CompTIA

Exam Questions 220-1202

CompTIA A+ Certification Exam: Core 2

NEW QUESTION 1
The screen of a previously working computer repeatedly displays an OS Not Found error message when the computer is started. Only a USB drive, a keyboard, and a mouse are plugged into the computer. Which of the following should a technician do first?

A. Run data recovery tools on the disk
B. Partition the disk using the GPT format
C. Check boot options
D. Switch from UEFI to BIOS

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
An "OS Not Found" error typically indicates that the computer is attempting to boot from a drive that doesn't contain a valid operating system or bootable partition. The presence of a USB drive might be confusing the boot order. Therefore, the first step a technician should take is to verify and adjust the boot sequence in the system??s firmware (BIOS or UEFI). It's possible that the USB drive is being prioritized over the internal hard drive, which may cause the system to miss the OS entirely.
* A. Running data recovery tools is premature before confirming boot order.
* B. Repartitioning the disk would destroy existing data—this should not be done until confirmed the OS is actually missing.
* D. Switching between UEFI and BIOS (legacy mode) might help in rare cases, but it is not the first step in standard OS boot issue troubleshooting.
Reference:
CompTIA A+ 220-1102 Objective 1.7: Troubleshoot common operating system problems. Study Guide Section: Boot process and boot order configuration.
==========

NEW QUESTION 2
A technician uses AI to draft a proposal about the benefits of new software. When reading the draft, the technician notices that the draft contains factually incorrect information. Which of the following best describes this scenario?

A. Data privacy
B. Hallucinations
C. Appropriate use
D. Plagiarism

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
In the context of artificial intelligence, "hallucinations" refer to instances where an AI system generates information that is plausible-sounding but factually incorrect or entirely fabricated. This is a known limitation of large language models, including generative AI tools.
* A. Data privacy refers to the protection of personal or sensitive data, not content accuracy.
* C. Appropriate use relates to ethical and policy-based concerns, not factual correctness.
* D. Plagiarism involves presenting someone else's work as your own — this situation is about accuracy, not ownership.
Reference:
CompTIA A+ 220-1102 Objective 4.4: Identify basic concepts of scripting and automation. Study Guide Section: AI tools and responsible usage — hallucinations and fact-checking outputs
==========

NEW QUESTION 3
A company would like to deploy baseline images to new computers as they are started up on the network. Which of the following boot processes should the company use for this task?

A. ISO
B. Secure
C. USB
D. PXE

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
PXE (Preboot Execution Environment) allows workstations to boot over the network and download an OS image from a server. It is ideal for automating mass deployments using
baseline images across many machines without the need for physical media.
* A. An ISO is a disk image file but requires mounting or physical media.
* B. Secure Boot is a security feature, not a method of deploying OS images.
* C. USB requires manual installation and is not suitable for automated deployment at scale. Reference:
CompTIA A+ 220-1102 Objective 1.4: Given a scenario, use appropriate Microsoft operating system installation methods.
Study Guide Section: Remote installation methods — PXE boot deployment
==========

NEW QUESTION 4
A technician is attempting to join a workstation to a domain but is receiving an error message stating the domain cannot be found. However, the technician is able to ping the server and access the internet. Given the following information:
? IP Address – 192.168.1.210
? Subnet Mask – 255.255.255.0
? Gateway – 192.168.1.1
? DNS1 – 8.8.8.8
? DNS2 – 1.1.1.1

? Server – 192.168.1.10
Which of the following should the technician do to fix the issue?

A. Change the DNS settings.
B. Assign a static IP address.
C. Configure a subnet mask.
D. Update the default gateway.

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The issue described—??domain cannot be found?? despite the ability to ping the server and access the internet—indicates aDNS resolution problem, not a network connectivity issue. The workstation is currently usingpublic DNS servers (8.8.8.8 and 1.1.1.1)which cannot resolve internal domain names, such as the ones used in Active Directory environments. To resolve this, the technician needs tochange the DNS settings to point to the internal DNS server, which in most domain setups is thedomain controller itself (likely 192.168.1.10 in this case).
Here??s the breakdown of the incorrect options:
? B. Assign a static IP address: The IP is already assigned and functioning; the
device can ping and reach the network and internet.
? C. Configure a subnet mask: The subnet mask is appropriate for the network range (Class C /24).
? D. Update the default gateway: The gateway is valid and allows internet access; this is not the issue.
CompTIA A+ 220-1102 Core 2 Objective Reference:
Objective 1.8 – Given a scenario, use features and tools of the operating system. Under this objective, candidates must know how to troubleshoot OS-based network configurations, includingproper DNS settings in domain environments.

NEW QUESTION 5
A company wants to use a single operating system for its workstations and servers and avoid licensing fees. Which of the following operating systems would the company most likely select?

A. Linux
B. Windows
C. macOS
D. Chrome OS

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Linux is an open-source operating system that is freely available and does not require traditional licensing fees. It is highly versatile and scalable, making it suitable for both workstations and servers. Many enterprise environments use Linux to reduce software costs and benefit from robust server features.
* B. Windows requires per-device or per-user licensing for both workstation and server editions.
* C. macOS is proprietary and limited to Apple hardware with licensing restrictions.
* D. Chrome OS is designed for lightweight devices and lacks server functionality. Reference:
CompTIA A+ 220-1102 Objective 1.8 & 1.9: Identify common features and tools of the Linux client/desktop OS.
Study Guide Section: Open-source operating systems and licensing considerations
==========

NEW QUESTION 6
A small office reported a phishing attack that resulted in a malware infection. A technician is investigating the incident and has verified the following:
All endpoints are updated and have the newest EDR signatures.
Logs confirm that the malware was quarantined by EDR on one system. The potentially infected machine was reimaged.
Which of the following actions should the technician take next?

A. Install network security tools to prevent downloading infected files from the internet
B. Discuss the cause of the issue and educate the end user about security hygiene
C. Flash the firmware of the router to ensure the integrity of network traffic
D. Suggest alternate preventative controls that would include more advanced security software

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
After containment and remediation, one of the final steps in incident response is user education. Since the root cause was a phishing attack, it is essential to educate users about identifying phishing attempts, safe browsing practices, and how to handle suspicious communications. This improves overall security posture and helps prevent future incidents.
* A. Installing additional tools may be helpful but is a long-term step.
* C. Flashing router firmware is not warranted unless the network hardware is known to be compromised.
* D. Suggesting more advanced tools might be excessive given that the EDR successfully contained the incident.
Reference:
CompTIA A+ 220-1102 Objective 2.5: Given a scenario, detect, remove, and prevent malware using appropriate tools and methods.
Study Guide Section: Incident response and user education after a security event

NEW QUESTION 7
A technician needs to map a shared drive from a command-line interface. Which of the following commands should the technician use?

A. pathping
B. nslookup
C. net use
D. tracert

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The net use command in Windows is used to map (assign) a shared drive from the command line. The syntax typically looks like: net use X: \server\share where X is the drive letter and \server\share is the network path.
* A. pathping tests network latency and packet loss.
* B. nslookup is used for DNS troubleshooting.
* D. tracert shows the route packets take to reach a destination — not for drive mapping. Reference:
CompTIA A+ 220-1102 Objective 1.7: Given a scenario, troubleshoot common operating system problems.
Study Guide Section: Command-line tools — net use for drive mapping
==========

NEW QUESTION 8
Which of the following prevents forced entry into a building?

A. PIV card
B. Motion-activated lighting
C. Video surveillance
D. Bollard

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
A bollard is a sturdy physical barrier—often a steel or concrete post—designed to prevent
vehicles or unauthorized individuals from ramming into or entering secure areas of a building. It provides physical security and is commonly used outside entrances to prevent forced entry.
* A. PIV (Personal Identity Verification) cards are used for identity access control, not physical blocking.
* B. Motion lighting may deter activity but doesn??t physically prevent entry.
* C. Surveillance records activity but cannot stop a forced entry. Reference:
CompTIA A+ 220-1102 Objective 2.4: Compare and contrast physical security measures. Study Guide Section: Physical security devices — barriers, bollards, and deterrents

NEW QUESTION 9
Which of the following methods involves requesting a user's approval via a push notification to verify the user's identity?

A. Call
B. Authenticator
C. Hardware token
D. SMS

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Authenticator apps (e.g., Microsoft Authenticator, Google Authenticator, Duo) often support push notifications. When the user logs in, the app sends a push to their mobile device, prompting the user to approve or deny the authentication request — a common and user- friendly form of multi-factor authentication (MFA).
* A. Phone call verification is a separate method involving voice-based confirmation.
* C. Hardware tokens generate one-time codes but do not send push notifications.
* D. SMS sends a text message with a code — again, no push mechanism. Reference:
CompTIA A+ 220-1102 Objective 2.2: Compare and contrast multi-factor authentication methods.
Study Guide Section: Authentication apps and push notification verification
==========

NEW QUESTION 10
Which of the following is used in addition to a password to implement MFA?

A. Sending a code to the user's phone
B. Verifying the user's date of birth
C. Prompting the user to solve a simple math problem
D. Requiring the user to enter a PIN

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Multi-Factor Authentication (MFA) requires at least two different types of authentication factors:
? Something you know (e.g., password or PIN)
? Something you have (e.g., smartphone or hardware token)
? Something you are (e.g., fingerprint or facial recognition)
Option A, sending a code to the user??s phone, is an example of "something you have" — a physical device that receives a one-time passcode. Combined with a password, this forms a proper MFA implementation.
* B. Date of birth is another knowledge-based factor (like a password), not a second factor type.
* C. Solving a math problem is not a recognized authentication factor.
* D. A PIN is also "something you know" and does not count as a distinct MFA factor when paired with a password.
Reference:
CompTIA A+ 220-1102 Objective 2.2: Compare and contrast common security measures and authentication technologies.
Study Guide Section: Authentication factors — password, biometrics, tokens, MFA
==========

NEW QUESTION 10
A technician thinks that an application a user downloaded from the internet may not be the legitimate one, even though the name is the same. The technician needs to confirm whether the application is legitimate. Which of the following should the technician do?

A. Compare the hash value from the vendor.
B. Run Task Manager and compare the process ID.
C. Run the application in safe mode.
D. Verify the file name is correct.

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
To ensure the authenticity of a downloaded application, the most reliable method is to verify the file??s hash (e.g., SHA256, MD5) against the value provided by the legitimate
vendor. If the hash values match, the file has not been altered or tampered with. This verification confirms the integrity and authenticity of the executable.
* B. Process IDs are dynamic and not unique to specific software.
* C. Running in safe mode doesn??t validate legitimacy—it only runs the app in a minimal environment.
* D. File names can be spoofed; matching the name does not prove authenticity. Reference:
CompTIA A+ 220-1102 Objective 2.2: Compare and contrast authentication and software integrity verification methods.
Study Guide Section: Hash verification for software authenticity and digital integrity

NEW QUESTION 15
A technician is using a credential manager to safeguard a large number of credentials. Which of the following is important for using this application?

A. Restricted log-in times
B. Secure master password
C. TPM module
D. Windows lock screen

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Credential managers or password vaults (e.g., Windows Credential Manager, KeePass, or LastPass) store passwords securely. The integrity of such tools heavily depends on the strength of the master password protecting the vault. If compromised, all saved credentials could be exposed. Therefore, setting a secure master password is crucial.
* A. Login time restrictions are general user account settings, not specific to credential managers.
* C. TPM is used more commonly for full disk encryption, not specifically required for password managers.
* D. The lock screen protects general access but does not protect stored credentials alone. Reference:
CompTIA A+ 220-1102 Objective 2.2: Compare and contrast authentication technologies and secure credential storage.
Study Guide Section: Password management and protection best practices
==========

NEW QUESTION 20
A technician installs VPN client software that has a software bug from the vendor. After the vendor releases an update to the software, the technician attempts to reinstall the software but keeps getting an error message that the network adapter for the VPN already exists. Which of the following should the technician do next to mitigate this issue?

A. Run the latest OS security updates.
B. Map the network adapter to the new software.
C. Update the network adapter's firmware.
D. Delete hidden network adapters.

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
VPN clients often create virtual network adapters. If the software wasn't uninstalled properly or crashed during install, leftover (often hidden) virtual adapters can prevent reinstallation. The proper solution is to delete hidden network adapters using Device Manager (with ??Show hidden devices?? enabled).
* A. OS updates won??t fix a leftover driver or adapter issue.
* B. Mapping an adapter to the software is not a standard or viable solution.
* C. Firmware updates apply to physical adapters, not virtual VPN adapters. Reference:
CompTIA A+ 220-1102 Objective 3.1: Troubleshoot common Windows OS and network issues.
Study Guide Section: Troubleshooting network adapter conflicts and VPN client errors

NEW QUESTION 25
A user is attempting to open on a mobile phone a HD video that is hosted on a popular media streaming website. The user is receiving connection timeout errors. The mobile reception icon area is showing two bars next to 3G. Which of the following is the most likely cause of the issue?

A. The user does not have Wi-Fi enabled.
B. The website's subscription has run out.
C. The bandwidth is not fast enough.
D. The mobile device storage is full.

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:

3G networks generally do not provide the bandwidth required for seamless HD video streaming. With only two signal bars and a 3G connection, the mobile device likely cannot maintain the necessary data throughput, resulting in timeouts or buffering failures. This is a classic symptom of insufficient network speed or signal strength.
* A. Lack of Wi-Fi may contribute, but the root cause is the low mobile bandwidth, not the Wi- Fi state.
* B. A website subscription lapse would return an account error, not a timeout.
* D. Full device storage can affect downloads but not streaming from the internet. Reference:
CompTIA A+ 220-1102 Objective 3.3: Troubleshoot mobile OS and application issues. Study Guide Section: Connectivity and network performance issues on mobile devices
==========

NEW QUESTION 30
Which of the following is found in an MSDS sheet for a battery backup?

A. Installation instructions
B. Emergency procedures
C. Configuration steps
D. Voltage specifications

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
An MSDS (Material Safety Data Sheet), now commonly referred to as SDS (Safety Data Sheet), is a document that provides detailed information on the properties of a particular substance. It includes safety guidelines and emergency procedures related to handling, exposure, fire hazards, and first aid—not installation or configuration instructions.
For a battery backup (UPS device), the MSDS would include emergency procedures such as what to do in case of a chemical spill, exposure to battery acid, or fire hazard due to overheating or chemical leakage. This ensures the safety of personnel and complies with hazardous materials handling regulations.
Reference:
CompTIA A+ 220-1102 Objective 4.1: Given a scenario, implement best practices associated with documentation and support systems information management.
Study Guide Section: MSDS/SDS usage and safety documentation

NEW QUESTION 35
Which of the following is used to apply corporate restrictions on an Apple device?

A. App Store
B. VPN configuration
C. Apple ID
D. Management profile

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
A management profile is used to enforce corporate policies on Apple devices. These profiles are installed via an MDM (Mobile Device Management) solution and control access, restrictions,Wi-Fi settings, app installations, and more. They??re critical for managing devices in a business environment.
* A. The App Store allows software downloads but doesn??t control policies.
* B. VPN configuration is used for secure remote connections, not enforcement of restrictions.
* C. Apple ID is for personal account access to Apple services, not corporate device management.
Reference:
CompTIA A+ 220-1102 Objective 2.2: Compare and contrast security tools and MDM features.
Study Guide Section: Mobile device management and configuration profiles (Apple/iOS)
==========

NEW QUESTION 36
Which of the following file types would a desktop support technician most likely use to automate tasks for a Windows user log-in?

A. .bat
B. .sh
C. .py
D. .js

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
* A .bat file (batch file) is a script file in DOS, OS/2, and Microsoft Windows. It contains a series of commands that are executed by the command-line interpreter. In Windows environments, batch files are commonly used to automate log-in tasks, such as mapping network drives, launching applications, or setting environment variables during the user's logon process.
* B. .sh is a shell script used in Linux/Unix environments.
* C. .py is a Python script, which can be used for automation but is not commonly run directly at user logon in standard Windows environments.
* D. .js is JavaScript, used mainly in web development and not for system-level scripting in Windows logon automation.
Reference:
CompTIA A+ 220-1102 Objective 1.3: Use appropriate Microsoft operating system features and tools.
Study Guide Section: Scripting basics and file types for automation — .bat for Windows
==========

NEW QUESTION 39
A customer is unable to open some files on their system. Each time the customer attempts to open a file, the customer receives a message that the file is encrypted. Which of the following best describes this issue?

A. Keylogger
B. Ransomware
C. Phishing
D. Cryptominer

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Ransomware is a type of malware that encrypts the user's files and demands a payment (ransom) for the decryption key. When a user receives a message stating that their files are encrypted and cannot be accessed, ransomware is the most likely cause. The attacker??s goal is to hold the data hostage until the victim pays to restore access.
* A. Keylogger records keystrokes and doesn??t encrypt files.
* C. Phishing is a social engineering tactic to gather credentials, not to encrypt data.
* D. Cryptominer uses system resources to mine cryptocurrency, not encrypt files. Reference:
CompTIA A+ 220-1102 Objective 2.3: Compare and contrast common types of malware and threats.
Study Guide Section: Ransomware behavior and user impact
==========

NEW QUESTION 42
A company recently transitioned to a cloud-based productivity suite and wants to secure the environment from external threat actors. Which of the following is the most effective method?

A. Multifactor authentication
B. Encryption
C. Backups
D. Strong passwords

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Multifactor authentication (MFA) is considered one of the most effective security measures for cloud environments. It requires users to verify their identity using two or more factors (e.g., password + phone app code), making it significantly harder for external attackers to gain access, even if the primary password is compromised.
* B. Encryption is important for data protection but doesn??t prevent unauthorized logins.
* C. Backups protect against data loss but don??t stop breaches.
* D. Strong passwords are helpful but can still be phished or cracked — MFA adds a critical
extra layer. Reference:
CompTIA A+ 220-1102 Objective 2.2: Compare and contrast authentication technologies. Study Guide Section: Cloud security best practices — MFA and access control

NEW QUESTION 45
A company executive is currently attending a major music festival with a large number of attendees and is having trouble accessing a work email account. The email application is not downloading emails and also appears to become stuck during connection attempts. Which of the following is most likely causing the disruption?

A. The phone has no storage space available.
B. Company firewalls are configured to block remote access to email resources.
C. Too many devices in the same area are trying to connect to the mobile network.
D. The festival organizer prohibits internet usage during the event and has blocked the internet signal

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
At large events such as music festivals, cellular towers may become congested due to the high volume of users attempting to connect simultaneously. This congestion causes slow or failed data connections, which explains the email application being unable to sync or connect. This is a common real-world mobile connectivity issue in crowded areas.
* A. Lack of storage would prevent saving attachments, not prevent connection attempts.
* B. Company firewalls usually don??t affect mobile access unless specific device restrictions are enforced.
* D. Organizers do not have the ability to block the internet signal; only carriers manage mobile bandwidth.
Reference:
CompTIA A+ 220-1102 Objective 3.3: Troubleshoot mobile OS and connectivity issues. Study Guide Section: Mobile network limitations — signal congestion and bandwidth issues
==========

NEW QUESTION 47
A technician notices that the weekly backup is taking too long to complete. The daily backups are incremental. Which of the following would most likely resolve the issue?

A. Changing the backup window
B. Performing incremental weekly backups
C. Increasing the backup storage
D. Running synthetic full weekly backups

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:

A synthetic full backup combines the last full backup with subsequent incremental backups to create a new full backup without re-reading data from the source system. This method significantly reduces the backup window and network impact. It is especially useful when traditional full backups are too time-consuming.
* A. Changing the backup window only shifts timing, not duration.
* B. Incremental weekly backups would lack a proper full recovery point and aren't ideal alone.
* C. Storage space isn't the bottleneck in backup speed—it??s read/write operations and network load.
Reference:
CompTIA A+ 220-1102 Objective 4.2: Summarize backup and recovery concepts.
Study Guide Section: Backup types — full, incremental, differential, and synthetic backups
==========

NEW QUESTION 52
Which of the following is the quickest way to move from Windows 10 to Windows 11 without losing data?

A. Using gpupdate
B. Image deployment
C. Clean install
D. In-place upgrade

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
An in-place upgrade is the fastest and most efficient way to upgrade from Windows 10 to Windows 11 while keeping all user data, applications, and settings intact. This method is often used when the hardware meets Windows 11 requirements and no system reconfiguration is necessary.
* A. gpupdate is used to refresh Group Policy settings — unrelated to OS upgrades.
* B. Image deployment typically replaces the current OS and may not retain user data unless specifically customized.
* C. A clean install requires formatting the drive and starting fresh, which removes all data. Reference:
CompTIA A+ 220-1102 Objective 1.4: Given a scenario, use appropriate Microsoft operating system installation methods.
Study Guide Section: In-place upgrade vs. clean install methods
==========

NEW QUESTION 55
Users are reporting that an unsecured network is broadcasting with the same name as the
normal wireless network. They are able to access the internet but cannot connect to the file share servers. Which of the following best describes this issue?

A. Unreachable DNS server
B. Virtual local area network misconfiguration
C. Incorrect IP address
D. Rogue wireless access point

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
This scenario describes a rogue access point — a malicious or unauthorized wireless access point that uses the same SSID as the legitimate network. Users may connect to it unknowingly, which can result in limited network access, data interception, or redirection of traffic. The inability to reach internal file servers supports this being an unauthorized AP with no connection to internal resources.
* A. A DNS issue would impact name resolution, not connectivity to file servers directly.
* B. VLAN issues generally affect segmentation, not mimic SSID problems.
* C. An incorrect IP address could cause connectivity issues, but not in the presence of a malicious AP broadcasting the same SSID.
Reference:
CompTIA A+ 220-1102 Objective 2.4: Compare and contrast wireless and physical security threats.
Study Guide Section: Rogue access points and their detection
==========

NEW QUESTION 60
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?

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 toformally 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.
Reference:
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
==========

NEW QUESTION 62
Which of the following is the best reason for a network engineering team to provide a help desk technician with IP addressing information to use on workstations being deployed in a secure network segment?

A. Only specific DNS servers are allowed outbound access.
B. The network allow list is set to a specific address.
C. DHCP services are not enabled for this subnet.
D. NAC servers only allow for security updates to be installed.

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
In secure or isolated network segments, DHCP may be disabled to reduce the risk of unauthorized device connections or to maintain strict IP assignment control. In such cases, the help desk technician must manually configure IP settings (including IP address, subnet mask, gateway, and DNS servers). This ensures the workstation communicates properly within that segment.
* A. DNS server restriction is unrelated to manual IP configuration.
* B. Allow lists refer to traffic access, but manual IP assignment is due to lack of DHCP, not allow lists.
* D. NAC servers control access but don't replace the need for IP addressing. Reference:
CompTIA A+ 220-1102 Objective 1.7: Given a scenario, troubleshoot common operating system and network issues.
Study Guide Section: IP configuration and DHCP-related deployment scenarios
==========

NEW QUESTION 65
A computer technician is implementing a solution to support a new internet browsing policy for a customer's business. The policy prohibits users from accessing unauthorized websites based on categorization. Which of the following should the technician configure on the SOHO router?

A. Secure management access
B. Group Policy Editor
C. Content filtering
D. Firewall

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Content filtering allows administrators to block or allow access to websites based on categories (e.g., social media, adult content, streaming). On a SOHO (Small Office/Home Office) router, this is often built-in or available via DNS-level filtering, and is the most appropriate method for enforcing browsing policies without needing to touch each individual device.
* A. Secure management access protects router admin interfaces but doesn??t control user browsing.
* B. Group Policy Editor is a Windows tool, not used on routers.
* D. A firewall can block specific IPs or ports, but it doesn't categorize web content. Reference:
CompTIA A+ 220-1102 Objective 2.2: Compare and contrast security measures and tools. Study Guide Section: SOHO router security features — content filtering, parental controls

NEW QUESTION 70
A technician is preparing to replace the batteries in a rack-mounted UPS system. After ensuring the power is turned off and the batteries are fully discharged, the technician needs to remove the battery modules from the bottom of the rack. Which of the following steps should the technician take?

A. Ensure the fire suppression system is ready to be activated.
B. Use appropriate lifting techniques and guidelines.
C. Place the removed batteries in an antistatic bag.
D. Wear a face mask to filter out any harmful fumes.

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
UPS batteries are heavy and often located at the bottom of racks to maintain balance. Safe removal requires the use of correct lifting techniques to avoid injury. OSHA and workplace safety standards emphasize ergonomic handling when dealing with heavy equipment.
* A. Fire suppression readiness is important for fire safety but not specifically relevant to battery removal.
* C. Antistatic bags are for electronic components, not heavy battery modules.
* D. A face mask is not generally necessary unless there is a chemical leak, which is not indicated here.
Reference:
CompTIA A+ 220-1102 Objective 4.3: Explain common safety and environmental impacts
and procedures.
Study Guide Section: Safe handling procedures — lifting techniques, battery handling
==========

NEW QUESTION 71
Which of the following types of social engineering attacks sends an unsolicited text message to a user's mobile device?

A. Impersonation
B. Vishing
C. Spear phishing

D. Smishing

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Smishing (SMS phishing) is a type of social engineering attack where attackers send fraudulent text messages to trick users into revealing sensitive information or downloading malware. These messages often impersonate banks, delivery services, or official institutions to lure the victim into clicking malicious links.
* A. Impersonation is an in-person or voice-based tactic.
* B. Vishing refers to voice phishing over phone calls.
* C. Spear phishing is a targeted email-based phishing method. Reference:
CompTIA A+ 220-1102 Objective 2.3: Compare and contrast social engineering techniques.
Study Guide Section: Smishing as a type of phishing via SMS or mobile messaging.
==========

NEW QUESTION 73
A help desk technician needs to remove RAM from retired workstations and upgrade other workstations that have applications that use more memory with this RAM. Which of the following actions would the technician most likely take?

A. Demagnetize memory for security.
B. Use antistatic bags for storage and transport.
C. Plug in the power supply to ground each workstation.
D. Install memory in identical pairs.

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
RAM is an electrostatic-sensitive component. When removing or transporting RAM modules, they should be stored in antistatic bags to protect against electrostatic discharge (ESD), which can damage the memory. This is a standard best practice in hardware handling.
* A. Demagnetization is not applicable to RAM.
* C. Plugging in power to ground is not safe or recommended for static protection.
* D. Installing identical memory pairs is applicable for dual-channel configuration, but not directly related to transporting or handling RAM.
Reference:
CompTIA A+ 220-1102 Objective 4.3: Explain environmental impacts and procedures. Study Guide Section: ESD safety practices and component handling procedures
—

NEW QUESTION 77
A technician is assigned to offboard a user. Which of the following are common tasks on an offboarding checklist? (Choose two.)

A. Quarantine the hard drive in the user's laptop.
B. Deactivate the user's key fobs for door access.
C. Purge all PII associated with the user.
D. Suspend the user's email account.
E. Turn off the network ports underneath the user's desk.
F. Add the MAC address of the user's computer to a blocklist.

Answer: BD

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
User offboarding involves disabling the departing user's access to company systems and facilities. Two key tasks typically include:
? Deactivating physical access credentials (e.g., key fobs or badges) to prevent unauthorized entry (B).
? Suspending or disabling the user??s email account to prevent future use and to retain business communications (D).
* A. Quarantining a hard drive is not standard unless malware or legal issues are involved.
* C. Purging PII must follow legal retention policies; it's not typically an immediate offboarding task.
* E. Disabling network ports may be relevant in some cases but is not a standard offboarding step.
* F. Blocking MAC addresses is not typical unless the device is considered a security threat. Reference:
CompTIA A+ 220-1102 Objective 4.1: Given a scenario, implement proper documentation and offboarding procedures.
Study Guide Section: User lifecycle management — onboarding and offboarding tasks
==========

NEW QUESTION 78
A technician needs to provide remote support for a legacy Linux-based operating system from their Windows laptop. The solution needs to allow the technician to see what the user is doing and provide the ability to interact with the user's session. Which of the following remote access technologies would support the use case?

A. VPN
B. VNC
C. SSH
D. RDP

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The correct answer isVNC (Virtual Network Computing). VNC is a graphical desktop- sharing system that uses the Remote Frame Buffer protocol (RFB) to remotely control another computer. It is platform-independent and widely supported on Linux, which makes it ideal for providinginteractive remote support for a

Linux-based operating system. It allows the technician not only to view the remote desktop session but also tocontrol it, fulfilling the need to see and interact with the user??s session.
? A. VPN(Virtual Private Network) creates a secure tunnel to a network but doesnot
provide desktop sharing or session controlby itself.
? C. SSH(Secure Shell) provides secure command-line access to Unix/Linux systems but does not offergraphical desktop interaction, which is a requirement in this case.
? D. RDP(Remote Desktop Protocol) is primarily a Microsoft protocol, and although it can be made to work on Linux, it isnot natively supported on legacy Linux systems, and thusless suitablethan VNC in this scenario.
CompTIA A+ 220-1102 Core 2 Objective Reference:
Objective 1.8 – Given a scenario, use features and tools of the operating system. Under this objective, candidates are expected to be familiar with remote access technologies, includingRDP, SSH, and VNC, and understand their appropriate uses and limitations on different platforms such as Windows and Linux.

NEW QUESTION 81
A support specialist needs to decide whether to install a 32-bit or 64-bit OS architecture on a new computer. Which of the following specifications will help the specialist determine which OS architecture to use?

A. 16GB RAM
B. Intel i7 CPU
C. 500GB HDD
D. 1Gbps Ethernet

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The amount of installed RAM is the key factor in determining whether a 64-bit OS is needed. A 32-bit operating system cannot effectively address more than 4GB of RAM. Since this system has 16GB of RAM, a 64-bit OS is required to utilize the full memory.
* B. An Intel i7 CPU supports both 32-bit and 64-bit OS installations, so it alone doesn??t determine the need.
* C. HDD size does not influence OS architecture selection.
* D. Ethernet speed is a network consideration and not related to OS architecture. Reference:
CompTIA A+ 220-1102 Objective 1.4: Given a scenario, choose the appropriate Microsoft OS installation methods and configurations.
Study Guide Section: 32-bit vs. 64-bit system requirements and memory limitations
==========

NEW QUESTION 84
A customer wants to be able to work from home but does not want to be responsible for bringingcompany equipment back and forth. Which of the following would allow the user to remotely access and use a Windows PC at the main office? (Choose two.)

A. SPICE
B. SSH
C. RDP
D. VPN
E. RMM
F. WinRM

Answer: CD

Explanation:
Comprehensive and Detailed Explanation From Exact Extract: To work remotely without physically transporting a workstation, the user needs:
? C. RDP (Remote Desktop Protocol): Allows graphical remote access to a Windows
PC at the office.
? D. VPN (Virtual Private Network): Establishes a secure tunnel to access the corporate network remotely, making the internal PC reachable.
* A. SPICE is used in virtual machine environments and is not typically used for end-user remote desktop access.
* B. SSH is a text-based remote access tool used mostly for Linux systems.
* E. RMM (Remote Monitoring and Management) is used by IT administrators for support — not end-user remote access.
* F. WinRM is used for Windows remote management via PowerShell, not for full desktop access.
Reference:
CompTIA A+ 220-1102 Objectives 2.2 & 4.4: Compare and contrast security tools and remote access methods.
Study Guide Section: Remote access tools — RDP and VPN for secure remote work

NEW QUESTION 89
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

220-1202 Practice Exam Features:

* 220-1202 Questions and Answers Updated Frequently

* 220-1202 Practice Questions Verified by Expert Senior Certified Staff

* 220-1202 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 220-1202 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year