Lpi.303-300.v2026-10-24.q79

Exam Code:	303-300
Exam Name:	LPIC Exam 303: Security, version 3.0
Certification Provider:	Lpi
Free Question Number:	79
Version:	v2026-10-24
# of views:	102
# of Questions views:	790
https://www.freecram.net/torrent/Lpi.303-300.v2026-10-24.q79.html	

NEW QUESTION: 1
What is host intrusion detection (HID)?
A. A system that detects malicious traffic on a network
B. A system that monitors and detects potential security threats on a single computer or server
C. A system that scans files and folders for viruses
D. A system that prevents malware from infecting a network
Answer: (SHOW ANSWER)

NEW QUESTION: 2
Which of the following statements describes the purpose of ndpmon?
A. It monitors the availability of a network link by querying network interfaces.
B. It monitors the network for neighbor discovery messages from new IPv6 hosts and routers.
C. It monitors remote hosts by periodically sending echo requests to them.
D. It monitors log files for failed login attempts in order to block traffic from offending network nodes.
E. It monitors the network for IPv4 nodes that have not yet migrated to IPv6.
Answer: (SHOW ANSWER)

NEW QUESTION: 3
Which tool can be used to check for rootkits on a Linux system?
A. rpm
B. AIDE
C. OpenSCAP
D. chkrootkit
Answer: (SHOW ANSWER)

NEW QUESTION: 4

Which command, included in BIND, generates DNSSEC keys? (Specify ONLY the command without any path or parameters.) Solution: dnssec-keygen Determine whether the given solution is correct?

A. Incorrect

B. Correct

Answer: (SHOW ANSWER)

NEW QUESTION: 5

Which of the following is NOT a benefit of using HID?

A. Provides real-time detection of security incidents

B. Helps prevent security incidents from occurring

C. Provides automatic removal of detected threats

D. Allows for quick response to security incidents

Answer: (SHOW ANSWER)

NEW QUESTION: 6

Linux Extended File Attributes are organized in namespaces. Which of the following names correspond to existing attribute namespaces?(Choose THREE correct answers.)

A. system

B. user

C. owner

D. default

E. trusted

Answer: (SHOW ANSWER)

NEW QUESTION: 7

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

A. lsattr

B. getfacl

C. getfattr

D. stat

Answer: (SHOW ANSWER)

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.

NEW QUESTION: 8

What is phishing?

A. A type of malware that disguises itself as legitimate software
B. A type of social engineering attack
C. A type of denial-of-service attack
D. A type of virus
Answer: (SHOW ANSWER)

NEW QUESTION: 9
What option of mount.cifs specifies the user that appears as the local owner of the files of a mounted CIFS share when the server does not provide ownership information? (Specify ONLY the option name without any values or parameters.) Solution: uid=arg Determine whether the given solution is correct?
A. Incorrect
B. Correct
Answer: (SHOW ANSWER)

NEW QUESTION: 10
Which of the following access control models is established by using SELinux?
A. Group Access Control (GAC)
B. Security Access Control (SAC)
C. User Access Control (UAC)
D. Mandatory Access Control (MAC)
E. Discretionary Access Control (DAC)
Answer: (SHOW ANSWER)

NEW QUESTION: 11
Which of the following terms refer to existing scan techniques with nmap? (Choose TWO correct answers.)
A. Zero Scan
B. Xmas Scan
C. IP Scan
D. FIN Scan
E. UDP SYN Scan
Answer: (SHOW ANSWER)

NEW QUESTION: 12
What is the purpose of a Certificate Authority (CA)?
A. To decrypt X.509 certificates
B. To issue and sign X.509 certificates
C. To encrypt X.509 certificates
D. To store X.509 certificates
Answer: (SHOW ANSWER)

NEW QUESTION: 13
Which command is used to generate a new GnuPG key pair interactively?
A. gpg --gen-key
B. gpg --export
C. gpg --encrypt
D. gpg --list-keys
Answer: (SHOW ANSWER)
The command "gpg --gen-key" (or the more configurable "gpg --full-gen-key") starts an interactive process that guides the user through generating a new GnuPG key pair, prompting for the key type, key size, expiration date, and user identity information. gpg --export outputs an existing public key for sharing, gpg --encrypt encrypts data using a recipient's public key, and gpg --list-keys displays the keys already present in the local keyring rather than generating a new one.

NEW QUESTION: 14
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: (SHOW ANSWER)
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.

NEW QUESTION: 15
What is the purpose of IP sets?
A. They group together IP and MAC addresses used by the neighbors on the local network.
B. They group together IP addresses and networks that can be referenced by the network routing table.
C. They group together IP addresses and user names that can be referenced from /etc/hosts.allow and /etc/hosts.deny
D. They group together IP addresses that can be referenced by netfilter rules.
E. They group together IP addresses that are assigned to the same network interfaces.
Answer: (SHOW ANSWER)

NEW QUESTION: 16
What is a certificate chain?

A. A sequence of certificates used to verify the authenticity of a digital certificate
B. A chain of digital signatures used to verify the authenticity of a certificate
C. A sequence of public and private keys used for encryption and decryption
D. A chain of public and private keys used for encryption and decryption
Answer: (SHOW ANSWER)

Valid 303-300 Dumps shared by ExamDiscuss.com for Helping Passing 303-300 Exam! ExamDiscuss.com now offer the **newest 303-300 exam dumps**, the ExamDiscuss.com 303-300 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 303-300 dumps with Test Engine here: https://www.examdiscuss.com/Lpi/exam/303-300/premium/ (**163** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 17
What is the purpose of the Linux Audit system?
A. To automate host scans
B. To manage installed packages
C. To detect intrusions and system changes
D. To manage system log files
Answer: (SHOW ANSWER)

NEW QUESTION: 18
Which command-line tool is commonly used to test and verify TLS/SSL configuration and certificate details of a remote server?
A. openssl s_client
B. nmap -sV
C. tcpdump
D. ss -tlnp
Answer: (SHOW ANSWER)
The "openssl s_client" command connects to a remote server using TLS/SSL and displays detailed information about the negotiated protocol version, cipher suite, and the server's certificate chain, making it a common tool for troubleshooting and verifying HTTPS or other TLS-secured services. nmap's version detection can identify running services but does not provide the same depth of TLS handshake detail, tcpdump captures raw packets, and ss displays socket statistics rather than TLS-layer details.

NEW QUESTION: 19
What is a plaintext?
A. The key used to encrypt the message

B. The encrypted message
C. The original message before encryption
D. The algorithm used to encrypt the message
Answer: (SHOW ANSWER)

NEW QUESTION: 20
What is the purpose of the OpenVPN "tls-auth" or "tls-crypt" directive?
A. To disable TLS entirely and use a static key instead.
B. To add an additional layer of HMAC authentication (or full encryption, with tls-crypt) to the TLS control channel, protecting against certain DoS and port-scanning attacks.
C. To generate the server's X.509 certificate automatically.
D. To compress the VPN traffic.
Answer: (SHOW ANSWER)
The tls-auth directive adds an additional layer of HMAC signing to all TLS handshake packets using a pre-shared static key, providing protection against certain denial-of-service attacks, TLS stack vulnerabilities, and port scanning, since packets without a valid HMAC are silently dropped before any TLS processing occurs. tls-crypt provides a similar benefit but additionally encrypts the entire TLS control channel, also hiding metadata like the certificate used, offering stronger protection than tls-auth alone while still requiring the standard TLS/certificate-based data channel.

NEW QUESTION: 21
What is a Certificate Revocation List (CRL)?
A. A list of public keys that have been compromised
B. A list of private keys that have been compromised
C. A list of X.509 certificates that have been issued by a particular CA
D. A list of X.509 certificates that have been revoked by a particular CA
Answer: (SHOW ANSWER)

NEW QUESTION: 22
What is the difference between a SetUID and SetGID bit?
A. SetUID allows a user to change the owner of a file, while SetGID allows a user to change the group owner of a file
B. SetUID applies to files, while SetGID applies to directories
C. There is no difference between SetUID and SetGID
D. SetUID allows a file to be executed with the permissions of the file owner, while SetGID allows a file to be executed with the permissions of the group owner
Answer: D (LEAVE A REPLY)

NEW QUESTION: 23
What is the primary purpose of Online Certificate Status Protocol (OCSP)?
A. To encrypt data in transit between a client and server.

B. To allow a client to check the revocation status of a specific X.509 certificate in real time.
C. To generate new X.509 certificates automatically.
D. To distribute the full Certificate Revocation List to all clients.
Answer: (SHOW ANSWER)
The Online Certificate Status Protocol (OCSP) allows a client to query a certificate authority's OCSP responder to check the real-time revocation status of a specific certificate, rather than downloading and parsing an entire Certificate Revocation List (CRL). OCSP responses are typically much smaller and faster to process than CRLs, especially as the number of revoked certificates grows, though OCSP does introduce a dependency on the availability of the OCSP responder at validation time, which OCSP stapling helps address.

NEW QUESTION: 24
What is a man-in-the-middle attack?
A. An attack that intercepts communications between two parties to steal information
B. An attack that targets a specific user or organization
C. An attack that floods a network or server with traffic to make it unavailable
D. An attack that aims to steal sensitive information
Answer: A (LEAVE A REPLY)

NEW QUESTION: 25
Which of the following commands makes the contents of the eCryptfs encrypted directory ~/Private available to the user?
A. decryptfs
B. ecryptfs-mount-private
C. ecryptfsclient
D. ecryptfs-manage-directory
E. ecryptfs.mount
Answer: (SHOW ANSWER)

NEW QUESTION: 26
What is a honeypot?
A. A type of phishing scam
B. A type of virus
C. A network security tool designed to lure attackers into a trap
D. A type of denial-of-service attack
Answer: (SHOW ANSWER)

NEW QUESTION: 27
How does TSIG authenticate name servers in order to perform secured zone transfers?
A. Both servers verify appropriate DANE records for the labels of the NS records used to delegate the transferred zone.

B. Both servers mutually verify their X509 certificates.
C. Both servers use DNSSEC to mutually verify that they are authoritative for the transferred zone.
D. Both servers use a secret key that is shared between the servers.
Answer: (SHOW ANSWER)

NEW QUESTION: 28
Which of the following methods can be used to deactivate a rule in Snort? (Choose TWO correct answers.)
A. By placing a # in front of the rule and restarting Snort.
B. By placing a pass rule in local.rules and restarting Snort.
C. By deleting the rule and waiting for Snort to reload its rules files automatically.
D. By adding a pass rule to /etc/snort/rules.deactivated and waiting for Snort to reload its rules files automatically.
Answer: (SHOW ANSWER)

NEW QUESTION: 29
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. ipa ad join addom -U Administrator -w
E. trustmanager add --domain ad: //addom --user Administrator -w
Answer: (SHOW ANSWER)

NEW QUESTION: 30
Which of the following parameters to openssl s_client specifies the host name to use for TLS Server Name Indication?
Freecram.net
A. -servername
B. -host
C. -vhost
D. -tlsname
E. -sniname
Answer: (SHOW ANSWER)

NEW QUESTION: 31
What is a Trojan?
A. A type of denial-of-service attack
B. A type of phishing scam
C. A type of malware that disguises itself as legitimate software

D. A type of virus
Answer: (SHOW ANSWER)

Valid 303-300 Dumps shared by ExamDiscuss.com for Helping Passing 303-300 Exam! ExamDiscuss.com now offer the **newest 303-300 exam dumps**, the ExamDiscuss.com 303-300 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 303-300 dumps with Test Engine here: https://www.examdiscuss.com/Lpi/exam/303-300/premium/ (**163** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 32
Which Fail2ban configuration file typically contains local, site-specific overrides that should not be modified in the default jail.conf file?
A. jail.local
B. fail2ban.conf
C. action.d/iptables.conf
D. filter.d/sshd.conf
Answer: (SHOW ANSWER)
Fail2ban's documentation recommends placing local, site-specific configuration overrides in jail.local (or files within jail.d/) rather than directly editing jail.conf, since jail.conf may be overwritten during package upgrades. Settings in jail.local take precedence over those in jail.conf. The filter.d/ and action.d/ directories contain definitions for how to detect failures in specific log formats and how to execute a ban action, respectively, and are typically only edited when creating custom filters or actions.

NEW QUESTION: 33
Which command is used to set the owner and group of a file in Linux?
A. chmod
B. setfacl
C. chown
D. chgrp
Answer: (SHOW ANSWER)

NEW QUESTION: 34
Which of the following commands displays all ebtable rules contained in the table filter including their packet and byte counters?
A. ebtables -L -t filter -Lv
B. ebtables -L -Lc -t filter
C. ebtables -t filter -L --Lc

D. ebtables -t nat -L -v
E. ebtables -t filter -Ln -L
Answer: (SHOW ANSWER)

NEW QUESTION: 35
Which IPsec mode encapsulates and protects the entire original IP packet, including its header, typically used for site-to-site VPN gateways?
A. Transport mode
B. Tunnel mode
C. Aggressive mode
D. Main mode
Answer: (SHOW ANSWER)
IPsec Tunnel mode encapsulates the entire original IP packet, including its original header, inside a new IP packet with a new header. This allows the original source and destination addresses to be hidden and enables IPsec to be used between gateways protecting entire private networks, such as in a site-to-site VPN. Transport mode, by contrast, only protects the payload of the original packet and retains the original IP header, making it more suitable for host-to-host communication.

NEW QUESTION: 36
Which permission bit allows a user to delete a file?
A. Read
B. Execute
C. Write
D. SetUID
Answer: (SHOW ANSWER)

NEW QUESTION: 37
Which auditd configuration file is used to define audit rules that control which system calls and files are monitored?
A. /etc/audit/auditd.conf
B. /etc/audit/rules.d/audit.rules
C. /etc/audisp/audispd.conf
D. /var/log/audit/audit.log
Answer: (SHOW ANSWER)
Audit rules, which define which system calls, files, or directories should be monitored and under what conditions, are typically defined in files under /etc/audit/rules.d/ and compiled into /etc/audit/audit.rules (or managed directly using the auditctl command for runtime changes). The /etc/audit/auditd.conf file, by contrast, configures the behavior of the auditd daemon itself, such as log rotation and storage settings, while /var/log/audit/audit.log is where the resulting audit events are actually recorded.

NEW QUESTION: 38
In apache configuration which directives are used to restrict access based on host/domain name and IP address?
A. order, deny and accept
B. allow IP, deny IP, allow DOMAIN and deny DOMAIN
C. restrict and allow
D. deny and accept
E. order, allow from and deny from
Answer: (SHOW ANSWER)

NEW QUESTION: 39
What is a ciphertext?
A. The algorithm used to encrypt the message
B. The key used to encrypt the message
C. The original message before encryption
D. The encrypted message
Answer: (SHOW ANSWER)

NEW QUESTION: 40
What is a buffer overflow?
A. A type of virus
B. A type of malware that disguises itself as legitimate software
C. A type of denial-of-service attack
D. A type of software vulnerability
Answer: (SHOW ANSWER)

NEW QUESTION: 41
Which command is used to add a temporary audit rule that monitors write access to the /etc/passwd file?
A. auditctl -w /etc/passwd -p wa -k passwd_changes
B. ausearch -f /etc/passwd
C. aureport -f /etc/passwd
D. auditd -w /etc/passwd
Answer: (SHOW ANSWER)
The command "auditctl -w /etc/passwd -p wa -k passwd_changes" adds a watch on the /etc/passwd file, monitoring for write and attribute change (wa) events, and tags any matching events with the key "passwd_changes" to make them easier to search for later. Rules added directly with auditctl are not persistent across a reboot unless also added to a rules file under /etc/audit/rules.d/. ausearch and aureport are used to search and summarize existing audit log entries, not to create new rules.

NEW QUESTION: 42
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: (SHOW ANSWER)
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.

NEW QUESTION: 43
Which OpenVPN configuration directive specifies that the tunnel should operate at Layer 3, routing IP packets rather than bridging Ethernet frames?
A. dev tap
B. dev tun
C. proto udp
D. topology subnet
Answer: (SHOW ANSWER)
The "dev tun" directive configures OpenVPN to create a Layer 3 (routed) tunnel interface, which encapsulates and routes IP packets between the client and server. In contrast, "dev tap" creates a Layer 2 (bridged) tunnel interface that carries entire Ethernet frames, allowing broadcast traffic and non-IP protocols to pass through the tunnel, which is useful for certain bridging scenarios but generally has more overhead than a routed tun-based configuration.

NEW QUESTION: 44
What is Cryptography?
A. The art of sending secret messages
B. The art of sending public messages
C. The art of decoding messages
D. The art of sending anonymous messages
Answer: (SHOW ANSWER)

NEW QUESTION: 45
What is an X.509 Certificate?
A. A digital document that verifies the identity of a person
B. A digital document that verifies the identity of a company

C. A digital document that verifies the identity of a website
D. A digital document that verifies the identity of a device
Answer: (SHOW ANSWER)

NEW QUESTION: 46
Which of the following commands changes the source IP address to 192.0.2.11 for all IPv4 packets which go through the network interface eth0?
A. iptables ~t nat ~A PREROUTING ~i eth0 ~j SNAT --to~source 192.0.2.11
B. iptables ~t mangle ~A POSTROUTING ~0 eth0 ~j SNAT -to~source 192.0.2.11
C. iptables ~t nat ~A POSTROUTING ~i eth0 ~j DNAT --to~source 192.0.2.11
D. iptables ~t nat ~A POSTROUTING ~o eth0 ~j SNAT --to~source 192.0.2.11
E. iptables ~t mangle ~A POSTROUTING ~i eth0 ~j SNAT -to~source 192.0.2.11
Answer: (SHOW ANSWER)

Valid 303-300 Dumps shared by ExamDiscuss.com for Helping Passing 303-300 Exam! ExamDiscuss.com now offer the **newest 303-300 exam dumps**, the ExamDiscuss.com 303-300 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 303-300 dumps with Test Engine here: https://www.examdiscuss.com/Lpi/exam/303-300/premium/ (**163** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 47
What is the primary function of an Intrusion Detection System (IDS) such as Snort or Suricata operating in network-based mode?
A. To actively block malicious traffic before it reaches its destination.
B. To passively monitor network traffic and generate alerts based on signature or anomaly-based detection rules.
C. To encrypt network traffic between hosts.
D. To perform DNS resolution for network hosts.
Answer: (SHOW ANSWER)
A network-based Intrusion Detection System (NIDS), such as Snort or Suricata operating in IDS mode, passively monitors network traffic, typically via a mirrored switch port or network tap, and compares it against a set of signatures or behavioral rules to detect potential malicious activity, generating alerts for further investigation. This differs from an Intrusion Prevention System (IPS), which operates inline with the traffic path and can actively drop or block traffic matching a detection rule in real time, rather than only alerting after the fact.

NEW QUESTION: 48

Which package management tools can be used to verify the integrity of installed files on a Linux system?

A. dpkg and aptitude

B. APT and YUM

C. RPM and DPKG

D. yum and zypper

Answer: C (LEAVE A REPLY)

NEW QUESTION: 49

Which of the following sections are allowed within the Kerberos configuration file krb5.conf? (Choose THREE correct answers.)

A. [realms]

B. [domain]

C. [crypto]

D. [plugins]

E. [capaths]

Answer: (SHOW ANSWER)

NEW QUESTION: 50

What is the purpose of the program snort-stat?

passcram.net

A. It reports whether the Snort process is still running and processing packets.

B. It displays the status of all Snort processes.

C. It returns the status of all configured network devices.

D. It displays statistics from the running Snort process.

E. It reads syslog files containing Snort information and generates port scan statistics.

Answer: (SHOW ANSWER)

NEW QUESTION: 51

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

A. All of the names of the virtual host must be within the same DNS zone.

B. The virtual host is served only to clients that support SNI.

C. The virtual host is used as a fallback default for all clients that do not support SNI.

D. 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.

E. Despite its configuration, the virtual host is served only on the common name and Subject Alternative

Answer: (SHOW ANSWER)

NEW QUESTION: 52

Which Linux kernel feature restricts a process's access to a subset of system calls, commonly used by container runtimes and sandboxing tools to reduce attack surface?

A. cgroups

B. seccomp

C. namespaces

D. capabilities

Answer: (SHOW ANSWER)

Secure Computing Mode (seccomp) is a Linux kernel feature that allows a process to restrict the set of system calls it is permitted to make, typically by loading a filter (often defined using BPF) that allows, denies, or traps specific syscalls. This significantly reduces a process's attack surface by preventing it from invoking syscalls it does not need, and is widely used by container runtimes like Docker and by sandboxing frameworks. cgroups control resource usage, namespaces provide isolated views of system resources, and capabilities divide root privileges into discrete units.

NEW QUESTION: 53

What is the purpose of the GnuPG "trust level" assigned to a key, as opposed to a signature on that key?

A. It indicates how strongly the key's authenticity has been verified.

B. It indicates how much the owner trusts that key's holder to properly verify and sign other people's keys.

C. It is identical in meaning to a key signature and is redundant.

D. It determines the key's expiration date.

Answer: (SHOW ANSWER)

A trust level in GnuPG is a personal, local judgment about how much a user trusts a particular key's owner to carefully and correctly verify the identity of others before signing their keys. This is distinct from a signature, which asserts that a specific key's authenticity has been verified. Trust levels (such as none, marginal, full, and ultimate) affect how GnuPG calculates the validity of other keys in the web of trust based on the chain of signatures connecting them back to the user's own key.

NEW QUESTION: 54

What is Linux Malware Detect?

A. A configuration management tool

B. A package management tool

C. A tool to automate host scans

D. A tool to detect malware on a Linux system

Answer: (SHOW ANSWER)

NEW QUESTION: 55

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: (SHOW ANSWER)
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.

NEW QUESTION: 56
How can host scans be automated on a Linux system?
A. Using OpenSCAP
B. Using Linux Audit system
C. Using chkrootkit
D. Using cron
Answer: (SHOW ANSWER)

NEW QUESTION: 57
What is the purpose of AIDE?
A. To automate host scans
B. To manage system log files
C. To detect intrusions and system changes
D. To manage installed packages
Answer: (SHOW ANSWER)

NEW QUESTION: 58
What is the primary purpose of Fail2ban?
A. To encrypt log files stored on disk.
B. To monitor log files for repeated failed authentication attempts and dynamically block the offending IP address using firewall rules.
C. To generate strong random passwords for user accounts.
D. To replace the need for a firewall entirely.
Answer: (SHOW ANSWER)
Fail2ban is a log-monitoring intrusion prevention tool that scans log files, such as those generated by SSH or web server authentication, for patterns indicating repeated failed login attempts. When a configured threshold of failures from a specific IP address is reached within a defined time

window, Fail2ban dynamically inserts a firewall rule (via iptables, nftables, or another supported backend) to temporarily block that IP address, helping to mitigate brute-force attacks without requiring permanent manual firewall configuration.

NEW QUESTION: 59
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: (SHOW ANSWER)
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.

NEW QUESTION: 60
How are SELinux permissions related to standard Linux permissions? (Choose TWO correct answers.)
A. SELinux permissions are verified before standard Linux permissions.
B. Standard Linux permissions override SELinux permissions.
C. SELinux permissions override standard Linux permissions.
D. SELinux permissions are verified after standard Linux permissions.
Answer: (SHOW ANSWER)

NEW QUESTION: 61
Which file is used to configure AIDE?
A. /etc/audit/auditd.conf
B. /etc/rkhunter.conf
C. /etc/maldet.conf
D. /etc/aide/aide.conf
Answer: (SHOW ANSWER)

Valid 303-300 Dumps shared by ExamDiscuss.com for Helping Passing 303-300 Exam! ExamDiscuss.com now offer the **newest 303-300 exam dumps**, the ExamDiscuss.com 303-300 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 303-300 dumps with Test Engine here:

https://www.examdiscuss.com/Lpi/exam/303-300/premium/ (**163** Q&As Dumps, **35%OFF**
Special Discount Code: freecram)

NEW QUESTION: 62
Which of the following statements is true regarding eCryptfs?
A. When a user changes his login password, the contents of his eCryptfs home directory has to be re- encrypted using his new login password.
B. For every file in an eCryptfs directory there exists a corresponding file that contains the encrypted content.
C. After unmounting an eCryptfs directory, the directory hierarchy and the original file names are still visible, although, it is not possible to view the contents of the files.
D. The content of all files in an eCryptfs directory is stored in an archive file similar to a tar file with an additional index to improve performance.
E. eCryptfs cannot be used to encrypt only directories that are the home directory of a regular Linux user.
Answer: (SHOW ANSWER)

NEW QUESTION: 63
What type of activity does HID monitor for?
A. File and folder changes
B. Unauthorized access attempts
C. Network traffic
D. Malware infections
Answer: B (LEAVE A REPLY)

NEW QUESTION: 64
Which of the following components are part of FreeIPA? (Choose THREE correct answers.)
A. DHCP Server
B. Kerberos KDC
C. Intrusion Detection System
D. Public Key Infrastructure
E. Directory Server
Answer: (SHOW ANSWER)

NEW QUESTION: 65
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.) Solution: ausearch Determine whether the given solution is correct?
A. Correct
B. Incorrect
Answer: (SHOW ANSWER)

NEW QUESTION: 66
A LUKS device was mapped using the command: cryptsetup luksOpen/dev/sda1 crypt-vol Given that this device has three different keys, which of the following commands deletes only the first key?
A. cryptsetup luksDelKey / dev /mapper/crypt- vol 0
B. cryptsetup luksDelKey / dev /mapper/crypt- vol 1
C. cryptsetup luksDelKey /dev/sda 1 0
D. cryptsetup luksDelkey /dev/sda 1 1
Answer: (SHOW ANSWER)

NEW QUESTION: 67
Which of the following keywords are built-in chairs for the iptables nat table? (Choose THREE correct answers.)
A. PROCESSING
B. PREROUTING
C. POSTROUTING
D. OUTPUT
E. MASQUERADE
Answer: (SHOW ANSWER)

NEW QUESTION: 68
Which of the following types can be specified within the Linux Audit system? (Choose THREE correct answers.)
A. File system rules
B. Network connection rules
C. Console rules
D. Control rules
E. System call rules
Answer: (SHOW ANSWER)

NEW QUESTION: 69
What is the purpose of OCSP stapling?
A. It allows the certificate authority to revoke a certificate faster.
B. It allows the server, rather than the client, to periodically query the OCSP responder and attach the signed response to the TLS handshake.
C. It replaces the need for a Certificate Revocation List entirely.
D. It encrypts the OCSP request between client and CA.
Answer: (SHOW ANSWER)
OCSP stapling allows a web server to periodically query its certificate authority's OCSP responder itself and cache (or "staple") the signed OCSP response directly to the TLS handshake

sent to clients. This eliminates the need for each individual client to contact the OCSP responder separately, improving performance and privacy, and also avoids failures if the OCSP responder is temporarily unreachable from the client's network, since the server provides an already-signed, time-stamped response.

NEW QUESTION: 70

Which of the following prefixes could be present in the output of getclfsacl? (Choose THREE correct answers.)

Freecram.net

A. OWNER
B. GROUP
C. SID
D. ACL
E. GRANT
Answer: (SHOW ANSWER)

NEW QUESTION: 71

Which command is used to set the permissions of a file in Linux?
A. chmod
B. chgrp
C. setfacl
D. chown
Answer: (SHOW ANSWER)

NEW QUESTION: 72

Which mount option prevents the execution of binaries located on the mounted filesystem?
A. nosuid
B. noexec
C. nodev
D. ro
Answer: (SHOW ANSWER)
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.

NEW QUESTION: 73

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 number of environment variables
B. The maximum number of newly created files

C. The maximum size of written files
D. The maximum number of open file descriptors
E. The maximum number of user processes
Answer: (SHOW ANSWER)

NEW QUESTION: 74
Which of the following stanzas is a valid client configuration for FreeRADIUS?
A. client private-network-1 {
ip = 192.0.2.0/24
secret = testing123-1
}
B. client private-network-1 {
ip = 192.0.2.0/24
passwd = testing123-1
}
C. client private-network-1 {
ipaddr = 192.0.2.0/24
secret = testing123-1
}
D. client private-network-1 {
ipaddr = 192.0.2.0/24
password = testing123-1
}
E. client private-network-1 {
ip = 192.0.2.0/24
password = testing123-1
}
Answer: (SHOW ANSWER)

NEW QUESTION: 75
What happens when the command getfattr afile is run while the file afile has no extended attributes set?
A. No outputs is produced and getfattr exits with a value of 1.
B. No output is produced and getfattr exits with a value of 0.
C. getfattr prints a warning and exits with a values of 0.
D. getfattr prints a warning and exits with a value of 1.
Answer: (SHOW ANSWER)

NEW QUESTION: 76
What is the purpose of a LUKS key slot?
A. It stores a copy of the encrypted data for redundancy.

B. It stores an encrypted copy of the master key, protected by a specific passphrase or keyfile, allowing multiple independent unlock methods.
C. It defines the filesystem type used on the encrypted volume.
D. It stores the device's UUID.
Answer: (SHOW ANSWER)
LUKS supports multiple key slots (typically up to eight), each of which stores an independently encrypted copy of the volume's master encryption key, protected by a different passphrase or keyfile. This allows multiple users or unlock methods to access the same encrypted volume without sharing a single passphrase, and allows a passphrase to be changed or revoked (by clearing its key slot) without needing to re-encrypt the entire underlying data, since the actual master key used to encrypt the data itself never changes.

Valid 303-300 Dumps shared by ExamDiscuss.com for Helping Passing 303-300 Exam! ExamDiscuss.com now offer the **newest 303-300 exam dumps**, the ExamDiscuss.com 303-300 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 303-300 dumps with Test Engine here: https://www.examdiscuss.com/Lpi/exam/303-300/premium/ (**163** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 77
Which option of the openvpn command should be used to ensure that ephemeral keys are not written to the swap space?
A. --no-swap
B. --root-swap
C. --mlock
D. --keys-no-swap
Answer: (SHOW ANSWER)

NEW QUESTION: 78
Which command displays currently listening TCP and UDP sockets along with the process ID and name of the associated program?
A. ss -tulnp
B. ping -c 4
C. traceroute
D. dig
Answer: (SHOW ANSWER)
The command "ss -tulnp" displays currently listening TCP (-t) and UDP (-u) sockets (-l), showing numeric addresses and ports (-n) along with the process ID and name of the program holding each socket open (-p), which requires appropriate privileges to view processes owned by other

users. This is useful for auditing which services are actively listening on a system and identifying unexpected or unauthorized listening services. ping, traceroute, and dig are used for connectivity testing, path tracing, and DNS lookups respectively, not for enumerating local listening sockets.

NEW QUESTION: 79
In which path is the data, which can be altered by the sysctl command, accessible?
A. /sys/
B. /sysctl/
C. /proc/sys/
D. /dev/sys/
Answer: (SHOW ANSWER)

Valid 303-300 Dumps shared by ExamDiscuss.com for Helping Passing 303-300 Exam! ExamDiscuss.com now offer the **newest 303-300 exam dumps**, the ExamDiscuss.com 303-300 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 303-300 dumps with Test Engine here: https://www.examdiscuss.com/Lpi/exam/303-300/premium/ (**163** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)