Exam Questions XK0-006

CompTIA Linux+ Exam

https://www.2passeasy.com/dumps/XK0-006/

NEW QUESTION 1
Which of the following is a protocol for accessing distributed directory services containing a hierarchy of users, groups, machines, and organizational units?

A. SMB
B. TLS
C. LDAP
D. KRB-5

Answer: C

Explanation:
Directory services are a key part of enterprise Linux environments and are covered under the Security domain in Linux+ V8. The Lightweight Directory Access Protocol (LDAP) is specifically designed to access and manage distributed directory information.
LDAP directories store structured, hierarchical data such as users, groups, computers, and organizational units. Linux systems commonly use LDAP for centralized authentication, authorization, and identity management. LDAP is also the foundation for services like Active Directory and FreeIPA.
The other options are incorrect. SMB is a file and printer sharing protocol. TLS is an encryption protocol used to secure communications. Kerberos (KRB-5) is an authentication protocol often used alongside LDAP but does not store directory information itself.
Linux+ V8 documentation highlights LDAP as the primary protocol for directory-based identity services. Therefore, the correct answer is C.

NEW QUESTION 2
A systems administrator needs to integrate a new storage array into the company's existing storage pool. The administrator wants to ensure that the server is able to detect the new storage array. Which of the following commands should the administrator use to ensure that the new storage array is presented to the systems?

A. lsscsi
B. lsusb
C. lsipc
D. lshw

Answer: A

Explanation:
Comprehensive and Detailed Explanation: From Exact Extract:
The lsscsi command is used to list information about SCSI devices (including storage arrays) that are attached to the system. This is critical when integrating a new storage array because it allows the administrator to verify that the operating system detects the new device at the SCSI layer, which is the underlying interface for most enterprise storage solutions. lsscsi outputs a list of recognized SCSI devices, their device nodes, and associated information.
Other options:
- B. lsusb: Lists USB devices, not storage arrays on SCSI/SATA/SAS.
- C. lsipc: Displays information on IPC (inter-process communication) facilities, unrelated to hardware detection.
- D. lshw: Lists hardware details and can show storage, but lsscsi is specifically designed for SCSI device detection and is the most direct method for this task.

Reference:
CompTIA Linux+ Study Guide: Exam XK0-006, Sybex, Chapter 7: "Managing Storage", Section: "Identifying and Accessing Storage Devices"
CompTIA Linux+ XK0-006 Objectives: Domain 4.0 – Storage and Filesystems
==========

NEW QUESTION 3
Which of the following most accurately describes a webhook?

A. An authentication method for web-server communication
B. An SNMP-based API for network device monitoring
C. A means to transmit sensitive information between systems
D. An HTTP-based callback function

Answer: D

Explanation:
Webhooks are commonly used in automation and DevOps workflows, which are emphasized in the Linux+ V8 objectives. A webhook is best described as anHTTP-based callback mechanismthat allows one system to notify another when a specific event occurs.
OptionDcorrectly defines a webhook. Instead of polling an API at regular intervals, a webhook allows an application to automatically send an HTTP request—typically a POST—to a predefined URL when an event happens. This makes webhooks efficient, event-driven, and well-suited for automation pipelines, CI/CD systems, and monitoring integrations.
The other options are incorrect. OptionAconfuses webhooks with authentication mechanisms. OptionBincorrectly associates webhooks with SNMP, which is a separate protocol. OptionCis misleading because webhooks are not inherently designed for transmitting sensitive data and require additional security measures such as TLS and authentication.
Linux+ V8 documentation highlights webhooks as a key integration method in automated environments, enabling systems to react in real time to changes or triggers.
Therefore, the correct answer isD.

NEW QUESTION 4
In the echo "profile-$num-$name" line of a shell script, the variable $num seems to not be expanding during execution. Which of the following notations ensures the value is expanded?

A. echo "profile-$(num)-$name"
B. echo 'profile-$num-$name'
C. echo "profile-'$num'-$name"
D. echo "profile-${num}-$name"

Answer: D

Explanation:
Shell variable expansion is a fundamental scripting concept included in Linux+ V8 objectives. In Bash and similar shells, variables are expanded only when they are interpreted within double quotes or unquoted contexts, and sometimes explicit syntax is required to avoid ambiguity.
The correct notation is ${num}, as shown in option D. Using curly braces around the variable name ensures the shell correctly identifies the variable boundary, especially when it is adjacent to other characters. This guarantees proper expansion of the variable's value.
The other options are incorrect. Single quotes prevent variable expansion entirely. The $(...) syntax is used for command substitution, not variable expansion. Quoting the variable name itself also prevents expansion.
Linux+ V8 documentation emphasizes ${VAR} notation as a best practice in shell scripting for clarity and correctness. Therefore, the correct answer is D.

NEW QUESTION 5
Which of the following is the main reason for setting up password expiry policies?

A. To avoid using the same passwords repeatedly
B. To mitigate the use of exposed passwords
C. To force usage of passwordless authentication
D. To increase password strength and complexity

Answer: B

Explanation:
Password management is a core topic in the Security domain of CompTIA Linux+ V8. Password expiry policies are implemented to reduce the risk associated with long-lived credentials.
The primary reason for enforcing password expiration is to mitigate the risk of exposed or compromised passwords. If a password is leaked through phishing, malware, keylogging, or data breaches, limiting its lifespan reduces the window of opportunity for attackers to exploit it. Requiring periodic password changes ensures that compromised credentials eventually become invalid.
Option B correctly captures this security objective. Linux+ V8 documentation emphasizes minimizing credential exposure as a key principle of access control.
The other options are secondary or incorrect. Avoiding password reuse and increasing complexity are addressed through password history and complexity policies, not expiration alone. Password expiry does not force passwordless authentication, making option C incorrect.
Therefore, the correct answer is B. To mitigate the use of exposed passwords.

NEW QUESTION 6
A systems administrator attempts to edit a file as root, but receives the following error:

```
E212: Cannot open file for writing

# ls -l /etc/resolv.conf
-rw-------. 1 root admin 141 May 30 11:00 /etc/resolv.conf

# lsattr /etc/resolv.conf
----i-----------  /etc/resolv.conf
```

Which of the following commands allows the administrator to edit the file?

A. chown root /etc/resolv.conf
B. chattr -i /etc/resolv.conf
C. chmod 750 /etc/resolv.conf
D. chgrp root /etc/resolv.conf

Answer: B

Explanation:
This scenario involves Linux file attributes and falls under theSystem Managementdomain of the CompTIA Linux+ V8 objectives. Although the administrator is operating as the root user, the system prevents the file from being modified. This behavior indicates that standard UNIX permissions are not the root cause of the problem.
The critical clue is provided by the lsattr /etc/resolv.conf output, which shows theimmutable (i) attributeset on the file. When a file is marked immutable, it cannot be modified, deleted, renamed, or written to by any user, including root. This restriction overrides normal file permissions and ownership settings.
The chattr command is used to modify extended file attributes on Linux filesystems such as ext4. The option -i specifically removes the immutable attribute, restoring the file??s ability to be edited. Therefore, running chattr -i /etc/resolv.conf allows the administrator to open and modify the file successfully.
The other options do not resolve the issue. chown root changes file ownership, but the file is already owned by root. chmod 750 modifies permission bits, but permissions are ignored when the immutable attribute is set. chgrp root changes the group ownership, which also has no effect when immutability is enforced.
Linux+ V8 documentation highlights immutable files as a security and stability feature, commonly used to protect critical configuration files from accidental or unauthorized changes. Administrators must explicitly remove this attribute before making modifications.
Therefore, the correct command to allow editing the file isB. chattr -i /etc/resolv.conf.

NEW QUESTION 7
An administrator needs to remove the directory /home/user1/data and all of its contents. Which of the following commands should the administrator use?

A. rmdir -p /home/user1/data
B. ln -d /home/user1/data
C. rm -r /home/user1/data
D. cut -d /home/user1/data

Answer: C

Explanation:
File and directory management is a core system administration skill addressed in Linux+ V8. When an administrator needs to delete a directory that contains files or subdirectories, a recursive deletion is required.
The correct command is rm -r /home/user1/data. The rm command removes files, and the -r (recursive) option allows it to delete directories and all of their contents, including nested files and subdirectories. This is the standard and correct method for removing non-empty directories.
The other options are incorrect. rmdir -p only removes empty directories and will fail if the directory contains files. ln -d is used to create directory hard links, not remove directories. cut -d is a text-processing command unrelated to filesystem operations.
Linux+ V8 documentation stresses caution when using rm -r, as it permanently deletes data without recovery unless backups exist. Therefore, the correct answer is C.

NEW QUESTION 8
A Linux user needs to download the latest Debian image from a Docker repository. Which of the following commands makes this task possible?

A. docker image init debian
B. docker image pull debian
C. docker image import debian
D. docker image save debian

Answer: B

Explanation:
Container management and image handling are part of modern Linux automation practices covered in CompTIA Linux+ V8. Docker images are stored in container registries such as Docker Hub, and administrators commonly need to download images to deploy containers.
The correct command for downloading an image from a Docker repository is docker image pull. This command retrieves the specified image from a configured container registry and stores it locally. When no tag is specified, Docker automatically pulls the latest available version of the image. Therefore, docker image pull debian downloads the most recent Debian image from Docker Hub.
The other options are incorrect. docker image init is not a valid Docker command and does not exist in Docker??s CLI. docker image import is used to create a Docker image from a tarball file, not to download an image from a repository. docker image save exports an existing local image into a tar archive and does not retrieve images from a remote registry.
Linux+ V8 documentation emphasizes understanding container image lifecycles, including pulling, tagging, and running images. Pulling images is a foundational step before container execution and automation workflows.
Therefore, the correct answer is B. docker image pull debian.

NEW QUESTION 9
A DevOps engineer made some changes to files in a local repository. The engineer realizes that the changes broke the application and the changes need to be reverted back. Which of the following commands is the best way to accomplish this task?

A. git pull
B. git reset
C. git rebase
D. git stash

Answer: B

Explanation:
Version control rollback operations are a core DevOps skill covered in the Linux+ V8 objectives. When changes in a local Git repository break an application and must be reverted, the administrator must choose a command that directly undoes those changes.
The command git reset is the most appropriate option in this scenario. It allows the engineer to move the current branch pointer (HEAD) to a previous commit, effectively discarding or undoing local changes. Depending on the reset mode (--soft, --mixed, or --hard), the engineer can control whether changes are preserved in the staging area or working directory. This flexibility makes git reset the primary tool for reverting problematic local changes.
The other options are not suitable. git pull fetches and merges changes from a remote repository and does not revert local modifications. git rebase rewrites commit history and is used to reapply commits on top of another base, not to undo broken changes. git stash temporarily saves uncommitted changes for later use but does not revert the repository to a stable state.
Linux+ V8 documentation emphasizes that git reset is commonly used during local development when changes need to be undone quickly before being shared with others. Therefore, the correct answer is B.

NEW QUESTION 10
Users report that a Linux system is unresponsive and simple commands take too long to complete. The Linux administrator logs in to the system and sees the following:
Output 1:
10:06:29 up 235 day, 19:23, 2 users, load average: 8.71, 8.24, 7.71
Output 2:

Linux 6.8.0-31-generic (host) 05/10/2024 _x86_64_ (4 CPU)

10:07:42	AM	CPU	%usr	%nice	%sys	%iowait	%irq	%soft	%steal	%guest	%gnice	%idle
10:07:42	AM	all	65.88	0	20.54	5.65	0	7.93	0	0	0	0

Which of the following is the system experiencing?

A. High latency
B. High uptime
C. High CPU load
D. High I/O wait times

Answer: C

Explanation:
This scenario is a classic performance troubleshooting case covered under the Troubleshooting domain of the CompTIA Linux+ V8 objectives. The key indicators to analyze are the load average values and the CPU utilization statistics.
The uptime command shows load averages of 8.71, 8.24, and 7.71 over the 1-, 5-, and 15-minute intervals. Load average represents the average number of processes that are either running on the CPU or waiting to run. On a system with 4 CPU cores, a healthy load average would typically be close to or below 4. Load averages consistently near or above 8 indicate that there are significantly more runnable processes than available CPU resources, causing processes to wait and resulting in poor system responsiveness.
The CPU output further confirms this condition. The %idle value is 0, meaning the CPU has no idle time available. The majority of CPU time is spent in user space (65.88%) and system/kernel space (20.54%), indicating heavy computational and kernel activity. While %iowait is present at 5.65%, it is not high enough to suggest that disk I/O is the primary bottleneck.
Option C, high CPU load, best explains the symptoms. High CPU load causes commands to execute slowly because processes are competing for limited CPU time. This directly matches the observed behavior of the system being unresponsive.
The other options are incorrect. High uptime simply indicates how long the system has been running and does not cause performance issues by itself. High latency is a general term and not a specific diagnosis shown by the metrics provided. High I/O wait times would require a significantly higher %iowait value.
According to Linux+ V8 documentation, correlating load averages with CPU core count and utilization is essential for accurate performance diagnosis. Therefore, the correct answer is C. High CPU load.

NEW QUESTION 10
A Linux administrator attempts to log in to a server over SSH as root and receives the following error message: Permission denied, please try again. The administrator is able to log in to the console of the server directly with root and confirms the password is correct. The administrator reviews the configuration of the SSH service and gets the following output:

```
Port 22
PermitRootLogin prohibit-password
PasswordAuthentication yes
PermitEmptyPassword no
Use PAM no
MaxSessions 1
MaxAuthTries 3
```

Based on the above output, which of the following will most likely allow the administrator to log in over SSH to the server?

A. Log out other user sessions because only one is allowed at a time.
B. Enable PAM and configure the SSH module.
C. Modify the SSH port to use 2222.
D. Use a key to log in as root over SSH.

Answer: D

Explanation:
The SSH configuration option PermitRootLogin prohibit-password prevents the root user from logging in with password authentication. This setting means root cannot use a password to log in via SSH; only key- based authentication is permitted for root. The administrator can still log in as root locally, which is not affected by this SSH configuration. To allow SSH access as root, the administrator must use an SSH key instead of a password.
Other options:
* A. MaxSessions controls the number of simultaneous SSH sessions but is not causing the login denial here.
* B. PAM (Pluggable Authentication Modules) is disabled, but enabling it is not required for basic SSH authentication.
* C. Changing the SSH port is unrelated to the authentication method issue.
Reference:
CompTIA Linux+ Study Guide: Exam XK0-006, Sybex, Chapter 11: "Securing Linux", Section: "Securing SSH Access"
CompTIA Linux+ XK0-006 Objectives, Domain 3.0: Security

NEW QUESTION 14
Which of the following can reduce the attack surface area in relation to Linux hardening?

A. Customizing the log-in banner
B. Reducing the number of directories created
C. Extending the SSH startup timeout period
D. Enforcing password strength and complexity

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Reducing the attack surface area in Linux hardening refers to limiting possible points of unauthorized access. According to the CompTIA Linux+ Official Study Guide (Exam XK0-006), enforcing strong password policies is a critical aspect of security hardening. This practice ensures that user accounts are protected by passwords that are difficult to guess or crack, thus minimizing the risk of successful brute-force attacks. Implementing password complexity requirements (such as minimum length, use of uppercase, lowercase, numbers, and special characters) directly addresses one of the primary vectors for unauthorized access.
Other options do not have a direct impact on reducing the attack surface:
* A. Customizing the log-in bannerserves as a legal notification and does not affect system vulnerabilities.
* B. Reducing the number of directories createdis not related to hardening or access control.
* C. Extending the SSH startup timeout periodmay give attackers more time to attempt a connection and does not increase security.
[Reference:, CompTIA Linux+ Study Guide: Exam XK0-006, Sybex, Chapter 11: "Securing the System", Section: "Implementing Password Policies", CompTIA Linux+ XK0-006 Exam Objectives, Domain 3.0: Security, , ,]

NEW QUESTION 15
A Linux systems administrator needs to extract the contents of a file named /home/dev/web.bkp to the /var/www/html/ directory. Which of the following commands should the administrator use?

A. cd /var/www/html/ && gzip -c /home/dev/web.bkp | tar xf -
B. pushd /var/www/html/ && cpio -idv < /home/dev/web.bkp && popd
C. tar -c -f /home/dev/web.bkp /var/www/html/
D. unzip -c /home/dev/web.bkp /var/www/html/

Answer: B

Explanation:
Comprehensive and Detailed 250 to 350 words of Explanation From Linux+ V8 documents:
File extraction and backup restoration are fundamentalSystem Managementtasks covered in CompTIA Linux+ V8. In this scenario, the administrator must extract the contents of an existing backup file into a target directory.
The correct command isoption B, which uses cpio in extract mode. The command changes into the destination directory (/var/www/html/) using pushd, extracts the archive contents with cpio -idv, and then returns to the original directory with popd. This ensures that files are restored into the correct location without modifying paths inside the archive.
The cpio utility is commonly used for backups created with cpio -o and supports reading archive data from standard input. Linux+ V8 documentation includes cpio as a valid and supported archive format for backup and restore operations.
The other options are incorrect. OptionAincorrectly assumes the backup is a gzip-compressed tar archive. OptionCcreates a new archive instead of extracting one. OptionDassumes the file is a ZIP archive, which is not indicated by the .bkp extension.
Linux+ V8 emphasizes using the correct tool based on the archive format and restoring files into the intended directory. Therefore, the correct answer isB.

NEW QUESTION 20
A Linux administrator needs to analyze a compromised disk for traces of malware. To complete the analysis, the administrator wants to make an exact, block-level copy of the disk. Which of the following commands accomplishes this task?

A. cp -rp /dev/sdc/* /tmp/image
B. cpio -i /dev/sdc -ov /tmp/image
C. tar cvzf /tmp/image /dev/sdc
D. dd if=/dev/sdc of=/tmp/image bs=8192

Answer: D

Explanation:
Disk forensics and malware analysis fall under theSecuritydomain in the CompTIA Linux+ V8 objectives. When analyzing a compromised disk, it is critical to preserve the data exactly as it exists, including unused space, deleted files, and hidden metadata. This requires ablock-level copy, not a file-level copy.
The dd command is the correct tool for this task. It operates at a low level, copying raw data from an input device (if=/dev/sdc) directly to an output file (of=/tmp/image) without interpreting filesystem structures. This ensures an exact, bit-for-bit replica of the disk, which is essential for forensic integrity and malware analysis. The bs=8192 option improves performance by specifying a larger block size during copying.
The other options are incorrect. cp -rp copies files and directories but does not capture free space, deleted data, or disk metadata. cpio and tar are archive utilities that operate at the filesystem level and cannot produce a true disk image. These tools also require the filesystem to be mounted and readable, which is not appropriate for forensic preservation.
Linux+ V8 documentation highlights dd as the preferred utility for disk imaging, backups, and forensic investigations. Administrators are also advised to perform such operations on unmounted disks to avoid altering evidence.
Therefore, the correct and best command for creating an exact block-level disk copy isD. dd if=/dev/sdc of=/tmp/image bs=8192.

NEW QUESTION 25
A systems administrator needs to set the IP address of a new DNS server. Which of the following files should the administrator modify to complete this task?

A. /etc/whois.conf
B. /etc/resolv.conf
C. /etc/nsswitch.conf
D. /etc/dnsmasq.conf

Answer: B

Explanation:
DNS client configuration is a foundational Linux networking task covered in Linux+ V8 system management objectives. When an administrator needs to specify the IP address of a DNS server that the system should use for name resolution, the correct file to modify is/etc/resolv.conf.
The /etc/resolv.conf file defines DNS resolver settings, including one or more nameserver entries that specify the IP addresses of DNS servers. Applications and system services rely on this file to resolve hostnames to IP addresses.
The other options are incorrect. /etc/whois.conf configures WHOIS queries. /etc/nsswitch.conf controls the order of name resolution sources but does not define DNS server IP addresses. /etc/dnsmasq.conf configures a local DNS caching service, not the system-wide resolver directly.
Linux+ V8 documentation highlights /etc/resolv.conf as the authoritative DNS client configuration file, though it may be dynamically managed by tools such as NetworkManager or systemd-resolved.
Therefore, the correct answer isB. /etc/resolv.conf.

NEW QUESTION 28
An administrator receives reports that a web service is not responding. The administrator reviews the following outputs:

```
$ echo $PWD
/etc/pki/nginx

$ ls -lRt
.:
total 8
drwxr-xr-x. 2 root root 6 Jul 10 10:57 private
-rw-r--r--. 1 root root 895 Jul 10 10:56 server.crt
-rw-------. 1 root root 227 Jul 10 10:56 server.key
./private:
total 0

$ sudo systemctl status nginx
  nginx.service - The nginx HTTP and reverse proxy server
       Loaded: loaded (/usr/lib/systemd/system/nginx.service; disabled; preset: disabled)
       Active: failed (Result: exit-code) since Wed 2023-11-01 06:56:51 EDT; 6s ago
    Process: 110551 ExecStartPre=/usr/bin/rm -f /run/nginx.pid (code=exited, status=0/SUCCESS)
    Process: 110552 ExecStartPre=/usr/sbin/nginx -t (code=exited, status=1/FAILURE)
       CPU: 144ms

Nov 01 06:56:51 webserver systemd[1]: Starting nginx.service - The nginx HTTP and reverse proxy server...
Nov 01 06:56:51 webserver nginx[110552]: nginx: [emerg] cannot load certificate key "/etc/pki/nginx/private/server.key": BIO_new_file()
failed (SSL: error:80000002:system library::No such file or directory:calli>
Nov 01 06:56:51 webserver nginx[110552]: nginx: configuration file /etc/nginx/nginx.conf test failed
Nov 01 06:56:51 webserver systemd[1]: nginx.service: Control process exited, code=exited, status=1/FAILURE
Nov 01 06:56:51 webserver systemd[1]: nginx.service: Failed with result 'exit-code'.
Nov 01 06:56:51 webserver systemd[1]: Failed to start nginx.service - The nginx HTTP and reverse proxy server.
```

Which of the following is the reason the web service is not responding?

A. The private key needs to be renamed from server.crt to server, key so the service can find it.
B. The private key does not match the public key, and both keys should be replaced.
C. The private key is not in the correct location and needs to be moved to the correct directory.
D. The private key has the incorrect permissions and should be changed to 0755 for the service.

Answer: C

Explanation:
This issue falls under the Troubleshooting domain of the CompTIA Linux+ V8 objectives, specifically service startup failures and certificate-related errors. The provided output clearly indicates that the NGINX service fails during startup due to an inability to locate the private key file.
The critical error message is:
cannot load certificate key "/etc/pki/nginx/private/server.key": No such file or directory
This message confirms that NGINX is explicitly configured to look for the private key in the directory /etc/pki/nginx/private/. However, the directory listing shows that the private directory exists but is empty, while the server.key file is located in /etc/pki/nginx/ instead. Because NGINX cannot find the private key at the configured path, the configuration test (nginx -t) fails, and systemd prevents the service from starting.
Option C correctly identifies the root cause: the private key is not in the correct location. Moving server.key into /etc/pki/nginx/private/ (or updating the NGINX configuration to match the current location) would resolve the issue. Linux+ V8 documentation stresses that service failures often result from misaligned configuration paths rather than corrupted files.
The other options are incorrect. Option A incorrectly refers to renaming a certificate file and does not address the path issue. Option B suggests a key mismatch, which would generate a different SSL error rather than a "file not found" error. Option D is also incorrect because private keys should not have executable permissions like 0755; typically, they are restricted (for example, 0600) for security reasons.
Therefore, the web service is not responding because the private key file is not located in the directory expected by the NGINX configuration. The correct answer is C.

NEW QUESTION 33
A systems administrator needs to check the statuses of all the services on a Linux server. Which of the following commands accomplishes this task?

A. systemctl is-active --services
B. systemctl list-sockets --type=services
C. systemctl is-enabled --services
D. systemctl list-units --type=services

Answer: D

Explanation:
Service management usingsystemdis a core Linux+ V8 system management objective. Administrators frequently need to view the current status of all services to determine which ones are running, stopped, failed, or inactive.
The correct command issystemctl list-units --type=services, which displays all loaded service units along with their current state, including whether they are active, inactive, failed, or running. This provides a comprehensive, real-time view of service statuses on the system and is commonly used during troubleshooting and audits.
OptionA, systemctl is-active, is designed to check the status of a single service, not all services. OptionBlists socket units, not services. OptionC, systemctl is-enabled, checks whether services are enabled at boot, not whether they are currently running.
Linux+ V8 documentation explicitly references systemctl list-units --type=service as the primary command for viewing service runtime states. Therefore, the correct answer isD.

NEW QUESTION 36
A systems administrator receives reports about connection issues to a secure web server. Given the following firewall and web server outputs:
Firewall output:
Status: active
To Action From
443/tcp DENY Anywhere
443/tcp (v6) DENY Anywhere (v6)
Web server output:
tcp LISTEN 0 4096 *:443 :
Which of the following commands best resolves this issue?

A. ufw disable
B. ufw allow 80/tcp
C. ufw delete deny https/tcp
D. ufw allow 4096/tcp

Answer: C

Explanation:
This scenario involves firewall configuration and service accessibility, which falls under the Security domain of the CompTIA Linux+ V8 objectives. The key to resolving this issue is interpreting both the firewall output and the web server status correctly.
The web server output shows that the service is actively listening on TCP port 443, which is the standard port for HTTPS (secure web traffic). The line tcp LISTEN 0 4096 *:443 *:* confirms that the web server is running properly and is ready to accept incoming connections on port 443 from any interface. This indicates that the problem is not with the web server configuration itself.
However, the firewall output clearly shows that incoming connections to port 443 are being blocked. The rules 443/tcp DENY Anywhere and 443/tcp (v6) DENY Anywhere (v6) indicate that the Uncomplicated Firewall (UFW) is explicitly denying HTTPS traffic for both IPv4 and IPv6. As a result, external clients cannot establish a secure connection to the server, even though the service is running correctly.
To resolve this issue securely and correctly, the administrator must remove the firewall rule that denies HTTPS traffic. Option C, ufw delete deny https/tcp, directly removes the blocking rule while preserving the rest of the firewall configuration. This aligns with Linux+ best practices, which emphasize making precise firewall changes rather than disabling security controls entirely.
The other options are incorrect. Option A, ufw disable, would completely turn off the firewall, creating a significant security risk. Option B, ufw allow 80/tcp, only opens HTTP traffic on port 80 and does not resolve HTTPS connectivity issues. Option D, ufw allow 4096/tcp, incorrectly attempts to open an internal socket backlog value rather than a valid service port.
Therefore, the correct and most secure solution is C.

NEW QUESTION 39
A technician wants to temporarily use a Linux virtual machine as a router for the network segment 10.10.204.0/24. Which of the following commands should the technician issue? (Select three).

A. echo "1" > /proc/sys/net/ipv4/ip_forward
B. iptables -A FORWARD -j ACCEPT
C. iptables -A PREROUTING -j ACCEPT
D. iptables -t nat -s 10.10.204.0/24 -p tcp -A PREROUTING -j MASQUERADE
E. echo "0" > /proc/sys/net/ipv4/ip_forward
F. echo "1" > /proc/net/tcp
G. iptables -t nat -s 10.10.204.0/24 -A POSTROUTING -j MASQUERADE

Answer: ABG

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
To temporarily configure a Linux virtual machine as a router, the technician must enable IP forwarding and set up iptables rules to allow and masquerade traffic:
* A. echo"1">/proc/sys/net/ipv4/ip_forward: Enables IPv4 forwarding in the Linux kernel, allowing the VM to forward packets between interfaces.
* B. iptables -A FORWARD -j ACCEPT: Adds a rule to the iptables firewall to accept all forwarded packets (allows traffic to be routed).
* G. iptables -t nat -s 10.10.204.0/24 -A POSTROUTING -j MASQUERADE: Sets up network address translation (NAT) for outgoing packets from the 10.10.204.0/24 subnet, masquerading them as if they are coming from the VM??s external IP.
Other options:
* C.andH.are not relevant for routing/NAT in this context (PREROUTING is generally used for DNAT, not for standard source NAT).
* D.is syntactically incorrect and mixes PREROUTING with MASQUERADE, which is not the proper combination for SNAT.
* E.disables forwarding.
* F.is not related to IP forwarding.
[Reference:, CompTIA Linux+ Study Guide: Exam XK0-006, Sybex, Chapter 9: "Networking", Section: "Configuring Linux as a Router", CompTIA Linux+ XK0-006 Objectives: Domain 2.0 – Networking, Official CompTIA Linux+ Cert Guide, Chapter 12: "Firewall and NAT configuration",]

NEW QUESTION 42
Which of the following is a reason multiple password changes on the same day are not allowed?

A. To avoid brute-forced password attacks by making them too long to perform
B. To increase password complexity and the system's security
C. To stop users from circulating through the password history to return to the originally used password
D. To enforce using multifactor authentication with stronger encryption algorithms instead of passwords

Answer: C

Explanation:
Password policy enforcement is a critical component of system security covered in the CompTIA Linux+ V8 objectives. One common control implemented in Linux systems is restricting how frequently users can change their passwords, often referred to asminimum password ageenforcement.
The primary reason multiple password changes within a short time frame are not allowed is toprevent password cycling attacks. Without this restriction, a user could repeatedly change their password in quick succession to bypass password history controls and eventually reuse a previously compromised or weak password. OptionCaccurately describes this scenario and aligns directly with Linux+ V8 security guidance.
Linux systems enforce this behavior through tools such as chage and PAM (Pluggable Authentication Modules). Administrators can configure minimum password age values to ensure users must wait a defined period before changing passwords again. This ensures that password history requirements are effective and meaningful.
The other options are incorrect. OptionAconfuses password expiration with brute-force mitigation, which is typically addressed through account lockout policies. OptionBrefers to password complexity, which is enforced through character requirements rather than change frequency. OptionDis unrelated, as password expiration policies do not enforce multifactor authentication.
Linux+ V8 documentation emphasizes layered access controls, and preventing password reuse through enforced timing restrictions is a core principle of secure authentication design.
Therefore, the correct answer isC.

NEW QUESTION 46

A Linux administrator needs to securely erase the contents of a hard disk. Which of the following commands is the best for this task?

A. sudo rm -rf /dev/sda1
B. sudo shred /dev/sda1
C. sudo parted rm /dev/sda1
D. sudo dd if=/dev/null of=/dev/sda1

Answer: B

Explanation:
Secure data destruction is an important security requirement addressed in Linux+ V8 objectives. When data must be permanently erased, standard file deletion commands are insufficient because they do not overwrite the data on disk.
The shred command is specifically designed to securely erase files or block devices by overwriting them multiple times with random data. Using sudo shred /dev/sda1 overwrites the entire partition, making data recovery extremely difficult or impossible. This aligns directly with Linux+ V8 best practices for secure data sanitization.
The other options are incorrect. rm -rf removes directory entries but does not overwrite disk data. parted rm deletes partition entries but leaves the underlying data intact. dd if=/dev/null writes zero bytes and does not overwrite existing data blocks.
Linux+ V8 documentation identifies shred as the most appropriate tool for secure erasure when compliance or confidentiality is required. Therefore, the correct answer isB.

NEW QUESTION 50
Which of the following best describes journald?

A. A system service that collects and stores logging data
B. A feature that creates crash dumps in case of kernel failure
C. A service responsible for keeping the filesystem journal
D. A service responsible for writing audit records to a disk

Answer: A

NEW QUESTION 53
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual XK0-006 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the XK0-006 Product From:

https://www.2passeasy.com/dumps/XK0-006/

Money Back Guarantee

XK0-006 Practice Exam Features:

* XK0-006 Questions and Answers Updated Frequently

* XK0-006 Practice Questions Verified by Expert Senior Certified Staff

* XK0-006 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* XK0-006 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year