LPI_117-202_Resubmit_v2011-11-08_230q_revised_by_venom

Number: 117-202
Passing Score: 500
Time Limit: 120 min
File Version: 2013-02-03

Originally LPI.RealExamQuestions.117-202.v2011-11-08.by. Haxtons.230q.

2013-02-03 revised by Venom

With all the corrections and my personal research for every answer here, i was able to pass with a score of 720.

CHANGELOG:

- It's all questions that had a configuration embedded in image was removed. I wrote all the information into the question itself. Better view for those who uses VCE Mobile.
- Removed questions that was transferred to LPI-201, like DNS, TCP Dump.
- Removed topics dropped by LPI itself, like MajorDomo and INN.
- Default exam score was lowered from 800 to 500 (the actual passing score as today).
- All questions had a default score of 5. Now all of them were adjusted for the actual score value based on each section. For example, Squid questions now is 2, LILO issues are 4 and so. Those scores are based on LPI 117-202 objective (you can check it at http://www.lpi.org/linux-certifications/programs/lpic-2/exam-202)
- All questions now have answers explained. Also I did some corrections. Those questions which I've changed the answer I've explained why i did it.
- Topics are now available. You can now study a particular section, like Samba, Squid and SSH.
- Removed duplicated questions on the same Exam (like 'Exam A' and 'Exam B' had a lot)!
- Added some new questions based on another test that I found on the internet (LPI.ActualTests.117-202.v2009-06-26.by.Jisuren).

REMEMBER: IT'S NOT IMPORTANT TO KNOW THE CORRECT ANSWER. IT'S IMPORTANT TO KNOW WHY IT'S CORRECT. THE OBJECTIVE OF THIS TEST IS JUST FOR YOUR OWN OBSERVATION OF HOW MUCH YOU KNOW ABOUT THE TOPICS! NOBODY CAN GUARANTEE YOU CAN PASS! WORK HARD AND YOU WILL SURELY MAKE IT, SINCE YOU DID IT SO FAR TO GET HERE.

Comments: http://www.examcollection.com/117-202.html
Have a good day.

Sections

1. 208.1 Implementing a web server
2. 208.2 Maintaining a web server
3. 208.3 Implementing a proxy server
4. 209.1 SAMBA Server Configuration
5. 209.2 NFS Server Configuration
6. 210.1 DHCP configuration
7. 210.2 PAM authentication
8. 210.3 LDAP client usage
9. 211.1 Using e-mail servers
10. 211.2 Managing Local E-Mail Delivery
11. 211.3 Managing Remote E-Mail Delivery
12. 212.1 Configuring a router
13. 212.2 Securing FTP servers
14. 212.3 Secure shell (SSH)
15. 212.4 TCP Wrapper
16. 212.5 Security tasks
17. 213.1 Identifying boot stages and troubleshooting bootloaders
18. 213.2 General troubleshooting
19. 213.3 Troubleshooting system resources
20. 213.4 Troubleshooting environment configurations

Exam A

QUESTION 1
Given this excerpt from an Apache configuration file, which of the numbered lines has **INCORRECT** syntax?

```
1: <VirtualHost *:80>
2: ServerAdmin admin9@server.example.org
3: DocumentRoot /home/http/admin
4: ServerName admin.server.example.org
5: DirectoryIndex index.php default.php
6: ErrorLog logs/admin.server.example.org-error_log
7: CustomLog logs/admin.server.example.org-access_log common
8: </VirtualHost>
```

A. 1
B. 1 and 4
C. 1, 4 and 7
D. 1 and 5
E. None. The configuration is valid

Correct Answer: E
Section: 208.2 Maintaining a web server
Explanation

Explanation/Reference:
VirtualHost declarations must start with <> and end with </>. You can make a Virtualhost which will work with only one IP address, use wildcard to use every interface which apache is bound, or even with none specified.
ServerAdmin - e-mail address
DocumentRoot - Full path for the directory you wish to be served.
ServerName - a fully qualified name or partial name (ex. www or www.example.com)
DirectoryIndex - You can specify one or more files.
ErrorLog - You can specify a partial or full path to the log file. If you pass partially, it will save logs under the ServerRoot directory.
CustomLog - You can specify a partial or full path to the log file but you MUST specify the LogFormat name for this log (in this case, it's 'common')

QUESTION 2
Select the **TWO** correct statements about the following excerpt from `httpd.conf`:

```
<Directory /var/web/dir1>

<Files private.html>
   Order allow, deny
   Deny from all
</Files>

</Directory>
```

A. The configuration will deny access to `/var/web/dir1/private.html`, `/var/web/dirl/subdir2/private.html`, `/var/web/dirl/subdir3/private.html` and any other instance of private.html found under the `/var/web/dir1/directory`.
B. The configuration will deny access to `/var/web/dir1/private.html`, but it will allow access to `/var/web/dirl/subdir2/private.html`, for example.
C. The configuration will allow access to any file named `private.html` under `/var/web/dir1`, but it will deny access to any other files
D. The configuration will allow access just to the file named `private.html` under `/var/web/dir1`

E. The configuration will allow access to `/var/web/private.html`, if it exists

Correct Answer: AE
Section: 208.1 Implementing a web server
Explanation

Explanation/Reference:
The Files Directive is inside a Directory Directive. With this configuration, Files Directive will work recursively only inside Directory `/var/web/dir1`. And `/var/web/` is another directory, ouside of Directory Diretive scope, so it's why option E is correct.

QUESTION 3
Considering the following excerpt from the `httpd.conf` file, select the correct answer below:

```
<Location>

    AllowOverride AuthConfig Indexes

</Location>
```

A. The `Indexes` directive in the excerpt allows the use of other index-related directives such as `DirectoryIndex`
B. Both directives `AuthConfig` and Indexes found in the server's `.htaccess` file will be overridden by the same directives found in the `httpd.conf` file
C. The `AuthConfig` used in the excerpt allows the use of other authentication-related directives such as `AuthType`
D. The excerpt is incorrect, as the `AllowOverride` cannot be used with Indexes, since the latter cannot be overridden
E. The excerpt is incorrect, because `AllowOverride` cannot be used inside a `Location` section

Correct Answer: E
Section: 208.1 Implementing a web server
Explanation

Explanation/Reference:
http://httpd.apache.org/docs/2.2/mod/core.html#allowoverride

(...)
Context: directory
(...)
Only available in <Directory> sections
AllowOverride is valid only in <Directory> sections specified without regular expressions, not in <Location>, <DirectoryMatch> or <Files> sections.
(...)

QUESTION 4
Which of the following lines in the Apache configuration file would allow only clients with a valid certificate to access the website?

A. `SSLCA conf/ca.crt`
B. `AuthType ssl`
C. `IfModule libexec/ssl.c`
D. `SSLRequire`
E. `SSLVerifyClient require`

Correct Answer: E
Section: 208.2 Maintaining a web server
Explanation

Explanation/Reference:
http://httpd.apache.org/docs/2.2/mod/mod_ssl.html#sslverifyclient

```
Description: Type of Client Certificate verification
Syntax:      SSLVerifyClient level
Default:     SSLVerifyClient none
```

This directive sets the Certificate verification level for the Client Authentication.(...)
The following levels are available for level:

- **none**: no client Certificate is required at all
- **optional**: the client may present a valid Certificate
- **require**: the client has to present a valid Certificate
- **optional_no_ca**: the client may present a valid Certificate but it need not to be (successfully) verifiable.

In practice only levels **none** and **require** are really interesting, because level optional doesn't work with all browsers and level **optional_no_ca** is actually against the idea of authentication (but can be used to establish SSL test pages, etc.)

QUESTION 5
Which TWO of the following options are valid, in the `/etc/exports` file?

A. `rw`
B. `ro`
C. `rootsquash`
D. `norootsquash`
E. `uid`

Correct Answer: AB
Section: 209.2 NFS Server Configuration
Explanation

Explanation/Reference:
exports(5) - Linux man page
(...)
exportfs understands the following export options:
(...)
rw

Allow both read and write requests on this NFS volume. The default is to disallow any request which changes the filesystem. This can also be made explicit by using the `ro` option.

C and D and E are not correted because it's "`root_squash`" and "`no_root_squash`". Also and there's no 'uid' in `/etc/exports`, but there's "`anonuid`" and "`anongid`".

QUESTION 6
Which of the following is needed, to synchronize the Unix password with the SMB password, when the encrypted SMB password in the `smbpasswd` file is changed?

A. Nothing, because this is not possible.

B. Run `netvamp` regularly, to convert the passwords.
C. Rin `winbind --sync`, to synchronize the passwords.
D. Add `unix password sync = yes` to smb.conf.
E. Add `smb unix password = sync` to smb.conf.

Correct Answer: D
Section: 209.1 SAMBA Server Configuration
Explanation

Explanation/Reference:
http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html

unix password sync (G)
This boolean parameter controls whether Samba attempts to synchronize the UNIX password with the SMB password when the encrypted SMB password in the smbpasswd file is changed. If this is set to yes the program specified in the passwd program parameter is called AS ROOT - to allow the new UNIX password to be set without access to the old UNIX password (as the SMB password change code has no access to the old password cleartext, only the new).

Default: unix password sync = no

QUESTION 7
The new file server is a member of the Windows domain "`foo`". Which **TWO** of the following configuration sections will allow members of the domain group "`all`" to read, write and execute files in "`/srv/smb/data`"?

A. `[data] comment = data share path = /srv/smb/data write list = @foo+all force group = @foo+all create mask = 0550 directory mask = 0770`
B. `[data] comment = data share path = /srv/smb/data write list = @foo+all force group = @foo+all create mask = 0770 directory mask = 0770`
C. `[data] path = /srv/smb/data write list = @foo+all force group = @foo+all create mask = 0770 directory mask = 0770`
D. `[data] comment = data share path = /srv/smb/data write list = @foo+all force group = @foo+all directory mask = 0770`
E. `[data] comment = data share path = /srv/smb/data write list = @foo+all force group = all create mask = 0550 directory mask = 0770`

Correct Answer: BC
Section: 209.1 SAMBA Server Configuration
Explanation

Explanation/Reference:
http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html
comment = anything you want to say. Optional.
path = full path of the directory you wanto to tshare
write list = This is a list of users that are given read-write access to a service. If the connecting user is in this list then they will be given write access, no matter what the read only option is set to. The list can include group names using the @group syntax.
create mask = work as the same way as umask and gmask.
A and E is wrong because of the create mask.
D is wrong because it misses the create mask.

QUESTION 8
Which command can be used to list all exported file systems from a remote NFS server:

A. `exportfs`

B. `nfsstat`
C. `rpcinfo`
D. `showmount`
E. `importfs`

Correct Answer: D
Section: 209.2 NFS Server Configuration
Explanation

Explanation/Reference:
http://linux.die.net/man/8/showmount

showmount - show mount information for an NFS server

showmount queries the mount daemon on a remote host for information about the state of the NFS server on that machine. With no options showmount lists the set of clients who are mounting from that host. The output from showmount is designed to appear as though it were processed through "sort -u".

QUESTION 9
During which stage of the boot process would this message be seen?

```
Ide0: BM-DMA at 0xff00-0xff07, BIOS settings: hda:DMA, hdb:DMA
```

A. Boot loader start and hand off to kernel
B. Kernel loading
C. Hardware initialization and setup
D. Daemon initialization and setup

Correct Answer: C
Section: 213.1 Identifying boot stages and troubleshooting bootloaders
Explanation

Explanation/Reference:
http://en.wikipedia.org/wiki/Linux_startup_process#Kernel_startup_stage

(...)
The startup function for the kernel (also called the swapper or process 0) establishes memory management (paging tables and memory paging), detects the type of CPU and any additional functionality such as floating point capabilities, and then switches to non-architecture specific Linux kernel functionality via a call to start_kernel().

start_kernel executes a wide range of initialization functions. It sets up interrupt handling (IRQs), further configures memory, starts the Init process (the first user-space process), and then starts the idle task via cpu_idle(). Notably, the kernel startup process also mounts the initial RAM disk ("initrd") that was loaded previously as the temporary root file system during the boot phase. **The initrd allows driver modules to be loaded directly from memory, without reliance upon other devices (e.g. a hard disk) and the drivers that are needed to access them (e.g. an SATA driver)**. **This split of some drivers statically compiled into the kernel and other drivers loaded from initrd allows for a smaller kernel.** The root file system is later switched via a call to pivot_root() which unmounts the temporary root file system and replaces it with the use of the real one, once the latter is accessible. The memory used by the temporary root file system is then reclaimed.
(...)
To me, the boot loader process only loads LILO or GRUB and then one these will load the kernel itself.
The Kernel loading phase just load the kernel into the memory, as described at the wiki:
(...)
The kernel as loaded is typically an image file, compressed into either zImage or bzImage formats with zlib.

A routine at the head of it does a minimal amount of hardware setup, decompresses the image fully into high memory, and takes note of any RAM disk if configured.[5] It then executes kernel startup via ./arch/i386/boot/ head and the startup_32 () (for x86 based processors) process.
(...)
Daemon initialization cant be, because usually it's associated with services and so...

QUESTION 10
Where should the LILO code reside, on a system with only one installation of Linux and no other operating systems?

A. In the master boot record
B. In the boot sector
C. In the `/boot` directory
D. At the start of the kernel

Correct Answer: A
Section: 213.1 Identifying boot stages and troubleshooting bootloaders
Explanation

Explanation/Reference:
http://en.wikipedia.org/wiki/LILO_%28boot_loader%29

(...)
LILO does not depend on a specific file system, and can boot an operating system (e.g., Linux kernel images) from floppy disks and hard disks. One of up to sixteen different images can be selected at boot time. Various parameters, such as the root device, can be set independently for each kernel. LILO can be placed either in the master boot record (MBR) or the boot sector of a partition. In the latter case something else must be placed in the MBR to load LILO.
(...)

So if Linux would be the only SO to be installed on a computer, you must install LILO at the MBR because there won't be any other boot loader which would load LILO for booting linux.

QUESTION 11
During which stage of the boot process would this message be seen?

```
ide_setup:hdc=ide-scsi
```

A. Boot loader start and hand off to kernel
B. Kernel loading
C. Hardware initialization and setup
D. Daemon initialization and setup

Correct Answer: B
Section: 213.1 Identifying boot stages and troubleshooting bootloaders
Explanation

Explanation/Reference:
That's tricky question.

While this looks like 'hardware initialization and setup', in fact it's the initrd doing its job.

http://en.wikipedia.org/wiki/Initrd#Mount_preparations

Some Linux distributions will generate a customized initrd image which contains only whatever is necessary **to boot some particular computer, such as ATA, SCSI and filesystem kernel modules.** These typically

embed the location and type of the root file system.
(...)
Any hardware drivers that the boot process depends on must be loaded. A common arrangement is to pack kernel modules for **common storage devices onto the initrd** and then invoke a hotplug agent to pull in modules matching the computer's detected hardware.

QUESTION 12
What happens when the Linux kernel can't mount the root filesystem when booting?

A. An error message is shown, showing which device couldn't be mounted or informing that init couldn't be found.
B. An error message is shown and the system reboots after a keypress.
C. An error message is shown and the system boots in maintenance mode.
D. An error message is shown and the administrator is asked to specify a valid root filesystem to continue the boot process.
E. An error message is shown, stating that the corresponding kernel module couldn't be loaded.

Correct Answer: A
Section: 213.1 Identifying boot stages and troubleshooting bootloaders
Explanation

Explanation/Reference:
An example that I found.
http://wiki.gentoo.org/wiki/Knowledge_Base:Unable_to_mount_root_fs

VFS: Cannot open root device "hda3" or unknown-block(2,0)
Please append a correct "root=" boot option; here are the available partions:
...
Kernel panic - not syncing: VFS: Unable to mount root fs on unknown-block(2,0)

Sometimes i think D would be correct because the message above tells you to specify a valid partitions. Since it gave a kernel panic, usually your system will halt, making D a bad answer.

QUESTION 13
When bash is invoked as an interactive login shell, which of the following sentences is true?

A. It first reads and executes commands in `/etc/profile` and then does same for `~/.bash_profile` and `~/.bashrc`
B. It first reads and executes commands in `/etc/bashrc` and then does same for `/etc/profile`
C. It reads and executes commands in `~/.bashrc` only if `/etc/profile` or another initialization script calls it.
D. It ignores `/etc/profile` and only reads and executes commands in `~/.bashrc`
E. It first reads and executes commands in `/etc/profile` and then does same for `~/.bash_profile`, `~/.bash_login` and `~/.profile`

Correct Answer: E
Section: 213.4 Troubleshooting environment configurations
Explanation

Explanation/Reference:
This exam came marked as C. I've changed to E. Let's try to understand why:

http://linux.die.net/man/1/bash
(...)
If bash is invoked with the name sh, it tries to mimic the startup behavior of historical versions of sh as closely as possible, while conforming to the POSIX standard as well. **When invoked as an interactive login shell**, or a non-interactive shell with the --login option, **it first attempts to read and execute commands from /etc/profile and ~/.profile**, in that order. The --noprofile option may be used to inhibit this behavior. When invoked as an interactive shell with the name sh, bash looks for the variable ENV, expands its value if it is defined, and uses the expanded value as the name of a file to read and execute. Since a shell invoked as sh does not attempt to read and execute commands from any other startup files, the --rcfile option has no effect. A non-interactive shell invoked with the name sh does not attempt to read any other startup files. When invoked as sh, bash enters posix mode after the startup files are read.

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

So since the question states it's an interactive login shell, it will execute /etc/profile and then ./.bash_profile and the other files. To make bash not loading these files, you must call bash with the -noprofile option, since it describes:
(...)
--noprofile
Do not read either the system-wide startup file /etc/profile or any of the personal initialization files ~/.bash_profile, ~/.bash_login, or ~/.profile. **By default, bash reads these files when it is invoked as a login shell** (see INVOCATION below).
(...)

QUESTION 14
Why is the root file system mounted read-only during boot and remounted with write permission later on?

A. Because if problems with the root file system are detected during the boot, `fsck` can be run, without risk of damage.
B. Because this way crackers cannot collect information about root with boot sniffers
C. To avoid writing to the disk, unless the root password is known.
D. To avoid other operating systems overwriting the Linux root partition
E. Because the disk has its own write protection that cannot change by the operating system.

Correct Answer: A
Section: 213.1 Identifying boot stages and troubleshooting bootloaders
Explanation

Explanation/Reference:
Seriously, from B to E does not make sense at all. That's why A is valid.
Well, let's be really serious: It's not just because of the possibility the root filesystem could be damage, it's also because the kernel will load other kernel modules to complete the boot process.

http://en.wikipedia.org/wiki/Linux_startup_process#Kernel_startup_stage

(...)
Thus, the kernel initializes devices, **mounts the root filesystem specified by the boot loader as read only**, and runs Init (/sbin/init) which is designated as the first process run by the system (PID = 1).[2] A message is printed by the kernel upon mounting the file system, and by Init upon starting the Init process. It may also optionally run Initrd[clarification needed] to allow setup and device related matters (RAM disk or similar) to be handled before the root file system is mounted.[2]

QUESTION 15

A GRUB boot loader installed in the MBR was accidentally overwritten. After booting with a rescue CD-ROM, how can the lost GRUB first stage loader be recovered?

A. Use `dd` to restore a previous backup of the MBR
B. Install LILO since there is no easy way to recover GRUB
C. Running `mformat` will create a new MBR and fix GRUB using info from `grub.conf`
D. Run `grub-install` after verifying that grub.conf is correct.
E. Run `fdisk --mbr /dev/had` assuming that the boot harddisk is `/dev/hda`.

Correct Answer: D
Section: 213.1 Identifying boot stages and troubleshooting bootloaders
Explanation

Explanation/Reference:
http://linux.die.net/man/8/grub-install

grub-install - install GRUB on your drive.

QUESTION 16
Journalling doesn't appear to be working on an ext3 file-system. When booting, the following line appears:

```
VFS: Mounted root (ext2 filesystem) readonly.
```

What could be causing the problem?

A. An old version of `e2fsprogs` is installed.
B. The kernel does not contain ext3 support.
C. The file-system is specified as ext2 in `/etc/fstab`.
D. The system was not shut down cleanly.

Correct Answer: B
Section: 209.2 NFS Server Configuration
Explanation

Explanation/Reference:
http://en.wikipedia.org/wiki/Ext3

The filesystem was merged with the mainline Linux kernel in November 2001 from 2.4.15 onward.
(...)
Without these features, **any ext3 file system is also a valid ext2 file system**. This situation has allowed well-tested and mature file system maintenance utilities for maintaining and repairing ext2 file systems to also be used with ext3 without major changes. The ext2 and ext3 file systems share the same standard set of utilities, e2fsprogs, which includes an fsck tool. The close relationship also makes conversion between the two file systems (both forward to ext3 and backward to ext2) straightforward.
(...)

BTW, this looks like a LPI 117-201 question, but it's also could be applied as Troubleshooting (213.1)

QUESTION 17
What is the name of the dovecot configuration variable that specifies the location of user mail?

A. `mbox`
B. `mail_location`
C. `user_dir`
D. `maildir`

E. `user_mail_dir`

Correct Answer: B
Section: 211.3 Managing Remote E-Mail Delivery
Explanation

Explanation/Reference:
http://wiki2.dovecot.org/MailLocation

There are three different places where the mail location is looked up from:

mail_location setting in dovecot.conf is used if nothing else overrides it.

mail userdb field overrides mail_location setting.

location setting inside namespaces overrides everything. Usually this should be used only for public and shared namespaces.

By default the mail_location setting is empty, which means that Dovecot attempts to locate automatically where your mails are. This is done by looking at ~/Maildir, /var/mail/username, ~/mail and ~/Mail in that order. It's usually a good idea to explicitly specify where the mails are, even if the autodetection happens to work. Autodetection commonly fails for new users who don't have the mail directory created yet.

QUESTION 18
What is the missing keyword in the following configuration sample for dovecot which defines which authentication types to support? (Specify only the keywork)

```
auth default {
______ = plain login cram-md5
}
```

A. `auth_order`
B. `mechanisms`
C. `methods`
D. `supported`

Correct Answer: B
Section: 211.3 Managing Remote E-Mail Delivery
Explanation

Explanation/Reference:
http://wiki.dovecot.org/Authentication/Mechanisms

(...)
Configuration

By default only PLAIN mechanism is enabled. You can change this by modifying dovecot.conf:

```
auth default {
  mechanisms = plain login cram-md5
  # ..
}
```

QUESTION 19
What does the following procmail configuration section do?

```
:0fw
```

```
* < 256000

| /usr/bin/foo
```

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

Correct Answer: E
Section: 211.2 Managing Local E-Mail Delivery
Explanation

Explanation/Reference:
http://pm-doc.sourceforge.net/doc/#flag_f_and_w_together

(...) Of course the f flag is enough to make procmail wait for the filter to finish, but the w means something more: to wait to learn the exit code of the filtering command. If sed fails with a syntax error and gives no output, without W or w procmail would happily accept the null output as the results of the filter and go on reading recipes for the now body-less message. On the other hand, with W or w sed will respond to a non-zero exit code by recovering the unfiltered text.

http://pm-doc.sourceforge.net/doc/#determining_if_body_is_longer_than_header

```
:0
*  1^1 B ?? > 1
* -1^1 H ?? > 1
{
   ..body was longer
}
```

http://pm-doc.sourceforge.net/doc/#flag_w_and_recipe_with_pipe

QUESTION 20
Which setting in the Courier IMAP configuration file will tell the IMAP daemon to only listen on the localhost interface?

A. `ADDRESS=127.0.0.1`
B. `Listen 127.0.0.1`
C. `INTERFACE=127.0.0.1`
D. `LOCALHOST_ONLY=1`

Correct Answer: A
Section: 211.3 Managing Remote E-Mail Delivery
Explanation

Explanation/Reference:
http://www.courier-mta.org/couriertcpd.html

-address=n.n.n.n

Accept network connections only to IP address n.n.n.n. If not specified, couriertcpd accepts connections to any IP address that the system accepts connections on. If the system has multiple network interfaces with

separate IP addresses, this option makes couriertcpd accept connections only to one specific IP address. Most systems have multiple network interfaces: the loopback interface, plus the local network interface, so that -address=127.0.0.1 accepts connections only from the local system. When multiple port numbers are specified, it is also possible to selectively bind different network addresses to each port number when list specifies more than one port number. See "Multiple port list" below for more information.

QUESTION 21
You suspect that you are receiving messages with a forged `From:` address. What could help you find out where the mail is originating?

A. Install TCP wrappers, and log all connections on port 25
B. A dd the command '`FR-strlog`' to the `sendmail.cf` file
C. Add the command '`define ('LOG_REAL_FROM') dnl`' to the `sendmail.mc` file
D. Run a filter in the aliases file that checks the originating address when mail arrives
E. Look in the `Received:` and `Message-ID:` parts of the mail header

Correct Answer: E
Section: 212.5 Security tasks
Explanation

Explanation/Reference:
A - TCP wrappers filters IP address and ports.
B and C- Even google doesn't know what 'FR-strlog' means.
D - aliases will only work to forward e-mails to another account in your mail host, not to check a suspicious "From".
http://en.wikipedia.org/wiki/Email#Header_fields

Message-ID: Also an automatically generated field; used to prevent multiple delivery and for reference in In-Reply-To: (see below).
Received: when an SMTP server accepts a message it inserts this trace record at the top of the header (last to first).

QUESTION 22
You have to mount the `/data` filesystem from an NFS server(`srvl`) that does not support locking. Which of the following mount commands should you use?

A. `mount -a -t nfs`
B. `mount -o locking=off srvl:/data /mnt/data`
C. `mount -o nolocking srvl:/data /mnt/data`
D. `mount -o nolock srvl:/data /mnt/data`
E. `mount -o nolock /data@srvl /mn/data`

Correct Answer: D
Section: 209.2 NFS Server Configuration
Explanation

Explanation/Reference:
http://linux.die.net/man/5/nfs

lock / nolock

Selects whether to use the NLM sideband protocol to lock files on the server. If neither option is specified (or if lock is specified), NLM locking is used for this mount point. When using the nolock option, applications can lock files, but such locks provide exclusion only against other applications running on the same client. Remote applications are not affected by these locks.

NLM locking must be disabled with the nolock option when using NFS to mount /var because /var contains files used by the NLM implementation on Linux. Using the nolock option is also required when mounting exports on NFS servers that do not support the NLM protocol.

QUESTION 23
In what mode is your FTP session when the client side makes the connections to both the data and command ports of the FTP server?

A. passive
B. active
C. impassive
D. safe
E. inactive

Correct Answer: A
Section: 212.2 Securing FTP servers
Explanation

Explanation/Reference:
http://en.wikipedia.org/wiki/File_Transfer_Protocol#Communication_and_data_transfer

FTP may run in active or passive mode, which determines how the data connection is established.(..) In situations where the client is behind a firewall and unable to accept incoming TCP connections, passive mode may be used. In this mode, the client uses the control connection to send a PASV command to the server and then receives a server IP address and server port number from the server, **which the client then uses to open a data connection from an arbitrary client port to the server IP address and server port number received.**

QUESTION 24
Which of the following organisations track and report on security related flaws in computer technology? (Please select TWO answers)

A. Bugtraq
B. CERT
C. CSIS
D. Freshmeat
E. Kernel.org

Correct Answer: AB
Section: 212.5 Security tasks
Explanation

Explanation/Reference:
Originally this answer was incorrect, so I correct it. It was saying CSIS as right and CERT was wrong. Here's why I've corrected it:

http://www.us-cert.gov/ - United States Computer Emergency Readiness Team
http://en.wikipedia.org/wiki/Bugtraq - Bugtraq is an electronic mailing list dedicated to issues about computer security. On-topic issues are new discussions about vulnerabilities, vendor security-related announcements, methods of exploitation, and how to fix them. It is a high-volume mailing list, and almost all new vulnerabilities are discussed there.

QUESTION 25
Which of the following Linux services has support for only the Routing Information Protocol (RIP) routing protocol?

A. `gated`
B. `ipchains`
C. `netfilter`
D. `routed`
E. `zebra`

Correct Answer: D
Section: 212.1 Configuring a router
Explanation

Explanation/Reference:
Boy, I just found it on the FreeBSD man page...

http://www.freebsd.org/cgi/man.cgi?query=routed&sektion=8

ROUTED(8) FreeBSD System Manager's Manual ROUTED(8)

NAME
routed, rdisc -- network **RIP** and router discovery routing daemon

QUESTION 26
Which of the following is NOT included in a Snort rule header?

A. protocol
B. action
C. source IP address
D. packet byte offset
E. source port

Correct Answer: D
Section: 212.5 Security tasks
Explanation

Explanation/Reference:
http://manual.snort.org/node280.html

Rules are specific to configurations but only some parts of a rule can be customized for performance reasons. If a rule is not specified in a configuration then the rule will never raise an event for the configuration. A rule shares all parts of the rule options, including the general options, payload detection options, non-payload detection options, and post-detection options. Parts of the rule header can be specified differently across configurations, limited to:

Source IP address and port
Destination IP address and port
Action

http://manual.snort.org/node295.html

The next field in a rule is the protocol. There are four protocols that Snort currently analyzes for suspicious behavior - TCP, UDP, ICMP, and IP. In the future there may be more, such as ARP, IGRP, GRE, OSPF, RIP, IPX, etc.

QUESTION 27

Which environment variables are used by `ssh-agent`? (Please select TWO variables)

A. SSH_AGENT_KEY
B. SSH_AGENT_SOCK
C. SSH_AGENT_PID
D. SSH_AUTH_SOCK
E. SSH_AUTH_PID

Correct Answer: CD
Section: 212.3 Secure shell (SSH)
Explanation

Explanation/Reference:
Originally wrong. It was said that ssh-agent uses SSH_AGENT_SOCK, but in fact is SSH_AUTH_SOCK. I've corrected.

SSH-AGENT(1) BSD General Commands Manual SSH-AGENT(1)

(...)
There are two main ways to get an agent set up: The first is that the agent starts a new subcommand into which some environment variables are exported(...)A UNIX-domain socket is created and the name of this socket is stored in the SSH_AUTH_SOCK environment variable.(...) The SSH_AGENT_PID environment variable holds the agent's process ID.(...)

QUESTION 28
What tool scans log files for unsuccessful login attempts and blocks the offending IP addresses with firewall rules?

A. nessus
B. nmap
C. nc
D. watchlogs
E. fail2ban

Correct Answer: E
Section: 212.5 Security tasks
Explanation

Explanation/Reference:
http://www.fail2ban.org/wiki/index.php/Main_Page

Fail2ban scans log files (e.g. /var/log/apache/error_log) and bans IPs that show the malicious signs -- too many password failures, seeking for exploits, etc. Generally Fail2Ban then used to update firewall rules to reject the IP addresses for a specified amount of time, although any arbitrary other action (e.g. sending an email, or ejecting CD-ROM tray) could also be configured. Out of the box Fail2Ban comes with filters for various services (apache, curier, ssh, etc).

QUESTION 29
Running `sysctl` has the same effect as:

A. Changing the kernel compilation parameters
B. Writing to files inside `/proc`
C. Changing process limits using ulimit

D. Editing files inside `/etc/sysconfig`
E. There is no equivalent to this utility

Correct Answer: B
Section: 213.3 Troubleshooting system resources
Explanation

Explanation/Reference:
from sysctl man page
SYSCTL(8) SYSCTL(8)

sysctl - configure kernel parameters at runtime

(...)
sysctl is used to modify kernel parameters at runtime. The parameters available are those listed under / proc/sys/. Procfs is required for sysctl support in Linux. You can use sysctl to both read and write sysctl data.

QUESTION 30
Which files are read by the `lsdev` command? (Please specify THREE answers)

A. `/proc/dma`
B. `/proc/filesystems`
C. `/proc/interrupts`
D. `/proc/ioports`
E. `/proc/swaps`

Correct Answer: ACD
Section: 213.2 General troubleshooting
Explanation

Explanation/Reference:
http://linux.die.net/man/8/lsdev

lsdev gathers information about your computer's installed hardware from the interrupts, ioports and dma files in the /proc directory, thus giving you a quick overview of which hardware uses what I/O addresses and what IRQ and DMA channels.

Files

/proc/interrupts
IRQ channels.
/proc/ioports
I/O memory addresses.
/proc/dma
DMA channels.

QUESTION 31
Which of the following describes the main purpose of strace?

A. Show the TCP/IP stack data, to help to solve network problems
B. Help to follow the traces of intruders of the internal network
C. Debug programs by displaying the original code of the program. Itis a kind of "disassembler"
D. Reverse engineer applications, resulting in the source code of the program

E. Debug programs by monitoring system calls and reporting them

Correct Answer: E
Section: 213.2 General troubleshooting
Explanation

Explanation/Reference:
http://linux.die.net/man/1/strace

strace - trace system calls and signals

QUESTION 32
The following data is some of the output produced by a program. Which program produced this output?

```
strftime (" Thu", 1024, "%a", 0xb7f64380) =4
fwrite ("Thu", 3, 1, 0xb7f614e0) =1
fputc (' ', 0xb7f614e0) =32
strftime (" Feb", 1024, " %b", 0xb7f64380) =4
fwrite ("Feb", 3, 1, 0xb7f614e0) =1
fputc (' ', 0xb7f614e0) =32
fwrite ("19", 2, 1, 0xb7f614e0) =1
```

A. `lsof`
B. `ltrace`
C. `nm`
D. `strace`
E. `time`

Correct Answer: B
Section: 213.2 General troubleshooting
Explanation

Explanation/Reference:
http://linux.die.net/man/1/ltrace

ltrace - A library call tracer

practical example:
$ ltrace echo example
__libc_start_main(0x8048f80, 2, 0xbffd8c54, 0x804b280, 0x804b2e0 <unfinished ...>
getenv("POSIXLY_CORRECT") = NULL
strrchr("echo", '/') = NULL
setlocale(6, "")
(...)

QUESTION 33
On bootup, LILO prints out `LIL` and stops. What is the cause of this?

A. The descriptor table is bad
B. LILO failed to load the second stage loader
C. LILO failed to load the primary stage loader
D. LILO failed to locate the kernel image

Correct Answer: A

Section: 213.1 Identifying boot stages and troubleshooting bootloaders
Explanation

Explanation/Reference:
http://tldp.org/HOWTO/Bootdisk-HOWTO/a1483.html

LIL = The second stage boot loader has been started, but it can't load the descriptor table from the map file. This is typically caused by a media failure or by a geometry mismatch.

QUESTION 34
A server was rebuilt using a full system backup but with a different disk setup. The kernel won't boot, complaining it cannot find the root filesystem. Which of the following commands will fix this error by pointing the kernel image to the new root partition?

A. `mkbootdisk`
B. `tune2fs`
C. `rdev`
D. `grub-install`
E. `fdisk`

Correct Answer: D
Section: 213.1 Identifying boot stages and troubleshooting bootloaders
Explanation

Explanation/Reference:
Originally wrong. It was markng as "`rdev`", which might do it, but the correct way to do it is running "`grub-install`". Hell, "`rdev`" is isn't listed as LPI 202 objectives.

http://linux.die.net/man/8/grub-install

grub-install copies GRUB images into the DIR/boot directory specfied by --root-directory, and uses the grub shell to install grub into the boot sector.

Here's what i found about rdev on its man page

http://linux.die.net/man/8/rdev

(...)
The rdev utility, when used other than to find a name for the current root device, is an ancient hack that works by patching a kernel image at a magic offset with magic numbers. **It does not work on architectures other than i386. Its use is strongly discouraged. Use a boot loader like SysLinux or LILO instead.**
(...)
Besides, this command is so old that recommends LILO! For those who doesn't know, LPI is thinking about dropping out LILO knowledge at LPIC-2 certification.

QUESTION 35
An administrator wants to issue the command `echo 1 >/var/log/boater.log` once all of the scripts in `/etc/rc2.d` have been executed. What is the best way to accomplish this?

A. Add the command to `/etc/rc.local`
B. Create a script in `~/.kde/Autostart/` and place the command in it
C. Create a script in `/etc/init.d/` and place a link to it in `/etc/rc2.d/`
D. Create a script in `/etc/rc2.d/` and place the command in it

Correct Answer: A

Section: 213.4 Troubleshooting environment configurations
Explanation

Explanation/Reference:

```
$ more /etc/rc.local
#!/bin/sh -e
#
# rc.local
#
# This script is executed at the end of each multiuser runlevel.
# Make sure that the script will "exit 0" on success or any other
# value on error.
#
# In order to enable or disable this script just change the execution
# bits.
#
# By default this script does nothing.

exit 0
```

QUESTION 36
An administrator has placed an executable in the directory `/etc/init.d`, however it is not being executed when the system boots into runlevel 2. What is the most likely cause of this?

A. The script has not been declared in `/etc/services`
B. runleve1 2 is not declared in `/etc/inittab`
C. The script has the permissions 700 and is owned by root
D. A corresponding link was not created in `/etc/rc2.d`

Correct Answer: D
Section: 213.4 Troubleshooting environment configurations
Explanation

Explanation/Reference:
http://www.togaware.com/linux/survivor/Run_Levels.html

Basically all the scripts in /etc/rcX.d will have something like
"XYYZZZZZ"
Where X is a capital S (for start) and K (for finish), followed by a number (YY) which mean in which order the script will be called (after or before another script) and ZZZ is the name of this script. So you might see something like "S95apache" which means to 'start' apache and "K98samba" to stop samba.

QUESTION 37
For an LDAP client configuration, the LDAP base needs to be set. Which TWO of the following actions would achieve that?

A. `export LDAPBASE=dc=linuxfoo,dc=com`
B. `export BASE=dc=linuxfoo,dc=com`
C. Edit `ldapbase.conf` and add "`BASE dc=linuxfoo,dc=com`".
D. Edit `cldap.conf` and add "`BASE dc=linuxfoo,dc=com`".
E. Edit `ldap.conf` and add "`BASE dc=linuxfoo,dc=com`".

Correct Answer: AE
Section: 210.3 LDAP client usage
Explanation

Explanation/Reference:
http://linux.die.net/man/5/ldap.conf

ldap.conf, .ldaprc - LDAP configuration file/environment variables

(...)
Environmental variables may also be used to augment the file based defaults. The name of the variable is the option name with an added prefix of LDAP. For example, to define BASE via the environment, set the variable **LDAPBASE to the desired value.**
(...)
Syntax

The configuration options are case-insensitive; their value, on a case by case basis, may be case-sensitive.
(...)
BASE ou=IT staff,o="Example, Inc",c=US

QUESTION 38
Which of the following options can be passed to a DHCP client machine using configuration options on the DHCP server?

A. The NIS domain name
B. The resolving order in `/etc/resolv.conf`
C. The priority order in `nsswitch.conf`
D. The filter rules for `iptables`
E. The contents of `hosts.allow` and `hosts.deny`

Correct Answer: A
Section: 210.1 DHCP configuration
Explanation

Explanation/Reference:
DHCP server only passes configurations to clients, it does not SET things on client machines. That's DHCP client job.

List of what parameters DHCP server can send to clients:
http://www.iana.org/assignments/bootp-dhcp-parameters/bootp-dhcp-parameters.xml

(...)
40 NIS Domain N NIS Domain Name [RFC2132]

QUESTION 39
Which answer best describes the meaning of the following LDAP search command: `ldapsearch -x" (&(cn=marie)(telephoneNumber=9*))"`

A. It is searching for all entries that don't have the cn attribute equal to marie OR the telephoneNumber attribute starting with number 9
B. It is searching for all entries that have the cn attribute equal to marie AND the telephoneNumber attribute starting with number 9
C. It is searching for all entries that have the cn attribute equal to marie AND the telephoneNumber attribute ending with number 9
D. It is searching for all entries that don't have the cn attribute equal to marie AND the telephoneNumber attribute starting with number 9

E. It is searching for all entries that have the cn attribute different than marie OR the telephoneNumber attribute starting with number 9

Correct Answer: B
Section: 210.3 LDAP client usage
Explanation

Explanation/Reference:
B.2. Using ldapsearch

http://www.centos.org/docs/5/html/CDS/ag/8.0/Finding_Directory_Entries-Using_ldapsearch.html

If you don't know anything about regular expressions, please read:

http://www.regular-expressions.info/reference.html

QUESTION 40
In a PAM configuration file, a `sufficient` control allows access:

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

Correct Answer: A
Section: 210.2 PAM authentication
Explanation

Explanation/Reference:
http://linux.die.net/man/5/pam.d

(...)
sufficient
success of such a module is enough to satisfy the authentication requirements of the stack of modules (if a prior required module has failed the success of this one is ignored). A failure of this module is not deemed as fatal to satisfying the application that this type has succeeded. If the module succeeds the PAM framework returns success to the application immediately without trying any other modules.

QUESTION 41
After setting up Apache to run inside a chroot jail as a non-root user, httpd no longer starts. What is the primary cause of the problem?

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

Correct Answer: A
Section: 208.1 Implementing a web server
Explanation

Explanation/Reference:
http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

The port numbers in the range from 0 to 1023 are the well-known ports. They are used by system processes that provide widely used types of network services. **On Unix-like operating systems, a process must execute with superuser privileges to be able to bind a network socket to an IP address using one of the well-known ports.**

QUESTION 42
Which is a valid Squid option to define a listening port?

A. `port = 3128`
B. `http-listen-port = 3128`
C. `http_port 3128`
D. `squid_port 3128`

Correct Answer: C
Section: 208.3 Implementing a proxy server
Explanation

Explanation/Reference:
http://linux.die.net/man/8/squid

-a port
Specify HTTP port number where Squid should listen for requests, in addition to any **http_port** specifications in squid.conf.

QUESTION 43
What is the name of the network security scanner project which, at the core, is a server with a set of network vulnerability tests (NVTs)?

A. nmap
B. OpenVAS
C. Snort
D. wireshark

Correct Answer: B
Section: 212.5 Security tasks
Explanation

Explanation/Reference:
http://www.openvas.org/

The world's most advanced Open Source vulnerability scanner and manager

OpenVAS is a framework of several services and tools offering a comprehensive and powerful vulnerability scanning and vulnerability management solution.

QUESTION 44
How must Samba be configured, so that it can check passwords against the ones in `/etc/passwd` and `/etc/shadow`?

A. Set the parameters "`encrypt passwords = yes`" and "`password file = /etc/passwd`".
B. Set the parameters "`encrypt passwords = yes`", "`password file = /etc/passwd`" and "`password algorithm = crypt`"
C. Delete the `smbpasswd` file and create a symbolic link to the `passwd` and `shadow` file

D. It is not possible for Samba to use `/etc/passwd` and `/etc/shadow`
E. Run `smbpasswd` to convert `/etc/passwd` and `/etc/shadow` to a Samba pass word file

Correct Answer: D
Section: 209.1 SAMBA Server Configuration
Explanation

Explanation/Reference:
A and B is incorrect because the correct parameter is "smb password file" and to really use Linux/Unix accounts, you must set "unix password sync = yes" in smb.conf to work with local *nix authentication. 'smbpasswd' can CHANGE the SMB password into a *nix password but not CONVERT those two files into smbpasswd file.

http://oreilly.com/openbook/samba/book/ch06_04.html
http://www.samba.org/samba/docs/man/manpages-3/smbpasswd.8.html

C is wrong because smbpasswd is very similar to unix passwd file, but it has extra fields.

http://www.samba.org/samba/docs/man/manpages-3/smbpasswd.5.html

I almost thought E was right, but smbpasswd program only CHANGES passwords. It does not convert original Unix passwd and shadow files, but it will sync it if "unix password sync" is marked as "Yes". Also, to make use of Unix authentication, on smb.conf the "Securiy" parameter should be configured to "User". Since E does not comment anything about it, i don't think it's quite right.

NOTE: When you do the actual exam, check ALL the answers again because I think this question in this VCE is missing informations.

QUESTION 45
What is the standard port number for the unencrypted IMAP service?

A. 25
B. 143
C. 443
D. 993
E. 1066

Correct Answer: B
Section: 211.3 Managing Remote E-Mail Delivery
Explanation

Explanation/Reference:
http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

143 TCP Internet Message Access Protocol (IMAP)—management of email messages

25 - unencrypted SMTP
443 - HTTP SSL
993 - Internet Message Access Protocol over SSL (IMAPS)
1066 - not a standard port.

QUESTION 46
After changing `/etc/exports` on a server, remote hosts are still unable to mount the exported directories. What should be the next action?
Please select **TWO** correct answers.

A. Restart the NFS daemon
B. Run `exportfs -a` on the server
C. Run `exportfs -f` on the server
D. Run `showmount -a` on the server
E. Restart the remote hosts

Correct Answer: BC
Section: 209.2 NFS Server Configuration
Explanation

Explanation/Reference:
http://linux.die.net/man/8/exportfs

-a Export or unexport all directories.
(...)

-f If /proc/fs/nfsd or /proc/fs/nfs is mounted, flush everything out of the kernel's export table. Fresh entries for active clients are added to the kernel's export table by rpc.mountd when they make their next NFS mount request.

QUESTION 47
Which Squid configuration directive defines the authentication method to use?

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

Correct Answer: A
Section: 208.3 Implementing a proxy server
Explanation

Explanation/Reference:
http://www.squid-cache.org/Doc/config/auth_param/

This is used to define parameters for the various authentication schemes supported by Squid.

QUESTION 48
Which entry in the `.procmailrc` file will send a copy of an email to another mail address?

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

Correct Answer: A
Section: 211.2 Managing Local E-Mail Delivery
Explanation

Explanation/Reference:
http://linux.die.net/man/5/procmailrc

c - Generate a carbon copy of this mail. This only makes sense on delivering recipes. The only non-delivering recipe this flag has an effect on is on a nesting block, in order to generate a carbon copy this will clone the running procmail process (lockfiles will not be inherited), whereby the clone will proceed as usual and the parent will jump across the block.

QUESTION 49
A security-conscious administrator would change which TWO of the following lines found in an SSH configuration file?

A. `Protocol 2,1`
B. `PermitEmptyPasswords no`
C. `Port 22`
D. `PermitRootLogin yes`
E. `IgnoreRhosts yes`

Correct Answer: AD
Section: 212.3 Secure shell (SSH)
Explanation

Explanation/Reference:
http://unixhelp.ed.ac.uk/CGI/man-cgi?sshd_config+5

Protocol
Specifies the protocol versions sshd supports. The possible values are "1" and "2". Multiple versions must be comma-separated. The default is "2,1". Note that the order of the protocol list does not indicate preference, because the client selects among multiple protocol versions offered by the server. Specifying "2,1" is identical to "1,2".
(...)
PermitRootLogin
Specifies whether root can log in using ssh(1). The argument must be "yes", "without-password", "forced-commands-only" or "no". The default is "yes".

If this option is set to "without-password" password authentication is disabled for root.

If this option is set to "forced-commands-only" root login with public key authentication will be allowed, but only if the command option has been specified (which may be useful for taking remote backups even if root login is normally not allowed). All other authentication methods are disabled for root.

If this option is set to "no" root is not allowed to log in.

QUESTION 50
You would like remote access to a Linux workstation via SSH. The system is on a network that is behind a firewall which blocks incoming connections to TCP ports below 1024. Which option in your `sshd_config` could you use to work around the firewall?

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

Correct Answer: E
Section: 212.3 Secure shell (SSH)
Explanation

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

QUESTION 51
When setting up a Squid proxy server, what would be a reason to limit the incoming `reply_body_max_size`?

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

Correct Answer: D
Section: 208.3 Implementing a proxy server
Explanation

Explanation/Reference:
reply_body_max_size parameter is used prevent users from downloading very large files.
Example: reply_body_max_size size allow all

QUESTION 52
Which Apache directive allows the use of external configuration files defined by the directive `AccessFileName`?

A. `AllowExternalConfig`
B. `AllowAccessFile`
C. `AllowConfig`
D. `IncludeAccessFile`
E. `AllowOverride`

Correct Answer: E
Section: 208.1 Implementing a web server
Explanation

Explanation/Reference:
http://httpd.apache.org/docs/current/mod/core.html#accessfilename

While processing a request the server looks for the first existing configuration file from this list of names in every directory of the path to the document, if distributed configuration files are enabled for that directory. For example:

AccessFileName .acl

before returning the document /usr/local/web/index.html, the server will read /.acl, /usr/.acl, /usr/local/.acl and /usr/local/web/.acl for directives, unless they have been disabled with

<Directory />
AllowOverride None

</Directory>

QUESTION 53
A web server is expected to handle approximately 200 simultaneous requests during normal use with an occasional spike in activity and is performing slowly. Which directives in httpd.conf need to be adjusted?

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

Correct Answer: D
Section: 208.1 Implementing a web server
Explanation

Explanation/Reference:
http://httpd.apache.org/docs/current/mod/prefork.html
http://httpd.apache.org/docs/current/mod/mpm_common.html#startservers
http://httpd.apache.org/docs/2.2/mod/mpm_common.html#maxclients
http://httpd.apache.org/docs/2.2/mod/core.html#keepalive

MinSpareServers - Minimum number of idle child server processes
MaxSpareServers - Maximum number of idle child server processes
StartServers - Number of child server processes created at startup
MaxClients - Maximum number of connections that will be processed simultaneously
KeepAlive - Enables HTTP persistent connections (...)**When a client uses a Keep-Alive connection it will be counted as a single "request" for the MaxRequestsPerChild directive, regardless of how many requests are sent using the connection.**

QUESTION 54
The Internet gateway connects the clients with the Internet by using a Squid proxy. Only the clients from the network 192.168.1.0/24 should be able to use the proxy. Which of the following configuration sections is correct?

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

Correct Answer: B
Section: 208.3 Implementing a proxy server
Explanation

Explanation/Reference:
http://www.squid-cache.org/Doc/config/acl/

(...) acl aclname src ip-address/mask ... # clients IP address [fast]

http://www.squid-cache.org/Doc/config/http_access/
(...)

Allowing or Denying access based on defined access lists

Access to the HTTP port:
http_access allow|deny [!]aclname ...

QUESTION 55
Which Apache directive is used to configure the main directory for the site, out of which it will serve documents?

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

Correct Answer: E
Section: 208.1 Implementing a web server
Explanation

Explanation/Reference:
http://httpd.apache.org/docs/2.2/mod/core.html#documentroot

Directory that forms the main document tree visible from the web

QUESTION 56
Which of the following is recommended to reduce Squid's consumption of disk resources?

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

Correct Answer: B
Section: 208.3 Implementing a proxy server
Explanation

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

QUESTION 57
When Apache is configured to use name-based virtual hosts:

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

Correct Answer: D
Section: 208.2 Maintaining a web server
Explanation

Explanation/Reference:
See the Sample Configuration of Name Based Virtual Host

```
NameVirtualHost 192.168.0.1

<VirtualHost www.abc.com>
Servername www.abc.com
DocumentRoot /var/www/abc
DirectoryIndex index.html index.htm index.php
ServerAdmin webmaster@abc.com
</VirtualHost>

<VirtualHost www.example.com>
Servername www.example.com
DocumentRoot /var/www/example
DirectoryIndex index.html index.htm index.php
ServerAdmin webmaster@example.com
</VirtualHost>
```

So, First You should specified the IP Address in which you are going to create multiple Name Based Virtual Host. As well as you should create the multiple virtual host directive.
Besides, if a requests comes to your apache and it specifies a wrong host (for example www.google.com), this request will be served by www.abc.com, because it's the first VirtualHost declared.

QUESTION 58
There is a restricted area in an Apache site, which requires users to authenticate against the file `/srv/www/security/site-passwd`. Which command is used to CHANGE the password of existing users, without losing data, when Basic authentication is being used.

A. `htpasswd -c /srv/www/security/site passwd user`
B. `htpasswd /srv/www/security/site-passwd user`
C. `htpasswd -n /srv/www/security/site-passwd user`
D. `htpasswd -D /srv/www/security/site-passwd user`

Correct Answer: B
Section: 208.1 Implementing a web server
Explanation

Explanation/Reference:
http://httpd.apache.org/docs/2.2/programs/htpasswd.html

For User based Authentication, you should create the htpasswd user. First Time To create the user:
htpasswd -c filename username

From Second Time either to change the password of httpuser

-D - Delete user. If the username exists in the specified htpasswd file, it will be deleted.
-n - Display the results on standard output rather than updating a file. This is useful for generating password records acceptable to Apache for inclusion in non-text data stores. This option changes the syntax of the command line, since the passwdfile argument (usually the first one) is omitted. It cannot be combined with the -c option.

QUESTION 59
Which `dhcpd.conf` option defines the DNS server address(es) to be sent to the DHCP clients?

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

D. `domain-server`

Correct Answer: B
Section: 210.1 DHCP configuration
Explanation

Explanation/Reference:
http://linux.die.net/man/5/dhcpd.conf
(...)

Notice that at the beginning of the file, there's a place for global parameters. These might be things like the organization's domain name, the addresses of the name servers (if they are common to the entire organization), and so on. So, for example:

option domain-name "isc.org";
option domain-name-servers ns1.isc.org, ns2.isc.org;

QUESTION 60
LDAP-based authentication against a newly-installed LDAP server does not work as expected. The file `/etc/pam.d/login` includes the following configuration parameters. Which of them is NOT correct?

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

Correct Answer: E
Section: 210.3 LDAP client usage
Explanation

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

Exam B

QUESTION 1
Which of the following sentences is true about ISC DHCP?

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

Correct Answer: D
Section: 210.1 DHCP configuration
Explanation

Explanation/Reference:
Via MAC ADDRESS.

http://linux.die.net/man/5/dhcpd.conf

Host declarations can match client messages based on the DHCP Client Identifier option or **based on the client's network hardware type and MAC address**. If the MAC address is used, the host declaration will match any client with that MAC address - even clients with different client identifiers. This doesn't normally happen, but is possible when one computer has more than one operating system installed on it - for example, Microsoft Windows and NetBSD or Linux.

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

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

Correct Answer: D
Section: 210.1 DHCP configuration
Explanation

Explanation/Reference:
http://linux.die.net/man/5/dhcpd.conf

(...)

So, for example,
(...)
is equivalent to

```
host joe {
  hardware ethernet 08:00:2b:4c:29:32;
  fixed-address joe.fugue.com;
  option host-name "joe";
 }
```

(...)
Reserved Leases

It's often useful to allocate a single address to a single client, in approximate perpetuity. Host statements with **fixed-address** clauses exist to a certain extent to serve this purpose, but because host statements are intended to approximate 'static configuration', they suffer from not being referenced in a littany of other Server Services, such as dynamic DNS, failover, 'on events' and so forth.

QUESTION 3
Which `dhcpd.conf` option defines the DNS server address(es) to be sent to the DHCP clients?

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

Correct Answer: B
Section: 210.1 DHCP configuration
Explanation

Explanation/Reference:
http://linux.die.net/man/5/dhcpd.conf

Notice that at the beginning of the file, there's a place for global parameters. These might be things like the organization's domain name, the addresses of the name servers (if they are common to the entire organization), and so on. So, for example:

(...)
option domain-name-servers ns1.isc.org, ns2.isc.org;

QUESTION 4
There is a restricted area in an Apache site, which requires users to authenticate against the file `/srv/www/security/site-passwd`.

Which command is used to CHANGE the password of existing users, without losing data, when Basic authentication is being used.

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

Correct Answer: B
Section: 208.1 Implementing a web server
Explanation

Explanation/Reference:
http://httpd.apache.org/docs/2.2/programs/htpasswd.html

For User based Authentication, you should create the htpasswd user. First Time To create the user:
htpasswd -c filename username

From Second Time either to change the password of httpuser

-D - Delete user. If the username exists in the specified htpasswd file, it will be deleted.
-n - Display the results on standard output rather than updating a file. This is useful for generating password records acceptable to Apache for inclusion in non-text data stores. This option changes the syntax of the command line, since the passwdfile argument (usually the first one) is omitted. It cannot be combined with the -c option.

QUESTION 5
Consider the following `/srv/www/default/html/restricted/.htaccess`

```
AuthType Basic
AuthUserFile /srv/www/security/site-passwd
AuthName Restricted
Require valid-user
Order deny,allow
Deny from all
Allow from 10.1.2.0/24
Satisfy any
```

Considering that `DocumentRoot` is set to `/srv/www/default/html`, which TWO of the following sentences are true?

A. Apache will only grant access to `http://server/restricted/` to authenticated users connecting from clients in the 10.1.2.0/24 network
B. This setup will only work if the directory `/srv/www/default/html/restricted/` is configured with `AllowOverride AuthConfig Limit`
C. Apache will require authentication for every client requesting connections to `http://server/restricted/`
D. Users connecting from clients in the 10.1.2.0/24 network won't need to authenticate themselves to access `http://server/restricted/`
E. The Satisfy directive could be removed without changing Apache behaviour for this directory

Correct Answer: BD
Section: 208.1 Implementing a web server
Explanation

Explanation/Reference:
http://httpd.apache.org/docs/2.2/mod/core.html#allowoverride

AuthConfig - Allow use of the authorization directives (AuthDBMGroupFile, AuthDBMUserFile, AuthGroupFile, AuthName, AuthType, AuthUserFile, Require, etc.).
Limit - Allow use of the directives controlling host access (Allow, Deny and Order).

http://httpd.apache.org/docs/2.2/mod/mod_authz_host.html#allow
The Allow directive affects which hosts can access an area of the server. Access can be controlled by hostname, IP address, IP address range, or by other characteristics of the client request captured in environment variables.

That's why E is not right and `Satisfy any` makes D correct.
http://httpd.apache.org/docs/2.2/mod/core.html#satisfy

Access policy if both Allow and Require used. The parameter can be either All or Any. This directive is only useful if access to a particular area is being restricted by both username/password and client host address. In this case the default behavior (All) is to require that the client passes the address access restriction and enters a valid username and password. **With the `Any` option the client will be granted access if they either pass the host restriction or enter a valid username and password. This can be used to password restrict an area, but to let clients from particular addresses in without prompting for a password.**

QUESTION 6
A web server is expected to handle approximately 200 simultaneous requests during normal use with an occasional spike in activity and is performing slowly. Which directives in httpd.conf need to be adjusted?

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

Correct Answer: B
Section: 208.1 Implementing a web server
Explanation

Explanation/Reference:
http://httpd.apache.org/docs/current/mod/prefork.html
http://httpd.apache.org/docs/current/mod/mpm_common.html#startservers
http://httpd.apache.org/docs/2.2/mod/mpm_common.html#maxclients
http://httpd.apache.org/docs/2.2/mod/core.html#keepalive

MinSpareServers - Minimum number of idle child server processes
MaxSpareServers - Maximum number of idle child server processes
StartServers - Number of child server processes created at startup
MaxClients - Maximum number of connections that will be processed simultaneously
KeepAlive - Enables HTTP persistent connections (...)When a client uses a Keep-Alive connection it will be counted as a single "request" for the MaxRequestsPerChild directive, regardless of how many requests are sent using the connection.

QUESTION 7
Which statements about the `Alias` and `Redirect` directives in Apache's configuration file are true?

A. Alias can only reference files under `DocumentRoot`
B. `Redirect` works with regular expressions
C. `Redirect` is handled on the client side
D. `Alias` is handled on the server side
E. `Alias` is not a valid configuration directive

Correct Answer: CD
Section: 208.1 Implementing a web server
Explanation

Explanation/Reference:
http://httpd.apache.org/docs/2.2/mod/mod_alias.html#redirect

Sends an external redirect asking the client to fetch a different URL

http://httpd.apache.org/docs/2.2/mod/mod_alias.html#alias

Maps URLs to filesystem locations

QUESTION 8
When Apache is configured to use name-based virtual hosts:

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

Correct Answer: D
Section: 208.2 Maintaining a web server
Explanation

Explanation/Reference:
See the Sample Configuration of Name Based Virtual Host
NameVirtualHost 192.168.0.1

<VirtualHost www.abc.com>
Servername www.abc.com
DocumentRoot /var/www/abc
DirectoryIndex index.html index.htm index.php
ServerAdmin webmaster@abc.com
</VirtualHost>

<VirtualHost www.example.com>
Servername www.example.com
DocumentRoot /var/www/example
DirectoryIndex index.html index.htm index.php
ServerAdmin webmaster@example.com
</VirtualHost>

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

QUESTION 9
Which Apache directive is used to configure the main directory for the site, out of which it will serve documents?

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

Correct Answer: E
Section: 208.1 Implementing a web server
Explanation

Explanation/Reference:
http://httpd.apache.org/docs/2.2/mod/core.html#documentroot

Directory that forms the main document tree visible from the web

QUESTION 10
Which Apache directive allows the use of external configuration files defined by the directive `AccessFileName`?

A. `AllowExternalConfig`
B. `AllowAccessFile`
C. `AllowConfig`
D. `IncludeAccessFile`
E. `AllowOverride`

Correct Answer: E
Section: 208.1 Implementing a web server
Explanation

Explanation/Reference:
http://httpd.apache.org/docs/current/mod/core.html#accessfilename

While processing a request the server looks for the first existing configuration file from this list of names in every directory of the path to the document, if distributed configuration files are enabled for that directory. For example:

AccessFileName .acl

before returning the document /usr/local/web/index.html, the server will read /.acl, /usr/.acl, /usr/local/.acl and /usr/local/web/.acl for directives, unless they have been disabled with

<Directory />
AllowOverride None
</Directory>

QUESTION 11
Which of the following is recommended to reduce Squid's consumption of disk resources?

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

Correct Answer: B
Section: 208.3 Implementing a proxy server
Explanation

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

QUESTION 12
Which ACL type in Squid's configuration file is used for authentication purposes?

A. `proxyAuth`
B. `proxy_auth`
C. `proxy_passwd`

D. `auth`
E. `auth_required`

Correct Answer: B
Section: 208.3 Implementing a proxy server
Explanation

Explanation/Reference:
http://wiki.squid-cache.org/Features/Authentication

(...)
Users will be authenticated if squid is configured to use proxy_auth ACLs.

QUESTION 13
The listing below is an excerpt from a Squid configuration file:

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

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

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

Correct Answer: D
Section: 208.3 Implementing a proxy server
Explanation

Explanation/Reference:
Because there's no Safe_ports for FTP, which is 21, and there's a `deny !Safe_ports`, which will deny any access that's not mapped in "`Safe_Ports`"

http://www.squid-cache.org/Doc/config/acl/

```
acl Safe_ports port 21        # ftp
```

QUESTION 14
In the file `/var/squid/url_blacklist` is a list of URLs that users should not be allowed to access. What is the correct entry in Squid's configuration file to create an acl named "blacklist" based on this file?

A. `acl blacklist urlpath_regex /var/squid/url_blacklist`

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

Correct Answer: D
Section: 208.3 Implementing a proxy server
Explanation

Explanation/Reference:
http://www.squid-cache.org/Doc/config/acl/

Defining an Access List

Every access list definition must begin with an aclname and acltype, followed by either type-specific arguments or a quoted filename that they are read from.

acl aclname acltype argument ...
acl aclname acltype "file" ...

When using "file", the file should contain one item per line. aclname acltype "file"
(...)
acl aclname urlpath_regex [-i] \.gif$ ...
regex matching on URL path [fast]

QUESTION 15
Users in the acl named `'sales_net'` must only be allowed to access to the Internet at times specified in the time_acl named `'sales_time'`. Which is the correct `http_access` directive, to configure this?

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

Correct Answer: B
Section: 208.3 Implementing a proxy server
Explanation

Explanation/Reference:
Allowing or Denying access based on defined access lists

Access to the HTTP port:
http_access allow|deny [!]aclname ...

QUESTION 16
What of the following is **NOT** a valid ACL type, when configuring squid?

A. `src`
B. `source`
C. `dstdomain`
D. `url_regex`
E. `time`

Correct Answer: B
Section: 208.3 Implementing a proxy server
Explanation

Explanation/Reference:
http://www.squid-cache.org/Doc/config/acl/

```
acl aclname src ipv6                    # request from IPv6 address
acl aclname dstdomain   .foo.com ...  # Destination server from URL [fast]
acl aclname url_regex [-i] ^http:// ...  # regex matching on whole URL [fast]
acl aclname time [day-abbrevs] [h1:m1-h2:m2]
    # [fast]
    #  day-abbrevs:
    #    S - Sunday
    #    M - Monday
    #    T - Tuesday
    #    W - Wednesday
    #    H - Thursday
    #    F - Friday
    #    A - Saturday
    #  h1:m1 must be less than h2:m2
```

QUESTION 17
Which Squid configuration directive defines the authentication method to use?

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

Correct Answer: A
Section: 208.3 Implementing a proxy server
Explanation

Explanation/Reference:
http://www.squid-cache.org/Doc/config/auth_param/

This is used to define parameters for the various authentication schemes supported by Squid.

QUESTION 18
The Internet gateway connects the clients with the Internet by using a Squid proxy. Only the clients from the network 192.168.1.0/24 should be able to use the proxy. Which of the following configuration sections is correct?

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

Correct Answer: B
Section: 208.3 Implementing a proxy server
Explanation

Explanation/Reference:
http://www.squid-cache.org/Doc/config/acl/
Example rule allowing access from your local networks.
Adapt to list your (internal) IP networks from where browsing
should be allowed
acl localnet src 10.0.0.0/8 # RFC1918 possible internal network
acl localnet src 172.16.0.0/12 # RFC1918 possible internal network
acl localnet src 192.168.0.0/16 # RFC1918 possible internal network
acl localnet src fc00::/7 # RFC 4193 local private network range
acl localnet src fe80::/10 # RFC 4291 link-local (directly plugged) machines

http://www.squid-cache.org/Doc/config/http_access/

Example rule allowing access from your local networks.
Adapt localnet in the ACL section to list your (internal) IP networks
from where browsing should be allowed
http_access allow localnet
http_access allow localhost

QUESTION 19
The syntax of the procmail configuration file is?

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

Correct Answer: A
Section: 211.2 Managing Local E-Mail Delivery
Explanation

Explanation/Reference:
http://www.gsp.com/cgi-bin/man.cgi?topic=procmailrc

A line starting with ':' marks the beginning of a recipe. It has the following format:

:0 [flags] [: [locallockfile]]
<zero or more conditions (one per line)>
<exactly one action line>

QUESTION 20
Which of the following recipes will append emails from "root" to the "rootmails" mailbox?

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

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

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

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

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

Correct Answer: B
Section: 211.2 Managing Local E-Mail Delivery
Explanation

Explanation/Reference:
http://www.gsp.com/cgi-bin/man.cgi?topic=procmailrc

A line starting with ':' marks the beginning of a recipe. It has the following format:

:0 [flags] [: [locallockfile]]
<zero or more conditions (one per line)>
<exactly one action line>

QUESTION 21
The internal network (192.168.1.0-192.168.1.255) needs to be able to relay email through the site's sendmail server. What line must be added to `/etc/mail/access` to allow this?

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

Correct Answer: B
Section: 211.1 Using e-mail servers
Explanation

Explanation/Reference:
http://www.sendmail.com/sm/open_source/docs/m4/anti_spam.html#access_db

```
spammer@aol.com              REJECT
cyberspammer.com             REJECT
TLD                          REJECT
192.168.212                  REJECT
IPv6:2002:c0a8:02c7          RELAY
IPv6:2002:c0a8:51d2::23f4    REJECT
```

would refuse mail from spammer@aol.com, any user from cyberspammer.com (or any host within the cyberspammer.com domain), any host in the entire top level domain TLD, 192.168.212.* network, and the IPv6 address 2002:c0a8:51d2::23f4. It would allow relay for the IPv6 network 2002:c0a8:02c7::/48.

The value part of the map can contain:

OK - Accept mail even if other rules in the running ruleset would reject it, for example, if the domain name is unresolvable. "Accept" does not mean "relay", but at most acceptance for local recipients. That is, OK allows less than RELAY.
RELAY- Accept mail addressed to the indicated domain or received from the indicated domain for relaying through your SMTP server. RELAY also serves as an implicit OK for the other checks.

QUESTION 22
The following is an excerpt from a procmail configuration file:

```
:0 c
* ! ^To: backup
! backup
```

Which of the following is correct?

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

Correct Answer: D
Section: 211.2 Managing Local E-Mail Delivery
Explanation

Explanation/Reference:
http://www.gsp.com/cgi-bin/man.cgi?topic=procmailrc

(...)
c - Generate a carbon copy of this mail. This only makes sense on delivering recipes. The only non-delivering recipe this flag has an effect on is on a nesting block, in order to generate a carbon copy this will clone the running procmail process (lockfiles will not be inherited), whereby the clone will proceed as usual and the parent will jump across the block.
(...)
Flags can be any of the following:

! Invert the condition.
(....)
The action line can start with the following characters:
! Forwards to all the specified mail addresses.

QUESTION 23
Which network service or protocol is used by sendmail for RBLs (Realtime Blackhole Lists)?

A. RBLP
B. SMTP
C. FTP
D. HTTP
E. DNS

Correct Answer: E
Section: 211.1 Using e-mail servers
Explanation

Explanation/Reference:
http://www.sendmail.com/sm/open_source/docs/m4/anti_spam.html

(...)
There are several DNS based blacklists, the first of which was the RBL (``Realtime Blackhole List'') run by the MAPS project, see http://mail-abuse.org/. These are databases of spammers maintained in DNS. To use such a database, specify

```
FEATURE(`dnsbl')
```

This will cause sendmail to reject mail from any site in the original Realtime Blackhole List database. This default DNS blacklist, blackholes.mail-abuse.org, is a service offered by the Mail Abuse Prevention System (MAPS). As of July 31, 2001, MAPS is a subscription service, so using that network address won't work if you haven't subscribed. Contact MAPS to subscribe (http://mail-abuse.org/).

QUESTION 24
On a newly-installed mail server with the IP address 10.10.10.1, ONLY local networks should be able to send email. How can the configuration be tested, using telnet, from outside the local network?

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

Correct Answer: D
Section: 211.1 Using e-mail servers
Explanation

Explanation/Reference:
http://exchange.mvps.org/smtp_frames.htm

QUESTION 25
Which entry in the .procmailrc file will send a copy of an email to another mail address?

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

Correct Answer: A
Section: 211.2 Managing Local E-Mail Delivery
Explanation

Explanation/Reference:

http://www.gsp.com/cgi-bin/man.cgi?topic=procmailrc

c - Generate a carbon copy of this mail. This only makes sense on delivering recipes. The only non-delivering recipe this flag has an effect on is on a nesting block, in order to generate a carbon copy this will clone the running procmail process (lockfiles will not be inherited), whereby the clone will proceed as usual and the parent will jump across the block.

QUESTION 26
Which file can be used to make sure that `procmail` is used to filter a user's incoming email?

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

Correct Answer: B
Section: 211.1 Using e-mail servers
Explanation

Explanation/Reference:
http://linux.die.net/man/1/procmail

Procmail should be invoked automatically over the .forward file mechanism as soon as mail arrives.(...)

QUESTION 27
A user is on holiday for two weeks. Anyone sending an email to that account should receive an auto-response. Which of the following procmail rules should be used, so that all incoming emails are processed by vacation?

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

Correct Answer: A
Section: 211.2 Managing Local E-Mail Delivery
Explanation

Explanation/Reference:
http://www.gsp.com/cgi-bin/man.cgi?topic=procmailrc

A line starting with ':' marks the beginning of a recipe. It has the following format:

:0 [flags] [: [locallockfile]]
<zero or more conditions (one per line)>
<exactly one action line>
(...)
The action line can start with the following characters:

| - Starts the specified program, possibly in $SHELL if any of the characters $SHELLMETAS are spotted. You can optionally prepend this pipe symbol with variable=, which will cause stdout of the program to be captured

in the environment variable (procmail will not terminate processing the rcfile at this point). If you specify just this pipe symbol, without any program, then procmail will pipe the mail to stdout.

QUESTION 28
What security precautions must be taken when creating a directory into which files can be uploaded anonymously using FTP?

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

Correct Answer: B
Section: 212.2 Securing FTP servers
Explanation

Explanation/Reference:
I think it's to avoid anonymous users to download critical files from your system.

I took this conclusion after reading this:

https://security.appspot.com/vsftpd/vsftpd_conf.html

anon_world_readable_only
When enabled, anonymous users will only be allowed to download files which are world readable. This is recognising that the ftp user may own files, especially in the presence of uploads.

Default: YES

QUESTION 29
What is the correct format for an `ftpusers` file entry?

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

Correct Answer: A
Section: 212.2 Securing FTP servers
Explanation

Explanation/Reference:
http://linux.die.net/man/5/ftpusers

Format:
The format of ftpusers is very simple. There is one account name (or username) per line. Lines starting with a # are ignored.

QUESTION 30
A security-conscious administrator would change which TWO of the following lines found in an SSH configuration file?

A. `Protocol 2,1`
B. `PermitEmptyPasswords no`
C. `Port 22`
D. `PermitRootLogin yes`
E. `IgnoreRhosts yes`

Correct Answer: AD
Section: 212.3 Secure shell (SSH)
Explanation

Explanation/Reference:
http://unixhelp.ed.ac.uk/CGI/man-cgi?sshd_config+5

Protocol
Specifies the protocol versions sshd supports. The possible values are "1" and "2". Multiple versions must be comma-separated. The default is "2,1". Note that the order of the protocol list does not indicate preference, because the client selects among multiple protocol versions offered by the server. Specifying "2,1" is identical to "1,2".
(...)
PermitRootLogin
Specifies whether root can log in using ssh(1). The argument must be "yes", "without-password", "forced-commands-only" or "no". The default is "yes".

If this option is set to "without-password" password authentication is disabled for root.

If this option is set to "forced-commands-only" root login with public key authentication will be allowed, but only if the command option has been specified (which may be useful for taking remote backups even if root login is normally not allowed). All other authentication methods are disabled for root.

If this option is set to "no" root is not allowed to log in.

QUESTION 31
A system monitoring service checks the availability of a database server on port 5432 of destination. example.com. The problem with this is that the password will be sent in clear text. When using an SSH tunnel to solve the problem, which command should be used?

A. `ssh -1 5432:127.0.0.1:5432 destination.example.com`
B. `ssh -L 5432:destination.example.com:5432 127.0.0.1`
C. `ssh -L 5432:127.0.0.1:5432 destination.example.com`
D. `ssh -x destination.example.com:5432`
E. `ssh -R 5432:127.0.0.1:5432 destination.example.com`

Correct Answer: C
Section: 212.3 Secure shell (SSH)
Explanation

Explanation/Reference:
http://www.linuxhorizon.ro/ssh-tunnel.html

```
ssh -L localport:host:hostport user@ssh_server -N
```

where:
-L - port forwarding parameters (see below)
localport - local port (chose a port that is not in use by other service)
host - server that has the port (hostport) that you want to forward
hostport - remote port
-N - do not execute a remote command, (you will not have the shell, see below)
user - user that have ssh access to the ssh server (computer)
ssh_server - the ssh server that will be used for forwarding/tunneling

QUESTION 32
What must be done on a host to allow a user to log in to that host using an SSH key?

A. Add their private key to `~/. ssh/authorized_keys`
B. Reference their public key in `~/. ssh/config`
C. Run `ssh-agent` on that host
D. Add their public key to `~/. ssh/authorized_keys`
E. Reference their private key in `~/. ssh/config`

Correct Answer: D
Section: 212.3 Secure shell (SSH)
Explanation

Explanation/Reference:
http://linux.die.net/man/1/ssh

The file ~/.ssh/authorized_keys lists the public keys that are permitted for logging in. When the user logs in, the ssh program tells the server which key pair it would like to use for authentication. The client proves that it has access to the private key and the server checks that the corresponding public key is authorized to accept the account.

QUESTION 33
An SSH port-forwarded connection to the web server `www.example.com` was invoked using the command `ssh -TL 80:www.example.com:80 user@www.example.com`. Which TWO of the following are correct?

A. The client can connect to the web server by typing http://www.example.com/ into the browser's address bar and the connection will be encrypted
B. The client can connect to www.example.com by typing http://localhost/ into the browser's address bar and the connection will be encrypted
C. The client can't connect to the web server by typing http://www.example.com/ into the browser's address bar. This is only possible using http://localhost/
D. It is only possible to port-forward connections to insecure services that provide an interactive shell (like telnet)
E. The client can connect to the web server by typing http://www.example.com/ into the browser's address bar and the connection will not be encrypted

Correct Answer: BE
Section: 212.3 Secure shell (SSH)
Explanation

Explanation/Reference:
Refer the ssh tunnel command format:

http://www.linuxhorizon.ro/ssh-tunnel.html

```
ssh -L localport:host:hostport user@ssh_server -N
```

where:
-L - port forwarding parameters (see below)
localport - local port (chose a port that is not in use by other service)
host - server that has the port (hostport) that you want to forward
hostport - remote port
-N - do not execute a remote command, (you will not have the shell, see below)
user - user that have ssh access to the ssh server (computer)
ssh_server - the ssh server that will be used for forwarding/tunneling

QUESTION 34
Which of the following configuration lines will export `/usr/local/share/` to `nfsclient` with read-write access, ensuring that all changes are straight to the disk?

A. `/usr/local/share nfsclient(rw) written`
B. `nfsclient: /usr/local/share/:rw,sync`
C. `/usr/local/share nfsclient:rw:sync`
D. `/usr/local/share nfsclient(rw,sync)`
E. `nfsclient(rw,sync) /usr/local/share`

Correct Answer: D
Section: 209.2 NFS Server Configuration
Explanation

Explanation/Reference:
http://linux.die.net/man/5/exports

(...)
rw - Allow both read and write requests on this NFS volume. The default is to disallow any request which changes the filesystem. This can also be made explicit by using the ro option
(...)
sync - Reply to requests only after the changes have been committed to stable storage.
(...)
sample /etc/exports file
/ master(rw) trusty(rw,no_root_squash)

QUESTION 35
Given this excerpt from an Apache configuration file, which of the numbered lines has INCORRECT syntax?

```
1: <VirtualHost *:80>
2: ServerAdmin admin9@server.example.org
3: DocumentRoot /home/http/admin
4: ServerName admin.server.example.org
5: DirectoryIndex index.php default.php
6: ErrorLog logs/admin.server.example.org-error_log
7: CustomLog logs/admin.server.example.org-access_log common
8: </VirtualHost>
```

A. 1
B. 1 and 4
C. 1, 4 and 7
D. 1 and 5
E. None. The configuration is valid

Correct Answer: E
Section: 208.2 Maintaining a web server
Explanation

Explanation/Reference:
VirtualHost declarations must start with <> and end with </>. You can make a Virtualhost which will work with only one IP address, use wildcard to use every interface which apache is bound, or even with none specified.
ServerAdmin - e-mail address
DocumentRoot - Full path for the directory you wish to be served.
ServerName - a fully qualified name or partial name (ex. www or www.example.com)
DirectoryIndex - You can specify one or more files.
ErrorLog - You can specify a partial or full path to the log file. If you pass partially, it will save logs under the ServerRoot directory.
CustomLog - You can specify a partial or full path to the log file but you MUST specify the LogFormat name for this log (in this case, it's 'common')

QUESTION 36
You suspect that you are receiving messages with a forged `From:` address. What could help you find out where the mail is originating?

A. Install TCP wrappers, and log all connections on port 25
B. A dd the command '`FR-strlog`' to the `sendmail.cf` file
C. Add the command '`define ('LOG_REAL_FROM') dnl`' to the `sendmail.mc` file
D. Run a filter in the aliases file that checks the originating address when mail arrives
E. Look in the `Received:` and `Message-ID:` parts of the mail header

Correct Answer: E
Section: 212.5 Security tasks
Explanation

Explanation/Reference:
A - TCP wrappers filters IP address and ports.
B and C- Even google doesn't know what 'FR-strlog' means.
D - aliases will only work to forward e-mails to another account in your mail host, not to check a suspicious "From".
http://en.wikipedia.org/wiki/Email#Header_fields

Message-ID: Also an automatically generated field; used to prevent multiple delivery and for reference in In-Reply-To: (see below).
Received: when an SMTP server accepts a message it inserts this trace record at the top of the header (last to first).

QUESTION 37
Which is a valid Squid option to define a listening port?

A. `port = 3128`
B. `http-listen-port=3128`
C. `http_port 3128`
D. `squid_port 3128`

Correct Answer: C
Section: 208.3 Implementing a proxy server
Explanation

Explanation/Reference:
http://www.squid-cache.org/Doc/config/http_port/

```
# Squid normally listens to port 3128
http_port 3128
```

QUESTION 38
Select the TWO correct statements about the following excerpt from httpd.conf:

```
<Directory /var/web/dir1>

<Files private.html>
   Order allow, deny
   Deny from all
</Files>

</Directory>
```

A. The configuration will deny access to `/var/web/dir1/private.html, /var/web/dirl/subdir2/private.html, /var/web/dirl/subdir3/private.html` and any other instance of private.html found under the `/var/web/dir1/directory`.
B. The configuration will deny access to `/var/web/dir1/private.html`, but it will allow access to `/var/web/dirl/subdir2/private.html`, for example.
C. The configuration will allow access to any file named `private.html` under `/var/web/dir1`, but it will deny access to any other files
D. The configuration will allow access just to the file named `private.html` under `/var/web/dir1`
E. The configuration will allow access to `/var/web/private.html`, if it exists

Correct Answer: AE
Section: 208.1 Implementing a web server
Explanation

Explanation/Reference:
The Files Directive is inside a Directory Directive. With this configuration, Files Directive will work recursively only inside Directory /var/web/dir1. /var/web/ is another directory, ouside of Directory Diretive scope, so it's why option E is correct.

QUESTION 39
To enable FORWARD on IPTables, you must do as root:
`# echo "1" > _____`
(provide full path of the file)

Correct Answer: /proc/net/ipv4/ip_forward
Section: 212.1 Configuring a router
Explanation

Explanation/Reference:
http://www.cs.unh.edu/cnrg/people/gherrin/linux-net.html

This is the first file the network script will read; it sets several environment variables. The first two simply determine that the computer will do networking (since it is on a network) and that this one will forward packets (from one network to the other). IP Forwarding is built into most kernels, but it is not active unless there is a 1 ``written'' to the /proc/net/ipv4/ip_forward file. (One of the network scripts performs an **`echo 1 > /proc/net/ipv4/ip_forward`** if FORWARD_IPV4 is true). The last four variables identify the computer and its link to the rest of the Internet (everything that is not on one of its own networks).

QUESTION 40
You need to retrieve mail on a remote mailserver and distribute it to users on your local system.
Which of the following could be used to accomplish this task? (Please make TWO selections.)

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

Correct Answer: CD
Section: 211.2 Managing Local E-Mail Delivery
Explanation

Explanation/Reference:
http://linux.die.net/man/8/rmail

http://linux.die.net/man/1/fetchmail

QUESTION 41
What steps are required to activate changes to Sendmail's aliases file?

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

Correct Answer: A
Section: 211.1 Using e-mail servers
Explanation

Explanation/Reference:
Couldn't find the newaliases man pages on the internet. If you really study LPI 202, you are aware that Postfix, Exim and other MTA/Mailers uses the same sendmail binary names for an easy transitions for every program from Sendmail to Postfix.

http://linux.die.net/man/1/newaliases.postfix

sendmail - Postfix to Sendmail compatibility interface

http://linux.die.net/man/8/sendmail.sendmail

-bi

Initialize the alias database.

QUESTION 42
What is the role of the file `/etc/ftpusers`?

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

Correct Answer: E
Section: 212.2 Securing FTP servers
Explanation

Explanation/Reference:
http://linux.die.net/man/5/ftpusers

ftpusers - list of users that may not log in via the FTP daemon

QUESTION 43
You are using a PAM aware sshd and you want to enable null password logins. What option would you add to the `/etc/pam.d/sshd` file to allow this?

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

Correct Answer: D
Section: 210.2 PAM authentication
Explanation

Explanation/Reference:
http://linux.die.net/man/8/pam_unix

nullok - The default action of this module is to not permit the user access to a service if their official password is blank. The nullok argument overrides this default.

Exam C

QUESTION 1
If the command `arp -f` is run, which file will be read by default?

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

Correct Answer: B
Section: 210.1 DHCP configuration
Explanation

Explanation/Reference:
http://linux.die.net/man/8/arp

-f filename, --file filename
Similar to the -s option, only this time the address info is taken from file filename set up. The name of the data file is very often /etc/ethers, but this is not official. If no filename is specified /etc/ethers is used as default.

QUESTION 2
What command must be used to print the kernel's routing table?

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

Correct Answer: E
Section: 212.1 Configuring a router
Explanation

Explanation/Reference:
route - show / manipulate the IP routing table

```
$ route
Tabela de Roteamento IP do Kernel
Destino         Roteador        MáscaraGen.     Opções Métrica Ref   Uso Iface
10.0.2.0        *               255.255.255.0   U      1      0        0 eth0
192.168.56.0    *               255.255.255.0   U      0      0        0 eth1
link-local      *               255.255.0.0     U      1000   0        0 eth1
default         10.0.2.2        0.0.0.0         UG     0      0        0 eth0
$
```

QUESTION 3
A server with 2 network interfaces, `eth0` and `eth1`, should act as a router. `eth0` has the IP address 192.168.0.1 in the subnet 192.168.0.1/24 and `eth1` has the IP address 10.0.0.1 in the subnet 10.0.0.0/16. The routing table looks fine, but no data is traversing the networks. Which TWO of the following need to be done?

A. Enable IP forwarding with `echo "1" > /proc/sys/net/ipv4/ip_forward`

B. Add new firewall chains to handle inbound & outbound traffic on both interfaces.
C. Reconfigure the firewall rules to allow traffic to traverse the networks.
D. The routing table needs to be restarted, for the changes to take effect.
E. The server needs to be restarted, for the changes to take effect.

Correct Answer: AC
Section: 212.1 Configuring a router
Explanation

Explanation/Reference:
http://www.cs.unh.edu/cnrg/people/gherrin/linux-net.html

This is the first file the network script will read; it sets several environment variables. The first two simply determine that the computer will do networking (since it is on a network) and that this one will forward packets (from one network to the other). IP Forwarding is built into most kernels, but it is not active unless there is a 1 ``written'' to the /proc/net/ipv4/ip_forward file. (One of the network scripts performs an **`echo 1 > /proc/net/ipv4/ip_forward`** if FORWARD_IPV4 is true). The last four variables identify the computer and its link to the rest of the Internet (everything that is not on one of its own networks).

And about routing:
http://www.centos.org/docs/4/html/rhel-sg-en-4/s1-firewall-ipt-fwd.html

QUESTION 4
Which of the following sentences is true, when using the following /etc/pam.d/login file?

```
#%PAM-1.0
auth required /lib/security/pam_securetty.so
auth required /lib/security/pam_nologin.so
auth sufficient /lib/security/pam_unix.so shadow nullok md5 use_authtok
auth required /lib/security/pam_ldap.so use_first_pass
account sufficient /lib/security/pam_unix.so
account required /lib/security/pam_ldap.so
password required /lib/security/pam_cracklib.so
password sufficient /lib/security/pam_unix.so nullok use_authtok md5 shadow
password required /lib/security/pam_ldap.so use_first_pass
session optional /lib/security/pam_console.so
session sufficient /lib/security/pam_unix.so
session required /lib/security/pam_ldap.so
```

A. All users will be authenticated against the LDAP directory
B. This is the only file needed to configure LDAP authentication on Linux
C. Only local users will be able to log in, when the file `/etc/nologin` exists
D. Ordinary users will be able to change their password to be blank
E. If the control flags for `auth` were changed to `required`, local users wouldn't be able to log in

Correct Answer: D
Section: 210.2 PAM authentication
Explanation

Explanation/Reference:
Because of the nullok at password pam_unix.so

http://linux.die.net/man/8/pam_unix

nullok - The default action of this module is to not permit the user access to a service if their official password

is blank. The nullok argument overrides this default.

QUESTION 5
LDAP-based authentication against a newly-installed LDAP server does not work as expected. The file `/etc/pam.d/login` includes the following configuration parameters. Which of them is NOT correct?

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

Correct Answer: E
Section: 210.2 PAM authentication
Explanation

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

QUESTION 6
What is the advantage of using SASL authentication with OpenLDAP?

A. It can prevent the transmission of plain text passwords over the network.
B. It disables anonymous access to the LDAP server.
C. It enables the use of Access Control Lists.
D. It allows the use of LDAP to authenticate system users over the network.
E. All of the above.

Correct Answer: A
Section: 210.2 PAM authentication
Explanation

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

QUESTION 7
In a PAM configuration file, which of the following is true about the `required` control flag?

A. If the module returns success, no more modules of the same type will be invoked
B. The success of the module is needed for the module-type facility to succeed. If it returns a failure, control is returned to the calling application
C. The success of the module is needed for the module-type facility to succeed. However, all remaining modules of the same type will be invoked.
D. The module is not critical and whether it returns success or failure is not important.
E. If the module returns failure, no more modules of the same type will be invoked

Correct Answer: C
Section: 210.2 PAM authentication
Explanation

Explanation/Reference:

http://linux.die.net/man/5/pam.d

required - failure of such a PAM will ultimately lead to the PAM-API returning failure but only after the remaining stacked modules (for this service and type) have been invoked.

QUESTION 8
Which of the following is true, when a server uses PAM authentication and both `/etc/pam.conf` & `/etc/pam.d/` exist?

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

Correct Answer: B
Section: 210.2 PAM authentication
Explanation

Explanation/Reference:
http://linux.die.net/man/5/pam.d

When a PAM aware privilege granting application is started, it activates its attachment to the PAM-API. This activation performs a number of tasks, the most important being the reading of the configuration file(s): /etc/pam.conf. Alternatively, this may be the contents of the /etc/pam.d/ directory. **The presence of this directory will cause Linux-PAM to ignore /etc/pam.conf**.

QUESTION 9
To configure an LDAP service in the company "Certkiller Ltd", which of the following entries should be added to `slapd.conf`, in the Database Directives section, to set the `rootdn` so that the common name is Manager and the company's domain is `Certkiller.com`?

A. `rootdn cn=Manager dc=Certkiller dc=com`
B. `rootdn "cn=Manager, dc=Certkiller, dc=com"`
C. `rootdn cn=Certkiller, dc=com,dc=Manager`
D. `rootdn "cn= Certkiller, dc=com,dc=Manager"`
E. `rootdn "cn=Manager dc= Certkiller dc=com"`

Correct Answer: B
Section: 210.3 LDAP client usage
Explanation

Explanation/Reference:
http://ldapman.org/articles/intro_to_ldap.html

(...)and the name is frequently stored in the cn (Common Name) attribute. Since nearly everything has a name, most objects you'll store in LDAP will use their cn value as the basis for their RDN. If I'm storing a record for my favorite oatmeal recipe, I'll be using cn=Oatmeal Deluxe as the RDN of my entry.
(...)
dc=foobar, dc=com
(base DN derived from the company's DNS domain components)
As with the previous format, this uses the DNS domain name as its basis. (...)this format is split into domain components: foobar.com becomes dc=foobar, dc=com.

QUESTION 10

What could be a reason for invoking vsftpd from (x) inetd?

A. It's not a good idea, because `(x) inetd` is not secure
B. Running `vsftpd` in standalone mode is only possible as root, which could be a security risk
C. `vsftpd` cannot be started in standalone mode
D. `(x) inetd` has more access control capabilities
E. `(x) inetd` is needed to run `vsftpd` in a chroot jail

Correct Answer: D
Section: 212.2 Securing FTP servers
Explanation

Explanation/Reference:
Well, i didn't find any good explanation, but let's face it:

inetd and xinetd uses tcpwrappers and has a lot of controls, so it's not about security (A)
You can change default FTP port to something above 1024, so you CAN start as another user (B)
You can start vsftpd as a daemon (C)
You can make vsftpd run in a chroot jail by just setting `chroot_local_user=YES`(E)

QUESTION 11
An SSH server is configured to use tcp_wrappers and only hosts from the class C network 192.168.1.0 should be allowed to access it. Which of the following lines would achieve this, when entered in `/etc/hosts.allow`?

A. `ALLOW: 192.168.1.0/255.255.255.0 : sshd`
B. `sshd : 192.168.1.0/255.255.255.0 : ALLOW`
C. `192.168.1.0/255.255.255.0 : ALLOW: sshd`
D. `tcpd: sshd : 192.168.1.0/255.255.255.0 : ALLOW`
E. `sshd : ALLOW: 192.168.1.0/255.255.255.0`

Correct Answer: B
Section: 212.4 TCP Wrapper
Explanation

Explanation/Reference:
http://linux.die.net/man/5/hosts.allow

All other lines should satisfy the following format, things between [] being optional:
daemon_list : client_list [: shell_command]
daemon_list is a list of one or more daemon process names (argv[0] values) or wildcards (see below).

client_list is a list of one or more host names, host addresses, patterns or wildcards (see below) that will be matched against the client host name or address.

QUESTION 12
Which TWO of the following statements about xinetd and inetd are correct?

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

Correct Answer: AE
Section: 212.4 TCP Wrapper
Explanation

Explanation/Reference:
http://linux.die.net/man/8/xinetd

xinetd performs the same function as inetd: it starts programs that provide Internet services. Instead of having such servers started at system initialization time, and be dormant until a connection request arrives, xinetd is the only daemon process started and it listens on all service ports for the services listed in its configuration file. When a request comes in, xinetd starts the appropriate server. Because of the way it operates, xinetd (as well as inetd) is also referred to as a super-server.

http://linux.die.net/man/5/xinetd.conf

access_times

determines the time intervals when the service is available. An interval has the form hour:min-hour:min (connections will be accepted at the bounds of an interval). Hours can range from 0 to 23 and minutes from 0 to 59.

QUESTION 13
A correctly-formatted entry has been added to `/etc/hosts.allow` to allow certain clients to connect to a service, but this is having no effect. What would be the cause of this?

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

Correct Answer: E
Section: 212.4 TCP Wrapper
Explanation

Explanation/Reference:
Apache does not use TCP Wrappers, for example. It has his own Access/Deny policies.

http://httpd.apache.org/docs/2.2/en/mod/mod_authz_host.html#order

QUESTION 14
Which **TWO** `/etc/hosts.allow` entries will allow access to sshd from the class C network 192.168.1.0?

A. `sshd : 192.168.1.`
B. `sshd : 192.168.1`
C. `sshd : 192.168.1.0 netmask 255.255.255.0`
D. `sshd : 192.168.1.0/255.255.255.0`
E. `sshd : 192.168.1.0`

Correct Answer: AD
Section: 212.4 TCP Wrapper
Explanation

Explanation/Reference:
http://linux.die.net/man/5/hosts.allow

All other lines should satisfy the following format, things between [] being optional:
daemon_list : client_list [: shell_command]
daemon_list is a list of one or more daemon process names (argv[0] values) or wildcards (see below).

client_list is a list of one or more host names, host addresses, patterns or wildcards (see below) that will be matched against the client host name or address.

QUESTION 15
Which **TWO** of the following statements about the tcp_wrappers configuration files are correct?

A. Both files must be edited, to get tcp_wrappers to work properly
B. It is possible to configure tcp_wrappers using just one file
C. `(x) inetd` requires these files
D. All programs that provide network services use these files to control access
E. `tcpd` uses these files to control access to network services

Correct Answer: BE
Section: 212.4 TCP Wrapper
Explanation

Explanation/Reference:
http://linux.die.net/man/5/hosts_access

This manual page describes a simple access control language that is based on client (host name/address, user name), and server (process name, host name/address) patterns. Examples are given at the end. The impatient reader is encouraged to skip to the EXAMPLES section for a quick introduction.

http://linux.die.net/man/8/tcpd

(...)
Files

The default locations of the host access control tables are:

/etc/hosts.allow
/etc/hosts.deny

QUESTION 16
What is the appropriate configuration file entry to allow SSH to run from `inetd`?

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

Correct Answer: A
Section: 212.3 Secure shell (SSH)
Explanation

Explanation/Reference:
http://linux.die.net/man/8/tcpd

Example 2

This example applies when tcpd expects that the network daemons are left in their original place.

In order to monitor access to the finger service, perform the following edits on the inetd configuration file (usually /etc/inetd.conf or /etc/inet/inetd.conf):

```
finger  stream  tcp  nowait  nobody  /usr/etc/in.fingerd  in.fingerd
```

QUESTION 17
A program, called `vsftpd`, running in a chroot jail, is giving the following error:
`/bin/vsftpd: error while loading shared libraries: libc.so.6: cannot open shared object file: No such file or directory.`
Which **TWO** of the following are possible solutions?

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

Correct Answer: AD
Section: 212.2 Securing FTP servers
Explanation

Explanation/Reference:
http://en.wikipedia.org/wiki/Chroot

(...)
At startup, programs expect to find scratch space, configuration files, device nodes and shared libraries at certain preset locations. **For a chrooted program to successfully start, the chroot directory must be populated with a minimum set of these files**.
---
http://en.wikipedia.org/wiki/Static_build
In a statically built program, **no dynamic linking occurs: all the bindings have been done at compile time**.

QUESTION 18
Which of the following can the program `tripwire` **NOT** check?

A. File size.
B. File signature.
C. Permissions.
D. File existence.
E. Boot sectors.

Correct Answer: E
Section: 212.5 Security tasks
Explanation

Explanation/Reference:
http://linux.die.net/man/8/tripwire

tripwire - a file integrity checker for UNIX systems

Boot sector is not a file.

QUESTION 19
A server is being used as a smurf amplifier, whereby it is responding to ICMP Echo-Request packets sent to its broadcast address. To disable this, which command needs to be run?

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

Correct Answer: D
Section: 212.5 Security tasks
Explanation

Explanation/Reference:
http://www.cyberciti.biz/faq/linux-kernel-etcsysctl-conf-security-hardening/

# Ignore all ICMP ECHO and TIMESTAMP requests sent to it via broadcast/multicast
net.ipv4.icmp_echo_ignore_broadcasts = 1

QUESTION 20
When the default policy for the iptables `INPUT` chain is set to `DROP`, why should a rule allowing traffic to localhost exist?

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

Correct Answer: D
Section: 212.1 Configuring a router
Explanation

Explanation/Reference:
http://wiki.centos.org/HowTos/Network/IPTables
`iptables -A INPUT -i lo -j ACCEPT` - Now it's time to start adding some rules. We use the -A switch to append (or add) a rule to a specific chain, the INPUT chain in this instance. Then we use the -i switch (for interface) to specify packets matching or destined for the lo (localhost, 127.0.0.1) interface and finally -j (jump) to the target action for packets matching the rule - in this case ACCEPT. So this rule will allow all incoming packets destined for the localhost interface to be accepted. **This is generally required as many software applications expect to be able to communicate with the localhost adaptor.**

QUESTION 21
To be able to access the server with the IP address 10.12.34.56 using HTTPS, a rule for iptables has to be written. Given that the client host's IP address is 192.168.43.12, which of the following commands is correct?

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

Correct Answer: C
Section: 212.1 Configuring a router
Explanation

Explanation/Reference:
http://wiki.centos.org/HowTos/Network/IPTables

FORWARD - All packets neither destined for nor originating from the host computer, but passing through (routed by) the host computer. This chain is used if you are using your computer as a router.

Your Linux server is acting as a router in this case. B is missing a minus signal at (d)estination

QUESTION 22
Which **THREE** of the following actions should be considered when a FTP chroot jail is created?

A. Create `/dev/` and `/etc/` in the chroot enviroment
B. Create `/etc/passwd` in the chroot enviroment
C. Create `/var/cache/ftp` in the chroot enviroment
D. Create the user ftp in the chroot enviroment
E. Create `/usr/sbin/` in the chroot enviroment

Correct Answer: ABD
Section: 212.2 Securing FTP servers
Explanation

Explanation/Reference:
http://en.wikipedia.org/wiki/Chroot
A chroot on Unix operating systems is an operation that changes the apparent root directory for the current running process and its children. **A program that is run in such a modified environment cannot name (and therefore normally not access) files outside the designated directory tree**.

https://security.appspot.com/vsftpd/vsftpd_conf.html
chroot_local_user - If set to YES, local users will be (by default) placed in a chroot() jail in their home directory after login. Warning: This option has security implications, especially if the users have upload permission, or shell access. Only enable if you know what you are doing. Note that these security implications are not vsftpd specific. They apply to all FTP daemons which offer to put local users in chroot() jails.

QUESTION 23
Connecting to a remote host on the same LAN using ssh public-key authentication works but forwarding X11 doesn't. The remote host allows access to both services. Which of the following can be the reason for that behaviour?

A. The remote user's `ssh_config` file disallows X11 forwarding
B. The remote server's `sshd_config` file disallows X11 forwarding
C. A different public key has to be used for X11
D. X11 cannot be forwarded if public-key authentication was used
E. X11 though SSH needs a special X11 server application installed

Correct Answer: B
Section: 212.3 Secure shell (SSH)
Explanation

Explanation/Reference:
http://linux.die.net/man/5/sshd_config

X11Forwarding
Specifies whether X11 forwarding is permitted. The argument must be "yes" or "no". The default is "no".

QUESTION 24
An iptables firewall was configured to use the target `MASQUERADE` to share a dedicated wireless connection to the Internet with a few hosts on the local network.
The Internet connection becomes very unstable in rainy days and users complain their connections drop when downloading e-mail or large files, while web browsing seems to be working fine.
Which change to your iptables rules could alleviate the problem?

A. Change the target `MASQUERADE` to `SNAT`
B. Change the target `MASQUERADE` to `DNAT`
C. Change the target `MASQUERADE` to `BALANCE` and provide a backup Internet connection
D. Change the target `MASQUERADE` to `REDIRECT` and provide a backup Internet connection
E. Change the target `MASQUERADE` to `BNAT`

Correct Answer: A
Section: 212.1 Configuring a router
Explanation

Explanation/Reference:
http://ipset.netfilter.org/iptables.man.html
MASQUERADE
It should only be used with dynamically assigned IP (dialup) connections: if you have a static IP address, you should use the SNAT target. **Masquerading is equivalent to specifying a mapping to the IP address of the interface the packet is going out, but also has the effect that connections are forgotten when the interface goes down. This is the correct behavior when the next dialup is unlikely to have the same interface address (and hence any established connections are lost anyway).**
SNAT
It specifies that the source address of the packet should be modified (and all future packets in this connection will also be mangled), and rules should cease being examined.

QUESTION 25
Which command line create an SSH tunnel for POP and SMTP protocols?

A. `ssh- L :110 -L :25 -1 user -N mailhost`
B. `ssh -L 25:110 -1 user -N mailhost`
C. `ssh -L mailhost:110 -L mailhost:25 -1 user -N mailhost`
D. `ssh -L mailhost:25:110 -1 user`
E. `ssh -L 110:mailhost:110 -L 25:mailhost:25 -1 user -N mailhost`

Correct Answer: E
Section: 212.3 Secure shell (SSH)
Explanation

Explanation/Reference:
http://www.linuxhorizon.ro/ssh-tunnel.html

```
ssh -L localport:host:hostport user@ssh_server -N
```

where:
-L - port forwarding parameters (see below)
localport - local port (chose a port that is not in use by other service)
host - server that has the port (hostport) that you want to forward

hostport - remote port
-N - do not execute a remote command, (you will not have the shell, see below)
user - user that have ssh access to the ssh server (computer)
ssh_server - the ssh server that will be used for forwarding/tunneling

QUESTION 26
Which command would release the current IP address leased by a DHCP server?

A. `ipconfig /release`
B. `ifconfig --release-all`
C. `dhclient -r`
D. `ifconfig --release`
E. `pump --release`

Correct Answer: C
Section: 210.1 DHCP configuration
Explanation

Explanation/Reference:
http://linux.die.net/man/8/dhclient

-r
Tell dhclient to release the current lease it has from the server. This is not required by the DHCP protocol, but some ISPs require their clients to notify the server if they wish to release an assigned IP address.

QUESTION 27
Remote access to a CD-RW device on a machine on a LAN must be restricted to a selected user group. Select the TWO correct alternatives that describe the possible solutions for this problem.

A. The remote access to these devices can be allowed to users by changing the display manager configuration and allowing `sudo` access for the user that will log in remotely
B. The `pam_console` module allows access configuration to these devices via console, including simultaneous access by many users
C. The `pam_console` module can be used to control access to devices via console, allowing/denying access to these devices in the user's session
D. If the `pam_console` module is used, it must be checked as required, because it is essential for user authentication
E. Through the `sudo` configuration file, it is possible to set users that will have the power of the root user, so they can access the devices. Besides that, it is important to configure the `/etc/pam.d/su` file, so the PAM modules can secure the service.

Correct Answer: CE
Section: 210.2 PAM authentication
Explanation

Explanation/Reference:
http://linux.die.net/man/8/pam_console

When a user logs in at the console and **no other user is currently logged in at the console**, pam_console.so will run handler programs specified in the file /etc/security/console.handlers such as pam_console_apply which changes permissions and ownership of files as described in the file /etc/security/console.perms. That user may then log in on other terminals that are considered part of the console, and as long as the user is still logged in at any one of those terminals, **that user will own those devices**.

http://www.cyberciti.biz/tips/restrict-the-use-of-su-command.html

For example add existing user rocky to wheel group
```
# usermod -G wheel rocky
# vi /etc/pam.d/su
```

Append line as follows:
```
auth required /lib/security/pam_wheel.so use_uid
```
OR
```
auth required pam_wheel.so use_uid
```

Save and close the file.

QUESTION 28
Select the alternative that shows the correct way to disable a user login (except for root)

A. The use of the `pam_nologin` module along with the `/etc/login` configuration file
B. The use of the `pam_deny` module along with the `/etc/deny` configuration file
C. The use of the `pam_pwdb` module along with the `/etc/pwdb.conf` configuration file
D. The use of the `pam_console` module along with the `/etc/security/console.perms` configuration file
E. The use of the `pam_nologin` module along with the `/etc/nologin` configuration file

Correct Answer: E
Section: 210.2 PAM authentication
Explanation

Explanation/Reference:
http://linux.die.net/man/8/pam_nologin

pam_nologin - Prevent non-root users from login

http://linux.die.net/man/5/nologin

If the file /etc/nologin exists, login(1) will allow access only to root. Other users will be shown the contents of this file and their logins will be refused.

QUESTION 29
A network has many network printers connected and they should get their addresses using DHCP. What information from each printer is needed to always assign them the same IP address when dhcpd is used as the DHCP server?

A. MAC address
B. Host name
C. Serial number
D. Factory default IP address
E. Built-in network card type

Correct Answer: A
Section: 210.1 DHCP configuration
Explanation

Explanation/Reference:
http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/index.jsp?topic=%2Fcom.ibm.tivoli.tpm.osdimg.doc%2Finstall%2Frosd_dhcpdconfexample.html

```
# this is the section for the x86
host ibmx3655  {
```

```
hardware ethernet 00:14:5E:5A:31:57;
fixed-address 10.0.0.200;
option dhcp-parameter-request-list 1,6,15,60,43;
option subnet-mask 255.255.255.0;
option domain-name-servers 10.0.0.20;
option domain-name "site";
option vendor-class-identifier "PXEClient";
  vendor-option-space PXE;
    option PXE.discovery-control 7;
    option PXE.boot-server 15 1 10.0.0.20;
    option PXE.boot-menu 15  15 "Tpm for OSd 7.1";
    option PXE.menu-prompt 0 "Tpm for Osd";
}
```

QUESTION 30
Which daemon is required on the client if an ethernet device gets its IP address from a central server?

A. `dhcp`
B. `dhcpcd`
C. `bootpd`
D. `ethd`
E. `dhcpd`

Correct Answer: B
Section: 210.1 DHCP configuration
Explanation

Explanation/Reference:
http://www.daemon-systems.org/man/dhcpcd.8.html

DHCPCD(8) NetBSD System Manager's Manual DHCPCD(8)

NAME
dhcpcd -- an RFC 2131 compliant DHCP client

QUESTION 31
What command can be used to check the Samba configuration file?

A. `testconfig`
B. `testsmbconfig`
C. `smbtestcfg`
D. `smbtestparm`
E. `testparm`

Correct Answer: E
Section: 209.1 SAMBA Server Configuration
Explanation

Explanation/Reference:
http://linux.die.net/man/1/testparm

testparm - check an smb.conf configuration file for internal correctness

QUESTION 32
Which Squid configuration directive defines the authentication method to use?

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

Correct Answer: A
Section: 208.3 Implementing a proxy server
Explanation

Explanation/Reference:
http://www.squid-cache.org/Doc/config/auth_param/

This is used to define parameters for the various authentication schemes supported by Squid.

QUESTION 33
Which entry in the `.procmailrc` file will send a copy of an email to another mail address?

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

Correct Answer: A
Section: 211.2 Managing Local E-Mail Delivery
Explanation

Explanation/Reference:
http://linux.die.net/man/5/procmailrc

c - Generate a carbon copy of this mail. This only makes sense on delivering recipes. The only non-delivering recipe this flag has an effect on is on a nesting block, in order to generate a carbon copy this will clone the running procmail process (lockfiles will not be inherited), whereby the clone will proceed as usual and the parent will jump across the block.

QUESTION 34
A security-conscious administrator would change which TWO of the following lines found in an SSH configuration file?

A. `Protocol 2,1`
B. `PermitEmptyPasswords no`
C. `Port 22`
D. `PermitRootLogin yes`
E. `IgnoreRhosts yes`

Correct Answer: AD
Section: 212.3 Secure shell (SSH)
Explanation

Explanation/Reference:
http://unixhelp.ed.ac.uk/CGI/man-cgi?sshd_config+5

Protocol

Specifies the protocol versions sshd supports. The possible values are "1" and "2". Multiple versions must be comma-separated. The default is "2,1". Note that the order of the protocol list does not indicate preference, because the client selects among multiple protocol versions offered by the server. Specifying "2,1" is identical to "1,2".

(...)

PermitRootLogin

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

If this option is set to "without-password" password authentication is disabled for root.

If this option is set to "forced-commands-only" root login with public key authentication will be allowed, but only if the command option has been specified (which may be useful for taking remote backups even if root login is normally not allowed). All other authentication methods are disabled for root.

If this option is set to "no" root is not allowed to log in.

QUESTION 35
When connecting to an SSH server for the first time, its fingerprint is received and stored in a file, which is located at:

A. `~/.ssh/fingerprints`
B. `~/.ssh/id_dsa`
C. `~/.ssh/known_hosts`
D. `~/.ssh/id_dsa.pub`
E. `~/.ssh/gpg.txt`

Correct Answer: C
Section: 212.3 Secure shell (SSH)
Explanation

Explanation/Reference:
http://linux.die.net/man/1/ssh

~/.ssh/known_hosts
Contains a list of host keys for all hosts the user has logged into that are not already in the systemwide list of known host keys. See sshd(8) for further details of the format of this file.

QUESTION 36
You have a web server running behind the firewall on IP 192.168.0.5 and you want to allow public access. The firewall's external IP is 10.0.0.10. Determine which rule(s) is/are required to make this work (your default policy is ACCEPT for all chains):

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

Correct Answer: B
Section: 212.1 Configuring a router
Explanation

Explanation/Reference:
Explanation: DNAT -> set in the PREROUTING chain where filtering uses translated address.
iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT --to-destination 192.168.0.5:80
redirects the request to 192.168.0.5 host on same port 80.
-p means protocol
--dport means destination port.

QUESTION 37
You use `pam_lastlog.so` modules to make sure that an entry is made in lastlog during login. Under which authentication management type should this module be listed?

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

Correct Answer: D
Section: 210.2 PAM authentication
Explanation

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

QUESTION 38
How can you manually add an entry to your system's ARP cache?

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

Correct Answer: D
Section: 210.1 DHCP configuration
Explanation

Explanation/Reference:
http://linux.die.net/man/8/arp

-s hostname hw_addr, --set hostname
Manually create an ARP address mapping entry for host hostname with hardware address set to hw_addr class, but for most classes one can assume that the usual presentation can be used. For the Ethernet class, this is 6 bytes in hexadecimal, separated by colons. When adding proxy arp entries (that is those with the publish flag set a netmask may be specified to proxy arp for entire subnets. This is not good practice, but is supported by older kernels because it can be useful. If the temp flag is not supplied entries will be permanent stored into the ARP cache.
NOTE: As of kernel 2.2.0 it is no longer possible to set an ARP entry for an entire subnet. Linux instead does automagic proxy arp when a route exists and it is forwarding. See arp(7) for details.

QUESTION 39

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

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

Correct Answer: AB
Section: 208.2 Maintaining a web server
Explanation

Explanation/Reference:
http://httpd.apache.org/docs/2.2/dns-caveats.html

```
<VirtualHost www.abc.dom>
ServerAdmin webgirl@abc.dom
DocumentRoot /www/abc
</VirtualHost>
```

In order for Apache to function properly, it absolutely needs to have two pieces of information about each virtual host: the ServerName and at least one IP address that the server will bind and respond to. The above example does not include the IP address, so Apache must use DNS to find the address of www.abc.dom. If for some reason DNS is not available at the time your server is parsing its config file, then this virtual host **will not be configured**. It won't be able to respond to any hits to this virtual host (prior to Apache version 1.2 the server would not even boot).

QUESTION 40
You receive complaints that a user sends large attachments to hundreds of users. What command do you use to investigate the mail message queued for delivery?

A. `mailq`
B. `sendmail -q`
C. `mqueue`
D. `qm`
E. `lpq`

Correct Answer: A
Section: 211.1 Using e-mail servers
Explanation

Explanation/Reference:
http://linux.die.net/man/1/mailq.postfix

List the mail queue. Each entry shows the queue file ID, message size, arrival time, sender, and the recipients that still need to be delivered. If mail could not be delivered upon the last attempt, the reason for failure is shown.

QUESTION 41
Your server is running Sendmail. The file `/etc/mail/access` contains the following line:
`Somedomain.com 550`
What does it mean?

A. Your server relays mail from all servers on domain somedomain.com

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

Correct Answer: D
Section: 211.1 Using e-mail servers
Explanation

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

Exam D

QUESTION 1
According to the dhcpd.conf file below, which domain name will clients in the 172.16.87.0/24 network get?

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

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

subnet 172.16.88.0 netmask 255.255.255.0 {
    range 172.16.88.128 172.16.88.254;
    option broadcast-address 172.16.88.255;
    option domain-name-servers 172.16.87.1;
}
```

Correct Answer: lab.certkiller.com
Section: 210.1 DHCP configuration
Explanation

Explanation/Reference:
http://linux.die.net/man/5/dhcpd.conf
In Figure 1 there is also a group statement, which provides common parameters for a set of three hosts - zappo, beppo and harpo. As you can see, these hosts are all in the test.isc.org domain, so it might make sense for a group-specific parameter to override the domain name supplied to these hosts:
option domain-name "test.isc.org";

QUESTION 2
Which file, in the local file-system, is presented when the client requests `http://server/~joe/index.html` and the following directive is present in server's Apache configuration file?

```
    UserDir site/html
```

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

Correct Answer: /home/joe/site/html/index.html
Section: 208.1 Implementing a web server
Explanation

Explanation/Reference:
http://httpd.apache.org/docs/2.2/mod/mod_userdir.html

mod_userdir- This module allows user-specific directories to be accessed using the http://example.com/~user/ syntax.

```
OptionName  directive used     Translated path
UserDir     /usr/web           /usr/web/bob/one/two.html
```

QUESTION 3
Enter one of the Apache configuration file directives that defines where log files are stored.

Correct Answer: ErrorLog

Section: 208.1 Implementing a web server
Explanation

Explanation/Reference:
http://httpd.apache.org/docs/2.2/mod/core.html#errorlog

ErrorLog - Location where the server will log errors

QUESTION 4
A malicious user has sent a 35MB video clip, as an attachment, to hundreds of Recipients. Looking in the outbound queue reveals that this is the only mail there.

This mail can be removed with the command rm _____ * . Complete the path below.

Correct Answer: /var/spool/mqueue/
Section: 211.1 Using e-mail servers
Explanation

Explanation/Reference:
http://linux.die.net/man/8/sendmail.sendmail

/var/spool/mqueue/*
temp files

QUESTION 5
A procmail recipe is required to delete all emails marked as spam. Please complete the recipe.

```
:0:

* X-Spam-Status: Yes
```

Correct Answer: /dev/null
Section: 211.2 Managing Local E-Mail Delivery
Explanation

Explanation/Reference:
http://www.gsp.com/cgi-bin/man.cgi?topic=procmailrc

A line starting with ':' marks the beginning of a recipe. It has the following format:

:0 [flags] [: [locallockfile]]
<zero or more conditions (one per line)>
<exactly one action line>
(...)

QUESTION 6
Where is the user foo's procmail configuration stored, if home directories are stored in `/home`?
Please enter the complete path to the file.

Correct Answer: /home/foo/.procmailrc
Section: 211.2 Managing Local E-Mail Delivery
Explanation

Explanation/Reference:
http://linux.die.net/man/5/procmailrc

procmailrc - procmail rcfile
Synopsis

$HOME/.procmailrc

QUESTION 7
What command must be used to create an SSH key-pair? Please enter the command without the path or any options or parameters.

Correct Answer: ssh-keygen
Section: 212.3 Secure shell (SSH)
Explanation

Explanation/Reference:
http://linux.die.net/man/1/ssh-keygen

ssh-keygen - authentication key generation, management and conversion

QUESTION 8
To allow X connections to be forwarded from or through an SSH server, what line must exist in the sshd configuration file?

Correct Answer: X11Forwarding yes
Section: 212.3 Secure shell (SSH)
Explanation

Explanation/Reference:
http://linux.die.net/man/5/sshd_config

X11Forwarding
Specifies whether X11 forwarding is permitted. The argument must be "yes" or "no". The default is "no".

QUESTION 9
Which keys are stored in the authorized_keys file?

Correct Answer: public
Section: 212.3 Secure shell (SSH)
Explanation

Explanation/Reference:
http://linux.die.net/man/8/sshd

~/.ssh/authorized_keys
Lists the **public keys** (RSA/DSA) that can be used for logging in as this user.

QUESTION 10
In which directory are the PAM modules stored?

Correct Answer: /lib/security
Section: 210.2 PAM authentication
Explanation

Explanation/Reference:
http://linux.die.net/man/5/pam.d
module-path is either the full filename of the PAM to be used by the application (it begins with a '/'), or a relative pathname from the default module location: /lib/security/ or /lib64/security/, depending on the architecture.

QUESTION 11
Which command can be used to change the password for an LDAP entry?

Correct Answer: ldappasswd
Section: 210.3 LDAP client usage
Explanation

Explanation/Reference:
http://linux.die.net/man/1/ldappasswd

ldappasswd - change the password of an LDAP entry

QUESTION 12
Which Apache directive is used to configure the main directory for the site, out of which it will serve documents?

Correct Answer: DocumentRoot
Section: 208.1 Implementing a web server
Explanation

Explanation/Reference:
http://httpd.apache.org/docs/2.2/mod/core.html#documentroot

DocumentRoot - Directory that forms the main document tree visible from the web

QUESTION 13
Which file on a Postfix server modifies the sender address for outgoing e-mails? Please enter only the file name without the path

Correct Answer: sender_canonical
Section: 211.1 Using e-mail servers
Explanation

Explanation/Reference:
http://www.postfix.org/postconf.5.html#sender_canonical_maps

Example:

sender_canonical_maps = hash:/etc/postfix/sender_canonical

CAREFUL IF ON THE ACTUAL TEST IF IT WOULD ASK FULL PATH OR NOT!

QUESTION 14
Which command can be used to save the current iptables rules into a file? Please enter only the command without path or parameters.

Correct Answer: iptables-save
Section: 212.5 Security tasks
Explanation

Explanation/Reference:
http://linux.die.net/man/8/iptables-save

iptables-save -- dump iptables rules to stdout

QUESTION 15
All machines outside the network are able to send emails through the server to addresses not served by that server. If the server accepts and delivers the email, then it is a(n) _____.

Please enter the English term, without any punctuation.

Correct Answer: open relay
Section: 211.1 Using e-mail servers
Explanation

Explanation/Reference:
http://www.spamhelp.org/shopenrelay/

What is an open relay?
An open relay (sometimes also referred to as a third-party relay) is a mail server that does not verify that it is authorised to send mail from the email address that a user is trying to send from. Therefore, users would be able to send email originating from any third-party email address that they want.

QUESTION 16
Please enter the complete command to create a new password file for HTTP basic authentication (/home/http/data/web _passwd) for user john.

Correct Answer: htpasswd -c /home/http/data/web_passwd john
Section: 208.1 Implementing a web server
Explanation

Explanation/Reference:
http://httpd.apache.org/docs/2.2/programs/htpasswd.html

For User based Authentication, you should create the htpasswd user. First Time To create the user:
htpasswd -c filename username

QUESTION 17
With which parameter in the smb.conf file can a share be hidden?

Correct Answer: $
Section: 209.1 SAMBA Server Configuration
Explanation

Explanation/Reference:
You add an "$" in the end of the share name.

Example:

```
[secret$]
   comment = Dont tell anyone
   path = /opt/secret_files
   read only = no
```

Also:

http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html
If this parameter is set to yes for a share, then the share will be an administrative share. The Administrative Shares are the default network shares created by all Windows NT-based operating systems. These are shares like C$, D$ or ADMIN$. The type of these shares is STYPE_DISKTREE_HIDDEN.

QUESTION 18
nfsd, portmap and _____ daemons must be running on an NFS server.

Correct Answer: rpc.mountd
Section: 209.2 NFS Server Configuration
Explanation

Explanation/Reference:
CORRECTED from mountd to rpc.mountd

In Linux, it's `rpc.mountd`. On unix systems it's `mountd`.
http://linux.die.net/man/8/rpc.mountd

rpc.mountd - NFS mount daemon

http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/network-nfs.html

(...)In order for this to function properly a few processes have to be configured and running.

The server has to be running the following daemons:

```
Daemon     Description
nfsd       The NFS daemon which services requests from the NFS clients.
mountd     The NFS mount daemon which carries out the requests that nfsd(8)
passes on to it.
rpcbind    This daemon allows NFS clients to discover which port the NFS server
is using.
```

QUESTION 19
You are not sure whether the kernel has detected a piece of hardware in your machine. What command, without options or parameters, should be run to present the contents of the kernel ring-buffer?

Correct Answer: dmesg
Section: 213.2 General troubleshooting
Explanation

Explanation/Reference:
http://linux.die.net/man/8/dmesg

dmesg is used to examine or control the kernel ring buffer.

The program helps users to print out their bootup messages.

QUESTION 20
Which program lists information about files opened by processes and produces output that can be parsed by other programs?

Correct Answer: lsof
Section: 213.2 General troubleshooting
Explanation

Explanation/Reference:
http://linux.die.net/man/8/lsof

lsof - list open files
Lsof revision N lists on its standard output file information about files opened by processes(...)

QUESTION 21
Which site-specific configuration file for the shadow login suite must be modified to log login failures? Please enter the complete path to that file.

Correct Answer: /etc/login.defs
Section: 213.4 Troubleshooting environment configurations
Explanation

Explanation/Reference:

http://linux.die.net/man/5/login.defs

FAILLOG_ENAB (boolean)
Enable logging and display of /var/log/faillog login failure info.

QUESTION 22
Which Samba-related command will show all options that were not modified using smb.conf and thus are set to their default values? Please enter the command and its parameter(s):

Correct Answer: testparm -v
Section: 209.1 SAMBA Server Configuration
Explanation

Explanation/Reference:
http://linux.die.net/man/1/testparm

-v
If this option is specified, testparm will also output all options that were not used in smb.conf(5) and are thus set to their defaults.

QUESTION 23
What is the path to the global postfix configuration file? (Please specify the complete directory path and file name)

Correct Answer: /etc/postfix/main.cf
Section: 211.1 Using e-mail servers
Explanation

Explanation/Reference:
http://linux.die.net/man/1/postconf

Files

/etc/postfix/main.cf, Postfix configuration parameters

QUESTION 24
What postfix configuration setting defines the domains for which Postfix will deliver mail locally? (Please provide only the configuration setting name with no other information)

Correct Answer: mydomain
Section: 211.1 Using e-mail servers
Explanation

Explanation/Reference:
http://linux.die.net/man/5/main.cf
mydomain (default: see postconf -d output)

The internet domain name of this mail system. The default is to use $myhostname minus the first component. $mydomain is used as a default value for many other configuration parameters.

Example:

mydomain = domain.tld

QUESTION 25
The command _____ -x foo will delete the user foo from the Samba database. (Specify the command only, no path information.)

Correct Answer: smbpasswd
Section: 209.1 SAMBA Server Configuration
Explanation

Explanation/Reference:
http://www.samba.org/samba/docs/man/manpages-3/smbpasswd.8.html

smbpasswd — change a user's SMB password

QUESTION 26
In which directory can all parameters available to sysctl be found? (Provide the full path)

Correct Answer: /proc/sys
Section: 213.3 Troubleshooting system resources
Explanation

Explanation/Reference:
http://linux.die.net/man/8/sysctl

sysctl is used to modify kernel parameters at runtime. The parameters available are those listed under `/proc/sys/`.

QUESTION 27
Instead of running the command `echo 1 >/proc/sys/net/ipv4/ip_forward`, the configuration setting is going to be added to /etc/sysctl.conf. What is the missing value in the configuration line below? (Please specify only the missing value)

Correct Answer: net.ipv4.ip_forward
Section: 212.1 Configuring a router
Explanation

Explanation/Reference:
https://wiki.archlinux.org/index.php/Sysctl

# Disable packet forwarding
net.ipv4.ip_forward = 0

QUESTION 28
What is the name of the module in Apache that provides the HTTP Basic Authentication functionality? (Please provide ONLY the module name)

Correct Answer: mod_auth
Section: 208.1 Implementing a web server
Explanation

Explanation/Reference:
I hope LPI will comply with Apache http 2.0, because in httpd 2.2 it was changed to mod_auth_basic.

We are lost because LPI says:

http://www.lpi.org/linux-certifications/programs/lpic-2/exam-202
Apache 2.x configuration files, terms and utilities

http://httpd.apache.org/docs/2.0/mod/mod_alias.html
Provides for mapping different parts of the host filesystem in the document tree and for URL redirection

http://httpd.apache.org/docs/2.2/en/mod/mod_auth_basic.html
This module allows the use of HTTP Basic Authentication to restrict access by looking up users in the given

providers.

QUESTION 29
What command is used to print NFS kernel statistics? (Provide the command with or without complete path)

Correct Answer: nfsstat
Section: 209.2 NFS Server Configuration
Explanation

Explanation/Reference:
linux.die.net/man/8/nfsstat

The nfsstat displays statistics kept about NFS client and server activity.

QUESTION 30
What is the default location for sendmail configuration files? (Please provide the complete path to the directory)

Correct Answer: /etc/mail
Section: 211.1 Using e-mail servers
Explanation

Explanation/Reference:
all files are in /etc/mail

http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/sendmail.html

sendmail uses the following configuration files:

```
Filename     Function
/etc/mail/access     sendmail access database file
/etc/mail/aliases     Mailbox aliases
/etc/mail/local-host-names     Lists of hosts sendmail accepts mail for
/etc/mail/mailer.conf     Mailer program configuration
/etc/mail/mailertable     Mailer delivery table
/etc/mail/sendmail.cf     sendmail master configuration file
/etc/mail/virtusertable     Virtual users and domain tables
```

QUESTION 31
Postfix daemons can be chroot'd by setting the chroot flag in _____. (Supply only the filename, without a path)

Correct Answer: master.cf
Section: 211.1 Using e-mail servers
Explanation

Explanation/Reference:
http://www.postfix.org/BASIC_CONFIGURATION_README.html#chroot_setup

Postfix daemon processes can be configured (via the master.cf file) to run in a chroot jail.

QUESTION 32
LDAP-based authentication against a newly-installed LDAP server does not work as expected. The file /etc/pam.d/login includes the following configuration parameters. Which of them is NOT correct?

A. `password required /lib/security/pam_ldap.so`
B. `auth sufficient /lib/security/pam_ldap.so use_first_pass`
C. `account sufficient /lib/security/pam_ldap.so`

D. `password required /lib/security/pam_pwdb.so`
E. `auth required /lib/security/pam_ldap.so`

Correct Answer: E
Section: 210.3 LDAP client usage
Explanation

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

QUESTION 33
When the default policy for the iptables INPUT chain is set to DROP, why should a rule allowing traffic to localhost exist?

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

Correct Answer: D
Section: 212.1 Configuring a router
Explanation

Explanation/Reference:
http://wiki.centos.org/HowTos/Network/IPTables
`iptables -A INPUT -i lo -j ACCEPT` - Now it's time to start adding some rules. We use the -A switch to append (or add) a rule to a specific chain, the INPUT chain in this instance. Then we use the -i switch (for interface) to specify packets matching or destined for the lo (localhost, 127.0.0.1) interface and finally -j (jump) to the target action for packets matching the rule - in this case ACCEPT. So this rule will allow all incoming packets destined for the localhost interface to be accepted. **This is generally required as many software applications expect to be able to communicate with the localhost adaptor.**

QUESTION 34
When connecting to an SSH server for the first time, its fingerprint is received and stored in a file, which is located at:

A. `~/.ssh/fingerprints`
B. `~/.ssh/id_dsa`
C. `~/.ssh/known_hosts`
D. `~/.ssh/id_dsa.pub`
E. `~/.ssh/gpg.txt`

Correct Answer: C
Section: 212.3 Secure shell (SSH)
Explanation

Explanation/Reference:
http://linux.die.net/man/1/ssh

~/.ssh/known_hosts
Contains a list of host keys for all hosts the user has logged into that are not already in the systemwide list of known host keys. See sshd(8) for further details of the format of this file.

QUESTION 35

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

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

Correct Answer: E
Section: 208.1 Implementing a web server
Explanation

Explanation/Reference:
apachectl is a HTTP server control interface .
Syntax: apachectl [httpd-argument]
either reports Syntax OK or detailed information about the particular error. This is equivalent to apachectl -t .

QUESTION 36
What is the name and path of the default configuration file used by the syslogd daemon?

Correct Answer: /etc/syslog.conf
Section: 213.4 Troubleshooting environment configurations
Explanation

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

QUESTION 37
You wish to have all mail messages except those of type `info` to the `/var/log/mailmessages` file. Which of the following lines in your `/etc/syslog.conf` file would accomplish this?

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

Correct Answer: D
Section: 213.4 Troubleshooting environment configurations
Explanation

Explanation/Reference:
The first part of the answer, "mail.*" instructs syslogd to log all types of mail messages, which is not what we want (the syntax is mail.type). However, the second part of the answer, "mail.!=info" overrules that and instructs syslogd to ignore mail messages of the type 'info'. 'Info' is a 'serverity level' for the message. Examples of other levels are err and crit.

Reference: http://nodevice.com/sections/ManIndex/man1597.html
Incorrect Answers
A: There must be a dot (period) separating mail and !=info.
B: The exclamation mark (!) means to ignore this type. This answer will only log the info type.
We want to ignore the info type.
C: This answer will log all mail messages of type 'info' or above. We want to exclude the 'info' type.

QUESTION 38
Which of the following lines in your `/etc/syslog.conf` file will cause all critical messages to be logged to the file `/var/log/critmessages`?

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

Correct Answer: A
Section: 213.4 Troubleshooting environment configurations
Explanation

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

QUESTION 39
What daemon is responsible for tracking events on your system?

Correct Answer: syslogd
Section: 213.4 Troubleshooting environment configurations
Explanation

Explanation/Reference:
Syslogd (system log deamon) is responsible for tracking and logging system events.

QUESTION 40
What file defines the levels of messages written to system log files? Provide the file name only

Correct Answer: syslog.conf
Section: 213.4 Troubleshooting environment configurations
Explanation

Explanation/Reference:
The file /etc/syslog.conf contains information used by the system log daemon, syslogd to forward a system message to appropriate log files and/or users.

QUESTION 41
____ is a tool for creating and extracting archives, or copying files from one place to another. It has copy-out mode, copy-in mode and copy-pass mode.

Correct Answer: cpio
Section: 213.2 General troubleshooting
Explanation

Explanation/Reference:
I don't remember how in the exam asked about this, but it asked something similar of what i'm asking.

http://linux.die.net/man/1/cpio

Guess what? cpio is not part of LPI-202 (as far as i checked), so i'm filing this as 213.2 - general troubleshooting

QUESTION 42
Considering the following kernel IP routing table below, which of the following commands must be used to remove the route to the network `10.10.1.0/24`?

```
Kernel IP routing table
Destination      Gateway          Genmask         Flags  Metric  Ref  Use  Iface
200.207.199.162  0.0.0.0          255.255.255.255 UH     0       0    0    ppp0
172.16.87.0      0.0.0.0          255.255.255.0   U      0       0    0    eth0
192.168.246.0    0.0.0.0          255.255.255.0   U      0       0    0    eth1
10.10.1.0        192.168.246.11   255.255.255.0   UG     0       0    0    eth1
127.0.0.0        0.0.0.0          255.0.0.0       U      0       0    0    lo
0.0.0.0.0        200.207.199.162  0.0.0.0         UG     0       0    0    ppp0
```

A. `route del 10.10.1.0`
B. `route del 10.10.1.0/24`
C. `route del -net 10.10.1.24`
D. `route del 10.10.1.0/24 gw 192.168.246.11`
E. `route del -net 10.10.1.0`

Correct Answer: C
Section: 212.1 Configuring a router
Explanation

Explanation/Reference:
http://linux.die.net/man/8/route

When the **add** or **del** options are used, route modifies the routing tables. Without these options, route displays the current contents of the routing tables.

(...)

`route add -net 127.0.0.0`
adds the normal loopback entry, using netmask 255.0.0.0 (class A net, determined from the destination address) and associated with the "lo" device (assuming this device was prviously set up correctly with ifconfig (8)).

QUESTION 43
The command route shows the following output:

```
Destination    Gateway         Genmask           Flags  Metric  Ref  Use  Iface
194.168.123.5  -                255.255.255.255  !H     0       0    0    -
192.168.123.0  0.0.0.0          255.255.255.0    U      0       0    0    eth2
169.254.0.0    0.0.0.0          255.255.0.0      U      0       0    0    eth1
127.0.0.0      0.0.0.0          255.0.0.0        U      0       0    0    lo
0.0.0.0        192.168.123.254  0.0.0.0          UG     0       0    0    eth0
```

Which of the following statements is correct?

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

Correct Answer: C
Section: 212.1 Configuring a router
Explanation

Explanation/Reference:
http://linux.die.net/man/8/route
(...)
Flags
Possible flags include
U (route is up)
H (target is a host)
G (use gateway)
R (reinstate route for dynamic routing)
D (dynamically installed by daemon or redirect)
M (modified from routing daemon or redirect)
A (installed by addrconf)
C (cache entry)
! (reject route)

QUESTION 44
A network client has an ethernet interface configured with an IP address in the subnet 192.168.0.0/24. This subnet has a router, with the IP address 192.168.0.1, that connects this subnet to the Internet. What needs to be done on the client to enable it to use the router as its default gateway?

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

Correct Answer: A
Section: 212.1 Configuring a router
Explanation

Explanation/Reference:
http://www.cyberciti.biz/faq/linux-setup-default-gateway-with-route-command/

For example if your router IP address is 192.168.1.254 type the following command as the root user:

```
# route add default gw 192.168.1.254 eth0
```

QUESTION 45
What command is used to add a route to the 192.168.4.0/24 network via 192.168.0.2?

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

D. `route add -net 192.168.4.0 netmask 255.255.255.0 192.168.0.2`
E. `route add -net 192.168.4.0 netmask 255.255.255.0 gw 192.168.0.2`

Correct Answer: E
Section: 212.1 Configuring a router
Explanation

Explanation/Reference:
http://linux.die.net/man/8/route
(...)
examples:
`route add -net 192.57.66.0 netmask 255.255.255.0 gw ipx4`
This command adds the net "192.57.66.x" to be gatewayed through the former route to the SLIP interface.