LPI

Exam Questions 303-200

LPIC-3 Exam 303: Security, version 2.0

NEW QUESTION 1
Which command revokes ACL-based write access for groups and named users on the file afile?

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

Answer: C

NEW QUESTION 2
Which of the following authentication methods was added to NFS in version 4?

A. Kerberos authentication
B. SSH hostkey authentication
C. Winbind authentication
D. SSL certificate authentication

Answer: A

NEW QUESTION 3
Which of the following access control models is established by using SELinux?

A. Security Access Control (SAC)
B. Group Access Control (GAC)
C. User Access Control (UAC)
D. Discretionary Access Control (DAC)
E. Mandatory Access Control (MAC)

Answer: E

NEW QUESTION 4
Which command is used to run a new shell for a user changing the SELinux context? (Specify ONLY the command without any path or parameters.)

A. Mastered
B. Not Mastered

Answer: A

Explanation:
 https://www.centos.ofg/docs/5/html/DeployrnenLGuide-en-US/sec-sel-admincontrol.html

NEW QUESTION 5
What happens when the command getfattr afile is run while the file afile has no extended attributes set?

A. getfattr prints a warning and exits with a values of 0.
B. getfattr prints a warning and exits with a value of 1.
C. No output is produced and getfattr exits with a value of 0.
D. No outputs is produced and getfattr exits with a value of 1

Answer: C

NEW QUESTION 6
Which of the following are differences between AppArmor and SELinux? (Choose TWO correct answers).

A. AppArmor is implemented in user space onl
B. SELinux is a Linux Kernel Module.
C. AppArmor is less complex and easier to configure than SELinux.
D. AppArmor neither requires nor allows any specific configuratio
E. SELinux must always be manually configured.
F. SELinux stores information in extended file attribute
G. AppArmor does not maintain file specific information and states.
H. The SELinux configuration is loaded at boot time and cannot be changed later on AppArmor provides user space tools to change its behavior.

Answer: BD

NEW QUESTION 7
Which of the following commands defines an audit rule that monitors read and write operations to the file/etc/firewall/rules and associates the rule with the name firewall?

A. auditctl -N firewall -r r: /etc/firewall/rules -r w: etc/firewall/rules
B. auditctl -A -f /etc/firewall/rules -o r- o w -l firewall
C. auditctl -w /etc/firewall/rules -p rw -k firewall
D. auditctl -_read /etc/firewall/rules -_write /etc/firewall/rules --label firewall

E. echo "n: firewall r:/etc/firewall/rules: w:/ etc/firewall/rules:" I auditctl ~

Answer: C

NEW QUESTION 8
Which of the following resources of a shell and its child processes can be controlled by the Bash build-in command ulimit? (Choose THREE correct answers.)

A. The maximum size of written files
B. The maximum number of open file descriptors
C. The maximum number of newly created files
D. The maximum number of environment variables
E. The maximum number of user processes

Answer: ABE

NEW QUESTION 9
Given a proper network and name resolution setup, which of the following commands establishes a trust between a FreeIPA domain and an Active Directory domain?

A. ipa trust-add --type ad addom --admin Administrator --password
B. ipa-ad -add-trust --account ADDOM\Administrator--query-password
C. net ad ipajoin addom -U Administrator -p
D. trustmanager add -_domain ad: //addom --user Administrator -w
E. ipa ad join addom -U Administrator -w

Answer: A

NEW QUESTION 10
Which of the following statements is true about chroot environments?

A. Symbolic links to data outside the chroot path are followed, making files and directories accessible
B. Hard links to files outside the chroot path are not followed, to increase security
C. The chroot path needs to contain all data required by the programs running in the chroot environment
D. Programs are not able to set a chroot path by using a function call, they have to use the command chroot
E. When using the command chroot, the started command is running in its own namespace and cannot communicate with other processes

Answer: C

NEW QUESTION 10
Which of the following commands adds a new user usera to FreeIPA?

A. useradd usera --directory ipa --gecos *User A"
B. idap- useradd --H ldaps://ipa-server CN=UserA --attribs "Firstname: User: Lastname: A"
C. ipa-admin create user --account usera -_fname User --iname A
D. ipa user-add usera --first User --last A
E. ipa-user- add usera --name "User A"

Answer: D

NEW QUESTION 13
Which command included in the Linux Audit system provides searching and filtering of the audit log? (Specify ONLY the command without any path or parameters.)

A. Mastered
B. Not Mastered

Answer: A

Explanation:
ausearch

NEW QUESTION 18
Which of the following commands adds users using SSSD's local service?

A. sss_adduser
B. sss_useradd
C. sss_add
D. sss-addlocaluser
E. sss_local_adduser

Answer: B

NEW QUESTION 21
What effect does the configuration SSLStrictSNIVHostCheck on have on an Apache HTTPD virtual host?

A. The clients connecting to the virtual host must provide a client certificate that was issued by the same CA that issued the server's certificate.
B. The virtual host is served only to clients that support SNI.
C. All of the names of the virtual host must be within the same DNS zone.
D. The virtual host is used as a fallback default for all clients that do not support SNI.
E. Despite its configuration, the virtual host is served only on the common name and Subject Alternative Names of the server certificates.

Answer: B

NEW QUESTION 23
How does TSIG authenticate name servers in order to perform secured zone transfers?

A. Both servers mutually verify their X509 certificates.
B. Both servers use a secret key that is shared between the servers.
C. Both servers verify appropriate DANE records for the labels of the NS records used to delegate the transferred zone.
D. Both servers use DNSSEC to mutually verify that they are authoritative for the transferred zone.

Answer: B

NEW QUESTION 25
Which of the following statements are true regarding the certificate of a Root CA? (Choose TWO correct answers.)

A. It IS a self-signed certificate.
B. It does not include the private key of the CA
C. It must contain a host name as the common name.
D. It has an infinite lifetime and never expires.
E. It must contain an X509v3 Authority extension.

Answer: ABE

NEW QUESTION 29
Which option in an Apache HTTPD configuration file enables OCSP stapling? (Specify ONLY the option name without any values or parameters.)

A. Mastered
B. Not Mastered

Answer: A

Explanation:
httpd- ssl.conf

NEW QUESTION 31
Which of the following information, within a DNSSEC- signed zone, is signed by the key signing key?

A. The non-DNSSEC records like A, AAAA or MX
B. The zone signing key of the zone.
C. The RRSIG records of the zone.
D. The NSEC or NSEC3 records of the zone.
E. The DS records pointing to the zone

Answer: B

NEW QUESTION 32
Which of the following configuration options makes Apache HTTPD require a client certificate for authentication?

A. Limit valid-x509
B. SSLRequestClientCert always
C. Require valid-x509
D. SSLVerifyClient require
E. SSLPolicy valid-client-cert

Answer: D

NEW QUESTION 35
Which of the following practices are important for the security of private keys? (Choose TWO correct answers.)

A. Private keys should be created on the systems where they will be used and should never leave them.
B. private keys should be uploaded to public key servers.
C. Private keys should be included in X509 certificates.
D. Private keys should have a sufficient length for the algorithm used for key generation.
E. Private keys should always be stored as plain text files without any encryption.

Answer: CD

NEW QUESTION 39
Which DNS label points to the DANE information used to secure HTTPS connections to https://www.example.com/?

A. example.com
B. dane.www.example.com
C. soa.example com
D. www.example.com
E. _443_tcp.www example.com

Answer: E

NEW QUESTION 42
Which command, included in BIND, generates DNSSEC keys? (Specify ONLY the command without any path or parameters.)

A. Mastered
B. Not Mastered

Answer: A

Explanation:
 http://ripe60.ripe.net/presentations/Damas-BiND_9.7_-_DNSSE_for_humans.pdf

NEW QUESTION 45
What is the purpose of the program snort-stat?

A. It displays statistics from the running Snort process.
B. It returns the status of all configured network devices.
C. It reports whether the Snort process is still running and processing packets.
D. It displays the status of all Snort processes.
E. It reads syslog files containing Snort information and generates port scan statistics.

Answer: E

NEW QUESTION 49
Which of the following keywords are built-in chairs for the iptables nat table? (Choose THREE correct answers)

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

Answer: ADE

NEW QUESTION 54
What is the purpose of IP sets?

A. They group together IP addresses that are assigned to the same network interfaces.
B. They group together IP addresses and networks that can be referenced by the network routing table.
C. They group together IP addresses that can be referenced by netfilter rules.
D. They group together IP and MAC addresses used by the neighbors on the local network.
E. They group together IP addresses and user names that can be referenced from /etc/hosts allow and /etc/hosts deny

Answer: C

NEW QUESTION 55
Which of the following statements describes the purpose of ndpmon?

A. it monitors the network for neighbor discovery messages from new IPv6 hosts and routers
B. it monitors remote hosts by periodically sending echo requests to them.
C. it monitors the availability of a network link by querying network interfaces.
D. It monitors the network for IPv4 nodes that have not yet migrated to IPv6.
E. It monitors log files for failed login attempts in order to block traffic from offending network nodes

Answer: A

NEW QUESTION 59
Which of the following terms refer to existing scan techniques with nmap? (Choose TWO correct answers.)

A. Xmas Scan
B. Zero Scan
C. FIN Scan
D. IP Scan
E. UDP SYN Scan

Answer: AC

NEW QUESTION 61

Which of the following statements are valid wireshark capture filters? {Choose TWO correct answers.)

A. port range 10000:tcp-15000:tcp
B. port-range tcp 10000-15000
C. tcp portrange 10000-15000
D. portrange 10000/tcp-15000/tcp
E. portrange 10000-15000 and tcp

Answer: CE

NEW QUESTION 63
Which of the following stanzas is a valid client configuration for FreeRADIUS?

A. client pnvate-network-1 { ipaddr = 192 0 2.0/24 password = testing123-1 }
B. client private-network-1 { ip= 192.0.2.0/24 password-testing123-1 }
C. client private-network-1 { ip = 192 0 2.0/24 passwd = testing123-1 }
D. client private-network-1 { ip = 192 0.2.0/24 secret = testingl23-1 }
E. client private-network-1 { ipaddr = 192 0 2.0/24 secret = testing 123-1}

Answer: E

NEW QUESTION 65
What command is used to update NVTs from the OpenVAS NVT feed? (Specify ONLY the command without any path or parameters).

A. Mastered
B. Not Mastered

Answer: A

Explanation:
http://www.openvas.org/openvas-nvt-feed.html

NEW QUESTION 69
......