /etc/ntp.conf file.

Correct Answer: server
Section: 108.1 Maintain system time
Explanation

Explanation/Reference:
From the man pages:
server For type s and r addresses (only), this command normally mobilizes a persistent client mode association with the specified remote server or local reference clock. In client mode the client clock can synchronize to the remote server or local reference clock, but the remote server can never be synchronized to the client clock.

QUESTION 15
What command will display the mail servers for `lpi.org`?

(Provide command with parameters)

Correct Answer: dig lpi.org MX -or- dig lpi.org mx
Section: 109.4 Configure client side DNS
Explanation

Explanation/Reference:
From the man pages:
A typical invocation of dig looks like:
dig @server name type
where:
server is the name or IP address of the name server to query. This can be an IPv4 address in dotted-decimal notation or an IPv6 address in colon-delimited notation. When the supplied server argument is a

hostname, dig resolves that name before querying that name server. If no server argument is provided, dig consults /etc/resolv.conf and queries the name servers listed there. The reply from the name server that responds is displayed.
name is the name of the resource record that is to be looked up.
type indicates what type of query is required — ANY, A, MX, SIG, etc. type can be any valid query type. If no type argument is supplied, dig will perform a lookup for an A record.

The same result would be achieved with `nslookup -type=MX lpi.org`

QUESTION 16
What is the command to check the syntax of /etc/inetd.conf?

(Provide only the command)

Correct Answer: tcpdchk
Section: 109.3 Basic network troubleshooting
Explanation

Explanation/Reference:
From the man pages:
tcpdchk examines your tcp wrapper configuration and reports all potential and real problems it can find. The program examines the tcpd access control files (by default, these are /etc/hosts.allow and /etc/hosts.deny), and compares the entries in these files against entries in the inetd network configuration file. tcpdchk reports problems such as non-existent pathnames; services that appear in tcpd access control rules, but are not controlled by tcpd; services that should not be wrapped; non-existent host names or non-internet address forms; occurrences of host aliases instead of official host names; hosts with a name/address conflict; inappropriate use of wildcard patterns; inappropriate use of NIS netgroups or references to non-existent NIS netgroups; references to non-existent options; invalid arguments to options; and so on.

QUESTION 17
You want to connect to a secure webserver on https://localhost. What Port do you need to listen to?

Correct Answer: 443
Section: 109.1 Fundamentals of internet protocols
Explanation

Explanation/Reference:
From /etc/services:
https 443/tcp # http protocol over TLS/SSL
https 443/udp

QUESTION 18
The _____ file is the configuration file for ntpd

Correct Answer: /etc/ntp.conf
Section: 108.1 Maintain system time
Explanation

Explanation/Reference:
Ordinarily, ntpd reads the ntp.conf configuration file at startup time in order to determine the synchronization sources and operating modes. It is also possible to specify a working, although limited, configuration entirely on the command line, obviating the need for a configuration file. This may be particularly useful when the local host is to be configured as a broadcast/multicast client, with all peers being determined by listening to broadcasts at run time.
Usually, the configuration file is installed in the /etc directory, but could be installed elsewhere (see the -c conffile command line option). The file format is similar to other Unix configuration files - comments begin with a # character and extend to the end of the line; blank lines are ignored.

QUESTION 19
In your DNS configuration, MX records are used to point to the _____ server(s) for your domain.

(Please specify a single word answer)

Correct Answer: email -or- mail
Section: 109.4 Configure client side DNS
Explanation

Explanation/Reference:
See http://en.wikipedia.org/wiki/List_of_DNS_record_types

QUESTION 20
Within a script you create a loop. Following the variable list, the statements to be looped are found between the keywords ____ and done.

Correct Answer: do
Section: 105.2 Customize or write simple scripts
Explanation

Explanation/Reference:
From the man pages:
for ((expr1 ; expr2 ; expr3)) ; do list ; done
select name [in word] ; do list ; done
while list; do list; done

QUESTION 21
To prevent users from seeing who is logged in with the who command, you must remove the world readable bit from the file /var/run/____.

Correct Answer: utmp
Section: 107.1 Manage user and group accounts and related system files
Explanation

Explanation/Reference:
The utmp file allows one to discover information about who is currently using the system. There may be more users currently using the system, because not all programs use utmp logging.

QUESTION 22
The user "matt" has forgotten his password and you wish to reset it. Type in the command to change his password (you are currently logged in as root):

Correct Answer: passwd matt
Section: 107.1 Manage user and group accounts and related system files
Explanation

Explanation/Reference:
From the man pages:
NAME passwd - change user password
SYNOPSIS passwd [options] [LOGIN]

QUESTION 23
In the /etc/resolv.conf file are entries that describe where DNS queries can resolve names to IP addresses. Given a DNS server with an IP of 192.168.33.254, type the exact enry that should appear in this file:

Correct Answer: nameserver 192.168.33.254
Section: 109.4 Configure client side DNS

Explanation

Explanation/Reference:
From the man pages:
nameserver Name server IP address
Internet address (in dot notation) of a name server that the resolver should query. Up to MAXNS (currently 3, see <resolv.h>) name servers may be listed, one per keyword. If there are multiple servers, the resolver library queries them in the order listed. If no nameserver entries are present, the default is to use the name server on the local machine. (The algorithm used is to try a name server, and if the query times out, try the next, until out of name servers, then repeat trying all the name servers until a maximum number of retries are made.)

QUESTION 24
What file do you query for hostname resolution outside of the local system?

Correct Answer: /etc/resolv.conf
Section: 109.4 Configure client side DNS
Explanation

Explanation/Reference:
From the man pages:
The resolver is a set of routines in the C library that provide access to the Internet Domain Name System (DNS). The resolver configuration file contains information that is read by the resolver routines the first time they are invoked by a process. The file is designed to be human readable and contains a list of keywords with values that provide various types of resolver information.

QUESTION 25
What network configuration file defines the search order for name resolution?

Correct Answer: /etc/nsswitch.conf
Section: 109.2 Basic network configuration
Explanation

Explanation/Reference:
From the man pages:
nsswitch.conf - System Databases and Name Service Switch configuration file

QUESTION 26
Delivered mail for local users is stored in what directory?

Correct Answer: /var/spool/mail
Section: 108.3 Mail Tranfer Agent (MTA) basics
Explanation

Explanation/Reference:
see http://www.pathname.com/fhs/pub/fhs-2.3.html#VARSPOOLAPPLICATIONSPOOLDATA

actually the mail directory was changed to /var/mail in the FHS.

QUESTION 27
In what directory does undelivered remote mail get stored in?

Correct Answer: /var/spool/mqueue
Section: 108.3 Mail Tranfer Agent (MTA) basics
Explanation

Explanation/Reference:
http://www.pathname.com/fhs/pub/fhs-2.3.html#VARSPOOLAPPLICATIONSPOOLDATA

mqueue Outgoing mail queue (optional)

QUESTION 28
You wish to restart the network daemon on a Redhat server. Type in the command and any arguments to accomplish that.

Correct Answer: service network restart
Section: 109.3 Basic network troubleshooting
Explanation

Explanation/Reference:
See http://whatislinux.net/linux/how-to-restart-radhat/debian/ubuntu-linux-network-service

QUESTION 29
Type the command to change your Ethernet interface eth0 to the IP 10.4.4.100 with a class C subnet mask.

Correct Answer: ifconfig eth0 10.4.4.100 netmask 255.255.255.0
Section: 109.2 Basic network configuration
Explanation

Explanation/Reference:
From the man pages:
ifconfig - configure a network interface
SYNOPSIS
ifconfig [-v] [-a] [-s] [interface]
ifconfig [-v] interface [aftype] options | address ...

`ifconfig eth0 10.4.4.100 netmask 255.255.255.0` is equal to `ifconfig eth0 10.4.4.100/24`

QUESTION 30
You want to make sure all Bash users, when they login, get access to a new program in /opt/bin (not currently in their PATH). To ensure this you would put the command
`PATH=$PATH:/opt/bin; export PATH`
in what file?

Correct Answer: /etc/profile
Section: 105.1 Customize and use the shell environment
Explanation

Explanation/Reference:
From the man pages:
When bash is invoked as an interactive login shell it first reads and executes commands from the file **/etc/profile**, if that file exists. After reading that file, it looks for ~/.bash_profile, ~/.bash_login, and ~/.profile, in that order, and reads and executes commands from the first one that exists and is readable.

QUESTION 31
Please specify the directory containing the configuration files for the CUPS printing system.

(Provide the full path to the directory)

Correct Answer: /etc/cups
Section: 108.4 Manage printers and printing
Explanation

Explanation/Reference:
From the man pages:
The cupsd.conf file configures the CUPS scheduler, cupsd(8). It is normally located in the /etc/cups directory.

QUESTION 32
To allow IPs from network 111.222.55.0 and 111.222.56.0 networks in TCP wrappers, what network and netmask pair can be used in /etc/hosts.allow?

Correct Answer: 111.222.55.0/255.255.240.0
Section: 109.2 Basic network configuration
Explanation

Explanation/Reference:
111.222.55.0 = **01101111.11011110.0011**0111.00000000
111.222.56.0 = **01101111.11011110.0011**1000.00000000
The common part of both networks is /20 which translates to 255.255.240.0

If you use a more restrictive netmask (like /21, /22, ...) you won't be able to get both nets with one network and netmask pair.

From the man pages:
An expression of the form `n.n.n.n/m.m.m.m´ is interpreted as a `net/mask´ pair. An IPv4 host address is matched if `net´ is equal to the bitwise AND of the address and the `mask´. For example, the net/mask pattern `131.155.72.0/255.255.254.0´ matches every address in the range `131.155.72.0´ through `131.155.73.255´. `255.255.255.255´ is not a valid mask value, so a single host can be matched just by its IP.

QUESTION 33
You wish to execute the ls command, but it appears to be aliased. What is the easiest way to execute the original ls?

Correct Answer: \ls
Section: 105.1 Customize and use the shell environment
Explanation

Explanation/Reference:
see http://en.wikipedia.org/wiki/Alias_%28command%29#Overriding_aliases

In Unix shells, if an alias exists for a command, it is possible to override the alias by surrounding the command with quotes or prefixing it with a backslash. For example, consider the following alias definition:
```
alias ls='ls -la'
```
To override this alias and execute the ls command as it was originally defined, the following syntax can be used:
```
'ls'
```
or
```
\ls
```

QUESTION 34
Which option, when passed to the gpg command, will enter an interactive menu enabling the user to perform key management related tasks?

(Provide only the option)

Correct Answer: --edit-key
Section: 110.3 Securing data with encryption
Explanation

Explanation/Reference:
From the man pages:
--edit-key Present a menu which enables you to do most of the key management related tasks. It expects the specification of a key on the command line.

QUESTION 35
In the config file for xinetd, you can specify the interface to offer service by the attribute:

Correct Answer: bind
Section: 110.2 Setup host security
Explanation

Explanation/Reference:
From the man pages:
bind Allows a service to be bound to a specific interface on the machine. This means you can have a telnet server listening on a local, secured interface, and not on the external interface. Or one port on one interface can do something, while the same port on a different interface can do something completely different.

QUESTION 36
With the find command, which argument to the -name flag will match files or directories beginning with a '.' (period) ?

Correct Answer: [.]*
Section: 105.2 Customize or write simple scripts
Explanation

Explanation/Reference:
From the man pages:
-name pattern
Base of file name (the path with the leading directories removed) matches shell pattern pattern. The metacharacters (`*', `?', and `[]') match a `.' at the start of the base name (this is a change in findutils-4.2.2; see section STANDARDS CONFORMANCE below). To ignore a directory and the files under it, use -prune; see an example in the description of -path. Braces are not recognised as being special, despite the fact that some shells including Bash imbue braces with a special meaning in shell patterns. The filename matching is performed with the use of the fnmatch(3) library function.

This will not work in the unlikely event that a file exists that is actually named "[.]<anything>". So it is always better to enclose the search pattern in quotation marks to prevent the shell from expanding the pattern: `find -name '.*'`

QUESTION 37
You need to prohibit users to use Ctrl+Alt+Del to reboot the system. Complete the following line in /etc/inittab

ca:12345:_____:/bin/echo "Reboot not allowed"

Correct Answer: ctrlaltdel
Section: (none)
Explanation

Explanation/Reference:
`/etc/inittab` consists of many lines with the following format:
`id:runlevel:action:process`

`id` is just an unique identifier, with no higher meaning
`runlevel` defines for what runlevels the line is valid (empty means **all** runlevels)
`action` is one of the following: `boot bootwait boot ctrlaltdel initdefault once ondemand powerfail sysinit boot bootwait respawn wait`

Example:

```
ca:12345:ctrlaltdel:/sbin/shutdown -r -t 4 now
```

QUESTION 38
What file is displayed BEFORE users log in to the machine locally?

A. /etc/issue
B. /etc/issue.net
C. /etc/motd
D. /etc/local.banner

Correct Answer: A
Section: 107.1 Manage user and group accounts and related system files
Explanation

Explanation/Reference:
From the man pages:
The file /etc/issue is a text file which contains a message or system identification to be printed before the login prompt. It may contain various @char and \char sequences, if supported by the getty-type program employed on the system.

B) is used to display messages for users who log in to the machine remotely.
C) The contents of /etc/motd are displayed by login(1) after a successful login but just before it executes the login shell.
D) does not exist

QUESTION 39
In order to bypass print filters using lpr, which of following switches should be used:

A. lpr -o nofilter
B. lpr -l
C. lpr -o raw
D. lpr -r

Correct Answer: B
Section: 108.4 Manage printers and printing
Explanation

Explanation/Reference:
From the man pages
-l Specifies that the print file is already formatted for the destination and should be sent without filtering. This option is equivalent to "-o raw".
???

QUESTION 40
Which THREE statements about crontab are true?

A. Every user may have their own crontab.
B. Changing a crontab requires a reload/restart of the cron deamon.
C. The cron daemon reloads crontab files automatically when necessary.
D. hourly is the same as "0 * * * *".
E. A cron daemon must run for each existing crontab.

Correct Answer: ACD
Section: 107.2 Automate system administration tasks by scheduling jobs
Explanation

Explanation/Reference:
From the man pages:
Additionally, cron checks each minute to see if its spool directory's modtime (or the modtime on /etc/crontab) has changed, and if it has, cron will then examine the modtime on all crontabs and reload those which have changed. Thus cron need not be restarted whenever a crontab file is modified. Note that the crontab(1) command updates the modtime of the spool directory whenever it changes a crontab.

QUESTION 41
What does the following command accomplish:
```
$ export PATH=$PATH:$APPLICATIONS
```

A. Changes path to the applications directory.
B. Updates the path with the value of $APPLICATIONS.
C. All NFS users can mount the applications directly.
D. Updates path with the applications directory.

Correct Answer: B
Section: 105.1 Customize and use the shell environment
Explanation

Explanation/Reference:
????
There is no such thing as an "application directory"

QUESTION 42
You want a secure and fast DNS server that must also be quickly accessible remotely. You should:

A. Reject all udp packets.
B. Reject all icmp packets.
C. Reject all icmp untrusted-host packets.
D. Disable inetd, run ssh and named as standalone daemons.
E. Use tcpwrappers to only allow connections to ports 22 and 53.

Correct Answer: DE
Section: 109.4 Configure client side DNS
Explanation

Explanation/Reference:
If you want a dedicated DNS server, that must be accessible remotely, you should run named and sshd as standalone services, and not with the inetd (or xinetd).
??? tcpwrappers can not block connections to specific ports ???

QUESTION 43
Which statements are true regarding the following syslog.conf configuration directive?

```
*.err;kern.notice;auth.notice /dev/console
```

(Select THREE correct answers)

A. Severity crit messages from all facilities will be directed to /dev/console
B. Severity notice messages from the auth facility will be directed to /dev/console
C. Severity notice messages from the kern facility will be directed to /dev/console
D. Severity err messages from the mail facility will be directed /dev/console
E. Severity notice messages from all facilities will be directed to /dev/console

Correct Answer: BCD
Section: 108.2 System logging
Explanation

Explanation/Reference:
A) would be correct ???

From the man pages:
The priority is one of the following keywords, in ascending order: debug, info, notice, warning, warn (same as warning), err, error (same as err), crit, alert, emerg, panic (same as emerg). The keywords warn, error and panic are deprecated and should not be used anymore. The priority defines the severity of the message.
The behavior of the original BSD syslogd is that all messages of the **specified priority and higher** are logged according to the given action.
---
if the directive is `*.err;kern.=notice;auth.=notice /dev/`console BCD are the correct answers.

QUESTION 44
To increase system security, it is often desirable to run daemons for system services with nonroot user ids. Which one of the following services can be run as a non-root user?

A. inetd
B. named
C. rlogind
D. crond
E. telnetd

Correct Answer: B
Section: 110.2 Setup host security
Explanation

Explanation/Reference:
A) inetd is the Internet Super Server, that starts applications that may need root privileges
C)
D) crond has to start the contabs of many different users (including root), so it is impossible for crond to be run at user level.
E)

QUESTION 45
What are the first two bytes of a MD5 hash called?

A. salt
B. magic
C. magic bytes
D. encrypted bytes

Correct Answer: A
Section: 107.1 Manage user and group accounts and related system files
Explanation

Explanation/Reference:
See http://www.insidepro.com/eng/passwordspro.shtml#200
The MD5 hash begins with the $1 **signature**, followed by the salt ($ and up to 8 characters), followed by a $ and the actual hash.
The **DES** hash begins with a 2 Byte salt, followed by the actual hash.

QUESTION 46
Which of the following are valid commands to affect your systems printing

A. lpq
B. lprm
C. lpstatus
D. lpr
E. lpio

Correct Answer: ABD
Section: 108.4 Manage printers and printing
Explanation

Explanation/Reference:
lpq has no effect on printing, but is used to get job ids for the lprm (and other) command.
C) lpstatus does not exist
E) lpio does not exist