**QUESTION: 1**
An administrator has just configured an OpenVPN client. Upon starting the service, the following message is displayed:

*TLS Error: TLS key negotiation failed to occur within 60 seconds*

Which of the following statements is true?

- **A. The client was unable to establish a network connection with the server.**
- B. The client was able to establish a network connection with the server, however TLS key negotiation failed, resulting in a fallback to SSL.
- C. The client was able to establish a network connection with the server, however TLS and SSL security are not enabled.
- D. The client was able to establish a network connection with the server, however TLS key negotiation took longer than 60 seconds, indicating that there may be a problem with network performance.

http://openvpn.net/index.php/open-source/faq/79-client/253-tls-error-tls-key-negotiation-failed-to-occur-within-60-seconds-check-your-network-connectivity.html

**QUESTION: 2**
SELinux has just been installed on a Linux system and the administrator wants to use SELinux in permissive mode in order to audit the various services on the system. What command will switch SELinux into permissive mode?

- **A. setenforce 0**
- B. /etc/init.d/selinux stop
- C. selinux passive
- D. /etc/init.d/selinux startpassive

**QUESTION: 3**
Which of the following export options, when specified in /etc/exports, will tell the server to use the NFSv4 Pseudofilesystem?

- A. fsid=2
- **B. fsid=0**
- C. fsid=3
- D. fsid=1

**QUESTION: 4**
Which of the following are common techniques for securing a sendmail server? (Select THREE correct answers)

- A. Maintain user accounts in an LDAP directory.
- **B. Enable TLS.**
- **C. Disable VRFY.**
- **D. Run sendmail in a chroot'd environment.**
- E. Disable USRLKUP.

**QUESTION: 5**
What does ntop use for data collection?

- **A. Network packets**

- B. Log files
- C. Frame relay
- D. SNMP

http://luca.ntop.org/OpenSourceConf_Athens2008.pdf

**QUESTION: 6**
CORRECT TEXT
An administrator has successfully configured a cryptographic volume for dmcrypt, and has added the following line to /etc/fstab:

*/dev/mapper/cryptvol /media/crypt auto defaults 0 0*

Upon booting the system, the error message "mount: special device /dev/mapper/cryptvol does not exist" is displayed. What configuration file has the administrator forgotten to edit? (Provide the full path and filename)

**/etc/crypttab**

**QUESTION: 7**
CORRECT TEXT
What command will **remove** the dmcrypt mapping named crypt-vol? (Provide the command with any options and parameters)

**cryptsetup remove** crypt-vol// luksClose

**QUESTION: 8**
CORRECT TEXT
Which LUKS action, when supplied to the cryptsetup command, will initialize a LUKS partition and set the initial key? (Provide only the action name)

**luksFormat**

**QUESTION: 9**
An administrator has created a mapping with the following command: cryptsetup luksOpen /dev/sda1 cryptvol and has set three different keys. Which command below will delete the first key?

- **A. cryptsetup luksDelKey /dev/sda1 0**
- B. cryptsetup luksDelKey /dev/sda1 1
- C. cryptsetup luksDelKey /dev/mapper/cryptvol 1
- D. cryptsetup luksDelKey /dev/mapper/cryptvol 0

**QUESTION: 10**
CORRECT TEXT
What command will list basic information about all targets available to cryptmount? (Provide the command with any options or parameters)

**cryptmount -l** // cryptmount --list

If you create more than one encrypted filesystem **cryptsetup -l** displays a list. Users can change their passwords with **cryptsetup -c [targetname]**.

**QUESTION: 11**
Which of the following are valid dmcrypt modes? (Choose THREE correct answers)

- **A. XTS**
- **B. ESSIV**
- C. GMR
- D. KWG
- **E. LRW**

# Pista, sólo hay 4 en el temario: http://wiki.lpi.org/wiki/LPIC-303#320.3_Encrypted_Filesystems
CBC, ESSIV, LRW and XTS modes

**QUESTION: 12**
CORRECT TEXT
Which directive in the OpenVPN client.conf specifies the remote server and port that the client should connect to? (Provide only the directive, without any options or parameters)

**remote**

**QUESTION: 13**
You are certain that your kernel has been compiled with ACL support, however, when you try to set an ACL on a file, you get the following output:

*% setfacl -m user:hugh:r afile.txt*
*setfacl: afile.txt: Operation not supported*

What is the most likely reason for this problem?

- A. There is an error in the command line parameters.
- B. There is no user on the system named hugh.
- **C. The partition has not been mounted with the acl option.**
- D. The file afile.txt doesn't exist.

Ejemplo, en /etc/fstab:
/dev/sdb6 /media/data ext3 defaults,**acl** 0 1

http://www.techrepublic.com/article/learn-to-use-extended-filesystem-acls/

**QUESTION: 14**
Which of the following are valid **OpenVPN** authentication modes? (Choose TWO correct answers)

- A. S/Key
- B. Kerberos
- **C. Static Key**
- D. Password
- **E. TLS**

http://openvpn.net/index.php/open-source/documentation/security-overview.html
OpenVPN has two authentication modes:

- **Static Key** -- Use a pre-shared static key

http://openvpn.net/index.php/open-source/documentation/miscellaneous/78-static-key-mini-howto.html

- **TLS** -- Use SSL/TLS + certificates for authentication and key exchange

**QUESTION: 15**
What is true about the permissions for the file afile given the following output from getfacl? (Select TWO correct answers)

*% getfacl afile*
*# file: afile*
*# owner: matt*
*# group: support*

*user::rwx*
*user:hugh:**r**w* <----
*group::r*
*group:staff:**rx*** <----
*mask::rwx*
*other::r*

- A. Anyone in the support group will be able to read and execute the file.
- **B. The user hugh will be able to read the contents of the file.**
- C. Anyone in the users group will be able to read the file.
- D. The user matt will not be able to edit this file.
- **E. Anyone in the staff group will be able to read and execute the file.**

**QUESTION: 16**
You wish to revoke write access for all groups and named users on a file. Which command will make the correct ACL changes?

- A. setfacl -x group:*:rx,user:*:rx afile Option -x: Invalid argument)
- B. setfacl -x mask::rx afile (Option -x: Invalid argument)
- **C. setfacl -m mask::rx afile**
- D. setfacl -m group:*:rx,user:*:rx afile (Option -m: Invalid argument)

**mask::rwx** -- limita os permisos efectivos que se conceden aos usuarios e grupos enumerados. **(groups and named users)**
-- Os permisos do dono e de "others" non se ven afectados por mask

**QUESTION: 17**
CORRECT TEXT
What is the default UDP port for OpenVPN traffic?

**1194**

**QUESTION: 18**
When adding additional users to a file's extended ACLs, what is true about the default behaviour of the ACL mask for the file?

- A. The mask is modified to be the union of all permissions of the file owner, owning group and all named users and groups.
- B. The mask is left unchanged.
- C. If required, a warning is printed indicating that the mask is too restrictive for the permissions being granted.
- D. **The mask is modified to be the union of all permissions of the owning group and all named users and groups.**

**setfacl -m user:geeko:rwx,group:mascots:rwx mydir**
In addition to the entries initiated for the user geeko and the group mascots, a mask entry has been

generated. This mask entry is set automatically so that all permissions are effective. **setfacl** automatically adapts existing mask entries to the settings modified, unless you deactivate this feature with **-n**. mask defines the maximum effective access permissions for **all entries in the group class. This includes named user, named group, and owning group.** The group class permission bits displayed by **ls** -dl mydir now correspond to the mask entry.

**mask::rwx** -- limita os permisos efectivos que se conceden aos usuarios e grupos enumerados. (E GRUPO PROPIETARIO ???)
-- Os permisos do dono e de "others" non se ven afectados por mask

**QUESTION: 19**
In which of the following scenarios MUST an administrator use **ethernet bridging instead of routing** when configuring an **OpenVPN** site? (Select TWO correct answers)

- A. Some OpenVPN clients will be installed on laptops and must be able to connect from different locations.
- **B. NetBIOS traffic must be able to traverse the VPN without implementing a WINS server.**
- C. The IPv4 protocol is required.
- D. It will be necessary to use an MTU setting other than the default.
- **E. The IPX protocol is required.**

http://openvpn.net/index.php/open-source/documentation/howto.html#vpntype
**dev tap**
**server-bridge 10.8.0.4 255.255.255.0 10.8.0.50 10.8.0.100**
ethernet bridging :

- the VPN needs to be able to handle non-IP protocols **such as IPX**,
- you are running applications over the VPN which rely on network broadcasts (such as LAN games), or
- you would like to allow browsing of Windows file shares across the VPN **without setting up a Samba or WINS server.**

**QUESTION: 20**
Linux Extended Attributes include attribute classes. Which of the following are included in the defined attribute classes? (Select THREE correct answers)

- A. default
- **B. system**
- C. owner
- **D. trusted**
- **E. user**

man 5 attr ( falta **security)**
http://www.bestbits.at/acl/man/man5/attr.txt

**QUESTION: 21**
Which of the following statements are true about Linux Extended Attributes on files? (Select TWO correct answers)

- **A. An attribute value may be empty.**
- B. Attribute storage counts toward disk quota use.
- **C. Attribute use is enabled by mounting a partition with the attr option.**
- D. An attribute is file, notinode, specific. Thus, a hard linked file in two locations could have different attributes.

- E. Attributes are not used by SELinux and other kernel security modules.

Ejemplo:
/dev/sda2 /media/mount_point ext4 auto,users,**user_xattr** 0 2
http://askubuntu.com/questions/124102/how-do-i-enable-extended-attributes-on-ext4
http://www-01.ibm.com/support/knowledgecenter/linuxonibm/liaaz/fileprintxattr.htm?lang=en

**QUESTION: 22**
Which command will **set the user.author attribute** on the file afile.txt?

- A. setfattr user.author:"A. Author" afile.txt
- **B. setfattr -n user.author -v "A. Author" afile.txt**
- C. setfattr user.author="A. Author" afile.txt
- D. setfattr -a user.author="A. Author" afile.txt

http://wiki.kaspersandberg.com/doku.php?id=howtos:xattr

**QUESTION: 23**
Which of the following lines in the **OpenVPN** server.conf file will supply a DNS server for DHCP clients to use?

- **A. push "dhcp-option DNS 10.142.232.4"**
- B. push "dhcp DNS 10.142.232.4"
- C. push "options DNS 10.142.232.4"
- D. push "dhcp-options DNS 10.142.232.4"

https://openvpn.net/index.php/open-source/documentation/howto.html#server
**QUESTION: 24**
Which command will list all of the extended attributes on the file afile.txt along with the values?

- A. getfattr --all afile.txt
- B. getfattr afile.txt
- C. getfattr --list afile.txt
- **D. getfattr --dump afile.txt**

http://linux.die.net/man/1/getfattr
getfattr -d afile.txt (tambien)
http://wiki.kaspersandberg.com/doku.php?id=howtos:xattr

**QUESTION: 25**
Which of the following statements is true when querying the extended attributes of a file that has no extended attributes set?

- A. getfattr will print a warning and exit with a value of 0.
- B. getfattr will print a warning and exit with a value of 1.
- **C. No output will be produced and getfattr will exit with a value of 0.**
- D. No output will be produced and getfattr will exit with a value of 1.

**QUESTION: 26**
CORRECT TEXT
Which directive must be set to 0 in a host or service definition to prevent Nagios from sending more than one alert for a particular event? (Specify only the directive without any options or parameters).

**notification_interval**

http://www.ruby-doc.org/gems/docs/d/deprec-2.2.2/lib/deprec/templates/nagios/conf_d/services_nagios2_cfg.html

**QUESTION: 27**
What is the purpose of the Safe Checks option in a Nessus configuration?

- A. Enables secure scanning over an encrypted tunnel.
- **B. To prevent the use of plugins which may have a negative effect on the network being scanned.**
- C. To prevent the use of plugins which may leave the Nessus server vulnerable during the scanning process.
- D. When validating a Nessus configuration file, the nessusd process will not be

interrupted.

http://www.tenable.com/blog/understanding-the-nessus-safe-checks-option

**QUESTION: 28**
CORRECT TEXT
In Nessus, what does the acronym NASL stand for?
**Nessus Attack Scripting Language**

http://acronyms.thefreedictionary.com/Nessus+Attack+Scripting+Language

**QUESTION: 29**
An administrator is capturing traffic with Wireshark and is only seeing ARP traffic. What is the most likely cause of this?

- *A. The network interface on which the scan is running is not in promiscuous mode.*
- **B. The machine is on a switched network and is therefore only seeing local and broadcast/multicast packets.**
- C. The administrator did not enable the TCP and UDP options when starting the scan.
- D. The network interface on which the scan is running has the ARP_ONLY flag set.

http://www.wireshark.org/faq.html#q7.3

**QUESTION: 30**
Which statements are true of the following Wireshark capture filter:
(tcp[2:2] > 1500 and tcp[2:2] < 1550) or (tcp[4:2] > 1500 and tcp[4:2] < 1550) (Select TWO correct answers)

- A. Every packet being checked has a 2 byte offset.
- B. Traffic on ports 1500-1550 is being captured.
- **C. Traffic on ports 1501-1549 is being captured.**
- D. Only two bytes are being checked in each packet.
- **E. Up to four bytes are being check in each packet.**

http://www.wireshark.org/docs/man-pages/wireshark-filter.html#the_slice_operator

**QUESTION: 31**
The command 'nmap -sS -O 10.142.232.10' produces the following output:

*PORT STATE SERVICE*
*631/tcp open ipp*
*3306/tcp open mysql*

Which of these statements are true? (Select TWO correct answers)

- A. A simple scan was launched.
- **B. The scan was executed by the root user. (SYN scan)**
- C. Output will be sent to a file instead of stdout.
- **D. A stealth SYN scan was launched.**
- E. There are no other services running on this machine.

http://nmap.org/book/man-port-scanning-techniques.html

**QUESTION: 32**
Which of the following can be done to secure a BIND server? (Select THREE correct answers)

- **A. Run the BIND daemon as a non root user.**
- **B. Configure ACLs.**
- C. Require clients to authenticate with a password before querying the server.
- **D. Run the BIND daemon in a chroot jail**
- E. Encrypt DNS traffic using SSL/TLS.

http://www.aitechsolutions.net/dnsservertips.html
http://oreilly.com/catalog/dns4/chapter/ch11.html

**QUESTION: 33**
DNS servers are vulnerable to which of the following attacks? (Select THREE correct answers)

- **A. Cache Poisoning**
- B. Fork Bomb Attack
- C. Password Based Attack
- **D. Man in the Middle**
- **E. Smurf Attack**

http://www.serverbeach.com/resources/DNS-Smurf-Attacks-The-Lowdown
http://es.wikipedia.org/wiki/DNS_cache_poisoning
http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Understanding-Man-in-the-Middle-Attacks-ARP-Part2.html
**QUESTION: 34**

CORRECT TEXT
Which tool, distributed with BIND 9, will check the syntax of a named configuration file? (Supply only the program name, without any options or parameters)

**named-checkconf**
http://alopezaberasturi.blogspot.com.es/2012/09/valnidar-configuracion-bind-comandos.html

**QUESTION: 35**
The apache administrator has added the following lines to the configuration files:

*<Directory />*
*AllowOverride None*
*</Directory>*

What is the purpose of this directive?

- A. It stops users from serving HTML files from their home directories.
- B. It prevents HTML files from being served out of the / directory.
- **C. It stops users from setting up .htaccess files unless specifically allowed in additional configuration.**
- D. It prevents CGI scripts from modifying apache features dynamically.

http://httpd.apache.org/docs/current/misc/security_tips.html

**QUESTION: 36**
CORRECT TEXT
What command is used to create and maintain a Basic Authentication password file for apache? (Specify only the command, with no path or arguments)

**htpasswd**

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

**QUESTION: 37**
SELinux is a Linux feature that:

- A. monitors system file access by unprivileged users and warns them when they are trying to gain access to files beyond their permission levels set in the Mandatory Access Control policies.
- B. provides only Mandatory Access Control policies. Additional access control models such as Rolebased access control require additional tools to implement.
- **C. enforces Mandatory Access Control policies that can restrict user space programs and system servers to the minimum amount of privilege required to operate correctly.**
- D. ensures that system files referenced in the Mandatory Access Control policies are not modified and alerts administrators when changes occur.

**QUESTION: 38**
Which of the following statements are advantages that Mandatory Access Control has over Discretionary Access Control models? (Select TWO correct answers)

- A. MAC policies are easier to configure than use of DAC.
- B. MAC adds the concept of privileged remote users which is not available with simple DAC.
- C. MAC policies increase the ability of the root user to correct errors.
- D. **MAC lets the kernel help decide if an object, such as a device or process, can access another object.**
- E. **Trust is placed in the administrators and not in individual users.**

http://www.prep4cert.com/downloadable/download/sample/sample_id/2842/
(question 6)

**QUESTION: 39**
What are the steps which must be followed to enable server wide zone transfers between two BIND 9 servers securely using TSIG?

- A. Generate a key, specify the public key in the named configuration on both servers, create a server statement in the named configuration on both servers.
- **B. Generate a key, specify the private key in the named configuration on both servers, create a server statement in the named configuration on both servers.**

- C. Generate a key, specify the private key in the named configuration on one server and the public key in the named configuration on the other, create a remote statement in the named configuration on both servers.
- D. Generate a key, specify the private key in the named configuration on one server and the public key in the named configuration on the other, create a server statement in the named configuration on both servers.

La B es insuficiente, pero las demás son directamente incorrectas. A parte de todo eso, debemos autorizar la transferencia ( allow-transfer { key LOQUESEA; }; )
http://www.cyberciti.biz/faq/unix-linux-bind-named-configuring-tsig/

**QUESTION: 40**
Under which path is the selinux pseudofilesystem found?

- A. /dev/selinux
- B. /sys/selinux
- **C. /selinux**
- D. /var/selinux
- E. /proc/selinux

https://www.centos.org/docs/5/html/5.2/Deployment_Guide/s2-SELinux-files-selinux.html

**QUESTION: 41**
CORRECT TEXT
With SELinux, what is the command that is used for changing the context of a file? (Specify the command only, with no path information or arguments)
**chcon (**Temporary Changes)
https://access.redhat.com/site/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Security-Enhanced_Linux/sect-Security-Enhanced_Linux-Working_with_SELinux-SELinux_Contexts_Labeling_Files.html

**chsid** (old selinux)
Change security id
http://www.lurking-grue.org/gettingstarted_newselinuxHOWTO.html

Según libro de SELinux:
Para cambiar contexto nuestro dominio debe tener permiso, y cambiar con: **chcon, restorecon(junto con semanage) ,setfiles, rlpkg(Gentoo) y fixfiles(Fedora)**

**QUESTION: 42**
An unprivileged user issued a command which produced the following log message:

*avc: denied { **getattr** } for pid=984 exec=/usr/bin/vim path=/etc/shadow dev=03:01 inode=134343 scontext=hugh:user_r:user_t tcontext=system_u:object_r:shadow_t tclass=file*

What does the message mean?

- A. **User hugh was not running in a security context that permitted reading the file.**
- B. User hugh only needs to switch to the object_r role in order to edit /etc/shadow.
- C. The security context for hugh is misconfigured and needs access to read any system
- file.
- D. User hugh was not running in a security context that permitted writing to the file.

??????????????????????????????????????????????????????????????"
What permission was denied.
{ getattr } Shows the syscall (permission) that was denied.

Debería ser {read} ??????????????????????'

**QUESTION: 43**
When a user logs into a system using SSH, what is the format of SELinux security context which will assign the user_r role and the user_t domain to their login sessions?

- A. user_r:user_t system_r:sshd_t
- B. sshd_t:system_r user_t:user_r
- C. **system_r:sshd_t user_r:user_t**
- D. user_t:user_r sshd_t:system_r

**QUESTION: 44**
How are SELinux permissions related to standard Linux permissions?

- A. SELinux permissions override standard Linux permissions.
- B. Standard Linux permissions overrideSELinux permissions.
- C. SELinux permissions are verified before standard Linux permissions.
- D. **SELinux permissions are verified after standard Linux permissions.**

**QUESTION: 45**
CORRECT TEXT
A user that is allowed to use the su command under SELinux is also allowed to switch from the user role to the sysadmin role. What command will run a new shell for the user in the new context?
http://wiki.gentoo.org/wiki/SELinux/Tutorials/The_purpose_of_SELinux_roles
(Specify the command only, with no path, options or arguments)
**newrole**

cambiar con newrolel
**# newrole -r sysadm_r**

Con sudo (habitualmente preferido a newrole, *maneja **role and type)***:
**# sudo -r dbadm_r -t dbadm_t vim /etc/postgresql/pg_hba.conf**
configurando /etc/sudoers
**myuser ALL=(ALL) TYPE=dbadm_t ROLE=dbadm_r ALL**

cambio de roles ,types y sensitivities: RUNCON
ejecutar Firefox con la categoria de Salaries
**# runcon -l Salaries firefox**
con la opcion **-r** change current role to the specified role

**QUESTION: 46**
What is the difference between an SELinux domain and an SELinux type?

- A. A domain is a group ofSELinux types.
- B. A domain defines the range of access that an object has. A type is used to define an access level.
- C. **A domain is assigned to processes while a type is assigned to objects such as files and directories.**
- D. A domain is an alternative keyword for type.

loquesea_t : puede ser dominio o type
dominio----------> proceso
type --------------> object (file , directorio)

**QUESTION: 47**
A SELinux security context is required to ensure that all files in /opt have the default context of system_u:object_r:usr_t. How should the corresponding configuration entry be formatted?

- A. system_u:object_r:usr_t /opt/*
- B. **/opt/.* system_u:object_r:usr_t**
- C. /opt/* system_u:object_r:usr_t
- D. system_u:object_r:usr_t: /opt/.*
- E. system_u:object_r:usr_t /opt/.*

ejemplos
https://wiki.gentoo.org/wiki/SELinux/Tutorials/Controlling_file_contexts_yourself

**QUESTION: 48**
CORRECT TEXT
Specifying the **__AllowUsers__**_____ parameter in sshd_config will allow the administrator to systematically provide access to certain user accounts by name.

http://www.openssh.com/cgi-bin/man.cgi?query=sshd_config

**QUESTION: 49**
An administrator can prevent dictionary based attacks against an OpenSSH server by forcing keybased authentication with which TWO parameters in sshd_config?

- A. **PasswordAuthentication**
- B. HostKey
- C. PrivatekeyAuthentication
- D. **PubkeyAuthentication**
- E. ServerKey

http://www.openssh.com/cgi-bin/man.cgi?query=sshd_config

**QUESTION: 50**
A user is attempting to connect to a remote server via SSH and receives the following message: The authenticity of host 'mail.example.com (208.77.188.166)' can't be established. RSA key fingerprint is 92:32:55:e9:c4:20:ae:1b:2c:d7:91:40:90:89:1c:ad. Are you sure you want to continue connecting (yes/no)?

What does this indicate?

- A. The RSA key fingerprint was found in the SpamCop database, indicating that the remote host is a known spammer.
- B. The user'sSSH client was unable to connect to the remote host's authentication agent for verification.
- C. The user'sSSH client is incompatible with the server's RSA key.
- D. **The server's SSH host key cannot be found in the list of known hosts.**

http://docstore.mik.ua/orelly/networking_2ndEd/ssh/ch02_03.htm

**QUESTION: 51**
A user is attempting to connect to a remote host via SSH and following message is displayed: Host key verification failed. Which of the following options could resolve the problem? (Select TWO correct answers)

- A. **Add the StrictHostKeyChecking= no option to the command.**
- B. Enable thePasswordAuthentication parameter on the remote host.
- C. Generate new SSH host keys on the remote host.
- D. Generate a new private key which is compatible with the server's host key.
- E. **Update the remote host's SSH host key in the list of know hosts.**

http://pic.dhe.ibm.com/infocenter/wsdatap/v3r8m1/index.jsp?topic=%2Fxb60%2Fstrict-host-key-checking_sshclientprofile.htm

**QUESTION: 52**
CORRECT TEXT
Where is the global list of known SSH host keys located? (Supply the full path and filename)
**/etc/ssh/ssh_known_hosts**

**QUESTION: 53**
Which of the following are valid NFSv4 security types?

- A. RSA
- B. SSL
- **C. SPKM**
- **D. Kerberos**
- **E. LIPKEY**

Sección "Security": LIPKEY, SPKM-3 and Kerberos (tomo lsk no lsd)
http://www.iaps.com/NFSv4-new-features.html

**QUESTION: 54**
Which GPG command is used to sign a public key? (Select TWO correct answers)

- A. gpg --sign-public-key UID
- **B. gpg --sign-key UID**
- C. gpg --sign UID
- **D. gpg --edit-key UID** followed with the **sign** command.
- E. gpg --edit-key UID followed with the confirm command.

https://www.gnupg.org/gph/es/manual/r1040.html

**QUESTION: 55**
Which GPG command will publish a public key to a public key server?

- A. gpg exportkeys UID
- B. gpg publishkeys UID
- C. **gpg --send-keys UID**
- D. gpg pushkeys UID

https://www.gnupg.org/gph/es/manual/x481.html
https://www.gnupg.org/gph/es/manual/r767.html

**QUESTION: 56**
Which GPG command is used to create a revocation certificate in case a GPG key ever needs to be cancelled?

- **A. gpg --gen-revoke name**
- B. gpg --editkey name followed with the revoke command
- C. gpg --revoke name
- D. gpg --create-revoke name

https://www.gnupg.org/gph/es/manual/r755.html
https://www.gnupg.org/gph/es/manual/c252.html#AEN321

**QUESTION: 57**
Which command is used to add an additional name, email address and comment to an existing private key?

- **A. gpg --edit-key name followed with the adduid command.**
- B. gpg --add-subkey name
- C. gpg --add-alias name
- D. gpg --gen-alias name

**adduid** (añadir identificador usuario)
https://www.gnupg.org/gph/es/manual/c252.html#AEN298

**QUESTION: 58**
Someone who wishes to receive an encrypted file has provided a key UID and a key fingerprint for verification to the data sender. Assuming that this key is on a public keyserver, what command will fetch the public key from the server?

- A. gpg --find-keys UID
- **B. gpg --recv-keys UID**
- C. gpg --get-keys UID
- D. gpg --refresh-keys UID

**gpg [ --keyserver pgp.mit.edu ] --recv-keys ID1 ID2 ID3**

https://www.gnupg.org/gph/es/manual/x481.html
https://www.gnupg.org/gph/es/manual/r781.html

**QUESTION: 59**
You have downloaded a file named file.tgz along with a signature file named file.tgz.asc. Which commands can be used to verify that file.tgz has not been tampered with since the file creator created the signature?

Assume that you have already retrieved the public key of the file creator. (Select THREE correct answers)

- **A. gpg --verify file.tgz.asc file.tgz**
- B. gpg --verify file.tgz
- **C. gpg --verify file.tgz.asc**
- D. gpgv --verify file.tgz.asc
- **E. gpgv file.tgz.asc**

Fichero de distribución mysql-standard-5.0.9-beta-linux-i686.tar.gz

Fichero de firma **mysql-standard-5.0.9-beta-linux-i686.tar.gz.asc**
Se debe verificar que ambos ficheros se encuentran en el mismo directorio y entonces ejecutar el siguiente comando para verificar la firma del fichero de distribución:
**gpg --verify mysql-standard-5.0.9-beta-linux-i686.tar.gz.asc**

**pgpv** https://www.gnupg.org/documentation/manuals/gnupg/gpgv.html
gpgv2 pgpfile
gpgv2 sigfile [datafile]

**QUESTION: 60**
By default, when verifying a signed file or a file with a detached signature, which keyring is used to search for public keys?

- A. ~/.gnupg/trustdb.gpg
- B. ~/.gnupg/secring.gpg
- C. **~/.gnupg/trustedkeys.gpg**
- D. ~/.gnupg/pubring.gpg

man gpgv

**QUESTION: 61**
CORRECT TEXT
Which utility is used for retrieving, setting, and removing NFSv4 ACLs? (Supply only the command name, with no options or parameters)
**nfs4acl**
http://users.suse.com/~agruen/nfs4acl/

**QUESTION: 62**
An administrator has just configured vsftp and notices that she cannot follow symbolic links when connected to the FTP server. What is the most likely reason for this?

- A. Thefollow_symlinks=no option has been set in vsftpd.conf.
- B. **vsftpd is running in a chroot environment.**
- C. This installation ofvsftpd was not compiled with support for symbolic links.
- D. The user account she is connecting with is not listed in /etc/security/ftpusers.

**QUESTION: 63**
CORRECT TEXT
Which parameter in vsftp.conf will restrict users to their home directory? (Supply only the parameter name, with no options or values)

**chroot_local_user**

**QUESTION: 64**
What is one of the primary claimed benefits of Smack over SELinux?

- A. Smack implements Rule Set Based Access Control.SELinux doesn't support this model.
- B. SELinux has export restrictions placed on it by the NSA.
- **C. Configuration of Smack is much more simple.**
- D. Smack allows users to share files without administrator intervention.

http://en.wikipedia.org/wiki/Smack_%28Linux_security_module%29
Smack is a kernel based implementation of mandatory access control that **includes simplicity in its primary design goals**.
Smack's author replied that it would not be practical due to SELinux's complicated configuration syntax

and the philosophical difference between Smack and SELinux designs

**QUESTION: 65**
How does AppArmor configure its access control settings?

- A. AppArmor does not require any configuration.
- B. AppArmor inspects the Linux system to determine which applications are installed and configures itself. This configuration can then be modified manually.
- C. AppArmor relies on precompiled policies. These policies are updated with new releases or can be downloaded periodically.
- **D. A profile is assigned per application that specifies the system resources available to the application.**

http://en.wikipedia.org/wiki/AppArmor
AppArmor allows the system administrator to associate with each program a security profile that restricts the capabilities of that program.

**QUESTION: 66**
Which of the following is NOT and valid scan technique with nmap?

- A. Window
- B. SYN
- C. ACK
- D. Connect()
- E. **RST**

http://nmap.org/book/man-port-scanning-techniques.html

| | |
|---|---|
| TCP SYN scan | -sS (TCP SYN scan) |
| TCP connect scan | -sT (TCP connect scan) |
| UDP scans | -sU (UDP scans) |
| SCTP INIT scan | -sY (SCTP INIT scan) |
| TCP NULL, FIN, and Xmas scans | -sN; -sF; -sX (TCP NULL, FIN, and Xmas scan) |
| TCP ACK scan | -sA (TCP ACK scan) |
| TCP Window scan | -sW (TCP Window scan) |
| TCP Maimon scan | -sM (TCP Maimon scan) |
| Custom TCP scan | --scanflags (Custom TCP scan) |
| SCTP COOKIE ECHO scan | -sZ (SCTP COOKIE ECHO scan) |
| IP protocol scan | -sO (IP protocol scan) |
| FTP bounce scan | -b <*FTP relay host*> (FTP bounce scan) |
| IDLE scan | -sI <*zombie host*>[:<*probeport*>] (idle scan) |

**QUESTION: 67**
CORRECT TEXT
Postfix daemons can be chroot'd by setting the chroot flag in **__maste.cf_____**. (Supply only the filename, without a path)

http://www.postfix.org/master.5.html
http://www.postfix.org/BASIC_CONFIGURATION_README.html

**QUESTION: 68**
What can proxymap be used for in a Postfix installation? (Select TWO correct answers)

- A. **Consolidating the number of open lookup tables.**

- B. Creating and querying Postfix alias databases.
- C. Mapping mail user IDs to system accounts.
- D. **Overcoming chroot restrictions.**
- E. Creating and querying Postfix lookup tables.

http://www.postfix.org/proxymap.8.html
The purpose of these services is:

- To overcome chroot restrictions.
- To consolidate the number of open lookup tables by sharing one open table among multiple processes.
- To provide single-updater functionality for lookup tables that do not reliably support multiple writers

**QUESTION: 69**
Which of the following parameters should be set in main.cf to enable TLS in Postfix?

- A. **smtpd_tls_cert_file, smtpd_tls_key_file, smtpd_tls_CAfile, smtpd_use_tls**
- B. smtpd_tls_key_file, smtpd_tls_CAfile, smtpd_use_tls, ~~smtpd_tls_pem_file~~
- C. smtpd_tls_CAfile, smtpd_use_tls, smtpd_tls_pem_file, smtpd_tls_cert_file
- D. smtpd_use_tls, ~~smtpd_tls_pem_file~~, smtpd_tls_cert_file, smtpd_tls_key_file

**QUESTION: 70**
The system administrator wishes to use John the Ripper to confirm that the passwords in a file called passwords are not weak. john has finished but the terminal window running the program has closed. What command can be used to list any cracked passwords for this file?

- A. john -list passwords
- B. john -list
- C. john -show
- D. **john -show passwords**

**QUESTION: 71**
On a new Linux system, the root user is being asked to provide the root user password before being able to use the su command. What line in the /etc/pam.d/su file will allow root to use su without supplying passwords?

- A. auth required pam_norootpw.so
- B. auth sufficient pam_norootpw.so
- C. auth required pam_rootok.so
- D. **auth sufficient pam_rootok.so**

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

cd /etc/pam.d
grep -lir "pam_rootok.so *

**QUESTION: 72**
The system administrator wishes to use the **pam_listfile.so** module to **restrict which users are allowed to login via SSH.** Which line will configure this behaviour?

- A. auth required pam_listfile.so item=user sense=deny

file=/etc/sshd/sshd.deny onerr=succeed

- B. auth required pam_listfile.so item=user sense=allow

  file=/etc/sshd/sshd.allow onerr=succeed

- C. **auth required pam_listfile.so item=user sense=allow**

  **file=/etc/sshd/sshd.allow onerr=fail**

- D. auth required pam_listfile.so item=user sense=deny

  file=/etc/sshd/sshd.deny onerr=fail

http://linux.die.net/man/8/pam_listfile
cd /etc/pam.d
grep -lir "pam_listfile.so *

Ejemplos:
Classic 'ftpusers' authentication can be implemented with this entry in /etc/pam.d/ftpd:
#
# **deny ftp-access** to users listed in the /etc/ftpusers file
#
auth required pam_listfile.so \
onerr=succeed item=user sense=deny file=/etc/ftpusers
Note, users listed in /etc/ftpusers file are (counterintuitively) *not* allowed access to the ftp service.

To allow login access only for certain users, you can use a /etc/pam.d/login entry like this:
#
# **permit login** to users listed in /etc/loginusers
#
auth required pam_listfile.so \
onerr=fail item=user sense=allow file=/etc/loginusers

**onerr=[succeed|fail]**What to do if something weird happens like being unable to open the file.
En el caso **deny ftp-access** si ocurre algo extraño en el acceso al archivo ftpusers entonces deniega también el acceso, onerr=succeed
En el caso de **permit login,** si ocurre algo extraño en el acceso al fichero entonces deniega el logueo, onerr=fail

**QUESTION: 73**
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

**Estructura de una regla:**
Cabecera Regla + Opciones Regla
**Estructura Cabecera Regla:**
Acción + Protocolo + Red Origen + Puerto Origen +Dirección +Red Destino + Puerto Destino
**alert tcp $EXTERNAL_NET any -> $HOME_NET 53**

**QUESTION: 74**
What is the purpose of snort inline?

- A. To run the snort daemon without forking child processes.
- B. **To have iptables use snort rules to filter packets.**
- C. To have snort log suspicious activity only, without performing any actions
- D. To run the snort daemon as anonroot user.

The Snort_inline IPS is a modified version of the famous Snort IDS
**IDS (Intrusion Detection System)** logs an alert when a packet matches a signature rule but does not discard or even modify it.This is different with an **IPS (Intrusion Prevention System)** where a packet matching a signature rule is blocked or modified.
http://openmaniak.com/inline_final.php

**QUESTION: 75**
What is the purpose of tripwire?

- A. To act as ahoneypot and attract attackers.
- B. To enforce mandatory access control policies to confine users to the minimum
- amount of privilege required.
- C. To monitor a server forbreakin attempts and, if desired, ban the IP address.
- D. **To identify changes to critical system files and directories.**

**QUESTION: 76**
Which of the following commands will create a new, signed tw.pol file?

- A. twadmin --create-polfile -e -S mykey.key /etc/tripwire/twpol.txt
- B. twadmin --create-cfgfile -S mykey.key /etc/tripwire/twpol.txt
- C. twadmin --**create-polfile** -**S** mykey.key /etc/tripwire/twpol.txt
- D. twadmin --create-cfgfile -e -S mykey.key /etc/tripwire/twpol.txt

**-e**, --**no-encryption**
Do not sign the configuration file being stored. The configuration file will still be compressed, and will not be human-readable. **Mutually exclusive** with (**-Q**) and (**-S**). *configfile.txt*

man twadmin(8)

Synopsis
**twadmin** { **-m P** | **--create-polfile** } [ *options...* ]

options
-**S** *sitekey*, --**site-keyfile**
*sitekey*Use the specified site key file to encode and sign the new configuration file. Exactly one of (**-S**) or (**-e**) must be specified.

crear un archivo de políticas, a partir de **/etc/tripwire/twpol.tx**
En realidad Tripwire usa una versión compilada y encriptada del archivo de politicas, que se almacena en **/etc/tripwire/tw.pol.** Para generarlo (y regenerarlo cuantas veces se necesite), usar:
***twadmin -m P /etc/tripwire/twpol.txt***

**QUESTION: 77**

What openssl command will generate a private RSA key of 2048 bits and no passphrase?

- A. openssl genrsa -des3 -out privkey.pem 2048
- B. **openssl genrsa -out privkey.pem 2048**
- C. openssl genrsa nopass -out privkey.pem 2048
- D. openssl genrsa nopass -des3 out privkey.pem 2048

If you *don't want your key to be protected* by a password, *remove the flag '-des3'*

**QUESTION: 78**
What openssl command will generate a certificate signing request (CSR) using the private key file privkey.pem?

- A. openssl req -key privkey.pem -out cert.csr
- B. **openssl req -new -key privkey.pem -out cert.csr**
- C. openssl gencsr -key privkey.pem -out cert.csr
- D. openssl gencsr -new -key privkey.pem -out cert.csr

**QUESTION: 79**
What openssl command will generate a **selfsigned** test certificate?

- A. **openssl req -new -x509 -key privkey.pem -out cacert.pem days 365**
- B. openssl sign key privkey.pem out cacert.pem days 365
- C. openssl req key privkey.pem out cacert.pem days 365
- D. openssl sign new x509 key privkey.pem out cacert.pem days 365

If you don't want to deal with another certificate authority, or just want to create a test certificate **for yourself. -x509**

**QUESTION: 80**
Which openssl command is used to inspect the information stored in a certificate?

- A. **x509**
- B. show
- C. info
- D. req

How do I extract information from a certificate?
http://www.madboa.com/geek/openssl/#cert-exam

**QUESTION: 81**
The openssl command can be used to test connections with various secure services.
What command will open a connection with a remote POP3S (POP3 over SSL) server?

- A. openssl --connect host pop.example.com:pop3s
- B. openssl --connect pop.example.com:pop3s
- **C. openssl s_client --connect pop.example.com:pop3s**
- D. openssl s_client pop.example.com:pop3s

http://blog.yimingliu.com/2009/01/23/testing-a-pop3-server-via-telnet-or-openssl/

**QUESTION: 82**
Which of the following rule directives will email kevin@example.com and matt@example.com when the Mail Configuration rule is violated?**(¡¡TRIPWIRE DE LOS**

**COJONES!!)**

- A. (rulename= "Mail Configuration", severity= $(SIG_HI), emailto= kevin@example.com, emailto= matt@example.com)
- B. (rulename= "Mail Configuration", severity= $(SIG_HI), emailto= kevin@example.com,matt@example.com)
- **C. (rulename= "Mail Configuration", severity= $(SIG_HI), emailto= kevin@example.com;matt@example.com)**
- D. (rulename= "Mail Configuration", severity= $(SIG_HI), emailto= kevin@example.com, emailcc= matt@example.com)

http://www-uxsup.csx.cam.ac.uk/pub/doc/redhat/redhat7./rhl-rg-en-7.3/s1-tripwire-email.html

**QUESTION: 83**
Which of the following methods can be used to deactivate a rule in Snort? (Select TWO correct answers)

- A. **Place a # in front of the rule and restart snort.**
- B. **Write a pass rule inlocal.rules and restart snort with the -o option**.
- C. Delete the rule and snort will automatically reread its rules files within five minutes.
- D. Add the rule to /etc/snort/rules.deactivated and it will take effect immediately.

**Estructura Cabecera Regla:**
Acción + Protocolo + Red Origen + Puerto Origen +Dirección +Red Destino + Puerto Destino

**Acción:**
alert(genera alerta y loguea paquete)
log (archiva el log del paquete)
**pass (ignora paquete)**
activate (activa alerta y llama a una regla dinámica)
dynamic ( cuando es llamada por regla activate se pone a funcionar)

http://nsmwiki.org/Snort
**-o** Change the rule testing order to Pass|Alert|Log

**QUESTION: 84**
The system administrator is keeping local configuration file changes in RCS. What command will commit the file to RCS revision control AND keep a local, unlocked copy of the latest version of the file?

- A. ci file
- B. rcs commit file
- C. rcs -o file
- **D. ci -u file**

**QUESTION: 85**
CORRECT TEXT
There is a configuration file being managed by RCS. Based on timestamps, it appears that someone has modified the file without checking it into RCS. What command can be used to compare the configuration file with the latest committed version? (Specify the command only, no path or argument information)

rcsdiff

**QUESTION: 86**
What is an SO rule in the context of Snort?

- A. **A loadable snort module.**
- B. A rule which can be written in the Perl programming language.
- C. A simple object.
- D. A snort overflow

Commonly referred to as "Shared Object rules", "SO rules", "pre-compiled rules", or "Shared Objects" are detection that is written in the Shared Object rule language, which is, essentially, "C". This allows for primarily two things for the Snort platform:
http://www.snort.org/snort-rules/shared-object-rules
http://blog.snort.org/2011/02/snort-shared-object-rules.html

**QUESTION: 87**
Which of the following are valid ntop deployment scenarios? (Select THREE correct answers)

- A. Public Site
- B. Switched Gateway
- C. **Simple Host**
- D. **Border Gateway**
- E. **Mirror Line**

http://www.ntop.org/support/documentation/ntop-misusage-notes/

**QUESTION: 88**
In the Puppet centralized configuration management tool, a manifest is:

- A. a list of all target configurations.
- B. **a configuration document that describes the target configuration and the steps required to achieve it.**
- C. a list of all files related to a configuration target.
- D. a list of the important services on a target configuration.

http://docs.puppetlabs.com/learning/manifests.html
Puppet apply reads the manifest passed to it, compiles it into a catalog, and applies the catalog.

**QUESTION: 89**
What is the syntax error in the following simple Puppet configuration file?

```
class test_class {
        file{ "/tmp/test.txt":
        mode=> 600,
        owner=> root,
        group=> root
        }
}
# Define the node
 node testclient {
    isa test_class
}
```

- A. Comments begin with // character and not a #.
- B. The colon (:) after /tmp/test.txt should be a semicolon (;).
- C. class, node and file sections require a semicolon (;) at the end of their definitions.
- D. **isa** should be **include.**

http://docs.puppetlabs.com/learning/modules1.html

**QUESTION: 90**
Which of the following are valid Nagios objects? (Select THREE correct answers)

- **A. Contacts**
- **B. Commands**
- **C. Host Groups**
- D. Notification Groups
- E. Programs

http://nagios.sourceforge.net/docs/3_0/objectdefinitions.html
Host definitions
**Host group** definitions
Host dependency definitions
Host escalation definitions
Extended host information definitions
Service definitions
Service group definitions
Service dependency definitions
Service escalation definitions
Extended service information definitions
**Contact** definitions
Contact group definitions
Time period definitions
**Command** definitions

**QUESTION: 91**
Which of the following are common techniques for securing Nagios? (Select THREE correct answers)

- **A. Require authentication for access to the CGI scripts.**
- B. RunNagios in a chroot jail.
- C. CompileNagios with the enabletls option.
- **D. Do not run as the root user.**
- **E. Disable external commands.**

http://nagios.sourceforge.net/docs/3_0/security.html
Use a Dedicated Monitoring Box.
**Don't Run Nagios As Root**
Lock Down The Check Result Directory.
**Lock Down The External Command File**
**Require Authentication In The CGIs.**
Implement Enhanced CGI Security Measures.
Use Full Paths In Command Definitions
Hide Sensitive Information With $USERn$ Macros
Strip Dangerous Characters From Macros.
Secure Access to Remote Agents.
Secure Communication Channels

**QUESTION: 92**
Which of the following is not an iptables rule set?

- A. **chain**
- B. mangle

- C. filter
- D. nat

# Croquis de iptables o bien el script para descargar iptables que peina todas las tablas. "rule set" = tabla
man iptables

**QUESTION: 93**
Which of the following are builtin chains for the iptables **nat** table? (Select THREE correct answers)

- A. **OUTPUT**
- B. INPUT
- C. PROCESSING
- D. **POSTROUTING**
- E. **PREROUTING**

http://www.karlrupp.net/en/computer/nat_tutorial

**QUESTION: 94**
Which syslog configuration line will send out logged messages to a remote syslog server?

- A. *.* host:remotehost
- B. *.* remoteremotehost
- **C. *.* @remotehost**
- D. *.* host=remotehost

~~man rsyslogd~~
man syslogd

log remoto, enviados por el **puerto UDP 514**
*.emerg @mothership.mydomain.org

**QUESTION: 95**
Which option is required to syslogd in order for it to accept remote log messages?

- A. -s
- **B. -r**
- C. --remote
- D. -l

~~man rsyslogd~~ <--- no funciona igual q rsyslogd, juraría q falta la correcta :S
man syslogd
http://unixhelp.ed.ac.uk/CGI/man-cgi?syslogd+8

**Inicio servicio**
**# /etc/init.d/syslog**
-m minutes_btwn_marks
-a /additional/socket (ademas de /dev/log especificar socket adicional de escucha)
-f /path/to/syslog.conf
-r (escucha mensajes host remotos)

**QUESTION: 96**
What does the following iptables rule accomplish:

*iptables -A INPUT -s 208.77.188.166 -j DROP*

- A. Forwards all incoming traffic to the host 208.77.188.166.
- B. Accepts all traffic from 208.77.188.166.
- C. Nothing, there is a syntax error.
- **D. Drops all traffic from 208.77.188.166.**

#
man iptables

**QUESTION: 97**
What does the following iptables rule accomplish:

*iptables -A INPUT -s 208.77.188.166 -d 10.142.232.1 -p tcp --dport 22 -j ACCEPT*

A. Accepts traffic on port 22 only from the hosts 208.77.188.166 and 10.142.232.1.
B. Forwards all requests from the host 10.142.232.1 on port 22 the internal host 208.77.188.166
C. Forwards all requests from the host 208.77.188.166 on port 22 the internal host 10.142.232.1
D. Drops traffic on port 22 only from the hosts 208.77.188.166 and 10.142.232.1.

**DICE LA C, pero ninguna de esas es correcta. Simplemete acepta el trafico de *208.77.188.166 a 10.142.232.1 al puerto 22/TCP. Se parece a la A, pero no está correctamente explicada***

# Apuntes de iptables
man iptables

**QUESTION: 98**
What does the following iptables rule accomplish:

*iptables -A INPUT -d 10.142.232.1 -p tcp --dport 20:21 -j ACCEPT*

- A. Forwards all traffic not on port 20 or 21 to the host 10.142.232.1.
- B. Drops all traffic coming from the host 10.142.232.1 destined for port 20 or 21.
- *C. Accepts all traffic from the host 10.142.232.1 destined for port 20 or 21.??????????????*
- **D. Forwards all traffic on port 20 and 21 to the host 10.142.232.1.**

**SEGÚN LIBRO ES LA D**

# Apuntes de iptables
man iptables

**QUESTION: 99**
What does the following iptables rule accomplish:

*iptables -A INPUT -s !127.0.0.0/8 -p tcp --dport 111 -j DROP*

- A. Drops all packets from the LAN destined for port 111.
- B. Drops all packets originating from the local machine unless they are destined for port 111.
- C. Drops all packets destined for port 111 which originate from the local machine.
- **D. Drops all packets destined for port 111 unless they are from the local machine.**

# Apuntes de iptables
man iptables

**QUESTION: 100**
The local system administrator has created a configuration entry for apache version 2 that isn't working. What is wrong with the following configuration?

```
<Location /members>
      AuthName Members
      AuthType Basic
      AuthUserFile /www/passwd
</Location>
```

- **A. The directive "Require valid-user" is missing.**
- B. Basic Authentication has been removed from Apache 2.x.
- C. The format of the password file is not specified.
- D. The AuthUserFile must be in the apache configuration directory.

# Los apuntes de Apache :)
http://httpd.apache.org/docs/2.2/mod/core.html#authname

**QUESTION: 101**
In apache configuration which directives are used to restrict access based on host/domain name and IP address?

- A. restrict and allow
- **B. order, allow from and deny from**
- C. deny and accept
- D. allow IP, deny IP, allow DOMAIN and deny DOMAIN

http://httpd.apache.org/docs/2.2/howto/access.html