LPI_RealExamQuestions.Com_117-303_v2011-11-08_114q_By-akrenu

Number: 117-303
Passing Score: 700
Time Limit: 120 min
File Version: 2011-11-08

http://www.gratisexam.com/

LPI 117-303

Version 2011-11-08

Question : 114

Important and good questions uploaded in this dump for the exam.

Goodluck and Enjoy!

By-akrenu

Exam A

QUESTION 1
In apache configuration which directives are used to restrict access based on host/domain name and IP adress?

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
E. order, deny and accept

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
Someone who whises to receive and 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 findkeys UID
B. gpg recvkeys UID
C. gpg getkeys UID
D. gpg refreshkeys UID

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
Linux Extended Attributes include attributes classes. Which of the following are included in the defined attributes classes ?
(Select 3 correct answers)

A. default

B. system
C. owner
D. trusted
E. user

Correct Answer: BDE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
Which of the following is NOT and valid scan technique with nmap ?

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

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
Which of the following are common techniques for securing a sendmail server ?
(Select 3 correct answers)

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

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
Which tool, distributed with BIND 9, will check the syntax of a named configuration file? **(Supply only the program name, without any option or parameters)**

Correct Answer: named-checkconf or /usr/sbin/named-checkconf
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
What is the purpose of tripwire?

A. To act as a honeypot 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 for breakin attempts and, if desired, ban the IP address
D. To identify changes to critical system file and directories

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
You wish to revoke write access for all groups and named users on a file. Which command will make a correct ACL changes?

A. setfacl x group:*:rx,user:*:rx afile
B. setfacl x mask::rx afile
C. setfacl m mask::rx afile
D. setfacl m group:*:rx,user:*:rx afile

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
Which of the following are common techniques for securing Nagios ?
(Select 3 correct answers)

A. Require authentication for access to the CGI scripts
B. Run Nagios in a chroot jail
C. Compile Nagios with the enabletls option

D. Do not run as the root user
E. Disable external commands

Correct Answer: ADE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
Which GPG command us used to create a revocation certificate in case a GPG key ever needs to be called?

A. gpg genrevoke name
B. gpg editkey name followed with the revoke command
C. gpg revoke name
D. gpg createrevoke name

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
An administrator can prevent dictionary based attacks against an OpenSSH server by forcing keybased authentication **with which 2 parameters** in sshd_config ?

A. PasswordAuthentication
B. HostKey
C. PrivatekeyAuthentication
D. Serverkey

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
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 2 correct answers)

A. Every packet being checked has a 2 byte offset
B. Traffic on ports 15001550 is being captured
C. Traffic on ports 15011549 is being captured
D. Only two bytes are being checked in each packet
E. Up to four byted are being check in each packet

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
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)

Correct Answer: chcon chsid setfattr
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
Which of the following statements are advantages that Mandatory Access Control has over Discretionary Access Control models?
(Select 2 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 avaiable 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

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
Which of the following are valid OpenVPN authentications modes?
(Choose 2 correct answers)

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

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
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

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:

QUESTION 18
Which of the following is not an iptables rule set?

A. chain
B. mangle
C. filter
D. nat

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
Which of the following is NOT included in a Snort rule headers?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
In the Puppet centralized configuration management tool, a manifest is:

A. a list of all target configuration
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
Which syslog configuration line will send out logged messages to a remote syslog server?

A. *.* host:remotehost
B. *.* remote remotehost
C. *.* @remotehost
D. *.* host=remotehost

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
Which of the following are valid NFSv4 security types?

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

Correct Answer: CDE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
Which directive on 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)

Correct Answer: remote
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
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 session?

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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
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?
(Specify the command only, with no path, option or arguments)

Correct Answer: newrole
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
What is the difference between an SELinux domain an an SELinux type ?

A. A domain is a group of SELinux 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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
How are SELinux permissions related to standart Linux permissions?

A. SELinux permissions override standart Linux permissions
B. Standart Linux permissions override SELinux permissions
C. SELinux permissions are verified before standart permissions
D. SELinux permissions are verified after standart Linux permissions

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
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 2 correct answers)

A. Add the o StrictHostKeyChecking=no option to the command
B. Enable the PasswordAuthentication parameter to the remote host
C. Generate new SSH host keys on the remote host
D. Generate 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

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
SELinux is a Linux feature that:

A. monitors system file access by unprivileged users and warns them they are trying to gain access to files beyonf 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 privileges required to operate correctly
D. ensure that system files referenced in the Mandatory Access Control policies are not modified and alerts administrators when changes occur

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
Which of the following rule directives will email kevin@example.com and matt@example.com when the Mail Configuration rule is violated?

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
)

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
Specifying the _____ parameter in sshd_config will allow the administrator to systematically provide access to certain user accounts by name.

Correct Answer: AllowUsers
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
Which command will list all of the extended attributes on the file afile.txt with the values?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
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's SSH client was unable to connect to the remote host's authentication agent for verification
C. The user's SSH 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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
Which command is used to add an additional name, email address and comment to an existing private key?

A. gpg editkey name followed with the adduid command
B. gpg addsubkey
C. gpg addalias name
D. gpg genalias name

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
An administrator has just configured vsftp and notice that she cannot follow symbolic links when connected to the FTP server. What is the most likely reason for this?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
What can proxymap be used for in a Postfix installation?
(Select 2 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

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
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)

Correct Answer: notification_interval
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
Which of the following are builtin chains for the iptables nat table?
(Select 3 correct answers)

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

Correct Answer: ADE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
An administrator has created a mapping with the following command:

cryptsetup luksOpen /dev/sda1 cryptvol

and hat set 3 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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
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 a nonroot user

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
Which LUKS action, when supplied to the cryptsetup command, will initialize a LUKS partition and set the initial key?
(Provide only the action name)

Correct Answer: luksFormat
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44

What command is used to create and maintain a Basic Authentification password file for apache?
(Specify only the command, with no path or arguments)

Correct Answer: htpasswd
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
SELinux has just been installed on a Linux system and the administrator wants to use SELinux in permissive in order to audit the various service 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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
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 avaiable to the application

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
The system administrator wishes tu 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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49

What OpenSSL command will generate a selfsigned test certificate?

A. openssl req 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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
What is the default UDP port for OpenVPN traffic?

Correct Answer: 1194
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
DNS servers are vulnerable to which of the following attacks?
(Select 3 correct answers)

A. **Cache Poisoning**
B. Fork Bomb Attack
C. PasswordBased Attack
D. ManintheMiddle
E. Smurf Attack

Correct Answer: ADE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
What does ntop use for data collection?

A. Network packets
B. Log files
C. Frame relay
D. SNMP

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
Postfix daemons can be chroot'd by setting the chroot flag in _____.
(supply only the filename, without a path)

Correct Answer: master.cf
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
In Nessus, what does the acronym NASL stand for?

Correct Answer: Nessus Attack Scripting Language
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
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 or 21 to the host 10.142.232.1

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
Which of the following methods can be used to deactivate a rule in Snort?
(Select 2 correct answers)

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

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57

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

A. push "dhcpoption DNS 10.142.232.4"
B. push "dhcp DNS 10.142.232.4"
C. push "option DNS 10.142.232.4"
D. push "dhcpoption DNS 10.142.232.4"

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
Which of the following are valid Nagios objects?
(Select 3 correct answers)

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

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
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 the following statements are true ?
(Select 2 correct answers)

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

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
Which OpenSSL command is used to inspect the information stored in a certificate?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
Which of the following commands will create a new, signed tw.pol file?

A. twadmin createpolfile e S mykey.key /etc/tripwire/twpol.txt
B. twadmin createcfgfile S mykey.key /etc/tripwire/twpol.txt
C. twadmin createpolfile S mykey.key /etc/tripwire/twpol.txt
D. twadmin createcfgfile e S mykey.key /etc/tripwire/twpol.txt

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
By default, when verifying a signed file or a file with a detached signature, which keyring is used to search for a public keys?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
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 host 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 host 208.77.188.166 and 10.142.232.1

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
Which utility is used for retrieving, setting, and removing NFSv4 ACLs?
(Supply only the command name, with no options or parameters)

Correct Answer: nfs4acl or /usr/sbin/nfs4acl
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
Which GPG command is used to sign a public key?
(Select 2 correct answers)

A. gpg signpublickey UID
B. gpg signkey UID
C. gpg sign UID
D. gpg editkey UID followed with the sign command
E. gpg editkey UID followed with the confirm command

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
Which command will set the user.author attribute on the file afile.txt

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
There is a configuration file being managed by RCS. Base 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 arguments information)

Correct Answer: rcsdiff
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
An administrator is capturing traffic with Wireshark and is only seeing ARP traffic. What is most likely cause of this?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
An 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 formated?

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/.*

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
Which of the following can be done to secure BIND server?
(Select 3 correct answers)

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

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
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 fro 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 modifiying apache features dynamically

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
Where is the global list of known SSH host keys located ?
(Supply the full path and filename)

Correct Answer: /etc/ssh/sshd_known_hosts
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
What command will list basic information about all targets avaiable to cryptmount?
(Provide the command with any options or parameters)

Correct Answer: cryptmount --list or /usr/bin/cryptmount -l or /usr/bin/cryptmount --list or cryptmount -l
Section: (none)
Explanation

Explanation/Reference:
Every command is accepted !

QUESTION 77
What are the steps which must be followed to enable serverwide 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 name 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 in both servers

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 78
An administrator has successfully configured a cryptographic volume for dmcrypt, and 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)

Correct Answer: /etc/crypttab
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
Which of the following are valid deployment scenarios?
(Select 3 correct answers)

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

Correct Answer: CDE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
What is one of the primary claimed benefits of Smack over SELinux?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 81
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 npass des3 out privkey.pem 2048

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 82
An administrator has just configured an OpenVPN client. Upon starting the service, the following message is displayed:

TLS Error: TLS key negatiation 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 wit 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 TSL key negotiation took longer than 60 seconds, indicating that there may be a problem with network performance

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
Under which path is the SELinux pseudofilesystem found ?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
Which option is required to syslogd in order for it to accept remote log message?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
Which of the following statements are true about Linux Extended Attributes on files?
(Select 2 correct answers)

A. An attribute value may be empty
B. Attribute storage counts towords disk quota use
C. Attribute use is enabled by mounting a partition with the attr option
D. An attribute is file, not inode, specify. This, a hard linked file in two locations could have different attributes
E. Attributes are not used by SELinux and other kernel security modules

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
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_pem_file
C. smtpd_tls_CAfile, smtpd_use_tls, smtpd_tls_pem_file, smtpd_tls_cert_file
D. smtpd_use_tls, emtpd_tls_pem_file, smtpd_tls_cert_file, smtpd_tls_key_file

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87
An unprivileged user issued a command which produced the following log message:

avc: denied { getattr } for pid=984 exe=/usr/bin/vim path=/etc/shadow dev=03:01 ino=134343 scontext=hugh:user_r:user_t tcontext=system_u:object: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 fur 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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88
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 validuser is missing
B. Basic Authentification 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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
When adding additional users to a file's extended ACL's, what is true abount the default behaviour of the ACL mask for the file?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
The system administrator is keeping local configuration file changes in RCS. What command will commit the file 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

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:

QUESTION 91
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 section require a semicolon (;) at the end of their definitions
D. isa should be include

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
What is true about the permissions for the file afile give the following output from getfacl?
(Select 2 correct answers)

% getfacl afile
 # file: afile
 # owner: matt
 # group: support
user:: rwx
user:hugh:rw
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

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
You have downloaded a file named file.tgz along with a signature file named file.tgz.asc. Which command can be used to verify that file.tgz hat not beeing tampered with since the file creator created the signature?
Assume that you have already retrieved the public key of the file creator

(Select 3 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

Correct Answer: ACE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
What command will remove the dmcrypt mapping named cryptvol?
(Provide the command with any options and parameters)

Correct Answer: /sbin/cryptsetup remove crypt-vol or cryptsetup remove crypt-vol
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
In which of the following scenarios MUST an administrator use ethernet bridging instead of routing when configuring an OpenVPN site?
(Select 2 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

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97
Which GPG command will publish a public key to a public key server?

A. gpg exportkeys UID
B. gpg publishkeys UID
C. gpg sendkeys UID
D. gpg pushkeys UID

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98
Which of the following are valid dmcrypt modes?
(Chosse 3 correct answers)

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

Correct Answer: ABE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 99
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:pop3s
C. openssl s_client connect pop.example.com:pop3s
D. openssl s_client pop.example.com:pop3s

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 100
The system administartor wishes to use the pam_listfile.so module to restrict which user 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.deny onerr=succeed
C. auth required pam_listfile.so item=user sense=allow file=/etc/sshd/sshd.deny onerr=fail
D. auth required pam_listfile.so item=user sense=deny file=/etc/sshd/sshd.deny onerr=fail

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101
Which parameter in vsftp.conf will restrict users to their home directory?
(Supply only the parameter name, with no option or values)

Correct Answer: chroot_local_user
Section: (none)
Explanation

Explanation/Reference:

QUESTION 102
What is true about the permissions for the file afile give the following output from getfacl?
(Select 2 correct answers)

% getfacl afile
 # file: afile
 # owner: matt
 # group: support
user:: rwx
user:hugh:rw
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

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 103
What is true about the permissions for the file afile give the following output from getfacl?
(Select 2 correct answers)

% getfacl afile
 # file: afile
 # owner: matt
 # group: support
user:: rwx
user:hugh:rw
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

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104
What is true about the permissions for the file afile give the following output from getfacl?
(Select 2 correct answers)

% getfacl afile
 # file: afile
 # owner: matt
 # group: support
user:: rwx
user:hugh:rw
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

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 105
What is true about the permissions for the file afile give the following output from getfacl?
(Select 2 correct answers)

% getfacl afile
 # file: afile
 # owner: matt
 # group: support
user:: rwx
user:hugh:rw
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

Correct Answer: BE

Section: (none)
Explanation

Explanation/Reference:

QUESTION 106
What is true about the permissions for the file afile give the following output from getfacl?
(Select 2 correct answers)

% getfacl afile
 # file: afile
 # owner: matt
 # group: support
user:: rwx
user:hugh:rw
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

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 107
Which of the following is NOT and valid scan technique with nmap ?

A. Window
B. SYN

C. ACK
D. Connect()
E. RST

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 108
You wish to revoke write access for all groups and named users on a file. Which command will make a correct ACL changes?

A. setfacl x group:*:rx,user:*:rx afile
B. setfacl x mask::rx afile
C. setfacl m mask::rx afile

D. setfacl m group:*:rx,user:*:rx afile

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 109
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)

Correct Answer: chcon chsid setfattr
Section: (none)
Explanation

Explanation/Reference:

QUESTION 110
Postfix daemons can be chroot'd by setting the chroot flag in _____.
(supply only the filename, without a path)

Correct Answer: master.cf
Section: (none)
Explanation

Explanation/Reference:

QUESTION 111
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 112
When adding additional users to a file's extended ACL's, what is true abount the default behaviour of the ACL mask for the file?

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

D. The mask is modified to be the union of all permissions of the owning group and all named users and groups

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 113
What is true about the permissions for the file afile give the following output from getfacl?
(Select 2 correct answers)

```
% getfacl afile
# file: afile
# owner: matt
# group: support
user:: rwx
user:hugh:rw
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

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 114
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:pop3s
C. openssl s_client connect pop.example.com:pop3s
D. openssl s_client pop.example.com:pop3s

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference: