Download CompTIA 220-1202 Exam Dumps Free

Shared by Ray on 17-06-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A help desk technician recently installed an SSH client on a workstation in order to access remote servers. What does this enable?

Options:

A- To utilize an SSO connection
B- To securely establish a console session
C- To encrypt and decrypt protected messages
D- To facilitate device log reviews

Answer:

B

Explanation:

SSH (Secure Shell) allows encrypted console sessions to access and administer remote servers.

From Quentin Docter -- Complete Study Guide:

''Secure Shell (SSH) provides an encrypted console session to manage Linux, UNIX, or network devices securely over TCP port 22.'' .

Question 2

Question Type: MultipleChoice

A customer wants to format an external hard drive to work on both Windows and macOS. Which of the following filesystems is the best to use?

Options:

A- NTFS
B- exFAT
C- APFS
D- XFS

Answer:

B

Explanation:

The correct answer is B. exFAT, because exFAT (Extended File Allocation Table) is designed to provide cross-platform compatibility between Windows and macOS while supporting large files and large storage devices. When an external hard drive must be readable and writable by both operating systems without additional drivers or configuration, exFAT is the preferred choice.

According to the Quentin Docter -- CompTIA A+ Complete Study Guide, exFAT was developed to overcome the limitations of FAT32, such as file size and volume size restrictions, while maintaining broad operating system support. Both Windows and macOS include native support for exFAT, making it ideal for removable storage devices.

The Travis Everett & Andrew Hutz -- CompTIA A+ All-in-One Exam Guide explains that NTFS is fully supported on Windows but only has limited or read-only support on macOS by default. APFS is Apple's proprietary filesystem and is not natively supported by Windows. XFS is a Linux filesystem and is incompatible with both Windows and macOS without third-party tools.

The Mike Meyers / Mark Soper Lab Manual reinforces that for external drives shared across platforms, exFAT offers the best balance of compatibility, performance, and simplicity.

Therefore, exFAT is the best filesystem choice, making B the correct answer.

Question 3

Question Type: MultipleChoice

A user's computer is running slowly. Web pages take several seconds to open, and applications are slow to respond. A technician opens the Windows Task Manager and sees the following:

Disk: 2%

Network: 12%

GPU: 15%

CPU: 70%

Memory: 97%

Which option best would a technician most likely do to resolve the issue?

Options:

A- Clear browser cached data
B- Upgrade the network connection
C- Close unnecessary programs
D- Delete temporary files

Answer:

C

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

Highmemory usage (97%)suggests the system is overloaded with active processes. The technician should close unneeded applications to free up RAM and improve performance.

FromMike Meyers' Lab Manual:

''When memory usage is near capacity, close all non-essential programs. This can dramatically improve response time without needing hardware upgrades.''

Question 4

Question Type: MultipleChoice

An organization is experiencing an increased number of issues. A technician notices applications that are not installed by default. Users are reporting an increased number of system prompts for software licensing. Which of the following would the security team most likely do to remediate the root cause?

Options:

A- Deploy an internal PKI to filter encrypted web traffic.
B- Remove users from the local admin group.
C- Implement stronger controls to block suspicious websites.
D- Enable stricter UAC settings on Windows.

Answer:

B

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

If unauthorized or non-standard applications are appearing on systems and users are receiving licensing prompts, it's likely users are installing software themselves. Removing users from the local administrators group will prevent them from installing software without approval and reduce the likelihood of introducing unapproved or malicious programs.

A . Deploying a PKI helps with secure communications but doesn't address user software installation rights.

C . Blocking suspicious websites is helpful but doesn't prevent local installations.

D . Stricter UAC may add prompts but can still be bypassed by admin users.

CompTIA A+ 220-1102 Objective 2.2: Compare and contrast access control methods and user privilege settings.

Study Guide Section: Principle of least privilege and managing local admin rights

==========

Question 5

Question Type: MultipleChoice

A help desk team was alerted that a company-owned cell phone has an unrecognized password-cracking application. Which of the following should the help desk team do to prevent further unauthorized installations from occurring?

Options:

A- Configure Group Policy.
B- Implement PAM.
C- Install anti-malware software.
D- Deploy MDM.

Answer:

D

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

Mobile Device Management (MDM) is used to control, monitor, and enforce policies on mobile devices. It allows IT teams to restrict app installations, push approved apps, and monitor device compliance. Deploying MDM would prevent unauthorized applications, such as password crackers, from being installed on company-managed devices.

A . Group Policy is for managing Windows environments and not applicable to smartphones.

B . PAM (Privileged Access Management) controls administrative access, not app installation.

C . Anti-malware can help detect malicious apps but doesn't prevent their installation proactively.

CompTIA A+ 220-1102 Objective 2.2: Compare and contrast common security measures and tools.

Study Guide Section: Mobile Device Management (MDM) capabilities --- app control, security enforcement

Question 6

Question Type: MultipleChoice

Which of the following describes a vulnerability that has been exploited before a patch or remediation is available?

Options:

A- Spoofing
B- Brute-force
C- DoS
D- Zero-day

Answer:

D

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

A Zero-day vulnerability refers to a security flaw in software or hardware that is unknown to the vendor or has not yet been patched. If this vulnerability is exploited before the vendor has issued a fix or patch, it becomes a Zero-day exploit. These attacks are highly dangerous because they take advantage of the absence of defenses due to the lack of awareness or mitigation options.

A . Spoofing is a form of impersonation, not necessarily tied to unpatched vulnerabilities.

B . Brute-force attacks rely on repeatedly guessing credentials and are not related to software flaws.

C . DoS (Denial of Service) attacks are meant to overwhelm systems and don't necessarily exploit unknown vulnerabilities.

CompTIA A+ 220-1102 Objective 2.3: Compare and contrast common social engineering, threats, and vulnerabilities.

Study Guide Section: Threat types --- Zero-day attacks, definitions, and implications

Question 7

Question Type: MultipleChoice

A network technician notices that most of the company's network switches are now end-of-life and need to be upgraded. Which of the following should the technician do first?

Options:

A- Implement the change
B- Approve the change
C- Propose the change
D- Schedule the change

Answer:

C

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

The first step in the IT change management process is to identify and propose the change. In this case, the technician notices a need (end-of-life network switches), so the appropriate action is to formally propose a change. This proposal would be documented and submitted for approval before any planning or implementation occurs.

According to the CompTIA A+ 220-1102 objectives under Operational Procedures (Domain 4.0), the change management process follows these typical steps:

Submit a change request (Propose the change)

Review and approval (Approve the change)

Planning and scheduling (Schedule the change)

Implementation

Documentation and review

Therefore, proposing the change is the correct first step in accordance with standard ITIL-based change management practices.

CompTIA A+ 220-1102 Objective 4.1: Given a scenario, implement best practices associated with documentation and support systems information management.

Study Guide Section: Change Management Process

==========

Question 8

Question Type: MultipleChoice

Company employees do not have assigned workspaces and regularly work at different computers and physical locations. Which option best should the company implement to maintain data security and minimize the amount of user data that needs to be transferred?

Options:

A- Centralized certificate storage
B- Cloud email
C- Portable drives
D- Roaming profiles

Answer:

D

Explanation:

The correct answer is D. Roaming profiles, because roaming profiles allow users to log in to any domain-joined workstation and automatically access their personal settings, documents, and configuration without storing data locally on each machine. This is ideal for environments with hot-desking or shared workstations.

According to the Quentin Docter -- CompTIA A+ Complete Study Guide, roaming profiles store user data centrally on a server rather than on individual computers. When a user logs in, their profile is loaded; when they log out, changes are saved back to the server. This minimizes data duplication and reduces the risk of data being left behind on shared systems.

The Travis Everett & Andrew Hutz -- All-in-One Exam Guide emphasizes that roaming profiles improve security by preventing sensitive user data from being permanently stored on multiple endpoints. This also simplifies backup and recovery, since user data resides in a centralized location.

The Mike Meyers / Mark Soper Lab Manual clarifies that portable drives introduce data loss risks, cloud email only addresses messaging data, and certificate storage does not manage user profiles or documents.

Because the goal is to maintain data security while allowing mobility and minimizing data transfer, roaming profiles are the most appropriate solution, making D the correct answer.