LPI 117-102

LPI 102 General Linux, Part 2

Q&A with explanations

Version 26.0

Leading The Way
in IT Testing And Certification Tools

www.testking.com

Important Note, Please Read Carefully

Other TestKing products
A) Offline Testing engine
Use the offline Testing engine product topractice the questions in an exam environment.
B) Study Guide (not available for all exams)
Build a foundation of knowledge which will be useful also after passing the exam.

Latest Version
We are constantly reviewing our products. New material is added and old material is revised. Free updates are available for 90 days after the purchase. You should check your member zone at TestKing and update 3-4 days before the scheduled exam date.

Here is the procedure to get the latest version:

1.Go towww.testking.com
2.Click on **Member zone/Log in**
3.The latest versions of all purchased products are downloadable from here. Just click the links.
For mostupdates,itisenough just to print the new questions at the end of the new version, not the whole document.

Feedback
If you spot a possible improvement then please let us know. We always interested in improving product quality.
Feedback should be send to feedback@testking.com. You should include the following: Exam number, version, page number, question number, and your login ID.

Our experts will answer your mail promptly.

Copyright
Each iPAD file contains a unique serial number associated with your particular name and contact information for security purposes. So if we find out that a particular iPAD file is being distributed by you, TestKing reserves the right to take legal action against you according to the International Copyright Laws.

Table of contents

Total number of questions: 488

Topic 1, (105) Kernel (80 Questions)

Section 1, (1.105.1) Manage/Query kernel and kernel modules at runtime (44 Questions)

* Description: Candidates should be able to manage and/or query a kernel and kernel loadable modules. This objective includes using command-line utilities to get information about the currently running kernel and kernel modules. It also includes manually loading and unloading modules as appropriate. It also includes being able to determine when modules can be unloaded and what parameters a module accepts. Candidates should be able to configure the system to load modules by names other than their file name.

***Key files, terms, and utilities** include:

/lib/modules/kernel-version/modules.dep

`/etc/modules.conf & /etc/conf.modules`

depmod

insmod

lsmod

rmmod

modinfo

modprobe

uname

QUESTION NO: 1
What command would load the module msdos.o and all its dependancies?

A. modinfo -a msdos
B. lsmod -a msdos
C. modprobe msdos
D. insmod -d msdos

Answer: C
Explanation: modprobe command is used to load or unload the modules as well as it's dependencies from the kernel.
To Load the module:
modprobe modulename

To unload the module
modprobe -r modulename

QUESTION NO: 2
What command will unload a kernel module?

A. rmmod
B. unmod
C. delmod
D. modprobe
E. unloadmod

Answer: A
Explanation: rmmod is the simple program, which remove the modules from the kernel.
To unload module from kernel.

rmmod modulename
or
modprobe modulename

QUESTION NO: 3 CORRECT TEXT
The _____ command will list the currently loaded kernel modules.

Answer: lsmod
Explanation: lsmod command displays all modules loaded by kernel as well as modules status on current session.
See the sample output of lsmod command
Module Size Used by
i915 81349 2
md5 4033 1
ipv6 232705 10
parport_pc 24705 1
lp 12077 0
parport 37129 2 parport_pc,lp
autofs4 23237 0
sunrpc 157093 1
dm_mod 54741 2

button 6481 0
battery 8901 0
ac 4805 0
raid1 19905 1
uhci_hcd 31065 0
ehci_hcd 30917 0
snd_intel8x0 33769 0
snd_ac97_codec 63889 1 snd_intel8x0
snd_pcm_oss 49017 0
snd_mixer_oss 17985 1 snd_pcm_oss
snd_pcm 96841 2 snd_intel8x0,snd_pcm_oss
snd_timer 29893 1 snd_pcm
snd_page_alloc 9673 2 snd_intel8x0,snd_pcm
snd_mpu401_uart 8769 1 snd_intel8x0
snd_rawmidi 26597 1 snd_mpu401_uart
snd_seq_device 8137 1 snd_rawmidi
snd 54949 9
snd_intel8x0,snd_ac97_codec,snd_pcm_oss,snd_mixer_oss,snd_pcm,snd_timer,snd_mpu401_uart,snd_

soundcore 9889 1 snd
8139too 25921 0
mii 4673 1 8139too
floppy 58481 0
ext3 116809 6
jbd 71257 1 ext3

QUESTION NO: 4CORRECT TEXT
You wish to remove a module from the kernel called fat. Assume this module has no dependancies.
Type in the simplest command to do this:

Answer: rmmod fat
Explanation: rmmod command removes the module from the kernel. If there are other dependencies modules then rmmod command can't remove the module.
To remove the fat module from the kernel.

rmmod fat

QUESTION NO: 5
You have just added new modules to your system. What command would you execute to rebuild the modules.dep file?

A. depmod --rebuild
B. update-dependancies
C. depmod -a
D. insmod -dependancies

Answer: C
Explanation:
depmod creates a list of module dependencies, by reading each module under /lib/modules/version and determining what symbols it exports, and what symbols it needs. By default this list is written to modules.dep in the same directory.

QUESTION NO: 6
Which of the following correctly describe the relationship between depmod and modprobe?

A. depmod creates a dependency file for use by modprobe
B. modprobe creates a dependency file for use by depmod
C. they have no relationship
D. they can replace each other

Answer: A
Explanation:
depmod creates a list of module dependencies, by reading each module under /lib/modules/version and determining what symbols it exports, and what symbols it needs. By default this list is written to modules.dep in the same directory.

modprobe command is used to load or unload the modules as well as it's dependencies from the kernel.
To Load the module:
modprobe modulename

To unload the module
modprobe -r modulename

QUESTION NO: 7
The normal use of depmod is to include which of the following lines in one of the files in /etc/rc.d so the correct module dependencies will be available after booting the system?

A. /sbin/depmod -a
B. /sbin/depmod -p
C. /sbin/depmod -r
D. /sbin/depmod -c

Answer: A
Explanation:
depmod creates a list of module dependencies, by reading each module under /lib/modules/version and determining what symbols it exports, and what symbols it needs. By default this list is written to modules.dep in the same directory. The normal use of depmod is to include the line /sbin/depmod -a in one of the files in /etc/rc.d so the correct module dependencies will be available after booting the system.

QUESTION NO: 8
What command option of depmod allows you to print a list of all unresolved symbols?

A. -e
B. -l
C. -i
D. -a

Answer: A
Explanation: depmod creates a list of module dependencies, by reading each module under /lib/modules/version and determining what symbols it exports, and what symbols it needs. By default this list is written to modules.dep in the same directory. The normal use of depmod is to include the line /sbin/depmod -a in one of the files in /etc/rc.d so the correct module dependencies will be available after booting the system. depmod -e prints a list of all unresolved symbols.

QUESTION NO: 9

Which of the following commands loads the module file into the kernel and changes any symbols that are defined on the command line?

A. insmod
B. depmod
C. modprobe
D. setmod

Answer: A
Explanation: insmod is a system administration command. Load the module file into the kernel, changing any symbols that are defined on the command line. If the module file is named file.o or file.mod, the module will be named file.

QUESTION NO: 10
What option of the insmod command can you use to force the loading of module even if problems are encountered?

A. -f
B. -F
C. -u
D. -r

Answer: A
Explanation: insmod is a system administration command. -f: Force loading of module, even if some problems are encountered.

QUESTION NO: 11
Which of the following commands installs a loadable module in the running kernel?

A. insmod
B. depmod
C. modprobe
D. setmod

Answer: A
Explanation: insmod installs a loadable module in the running kernel. It tries to link a module into the running kernel by resolving all symbols from the kernel's exported symbol table.

QUESTION NO: 12
insmod tries to link a module into the running kernel by resolving all symbols obtained from:

A. the kernel's exported symbol table.
B. the kernel's internal pointer base.
C. the user command argument list.
D. None of the choices

Answer: A
Explanation: insmod installs a loadable module in the running kernel. It tries to link a module into the running kernel by resolving all symbols from the kernel's exported symbol table.

QUESTION NO: 13
With insmod, the paths listed in /etc/modules.conf override the paths defined in MODPATH.

A. true
B. false

Answer: A
Explanation: If the module file name is given without directories or extension, insmod will search for the module in some common default directories. The environment variable MODPATH can be used to override this default. If a module configuration file such as /etc/modules.conf or /etc/modprobe.conf exists, it will override the paths defined in MODPATH.

QUESTION NO: 14

lsmod shows information about:

A. all loaded modules
B. all updatable modules
C. all non-updatable modules
D. all unloaded modules

Answer: A
Explanation: lsmod shows information about all loaded modules as well as the status of loaded modules. The format is name, size, use count, list of referring modules. The information displayed is identical to that available from /proc/modules.

QUESTION NO: 15
lsmod shows information in which of the following formats?

A. name, size, use count, list of referring modules
B. name, use count, list of referring modules, size
C. name, size, list of referring modules, use count
D. None of the choices

Answer: A
Explanation: lsmod shows information about all loaded modules. The format is name, size, use count, list of referring modules. The information displayed is identical to that available from /proc/modules.
See the sample output
Module Size Used by
i915 81349 2
md5 4033 1
ipv6 232705 10
parport_pc 24705 1
lp 12077 0
parport 37129 2 parport_pc,lp
autofs4 23237 0
sunrpc 157093 1
dm_mod 54741 2
button 6481 0
battery 8901 0

ac 4805 0
raid1 19905 1
uhci_hcd 31065 0
ehci_hcd 30917 0
snd_intel8x0 33769 0
snd_ac97_codec 63889 1 snd_intel8x0
snd_pcm_oss 49017 0
snd_mixer_oss 17985 1 snd_pcm_oss
snd_pcm 96841 2 snd_intel8x0,snd_pcm_oss
snd_timer 29893 1 snd_pcm
snd_page_alloc 9673 2 snd_intel8x0,snd_pcm
snd_mpu401_uart 8769 1 snd_intel8x0
snd_rawmidi 26597 1 snd_mpu401_uart
snd_seq_device 8137 1 snd_rawmidi
snd 54949 9
snd_intel8x0,snd_ac97_codec,snd_pcm_oss,snd_mixer_oss,snd_pcm,snd_timer,snd_mpu401_uart,snd_rawm

soundcore 9889 1 snd
8139too 25921 0
mii 4673 1 8139too
floppy 58481 0
ext3 116809 6
jbd 71257 1 ext3

QUESTION NO: 16
The information displayed by lsmod is identical to that available from:

A. /proc/modules
B. /proc/depmod
C. /proc/ls
D. /proc/lsmod

Answer: A
Explanation: lsmod shows information about all loaded modules. The format is name, size, use count, list of referring modules. The information displayed is identical to that available from /proc/modules.

cat /proc/modules
Module Size Used by
i915 81349 2

md5 4033 1
ipv6 232705 10
parport_pc 24705 1
lp 12077 0
parport 37129 2 parport_pc,lp
autofs4 23237 0
sunrpc 157093 1
dm_mod 54741 2
button 6481 0
battery 8901 0
ac 4805 0
raid1 19905 1
uhci_hcd 31065 0
ehci_hcd 30917 0
snd_intel8x0 33769 0
snd_ac97_codec 63889 1 snd_intel8x0
snd_pcm_oss 49017 0
snd_mixer_oss 17985 1 snd_pcm_oss
snd_pcm 96841 2 snd_intel8x0,snd_pcm_oss
snd_timer 29893 1 snd_pcm
snd_page_alloc 9673 2 snd_intel8x0,snd_pcm
snd_mpu401_uart 8769 1 snd_intel8x0
snd_rawmidi 26597 1 snd_mpu401_uart
snd_seq_device 8137 1 snd_rawmidi
snd 54949 9
snd_intel8x0,snd_ac97_codec,snd_pcm_oss,snd_mixer_oss,snd_pcm,snd_timer,snd_mpu401_uart,snd_rawm

soundcore 9889 1 snd
8139too 25921 0
mii 4673 1 8139too
floppy 58481 0
ext3 116809 6
jbd 71257 1 ext3

QUESTION NO: 17
What command should you use to unload loadable modules from the running kernel?

A. rmmod
B. remove -mod

C. delmod
D. unload module

Answer: A
Explanation: rmmod unloads loadable modules from the running kernel. Rmmod tries to unload a set of modules from the kernel, with the restriction that they are not in use and that they are not referred to by other modules. If more than one module is named on the command line, the modules will be removed simultansously. This supports unloading of stacked modules.

QUESTION NO: 18
What command option of rmmod specifies that all outputs be sent to syslog?

A. -a
B. -i
C. -s
D. -d

Answer: C
Explanation: rmmod unloads loadable modules from the running kernel. -s: Output everything to syslog instead of the terminal.
Syntax:
Rmmod -s or --syslog modulename
Where -s or --syslog à Send errors to the syslog, instead of standard error.

QUESTION NO: 19
What utility examines the object file module_file associated with a kernel module and displays any information that it can glean?

A. modinfo
B. modprobe
C. insmod
D. depmod

Answer: A

Explanation: modinfo extracts information the Linux Kernel modules given on the command line. If the module name is not a filename, then the /lib/modules/version directory is searched, as done by modprobe

Syntax: modinfo modulename or filename
Example:
modinfo ext3
Sample output
filename: /lib/modules/2.6.9-5.EL/kernel/fs/ext3/ext3.ko
author: Remy Card, Stephen Tweedie, Andrew Morton, Andreas Dilger, Theodore Ts'o and others
description: Second Extended Filesystem with journaling extensions
license: GPL
vermagic: 2.6.9-5.EL 686 REGPARM 4KSTACKS gcc-3.4
depends: jbd

QUESTION NO: 20
What command option of modinfo can display its version number?

A. -V
B. -i
C. -I
D. -A

Answer: A
Explanation: -V option is used to display the version number of modules.
Example:
modinfo -V ext3
output like
module-init-tools version 3.1-pre5

QUESTION NO: 21
What option of modprobe specifies the loading of all matching modules instead of stopping after the first successful loading?

A. -a
B. -f
C. -c
D. -e

Answer: A
Explanation: -a, --all: Load all matching modules instead of stopping after the first successful loading.

QUESTION NO: 22
What option of modprobe allows you to set 'autoclean' on the loaded modules?

A. -k
B. -d
C. -c
D. -e

Answer: A
Explanation: -k, --autoclean: Set 'autoclean' on loaded modules. Used by the kernel when it calls on modprobe to satisfy a missing feature (supplied as a module). The -q option is implied by -k. These options will automatically be sent to insmod.

QUESTION NO: 23
modprobe can be used to load (choose all that apply):

A. a single module
B. a stack of dependent modules
C. all modules that are marked with a specified tag
D. None of the choices

Answer: A,B,C
Modprobe is used to load a single module, a stack of dependent modules, or all modules that are marked with a specified tag.

QUESTION NO: 24
modprobe will automatically load all base modules needed in the module stack as described by its dependency file. What file is this?

A. modules.dep
B. modprobe.dep

C. module.dep
D. modep.dep

Answer: A
Explanation: depmod creates a list of module dependencies, by reading each module under /lib/modules/version and determining what symbols it exports, and what symbols it needs. By default this list is written to modules.dep in the same directory. The normal use of depmod is to include the line /sbin/depmod -a in one of the files in /etc/rc.d so the correct module dependencies will be available after booting the system. depmod -e prints a list of all unresolved symbols.

When you tried to load the modules using modprobe command it checks the modules.dep file generated by depmod command to identify the dependencies and load all dependencies as well .

QUESTION NO: 25CORRECT TEXT
Which utility is used to create or update the modules.dep file? Type the command only.

Answer: depmod
Explanation: depmod creates a list of module dependencies, by reading each module under /lib/modules/version and determining what symbols it exports, and what symbols it needs. By default this list is written to modules.dep in the same directory. The normal use of depmod is to include the line /sbin/depmod -a in one of the files in /etc/rc.d so the correct module dependencies will be available after booting the system. depmod -e prints a list of all unresolved symbols.

QUESTION NO: 26CORRECT TEXT
Type in the simplest command to list all loaded modules:

Answer: lsmod
Explanation: lsmod shows information about all loaded modules. The format is name, size, use count, list of referring modules. The information displayed is identical to that available from /proc/modules.

QUESTION NO: 27CORRECT TEXT
You wish to get infomation on a module called msdos.o. Type in the simplest command that would list all information including author and description for the module:

Answer: modinfo msdos
Explanation: modinfo extracts information the Linux Kernel modules given on the command line. If the module name is not a filename, then the /lib/modules/version directory is searched, as done by modprobe

Syntax: modinfo modulename or filename
Example:
modinfo ext3
Sample output
filename: /lib/modules/2.6.9-5.EL/kernel/fs/ext3/ext3.ko
author: Remy Card, Stephen Tweedie, Andrew Morton, Andreas Dilger, Theodore Ts'o and others
description: Second Extended Filesystem with journaling extensions
license: GPL
vermagic: 2.6.9-5.EL 686 REGPARM 4KSTACKS gcc-3.4
depends: jbd

QUESTION NO: 28CORRECT TEXT
You have a module called msdos.o which has a dependancy on fat.o. What single command will load msdos.o and its dependant fat.o module in one command line?

Answer: modprobe msdos
Explanation: modprobe command load the modules with it's all dependencies by reading modules.dep file.

QUESTION NO: 29CORRECT TEXT
Type in the simplest command, including any switchs, to rebuild the modules.dep file after you have made changes to the modules.conf file:

Answer: depmod -a
Explanation: depmod creates a list of module dependencies, by reading each module under /lib/modules/version and determining what symbols it exports, and what symbols it needs. By default this list is written to modules.dep in the same directory. The normal use of depmod is to include the line /sbin/depmod -a in one of the files in /etc/rc.d so the correct module dependencies will be available after booting the system. depmod -e prints a list of all unresolved symbols.

QUESTION NO: 30CORRECT TEXT
Type in the command to list your current kernel version, including any switches:

Answer: uname -a
Answer: uname -r
Explanation: uname command print the system information ie kernel version, kernel name, machine hardware name etc.
Syntax: uname [option]
Options: -a or -all à print all information, in the following order:
-r or --kernel-release à print the kernel release

QUESTION NO: 31CORRECT TEXT
You wish to install the module fat.o into the kernel. Type in the simplest command to do this, assuming there are no dependencies for this module:

Answer: insmod fat
Explanation: insmod is a command insert the module into the kernel but it can't resolves the dependencies so to load the module into the kernel with dependencies use the modporbe command.

QUESTION NO: 32
What modprobe option will cause inactive kernel modules to be unloaded?

A. autoclean
B. inactive
C. remove
D. timeout
E. holdoff

Answer: A
Explanation: modprobe -k or --autoclean option will cause inactive kernel modules to be unloaded.

QUESTION NO: 33CORRECT TEXT
You are using insmod. You do not want to use the default configuration file /etc/modules.conf. What environment variable should you modify?

Answer: MODULECONF
Explanation: The environment variable MODULECONF can also be used to select a different configuration file from the default /etc/modules.conf or /etc/modprobe.conf (or /etc/conf.modules (deprecated)).This environment variable will override all the definitions above.

QUESTION NO: 34
You can find out how much memory the kernel is using by taking the total amount of memory in your machine and subtracting from it the amount of:

A. "total mem" in /proc/meminfo
B. "total mem" in /proc/memused
C. "total mem" in /proc/memcurrent
D. None of the choices

Answer: A
Explanation: You can find out how much memory the kernel is using by taking the total amount of memory in your machine and subtracting from it the amount of ``total mem'' in /proc/meminfo or the output of the command `free'.
See the sample output of /proc/meminfo
MemTotal: 118180 kB
MemFree: 19108 kB
Buffers: 4800 kB
Cached: 37860 kB
SwapCached: 8 kB
Active: 38564 kB
Inactive: 24820 kB

HighTotal: 0 kB
HighFree: 0 kB
LowTotal: 118180 kB
LowFree: 19108 kB
SwapTotal: 522072 kB
SwapFree: 522056 kB
Dirty: 100 kB
Writeback: 0 kB
Mapped: 32936 kB
Slab: 7084 kB
Committed_AS: 64768 kB
PageTables: 1036 kB
VmallocTotal: 901112 kB
VmallocUsed: 3252 kB
VmallocChunk: 897140 kB
HugePages_Total: 0
HugePages_Free: 0
Hugepagesize: 4096 kB

See the sample output of fee -m command

total used free shared buffers cached
Mem: 115 96 18 0 4 37
-/+ buffers/cache: 55 60
Swap: 509 0 509

QUESTION NO: 35CORRECT TEXT
What command will load groups of modules into the kernel as needed?

Answer: modprobe
Explanation: modprobe command load the modules with it's all dependencies by reading modules.dep file.

QUESTION NO: 36CORRECT TEXT
If the module file name is given without directories or extension, insmod will search for the module in some common default directories. What environment variable can be used to override this?

Answer: MODPATH
Explanation:

If the module file name is given without directories or extension, insmod will search for the module in some common default directories. The environment variable MODPATH can be used to override this default. If a module configuration file such as /etc/modules.conf exists, it will override the paths defined in MODPATH.

QUESTION NO: 37
Which of the following could be used to load kernel modules for a 2.4.x kernel?

A. **vi**/proc/modules
B. **rmmod**
C. **kmod**
D. **depmod**

Answer: C
Explanation: in 2.4.x version kernel, kmod command is used to load the modules.

QUESTION NO: 38
Loadable kernel modules can (choose all that apply):

A. save memory
B. ease configuration
C. include filesystems
D. include ethernet card drivers

Answer: A,B,C,D
Explanation: Loadable kernel modules can save memory and ease configuration. The scope of modules has grown to include filesystems, ethernet card drivers, tape drivers, printer drivers, and more.

QUESTION NO: 39
In which file can you find these lines?
alias eth0 ne2k-pci
options ne2k-pci io=0x300 irq=5

Answer: /etc/modules.conf

Answer: /etc/modprobe.conf
Explanation: /etc/modules.conf or /etc/modprobe.conf file contains the aliases of modules as well as parameter i.e aliases for ethenet card, sound card etc.

i.e alias eth0 8139too : Actually modules of device is 8139too and creating the aliases to eth0

QUESTION NO: 40
Which utility is used to create the modules.dep file that is required by modprobe?

A. ksyms
B. makemod
C. makedep
D. lsmod
E. depmod

Answer: E
Explanation: /lib/modules/Kernel-Version/modules.dep file contains the entry of module dependencies, which is created by depmod command.

depmod creates a list of module dependicies, by reading each module modules.dep identifies the module dependicies.

QUESTION NO: 41
You found these lines in the modules.dep file:

/lib/modules/2.2.5-15smp/fs/msdos.o:
/lib/modules/2.2.5-15smp/fs/fat.o

Which of the following is true?

A. The msdos module is dependent upon fat.
B. The fat and msdos modules cannot be loaded manually.
C. The fat and msdos modules are automatically loaded at startup.
D. The fat module is a submodule to the msdos module.

Answer: A
Explanation: modules.dep file contains the list of module dependicies.

Whenever you try to load the module , it checks the dependicies, whether dependicies from modules.dep.
modules.dep file contains
module name : dependicies modules.

QUESTION NO: 42
The network connection needs to be started during bootup which requires that the drive module for the network card be loaded properly. Which of the following files is used to map an ethernet device (eth0, for example) to a specific driver module?

A. /etc/module/config
B. /etc/modules.conf
C. /etc/conf/modules
D. /etc/insmod.conf

Answer: B
Explanation: Aliases provides uniform ways to address various types of hardware. By default, aliases are used for ethernet interface, sound cards and usb conrollers. See the example:
alias eth0 8139too : which creates the alias of 8139too module to eth0.
These aliases are written in /etc/modules.conf or /etc/modprobe.conf file.

QUESTION NO: 43
You need maximum performance of your machine and therefore you decide to unload all dispensable modules. Which command would you use?

A. rmmod
B. insmod -r
C. unmod
D. module -r

Answer: A
Explanaion: rmmod command remove or unload the module from the kernel. You can use the lsmod command to list all loaded modules.
Example: rmmod modulename
Verify using lsmod command

QUESTION NO: 44
What commands will load a kernel module? (Select TWO answers)

A. ldmod
B. modprobe
C. loadmod
D. insmod
E. modload

Answer: B, D
Exlanation: To load the modules into the kernel, use the modprobe or insmod command.
modprobe modulename : Loads the module
insmod modulename: Loads the module
lsmod : list all loaded module
rmmod modulename: removes or unload the module from the kernel
modprobe -r mdoulename: removes or unload the module from the kernel

Section 2, (1.105.2) Reconfigure, build, and install a custom kernel and kernel modules (31 Questions)

* Description: Candidates should be able to customize, build, and install a kernel and kernel loadable modules from source This objective includes customizing the current kernel configuration, building a new kernel, and building kernel modules as appropriate. It also includes installing the new kernel as well as any modules, and ensuring that the boot manager can locate the new kernel and associated files (generally located under /boot, see objective 1.102.2 for more details about boot manager configuration).

***Key files, terms, and utilities** include:

/usr/src/linux/*

```
/usr/src/linux/.config
 /lib/modules/kernel-version/*
 /boot/*
```

make

make targets: config, menuconfig, xconfig, oldconfig, modules, install, modules_install, depmod

QUESTION NO: 1
What command would rebuild the ld.so.cache file?

A. ldd
B. ldconfig
C. ld.so.cache -rebuild
D. ld

Answer: B
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.

QUESTION NO: 2
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

Answer: C
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 NO: 3
The command "make config" requires bash.

A. true
B. false

Answer: A

Explanation The command `make config' while in /usr/src/linux starts a configure script which asks you many questions. It requires bash, so verify that bash is /bin/bash, /bin/sh, or $BASH.

QUESTION NO: 4CORRECT TEXT
If you need to view per-user disk space usage on a filesystem, the _____ command can provide that information if the kernel is built to support it.

Answer: du
Explanation:
du - estimate file space usage
example: du -h file/directory.

QUESTION NO: 5
Rate this advice: In order to use the latest kernel, it is necessary to first upgrade to the newest utilities and libraries.

A. True
B. False

Answer: A
Explanation: In order to use the latest kernel, it is first necessary to upgrade to the newest utilities and libraries.

QUESTION NO: 6CORRECT TEXT
What is the name of the Kernel configuration file? Type just the filename.

Answer: .config
Explanation: config hidden file is the kernel configuration file so while you recompile the kernel, you should copy the .config file into /boot.
Example:
cp .config /boot/config-2.4.17

QUESTION NO: 7
GNU Make determines which pieces of a large program need to be recompiled and issues the commands to recompile them when necessary.

A. true
B. false

Answer: A
Explanation GNU Make is a program that determines which pieces of a large program need to be recompiled and issues the commands to recompile them, when necessary.

QUESTION NO: 8
What does "make bzImage" do as opposed to "make zImage"?

A. makes a bz encrypted kernel
B. makes a kernel with a better compression ratio
C. makes a kernel with built in gzip application
D. nothing

Answer: B
Explanation:
As the Kbuild documentation states:
Somecomputerswon'tworkwith'makebzImage',eitherduetohardware problemsorveryoldversionsofliloorloadlin.Ifyourkernelimage issmall,youmayuse'makezImage','makezdisk',or'makezlilo' onthesesystems.

QUESTION NO: 9
You have just recompiled a new kernel and rebooted your system with the new kernel. Unfortunately you are getting "Can't locate module" error messages. Which of the following is most likely to be the source of the problem?

A. You copied the modules to the wrong directory.
B. You did not configure modular support into the kernel.
C. You did not run depmod after installing the modules.
D. You dud not install the modules.

Answer: B
Explanation:

There is one more step needed for the build process, however. You have created the kernel, but now you need to create all the loadable modules if you have them configured. Be aware that typical distribution kernels tend to have almost every feature installed, plus a few others for good measure. These can typically take an hour or so to build on our Athlon XP1800. The stock kernels are somewhat leaner by default and take, on average, 25 minutes to compile. To build the modules we run:

```
$ make modules
```

If you forget to enter make modules command, you will get that message.

```
Follow these steps while recompile the kernel.
```

Installation steps

cd /usr/srcbzcat linux-2.4.17.tar.bz | tar xvf -cd linuxmake config | make menuconfig | make xconfigmake depmake cleanmake bzImagemake modules (if modular kernel)make modules_install (if modular kernel)cp System.map /boot/System.map-2.4.17cp arch/i386/boot/bzImage /boot/vmlinuz-2.4.17cp .config /boot/config-2.4.17mkinitrd /boot/initrd-<version> <kernel version> # Depending on kernel configurationUpdate LILO or GRUBReboot into new kernel

QUESTION NO: 10

When preparing to compile a new kernel, which of the following commands can be used to create the configuration file?

A. **make** config
B. **make** kernel
C. ./configure
D. **make** kernelconfig
E. [Kernel Source Path]/Configure

Answer: A

Explanation: while recompile the kernel, we can use config or oldconfig or menuconfig or xconfig command to create the configuration file.

QUESTION NO: 11

If your new kernel does not behave normally after a routine kernel upgrade, chances are that you forgot to _____ before compiling the new kernel.

A. make clean
B. make shot
C. make clear
D. make remove

Answer: A
Explanation: If your new kernel does really weird things after a routine kernel upgrade, chances are you forgot to make clean before compiling the new kernel. Symptoms can be anything from your system outright crashing, strange I/O problems, to crummy performance. Make sure you do a make dep, too.

QUESTION NO: 12
Upgrading a kernel involves which of the following tasks (choose all that apply):

A. configuring the desired modules
B. compiling the kernel and modules
C. installing the kernel image
D. conducting a system reboot

Answer: A,B,C,D
Explanation: Upgrading the kernel involves configuring desired modules, compiling the kernel and modules, and finally installing the kernel image. This is followed by a system reboot (with fingers crossed!) to load the new kernel. All of this is documented in the ``README'' file which comes with each kernel package. Further information can be found in the ``Documentation/'' subdirectory. A particularly helpful file there is ``Configure.help'' which contains detailed information on the available kernel compile options and modules.

QUESTION NO: 13
Which of the following insures that all of the dependencies, such as the include files, are in place?

A. make dep
B. make clean
C. make_dep
D. make_install

Answer: A
Explanation: When the configure script ends, it also tells you to `make dep' and (possibly) `clean'. So, do the `make dep'. This insures that all of the dependencies, such the include files, are in place. It does not take long, unless your computer is fairly slow to begin with. For older versions of the kernel, when finished, you should do a `make clean'. This removes all of the object files and some other things that an old version leaves behind. In any case, do not forget this step before attempting to recompile a kernel.

QUESTION NO: 14
Incremental upgrades of the kernel are distributed as:

A. patches.
B. fixes.
C. hotfixes.
D. service packs.

Answer: A
Explanation: Incremental upgrades of the kernel are distributed as patches. For example, if you have version 1.1.45, and you notice that there's a `patch46.gz' out there for it, it means you can upgrade to version 1.1.46 through application of the patch. You might want to make a backup of the source tree first (`make clean' and then `cd /usr/src; tar zcvf old-tree.tar.gz linux' will make a compressed tar archive for you.).

QUESTION NO: 15
Which of the following removes all of the object files and some other things that an old version leaves behind?

A. make dep
B. make clean
C. make_dep
D. make_install

Answer: B
Explanation When the configure script ends, it also tells you to `make dep' and (possibly) `clean'. So, do the `make dep'. This insures that all of the dependencies, such the include files, are in place. It does not take long, unless your computer is fairly slow to begin with. For older versions of the kernel, when finished, you should do a `make clean'. This removes all of the object files and some other things that an old version leaves behind. In any case, do not forget this step before attempting to recompile a kernel.

QUESTION NO: 16
What command will compile the Linux kernel and leave a file in arch/i386/boot called bzImage?

A. make bzImage
B. make compile
C. make Image
D. make bzdisk

Answer: A
Explanation After depending and cleaning, you may now `make bzImage' or `make bzdisk' (this is the part that takes a long time.). `make bzImage' will compile the kernel, and leave a file in arch/i386/boot called `bzImage' (among other things). This is the new compressed kernel. `make bzdisk' does the same thing, but also places the new bzImage on a floppy disk which you hopefully put in drive ``A:''. `bzdisk' is fairly handy for testing new kernels; if it bombs (or just doesn't work right), just remove the floppy and boot with your old kernel. It can also be a handy way to boot if you accidentally remove your kernel (or something equally as dreadful).

QUESTION NO: 17
What command will compile the Linux kernel and leave a file called bzImage in the floppy disk?

A. make bzImage
B. make compile
C. make Image
D. make bzdisk

Answer: D

Explanation After depending and cleaning, you may now `make bzImage' or `make bzdisk' (this is the part that takes a long time.). `make bzImage' will compile the kernel, and leave a file in arch/i386/boot called `bzImage' (among other things). This is the new compressed kernel. `make bzdisk' does the same thing, but also places the new bzImage on a floppy disk which you hopefully put in drive ``A:''. `bzdisk' is fairly handy for testing new kernels; if it bombs (or just doesn't work right), just remove the floppy and boot with your old kernel. It can also be a handy way to boot if you accidentally remove your kernel (or something equally as dreadful).

QUESTION NO: 18
Which of the following commands will attempt to configure the kernel from an old configuration file and run through the make config process for you?

A. make oldconfig
B. make newconfig
C. make clean
D. None of the choices

Answer: A
Explanation Make oldconfig' will attempt to configure the kernel from an old configuration file; it will run through the `make config' process for you. If you haven't ever compiled a kernel before or don't have an old config file, then you probably shouldn't do this, as you will most likely want to change the default configuration.

QUESTION NO: 19CORRECT TEXT
To produce a compiled kernel with slightly better than standard compression, type the command with and any options and arguments to accomplish just the compilation.

Answer: make bzImage

QUESTION NO: 20CORRECT TEXT
You are using X and wish to build a new kernel. What X tool would you use to build the .config file. Type in just the command, not the switches:

Answer: make xconfig
Explanation:
xconfigis a graphical frontend using qconfby Roman Zippel. It requires the **qtand X libraries to build and use. The interface is intuitive and customizable. Online help is automatically shown for each kernel configuration option. It also can show dependency information for each module which can help diagnose build errors.**

QUESTION NO: 21CORRECT TEXT
Type in the command to compile a kernel image with normal compression:

Answer: make zImage
Explanation: finally ready to start the actual kernel build with make bzimage command. At the prompt type:
`make bzImage it will create the kernel image with normal compression.`

QUESTION NO: 22
Which of the following is not a valid make command during a kernel recompile?

A. make dep
B. make clean
C. make xconfig
D. make modules
E. make gzlilo

Answer: E
Explanation:
We are now (finally) ready to start the actual kernel build. At the prompt type:
`make bzImage`
Somecomputerswon'tworkwith'makebzImage',eitherduetohardware problemsorveryoldversionsofliloorloadlin.Ifyourkernelimage issmall,youmayuse'makezImage','makezdisk',or'makezlilo' onthesesystems
Steps to recompile the Kernel
1. cd /usr/src2. bzcat linux-2.4.17.tar.bz | tar xvf -3. cd linux4. make config | make menuconfig | make xconfig 5. make dep6. make clean7. make bzImage8. make modules (if modular kernel)9.

make modules_install (if modular kernel)10. cp System.map /boot/System.map-2.4.1711. cp arch/i386/boot/bzImage /boot/vmlinuz-2.4.1712. cp .config /boot/config-2.4.1713. mkinitrd /boot/initrd-<version> <kernel version> # Depending on kernel configuration14. Update LILO or GRUB15. Reboot into new kernel

QUESTION NO: 23 CORRECT TEXT
You are working on a non graphical shell.
What command would you use to configure the kernel using a menu system. Type the command and its argument(s).

Answer: make menuconfig
Explanation menuconfig is an ncurses-based frontend. Your system must have the ncurses-devel libraries installed in order to use this utility. As the help text at the top of the screen indicates, use the arrow keys to navigate the menu. Press Enter to select sub-menus. Press the highlighted letter on each option to jump directly to that option. To build an option directly into the kernel, press Y. To disable an option entirely, press N

QUESTION NO: 24
Which of the following correctly describe a Monolithic Kernel (choose all that apply):

A. it is built into one single binary.
B. it is loaded completely into memory at boot time.
C. it pre-dates micro-kernel architecture by at least ten years.
D. None of the choices

Answer: A,B,C
Explanation: There are two types of kernel, modular and monolithic. Modular kernel has different modules to support different devices, filesystem etc but monolithic is one single bundle file.
Have everything they need in that binary.
Are loaded completely into memory at boot time.
Pre-date micro-kernel architecture by at least ten years.

QUESTION NO: 25
Which of the following correctly describe a Micro-kernel Architecture (choose all that apply):

A. it has an extremely small core.
B. only its small core remains in memory at all times.
C. its device drivers are loaded as-needed.
D. None of the choices

Answer: A,B,C
Explanation:
Micro-kernel Architectures:
Have an extremely small core.
Only the small core remains in memory at all times.
Device drivers and other additional items are loaded as-needed.

QUESTION NO: 26
Rate this comment: Linux by and large is monolithic.

A. true
B. false

Answer: A
Explanation:
Is Linux Purely Monolithic?
Linux by and large is monolithic. However, Linux permits modules, a system whereby certain parts of the kernel may be loaded at runtime. Linux modules are reminiscent of micro-kernel architectures, but Linux really remains basically a monolithic architecture.

QUESTION NO: 27
Which command would you use to apply the changes in a diff file to your existing kernel source?

A. up2date
B. patch
C. rpm
D. dpkg
E. diff

Answer: B

Explanation: patch takes a patch file containing difference listing produced by the diff program and applies those differences to one or more original files, producing patched versions.

QUESTION NO: 28
You just configured a kernel and now you want to check the dependencies. Please enter the command and its argument(s).

Answer: make dep
Explanation: To check the dependencies of files you should use the make dep command.
Steps to re-compile the kernel
We have so far extracted and patched the Linux sources. During our preparation we also determined what hardware is installed in the system so that we will know which modules will need compilation. Before we proceed to actually configuring the kernel there are a couple minor but important details to complete.
Inside the Linux source directory is the default `Makefile`. This file is used by the **makeutility to compile the Linux sources. The first few lines of the** `Makefile` contains some versioning information:

```
VERSION = 2
PATCHLEVEL = 4
SUBLEVEL = 22
EXTRAVERSION = -1
```

Note that there is an additional EXTRAVERSION field. To prevent overwriting any existing kernel modules on the system we will change this EXTRAVERSION to something unique. When the final installation steps are run, kernel module files will then get written to /lib/modules/$VERSION.$PATCHLEVEL.$SUBLEVEL-$EXTRAVERSION.
make mrpropermake config or make menuconfig or make oldconfig or make xconfigmake depmake cleanmake bzImagemake modulesmake modules_installmkinitrd /boot/initrd-2.6.0.img 2.6.0mkinitrd -k vmlinux-VERSION -i initrd-VERSIONcp arch/i386/boot/bzImage /boot/bzImage-KERNEL_VERSIONcp System.map /boot/System.map-KERNEL_VERSIONln -s /boot/System.map-KERNEL_VERSION /boot/System.map

QUESTION NO: 29
Which of the following commands can typically be used to configure a kernel?

A. ./config

B. ./configure
C. make config
D. make configure

Answer: C
Explanation:
config is the least user-friendly option as it merely presents a series of questions that must be answered sequentially. Alas, if an error is made you must begin the process from the top. Pressing Enter will accept the default entry, which is in upper case.

QUESTION NO: 30
Which file is read by the program ldconfig ?

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

Answer: B
Explanation: this file is scanned by ldconfig to create the hints files used by the run-time linker /usr/libexec/ld.so to locate shared libraries.

QUESTION NO: 31
You have a USB storage device that you can't get working. You have enabled all appropriate USB options in the latest 2.2 kernel but will can't get your device working. What is the most likely the source of the problem?

a. You have not configured your usb.usermap properly
b. You are using the Wrong kernel for this type of device.
c. The USB device is not USB 2.0 compliant
d. There is a USB resource conflict.

Answer: B
Explanation: The 2.2.18 kernel has some USB support but a 2.4.x or newer kernel is recommended.

Subsection 1, Boot Disks (5 Questions)

QUESTION NO: 1
On a debian system which of the following would build a boot disk

A. mkboot /dev/floppy
B. makeboot --device /dev/fd0 2.4.18-12
C. mkboot --device /dev/fd0 2.4.18-12
D. mkboot /boot/vmlinux-2.4.18-12
E. mkbootdisk /boot/vmlinux-2.4.18-12

Answer: C
Explanation:
mkboot creates a boot floppy appropriate for the running system. The boot disk is entirely self-contained, and includes an initial ramdisk image which loads any necessary SCSI modules for the system. The created boot disk looks for the root filesystem on the device suggested by /etc/fstab. The only required argument is the kernel version to put onto the boot floppy.
Syntax: mkbootdisk [options] kernel version.
Bydefault mkboot creates the boot disk on first floppy device. If you want to specify the device use the --device option. In debian you should specify the kernel filename which resides on /boot.

QUESTION NO: 2CORRECT TEXT
On a Red Hat system, with a single floppy drive and a returned output from the uname command of 2.4.20-12, what exact command string will create a customized boot disk for this system? Type the full command string to accomplish this.

Answer: mkbootdisk --device /dev/fd0 2.4.20-12
Explanation:
mkbootdisk creates a boot floppy appropriate for the running system. The boot disk is entirely self-contained, and includes an initial ramdisk image which loads any necessary SCSI modules for the system. The created boot disk looks for the root filesystem on the device suggested by /etc/fstab. The only required argument is the kernel version to put onto the boot floppy.
Syntax: mkbootdisk [options] kernel version.

Bydefault mkbootdisk creates the boot disk on first floppy device. If you want to specify the device use the --device option.

We can print the kernel version using uname -r command.

QUESTION NO: 3CORRECT TEXT
On a Debian-based system, what command will create a boot disk on the first floppy if your kernel image is named "vmlinux-2.4.18-4"? Type the full command string to accomplish this.

Answer: mkboot vmlinux-2.4.18-4
Answer: mkboot /boot/vmlinux-2.4.18-4
Explanation:
mkboot creates a boot floppy appropriate for the running system. The boot disk is entirely self-contained, and includes an initial ramdisk image which loads any necessary SCSI modules for the system. The created boot disk looks for the root filesystem on the device suggested by /etc/fstab. The only required argument is the kernel version to put onto the boot floppy.
Syntax: mkbootdisk [options] kernel version.
Bydefault mkboot creates the boot disk on first floppy device. If you want to specify the device use the --device option. In debian you should specify the kernel filename which resides on /boot.

QUESTION NO: 4 CORRECT TEXT
You want to create a boot floppy using a given image file on your hard disk.What utility would you use to do so?

Answer: mkbootdisk --device /dev/fd0 `uname -r`
Explanation:
mkbootdisk creates a boot floppy appropriate for the running system. The boot disk is entirely self-contained, and includes an initial ramdisk image which loads any necessary SCSI modules for the system. The created boot disk looks for the root filesystem on the device suggested by /etc/fstab. The only required argument is the kernel version to put onto the boot floppy.
Syntax: mkbootdisk [options] kernel version.
Bydefault mkbootdisk creates the boot disk on first floppy device. If you want to specify the device use the --device option.

We can print the kernel version using uname -r command.

QUESTION NO: 5
You've downloaded an image file of a boot floppy disk to your hard drive. What is the best utility to create a boot floppy from the disk image? (Specify a single command without options.)

Answer: dd
Explanation: dd command creates the disk images. Example:
dd if=diskboot.img of=/dev/fd0 : which creates the image of diskboot.img and transfer into floppy disk.

Topic 2, (106) Boot, Initialization, Shutdown and Runlevels (35 Questions)

Section 1, (1.106.1) Boot the system (18 Questions)

* Description: Candidates should be able to guide the system through the booting process. This includes giving commands to the boot loader and giving options to the kernel at boot time, and checking the events in the log files.

***Key files, terms, and utilities** include:

/var/log/messages

`/etc/conf.modules` or /etc/modules.conf

dmesg

LILO

GRUB

QUESTION NO: 1 CORRECT TEXT
To exclude all log messages of a given logging facility, you should use a logging priority of:

Answer: none
Explanation: You can see on /etc/syslog.conf configuration file to store the log messages about the proper facility. The pattern is facility.priority,
Example
mail.* à it means mail related all priority.
If you want to exclude all log messages of facility use none priority.
Eg. cron.none

QUESTION NO: 2
You are having some trouble with a disk partition and you need to do maintenance on this partition but your users home directories are on it and several are logged in. Which command would disconnect the users and allow you to safely execute maintenance tasks?

A. telinit 1
B. shutdown -r now
C. killall -9 inetd
D. /bin/netstop --maint
E. /etc/rc.d/init.d/network stop

Answer: E
Explanation: The network services allows users to logged in from other different host. If you stop the network service it disconnect to all users.
/etc/rc.d/init.d/ directory contains all services.
To start the service
service servicename start or restart
To stop the service
service servicename stop

QUESTION NO: 3
Some loadable kernel modules accept options at load time. This can be used to set interrupt or IO addresses, for example. The place to set these options is?

A. /etc/conf.modules
B. /etc/lilo.conf
C. /boot/System.map
D. /etc/sysconfig
E. /boot/module-info

Answer: E

QUESTION NO: 4
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`

Answer: B
Explanation: There are two log files contains the boot and kernel related log messages. /var/log/boot.log and /var/log/dmesg.

QUESTION NO: 5CORRECT TEXT
Which command will display messages from the kernel that were output during the normal bootup sequence?

Answer: dmesg
Explanation: dmesg is the program helps users to print out their bootup messages. Either cat /var/log/dmesg or use dmesg command

QUESTION NO: 6
Which bootloader can lie to Windows and make Windows believe that it's installed on the first partition even if it's not?

A. GRUB
B. XLoad
C. LILO
D. FILO

Answer: A
Explanation GRUB differs from bootloaders such as LILO in that it can lie to Windows and make Windows believe that it's installed on the first partition even if it's not. So you can keep your current Linux system where it is and install Windows on the side.

QUESTION NO: 7CORRECT TEXT

On your system exists a file that is described as a map file that is used to update the MBR or first sector of the partition with the appropriate booting information. Type the full path and name of the file:

Answer: /etc/lilo.conf
Explanation: /etc/lilo.conf is the file used by lilo command to update the MBR or first sector of the partition with the appropriate booting information ie. root partition, kernel file etc.

QUESTION NO: 8CORRECT TEXT
When booting your system, you believe you saw an error message go by too quickly to see. Type in the command that will show the last system bootup messages:

Answer: dmesg
Explanation: dmesg is the program helps users to print out their bootup messages. Either cat /var/log/dmesg or use dmesg command

QUESTION NO: 9CORRECT TEXT
The dmesg command outputs information from which file, include full path?

Answer: /var/log/dmesg

Explanation: dmesg is the program helps users to print out their bootup messages. Either cat /var/log/dmesg or use dmesg command

QUESTION NO: 10CORRECT TEXT
You have made changes to your /etc/lilo.conf file. Type in the simplest command that will reload the configuration to the MBR:

Answer: lilo
Explanation: /etc/lilo.conf is the file used by lilo command to update the MBR or first sector of the partition with the appropriate booting information ie. root partition, kernel file etc. After reconfiguring the file you should update the MBR or first sector of boot partition using lilo command.

QUESTION NO: 11
Where can you specify options that affect the booting of the system?

A. /etc/lilo.conf
B. boot= prompt
C. linux:
D. init 3
E. init 5

Answer: A, B
Explanation: To effect the system booting, you can specify the options of kernel arguments on bootloader configuration file ie. lilo.conf or bootloader prompt.

QUESTION NO: 12
Where can the lilo command install the boot menu and information? Choose all that apply:

A. Master Boot Record
B. BIOS
C. First Sector of a Partition
D. BootBlk
E. Boot Prom

Answer: A, C
Explanation: lilo command update the MBR or first sector of boot partition, it depends on where you installed the boot loader.

QUESTION NO: 13CORRECT TEXT
You boot a freshly installed system loaded with all the defaults, xdm loads and crashes, and the system halts. How can you force the system to multi-user text mode with networking from the LILO: or boot: prompt?

Answer: linux 3

Explanation: There is a configuration file named /etc/inittab contains default runlevel, run level specific scripts etc. If you want to boot the system other than default runlevel you can pass the kernel argument from boot loader.
When you get the lilo screen, press ctrl+x and type linux runlevel.

The available runlevel are
0 - halt (Do NOT set initdefault to this)
1 - Single user mode
2 - Multiuser, without NFS (The same as 3, if you do not have networking)
3 - Full multiuser mode
4 - unused
5 - X11
6 - reboot (Do NOT set initdefault to this)
Runlevel 3 is called multi user so you should boot your system on run level 3 using linux 3

QUESTION NO: 14
Upon booting one of your Linux boxes, you notice a message scrolling by that does not look right, but it goes so fast, you do not have a chance to read it. What command could you use to view that message after the boot process completes?

Answer: dmesg
Explanation: dmesg command helps to print out their bootup messages. What messages are generated at boot time by kernel, you can read by using the dmesg command.

QUESTION NO: 15
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?

Answer: /etc/syslog.conf
Explanation: /etc/syslog.conf is the log configuration file, where administrator can set where to send what type of logs !! . By default logs sends to local system's under /var/log/different log files.

*.user @logserver.example.com : Logs generated by user will send to logserver.example.com host.

QUESTION NO: 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

Answer: D
Explanation: logrotate rotates, compress, remname the log files to becoming the very large log file. It automatic rotates, compresses, renames and deletes the old log files by reading /etc/logrotate.conf configuration file.

QUESTION NO: 17
Identify the proper device for the third partition, on the second hard disk on the first IDE controller on a PC system.

A. /dev/hda3
B. /dev/hdb3
C. /dev/hd1b3
D. /dev/hdc3

Answer: B
Explanation: hda is the first hard disk on the first IDE controller, hdb is the second. Partitions are counted from 1 (not 0) so the third partion should be hdb3 (again, not hdb2)

QUESTION NO: 18
You have just upgraded your PC to a 60 gigabyte IDE drive. While partitioning the drive, you notice that only 32 gigabytes are available. Which of the following will most likely allow you to use the entire drive?

A. Create two smaller partitions of 30 gigabytes each
B. Set the PC BIOS to use LBA mode
C. Upgrade the PC BIOS to latest version available
D. Use GRUB or latest version of LILO as a bootloader

Answer: C

Explanation: Not being able to see and use all the space on a new IDE drive is almost always a problem with a old BIOS version.

Section 2, (1.106.2) Change runlevels and shutdown or reboot system (17 Questions)

* Description: Candidates should be able to manage the runlevel of the system. This objective includes changing to single user mode, shutdown or rebooting the system. Candidates should be able to alert users before switching runlevel, and properly terminate processes. This objective also includes setting the default runlevel.

***Key files, terms, and utilities** include:

/etc/inittab

shutdown

init

QUESTION NO: 1 CORRECT TEXT
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, not the path.

Answer: shutdown
Explanation:
shutdown brings the system down in a secure way. All logged-in users are notified that the system is going down, and login is blocked. It is possible to shut the system down immediately or after a specified delay. All processes are first notified that the system is going down by the signal SIGTERM. This gives programs like vi the time to save the file being edited, mail and news processing programs a chance to exit cleanly.
You can use the -k option to send the warning message to all logged in users without really shutdown down the system.

QUESTION NO: 2CORRECT TEXT

What is considered the normal exit value of a process?

Answer: 0
Answer: zero
Explanation: If any process exit with normal status that process return the zero.

QUESTION NO: 3
You've just rebooted your server. Users complain that the server is refusing secure connections.
Which of the following is most likely causing this problem?

A. The clients are not resolving the server name properly.
B. **sshd** is not configured to start in the default runlevel.
C. **sshd** is using tcpwrappers for security.
D. The public keys have been corrupted on the server.
E. The users need to restart their ssh-agent.

Answer: B
Explanation: To enable the ssh connection sshd service should start. Probably on first reboot sshd service is not started. So you should start the sshd service.
To start sshd service
service sshd start
To start sshd service automatically on next reboot
chkconfig sshd on

QUESTION NO: 4
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.

Answer: C
Explanation: To enable the ssh connection sshd service should start. Probably on first reboot sshd service is not started. So you should start the sshd service.
To start sshd service
service sshd start
To start sshd service automatically on next reboot
chkconfig sshd on

QUESTION NO: 5
What runlevels should never be declared as the default runlevel in `/etc/inittab`?

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

Answer: A, D
Explanation:
Standard Runlevel are:
0 - halt (Do NOT set initdefault to this)
1 - Single user mode
2 - Multiuser, without NFS (The same as 3, if you do not have networking)
3 - Full multiuser mode
4 - unused
5 - X11
6 - reboot (Do NOT set initdefault to this)

1 means single user mode and 6 means reboot. Which are not recommended for default runlevel.

QUESTION NO: 6CORRECT TEXT
Type in the simplest command to display the previous and current run level:

Answer: runlevel

Explanation:
runlevel -- find the current and previous system runlevel.

See the output of runlevel
N 3 àIt means currently system running on runlevel 3 and not switched to any runlevel.

QUESTION NO: 7CORRECT TEXT
You are in run level 5 and wish to change to run level 1. Type in the simplest command to do this:

Answer: init 1
Answer: init s
Answer: init S
Explanation: runlevel command displays the current and previous runlevel. To change runlevel from the command line, use
init runlevel
So, to change in runlevel init 1

QUESTION NO: 8
You need to change the default runlevel. Which file do you need to edit? (Write the full path including the filename)

A. /etc/init.d
B. /etc/init-table
C. /etc/inittab
D. /etc/init

Answer: C
Explanation: The file /etc/inittab contains the default run level as well as run level specific scripts.
id:3:initdefault:
If you haven't specified the run level system boots on run level 9 that is unknown run level.

QUESTION NO: 9CORRECT TEXT
You wish to change the daemons that start at a run level 3. Type in the command that would give a text menu based application to set the daemons for this runlevel:

Answer: ntsysv --level 3
Explanation:
ntsysv is a simple interface for configuring runlevel services which are also configurable through chkconfig. By default, it configures the current runlevel. If the user would like to configure other runlevels, those levels can be specified on the command line by listing the levels after --levels, without any spaces. For example, the option --levels 016 edits runlevels 0, 1, and 6.

QUESTION NO: 10CORRECT TEXT
Which process has a PID of 1. Type in the process name?

Answer: init
Explanation: init process has 1 process ID so init is called the parent of all process. You can check the process tree using pstree and using top command PID, memory stats, nice value etc.

QUESTION NO: 11CORRECT TEXT
What is the name of the file and location that governs what run level is to be booted to on startup. Give full path and file name

Answer: /etc/inittab
Explanation: The file /etc/inittab contains the default run level as well as run level specific scripts.
id:3:initdefault:
If you haven't specified the run level system boots on run level 9 that is unknown run level.

QUESTION NO: 12CORRECT TEXT
You wish to list out in text all the daemons running and stopped on your system for all run levels. Type in the simplest command

Answer: chkconfig --list
Explanation:

chkconfig provides a simple command-line tool for maintaining the /etc/rc[0-6].d directory hierarchy by relieving system administrators of the task of directly manipulating the numerous symbolic links in those directories.
To list the all services running and stopped (status) for all run levels.
chkconfig -list
To list the specific service:
chkconfig --list atd

QUESTION NO: 13
You need to change the default run-level for a machine. Which file should you edit?

A. /etc/init.d
B. /etc/init-table
C. /etc/inittab
D. /etc/init

Answer: C
Explanation: The file /etc/inittab contains the default run level as well as run level specific scripts.
id:RUNLEVEL:initdefault:
If you haven't specified the run level system boots on run level 9 that is unknown run level.

QUESTION NO: 14
You are about to do some administration tasks on a server. Which command would you use to change the runlevel?

Answer: telinit
Explanation: init or telinit is the parent of all processes. It's primary role is to create processes from a script stored in the file /etc/inittab.
To display the current and previous runlevel use the runlevel command
To change the runlevel
init runlevel or telinit runlevel

QUESTION NO: 15
Which configuration file should be modified to disable the ctrl-alt-delete key combination?

A. /etc/keys

B. /proc/keys
C. /etc/inittab
D. /proc/inittab
E. /etc/reboot

Answer: C
Explanation: /etc/inittab file contains functions of ctrl-alt-delete key combinations.
ca::ctrlaltdel:/sbin/shutdown -t3 -r now
which means reboot the system ater three seconds from now. If you want to disable this function just comment this line.

QUESTION NO: 16
Runlevels are configured _____.

A. in the kernel
B. in /etc/inittab
C. in /etc/runlevels
D. using the rl command
E. in rc.sysinit or rc.local

Answer: B
Explanation: Default runlevel, runlevel specific scripts are written in /etc/inittab file.
Id:5:initdefault: : which line defines the default runlevel
Similalry runlevel specific scripts to execute also written here:
Si::sysinit:/etc/rc.d/rc/rc.sysinit
10:0:wait:/etc/rc.d/rc 0
11:1:wait:/etc/rc.d/rc 1
12:2:wait:/etc/rc.d/rc 2
13:3:wait:/etc/rc.d/rc 3
14:4:wait:/etc/rc.d/rc 4
15:5:wait:/etc/rc.d/rc 5
16:6:wait:/etc/rc.d/rc 6

QUESTION NO: 17
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.

Answer: B
Explanation: According question, it is checking the secure and non-secure service. Telent also called non-secured service runs on port 23.
To deactive telnet service:
chckconfig telnet off
service xinetd restart

Topic 3, (107) Printing (23 Questions)

Section 1, (1.107.2) Manage printers and print queues (10 Questions)

* Description: Candidates should be able to manage print queues and user print jobs. This objective includes monitoring print server and user print queues and troubleshooting general printing problems.

***Key files, terms, and utilities** include:

/etc/printcap

lpc

lpq

lprm

lp

QUESTION NO: 1
A file exists on a server, but has no content. 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

Answer: D
Explanation:
The /etc/hosts.lpd file defines which remote systems are permitted to print on the local system.
Only that hosts specified in /etc/hosts.lpd can send the printing job. To solve that problem administrator should add the host name on that file.

QUESTION NO: 2
Which of the following are valid commands to affect your system's printing?

A. lpq
B. lprm
C. lpstatus
D. lpr
E. lpio

Answer: A, B, D
Explanation:
lpr command is used to send the printing job.
lpq command is used to query the printing job
lprm command is used to remove the printing job

QUESTION NO: 3
Which of the following commands 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

Answer: A
Explanation:
lprm -a all command is used to flush all print job on all configured queues.

QUESTION NO: 4
What program do you use to suspend a printer queue?

A. lpr
B. lpq
C. lpc

D. lpd
E. lprm

Answer: C
Explanation:
The lpc command is used to examine and control the print server operation. The lpc status command displays the administrative status of a print queue. The lpd program caches status and job information in order to improve performance. The lpc flush command will flush the cached information and cause the server to regenerate it. The lpc enable and lpc disable commands enable or disable spooling to the print queue, and the lpc stop and lpc start commands stop and start printing (or transfers) of jobs in the print queue

QUESTION NO: 5
Which parameters should appear in a valid /etc/printcap file to allow a local printer queue to point to another machine's print queue? Choose two.

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

Answer: A, B
Explanation:
rm à remote machine (hostname) (with rp)
rp à remote printer name (with rm)

QUESTION NO: 6 CORRECT TEXT
The normal filesystem location for the LPD queue directory is:

Answer: /var/spool/lpd/
Explanation: /var directory contains the spooling as well as log files.
/var/spool/cups contains the spooling queue of cups.
/var/spool/lpd contains the spooling queue of lpd
/var/spool/mail contains the mail spooling queue

QUESTION NO: 7
In the LPD system, a print queue is defined in what file?

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

Answer: D
Explanation: /etc/printcap file contains the print queue name of the system.

QUESTION NO: 8
Which of the following files is responsible for defining various options and values to control the printing and spooling of print jobs?

A. /etc/printers
B. /etc/print.conf
C. /etc/printcap
D. /etc/printd.conf

Answer: C
Explanation: /etc/printcap file contains a list of printer definitions, location of the spool files. Each entry of the file describes a printer with fields separately by ":". The first entry is the name of printer is known by and any aliases separated by "|". Subsequent entries indicate the localtion and capabilities of the printer.

QUESTION NO: 9
Which of the following tools is used to configure CUPS?

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

Answer: D
Explanation: lpd is the CUPS line printer Daemon mini-server that supports legacy client systems that use the LPD protocol. Cups-lpd does not act as a standalone network daemon but instead operates using the Internet "Super-Server" .
More : man cups-lpd

QUESTION NO: 10
You want to bypass printing filters using lpr. What command is correct?

A. lpr -o nofilter
B. lpr -r
C. lpr -o raw
D. lpr -l

Answer: C
Explanation: -o raw specifies that the print file is already formatted for the destination and should be sent without filtering.

Section 2, (1.107.3) Print files (9 Questions)

* Description: Candidates should be able to manage print queues and manipulate print jobs. This objective includes adding and removing jobs from configured printer queues and converting text files to postscript for printing.

***Key files, terms, and utilities** include:

lpr

lpq

mpage

QUESTION NO: 1
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

Answer: A
Explanation:
The lpc command is used to examine and control the print server operation. The lpc status command displays the administrative status of a print queue. The lpd program caches status and job information in order to improve performance. The lpc flush command will flush the cached information and cause the server to regenerate it. The lpc enable and lpc disable commands enable or disable spooling to the print queue, and the lpc stop and lpc start commands stop and start printing (or transfers) of jobs in the print queue.

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.

QUESTION NO: 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 putty
E. lpr -P hplaserj putty

Answer: B, E
Explanation: lpr command is used to send the printing job. If printer is not specified then it will send printing job to default printer. To specify the printer name should use the -P option.

Example:
lpr -Pprintername -#numberofcopies filename

-# or -K specify the number of copies.

QUESTION NO: 3
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. cat hosts > lpr ; cat hosts > lpr
E. for 1 in 2 lpr hosts

Answer: A, B
Explanation: lpr command is used to send the printing job. If printer is not specified then it will send printing job to default printer. To specify the printer name should use the -P option.

Example:
lpr -Pprintername -#numberofcopies filename

-# or -K specify the number of copies.

QUESTION NO: 4
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.

Answer: A
Explanation: lpr command is used to send the printing job. If printer is not specified then it will send printing job to default printer. To specify the printer name should use the -P option.

Example:
lpr -Pprintername -#numberofcopies filename

-# or -K specify the number of copies.

QUESTION NO: 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`

Answer: A
Explanation:
cat command reads the contents of foo.txt and send to print to the default printer twelve copies of same documents.

QUESTION NO: 6
What command will flush all jobs on all print queues on a Linux system that uses the LPD daemon? Type the command with any options and arguments.

Answer: lprm -a all
Explanation:
lprm -a all command is used to flush all print job on all configured queues.

QUESTION NO: 7
What command should be entered to print and then delete the filem foobar.txt?

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

Answer: C
Explanation: lpr command prints the files, when we use the lpr command without any option, it will print the document as well as document put as previous state. -r option helps to remove the file after printing.

QUESTION NO: 8
The correct command to view "verbose" line printer queue information is:

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

Answer: D
Explanation: lpq command shows the current print queue status on the named printer.
Example: lpq : List the current print queue of default printer
lpq -Pprinter1 : List the print queue of printer1
lpq -a -Pprinter1 : -a option reports jobs on all printers.

QUESTION NO: 9
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

Answer: B
Explanation: Ghostscript also called the Postscript and PDF language interpreter, which converts the postscript file into non-postscript.
#enscript -p outputifle inputfile : Which creates the postscript file.

Section 3, (1.107.4) Install and configure local and remote printers (3 Questions)

* Candidate should be able to install a printer daemon, install and configure a print filter (e.g.: apsfilter, magicfilter). This objective includes making local and remote printers accessible for a Linux system, including postscript, non-postscript, and Samba printers.

***Key files, terms, and utilities** include:

/etc/printcap
`/etc/apsfilter/*`
`/var/lib/apsfilter/*/`
`/etc/magicfilter/*/`
`/var/spool/lpd/*/`
lpd

QUESTION NO: 1CORRECT TEXT
What file on a remote host should be configured to allow your host to print to its already functioning printers? Type the full path and name of the file.

Answer: /etc/hosts.lpd
Explanation:
The /etc/hosts.lpd file defines which remote systems are permitted to print on the local system.
Only that hosts specified in /etc/hosts.lpd can send the printing job.

QUESTION NO: 2
The hosts.lpd file provides:

A. A list of network printer IP addresses.
B. A listing of printers available on the local network.
C. A listing of computers that have printer (lpd) daemons running.
D. A listing 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.

Answer: D
Explanation:
The /etc/hosts.lpd file defines which remote systems are permitted to print on the local system.
Only that hosts specified in /etc/hosts.lpd can send the printing job.
See the output of /etc/hosts.lpd
Station1.example.com
Station2.example.com
Station3.example.com

Only station1, 2 and 3 can send the print job.

QUESTION NO: 3
What file is used to deny hosts access to a system's printers? Type the filename including full path.

Answer: /etc/hosts.lpd
Explanation:
The /etc/hosts.lpd file defines which remote systems are permitted to print on the local system.
Only that hosts specified in /etc/hosts.lpd can send the printing job.
See the output of /etc/hosts.lpd
Station1.example.com
Station2.example.com
Station3.example.com

Only station1, 2 and 3 can send the print job. Other host can't send the printing job.

Topic 4, (108) Documentation (30 Questions)

Section 1, (1.108.1) Use and manage local system documentation (18 Questions)

* Candidates should be able to use and administer the man facility and the material in /usr/share/doc/. This objective includes finding relevant man pages, searching man page sections, finding commands and man pages related to them, and configuring access to man sources and the man system. It also includes using system documentation stored in /usr/share/doc/ and determining what documentation to keep in /usr/share/doc/.

***Key files, terms, and utilities** include:

MANPATH man

apropos

whatis

QUESTION NO: 1
Which two commands share the same database for retrieving information?

A. whatis
B. whereis
C. apropos
D. find
E. man

Answer: A, C
Explanation:
whatis as well as apropos command used the same database to retrieve the information. Database can update using makewhatis command

QUESTION NO: 2
What command will show only complete word matches for a search term?

A. whatis
B. apropos
C. locate
D. find
E. whereis

Answer: A
Explanation: whatis command will show only the complete word matches for a search term i.e
whatis ls
See the output
ls (1) - list directory contents

whatis clear
clear (1) - clear the terminal screen

QUESTION NO: 3
What command will show partial word matches for a search term?

A. apropos
B. locate
C. whereis
D. whatis
E. find

Answer: A
Explanation
apropos command show partial word matches for a search.
apropos clear
See the output
clear (1) - clear the terminal screen
clearenv (3) - clear the environment
clearerr [ferror] (3) - check and reset stream status
execstack (8) - tool to set, clear, or query executable stack flag of ELF binaries and shared libraries
feclearexcept [fenv] (3) - C99 floating point rounding and exception handling
klogctl [syslog] (2) - read and/or clear kernel message ring buffer; set console_loglevel
molecule (1) - draws 3D moleclear structures
pam_timestamp_check (8) - check or clear authentication timestamps
syslog (2) - read and/or clear kernel message ring buffer; set console_loglevel

QUESTION NO: 4
What command is the functional equivalent of the command "man -k searchterm"?

A. apropos searchterm
B. whatis searchterm
C. locate searchterm
D. find / -name searchterm
E. None of the selections

Answer: A
Explanation:
apropos command show partial word matches for a search. Same as man -k searchterm.
apropos clear
See the output
clear (1) - clear the terminal screen
clearenv (3) - clear the environment
clearerr [ferror] (3) - check and reset stream status
execstack (8) - tool to set, clear, or query executable stack flag of ELF binaries and shared libraries
feclearexcept [fenv] (3) - C99 floating point rounding and exception handling
klogctl [syslog] (2) - read and/or clear kernel message ring buffer; set console_loglevel
molecule (1) - draws 3D moleclear structures
pam_timestamp_check (8) - check or clear authentication timestamps
syslog (2) - read and/or clear kernel message ring buffer; set console_loglevel

Similar like:
man -k clear

QUESTION NO: 5
What command is the functional equivalent of the command "man -f searchterm"?

A. whatis searchterm
B. apropos searchterm
C. locate searchterm
D. find / -name searchterm
E. None of the selections

Answer: A

Explanation: whatis command will show only the complete word matches for a search term quivalent man -f command

whatis ls
See the output
ls (1) - list directory contents

man -f ls
ls (1) - list directory contents

QUESTION NO: 6
You want to find the man pages for utilities and tools related to PPP, but you don't know the name of the specific commands. How can you get a list of man pages that contain information about PPP?

A. **whatis** ppp
B. **man** ppp
C. **apropos** ppp
D. **mandb** ppp

Answer: C
Explanation:
apropos command show partial word matches for a search. Same as man -k searchterm.
See the output of apropos command
adsl-connect (8) - Shell script to manage a PPPoE link
adsl-setup (8) - Shell script to configure Roaring Penguin PPPoE client
adsl-start (8) - Shell script to bring up a PPPoE link
adsl-status (8) - Shell script to report on status of PPPoE link
adsl-stop (8) - Shell script to shut down a PPPoE link
capiplugin (8) - Plugin for pppd (Point-to-Point Protocol daemon)
Devel::PPPort (3pm) - Perl/Pollution/Portability
ibod (1) - ISDN MPPP bandwidth on demand daemon
ifcfg-ppp0 [pppoe] (5) - Configuration file used by adsl-start(8), adsl-stop(8), adsl-status(8) and adsl-connect(8)
ipppd (8) - (ISDN) Point to Point Protocol daemon
pppd (8) - Point-to-Point Protocol Daemon
pppdump (8) - convert PPP record file to readable format
pppoe (8) - user-space PPPoE client
pppoe-relay (8) - user-space PPPoE relay agent

pppoe-server (8) - user-space PPPoE server
pppoe-sniff (8) - examine network for non-standard PPPoE frames
pppstats (8) - print PPP statistics
pppstats [ipppstats] (8) - print PPP statistics
ppp-watch (8) - daemon to make PPP interfaces act more like other interfaces
wvdial (1) - PPP dialer with built-in intelligence

QUESTION NO: 7CORRECT TEXT
Type in the command that is equivalent to man -k:

Answer: apropos
Explanation:
apropos command show partial word matches for a search. Same as man -k searchterm.

QUESTION NO: 8CORRECT TEXT
Type in the command that is equivalent to man -f:

Answer: whatis
Explanation: whatis command will show only the complete word matches for a search term quivalent man -f command

whatis ls
See the output
ls (1) - list directory contents

man -f ls
ls (1) - list directory contents

QUESTION NO: 9
You need to find all references in your system documentation to the word "copy". Which of the following will best accomplish this task?

A. man copy
B. which copy
C. locate copy
D. apropos copy
E. grep "copy" /usr/man/*

Answer: D
Explanation:
apropos command show partial word matches for a search. Same as man -k searchterm.
apropos copy it will list all references having word copy.
bcopy (3) - copy byte sequence
bcopy [bstring] (3) - byte string operations
copysign (3) - copy sign of a number
copysignf [copysign] (3) - copy sign of a number
copysignl [copysign] (3) - copy sign of a number
cp (1) - copy files and directories
cpio (1) - copy files to and from archives
dd (1) - convert and copy a file
File::Copy (3pm) - Copy files or filehandles
ginstall [install] (1) - copy files and set attributes
intltoolize (8) - copy intltool related files to software package
mcopy (1) - copy MSDOS files to/from Unix
memccpy (3) - copy memory area
memcpy (3) - copy memory area
memmove (3) - copy memory area
mempcpy (3) - copy memory area
objcopy (1) - copy and translate object files
pax (1) - read and write file archives and copy directory hierarchies
rcp (1) - remote file copy
scp (1) - secure copy (remote file copy program)
stpcpy (3) - copy a string returning a pointer to its end
stpncpy (3) - copy a fixed-size string, returning a pointer to its end
strcpy (3) - copy a string
strncpy [strcpy] (3) - copy a string
tiffcp (1) - copy (and possibly convert) a TIFF file
wcpcpy (3) - copy a wide character string, returning a pointer to its end
wcpncpy (3) - copy a fixed-size string of wide characters, returning a pointer to its end
wcscpy (3) - copy a wide character string
wcsncpy (3) - copy a fixed-size string of wide characters
wmemcpy (3) - copy an array of wide-characters
wmemmove (3) - copy an array of wide-characters
wmempcpy [mempcpy] (3) - copy memory area

QUESTION NO: 10CORRECT TEXT
Assume that on your system, there are man pages for both the command crontab and the configuration file for crontab. What command would you use to access the man page for the crontab configuration file?

Answer: man 5 crontab
Explanation: Numerical value 5 is for configuration file. 8 for administration command. So, for crontab configuration file use man 5 crontab.

QUESTION NO: 11CORRECT TEXT
What section of the Man pages are system administration commands in? Type the numeral of the section:

Answer: 8
Explanation: Numerical value 8 for system administration command and 5 for configuration file.

QUESTION NO: 12CORRECT TEXT
What section of the Man pages are system files mentioned in? Type the numeral of the section.

Answer: 5
Explanation: Numerical value 5 is for configuration file. 8 for administration command. So, for crontab configuration file use man 5 crontab.

QUESTION NO: 13
The directory location `/usr/share/doc` contains what files?

A. All documentation created from application source code.
B. All documentation you wish to share with other users.
C. Supplemental information about installed packages.
D. Programs for reading documentation.

Answer: A
Explanation: /usr/share/doc/ directory contains the all documentation file create fromt the application source code.

QUESTION NO: 14
In what section of the man pages would you expect to find the man page that documents /dev/null?

Answer: man -K /dev/null
Explanation: -K option of man page helps to search for the specified string in all man pages.

QUESTION NO: 15
In compliance with the FHS, in which of the following places are man pages typically found?

A. /usr/share/man
B. /opt/man
C. /usr/doc
D. /var/pkg/man
E. /usr/local/man

Answer: A

QUESTION NO: 16
Your users report that they are using the program dia to create diagrams. They are having problems with the software and they think there is a bug. What command will give you help with functionality and contact information to report a possible bug?
Do not give the path or any options.

Answer: flea

QUESTION NO: 17
The directory /usr/share/doc/ contains:

A. HTML versions of man pages
B. Man pages for installed packages
C. Programs for reading documentation
D. User-created documentation about the system

E. Supplemental information about installed packages

Answer: E
Explanation: /usr/share/doc directory contains the documentation for installed packages.

QUESTION NO: 18 CORRECT TEXT
You already checked the manpages on PPPD. You need to find more information on PPPD related programs. Fill in the command without arguments and options to use.

Answer: apropos
Explanation: Each manual page has a short description available within it. Apropos searches the descriptions for instances of keyword. Keyword is usually a regular expression, or may contain wildcards, or match the exact keyword.

Section 2, (1.108.2) Find Linux documentation on the Internet (7 Questions)

* Description: Candidates should be able to find and use Linux documentation. This objective includes using Linux documentation at sources such as the Linux Documentation Project (LDP), vendor and third-party websites, newsgroups, newsgroup archives, and mailing lists.

***Key files, terms, and utilities** include:

not applicable

QUESTION NO: 1CORRECT TEXT
What is the preferred documentation tool of the FSF? Type in the name of the tool only:

Answer: info
Explanation: info is the preferred documentation tool for FSF.
Example: info date

QUESTION NO: 2

The main collection of Linux usenet newsgroups are found in which usenet hierarchy?

A. sys.linux
B. comp.linux
C. comp.os.linux
D. comp.sys.linux
E. comp.opsys.linux

Answer: C

QUESTION NO: 3CORRECT TEXT
What Internet based organization is primarily responsible for hosting and distributing the various Linux HOWTOs? (NOT the URL)

Answer: the linux documentation project

Explanation: The Linux Documentaion Project is primarily responsible for hosting and distributing the various Linux HOWTOs. The official site is www.tldp.org

QUESTION NO: 4CORRECT TEXT
You need to access the site for HOWTO's, Guides and mini HOWTO's. Type in the full URL as it would appear in any browser, including the protocol.

Answer: http://www.linuxdoc.org
Answer: http://www.tldp.org
Explanation: The Linux Documentaion Project is primarily responsible for hosting and distributing the various Linux HOWTOs. The official site is www.tldp.org. As well as Linux Documentation are found in www.linuxdoc.org .

QUESTION NO: 5
With the web site, www.tldp.org, what does "tldp" stand for?

Answer: The Linux Documentation Project
Explanaion: tldp is the Linux Documentation Project, which maintains the Linux HOWTO's, Documentation etc.

QUESTION NO: 6

Choose THREE websites that provide Linux-related news and documentation.

A. Linux Scoop
B. LWN.net
C. Tux Facts
D. Linux Today
E. NewsForge

Answer: B, D, E
Explanation: Like tldp.org other web sites also provides the news and documentation related to linux. Like: lwn.net, linux today, newsforge, freshmeat.com etc.

QUESTION NO: 7
You need to find the latest HOWTOs on using SATA devices. What web site hosts the latest HOWTOs?

Answer: www.serialata.org
Explanation: www.serialata.org is the site provides the latest HOWTO's, documentation on using the SATA devices.

Section 3, 1.108.5 Notify users on system-related issues (5 Questions)

* Description: Candidates should be able to notify the users about current issues related to the system. This objective includes automating the communication process, e.g. through logon messages.

***Key files, terms, and utilities** include:

/etc/issue
`/etc/issue.net`
`/etc/motd`

QUESTION NO: 1
What file is displayed BEFORE users log in for users who log in to the machine locally?

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

Answer: A
Explanation: The file /etc/issue is a text file which contains a message or system identification to be printed before the login prompt. And /etc/issue.net contains a message or syste, identification to be printed before the remote (telnet) login.

QUESTION NO: 2CORRECT TEXT
Type in the name of the file including full path that holds contains a daily message viewed by users when they log in?

Answer: /etc/motd
Explanation: motd (Message Of The Day) contains the daily message and displayed after login.

QUESTION NO: 3CORRECT TEXT
Type in the name of file and full path to the file that holds a message for remote users about possible system outages:

Answer: /etc/issue.net
Explanation: The file /etc/issue is a text file which contains a message or system identification to be printed before the login prompt. And /etc/issue.net contains a message or syste, identification to be printed before the remote (telnet) login.

QUESTION NO: 4
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.

Answer: /etc/issue
Explanation: /etc/issue file is called pre-login message and identification file, Whereever message you write into this file will display at local login prompt and /etc/issue.net is for remote login prompt i.e telnet.

QUESTION NO: 5
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

Answer: D
Explanation: /etc/issue file prints the pre-login message and identification for local login and /etc/issue.net file prints the messages for remote login.

Topic 5, (109) Shells, Scripting, Programming and Compiling (35 Questions)

* Description: Candidate should be able to customize shell environments to meet users' needs. This objective includes setting environment variables (e.g. PATH) at login or when spawning a new shell. It also includes writing bash functions for frequently used sequences of commands.

***Key files, terms, and utilities** include:

~/.bash_profile

`~/.bash_login`

`~/.profile`

`~/.bashrc`

`~/.bash_logout`

`~/.inputrc`

function (Bash built-in command)

export

env

set (Bash built-in command)

unset (Bash built-in command)

Section 1, (25 Questions)

QUESTION NO: 1
How can you enable onscreen (non-printing) numbers in a vi session?

A. :set num
B. :se nu
C. :set -o number
D. :set +o num
E. None of the choices

Answer: B

Explanation: To enable line numbers on vi editor :set number or :se nu. To remove the line number on vi editor :set nonumber or :se nonu

QUESTION NO: 2
When starting vi with the file nohup.out, which of the following will enable onscreen numbers?

A. vi +/set num nohup.out
B. vi +"se nu" nohup.out
C. vi /+"set number" nohup.out
D. vi +":set num" nohup.out
E. echo "set numb" | vi nohup.out

Answer: B
Explanation: If you want to set the onscreen line number on vi editor while starting the vi use the vi +" se nu" filename where + is like concatination symbol.

QUESTION NO: 3
What command with options will cause the redirection symbol (>) to fail to overwrite the contents of an existing file?

A. set -o noclobber
B. set +o nooverwrite
C. export OVERWRITE=no
D. alias >='!>'
E. None of the choices

Answer: A
Explanation: Shell can configure through variable, aliases, functions, set, shopt commands.
set -o : Lists all shell options
noclobber option prevent the overriwiting the file using > symbol. If status of noclobber is on then it overrides to file using >.
#set -o noclobber : Which brings the nocobber in on state
#set +o noclobber : Which brings the noclobber in off state.

QUESTION NO: 4CORRECT TEXT
You wish to execute the ls command but it appears to be aliased. What is the easiest way of execute the orignal ls command without the alias?

Answer: \ls
Explanation: \ symbol is used to kill the meaning of predefined characters.
Example: echo "Total Amount is \$5" it displays the $5 because \ removing the meaning of $ here.
alias ls="clear"
#ls :Clear the screen
#\ls : Previous meaning then alias

QUESTION NO: 5
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.

Answer: B
Explanation: Using the export command, we can export the local variable into the sub-shells.
Example:
#X=100
#bash :Entered into the sub-shell
#echo $X : not accessing
#exit : Return back to previous shell
#export X : Exporting the X variable to sub-shell
#bash :Entering into the sub-shell
#echo $X : It display the value of X variable.

QUESTION NO: 6

You've just finished editing a new entry in the /etc/exports file. Which of the following will cause the changes to take effect without interrupting current connected users or rebooting the machine? Choose all that apply.

A. exportfs -a
B. /etc/rc.d/init.d/nfs restart
C. service nfs restart
D. kill -1 HUP nfs
E. init 1

Answer: A
Explanation: exportfs command is used to maintain the current table of exported file systems for the NFS.
exportfs -a : Export all shared directories written in /etc/export
exportfs -v : Shows locally shared directories
exportfs -r : Refresh the changes in /etc/export file
expotfs -u : Unshared the exported directories

QUESTION NO: 7CORRECT TEXT
After modifying /etc/exports, what must be done to make the modifications available to users? Type the command with any options and arguments.

Answer: exportfs -r
Explanation: exportfs command is used to maintain the current table of exported file systems for the NFS.
exportfs -a : Export all shared directories written in /etc/export
exportfs -v : Shows locally shared directories
exportfs -r : Refresh the changes in /etc/export file
expotfs -u : Unshared the exported directories

QUESTION NO: 8CORRECT TEXT
You added `/usr/local/bin` to your `PATH` environment variable. Next you executed the command `make`, which calls `gcc`. This failed because `gcc` couldn't find the executable in `/usr/local/bin` that it needed. To fix this, you should execute:
_____PATH allowable

Answer: export

Explanation: Using the export command, we can export the local variable into the sub-shells.
Example:
#X=100
#bash :Entered into the sub-shell
#echo $X : not accessing
#exit : Return back to previous shell
#export X : Exporting the X variable to sub-shell
#bash :Entering into the sub-shell
#echo $X : It display the value of X variable.

QUESTION NO: 9
What two files acting together make up the login environment for a user on a default install of Linux?

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

Answer: A, D
Explanation: profile script file is used to declare the environmental variable as well as to run the program automatically at login time.
/etc/profile : It is a global scripts, when you write in this file it applies to all users
~/.bash_profile : It is user specific file, when you write in this file it applies only to that particular user.

QUESTION NO: 10
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

Answer: B
Explanation: profile script file is used to declare the environmental variable as well as to run the program automatically at login time.
/etc/profile : It is a global scripts, when you write in this file it applies to all users
~/.bash_profile : It is user specific file, when you write in this file it applies only to that particular user.

QUESTION NO: 11
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

Answer: D
Explanation: user has lots of hidden files in home directory, which is used to modify the user's environment.
Like: ~/.bashrc : User specific alias, function
~/.bash_profile : User specific startup program, variables
~/.bash_history : contains the user's history
~/bash_logout : Executes when user logout from the shell

QUESTION NO: 12
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

Answer: C
Explanation: Shell can configure through variable, aliases, functions, set, shopt commands.
set -o : Lists all shell options
noclobber option prevent the overriwiting the file using > symbol. If status of noclobber is on then it overrides to file using >.
#set -o noclobber : Which brings the nocobber in on state
#set +o noclobber : Which brings the noclobber in off state.

QUESTION NO: 13 CORRECT TEXT
You issued the command: `export CFLAGS="-march-i586". You can remove this environment variable by using the command: _____`CFLAGS

Answer: unset
Explanation: unset command removes the variables as well as command line functions.
#X=100
#echo $X
#unset X

QUESTION NO: 14
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`

Answer: B
Explanation: Using the export command, we can export the local variable into the sub-shells.
Example:
#X=100
#bash :Entered into the sub-shell
#echo $X : not accessing

#exit : Return back to previous shell
#export X : Exporting the X variable to sub-shell
#bash :Entering into the sub-shell
#echo $X : It display the value of X variable.

QUESTION NO: 15 CORRECT TEXT
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?`

Answer: /etc/profile

Explanation: profile script file is used to declare the environmental variable as well as to run the program automatically at login time called the startup programs.
/etc/profile : It is a global scripts, when you write in this file it applies to all users.
Example: If you declare some variable in this file can access by all users. So if you want to modify the value of environmental variable, you should edit this file. Eg HOME, LANG, SHELL, PATH, PWD, PS1 etc.
~/.bash_profile : It is user specific file, when you write in this file it applies only to that particular user.

QUESTION NO: 16
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.

Answer: D
Explanation: Using the export command, we can export the local variable into the sub-shells.
Example:
#X=100
#bash :Entered into the sub-shell

#echo $X : not accessing
#exit : Return back to previous shell
#export X : Exporting the X variable to sub-shell
#bash :Entering into the sub-shell
#echo $X : It display the value of X variable.

QUESTION NO: 17CORRECT TEXT
Where are command line aliases defined for a user? Type the full path and name of the file for the currently logged in user.

Answer: ~/.bashrc
Explanation: user has lots of hidden files in home directory, which is used to modify the user's environment.
Like: ~/.bashrc : User specific alias, function
~/.bash_profile : User specific startup program, variables
~/.bash_history : contains the user's history
~/bash_logout : Executes when user logout from the shell

QUESTION NO: 18CORRECT TEXT
A user wishes to modify his Environment variable PATH, What file should you tell him to edit in his home directory. Give filename only, no path.

Answer: .bash_profile
Explanation: user has lots of hidden files in home directory, which is used to modify the user's environment.
Like: ~/.bashrc : User specific alias, function
~/.bash_profile : User specific startup program, variables
~/.bash_history : contains the user's history
~/bash_logout : Executes when user logout from the shell

QUESTION NO: 19
You need to find all references in system documentation to the word backup. What command would you type? (Do not provide full path)

Answer: grep
Explanation: grep command print the lines matching the pattern from file.
Example: grep root /etc/passwd : It prints all lines having root pattern.

QUESTION NO: 20
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: '\'7b print $3 }'
D. grep Bob /etc/passwd | awk -f: '\'7b print $3 }'
E. grep Bob /etc/passwd | cut -F: -d3

Answer: A, C
Explanation: cut command is used to display certain fileds from file and grep displays the line which matched the pattern.
Example: cut -d: -f3 /etc/passwd : where -d means field delimeter, -f means field number.
grep root /etc/passwd : displays the line having root pattern
Similarly awk the is programming language for eitin text, searches a file for lines matching a patterns or pattern.
Example: awk '/bash/ { print }' /etc/passwd : which prints all lines having bash pattern.

QUESTION NO: 21
What command will allow you to see all of your environment variables?

A. echo $*
B. env
C. which
D. export

Answer: B
Explanation: env command displays all environmental and set command displays all environmental as well as shell variables.

QUESTION NO: 22
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

Answer: B

QUESTION NO: 23
How can you find all possible parameters which you may use when loading a specific module?

A. modinfo -p
B. modinfo --list
C. modprobe -...

Answer: A
Explanation: modinfo extracts information from the Linux Kernel modules given on the command line. -p, param will show you possible parameters.

QUESTION NO: 24
User space daemon ..... ?

A. klog
B. klogd
C. syslog
D. syslogd

Answer: D
Explanation: Daemons are often named with a d in the end (like klogd and syslogd). klogd is a kernel space log daemon, and syslogd is a user space log daemon.

QUESTION NO: 25
The command "echo $$" outputs 14292 to the screen. What does the output mean?

A. the PID of your active shell
B. the PID of .....
C. the PID of the last command

D. the PID of the last backgrounded command

Answer: A
Explanation: $$ evaluates to the pid of the current shell

Section 2, (1.109.2) Customize or write simple scripts (10 Questions)

* Description: Candidate should be able to customize existing scripts, or write simple new (ba)sh scripts. This objective includes using standard sh syntax (loops, tests), using command substitution, testing command return values, testing of file status, and conditional mailing to the superuser. This objective also includes making sure the correct interpreter is called on the first (#!) line of scripts. This objective also includes managing location, ownership, execution and suid-rights of scripts.

***Key files, terms, and utilities** include:

while

for
test
chmod

QUESTION NO: 1 CORRECT TEXT
Within a script you need to create a loop. Following the for variable list, the statements to be lopped are found between the keywords _____ and done.

Answer: do
Explanation: Here is the simple example of for and while loop

For.sh

```
#!/bin/bash
clear
echo -n "Enter Several Words"
read words
for word in $words
do
 echo "Current Word is: $word"
done
```

while.sh

```
#!/bin/bash
ans="yes"
while [ $ans = "yes" ]
```

```
do
 echo -n "Enter filename to read"
 read file
 cat $file
 echo -n "Do you want to read another file ?"
 read ans
done
```

QUESTION NO: 2
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

Answer: A
Explanation:
cron executes the system job in different time interval.
Syntax for cron is:
Minute Hour day of Month Month Day of Week Command

Minute can be 0-59
Hour can be 0-23
Day of Month 1-31
Month 1-12
Day of Week 0-7 Where 0 or 7 is Sunday.

QUESTION NO: 3 CORRECT TEXT
Within a script you need to crate a loop. Following the for variable in list, the statements to be looped are found between the keywords ____ and done.

Answer: do
Explanation: do .... done defines the scope of loop to be executed when condition becomes true.

Here is the simple example of for and while loop

For.sh

```
#!/bin/bash
clear
echo -n "Enter Several Words"
read words
for word in $words
do
 echo "Current Word is: $word"
done
```

while.sh

```
#!/bin/bash
ans="yes"
while [ $ans = "yes" ]
do
 echo -n "Enter filename to read"
 read file
 cat $file
 echo -n "Do you want to read another file ?"
 read ans
done
```

QUESTION NO: 4CORRECT TEXT
You are running a Red Hat machine. You have added a 2nd NIC to your machine and rebooted it. The card is detected in the BIOS but is not configured along with the eth0 interface upon network start. A file must be created to allow this interface to function. Type the full path and name of the file.

Answer: /etc/sysconfig/network-scripts/ifcfg-eth1
Explanation: eth0 is the first ethernet card name and eth1 is the second ethernet card name. Interface configuration filename is /etc/sysconfig/network-scripts/ifcfg-eth? Containing the following directives
DEVICE=eth?
ONBOOT=yes | no
BOOTPROTO=static || dhcp
IPADDR=x.x.x.x

NETMASK=x.x.x.x
GATEWAY=x.x.x.x

QUESTION NO: 5
You are looking into a new script you received from your senior administrator. In the very fist line you notice a #! followed by a path to a binary. The shell will:

A. Igore the script.
B. Use that binary to interpet the script.
C. Use that binary to compile the script.
D. Be placed by that binary.

Answer: B
Explanation: On Every Script file, we should write the path of binary interpreter
Example: #!/bin/bash where bash is the interpreter of bash shell scripts.

QUESTION NO: 6
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

Answer: C
Explanation: Using bash script we can print the parameter passing from the command line, which start from 1 index number,
echo $2 : prints the second parameter passing from the command line. $* means all parameter passing from the command line.
However, there is a SHIFT command before the ECHO $2 command so there correct answer is gamma.

QUESTION NO: 7 CORRECT TEXT
The very first line of a shell script should always contain what two characters at the beginning of the line?

Answer: #!
Explanation: The first line in a shell scripts should contain 'magic', which is commonly referred to as the she-bang. This tells the operating system which interpreter to use in order to execute the script.
Some example:
#!/bin/bash : Used for bash scripts
#!/bin/sh : Used for Bourne shell scripts
#!/usr/bin/perl: Used for Perl Scripts

QUESTION NO: 8
What command prints available functions?

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

Answer: A
Explanation: declare -f command prints all available functions.

QUESTION NO: 9
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.

Answer: D
Explanation: When we run the scripts, it returns the exit value that can be either 0 or 1-255 where 0 means exited without error and non-zero means exited with error. Return value can print using echo $?

QUESTION NO: 10
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

Answer: B
Explanation: function is a collection of similar commands. To execute a series of commands on a recurring, you should create a function and execute it.

Creating function:
function()
{
command1
command2
command2
}
To execute function :
function1 : just call the function by name

Topic 6, (111) Administrative Tasks (78 Questions)

Section 1, (1.111.1) Manage users and group accounts and related system files (22 Questions)

* Description: Candidate should be able to add, remove, suspend and change user accounts. Tasks include to add and remove groups, to change user/group info in passwd/group databases. The objective also includes creating special purpose and limited accounts.

***Key files, terms, and utilities** include:

/etc/passwd
`/etc/shadow`
`/etc/group`
`/etc/gshadow`
chage
gpasswd
groupadd
groupdel

groupmod
grpconv
grpunconv
passwd
pwconv
pwunconv
useradd
userdel
usermod

QUESTION NO: 1CORRECT TEXT
What command will tell you which groups you belong to?

Answer: groups
Explanation: groups command displays the belonging group name.
Example: groups : displays the group name you belongs to
 # groups user1 : Displays the groups name in which user1 belongs to

QUESTION NO: 2CORRECT TEXT
What file would you edit to make the current user's vi session options always take effect? Type the full path and filename.

Answer: ~/.vimrc
Answer: ~/.exrc
Explanation: ~/.vimrc or ~/.exrc are called vi configuration file. when you open the vi editor it opens with the configuration configured in configuration file.
Example: when you set the line numbers using :set number, it sets only for current session. If you want always the line number you need to write in configuration file.
Example:
#vi .vimrc
:set number
:set ignorecase
#vi filename

When you try to open file using vi editor it tries to open by .vimrc configuration, if file not found then tries to open with configuration of .exrc

QUESTION NO: 3
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

Answer: E
Explanation: Here is the sample entry of /etc/shadow
User1:!!:13322:0:99999:7:::
This file contains users password as well as password aging policy. Better editing this file use chage command.
 # chage -l username : List the password aging policy eg minimum days to change password, maximum days to use same password, password expire days, number of days to give warning before password expiration etc.

 # chage -M 20 username : Sets the maximum number of days to user same password.
#chage -m 10 username : Sets minimum number of days to use same password.
#chage -W 7 username : Sets the warning starts days before password expire.

QUESTION NO:4
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.

Answer: B
Explanation: By default password stores in /etc/shadow by encrypting using MD5 tool. So when you read /etc/passwd it shows like following entry:
User1:x:500:500:/home/user1:/bin/bash
Where x represents that user's password is in /etc/shadow file.
To store the user information as well as user's password in /etc/passwd
#pwunconv
To store users password in /etc/shadow
#pwconv

QUESTION NO: 5
Your /etc/passwd file appears to have approximately 1/2 shadow passwords and 1/2 standard unix encrypted passwords. What utility would you most likely run again to fix this?

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

Answer: A
Explanation: By default password stores in /etc/shadow by encrypting using MD5 tool. So when you read /etc/passwd it shows like following entry:
User1:x:500:500:/home/user1:/bin/bash
Where x represents that user's password is in /etc/shadow file.
To store the user information as well as user's password in /etc/passwd
#pwunconv
To store users password in /etc/shadow
#pwconv

QUESTION NO: 6
Where are the default settings for the useradd command kept?

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

E. /etc/login.defs

Answer: A
Explanation: useradd command reads the default settings from /etc/default/useradd as well as from /etc/login.defs file. Like some default settings are password never expire, never account expire, normar user's ID starts from 500 etc. If you want to chage default settings just modify these file.

QUESTION NO: 7CORRECT TEXT
What command with switches allows you to set the defaults for the useradd command? Type the command with any options and arguments.

Answer: useradd -D

Explanation: When useradd command invokes without -D option, the useradd command creates a new user account using the values specified on the command line and the default values from the system.

QUESTION NO: 8CORRECT TEXT
You wish to add the user king to the system including his home directory. Type in the simplest command to do this including switches:

Answer: useradd -m king
Explanation: -m option is used to create the user's home directory if aleady doesn't exists.

QUESTION NO: 9CORRECT TEXT
You wish to remove the user stef from the system, including his home directories. Type in the simplest command to do this:

Answer: userdel -r stef
Explanation: userdel command is used to remove the user from the system. Where -r option is used to remove the user with home directory.

 # userdel username : Deletes the user from system but preserves the user's home directory.
#userdel -r username : Deletes the user with home directory.

QUESTION NO: 10CORRECT TEXT
User rick has been suspended from your company and you wish to lock his account to stop anyone using it. Type in the simplest command to do this:

Answer: usermod rick -L
Answer: passwd -L rick
Explanation: We can lock the user account either usermod or passwd command.
#usermod -L username : Which locks the user account
#usermod -U username : which unlocaks the user account

QUESTION NO: 11CORRECT TEXT
User king has been exiled to the marketing department who has a group name mktg. You now wish to change the primary group for the user king to the mktg group. Type in the simplest command to do this:

Answer: usermod -g mktg king
Explanation: usermod command is used to modify the user's account.
#usermod -g groupname username : Make user primarily belongs to group
#usermod -G groupname username : Make user Suppliementarly belongs to group
#usermod -d directory username : Set the home directory
#usermod -s shell username :Change the login shell
#usermod -L username : Locks the user account
#usermod -U username : Unlocks the user account

QUESTION NO: 12CORRECT TEXT
What command will insert a single "!" symbol in from of the encrypted password in the system's shadow file? Type the command with any options and arguments:

Answer: usermod -L
Answer: passwd -l

Explanation: when user account lock it insert ! symbol in form of encrypted password in /etc/shadow. User account can lock using
#usermod -L username
or
#passwd -l username

QUESTION NO: 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

Answer: C
Explanation: usermod command is used to modify the user accounts.
To lock the user account:
usermod -L username
To unlock the user account
usermod -U username

QUESTION NO: 14

You are logged in as root. What command do you run to find out what groups user testking belongs to?

Answer: groups testking
Explanation: groups command prints group name belonging the user.
Example, groups user1 : prints the all group name in which user belongs

QUESTION NO: 15 CORRECT TEXT
You are logged in as root. How to check user brown's group?

Answer: groups brown
Explanation: groups command prints group name belonging the user.
Example, groups user1 : prints the all group name in which user belongs

QUESTION NO: 16
The _____ command is used to modify or set the password expiration for a user.

Answer: passwd
Answer: usermod
Explanation: usermod command is used to modify the user's account.
#usermod -g groupname username : Make user primarily belongs to group
#usermod -G groupname username : Make user Suppliementarly belongs to group
#usermod -d directory username : Set the home directory
#usermod -s shell username :Change the login shell
#usermod -L username : Locks the user account
#usermod -U username : Unlocks the user account
#usermod -E data username :Sets account expiration date

QUESTION NO: 17
User Bob Swanson (bswanson) has left TestKing.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. uderdel -r bswanson

Answer: C

Explanation: userdel command is used to remove the user from the system. Where -r option is used to remove the user with home directory.
 # userdel username : Deletes the user from system but preserves the user's home directory.
#userdel -r username : Deletes the user with home directory.

QUESTION NO: 18
You are the system administrator for a consulting firm where several people use Linux as their desktop operating system. One of yours 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 difficulty 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

Answer: A
Explanation: The file called .Xdefaults in the home directory is loaded into the X server using the xrdb program when you start a X session. In this file, each X application has a number of options which can be set, such as reverse video, window size, window location, and many others. You can set these options so that they are set every time you start up an application.

QUESTION NO: 19
What is a reasonable command to uinstall a Debian Package from your System?

a. dpkg -Ra Package
b. dpkg -R Package
c. dpkg -r Package
d. dpkg -ra package

Answer: C
Explanation: -r is for --remove, -R is for --recursive.With -ra all packages unpacked, but marked to be removed or purged in file /var/lib/dpkg/status, are removed or purged, respectively.

QUESTION NO: 20
After Minor security incident you are instructed by your lead system administrator to verify the RPMs installed on a running system. Which command will create a complete report that you can analyze for changes that my be security related?

A. rpm -Va >result
B. rpm -Qavy >result
C. rpm -Vqt md5 >result
D. rpm --checksig >result

Answer: A
Explanation: -V is for verify, -a is for all. > result will redirect the results to a file named result.

QUESTION NO: 21
You need to know where all the configuration files are located for the installed postfix. Assuming it was installed with rpm, which command will list this information for you ?
a. rpm -qc postfix
b. rpm -Vc postfix
c. rpm -ql postfix
d. rpm -qa postfix

Answer: A
Explanation: rpm {-q | --query}[PACKAGE_NAME] [-a, --all] [-f, --file FILE] [-g, --group GROUP] [-p, --package URLFILE] [--querybynumber NUMBER] [--triggeredby PACKAGE_NAME] [--whatprovides CAPABILITY] [--whatrequires CAPABILITY] [pkgselect-options] [query-options]
-c, --configfiles will list only configuration files (implies -l).

QUESTION NO: 22
You want to examine the changelog for the installed package postfix. Which command will display the changelog?

a. rpm -Vc postfix
b. rpm -qpil postfix
c. rpm -changelog postfix
d. rpm -q changelog postfix

Answer: D
Explanation: rpm {-q | --query}[PACKAGE_NAME] [-a, --all] [-f, --file FILE] [-g, --group GROUP] [-p, --package URLFILE] [--querybynumber NUMBER] [--triggeredby PACKAGE_NAME] [--whatprovides CAPABILITY] [--whatrequires CAPABILITY] [pkgselect-options] [query-options]
`--changelog` Display change information for the package.

Section 2, (1.111.2) Tune the user environment and system environment variables (9 Questions)

* Description: Candidate should be able to modify global and user profiles. This includes setting environment variables, maintaining skel directories for new user accounts and setting command search path with the proper directory.

***Key files, terms, and utilities** include:

/etc/profile

`/etc/skel`

env

export

set

unset

QUESTION NO: 1CORRECT TEXT

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?

Answer: /etc/skel

Explanation: /etc/skel directory is called the template directory. When new user will create into system it automatically copies all the contents of /etc/skel into users home directory.

QUESTION NO: 2 CORRECT TEXT

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?

Answer: /etc/skel

Explanation: /etc/skel directory is called the template directory. When new user will create into system it automatically copies all the contents of /etc/skel into users home directory.

QUESTION NO: 3CORRECT TEXT
Where should you put the .pinerc file so that all new users get it as part of their initial creation? Type the full path of the directory.

Answer: /etc/skel
Explanation: /etc/skel directory is called the template directory. When new user will create into system it automatically copies all the contents of /etc/skel into users home directory.
If you create welcome file in /etc/skel it will copy into user's home directory while creating the users.

QUESTION NO: 5CORRECT TEXT
Type in the full path and name of the global environment and startup program configuration file; this file typically contains the PATH, umask and ulimit system wide settings.

Answer: /etc/profile

Explanation: /etc/profile is used to declare the global environmental variable as well as startup program. When declare into this file it applies to all users. And user specific variable and startup program is declared in ~/.bash_profile.

QUESTION NO: 6
Which command will delete the environment variable, FOOBAR?

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

Answer: A
Explanation: unset command is used to delete the environmental variable or shell variable.
Example: X=10

echo $X (Available)
unset X
echo $X (not available)

QUESTION NO: 7 CORRECT TEXT
When adding a new user to the system using standard Linux commands, which directory contains the intital files copied to the new user's home directory?

Answer: /etc/skel
Explanation: /etc/skel directory is called the template directory which contains the .bashrc, bash_profile, bash_logout, bash_history etc and which files used to modify the user's environment.
When we use the useradd command, it automatically copy all the contents of /etc/skel into the user's home directory.

QUESTION NO: 8
Which file would be used to configure a user's interactive bash shell?

A. ~/.int_bash
B. .bashrc
C. .profile
D. .bash

Answer: B
Explanation: Some important files are in user's home directory, which is used to modify the user's bash shell i.e .bash_profile, .bashrc, .bash_history, .nash_logout etc.
.bash_profile: This file is used to run the user specific startup program, to set the value in environmental variable.
.bashrc : This file is used to set the user specific aliases, functions.

QUESTION NO: 9
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? (Please include the command only, without arguments or path.)

Answer: ulimit

Explanation: ulimit 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 resources.

Section 3, (1.111.3) Configure and use system log files to meet administrative and security needs (7 Questions)

* Description: Candidate should be able to configure system logs. This objective includes managing the type and level of information logged, manually scanning log files for notable activity, monitoring log files, arranging for automatic rotation and archiving of logs and tracking down problems noted in logs.

***Key files, terms, and utilities** include:

/etc/syslog.conf

`/var/log/*`

logrotate

tail -f

QUESTION NO: 1
You are working in a graphical environment and trying to configure PPP, but 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 sent 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 *`

Answer: A
Explanation: /etc/syslog.conf file the main configuration of syslogd and klogd service. In this file can specify the facility and priority.
Facility.priority
Example:
Mail.info : which means info priority of mail facility.

QUESTION NO: 2CORRECT TEXT
What is the full path and file name of the file that contains the configuration files for system logging? Type in full path and file name.

Answer: /etc/syslog.conf

Explanation: /etc/syslog.conf file the main configuration of syslogd and klogd service. In this file can specify the facility and priority.
Facility.priority
Example:
Mail.info : which means info priority of mail facility.

QUESTION NO: 3CORRECT TEXT
Type in the file and full path to the configuration file for the Sytem logging daemons:

Answer: /etc/syslog.conf

Explanation: /etc/syslog.conf file the main configuration of syslogd and klogd service. In this file can specify the facility and priority.
Facility.priority
Example:
Mail.info : which means info priority of mail facility.

QUESTION NO: 4 CORRECT TEXT
You want to display a list of all last logged in users. The file `/var/log/wtmp` `exists.`
Which command would you use?

Answer: last
Explanation: last command displays the loggin and reboot history. /var/log/wtmp file maintains this record but file in binary mode. last command reads the record from this file.

QUESTION NO: 5CORRECT TEXT
The last command functionality needs what log file to be present to operate properly? Type the full path and name of the file:

Answer: /var/log/wtmp
Explanation: /var/log/wtmp file contains all users logged in and system reboot record since this file is created. Names of users and tty's can be given, in which case last will show only those entries matching the arguments.

QUESTION NO: 6
A remote logging system 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

Answer: B
Explanation: The standard system logging daemons syslogd and klogd are both configured with /etc/syslog.conf. It is possible to configure what kind and what amount of system messages is stored in specific log files.

The format is straightforward, the first entry specifies a semi-colon delimited of facility.priority declarations. The second filed specifies the log locations, which is usually a file.
Facility ie. cron, mail, authpriv, daemons, kern, lpr, news, syslog, user etc
Priority: debug, info, notice, warning, err, crit, alert, emerg etc
mail.info means à information or more than information of log message of mail service send to /var/log/maillog

***.* means all facility and all priority send to @foobar host.**

QUESTION NO: 7
What file contains kernel level logging information such as output from a network driver module when it is loaded?

Answer: /var/log/messages
Explanation: /var/log/messages file contains the standard log messages as defined in /etc/syslog.conf file.

See the sample line of /etc/syslog.conf
***.info,mail.none;authpriv.none;cron.none /var/log/messages**

Section 4, (1.111.4) Automate system administration tasks by scheduling jobs to run in the future (17 Questions)

* Description: Candidate should be able to use cron or anacron to run jobs at regular intervals and to use at to run jobs at a specific time. Task include managing cron and at jobs and configuring user access to cron and at services.

***Key files, terms, and utilities** include:

/etc/anacrontab

```
/etc/at.deny
 /etc/at.allow
 /etc/crontab
 /etc/cron.allow
 /etc/cron.deny
 /var/spool/cron/*
```

at

atq

atrm

crontab

QUESTION NO: 1 CORRECT TEXT
You are working an evening shift and want to look at which jobs are pending for the at command.
What command would you use?

Answer: atq
Explanation:
at command is used to set the job to execute later. Example:
at now + 5 minutes
at> poweroff
at>ctlr+d
It will set the job to execute after 5 minutes to poweroff the system.
atq lists all jobs pending to execute
atrm is used to remove the at queues.

QUESTION NO: 2
Which daemon or service can be configured as a non-root user?

A. cron
B. ntp
C. lpr
D. nmbd
E. slocate

Answer: A
Explanation: cron is used to execute recurring jobs. Cron searches /var/spool/cron for crontab fles which are named after accounts in /etc/passwd; crontabs found are loaded into memory. Cron also searches for /etc/crontab and the files in the /etc/cron.d directory, which are in a different format.

QUESTION NO: 3
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

Answer: A, D
Explanation: If the file cron.allow exists and your username appears in it, you may use or access the cron scheduling. If the cron.allow file does not exists and the file cron.deny does, you must not be listed in cron.deny to use cron schedule. If neither file exists the default behaviour is not allow all users to schedule jobs, with cron.

QUESTION NO: 4CORRECT TEXT
The correct crontab entry in the minutes column to create a command in cron that runs every two minutes would be _____.

Answer: */2
Explanation: To schedule the job with cron you need to create in following syntax:
Minute Hour Day Of Month Month Day of Week Command
Where * represents every example:
*** */5 * * * echo "hello" >/dev/tty9**

Which means on every 5 hours of all day execute the echo hello and display on terminal 9.

QUESTION NO: 5
To increase system security, it is often desirable to run daemons for system services with non-root 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**

Answer: D
Explanation: cron is used to execute recurring jobs. Cron searches /var/spool/cron for crontab fles which are named after accounts in /etc/passwd; crontabs found are loaded into memory. Cron also searches for /etc/crontab and the files in the /etc/cron.d directory, which are in a different format. Where crond is the daemon of cron schedule. There crond should be in running state to execute the cron job.

QUESTION NO: 6
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

Answer: D
Explanation: To schedule the job with cron you need to create in following syntax:
Minute Hour Day Of Month Month Day of Week Command
Where * means every example:
*** */5 * * * echo "hello" >/dev/tty9**

Which means on every 5 hours of all day execute the echo hello and display on terminal 9.

QUESTION NO: 7
Which crontab entry could be used to set the system time at regular intervals?

A. 10 * * * date dt$24
B. 10 * * * settime dt$24
C. 10 * * * date<ntpl.digex.net
D. **10 * * * * /usr/sbin/runcron date <ntpl.digex.net**
E. **10 * * * * /usr/sbin/ntpdate ntp1.digex.net> /dev/null2>&1**

Answer: E
Explanation: Syntax of adding the job in cron is:
Minute Hour Day Of Month Month Day of Week Command
Where * means every example:
*** */5 * * * echo "hello" >/dev/tty9**
Which means on every 5 hours of all day execute the echo hello and display on terminal 9.
ntpdate command is used to set date and time by pooling the Network Time Protocol (NTP) Server given as the server arguments to determine the crrect time.

10 * * * * /usr/sbin/ntpdate ntp1.digex.net> /dev/null2>&1 : This line executes the ntpdate command on every 10 seconds to synchronize the date and time with NTP server ntp1.digex.net and sends the standard output and error into /dev/null.

QUESTION NO: 8
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`

Answer: C
Explanation : Time can specify using *, / and , etc wildcard.
Example: 3,4,5 means in 3, 4 and 5, */20 on every 20, * on every etc
So Answer C means between 15, 16, 17 on every day of month, every months on Monday and Thursday should execute the chklog. Remember the time format :
Minute Hour Day Of Month Month Day of Week Command
Minute can be: 0-59
Hour can be: 0-23
Day of Month can be : 1-31
Month can be : 1-12
Day of Week can be : 0-7 where 0 or 7 is Sunday.

QUESTION NO: 9CORRECT TEXT
What file or utility is used by normal users to configure the cron daemon? Type in the name of the tool:

Answer: crontab

Explanation: crontab command maintains files for individual users.
Example: crontab filename : Adds the file into cron schedule
#crontab -l : List all scheduled files using crontab
#crontab -r : Removes the cron schedules
#crontab -e : Edits the cron schedules

QUESTION NO: 10CORRECT TEXT
You wish to list the contents of your crontab. Type in the simplest command to do this:

Answer: crontab -l
Explanation: crontab command maintains files for individual users.
Example: crontab filename : Adds the file into cron schedule
#crontab -l : List all scheduled files using crontab
#crontab -r : Removes the cron schedules
#crontab -e : Edits the cron schedules

QUESTION NO: 11CORRECT TEXT
You wish to make changes to your crontab entry. Type in the simplest command to make this change:

Answer: crontab -e
Explanation: crontab command maintains files for individual users.
Example: crontab filename : Adds the file into cron schedule
#crontab -l : List all scheduled files using crontab
#crontab -r : Removes the cron schedules
#crontab -e : Edits the cron schedules

QUESTION NO: 12CORRECT TEXT
You have a job scheduled to run at 16:30 using the AT scheduler.
When you type atq it displays the following information

```
[root@localhost root]# atq
2 2003-03-14 16:00 a root
[root@localhost root]#
```

Type in the command to remove only this job:

Answer: atrm 2

Explanation:
at command is used to set the job to execute later. Example:
at now + 5 minutes
at> poweroff
at>ctlr+d
It will set the job to execute after 5 minutes to poweroff the system.
atq lists all jobs pending to execute
atrm is used to remove the pending at job, it requires the job id number.
#atrm 2

QUESTION NO: 13CORRECT TEXT

What command will show pending jobs that will be executed once on a given date and time? Type just the command to accomplish this:

Answer: atq
Explanation:
at command is used to set the job to execute later. Example:
at now + 5 minutes
at> poweroff
at>ctlr+d
It will set the job to execute after 5 minutes to poweroff the system.
atq lists all jobs pending to execute

QUESTION NO: 14
A user cannot access the cron scheduling system. What file needs to be configured to provide that access?

Answer: /etc/cron.deny and /etc/cron.allow
Explanation: If the file cron.allow exists and your username appears in it, you may use or access the cron scheduling. If the cron.allow file does not exists and the file cron.deny does, you must not be listed in cron.deny to use cron schedule. If neither file exists the default behaviour is not allow all users to schedule jobs, with cron.

QUESTION NO: 15
What command is used to view pending jobs for the at command? (Do NOT specify path).

Answer: atq
Explanation: at command is used to set the job to execute in exact point in time.
Example: at now+ 5 minutes
At> poweroff
At>ctl+d

This command will set the schedule to execute the poweroff command after five minutes from now. To display all the queue adding by using the at command use the atq command

QUESTION NO: 16
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

Answer: A
Explanation:
atrm is used to remove the pending at jobs, it requires the job id number.
Example:
#atrm 2 : Where 2 is at job id

QUESTION NO: 17
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

Answer: D
Explanation : Time can specify using *, / and , etc wildcard.
Example: 3,4,5 means in 3, 4 and 5, */20 on every 20, * on every etc
Time pattern of cron schedule is :
Minute Hour Day Of Month Month Day of Week Command
Minute can be: 0-59
Hour can be: 0-23
Day of Month can be : 1-31
Month can be : 1-12
Day of Week can be : 0-7 where 0 or 7 is Sunday.

Section 5, (1.111.5) Maintain an effective data backup strategy (14 Questions)

* Candidate should be able to plan a backup strategy and backup filesystems automatically to various media. Tasks include dumping a raw device to a file or vice versa, performing partial and manual backups, verifying the integrity of backup files and partially or fully restoring backups.

*Key files, terms, and utilities include:

cpio

dd

dump
restore
tar

QUESTION NO: 1
Which backup method resets the archive bit? Select all that apply.

A. Full
B. Incremental
C. Differential
D. Copy
E. DirTree

Answer: A, B
Explanation: Backup methods are incremental and full. Full backup copies all conents and incremental backup backups the contents modified after full backup. Here is the example of Full Backup:
#dump -0u -f /dev/sda /dev/hda5 : Which backups the full backup of /dev/hda5 into first SCSI disk.

QUESTION NO: 2CORRECT TEXT
What command with options will show you the contents with associated pathnames of an archive file named archive.tar.gz? The file must not be unpacked with the command string. Type the full command string to accomplish this.

Answer: tar -tzvf archive.tar.gz
Answer: tar tzvf archive.tar.gz
Answer: tar zxvf archive.tar.gz
Answer: tar -zxvf archive.tar.gz
Explanation: files is archived as well as compressed using gzip tool. To unpack the compressed and archived file : tar -zxvf filename
Where -z option is used to compress or uncompress using zip or gunzip tool.
-x : Extract the archive file
-t : Test the archived file
v: Verbose

If file is compresed by bzip2 command you should use j option instead of z.

QUESTION NO: 3CORRECT TEXT
What command will most effectively send a list of certain files from a directory to the tar or cpio command? Type just the command name.

Answer: ls
Explanation: ls commnd list all directory contents. Output of ls command can sends to tar or cpio.
Example: ls | tar -cvf mytar.tar *

QUESTION NO: 4CORRECT TEXT
You wish to archive and compress all the files in your home directory starting with the word projects into a file called myprojects.tar.gz. You are currently in your home directory. Type in the command that would do this:

Answer: tar -czf myprojects.tar.gz projects*
Answer: tar czf myprojects.tar.gz projects*
Answer: tar -zcf myprojects.tar.gz projects*
Answer: tar zcf myprojects.tar.gz projects*
Explanation: tar is the standard archiving tool in redhat enterprise linux used to manage the archive files.
#tar -cvf mytar.tar file or files or wildcard : which creates the archive files of mytar.tar
#tar -tvf mytar.tar : Which test the archived file
#tar -xvf mytar.tar : Which extract the mytar.tar file
tar may also compressed the archived files but using the gzip or bzip2 tools are very good to compress. Using z for zip and j for bzip2 option is used to compress the archive file with tar command.

QUESTION NO: 5CORRECT TEXT
You have a tarball called myprojects.tar.gz and you wish to view the permissions and ownership of its contents without unpacking it. Type in the simplest command to do this:

Answer: tar -tzvf myprojects.tar.gz
Answer: tar tvzf myprojects.tar.gz
Answer: tar zvtf myprojects.tar.gz
Answer: tar ztvf myprojects.tar.gz

Explanation: tar is the standard archiving tool in redhat enterprise linux used to manage the archive files.
#tar -cvf mytar.tar file or files or wildcard : which creates the archive files of mytar.tar
#tar -tvf mytar.tar : Which test the archived file
#tar -xvf mytar.tar : Which extract the mytar.tar file
tar may also compressed the archived files but using the gzip or bzip2 tools are very good to compress. Using z for zip and j for bzip2 option is used to compress the archive file with tar command.

QUESTION NO: 6CORRECT TEXT
You have just downloaded an application called rdesktop from the internet. The file downloaded is named rdesktop.tar.gz. Type in the simplest command to decompress and untar this file into the current directory:

Answer: tar -zxf rdesktop.tar.gz
Answer: tar zxf rdesktop.tar.gz

Explanation: tar is the standard archiving tool in redhat enterprise linux used to manage the archive files.
#tar -cvf mytar.tar file or files or wildcard : which creates the archive files of mytar.tar
#tar -tvf mytar.tar : Which test the archived file
#tar -xvf mytar.tar : Which extract the mytar.tar file
tar may also compressed the archived files but using the gzip or bzip2 tools are very good to compress. Using z for zip and j for bzip2 option is used to compress the archive file with tar command.

QUESTION NO: 7
Which file system should never be backed up and therefore never have to be restored?

A. ufs
B. usr

C. tmp
D. home
E. swap

Answer: E
Explanation: swap also called the virtual memory, which means using disk space as RAM. We never take the backup of swap filesystem and never restore also.

QUESTION NO: 8CORRECT TEXT
What one filesystem should you never restore (and therefore not backup): _____.

Answer: swap
Explanation: swap also called the virtual memory, which means using disk space as RAM. We never take the backup of swap filesystem and never restore also.

QUESTION NO: 9
On a default Linux system, what file system type does the dump command act upon?

A. Ext2
B. UFS
C. JFS
D. XFS
E. ReiserFS

Answer: A
Explanation: dump examines files on an ext2/3 filesystem and determines which files need to be backedup. These files are copied to the given disk, tape, other storage medium for safe keeping. By default dump command ext2/ext3 filesystem does the dump act upon.

QUESTION NO: 10CORRECT TEXT
What is a filesystem type the dump utility can work with?

Answer: ext2/ext3
Explanation: dump examines files on an ext2/3 filesystem and determines which files need to be backedup. These files are copied to the given disk, tape, other storage medium for safe keeping. By default dump command ext2/ext3 filesystem does the dump act upon.

QUESTION NO: 11
Which directory tree is ordinarily the least likely to be backup or restore?

A. /tmp
B. /var
C. /proc
D. /usr
E. /usr

Answer: C
Explanation: /proc is called the virtual filesystem, created automatically at boot time containing the information of running kernel. So no need to take backup.

QUESTION NO: 12
Which backup method will require the minimum tapes to restore?

A. Full
B. Incremental
C. Differential
D. Copy
E. DirTree

Answer: A
Explanation: To restore the data from tapes at least one full backup is required.
#restore -rf devicename

QUESTION NO: 13
Which of the following commands is used to restore files from backups made with dump?

A. extract
B. cpio -d
C. restore
D. udump

Answer: C
Explanation: dump is the standard backup utility in Linux, using dump utility we can take either full or incremental backup.
Example: dump -0u -f /dev/sda /dev/hda7 : which takes the full backup of /dev/hda7 into /dev/sda.

To restore from backup backuped by dump command :
restore -rf /dev/sda : Restore command restore from the backup file.

QUESTION NO: 14
You have an automated backup via tar to your tape drive /dev/st0 that runs each night. You've decided to manually check last night's tape. The command to list the contents of the tape is _____.

Answer: cpio -t < /dev/st0

Section 6, (1.111.6) Maintain system time (9 Questions)

* Description: Candidate should be able to properly maintain the system time and synchronize the clock over NTP. Tasks include setting the system date and time, setting the BIOS clock to the correct time in UTC, configuring the correct timezone for the system and configuring the system to correct clock drift to match NTP clock.

***Key files, terms, and utilities** include:

/usr/share/zoneinfo
`/etc/timezone`
`/etc/localtime`
`/etc/ntp.conf`
`/etc/ntp.drift`
date
hwclock
ntpd
ntpdate

QUESTION NO: 1CORRECT TEXT

You use the public NTP server time.nist.gov to make sure your system clock is accurate before using it to adjust your hardware clock. Complete the following command to accomplish this:
_____ time.nist.gov

Answer: ntpdate
Explanation: ntpdate sets the local date and time by polling the Network Time Protocol server given as the server arguments to determine the correct time. It must be run as a root on the local host.

QUESTION NO: 2CORRECT TEXT
To slave your NTP daemon to an external source, you need to modify the _____ variable in your `/etc/ntp.conf file.`

Answer: server
Explanation: needs to modify the server parameter in file to specify the master NTP server.

QUESTION NO: 3CORRECT TEXT
NTP is used to synchronize the system ____ with a central system resource.

Answer: clock
Explanation: ntp sets the clock by pooling the NTP server given as the server arguments.

QUESTION NO: 4
What protocol will allow you to keep accurate time on your hosts?

A. ntp
B. nntp
C. ncftp
D. inn
E. ntime

Answer: A
Explanation: ntp protocol sets the local date and time from other server given as the server arguments to determine the correct time. It must be run as a root on the local host.

QUESTION NO: 5 CORRECT TEXT
A user complains that his laptop shows the wrong time when it is not connected to the network.
What command must the superuser run to adjust the laptop's clock without entering in BIOS?

Answer: date
Explanation: date command is used to set or display the system date and time.
#date -s "new date and time" : It sets the new date and time into system

QUESTION NO: 6 CORRECT TEXT
The _____ file is the configuration file for ntpd.

Answer: /etc/ntp.conf
Explanation: The ntpd program is an operating system daemon which sets and maintains the system time of day in synchronism whith Internet standard time servers.
/etc/ntp.conf : Default configuration file.
/etc/ntp/keys : The default name of the key file
/etc/ntp/ntpservers : The file contains the NTP server to synchronize the time.

QUESTION NO: 7
To see the current time set by a NTP clock, you use the command

A. ntpd -clock
B. ndtime
C. hwdate
D. ntpdate

Answer: A

Explanation: The ntpd program s an operating system daemon which sets and maintains the system time of day in synchronism with Internet Standard time servers. ntpd -clock command shows the current time set by NTP.

QUESTION NO: 8
The _____ command is used to print out the current date and time on the system.

Answer: date
Explanation: date command is used to set or display the system date and time.
#date -s "new date and time" : It sets the new date and time into system

QUESTION NO: 9
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

Answer: hwclock
Explanation: hwclock command query and sets the hardware clock.

Topic 7, (112) Networking Fundamentals (71 Questions)

Section 1, (1.112.1) Fundamentals of TCP/IP (38 Questions)

* Description: Candidates should demonstrate a proper understanding of network fundamentals. This objective includes the understanding of IP-addresses, network masks and what they mean (i.e. determine a network and broadcast address for a host based on its subnet mask in "dotted quad" or abbreviated notation or determine the network address, broadcast address and netmask when given an IP-address and number of bits). It also covers the understanding of the network classes and classless subnets (CIDR) and the reserved addresses for private network use. It includes the understanding of the function and application of a default route. It also includes the understanding of basic internet protocols (IP, ICMP, TCP, UDP) and the more common TCP and UDP ports (20, 21, 23, 25, 53, 80, 110, 119, 139, 143, 161).

***Key files, terms, and utilities** include:

/etc/services

ftp

telnet

host
ping
dig
traceroute
whois

QUESTION NO: 1
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

Answer: C
Explanation: The whois service of web site shows more information regarding the web site i.e owner of site, contact information. There are lots of sites provides the whois service i.e www.dnsstuff.com

QUESTION NO: 2
Which protocol is used for the majority of the ping command's actions?

A. ICMP
B. UDP
C. TCP
D. NDP
E. NCP

Answer: A
Explanation:
ICMP works at the Network layer and is used by IP for many different services. ICMP is a management protocol and messaging service provider for IP. Its messages are carried as IP datagrams. RFC 1256 is an annex to ICMP, which affords hosts' extended capability in discovering routes to gateways. Ping checks the network connectivity using the ICMP protocol.

QUESTION NO: 3
Which protocol is used by ping?

A. TCP
B. UDP
C. SMB
D. ICMP
E. OSPF

Answer: D
Explanation:
ICMP works at the Network layer and is used by IP for many different services. ICMP is a management protocol and messaging service provider for IP. Its messages are carried as IP datagrams. RFC 1256 is an annex to ICMP, which affords hosts' extended capability in discovering routes to gateways. Ping checks the network connectivity using the ICMP protocol.

QUESTION NO: 4
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. nsloopup
D. ifconfig
E. traceroute

Answer: E
Explanation: traceroute command shows the local and remote routing path to reach on destination.
#traceroute www.yahoo.com

QUESTION NO: 5
In the following output, which 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. The 192.168.1.1 is the default gateway

Answer: B

QUESTION NO: 6CORRECT TEXT
You build and configured a bastion host to act as a router between two internal networks. Both eth0 and eth1 can see hosts on their respective networks, but the hosts on each network cannot see any hosts on the other network. After verifying that the hosts have the correct gateway route, you decide the bastion host does not have IP forwarding turned on. Which command would you type to check this cat the file `/proc/sys/net/ipv4/ _____ to ensure it has a 1?`

Answer: ip_forward
Explanation: Router forwards the packets from one network to another network. If you would like to make the Linux system as a router, you need to enable the IP forwarding. To enable for current session
#echo "1" >/proc/sys/net/ipv4
To enable automatically at boot time
#vi /etc/sysctl.conf
net.ipv4.ip_forward=1
Where 1 means enable and 0 means disable the ip forwarding.

QUESTION NO: 7
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 192.168.1.1 eth0

Answer: D
Explanation: route command is used to manipulate the routing table in Linux.
#route -n or netstat -rn : Shows the routing table
#route add -net remote_network netmask gw gateway : which sets the gateway for remote network.
#route add default gw gateway : Which sets the default gateway for all network

QUESTION NO: 8CORRECT TEXT
What command will most effectively track a network path problem?

Answer: traceroute

Explanation: traceroute command shows the local and remote routing path to reach on destination.
#traceroute www.testking.com : Which shows the local and remote routing path to reach to testking.com

QUESTION NO: 9CORRECT TEXT
What program will determine basic connectivity to a remote host? Type just the name of the program.

Answer: ping
Explanation: ping command is used to check the basic connectivity to a remote host. Ping command uses the ICMP protocol to communicate.
 # ping remotehost
 # ping -c 5 remotehost

QUESTION NO: 10
Which of the following options will speed up traceroute for distant network queries?

A. -n
B. -p
C. -0
D. -t
E. -q

Answer: A

QUESTION NO: 11
Which ports are used for FTP data and control? Choose Two.

A. 20
B. 23
C. 22
D. 21
E. 25

Answer: A, D
Explanation: FTP (File Transfer Protocol) uses 20 and 21 ports. Where 21 for authentication and 20 is for data transfer.
You can check the uses port in /etc/services file.

QUESTION NO: 12
Which of the following IP address ranges are considered private, according to RFC 1918? Choose all that apply.

A. 10.0.0.0 - 10.255.255.255
B. 192.168.0.0 - 192.168.255.255
C. 172.16.0.0 - 172.31.255.255
D. 191.168.16.0 - 192.168.31.255
E. 172.16.0.0 - 172.16.255.255

Answer: A, B, C
Explanation: Private IP Address on different class
Class A 10.0.0.0 through 10.255.255.255

Class B 172.16.0.0 through 172.31.255.255

Class C 192.168.0.0 through 192.168.255.255

QUESTION NO: 13
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

Answer: A
Explanation:
Example of Binary ConverationTo understand IP addressing, you must first understand binary. Binary is a computer language that is represented by a bit value of 0 or 1. A 32-bit binary address would resemble 10101010101010101010101010101010. Those 32 bits can be grouped into 4 octets, or 10101010 10101010 10101010 10101010, for conversion to decimal format. When the bit value is 1, the bit is considered to be on and you can calculate its binary value depending on its placement within the binary octet. When the bit value is 0, the bit is off and has no corresponding binary value. Figure 4.1 displays the binary value and the calculated decimal value of each bit within an octet. Notice that the binary value increases exponentially.

Figure 4.1. A list of binary and decimal conversion values.

Binary Value	27	26	25	24	23	22	21	20
Decimal Value	128	64	32	16	8	4	2	1

Converting Binary to DecimalBy using the value calculated for each bit you can easily convert to decimal format. Line up the binary octet with the decimal value that was calculated in Figure 4.1. To calculate the total decimal value of each octet, you would add up the binary value of each bit that is on (1).
The example in Table 4.1 uses binary octet 00000000.

Table 4.1. Example #1 of a Binary-to-Decimal Conversion

Bit Value	0	0	0	0	0	0	0	0
Decimal Value	128	64	32	16	8	4	2	1

In this case, all the bit values are off (0), so there is no corresponding decimal value. The IP address octet value is also 0.
Table 4.2 uses binary octet 00010001.

Table 4.2. Example #2 of a Binary-to-Decimal Conversion

Bit Value	0	0	0	1	0	0	0	1
Decimal Value	128	64	32	16	8	4	2	1
				16				1

In this example, the fourth and last bit values are 1. Add the decimal values to get the total decimal value of that octet. That is, the total decimal value = 17 (16 + 1).
Table 4.3 uses binary octet 11111111.

Table 4.3. Example #3 of a Binary-to-Decimal Conversion

Bit Value	1	1	1	1	1	1	1	1
Decimal Value	128	64	32	16	8	4	2	1
	128	64	32	16	8	4	2	1

In Table 4.3, the total decimal value = 255 (128 + 64 + 32 + 16 + 8 + 4 + 2 + 1).
In this case, all the bit values are on (1), so all the decimal values are added together to calculate the IP address octet. The IP address octet value is 255.
Now, you can convert a 32-bit binary address into a dotted decimal address. In this example the binary address is 10101010 01010101 11000011 00111100. Start with the first octet 10110000. Table 4.4 shows the conversion of 10101010 from binary to decimal value.

Table 4.4. Binary-to-Decimal Conversion of 10101010

Bit Value	1	0	1	1	0	0	0	0
Decimal Value	128	64	32	16	8	4	2	1
	128		32	16				

In Table 4.4, the total decimal value = 176 (128 + 32 + 16).
The second octet is 01010101. Table 4.5 shows the conversion of 01010101 from binary to decimal value.

Table 4.5. Binary-to-Decimal Conversion of 01010101

Bit Value	0	1	0	1	0	1	0	1
Decimal Value	128	64	32	16	8	4	2	1
		64		16		4		1

In Table 4.5, the IP octet value = 85 (64 + 16 + 4 + 1).
The third octet is 11000011. Table 4.6 shows the conversion of 11000011 from binary to decimal value.

Table 4.6. Binary-to-Decimal Conversion of 11000011

Bit Value	1	1	0	0	0	0	1	1
Decimal Value	128	64	32	16	8	4	2	1
	128	64					2	1

In Table 4.6, the total decimal value = 195 (128 + 64 + 2 + 1)
The fourth and final octet is 00111100. Table 4.7 shows the conversion of 00111100 from binary to decimal value.

Table 4.7. Binary-to-Decimal Conversion of 00111100

Bit Value	0	0	1	1	1	1	0	0
Decimal Value	128	64	32	16	8	4	2	1
			32	16	8	4		

In Table 4.7, the total decimal value = 60 (32 + 16 + 8 + 4).
Based on these calculations, the IP address in dotted decimal format is 176.85.195.60.

QUESTION NO: 14
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

Answer: B
Explanation: Services uses the TCP/UDP port to communication with client.
Imap uses 143, pop3 uses 110 pop2 uses 109, smtp uses 25 etc port.

QUESTION NO: 15
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

Answer: A, E
Explanation: Private IP Address on different class
Class A 10.0.0.0 through 10.255.255.255
Class B 172.16.0.0 through 172.31.255.255
Class C 192.168.0.0 through 192.168.255.255

QUESTION NO: 16
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

Answer: D

Subnet MasksSub-networks

(subnets) enable you to break a large network of IP addresses down into smaller, manageable address ranges. A smaller address range means fewer hosts on a network. Each subnet becomes a separate broadcast domain. All the devices that are in the same broadcast domain receive all broadcasts. Think if it were possible to have all 16,777,214 Class A network hosts sharing a broadcast domain and receiving all broadcasts. That would be a huge amount of traffic. Subnets enable you to break this large network into smaller address ranges. In this case, smaller is better.
A subnet mask is used to identify which part of an IP address is the network portion. Like the IP address itself, a subnet mask consists of 32 bits. The network portion is represented by all 1s.
The default subnet masks for Class A, Class B, and Class C networks are as follows:
* **Class A 255.0.0.0 (11111111 00000000 000000000 000000000)**
* **Class B 255.255.0.0 (111111111 1111111111 000000000 000000000)**
* **Class C 255.255.255.0 (111111111 1111111111 111111111 0000000000)**

QUESTION NO: 17
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

Answer: C, D
Explanation The address 192.168.x.x and 172.16.x.x are well known internal use addresses. 172.16 is a Class B IP number. 169.254 is an class B internal use IP number This IP range is also uses by Microsoft, then known as APIPA addresses when no DHCP address can be provided.

QUESTION NO: 18CORRECT TEXT
With a Class C address, and a subnet mask of 255.255.255.0, how many host addresses are assignable?

Answer: 254
Explanation: Class C addresses uses 24 bits for network and 8 bits for host address. So the number of host in one network is 28-2=254

QUESTION NO: 19CORRECT TEXT
Your IP address is 1.2.3.3. Which command would add a default gateway using the network 1.2.3.4?

Answer: route add default gw 1.2.3.4

Explanation: route command is used to manipulate the routing table in Linux.
#route -n or netstat -rn : Shows the routing table
#route add -net remote_network netmask gw gateway : which sets the gateway for remote network.
#route add default gw gateway : Which sets the default gateway for all network

QUESTION NO: 20CORRECT TEXT
Your IP address is 170.35.13.28 and your network mask is 255.255.255.192. What host IP address is NOT a 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

Type in just the letter of the answer:

Answer: B
Explanation: Subnetmask is 255.255.255.192
Network ID is : 256-192=64
64 host can belongs to one subnet but usable hosts are 62. First Subnet is 1-64 So B is correct answer.

QUESTION NO: 21
There is any entry like the following in the file `/etc/ftpusers`:

```
#root
```

Will root be allowed to connect via ftp to this host?

A. Yes
B. No
C. It depends

Answer: A
Explanation:
Explanation can be found in man ftpusers:

"NAME

ftpusers - list of users that may not log in via the FTP daemon

DESCRIPTION

The text file ftpusers contains a list of users that may not log in using the File Transfer Protocol (FTP) server daemon. This file is used not merely for system administration purposes but for improving security within a TCP/IP networked environment. It will typically contain a list of the users that either have no business using ftp or have too many privileges to be allowed to log in through the FTP server daemon. Such users usually include root, daemon, bin, uucp, and news. If your FTP server daemon doesn't use ftpusers then it is suggested that you read its documentation to find out how to block access for certain users. Washington University FTP server Daemon (wuftpd) and Professional FTP Daemon (proftpd) are known to make use of ftpusers.

FORMAT

The format of ftpusers is very simple. There is one account name (or user name) per line. Lines starting with a # are ignored."

QUESTION NO: 22CORRECT TEXT
To find the port used by a particular known service, you would look in what file? Type the full path and name of the file.

Answer: /etc/services

Explanation: /etc/services file contains the port of services. You can find out the details of protocol, port number of services.
tcpmux 1/tcp
tcpmux 1/udp
rje 5/tcp
rje 5/udp
echo 7/tcp
echo 7/udp

QUESTION NO: 23
What system file contains definitions of well known ports, their associated services and protocols?

A. /etc/services
B. /etc/sysconfig/network-scripts
C. /etc/services.conf
D. /etc/inet/hosts
E. None of the choices

Answer: A
Explanation: /etc/services file contains the port of services. You can find out the details of protocol, port number of services.
tcpmux 1/tcp
tcpmux 1/udp
rje 5/tcp
rje 5/udp
echo 7/tcp
echo 7/udp

QUESTION NO: 24

Select from the list below the daemons that are present on a standard Linux server to support routing. Choose all that apply.

A. gated
B. ripd
C. routed
D. ospfd
E. bgpd

Answer: B, C, D, E

Explanation: zebra provides services to support different routing protocol. Ripd is the daemon if RIP, ospfd is the service of ospf, bgpd is the service of BGP routing protocol.

QUESTION NO: 25
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.

Answer: C
Explanation: Simple Mail Transport Protocol is used to send mail to mail server, which uses the 25 TCP port number. While configuring the DNS needs to specify the mail exchanger of domain using MX record.
@ IN MX 5 mail.example.com.
@ IN MX 10 mail1.example.com.
Where mail.example.com is the primary mail exchanger of the domain and mail1.example.com is the secondary mail exchanger of domain.

QUESTION NO: 26
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.

Answer: C,D
Explanation: IP address classified into different classes. Class A, B, C, D and E. Among all these classes only class A, B C are usable and Class D use to Broad Cast and E for Research.
Class A: 1.0.0.0 to 127.255.255.255 where 10.0.0.0 to 10.255.255.255 is Private IP as well 127 reserve for Loopback.
Class B: 128.0.0.0 to 191.255.255.255 Where 172.168.0.0 to 172.31.255.255 is Private IP
Class C: 192.0.0.0 to 223.255.255.255 where 192.168.0.0 to 192.168.255.255 is Private IP
Class D: 224.0.0.0 to 239.255.255.255 called Multicasting Address
Class E : 240.0.0.0 to 254.255.255.255 Reserved For Research.

QUESTION NO: 27
Which IP protocol is connectionless and unreliable?

Answer: UDP
Explanation: UDP provides a service for applications to exchange messages. Unlike TCP, UDP is connectionless and provides no reliability, no windowing, and no reordering of the received data. However, UDP provides some functions of TCP, such as data transfer, segmentation, and multiplexing using port numbers, and it does so with fewer bytes of overhead and with less processing required.

QUESTION NO: 28
The _____ file maps TCP and UDP ports to common resources.

Answer: /etc/services
Explanation: /etc/services file maps the TCP/UDP ports to common resources. See the example
tcpmux 1/tcp
tcpmux 1/udp
rje 5/tcp
rje 5/udp
echo 7/tcp

echo 7/udp
FTP services uses the port 21 and 20, telnet 23, ssh 22, smtp 25 pop3 110 etc maps that port to services in /etc/services file

QUESTION NO: 29
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

Answer: C
Explanation: IP address classified into different classes. Class A, B, C, D and E. Among all these classes only class A, B C are usable and Class D use to Broad Cast and E for Research.
Class A: 1.0.0.0 to 127.255.255.255 where 10.0.0.0 to 10.255.255.255 is Private IP as well 127 reserve for Loopback.
Class B: 128.0.0.0 to 191.255.255.255 Where 172.168.0.0 to 172.31.255.255 is Private IP
Class C: 192.0.0.0 to 223.255.255.255 where 192.168.0.0 to 192.168.255.255 is Private IP
Class D: 224.0.0.0 to 239.255.255.255 called Multicasting Address
Class E : 240.0.0.0 to 254.255.255.255 Reserved For Research.

According to question subnetted by 26 bits so 11000000 6 bits for hosts address
Number of usable IP Address on one subnet is : 26-2 = 62
So First IP Address is for router and remaining 61 IP Addresses can assign to host.

QUESTION NO: 30
Which of the following lines would you expect to see in the file /etc/services?

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

Answer: C
Explanation: /etc/services file maps the TCP/UDP ports to common resources. See the example
tcpmux 1/tcp
tcpmux 1/udp
rje 5/tcp
rje 5/udp
echo 7/tcp
echo 7/udp
FTP services uses the port 21 and 20, telnet 23, ssh 22, smtp 25 pop3 110 etc maps that port to services in /etc/services file

tftp service runs on port 69 so, that entry has written in /etc/services file.

QUESTION NO: 31
What is the name of standard Linux service which provide RIP (Routing Information Protocol)?

A. zebra
B. -routed
C. -ipchains

Answer: A
Explanation: zebra is the service, which provides the facility to use different Routing Protocol in Linux. i.e RIP, OSPF etc

QUESTION NO: 32
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?

Answer: 61
Explanation:
32 bits of IP address minus 26 bits is 6 bits.
minus 1 for address of network
minus 1 for address of broadcast
minus 1 for address of router
2^6 - 3 = 61

QUESTION NO: 33
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

Answer: C
Explanation: By default Class C has 24 bits of network address so netmask is 255.255.255.0
11111111.11111111.11111111.0
Class A: 8 bits Network Address
11111111.0.0.0 : 255.0.0.0
Class B: 16 Bits Network Address
11111111.11111111.0.0 : 255.255.0.0

QUESTION NO: 34
Which of the following protocols uses two different network ports?

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

Answer: B
Explanation: FTP (File Transfer Protocol) is used to transfer the file. Which service uses the two different ports 20 and 21.

QUESTION NO: 35
What is the highest numbered TCP/IP port?

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

Answer: C

There are 65535 possible ports officially recognized.

Note: TCP uses the notion of port numbers to identify sending and receiving applications. Each side of a TCP connection has an associated 16-bit unsigned port number assigned to the sending or receiving application. Ports are categorized into three basic categories: well known, registered and dynamic/private. The well known ports are assigned by the Internet Assigned Numbers Authority (IANA) and are typically used by system-level or root processes. Well known applications running as servers and passively listening for connections typically use these ports. Some examples include: FTP (21), TELNET (23), SMTP (25) and HTTP (80). Registered ports are typically used by end user applications as ephemeral source ports when contacting servers, but they can also identify named services that have been registered by a third party. Dynamic/private ports can also be used by end user applications, but are less commonly so. Dynamic/private ports do not contain any meaning outside of any particular TCP connection.

QUESTION NO: 36
The following output shows an excerpt from a standard network configuration file:

time 37/tcp timserver
time 37/udp timeserver
rlp 39/udp resource # resource location
name 42/udp nameserver
whois 43/tcp nickname # usually to sri-nic
domain 53/tcp
domain 53/udp
mtp 57/tcp # deprecated
bootps 67/udp # bootp server
bootpc 68/udp # bootp client
tftp 69/udp

Which file could this be from?

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

Answer: D
Explanation: /etc/services file maps the TCP/UDP ports to common resources.

QUESTION NO: 37
Which TWO daemons may be used to support various routing protocols under Linux?

A. gated
B. ripd
C. ospfdm
D. bgpd
E. routed

Answer: A, E

QUESTION NO: 38
What is a line from the file /etc/host.conf?

A. order hosts,bind
B. 192.168.2.4 dns-server
C. hosts: files dns
D. mydomain test.com

Answer: A
Explanation: 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.

Section 2, (1.112.3) TCP/IP configuration and troubleshooting (20 Questions)

* Description: Candidates should be able to view, change and verify configuration settings and operational status for various network interfaces. This objective includes manual and automatic configuration of interfaces and routing tables. This especially means to add, start, stop, restart, delete or reconfigure network interfaces. It also means to change, view or configure the routing table and to correct an improperly set default route manually. Candidates should be able to configure Linux as a DHCP client and a TCP/IP host and to debug problems associated with the network configuration.

***Key files, terms, and utilities** include:

/etc/HOSTNAME or /etc/hostname
`/etc/hosts`
`/etc/networks`
`/etc/host.conf`

/etc/resolv.conf

/etc/nsswitch.conf

ifconfig

route

dhcpcd, dhcpclient, pump
host
hostname (domainname, dnsdomainname)
netstat
ping
traceroute
tcpdump
the network scripts run during system initialization.

QUESTION NO: 1CORRECT TEXT
What command will display the active connections and Unix domain sockets for a running Linux machine with networking configured? Type just the command to accomplish this.

Answer: netstat

Expanation: netstat command prints the network connections, routing tables, statistics, masquerade connections and multicast memberships.
#netstat -a : Shows both listening and non-listening sockets.
#netstat -l : Shows only listening sockets.
#netstat -p : Shows the PID and name of the program to which each socket belongs.

QUESTION NO: 2
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.

Answer: E

Expanation: netstat command prints the network connections, routing tables, statistics, masquerade connections and multicast memberships.
#netstat -a : Shows both listening and non-listening sockets.
#netstat -l : Shows only listening sockets.
#netstat -p : Shows the PID and name of the program to which each socket belongs.
E is the best answer.

QUESTION NO: 3CORRECT TEXT
You need to view the hardware address and IP address information for all of your configured and active interfaces. Type the simplest command string that will accomplish this.

Answer: ifconfig
Explanation: ifconfig command shows the information about the network devices ie. hardware address, ip address etc. By default ifconfig command shows only the enabled devices and ifconfig -a shows enabled as well as disabled devices.

QUESTION NO: 4CORRECT TEXT
To immediately stop a DDOS attack from 10.1.1.128, what can you do? Type the command with the necessary options and arguments.

Answer: route add 10.1.1.128 lo
Explanation: route command helps to manipulate the routing table in Linux.
#route -n : Shows the routing table
#route add -net remote_network netmask gw next_hop or connected_device_name
It adds the gateway for remote network. When adding the loopback in routing table it denies the DDOS attack on local machine.

QUESTION NO: 5
Your machine has two working NIC's with proper addresses. You want to split your network into two new subnets. What single command will accomplish this?

A. ifconfig
B. route
C. default

D. netstat
E. None of the choices

Answer: A
Explanation: Using ifconfig command can display the information of NIC card as well as can assign IP address on interface.
#ifconfig eth0 10.4.4.100 netmask 255.255.255.0 : Which assings the IP Address 10.4.4.100 with netmask 255.255.255.0 into first ethernet card.

QUESTION NO: 6
Your server has two fully functional NIC's with correct IP configuration. The server is not forwarding traffic between the NIC's. Which command string will set the cards to forward properly?

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

Answer: B

Explanation: IP Forwarding features enable the packets between networks. To use the linux system as a router box, needs to enable the IP forwarding.
/proc is called the virtual filesystem containing the information of running kernel. To modify the parameter of kernel in running state needs to modify from /proc.

#echo "1" >/proc/sys/net/ipv4/ip_forward : Which enables the IP Forwarding for current session. To enable automatically at next reboot also modify the parameter in /etc/sysctl.conf

net.ipv4.ip_forward=1

QUESTION NO: 8
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

Answer: C
Explanation: IP Forwarding features enable the packets between networks. To use the linux system as a router box, needs to enable the IP forwarding.
/proc is called the virtual filesystem containing the information of running kernel. To modify the parameter of kernel in running state needs to modify from /proc.

#echo "1" >/proc/sys/net/ipv4/ip_forward : Which enables the IP Forwarding for current session. To enable automatically at next reboot also modify the parameter in /etc/sysctl.conf

net.ipv4.ip_forward=1

QUESTION NO: 8
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

Answer: C, D, E
Explanation: dhclient is the DHCP client command, which sends the request to DHCP server for IP Address.

QUESTION NO: 9CORRECT TEXT
In what file can you configure your name server resolution queries to use the localhost first? Type the full path and name of the file.

Answer: /etc/nsswitch.conf
Explanation: nsswitch.conf called the system databases and name service switch configuration file. This specify the order of query. Example When you try to access the computer via name first it sends request to /etc/hosts file then only dns.
hosts: files dns : You can change the order if you want.
Similalry When user try to login on NIS or LDAP client machine, it tires to authenticate from local machine then only to NIS server.
Passwd: files nis ldap

QUESTION NO: 10CORRECT TEXT
Which local system networking file binds a hostname to an IP address? Type the full path and name of the file.

Answer: /etc/hosts

Explanation: /etc/hosts file bind a hostname into IP Address. This is a host file so needs to write in each and every host. So recommended only for small network. Where DNS is the central database no need to maps in each and every machine.
Example:
192.168.1.1 station1.example.com station1

QUESTION NO: 11CORRECT TEXT
To change your Ethernet interface eth0 to the IP address 10.4.4.100 with a default class C subnet mask, type the full command string to accomplish this.

Answer: ifconfig eth0 10.4.4.100 netmask 255.255.255.0
Explanation: ifconfig eth0 10.4.4.100 netmask 255.255.255.0
Alternative correct answer: ifconfig eth0 10.4.4.100 netmask 255.255.255.0 up
With the option up - you set these inferface active.

QUESTION NO: 12
What is the command most often used for configuring network interfaces?

Answer: ifconfig
Explanation: Using ifconfig command can display the information of NIC card as well as can assign IP address on interface.
#ifconfig eth0 10.4.4.100 netmask 255.255.255.0 : Which assings the IP Address 10.4.4.100 with netmask 255.255.255.0 into first ethernet card.

QUESTION NO: 13CORRECT TEXT
You wish to restart the network daemon on a Redhat Server. Type in the command and any arguments that to accomplish this without using any absolutes pathnames:

Answer: service network restart

Explanation: network daemon controls the network services on machine. When starting the network service it reads configuration from /etc/sysconfig/network as well as interface configuration files also.

QUESTION NO: 14 CORRECT TEXT
You wish to change you network settings permanently using a text/graphical tool. Type in the command to start this tool:

Answer: netconfig

Explanation: netconfig is a tool use to configuration network settings. Example: Assigning IP Addresses, Netmask, Gateway, DNS servers etc.

QUESTION NO: 15 CORRECT TEXT
Type in the name of the file including path of the static host name to IP address configuration file:

Answer: /etc/hosts

Explanation: /etc/hosts file bind a hostname into IP Address. This is a host file so needs to write in each and every host. So recommended only for small network. Where DNS is the central database no need to maps in each and every machine. Example:

192.168.0.254 server1.example.com server1

QUESTION NO: 16
Which of the following lines would you find the file /etc/hosts?

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

Answer: B
Explanation: /etc/hosts file naps the name of host to IP address. You need to map in each and every host.
Example:
192.168.0.254 server1.example.com server1
which maps the server1.example.com or server1 into 192.168.0.254.

QUESTION NO: 17
Which of these are name resolution related files? (Choose two)

A. /etc/hosts
B. /etc/hsswitch.conf
C. /etc/lmhosts
D. /etc/man
E. /etc/resolv.conf

Answer: A,E
Explanation: /etc/hosts and /etc/resolv.conf file used to resolve the name.
/etc/hosts is called the static file to map name, on each and every hosts you should manually update.
Example: 192.168.0.5 station5.example.com station5 : Which maps the 192.168.0.5 into station5.example.com bu you should write this information on each and every hosts.

/etc/resolv.conf : where we specified the name server.
Example: nameserver 192.168.0.1
When user try to access the host, it goes to nameserver to resolve and gets the maps name.

QUESTION NO: 18
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 lo0
0.0.0.0 192.168.165.1 0.0.0.0 UG eth0

What is the default gateway for the network?

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

Answer: A
Explanation: when you use the netstat -nr or route -n command it prints the routing table configured in your linux system.
0.0.0.0 192.168.165.1 UG 0 0 eth0 Where 192.168.165.1 is the default gateway for all network and packets goes through eth0 interface.

QUESTION NO: 19
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

Answer: C
Explanation: ifconfig is used to configure the kernel-resident network interfaces. It is used at boot time to set up interfaces as necessary.
ifconfig : display the layer 2 and layer 3 information of all enabled interfaces.
ifconfig eth1 : displays thelayer 2 and layer 3 information of eth1 interfaces.

QUESTION NO: 20
You can run the _____ command to see active network and UNIX domain socket connection.

Answer: netstat
Explanation: netstat is the multi-purpose command use to print network connetions, routing tables, interface statistics, masquerade connections and multicast memberships.
netstat -sTU : prints all TCP and UDP ports used and being used.

Section 3, (1.112.4) Configure Linux as a PPP client (13 Questions)

* Description: Candidates should understand the basics of the PPP protocol and be able to configure and use PPP for outbound connections. This objective includes the definition of the chat sequence to connect (given a login example) and the setup commands to be run automatically when a PPP connection is made. It also includes initialization and termination of a PPP connection, with a modem, ISDN or ADSL and setting PPP to automatically reconnect if disconnected.

***Key files, terms, and utilities**include:

/etc/ppp/options.*

`/etc/ppp/peers/*`

`/etc/wvdial.conf`

/etc/ppp/ip-up

/etc/ppp/ip-down

wvdial

pppd

QUESTION NO: 1
What command could you use to confirm function of a ppp connection before establishing it?

A. minicom
B. hyperterminal
C. setserial
D. modemset
E. None of the choices

Answer: A

Explanation: minicom is a communication program which somewhat resembles the shareware program TELIX but is free with source code.
To run minicom
#minicom
To setup

#minicom -s

QUESTION NO: 2
Select all of the protocols that are supported by the Linux implementation of ppp.

A. chap
B. mschap
C. pap
D. spap
E. eap

Answer: A, B, C
Explanation:

PAP PAP is the less secure of the two methods. Passwords are sent in clear text, and PAP is
only performed upon the initial link establishment. When the PPP link is first established, the
remote node sends the username and password back to the sending router until authentication
is acknowledged. That's it.
CHAP CHAP is used at the initial startup of a link and at periodic checkups on the link to
make sure the router is still communicating with the same host.
After PPP finishes its initial phase, the local router sends a challenge request to the remote
device. The remote device sends a value calculated using a one-way hash function called MD5.
The local router checks this hash value to make sure it matches. If the values don't match, the
link is immediately terminated.

QUESTION NO: 3
What ppp option governs how long an interrupted connection will remain down before it attempts to reconnect?

A. holddown
B. holdoff

C. inactive
D. delay
E. wait

Answer: B

QUESTION NO: 4
When using the PPP daemon make a connection, what option is set to configure it to use hardware flow control?

A. crtscts
B. rsync
C. nsync
D. connect

Answer: A

QUESTION NO: 5
When using pppd which authentication protocol is the most secure?

A. clear text
B. PAP
C. CHAP
D. LAP

Answer: C
Explanation:
PAP PAP is the less secure of the two methods. Passwords are sent in clear text, and PAP is only performed upon the initial link establishment. When the PPP link is first established, the
remote node sends the username and password back to the sending router until authentication
is acknowledged. That's it.
CHAP CHAP is used at the initial startup of a link and at periodic checkups on the link to

make sure the router is still communicating with the same host.
After PPP finishes its initial phase, the local router sends a challenge request to the remote device. The remote device sends a value calculated using a one-way hash function called MD5.
The local router checks this hash value to make sure it matches. If the values don't match, the
link is immediately terminated.

QUESTION NO: 6
According to the PPP HOWTO which piece of software could help you test a modem?

A. chat
B. dhcpd
C. minicom
D. Hylafax
E. netconfig

Answer: C
Explanation: minicom is a communication program which somewhat resembles the shareware program TELIX but is free with source code.
To run minicom
#minicom

QUESTION NO: 7
When using `/etc/ppp/peers/*` files, which of the following is `true:`

A. The /etc/ppp/options should be empty.
B. Any user can run pppd from the command line.
C. The dial-on-demand option cannot be used.
D. You must use chap authentication.

Answer: A

QUESTION NO: 8CORRECT TEXT
What command would help you test if your ppp connection was functional? Type just the command name.

Answer: minicom

Explanation: minicom is a communication program which somewhat resembles the shareware program TELIX but is free with source code.
To run minicom
#minicom

QUESTION NO: 9CORRECT TEXT
What is the exact, case-sensitive option that governs flow-control for the ppp daemon?

Answer: crtscts

QUESTION NO: 10
When using PAP and PPP, the /etc/ppp/pap-secrets file must be:

A. world-readbale.
B. readable only by the ppp user.
C. readable only by root.
D. readable and executable by user root and group ppp.

Answer: C
Explanation: By default permission of /etc/ppp/pap-secrets is:
-rw------- 1 root root 231 Jan 3 09:25 /etc/ppp/pap-secrets

QUESTION NO: 11
Which of the following PPP authentication protocols never sends a password in the clear?

A. PAM
B. PAP
C. PGP
D. CHAP

Answer: D

Explanation:
CHAP Challenge Handshake Authentication Protocol. A security feature supported on lines using PPP encapsulation that prevents unauthorized access. CHAP does not itself prevent unauthorized access; it merely identifies the remote end. The router or access server then determines whether that user is allowed access.

QUESTION NO: 12
Which of the following is used to establish a PPP link to another computer?

A. pppconn
B. linkppp
C. pppd
D. pppconf

Answer: C
Explanation: On Linux, PPP functionality is split into two parts: a kernel component that handles the low-level protocols (HDLC, IPCP, IPXCP, etc.) and the user space pppd daemon that handles the various higher-level protocols, such as PAP and CHAP. The current release of the PPP software for Linux contains the PPP

QUESTION NO: 13
The _____ file contains the system default options for the PPP daemon.

Answer: /etc/ppp/options
daemon pppd and a program named chat that automates the dialing of the remote system.

Topic 8, (113) Networking Services (101 Questions)

Section 1, (1.113.1) Configure and manage inetd, xinetd, and related services (13 Questions)

* Description: Candidates should be able to configure which services are available through inetd, use tcpwrappers to allow or deny services on a host-by-host basis, manually start, stop, and restart internet services, configure basic network services including telnet and ftp. Set a service to run as another user instead of the default in inetd.conf.

***Key files, terms, and utilities** include:

/etc/inetd.conf
`/etc/hosts.allow`
`/etc/hosts.deny`
`/etc/services`
`/etc/xinetd.conf`

```
/etc/xinetd.log
```

QUESTION NO: 1
To disable telnet service on a system, which action should you take?

A. Put NONE in /etc/telnet.allow
B. Remove the appropriate telnet 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

Answer: E
Explanation: inetd called 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 strt for each port.
Edit the inetd.conf file vi /etc/inetd.conf and disable services like telnet, ftp, exec, talk, ntalk imap pop2, pop3 etc

QUESTION NO: 2
On a default install of a Linux server, regardless of the distribution version, what are the easiest methods to disable telnet, but not uninstall or remove the service? Choose two.

A. Comment telnet out of the /etc/inetd.conf file
B. Delete the /etc/rc.d/init.d/telnet file
C. Rename all SXXtelnet links in the /etc/rc or /etc/rc.d directories
D. Run "chmod 554 /etc/xinetd.d/telnet"
E. Nothing, it's not enabled by default

Answer: A, E
Explanation: inetd called 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 strt for each port.
Edit the inetd.conf file vi /etc/inetd.conf and disable services like telnet, ftp, exec, talk, ntalk imap pop2, pop3 etc

When you comment on service it disable the services as well as telnet by default not enabled.

QUESTION NO: 3
Your DNS server needs to be configured for speed and security. Choose the best answer.

A. Disable inetd, run named standalone, only allow tcp on ports 25 and 53
B. Disable inetd, run named standalone, only allow tcp on ports 25 and 110
C. Enable inetd, run named as an inetd service, only allow tcp on ports 25 and 53
D. Disable inetd, run named as a standalone on the apache server.

Answer: A
Explanation: inetd called 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 strt for each port. So run the named service standalone using service servicename start|restart. Named service uses the 53 ports and tcp, udp protocol.

QUESTION NO: 4
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

Answer: A
Explanation: inetd called 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 strt for each port.
Edit the inetd.conf file vi /etc/inetd.conf and disable services like telnet, ftp, exec, talk, ntalk imap pop2, pop3 etc

QUESTION NO: 5

You decide to use xinetd instead of inetd.
What must be done in order to properly configure xinetd?

A. You must create a new configuration file for xinetd.
B. You must add xinetd to /etc/services.
C. You must add xinetd support to your tcpwrappers configuration files.
D. Nothing, xinetd uses the same configuration files as inetd.

Answer: D
Explanation: inetd service is replaced by xinetd
/etc/xinetd.conf is the configuration file for xinetd service and all transient daemons are located in /etc/xinetd.d/.

QUESTION NO: 6
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.

Answer: B
Explanation: Both use the same configuration file.

QUESTION NO: 7CORRECT TEXT
Converting from the inetd to xinetd services requires populating entries in what file, including the full path and name?

Answer: /etc/xinetd.conf
Explanation:
/etc/xinetd.conf is the configuration file for xinetd service and all transient daemons are located in /etc/xinetd.d.

QUESTION NO: 8CORRECT TEXT
What is the command to check the syntax of your /etc/inetd.conf?

Answer: tcpdchk
Explanation: tcpdchk examines your tcp wrappers configuration and reports all potential and real problem it can find. The program examines the tcpd access control files and compares the entries in these files against entries in the inetd or tlid network configuration files.

QUESTION NO: 9CORRECT TEXT
What command can you use to determine the users connected to a Linux ftp server? Type just the command to accomplish this.

Answer: ftpwho
Explanation: ftpwho command shows process information for all active proftpd connections and a count of all connected users off of each server. Proftpd sessions spawned from inetd are counted separately from those created by a master proftpd standalone server.

QUESTION NO: 10CORRECT TEXT
What is the file that contains the settings and conversion parameters for the ftp server? Type in the name of the file only:

Answer: ftpconversions
Explanation: /etc/ftpconversions file contains instructions that permit you to compress files on demand before the transfer.

QUESTION NO: 11
What configuration file is used for settings and conversion parameters for the ftp daemon?

A. ftpusers
B. ftpconvert
C. ftpconversions
D. in.ftpd
E. ftpdefaults

Answer: C
Explanation: /etc/ftpconversions file contains instructions that permit you to compress files on demand before the transfer.

QUESTION NO: 12CORRECT TEXT
What file is used to define a list of users that may NOT login to via the ftp daemon? Type just the name of the file.

Answer: ftpusers
Explanation: /etc/ftpusers file listing users to be disallowed ftp login privileges. Each ftpusers entry is a single line of username

QUESTION NO: 13
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.

Answer: D, E

Explanation: inetd called 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 strt for each port. So run the named service standalone using service servicename start|restart. Named service uses the 53 ports and tcp, udp protocol.

Section 2, (1.113.2) Operate and perform basic configuration of sendmail (15 Questions)

* Description: Candidate should be able to modify simple parameters in sendmail configuration files (including the "Smart Host" parameter, if necessary), create mail aliases, manage the mail queue, start and stop sendmail, configure mail forwarding and perform basic troubleshooting of sendmail. The objective includes checking for and closing open relay on the mailserver. It does not include advanced custom configuration of Sendmail.

***Key files, terms, and utilities** include:

/etc/aliases or /etc/mail/aliases

`/etc/mail/*`

`~/.forward`

mailq

sendmail

newaliases

QUESTION NO: 1
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

Answer: B
Explanation: Setting up .forward files is particularly useful in situations where you have more than one account on ACS systems or your account exists on more than one mail server and you want to direct all your mail to one account on one server. Place identical .forward files in all your accounts except for the account in which you intend to read maill.
Example:
#vi .forward
user1@example.com

QUESTION NO: 2CORRECT TEXT
What command with options and arguments will display the mail servers for lpi.org?

Answer: dig lpi.org mx
Answer: dig lpi.org MX

Explanation:
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. Other lookup tools tend to have less functionality than dig.

A typical invocation of dig looks like:
dig @server name type

QUESTION NO: 3
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`

Answer: A
Explanation:
The /etc/aliases file contains the required aliases for the sendmail command. Do not change these defaults, as they are required by the system. The file is formatted as a series of lines in the form:
name:name_1,name_2,name_3,...
The name: is the name of the alias, and the name_n are the aliases for that name. Lines beginning with white space are continuation lines. Lines beginning with a # (pound sign) are comments.

Aliasing occurs only on local names. System-wide aliases are used to redirect mail. For example, if you receive mail at three different systems, you can use the /etc/aliases file to redirect your mail to one of the systems. As an individual user, you can also specify aliases in your .mailrc file.
Aliases can be defined to send mail to a distribution list. For example, you can send mail to all of the members of a project by sending mail to a single name.
The sender of a message is not included when the sendmail command expands an alias address. For example, if amy sends a message to alias D998 and she is defined as a member of that alias, the sendmail command does not send a copy of the message to amy.
The /etc/aliases file is a raw data file; the actual aliasing information is placed into a binary format in the /etc/aliasesDB/DB.dir and /etc/aliasesDB/DB.pag files by using the newaliases command. The newaliases command must be executed each time the aliases file is modified.

QUESTION NO: 4
What directory be default contains the delivered mail for each user?

A. `~/mail/`
B. `/usr/mail/`
C. `/var/mail/`
D. `/var/mail/spool/`
E. `/var/spool/mail/`

Answer: E
Explanation: /var/spool/mail is the default mail spoolin directory. Where you will find the username file containing the spooled mails.

QUESTION NO: 5
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.

Answer: B
Explanation:
The /etc/sendmail.cf configuration file contains the configuration information for the sendmail command. Information contained in this file includes such items as the host name and domain, and the sendmail rule sets.
The /etc/sendmail.cf file:
1. **Stores information about the type of mailer programs running.**
2. **Defines how the sendmail command rewrites addresses in messages.**
3. **Defines how the sendmail command operates in the following environments:**
4. 1. **Local mail delivery**
2. **Local area network delivery using TCP/IP**
3. **Remote delivery using Basic Utilities Network (BNU).**

QUESTION NO: 6
You are running an email server configured with the default settings.
In which directory will you found the delivered mail for the user foo?

A. `/var/spool/mail`
B. `/home/foo/mail`
C. `/var/mail/spool`
D. `/var/users/mail`

Answer: A
Explanation: /var/spool/mail is the default mail spoolin directory. you will find a file named foo in /var/mail/spool containing spool mails of foo.

QUESTION NO: 7CORRECT TEXT
What commands with any options, will cause sendmail to recognize newly added aliases while it's running?

Answer: sendmail -bi
Answer: newaliases
Explanation:

The /etc/aliases file contains the required aliases for the sendmail command. Do not change these defaults, as they are required by the system. The file is formatted as a series of lines in the form:
name:name_1,name_2,name_3,...
The name: is the name of the alias, and the name_n are the aliases for that name. Lines beginning with white space are continuation lines. Lines beginning with a # (pound sign) are comments.
Aliasing occurs only on local names. System-wide aliases are used to redirect mail. For example, if you receive mail at three different systems, you can use the /etc/aliases file to redirect your mail to one of the systems. As an individual user, you can also specify aliases in your .mailrc file.
Aliases can be defined to send mail to a distribution list. For example, you can send mail to all of the members of a project by sending mail to a single name.
The sender of a message is not included when the sendmail command expands an alias address. For example, if amy sends a message to alias D998 and she is defined as a member of that alias, the sendmail command does not send a copy of the message to amy.
The /etc/aliases file is a raw data file; the actual aliasing information is placed into a binary format in the /etc/aliasesDB/DB.dir and /etc/aliasesDB/DB.pag files by using the newaliases command. The **newaliases** command must be executed each time the aliases file is modified.

QUESTION NO: 8CORRECT TEXT
In what directory does undelivered remote mail get stored in? Type the full path and name of the file.

Answer: /var/spool/mqueue
Explanation: /var/spool/mqueue directory contains the remote undelivered mails.

QUESTION NO: 9CORRECT TEXT
Undelivered mail for local system users is stored in what directory? Type the full path of the directory.

Answer: /var/spool/mail/username
Explanation: /var/spool/mail is the default mail spoolin directory. Where you will find the username file containing the spooled mails.

QUESTION NO: 10
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

Answer: D
Explanation: /etc/aliases file is used to send the mail to different address then coming address.
Syntax: boob: peter : means mail of boob will get by peter. After modifying the file /etc/aliases you should re-build the database using newaliases command

QUESTION NO: 11 CORRECT TEXT
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?

Answer: newaliases
Explanation: /etc/aliases file is used to send the mail to different address then coming address.
Syntax: boob: peter : means mail of boob will get by peter. After modifying the file /etc/aliases you should re-build the database using newaliases command

QUESTION NO: 12
The _____ command prints a list of email that is currently in the queue waiting for delivery.

Answer: mailq
Explanation: mailq command prints a summary of mail messges queued for future delivery.
Syntax: mailq [options]
mailq -Ac : show the mail submission queue specified in /etc/mail/submit.cf instead of the MTA queue specified in /etc/mail/sendmail.cf

QUESTION NO: 13
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

Answer: C
Explanation: mailq command prints a summary of mail messges queued for future delivery.
Syntax: mailq [options]
mailq -Ac : show the mail submission queue specified in /etc/mail/submit.cf instead of the MTA queue specified in /etc/mail/sendmail.cf

QUESTION NO: 14

The user bob complains that he cannot access his email. In witch 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

Answer: A
Explanation: /var/spool/mail/ directory contains the user's spooling mail. If user unable to check the mail you should check the permission and owner of mail spooling file under /var/spool/mail

QUESTION NO: 15
When you run the command newaliasses, 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.

Answer: D
Explanation: /etc/aliases file is used to send the mail to different address then coming address.

Syntax: boob: peter : means mail of boob will get by peter. After modifying the file /etc/aliases you should re-build the database using newaliases command

Section 3, (1.113.3) Operate and perform basic configuration of Apache (17 Questions)

* Description: Candidates should be able to modify simple parameters in Apache configuration files, start, stop, and restart httpd, arrange for automatic restarting of httpd upon boot. Does not include advanced custom configuration of Apache.

***Key files, terms, and utilities** include:

httpd.conf

apachectl

httpd

QUESTION NO: 1
You are performing an onsite security inspection of division of your company. On an Apache server, you want to determine what files are needed and which can be removed from the /etc/httpd folder.
Which of the following are possibly valid Apache confguration files? Choose all that apply:

A. httpd.conf
B. apached.conf
C. srm.conf
D. access.conf
E. in.http.conf

Answer: A, C, D
Explanation:
Apache's configuration files reside in the directory /etc/httpd. For historical reasons that no longer apply, Apache has three configuration files:
access.conf
Specifies what hosts and users are allowed access to what documents and services
httpd.conf
Specifies options that govern the operation of the httpd daemon
srm.conf
Specifies how your server's documents and organized and formatted

QUESTION NO: 2
Which of the following files typically are used to configure Apache? (Choose two)

A. srm.conf
B. www.conf
C. `http.boot`
D. `httpd.conf`
E. `apache.conf`

Answer: A, D
Explanation:
Specifies what hosts and users are allowed access to what documents and services
httpd.conf
Specifies options that govern the operation of the httpd daemon
srm.conf
Specifies how your server's documents and organized and formatted

QUESTION NO: 3
You have a standard Apache web server installation and want to make it respond to requests on port 8088. To do this, what configuration file do you need to change?

A. None. This is the default port.
B. /etc/httpd/apache.conf
C. /etc/httpd/ports.conf
D. /etc/httpd/httpd.conf
E. /etc/httpd/access.conf

Answer: D
Explanation:
The httpd.conf file is the main configuration file for the Apache web server. A lot options exist, and it's important to read the documentation that comes with Apache for more information on different settings and parameters. The following configuration example is a minimal working configuration file for Apache, with SSL support. Also, it's important to note that we only comment the parameters that relate to security and optimization, and leave all the others to your own research.
Edit the httpd.conffile, vi /etc/httpd/conf/httpd.conf and add/change:

Section 1: Global Environment # ServerType standalone ServerRoot "/etc/httpd" PidFile /var/run/httpd.pid ResourceConfig /dev/null AccessConfig /dev/null Timeout 300 KeepAlive On MaxKeepAliveRequests 0 KeepAliveTimeout 15 MinSpareServers 16 MaxSpareServers 64 StartServers 16 MaxClients 512 MaxRequestsPerChild 100000 ### Section 2: 'Main' server configuration # Port 80 <IfDefine SSL> Listen 80 Listen 443 </IfDefine> User www Group www ServerAdmin admin@openna.com ServerName www.openna.com DocumentRoot "/home/httpd/ona" <Directory /> Options None AllowOverride None Order deny,allow Deny from all </Directory> <Directory "/home/httpd/ona"> Options None AllowOverride None Order allow,deny Allow from all </Directory> <Files .pl> Options None AllowOverride None Order deny,allow Deny from all </Files> <IfModule mod_dir.c> DirectoryIndex index.htm index.html index.php index.php3 default.html index.cgi </IfModule> #<IfModule mod_include.c> #Include conf/mmap.conf #</IfModule> UseCanonicalName On <IfModule mod_mime.c> TypesConfig /etc/httpd/conf/mime.types </IfModule> DefaultType text/plain HostnameLookups Off ErrorLog /var/log/httpd/error_log LogLevel warn LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined SetEnvIf Request_URI \.gif$ gif-image CustomLog /var/log/httpd/access_log combined env=!gif-image ServerSignature Off <IfModule mod_alias.c> ScriptAlias /cgi-bin/ "/home/httpd/cgi-bin/" <Directory "/home/httpd/cgi-bin"> AllowOverride None Options None Order allow,deny Allow from all </Directory> </IfModuleGT; <IfModule mod_mime.c> AddEncoding x-compress Z AddEncoding x-gzip gz tgz AddType application/x-tar .tgz </IfModule> ErrorDocument 500 "The server made a boo boo. ErrorDocument 404 http://192.168.1.1/error.htm ErrorDocument 403 "Access Forbidden -- Go away. <IfModule mod_setenvif.c> BrowserMatch "Mozilla/2" nokeepalive BrowserMatch "MSIE 4\.0b2;" nokeepalive downgrade-1.0 force-response-1.0 BrowserMatch "RealPlayer 4\.0" force-response-1.0 BrowserMatch "Java/1\.0" force-response-1.0 BrowserMatch "JDK/1\.0" force-response-1.0 </IfModule> ### Section 3: Virtual Hosts # <IfDefine SSL> AddType application/x-x509-ca-cert .crt AddType application/x-pkcs7-crl .crl </IfDefine> <IfModule mod_ssl.c> SSLPassPhraseDialog builtin SSLSessionCache dbm:/var/run/ssl_scache SSLSessionCacheTimeout 300 SSLMutex file:/var/run/ssl_mutex SSLRandomSeed startup builtin SSLRandomSeed connect builtin SSLLog /var/log/httpd/ssl_engine_log SSLLogLevel warn </IfModule> <IfDefine SSL> <VirtualHost _default_:443> DocumentRoot "/home/httpd/ona" ServerName www.openna.com ServerAdmin admin@openna.com ErrorLog /var/log/httpd/error_log SSLEngine on SSLCipherSuite ALL:!ADH:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL SSLCertificateFile /etc/ssl/certs/server.crt SSLCertificateKeyFile /etc/ssl/private/server.key SSLCACertificatePath /etc/ssl/certs SSLCACertificateFile /etc/ssl/certs/ca.crt SSLCARevocationPath /etc/ssl/crl SSLVerifyClient none SSLVerifyDepth 10 SSLOptions +ExportCertData +StrictRequire SetEnvIf User-Agent ".*MSIE.*" nokeepalive

This tells httpd.conffile to set itself up for this particular configuration setup with:

ServerType standalone

The option ServerType specifies how Apache should run on the system. You can run it from the super-server inetd, or as standalone daemon. It's highly recommended to run Apache in standalone type for better performance and speed.

ServerRoot "/etc/httpd"

The option ServerRoot specifies the directory in which the configuration files of the Apache server lives. It allows Apache to know where it can find its configuration files when it starts.

PidFile/var/run/httpd.pid

The option PidFile specifies the location where the server will record the process id of the daemon when it starts. This option is only required when you configure Apache in standalone mode.

ResourceConfig/dev/null

The option ResourceConfig specifies the location of the old srm.conf file that Apache read after it finished reading the httpd.conf file. When you set the location to /dev/null, Apache allows you to include the content of this file in httpd.conf file, and in this manner, you have just one file that handles all your configuration parameters for simplicity.

AccessConfig/dev/null

The option AccessConfig specifies the location of the old access.conf file that Apache read after it finished reading the srm.conf file. When you set the location to /dev/null, Apache allows you to include the content of this file in httpd.conf file, and in this manner, you have just one file that handles all your configuration parameters for simplicity.

Timeout 300

The option Timeout specifies the amount of time Apache will wait for a GET, POST, PUT request and ACKs on transmissions. You can safely leave this option on its default values.

KeepAlive On

The option KeepAlive, if set to On, specifies enabling persistent connections on this web server. For better performance, it's recommended to set this option to On, and allow more than one request per connection.

MaxKeepAliveRequests 0

The option MaxKeepAliveRequests specifies the number of requests allowed per connection when the KeepAlive option above is set to On. When the value of this option is set to 0then unlimited requests are allowed on the server. For server performance, it's recommended to allow unlimited requests.

KeepAliveTimeout 15

The option KeepAliveTimeout specifies how much time, in seconds, Apache will wait for a subsequent request before closing the connection. The value of 15 seconds is a good average for server performance.

MinSpareServers 16

The option MinSpareServers specifies the minimum number of idle child server processes for Apache, which is not handling a request. This is an important tuning parameter regarding the performance of the Apache web server. For high load operation, a value of 16 is recommended by various benchmarks on the Internet.

MaxSpareServers 64

The option MaxSpareServers specifies the maximum number of idle child server processes for Apache, which is not handling a request. This is also an important tuning parameter regarding the performance of the Apache web server. For high load operation, a value of 64 is recommended by various benchmarks on the Internet.

StartServers 16

The option StartServers specifies the number of child server processes that will be created by Apache on start-up. This is, again, an important tuning parameter regarding the performance of the Apache web server. For high load operation, a value of 16 is recommended by various benchmarks on the Internet.

MaxClients 512

The option MaxClients specifies the number of simultaneous requests that can be supported by Apache. This too is an important tuning parameter regarding the performance of the Apache web server. For high load operation, a value of 512 is recommended by various benchmarks on the Internet.

MaxRequestsPerChild 100000

The option MaxRequestsPerChild specifies the number of requests that an individual child server process will handle. This too is an important tuning parameter regarding the performance of the Apache web server.

User www

The option User specifies the UID that Apache server will run as. It's important to create a new user that has minimal access to the system, and functions just for the purpose of running the web server daemon.

Group www

The option Group specifies the GID the Apache server will run as. It's important to create a new group that has minimal access to the system and functions just for the purpose of running the web server daemon.

DirectoryIndex index.htm index.html index.php index.php3 default.html index.cgi

The option DirectoryIndex specifies the files to use by Apache as a pre-written HTML directory index. In other words, if Apache can't find the default index page to display, it'll try the next entry in this parameter, if available. To improve performance of your web server it's recommended to list the most used default index pages of your web site first.

Include conf/mmap.conf

The option Include specifies the location of other files that you can include from within the server configuration files httpd.conf. In our case, we include the mmap.conf file located under /etc/httpd/confdirectory. This file mmap.conf maps files into memory for faster serving. See the section on Optimizing Apache for more information.

HostnameLookups Off

The option HostnameLookups, if set to Off, specifies the disabling of DNS lookups. It's recommended to set this option to Off in order to save the network traffic time, and to improve the performance of your Apache web server

If you want to run the httpd service on different port, just change on listen parameter.

QUESTION NO: 4CORRECT TEXT

What file is used in recent apache distributions to configure the service? Type the full path and name of the file.

Answer: /etc/apache/httpd.conf

Answer: /etc/apache2/httpd.conf

Explanation: On new systems (since Suse Linux V9.0) are these the correct files.

On older systems (before Suse Linux V9.0) the apache config file is found in /etc/httpd.conf

QUESTION NO: 5

What configuration file and directive will alter your apache server IP and or port that it listens to?

A. Port
B. IPAddress
C. Listen
D. MinSpareServers

Answer: C

Explanation:

The httpd.conffile is the main configuration file for the Apache web server. A lot options exist, and it's important to read the documentation that comes with Apache for more information on different settings and parameters. The following configuration example is a minimal working configuration file for Apache, with SSL support. Also, it's important to note that we only comment the parameters that relate to security and optimization, and leave all the others to your own research.

Edit the httpd.conffile, vi /etc/httpd/conf/httpd.confand add/change:

Section 1: Global Environment # ServerType standalone ServerRoot "/etc/httpd" PidFile /var/run/httpd.pid ResourceConfig /dev/null AccessConfig /dev/null Timeout 300 KeepAlive On MaxKeepAliveRequests 0 KeepAliveTimeout 15 MinSpareServers 16 MaxSpareServers 64 StartServers 16 MaxClients 512 MaxRequestsPerChild 100000 ### Section 2: 'Main' server configuration # Port 80 <IfDefine SSL> Listen 80 Listen 443 </IfDefine> User www Group www ServerAdmin admin@openna.com ServerName www.openna.com DocumentRoot "/home/httpd/ona" <Directory /> Options None AllowOverride None Order deny,allow Deny from all </Directory> <Directory "/home/httpd/ona"> Options None AllowOverride None Order allow,deny Allow from all </Directory> <Files .pl> Options None AllowOverride None Order deny,allow Deny from all </Files> <IfModule mod_dir.c> DirectoryIndex index.htm index.html index.php index.php3 default.html index.cgi </IfModule> #<IfModule mod_include.c> #Include conf/mmap.conf #</IfModule> UseCanonicalName On <IfModule mod_mime.c> TypesConfig /etc/httpd/conf/mime.types </IfModule> DefaultType text/plain HostnameLookups Off ErrorLog /var/log/httpd/error_log LogLevel warn LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined SetEnvIf Request_URI \.gif$ gif-image CustomLog /var/log/httpd/access_log combined env=!gif-image ServerSignature Off <IfModule mod_alias.c> ScriptAlias /cgi-bin/ "/home/httpd/cgi-bin/" <Directory "/home/httpd/cgi-bin"> AllowOverride None Options None Order allow,deny Allow from all </Directory> </IfModuleGT; <IfModule mod_mime.c> AddEncoding x-compress Z AddEncoding x-gzip gz tgz AddType application/x-tar .tgz </IfModule> ErrorDocument 500 "The server made a boo boo. ErrorDocument 404 http://192.168.1.1/error.htm ErrorDocument 403 "Access Forbidden -- Go away. <IfModule mod_setenvif.c> BrowserMatch "Mozilla/2" nokeepalive BrowserMatch "MSIE 4\.0b2;" nokeepalive downgrade-1.0 force-response-1.0 BrowserMatch "RealPlayer 4\.0" force-response-1.0 BrowserMatch "Java/1\.0" force-response-1.0 BrowserMatch "JDK/1\.0" force-response-1.0 </IfModule> ### Section 3: Virtual Hosts # <IfDefine SSL> AddType application/x-x509-ca-cert .crt AddType application/x-pkcs7-crl .crl </IfDefine> <IfModule mod_ssl.c> SSLPassPhraseDialog builtin SSLSessionCache dbm:/var/run/ssl_scache SSLSessionCacheTimeout 300 SSLMutex file:/var/run/ssl_mutex SSLRandomSeed startup builtin SSLRandomSeed connect builtin SSLLog /var/log/httpd/ssl_engine_log SSLLogLevel warn </IfModule> <IfDefine SSL> <VirtualHost _default_:443> DocumentRoot "/home/httpd/ona" ServerName www.openna.com ServerAdmin admin@openna.com ErrorLog /var/log/httpd/error_log SSLEngine on SSLCipherSuite ALL:!ADH:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL SSLCertificateFile /etc/ssl/certs/server.crt SSLCertificateKeyFile /etc/ssl/private/server.key SSLCACertificatePath /etc/ssl/certs SSLCACertificateFile /etc/ssl/certs/ca.crt SSLCARevocationPath /etc/ssl/crl SSLVerifyClient none SSLVerifyDepth 10 SSLOptions

This tells httpd.conffile to set itself up for this particular configuration setup with:

ServerType standalone

The option ServerTypespecifies how Apache should run on the system. You can run it from the super-server inetd, or as standalone daemon. It's highly recommended to run Apache in standalone type for better performance and speed.

ServerRoot "/etc/httpd"

The option ServerRootspecifies the directory in which the configuration files of the Apache server lives. It allows Apache to know where it can find its configuration files when it starts.

PidFile /var/run/httpd.pid

The option PidFilespecifies the location where the server will record the process id of the daemon when it starts. This option is only required when you configure Apache in standalone mode.

ResourceConfig /dev/null

The option ResourceConfigspecifies the location of the old **srm.conffile that Apache read after it finished reading the httpd.conf**file. When you set the location to **/dev/null,Apache allows you to include the content of this file in httpd.conf**file, and in this manner, you have just one file that handles all your configuration parameters for simplicity.

AccessConfig /dev/null

The option AccessConfigspecifies the location of the old **access.conffile that Apache read after it finished reading the srm.conf**file. When you set the location to **/dev/null, Apache allows you to include the content of this file in httpd.conf**file, and in this manner, you have just one file that handles all your configuration parameters for simplicity.

Timeout 300

The option Timeoutspecifies the amount of time Apache will wait for a GET, POST, PUT request and ACKs on transmissions. You can safely leave this option on its default values.

KeepAlive On

The option KeepAlive, if set to **On, specifies enabling persistent connections on this web server. For better performance, it's recommended to set this option to On**, and allow more than one request per connection.

MaxKeepAliveRequests 0

The option MaxKeepAliveRequestsspecifies the number of requests allowed per connection when the **KeepAliveoption above is set to On.**When the value of this option is set to **0then unlimited requests are allowed on the server. For server performance, it's recommended to allow unlimited requests.**

KeepAliveTimeout 15

The option KeepAliveTimeoutspecifies how much time, in seconds, Apache will wait for a subsequent request before closing the connection. The value of **15seconds is a good average for server performance.**

MinSpareServers 16

The option MinSpareServersspecifies the minimum number of idle child server processes for Apache, which is not handling a request. This is an important tuning parameter regarding the performance of the Apache web server. For high load operation, a value of **16is recommended by various benchmarks on the Internet.**

MaxSpareServers 64

The option MaxSpareServersspecifies the maximum number of idle child server processes for Apache, which is not handling a request. This is also an important tuning parameter regarding the performance of the Apache web server. For high load operation, a value of **64is recommended by various benchmarks on the Internet.**

StartServers 16

The option StartServersspecifies the number of child server processes that will be created by Apache on start-up. This is, again, an important tuning parameter regarding the performance of the Apache web server. For high load operation, a value of **16is recommended by various benchmarks on the Internet.**

MaxClients 512

The option MaxClientsspecifies the number of simultaneous requests that can be supported by Apache. This too is an important tuning parameter regarding the performance of the Apache web server. For high load operation, a value of **512is recommended by various benchmarks on the Internet.**

MaxRequestsPerChild 100000

The option MaxRequestsPerChildspecifies the number of requests that an individual child server process will handle. This too is an important tuning parameter regarding the performance of the Apache web server.

User www

The option Userspecifies the UID that Apache server will run as. It's important to create a new user that has minimal access to the system, and functions just for the purpose of running the web server daemon.

Group www

The option Groupspecifies the GID the Apache server will run as. It's important to create a new group that has minimal access to the system and functions just for the purpose of running the web server daemon.

DirectoryIndex index.htm index.html index.php index.php3 default.html index.cgi

The option DirectoryIndexspecifies the files to use by Apache as a pre-written HTML directory index. In other words, if Apache can't find the default index page to display, it'll try the next entry in this parameter, if available. To improve performance of your web server it's recommended to list the most used default index pages of your web site first.

Include conf/mmap.conf

The option Includespecifies the location of other files that you can include from within the server configuration files **httpd.conf. In our case, we include the mmap.conf**file located under **/etc/httpd/confdirectory. This file mmap.conf**

maps files into memory for faster serving. See the section on **Optimizing Apache for more information.**

HostnameLookups Off

The option HostnameLookups, if set to **Off, specifies the disabling of DNS lookups. It's recommended to set this option to Off**in order to save the network traffic time, and to improve the performance of your Apache web server

QUESTION NO: 6
What Apache directive must you change when using inetd to control your Apache server?

A. ServerType
B. ServerInetd
C. InetServer
D. StartServer
E. ServerMethod

Answer: A
Explanation:

ServerType standalone

The option ServerTypespecifies how Apache should run on the system. You can run it from the super-server inetd, or as standalone daemon. It's highly recommended to run Apache in standalone type for better performance and speed.

QUESTION NO: 7
Which Apache Directive specifies the location of the HTTP documents?

A. RootDocument
B. ServerRoot
C. DocumentRoot
D. RootServer
E. DocPath

Answer: C

QUESTION NO: 8
What command can be used to shut down the Apache server gracefully?

A. apacheshut
B. apachectl
C. apachestop
D. apachestart

Answer: B
Explanation: But the option is missing.

QUESTION NO: 9
What is the recommended setting for StartServers in a medium sized Apache installation?

A. 5
B. 10
C. 15
D. 20

Answer: B

QUESTION NO: 10
How many spare server processes are required by Apache for the typical, low-to-moderate volume website?

A. 1
B. 50
C. 10
D. 200

Answer: C

QUESTION NO: 11
When an Apache server is configured to provide 10 spare server processes, which kind of website would it typically serve?

A. A low-to-moderate volume website
B. A website for no more than 10 users
C. A high volume web site
D. A one-user volume website

Answer: A

QUESTION NO: 12
You need to run a second Apache server on the same IP address. Which of the following is true?

A. You cannt run more than one Apache on one IP address.
B. You have to add a new entry in /etc/services.
C. The second Apache server must listen on an other port.
D. The second Apache must be a child process of the first.

Answer: A
Explanation: We can't run the more than one Web server on Same IP address.

QUESTION NO: 13 CORRECT TEXT
How to check is Apache's configuration file correct?

Answer: apachectl configtest

Explanation: apachectl is the Apache HTTP server control Interface. You can start, sopt, restart the httpd daemon as well as can check the configuration.
To check the configuration of httpd.conf use the : apachectl configtest
To restart the httpd daemon: apachectl restart

QUESTION NO: 14
The _____ command is the Apache HTTP server control interface.

Answer: apachectl
Explanation: apachectl is the Apache HTTP server control Interface. You can start, sopt, restart the httpd daemon as well as can check the configuration.
To check the configuration of httpd.conf use the : apachectl configtest

To restart the httpd daemon: apachectl restart

QUESTION NO: 15
The normal way of starting your Apache server would be the command:

A. apachectl start
B. http -start
C. inetd apache
D. apachestart -n
E. apache start

Answer: A
Explanation: apachectl is the Apache HTTP server control Interface. You can start, sopt, restart the httpd daemon as well as can check the configuration.
To start the httpd daemon: apachectl start

QUESTION NO: 16
What is the name of the primary configuration file for Apache?

A. srm.cfg
B. httpd.cfg
C. access.cfg
D. apache.conf
E. httpd.conf

Answer: E
Explanation: /etc/httpd/conf/httpd.conf is the primary configuration file for apache web server and /etc/httpd/conf.d/ssl.conf is the configuration file for HTTPS.

QUESTION NO: 17
You are a junior system engineer and have been asked to refresh the webpages for a busy website. You don't want to break the connections. What command can you use?

A. apachectl restart
B. apachectl reload
C. apachectl graceful
D. /etc/init.d/httpd restart

Answer: C
Explanation: Reload restarts the Apache daemon by sending it a SIGUSR1. If the daemon is not running, it is started. This differs from a normal restart in that currently open connections are not aborted. A side effect is that old log files will not be closed immediately.

Section 4, (1.113.4) Properly manage the NFS, smb, and nmb daemons (30 Questions)

* Description: Candidate should know how to mount remote filesystems using NFS, configure NFS for exporting local filesystems, start, stop, and restart the NFS server. Install and configure Samba using the included GUI tools or direct edit of the /etc/smb.conf file (Note: this deliberately excludes advanced NT domain issues but includes simple sharing of home directories and printers, as well as correctly setting the nmbd as a WINS client).

***Key files, terms, and utilities** include:

/etc/exports

`/etc/fstab`

`/etc/smb.conf`

mount

umount

QUESTION NO: 1
In order to allow a Win95 host to resolve the name of and map network drives to your Linux server, what services should be running? Choose Two.

A. nmbd
B. smbd
C. named
D. routed
E. winsd

Answer: A, B

QUESTION NO: 2
What is the simplest method to connect a Win98 host to a Linux Server?

A. Velcro
B. Samba
C. NFS
D. DNS
E. WINS

Answer: B

QUESTION NO: 3
What is true about the root user and NFS?

A. NFS shares don't allow root access by default
B. NFS automatically masks out share permissions
C. NFS automatically maps all root UID's to the local user "rootsquash"
D. NFS ignores all users with a UID of 0 and a GID of 0
E. NFS pays no attention whatsoever to security

Answer: A

QUESTION NO: 4
What configuration files on a Linux Server can be configured to share file systems with clients? Choose Two.

A. /etc/nmbd
B. /etc/smbd
C. /etc/smb/samba.conf
D. /etc/smb.conf
E. /etc/samba/smb.conf

Answer: D, E

QUESTION NO: 5
What command is used to monitor connections to the SMB server?

A. smbclient
B. testparm
C. smbstatus
D. smbstat

Answer: C

QUESTION NO: 6
What is the command to map a Windows user ID to a Linux user ID for use with the Samba Server?

A. smbuser
B. smbpasswd
C. smbadduser
D. useraddsmb
E. useradd

Answer: C

QUESTION NO: 7CORRECT TEXT
What file do you configure to make changes to your smbd and nmbd daemons? Type the full path and name of the file.

Answer: /etc/smb.conf
Answer: /etc/samba/smb.conf

QUESTION NO: 8CORRECT TEXT
Type in the command to monitor connections to Samba:

Answer: smbstatus

QUESTION NO: 9CORRECT TEXT
You wish to restart both Samba daemons. Type in the command and any arguments that to accomplish this without using any absolutes pathnames:

Answer: service smb restart

QUESTION NO: 10CORRECT TEXT
Type in the name of the samba daemon that is responsible for WINS names resolution

Answer: nmbd

QUESTION NO: 11
Which option in the /etc/fstab file causes all users IDs to be mapped to the system's anonymous ID when mounting a NFS mounted file system?

A. no-root-squash
B. all-squash
C. all-id-squash
D. root-squash

Answer: B

QUESTION NO: 12
Which fstab option governs that all root ID are mapped to anonymous ID when mounting a NFS mounted file system?

A. no-root-squash

B. root-squash
C. all-squash
D. squash-root

Answer: B

QUESTION NO: 13
This is a line from the file `/etc/export`:
```
/product testking(rw)
```

What does it mean?

A. Only user testking may access the filesystem /product when it is NFS mounted.
B. This computer will mount the filesystem /product on testking via NFS.
C. The filesystem /product is exported for NFS mount to computer testking.
D. All NFS access to /product will use suid testking.

Answer: C

QUESTION NO: 14
You are not using the WINS service on your network, but need to provide NETBIOS resolution to your hosts. What is the name of the daemon that provides these services on a Linux server?

A. nmbd
B. dns
C. winsd
D. lmhostsd
E. smbd

Answer: A

QUESTION NO: 15
These lines are taken from `/etc/smb.conf`:

```
 workgroup = group1
guest account = nobody
```

What else is needed for this to work?

A. nobody must be a valid group on the server.
B. nobody must be a user name listed in /etc/passwd.
C. group1 must be a valid group on the server.
D. workgroup must be a valid group on the server.

Answer: B

QUESTION NO: 16CORRECT TEXT
Type the command to check the syntax and contents of the smb.conf file:

Answer: testparm

QUESTION NO: 17CORRECT TEXT
Type in the name of the samba daemon that is responsible for printer and file sharing:

Answer: smbd

QUESTION NO: 18
Which daemon allows Linux to share its file systems and printers with unmodified Windows clients?

A. X Window
B. nmbd
C. smbd
D. WINS
E. NFS

Answer: C

QUESTION NO: 19
Shares can be configured for export via the NFS service by editing what file?

A. /etc/exports
B. /etc/export
C. /etc/exportfs
D. /etc/nfs/exports

Answer: A

QUESTION NO: 20 CORRECT TEXT
What file contains a list of directories for an NFS daemon to server to other systems? (Provide the complete answer)

Answer: /etc/exports

QUESTION NO: 21 CORRECT TEXT
You are running a machine which exports a list of directories using NFS.
Provide the complete path to the file which contains this list.

Answer: /etc/exports

QUESTION NO: 22
Which two services resolve Netbios names to IP addresses?

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

Answer: A, D

QUESTION NO: 23
Which of the following brings up a user friendly GUI interface (choose all that apply):

A. make xconfig
B. make menuconfig
C. make config
D. make compile

Answer: A,B
Explanation:
The "make xconfig" or "make menuconfig" brings up a user friendly GUI interface. And "make config" brings up command-line console mode interface. You can load the configuration file from /usr/src/linux/.config (dot config file. Note the dot before config).

QUESTION NO: 24CORRECT TEXT
What file contains a list of shared directories on a Linux/Unix system? Type the full path and name of the file.

Answer: /etc/exports

QUESTION NO: 25
Within smb.conf, which security setting will NOT require that a client connect using a valid username and password before connecting to a shared resource?

A. security = user
B. security = share
C. security = server
D. security = guest

Answer: D
Explanation:
1. Security=Server : Server Security mode is left over from the time when samba was nt capable of acting as a domain member server. It is higly recomemded not to use this feature.
2.

Security=User : User level security first because it's simpler. In user-leel security, the client sends a session setup request directly following protocol negotiation. This request provides a username and password. The server can either accept or reject the username and password combination.
3. security=share : In share level security, the client authenticates itself separately for each share. It sends a password along with each tree connection request, but it does not explicitly send a username with this operation.

QUESTION NO: 26
You want to make the directory /home/tess available via NFS. Which option do you have to use to grant read permission for the root user on the NFS mounted file system?

A. no_root_squash
B. root_squash
C. root(rw)
D. For safety, the NFS protocol does not allow this?

Answer: A
Explanation: Entries in /etc/exports are exported with root_squashing turned on. This ensures that requests from the root user on a client machine are denied root access to root-owned files on a server machine. Such requests are mapped instead to a uid such as 65534. This behaviour can be defeated with the no_root_squash option but this not recommended.

QUESTION NO: 27
What configuration file contains the list of directories shared via NFS?

A. /etc/share
B. /etc/exports
C. /etc/dfs/dfstab
D. /etc/fstab

Answer: B
Explanation: /etc/exports file is used to share the data via NFS.
Syntax: directory client(permission)
Example:
/public *(rw,sync)
/data *.example.com(ro,sync)

QUESTION NO: 28 CORRECT TEXT
When a change is made to the file controlling what files are made available by NFS, what command must be run to make the changes effective? (Provide only the command name, not the path or any command switches.)

Answer: exportfs
Explanation: exportfs command is used to maintain the current table of exported file systems of NFS.
To List all shared data:
exportfs -v
To Refresh /etc/exports
exportfs -r

QUESTION NO: 29
Enter the command/servicename that dynamically assigns ports for Remote Procedure Calls (RPC) services like NIS, NFS and similar.

Answer: portmap
Explanation: portmap is a server that converts RPC program numbers into DARPA protocol port numbers. It must be running in order to make RPC calls.
When an RPC server is started, it will tell portmap what port number it is listening to, and what RPC program numbers it is prepared to serve.

QUESTION NO: 30
You want to make the directory /local available via NFS. Everything works fine, but on the client machine, the super user is unable to read any files on the NFS-mounted file system. Why?

A. The NFS protocol does not allow this.
B. The super user has different user IDs on the client and the server machine.
C. The client, when mounting the NFS filesystem, must specify the option trusted.
D. The exports entry on the server machine does not include the option no_root_squash.

Answer: D
Explanation: Entries in /etc/exports are exported with root_squashing turned on. This ensures that requests from the root user on a client machine are denied root access to root-owned files on a server machine. Such requests are mapped instead to a uid such as 65534. This behaviour can be defeated with the no_root_squash option but this not recommended.

Section 5, (1.113.5) Setup and configure basic DNS services (14 Questions)

* Description: Candidate should be able to configure hostname lookups and troubleshoot problems with local caching-only name server. Requires an understanding of the domain registration and DNS translation process. Requires understanding key differences in configuration files for bind 4 and bind 8.

***Key files, terms, and utilities** include:

/etc/hosts

`/etc/resolv.conf`

`/etc/nsswitch.conf`

`/etc/named.boot (v.4) or /etc/named.conf (v.8)`

named

QUESTION NO: 1CORRECT TEXT
Type in the name and full path to the network configuration file that defines the search order for name resolution:

Answer: /etc/nsswitch.conf

QUESTION NO: 2CORRECT TEXT
What file with full path is used to set the location to query for hostname resolution outside of the local system?

Answer: /etc/resolv.conf

QUESTION NO: 3
What files affect the name resolution functionality of a Linux host? Choose Three.

A. /etc/resolv.conf
B. /etc/hosts
C. /etc/default/names
D. /etc/nsswitch.conf
E. /etc/inet/hosts

Answer: A, B, D

QUESTION NO: 4
Which port is used for DNS

A. 110
B. 21
C. 23
D. 52
E. 53

Answer: E

QUESTION NO: 5
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.

Answer: C

QUESTION NO: 6
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

Answer: D

QUESTION NO: 7
This is the file `/etc/named.boot` from the computer named tellus with IP address 128.66.12.10.

```
directory /etc

secondary testking.com 128.66.12. testking.com.hosts
secondary 66.128.IN-ADDR.ARPA 128.66.12.5 128.66.rev
primary 0.0.127.IN-ADDR.ARPA named.local
cache named.ca
```

From this file, you know that:

A. tellus is the primary DNS server for domain testking.com.
B. There is a secondary DNS server for domain testking.com at the IP address 128.66.12.5.
C. tellus is a secondary DNS server for domain testking.com and it downloads the domain data from the server at IP address 128.66.12.5.
D. The server at IP address 128.66.12.5 is allowed to download domain and reverse lookup data from tellus.

Answer: B

QUESTION NO: 8
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

Answer: A

QUESTION NO: 9CORRECT TEXT

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 address of 192.168.33.254, type the exact entry that should appear in this file:

Answer: nameserver 192.168.33.254

QUESTION NO: 10CORRECT TEXT
Type in the name and full path to the config file that contains the IP address of DNS servers for hostname resolution:

Answer: /etc/resolv.conf

QUESTION NO: 11
What kind of DNS entries are used to get the hostname of a given IP address? Please enter exactly ONE word.

Answer: reverse
Explanation:
i. Forward Lookup : resolves the hostname into IP address
ii. Reverse Lookup : Resolves the IP addres into Hostname

QUESTION NO: 12
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.

Answer: A
Explanation: /etc/nsswitch.conf file is called system databases and name service switch configuration file.
By default it checks in /etc/hosts if not found then only send the request to DNS server if
Hosts: files dns : is written in /etc/nsswitch.conf file.

QUESTION NO: 13
In your DNS configuration, MX records are used to point to the _____ server(s) for your domain. (Please specify a single word answer.)

Answer: email
Answer: e-mail

Explanation: MX record in DNS configuration specifies the Mail Exchanger or mail server for the domain.
Example:
abc.com. IN MX 5 mail.abc.com.
abc.com. IN MX 10 mail1.abc.com.
Where mail.abc.com is the primary mail Exchanger for abc.com domain and mail1.abc.com is the secondary mail exchanger for the abc.com domain.

QUESTION NO: 14
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

Answer: A
Explanation: CNAME helps to aliases to existing host in DNS record.
Example:
mail IN A 192.168.100.1
pop IN CNAME mail

Section 6, (1.113.7) Set up secure shell (OpenSSH) (12 Questions)

* Description: The candidate should be able to obtain and configure OpenSSH. This objective includes basic OpenSSH installation and troubleshooting, as well as configuring sshd to start at system boot..

***Key files, terms, and utilities** include:

/etc/hosts.allow
`/etc/hosts.deny`
`/etc/nologin`
`/etc/ssh/sshd_config`
`/etc/ssh_known_hosts`
`/etc/sshrc`

sshd
ssh-keygen

QUESTION NO: 1
What file on a system contains a list of hosts that can't connect to the machine's services?

A. /etc/hosts/denial
B. /etc/hosts.deny
C. /etc/host.notallow
D. /etc/inetd.conf
E. /etc/hosts.not

Answer: B

QUESTION NO: 2
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

Answer: B

QUESTION NO: 3
Which of the following services would you be least likely to configure to be governed over by the Internet Super Server?

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

E. bind

Answer: C

QUESTION NO: 4
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.

Answer: B

QUESTION NO: 5
The file `/etc/ssh_host_key` should be:

A. world-readable
B. readable to group sys
C. readable to root only
D. readable by all SSH users

Answer: D

QUESTION NO: 6
What command will verify the syntax of a hosts.allow and hosts.deny file combination?

A. tcpdchk
B. verify --tcp

C. ipswitch
D. tcpdump
E. tcpdmatch

Answer: A

QUESTION NO: 7
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`

Answer: A

QUESTION NO: 8
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 ss --recover command.
C. A lost passphrase cannot be recovered.
D. Decrypt the authentication key with gpg.
E. Decrypt the authentication key with ssh --decrypt.

Answer: C
Reference:
http://www.cs.utah.edu/support/index.php?option=com_content&task=view&id=32&Itemid=58

QUESTION NO: 9
What command do you use to generate an OpenSSH host key?

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

D. ssh-add

Answer: C
Explanation: ssh-keygen command generates, manage and converts authentication keys for ssh. Ssh-keyen can create RSA keys for user by SSH protocol veriosn and RSA or DSA for use by SSH version 2.
By default it will create the public key file and private key file in ~.ssh/
Filename_dsa is the private key file
filename_dsa.pub is the public key file

QUESTION NO: 10
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

Answer: D

QUESTION NO: 11
Which file contains a list of services and hosts that will be denied by a TCP Wrapper such as tcpd? (type full path)

Answer: /etc/hosts.deny
Explanation:
The /etc/hosts.allow and /etc/hosts.deny each have two or more colon-separated fields. The first filed specifies the comma separated list of executable name . The second field contains a comma-separated list of client specifications, using IP address or host name or network name.

httpd: 192.168.1.0/24 à specified the network
vsftpd: .example.com à specified the domain.
We can allow or deny to client by name or ip.
Example of /etc/hosts.deny

vsftpd:ALL à Deny the ftp service to all client
vsftpd: ALL EXCEPT .example.com à Deny the ftp service to all client except example.com domain members.

QUESTION NO: 12
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.

Answer: B
Explanation:
Reference: http://acd.ucar.edu/~fredrick/mpark/ssh/rsa-unix.html

Topic 9, (114) Security (35 Questions)

Section 1, (1.114.1) Perform security administration tasks (13 Questions)

* Description: Candidates should know how to review system configuration to ensure host security in accordance with local security policies. This objective includes how to configure TCP wrappers, find files with SUID/SGID bit set, verify packages, set or change user passwords and password aging information, update binaries as recommended by CERT, BUGTRAQ, and/or distribution's security alerts. Includes basic knowledge of ipchains and iptables.

***Key files, terms, and utilities** include:

/proc/net/ip_fwchains

`/proc/net/ip_fwnames`

`/proc/net/ip_masquerade`

find

ipchains

passwd

socket

iptables

QUESTION NO: 1
What files affect the functioning of TCP Wrappers? Choose Two.

A. /etc/hosts.deny
B. /etc/nsswitch.conf
C. /etc/security/authconfig
D. /etc/default/clients
E. /etc/hosts.allow

Answer: A, E

QUESTION NO: 2CORRECT TEXT
What command with options will find all files on your system that have either the SUID or GUID bits set? Type the exact command with options to accomplish this.

Answer: find / -perm +6000

QUESTION NO: 3
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

Answer: B, C

QUESTION NO: 3CORRECT TEXT
Your user matt has forgotten his passwd and you wish to reset it. Type in the command line to change his password (you are currently logged in as root):

Answer: passwd matt

QUESTION NO: 4
What command will set a regular users password, so it forces them to change it every 60 days? Choose all that apply.

A. passwd -x 60 user1
B. chage -M 60 user1
C. passwd +x 60 user1
D. useradd -e 60 user1
E. usermod -f 60 user1

Answer: A, B

QUESTION NO: 5
In the output of iptables -L -n is the line:

ACCEPT all -- 10.69.70.5 0.0.0.0/

Listed under the INPUT chain. What does this line mean?

A. That all traffic from 0.0.0.0/0 to 10.69.70.5 is explicitly allowed.
B. TCP traffic from 10.69.70.5 with all of the TCP flags is allowed.
C. All traffic from 10.69.70.5 to anywhere is allowed.
D. The ACCEPT chain is responsible for all traffic from 10.69.70.1 to 0.0.0.0.

Answer: C
Explanation: ipables is used to set up, maintain and inspect the tables of IP packet filter rules in the Linux kernel. Serveral different tables my be defined, each table contains a number of built-in chains and may also contains user-defined chains. Each chain is a list of rules which can match a set of packets. Each rule specifies what to do with a packet that matches this is called target.
You can list the policy and rules of iptables using the iptables -L command
Output will get in this syntax:

target prot opt source destination

in output target is Accept, protocol is all no any options, source is 10.69.70.5 and any destination.
Means from 10.69.70.5 to any destination in any port is accepted.

QUESTION NO: 6
You are using iptables to protect your private network but allow it to access the Internet. What command do you run to view the current list of rules for masquerading?

A. iptables -L masquerade
B. iptables -t filter -L
C. iptables -t block -L
D. iptables -t nat -L

Answer: D
Explanation: ipables is used to set up, maintain and inspect the tables of IP packet filter rules in the Linux kernel. Serveral different tables my be defined, each table contains a number of built-in chains and may also contains user-defined chains. Each chain is a list of rules which can match a set of packets. Each rule specifies what to do with a packet that matches this is called target.

You can list the policy and rules of iptables using the iptables -L command
Output will get in this syntax:

target prot opt source destination

Default table is filter: when you use the iptables -L it will display the chains and rules of filter table.

To list rules of masquerading:
 # iptables -t nat -L

QUESTION NO: 7
The _____ command is used to setup, view, and modify packet filtering, network and port translation, and other packet mangling rules within 2.4 and later kernel.

Answer: iptables
Explanation: iptables is used to set up, maintain and inspect the tables of IP packet filter rules in the linux kernel. Several different tables may be defined. Each table contains a number of built-in chains and may also contain user-defined chains.

QUESTION NO: 8
Your gateway to the internet is using iptables and NAT to allow your private network to access the Internet. You've verified that the gateway is not set up to block packets, but you need to verify that it is properly masquerading them. Which of the following commands would you use to look at your NAT tables?

A. iptables -L -n

B. iptables -t nat -L
C. iptables -t mangle -L
D. iptables -t filter -L

Answer: B
Explanation: ipables is used to set up, maintain and inspect the tables of IP packet filter rules in the Linux kernel. Serveral different tables my be defined, each table contains a number of built-in chains and may also contains user-defined chains. Each chain is a list of rules which can match a set of packets. Each rule specifies what to do with a packet that matches this is called target.

You can list the policy and rules of iptables using the iptables -L command
Output will get in this syntax:

target prot opt source destination

Default table is filter: when you use the iptables -L it will display the chains and rules of filter table.

To list rules of masquerading:
 # iptables -t nat -L

QUESTION NO: 9
Which of the following services is NOT usually protected via TCP wrappers?

A. ftp
B. finger
C. auth
D. http

Answer: D
Explanation: TCP wrappers control only the services linked with the libwrap.so module i.e
sendmail
slapd
sshd
stunnel
xinetd
gdm
portmap

QUESTION NO: 10
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 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

Answer: A
Explanation:
The /etc/hosts.allow and /etc/hosts.deny each have two or more colon-separated fields. The first filed specifies the comma separated list of executable name . The second field contains a comma-separated list of client specifications, using IP address or host name or network name.

httpd: 192.168.1.0/24 à specified the network
vsftpd: .example.com à specified the domain.
To deny the service access you should write in /etc/hosts.deny

QUESTION NO: 11
You decide to use xinetd instead of inetd. Now, you need to transfer information from /etc/inetd.conf to another file. What file?

Answer: /etc/xinetd.conf
Explanation: xinetd.conf is the configuration file that determines the services provided by xinetd.
/etc/inetd.conf is replaced by /etc/xinetd.conf.

QUESTION NO: 12
What is a valid target for IPTABLES?

A. TCP
B. LOG

C. UDP
D. NAT

Answer: B
Explanation: Each firewall rule inspects each IP packet and then tries to identify it as the target of some sort of operation. Once a target is identified, the packet needs to jump over to it for further processing. Valid targets are: ACCEPT, DROP, LOG, REJECT, DNAT, SNAT and MASQUERADE

QUESTION NO: 13
How can you delete all rules from a chain in IPTABLES?

A. iptables -P
B. iptables -F
C. iptables -R
D. iptables -E

Answer: B
Explanation: -F stands for flush. It will flush the selected chain (all the chains in the table if none is given). This is equivalent to deleting all the rules one by one.

Section 2, (1.114.2) Setup host security (9 Questions)

* Description: Candidate should know how to set up a basic level of host security. Tasks include syslog configuration, shadowed passwords, set up of a mail alias for root's mail and turning off all network services not in use.

***Key files, terms, and utilities** include:

/etc/inetd.conf or /etc/inet.d/*

```
/etc/nologin
 /etc/passwd
 /etc/shadow
 /etc/syslog.conf
```

QUESTION NO: 1

What command will convert your shadow password file to md5 compatible passwords?

A. passconv
B. pwconv
C. mdconv
D. mdsum
E. passwd --convert

Answer: B

QUESTION NO: 2
You've decided to convert from standard shadow passwords to MD5 passwords. You make the appropriate changes to the `/etc/pam.d/ files`.
What should 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.

Answer: C

QUESTION NO: 3
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-------

Answer: C

QUESTION NO: 4
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 /ect/shadow`

Answer: D

QUESTION NO: 5
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

Answer: A

QUESTION NO: 6
You want to temporarily prevent users from logging in. Please complete the following command:

touch /etc/_____

Answer: nologin

Explanation: pam_nologin.so modules prevents non-root user login into the system, this module checks whether /etc/nologin file is created or not, if created deny to all non-root user to login locally.

QUESTION NO: 7
What are the first two bytes of a MD5 hash called?

A. salt
B. magic
C. magic bytes
D. encrypted bytes

Answer: A
Explanation: Recently, a number of projects have created MD5 "rainbow tables" which are easily accessible online, and can be used to reverse many MD5 hashes into strings that collide with the original input, usually for the purposes of password cracking. Salts helps protecting against rainbow tables as they, in effect, extend the length and potentially the complexity of the password. If the rainbow tables do not have passwords matching the length (e.g. 8 bytes password, and 2 bytes salt, is effectively a 10 byte password) and complexity (non-alphanumeric salt increases the complexity of strictly alphanumeric passwords) of the salted password, then the password will not be found. If found, one will have to remove the salt from the password before it can be used.

QUESTION NO: 8
What are the first two characters of an MD5 hashed password?

A. $1
B. $2
C. $3
D. $4

Answer: A
Explanation: MD5 hashes use the prefix 1 on all passwords in /etc/shadow

QUESTION NO: 9
How can you verify the integrity of the /etc/passwd file?

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

Answer: B
Explanation: pwck verifies the integrity of the system authentication information. All entries in the /etc/passwd and /etc/shadow are checked to see that the entry has the proper format and valid data in each field. The user is prompted to delete entries that are improperly formatted or which have other incorrectable errors.

Section 3, (1.114.3) Setup user level security (14 Questions)

* Description: Candidate should be able to configure user level security. Tasks include limits on user logins, processes, and memory usage.

***Key files, terms, and utilities** include:

quota

usermod

QUESTION NO: 1
What will the following line in the /etc/exports file do?

```
/data snowblower(rw) badhost (ro)
```

A. Give snowblower rw access to the data share, deny badhost any access, and allow ro for all other hosts
B. Give snowblower rw access to the data share, give badhost ro access to share and deny all others
C. Give snowblower no access to the data share, give badhost rw access and set ro access for all others
D. Cause a syntax error

Answer: B

QUESTION NO: 2CORRECT TEXT
What command would be used to check the gpgp signature on a downloaded source file? Type just the name of the command:

Answer: gpg

QUESTION NO: 3 CORRECT TEXT
To prevent users from seeing who is logged in with the who command, you must remove the world readable but from the file `/var/run` _____.

Answer: utmp

QUESTION NO: 4
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.

Answer: C

QUESTION NO: 5
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 file 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.

Answer: D

QUESTION NO: 6

Which of the following regarding user account configuration is true (choose all that apply):

A. username is case-sensitive
B. password is case-sensitive
C. username is case-insensitive
D. password is case-insensitive

Answer: A, B
Explanation Please note that everything should be entered in lowercase, except for the full name of the user which can be entered in a "pleasing format" (eg. Joe Smith) and the password. Case is sensitive, so inform your user(s) they must use identical case when entering their username and password.

QUESTION NO: 7
To create a user account, keep in mind that the username is at most ____ characters long.

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

Answer: B
Explanation Please note that everything should be entered in lowercase, except for the full name of the user which can be entered in a "pleasing format" (eg. Joe Smith) and the password. Case is sensitive, so inform your user(s) they must use identical case when entering their username and password.

QUESTION NO: 8
Rate this comment: The "root" account has no security restrictions imposed upon it.

A. True
B. False

Answer: A
Explanation When using this account it is crucial to be as careful as possible. The "root" account has no security restrictions imposed upon it. This means it is easy to perform administrative duties without hassle. However, the system assumes you know what you are doing, and will do exactly what you request -- no questions asked. Therefore it is easy, with a mistyped command, to wipe out crucial system files.

QUESTION NO: 9CORRECT TEXT
Type the full path and name of the file whose global read bit you would change to deny normal users the ability to get useful information from the who and w commands.

Answer: /var/run/utmp

QUESTION NO: 10CORRECT TEXT
What command was typed in to produce the output shown below? The entries shown are the full output of the command, less the actual command. Type the command and the options to reproduce similar output:

USER PID %CPU %MEM VSZ RSS TTY STAT START TIME COMMAND
root 394 0.0 0.0 1200 444 tty1 S 01:05 0:00 /sbin/getty 38400 tty1
root 396 0.0 0.0 1200 444 tty3 S 01:05 0:00 /sbin/getty 38400 tty3
root 397 0.0 0.0 1200 444 tty4 S 01:05 0:00 /sbin/getty 38400 tty4
root 398 0.0 0.0 1200 444 tty5 S 01:05 0:00 /sbin/getty 38400 tty5
root 399 0.0 0.0 1200 444 tty6 S 01:05 0:00 /sbin/getty 38400 tty6
root 423 0.0 0.0 1200 444 tty2 S 01:06 0:00 /sbin/getty 38400 tty2
root 426 0.2 0.3 2880 1964 pts/0 S 01:07 0:00 -bash

Answer: ps -aux

QUESTION NO: 11
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

Answer: D
http://www.faqs.org/docs/securing/chap5sec36.html

QUESTION NO: 12
inetd.conf was changed. How to reinit changes?

A. restart inetd
B. find inetd's PID and send signal 15 to it
C. find inetd's PID and send signal SIGHUP to it
D. ...

Answer: C
Explanation: find .... SIGHUP to it - is the correct line

QUESTION NO: 13
You need to find all references in system document to the word "backup". What command would you type? (Do not provide full path).

Answer: grep
Explanation: grep command prints the lines matching a pattern.
Example: grep root /etc/passwd : which prints all lines from /etc/passwd file having root pattern.

QUESTION NO: 14
The _____ command is used to modify a user's account information.

Answer: usermod
Explanation: usermod command is used to modify the user accounts.
Example: usermod -L username :Locks the account
usermod -U username : Unlocks the account
usermod -e "date" userame : sets the Accoun expire date