Vendor: LPI

Exam Code: 303-300

Exam Name: LPIC-3 Exam 303: Security, version 3.0

Version: DEMO

QUESTION 1
Which of the following commands lists the extended attributes set on a file?

A. lsattr
B. getfacl
C. getfattr
D. stat

Answer: C
Explanation:
The getfattr command is used to display the extended attributes of a file, such as user-defined metadata or security-related attributes stored outside the standard inode fields. lsattr, in contrast, displays file attributes specific to certain filesystems (such as ext2/3/4), like the immutable or append-only flags. getfacl is used to display POSIX Access Control Lists, not extended attributes. stat displays general file status information, such as size, permissions, and timestamps, but not extended attributes.

QUESTION 2
Which mount option prevents the execution of binaries located on the mounted filesystem?

A. nosuid
B. noexec
C. nodev
D. ro

Answer: B
Explanation:
The noexec mount option prevents any binary or script located on that filesystem from being executed directly. This is commonly applied to filesystems such as /tmp or removable media to reduce the risk of malicious code execution. nosuid disables the effect of the setuid and setgid bits on that filesystem, nodev prevents device files from being interpreted as such, and ro mounts the filesystem as read-only, none of which specifically block execution of binaries.

QUESTION 3
Which SELinux mode logs policy violations without actually enforcing the policy?

A. Enforcing
B. Permissive
C. Disabled
D. Targeted

Answer: B
Explanation:
In Permissive mode, SELinux evaluates access requests against the loaded policy and logs any actions that would have been denied, but it does not actually block them. This mode is useful for troubleshooting and policy development, allowing an administrator to review the audit log for potential AVC denials before switching to Enforcing mode, in which violations are actively blocked. Disabled mode turns SELinux off entirely, and Targeted is not a mode but rather a type of policy that only confines specific processes.

QUESTION 4

Which command is used to relabel files according to the currently loaded SELinux policy?

A. chcon
B. restorecon
C. semanage
D. setsebool

Answer: B
Explanation:
The restorecon command restores the default SELinux security context of one or more files based on the rules defined in the currently loaded policy's file contexts database. This is useful after files have been moved, copied, or had their context manually altered. chcon changes a file's context to an arbitrary value, but does not use policy-defined defaults and does not persist across a full relabel. semanage manages various aspects of SELinux policy, such as port and user mappings, while setsebool toggles SELinux boolean values.

QUESTION 5
In an AppArmor profile, what does the "complain" mode do?

A. It blocks all restricted actions and terminates the process.
B. It logs policy violations without enforcing restrictions, similar to SELinux permissive mode.
C. It disables AppArmor for that specific profile only.
D. It automatically generates a new profile based on observed behavior.

Answer: B
Explanation:
When an AppArmor profile is placed into complain mode, actions that would violate the profile's rules are logged but not blocked, allowing an administrator to observe an application's actual behavior before switching the profile to enforce mode. This is conceptually similar to SELinux's permissive mode. The aa-genprof and aa-logprof tools can process these complain-mode logs to help build or refine a profile, but complain mode itself does not automatically generate profiles.

QUESTION 6
Which command switches an AppArmor profile from complain mode into enforce mode?

A. aa-complain
B. aa-audit
C. aa-enforce
D. aa-disable

Answer: C
Explanation:
The aa-enforce command places one or more specified AppArmor profiles into enforce mode, causing violations of the profile's rules to be actively blocked rather than merely logged. The corresponding aa-complain command places a profile into complain mode, and aa-disable unloads a profile entirely, preventing it from being applied. aa-audit is used to enable full auditing of ALLOWED actions in addition to denied ones, but does not itself change enforcement.

QUESTION 7
Which PAM module is used to enforce password complexity requirements, such as minimum length and character class requirements?

A. pam_unix
B. pam_cracklib or pam_pwquality
C. pam_limits
D. pam_access

Answer: B
Explanation:
The pam_pwquality module (the modern successor to the older pam_cracklib) is used to enforce password quality and complexity requirements, such as minimum length, required character classes, and checks against dictionary words. pam_unix handles standard Unix password authentication and hashing but not complexity enforcement itself. pam_limits enforces resource limits like the maximum number of open files or processes for a user, and pam_access controls login access based on user, host, or service criteria.

QUESTION 8
Which PAM module can be used to restrict login access based on the combination of user, origin, and service?

A. pam_access
B. pam_limits
C. pam_nologin
D. pam_selinux

Answer: A
Explanation:
The pam_access module enforces login restrictions defined in the access.conf configuration file, which specifies rules based on combinations of users or groups, the origin (such as a hostname, IP address, or tty), and often the PAM service being used. This allows administrators to build fine-grained login policies, such as allowing a particular user to log in only from specific hosts. pam_nologin instead simply prevents all non-root logins when the /etc/nologin file is present.

QUESTION 9
What is the purpose of the pam_tally2 or pam_faillock module?

A. To enforce password expiration policies.
B. To track failed login attempts and lock an account after a specified number of failures.
C. To restrict resource usage per user session.
D. To require multi-factor authentication.

Answer: B
Explanation:
The pam_faillock module (and its older counterpart, pam_tally2) tracks the number of consecutive failed authentication attempts for a user account and can automatically lock the account after a configured threshold is reached, helping to mitigate brute-force password guessing attacks. Administrators can configure the number of allowed attempts, the lockout duration, and whether the lockout applies even to the root account. This differs from password expiration, which is handled by fields in /etc/shadow and related PAM modules.

QUESTION 10
Which file defines the default set of resource limits, such as maximum open files or processes,

applied to users via PAM?

A. /etc/security/limits.conf
B. /etc/pam.d/common-session
C. /etc/login.defs
D. /etc/sysctl.conf

Answer: A
Explanation:
The /etc/security/limits.conf file, used in conjunction with the pam_limits module, defines soft and hard resource limits for users and groups, such as the maximum number of open file descriptors, maximum number of processes, or maximum CPU time. /etc/login.defs contains more general login and password aging defaults for the shadow password suite, while /etc/sysctl.conf configures kernel parameters system-wide, not per-user PAM-enforced limits.

QUESTION 11
Which nftables command displays the currently active ruleset, including all tables, chains, and rules?

A. nft list ruleset
B. nft show tables
C. nft dump chains
D. nft get rules

Answer: A
Explanation:
The command "nft list ruleset" displays the complete, currently active nftables configuration, including all defined tables, chains, and the rules within them. This is the nftables equivalent of the older "iptables -L -v" command. nftables organizes rules hierarchically into tables (grouped by address family) and chains (which contain the actual rules), and this command provides a full view of that hierarchy exactly as it is loaded into the kernel.

QUESTION 12
In nftables, what is the purpose of a "base chain" as opposed to a "regular chain"?

A. A base chain can only contain accept rules.
B. A base chain is directly attached to a netfilter hook, such as input or forward, allowing it to receive packets from the kernel.
C. A base chain is used only for NAT rules.
D. There is no functional difference between base and regular chains.

Answer: B
Explanation:
A base chain in nftables is attached directly to one of the underlying netfilter hooks (such as prerouting, input, forward, output, or postrouting), which allows packets traversing the network stack at that point to be evaluated against the chain's rules. A regular chain, by contrast, is not attached to any hook and can only be reached when explicitly called (jumped or goto'd) from another chain, functioning similarly to a subroutine used for rule organization.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**