ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

Question: 1

SIMULATION

You are configuring a home network for a customer. The customer has requested the ability to access a Windows PC remotely, and needs all chat and optional functions to work in their game console.

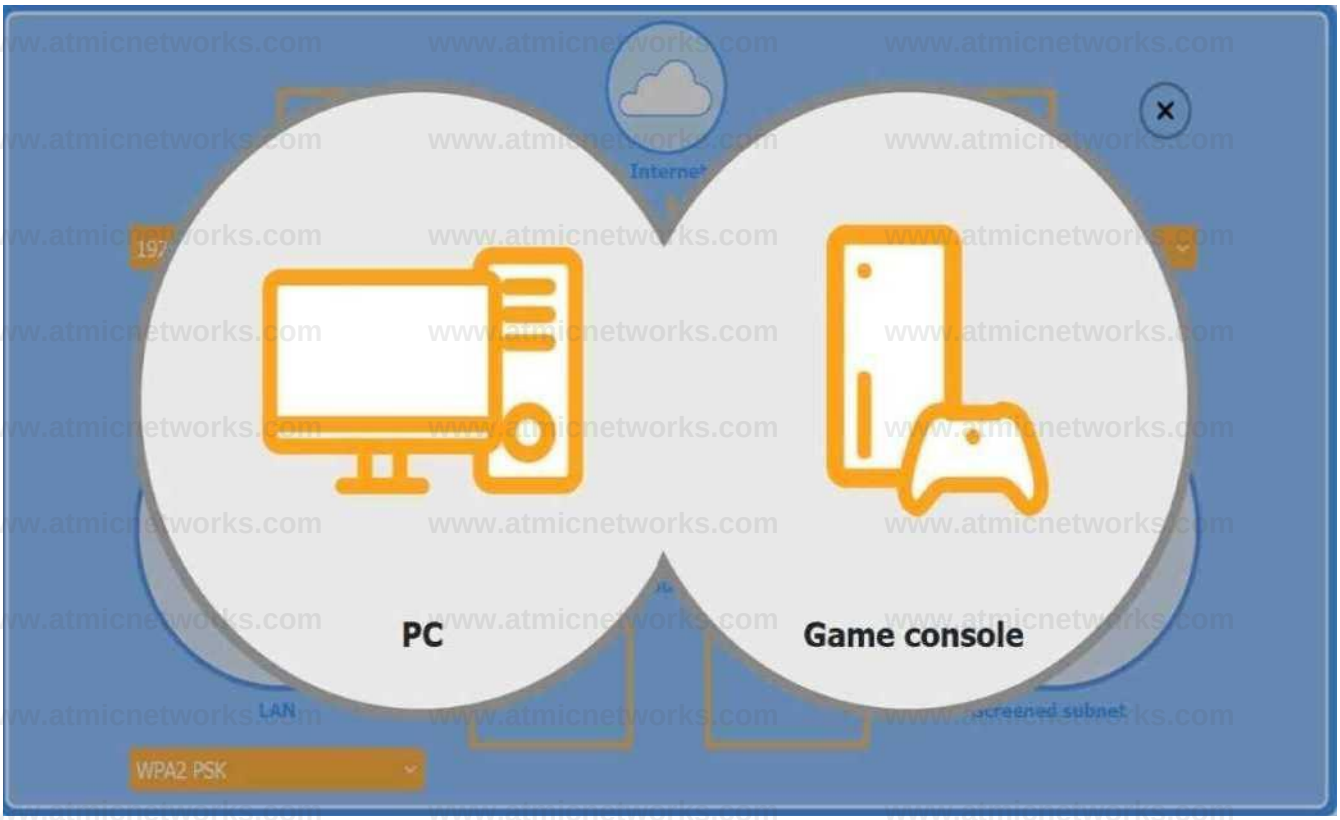
INSTRUCTIONS

Use the drop-down menus to complete the network configuration for the customer. Each option may only be used once, and not all options will be used.

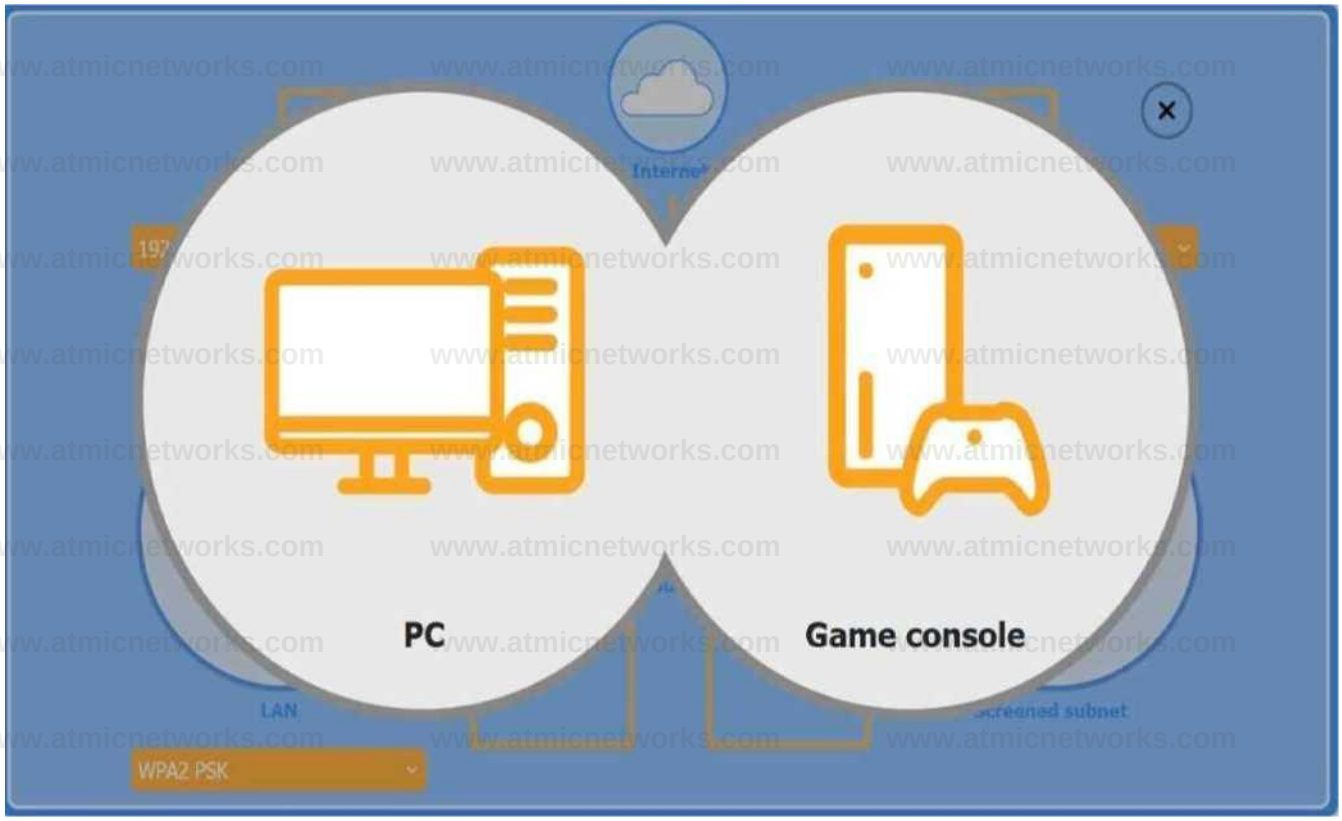
Then, click the + sign to place each device in its appropriate location.

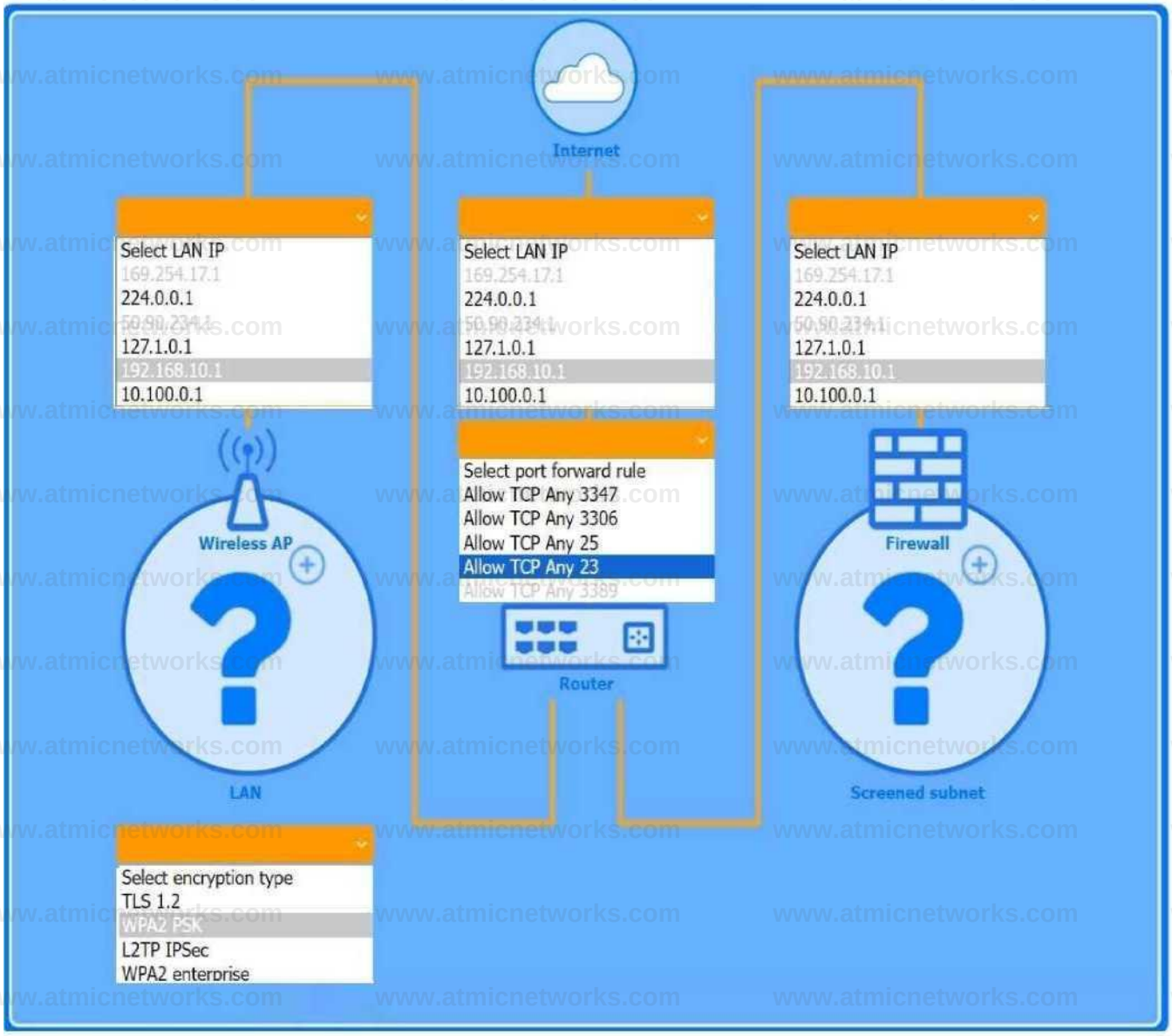
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Wireless AP LAN



Firewall Screened Subnet





Answer: See explanation below.

Explanation:

The completed configuration:

1. Wireless AP (LAN side)
2. LAN IP: 192.168.10.1
3. Encryption: WPA2 PSK
4. Router (port-forward rule)

1. Allow TCP Any 3389

This forwards inbound RDP traffic (TCP/3389) from the Internet to the Windows PC, enabling Remote Desktop access.

5. Firewall (screened subnet side)

1. LAN IP: 10.100.0.1

6. Device placement

1. PC: place behind the router (where the port-forward rule points).
2. Game console: place on the Wireless AP (so it can use chat and extra services over WPA2 PSK).
3. Firewall: place in front of the screened subnet (with its 10.100.0.1 IP facing that subnet).

The Windows PC is placed in the screened subnet (behind the firewall) for enhanced security. Remote access to this PC requires port forwarding of TCP port 3389 (RDP), which is correctly configured through the router.
The Game Console is placed on the Wireless AP LAN, using WPA2 PSK for a secure wireless connection.
Game consoles typically use peer-to-peer chat and online services that require open access without firewall restrictions, which is why the console is not placed behind the firewall. CompTIA A+ 220-1102 Reference Points:
Objective 3.4: Given a scenario, implement best practices associated with data and device security.
Objective 2.4: Given a scenario, use appropriate tools to support and configure network settings. Study Guide Reference:
CompTIA A+ Core 2 guides recommend using screened subnets (a type of DMZ) for systems needing controlled external access, such as remote desktops, while placing gaming and media devices on less restricted networks for full functionality.

Question: 2

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.

Question: 3

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)whichcannot 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.

Question: 4

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 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.

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

Question: 5

MFA for a custom web application on a user's smartphone is no longer working. The last time the user remembered it working was before taking a vacation to another country. Which of the following should the technician do first?

A. Verify the date and time settings
B. Apply mobile OS patches
C. Uninstall and reinstall the application
D. Escalate to the website developer

Answer: A

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
Multi-Factor Authentication (MFA) apps, especially time-based one-time password (TOTP) apps (e.g., Google Authenticator, Authy), rely on accurate time synchronization between the device and the authentication server. If the user recently traveled internationally, the device may have incorrect date/time settings due to time zone changes or failed synchronization, leading to MFA failure.
The most logical and non-intrusive first step is to verify and correct the date and time settings. This aligns with basic troubleshooting principles—start with the simplest and most likely cause before taking more drastic action.

Reference:
CompTIA A+ 220-1102 Objective 2.6: Given a scenario, apply cybersecurity best practices to secure a workstation.
Study Guide Section: Authentication technologies and MFA troubleshooting

Question: 6

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

Question: 7

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.

Question: 8

A security administrator teaches all of an organization's staff members to use BitLocker To Go. Which of the following best describes the reason for this training?

A. To ensure that all removable media is password protected in case of loss or theft
B. To enable Secure Boot and a BIOS-level password to prevent configuration changes
C. To enforce VPN connectivity to be encrypted by hardware modules
D. To configure all laptops to use the TPM as an encryption factor for hard drives

Answer: A

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

BitLocker To Go is a Microsoft encryption feature specifically designed for removable drives such as USB flash drives and external hard drives. It allows users to protect the data on these devices by requiring a password to decrypt the contents, thereby preventing unauthorized access in the event the device is lost or stolen.

A is correct because BitLocker To Go is directly tied to password-protecting removable media.

B and C are unrelated to BitLocker To Go; Secure Boot and VPN encryption are entirely different security layers.

D applies to BitLocker (not BitLocker To Go) and full disk encryption on internal drives using TPM. Reference:

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

Study Guide Section: Encryption technologies (BitLocker, BitLocker To Go)

Question: 9

Which of the following is used to detect and record access to restricted areas?

A. Bollards
B. Video surveillance
C. Badge readers
D. Fence

Answer: C

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

Badge readers are electronic access control systems that require authorized users to scan a badge (e.g., RFID or magnetic strip cards) to gain access to restricted physical locations. These systems typically log all access attempts—successful or denied—providing both detection and recording of access events.

A . Bollards are physical barriers to prevent vehicle access.

B . Video surveillance can record access visually but does not track identity unless integrated with access control systems.

D . A fence restricts access but doesn't detect or record who entered.

Reference:

CompTIA A+ 220-1102 Objective 2.4: Compare and contrast physical security measures.

Study Guide Section: Physical access controls (e.g., badge readers, mantraps)

Question: 10

An administrator received an email stating that the OS they are currently supporting will no longer be issued security updates and patches. Which of the following is most likely the reason the administrator received this message?

A. Support from the computer's manufacturer is expiring
B. The OS will be considered end of life
C. The built-in security software is being removed from the next OS version
D. A new version of the OS will be released soon

Answer: B

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

Operating systems periodically reach a status known as "end of life" (EOL), at which point the developer (e.g., Microsoft, Apple) ceases to provide security updates, patches, or technical support. When this happens, the OS becomes vulnerable and non-compliant with security best practices, which is why organizations typically receive advance notifications from

vendors or support teams. A . Manufacturer support expiration only applies to hardware, not OS patching.
C . Security software may be upgraded or removed, but that does not affect patching the OS itself. D . The release of a new version doesn't automatically stop updates for the current version.

Reference:

CompTIA A+ 220-1102 Objective 1.3: Given a scenario, use appropriate Microsoft operating system features and tools.
Study Guide Section: OS lifecycle management and vendor support phases (e.g., EOL)

Question: 11

Which of the following is the best way to distribute custom images to 800 devices that include four device vendor classes with two types of user groups?

A. Use xcopy to clone the hard drives from one to another
B. Use robocopy to move the files to each device
C. Use a local image deployment tool for each device
D. Use a network-based remote installation tool

Answer: D

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
In enterprise environments, network-based deployment solutions (such as Windows Deployment Services or SCCM) allow administrators to push images across the network to hundreds of devices efficiently. These tools support hardware-specific drivers (for different vendor classes) and can

accommodate user-group configurations using task sequences or answer files.
A and B (xcopy and robocopy) are file-level tools and not designed for full OS image deployment.
C . Using local tools per device is inefficient for large-scale rollouts (800 devices).
D . Network-based deployment is the industry standard for this scale.

Reference:

CompTIA A+ 220-1102 Objective 1.4: Given a scenario, use appropriate Microsoft operating system installation methods.
Study Guide Section: Deployment methods (including PXE boot, image deployment)

Question: 12

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.

Question: 13

A user reports some single sign-on errors to a help desk technician. Currently, the user is able to sign in to the company's application portal but cannot access a specific SaaS-based tool. Which of the following would the technician most likely suggest as a next step?

A. Reenroll the user's mobile device to be used as an MFA token
B. Use a private browsing window to avoid local session conflicts
C. Bypass single sign-on by directly authenticating to the application
D. Reset the device being used to factory defaults

Answer: B

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
SSO issues are often related to cached session data, cookies, or browser artifacts. The fact that the user can access the company portal but not one specific SaaS tool suggests a session or token problem. Using a private/incognito browsing window allows a clean session to be initiated, which often resolves SSO conflicts.
A . Reenrolling MFA is not related unless access issues stem from failed multifactor authentication. C . Bypassing SSO may not be possible depending on the SaaS tool and company policies.
D . Factory resetting a device is a last resort and unnecessary in this case.
Reference:
CompTIA A+ 220-1102 Objective 3.3: Troubleshoot common software, application, and OS security issues.
Study Guide Section: Troubleshooting login and authentication issues, especially with SSO services.

Question: 14

A technician verifies that a malware incident occurred on some computers in a small office. Which of the following

should the technician do next?

A. Quarantine the infected systems
B. Educate the end users
C. Disable System Restore
D. Update the anti-malware and scan the computers

Answer: A

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

Once a malware incident has been confirmed, the immediate next step is to contain the threat. Quarantining infected systems prevents the malware from spreading to other devices and isolates the malicious code for further analysis or remediation.

B . Educating end users is important but occurs later in the incident response process.

C . Disabling System Restore is part of cleanup, not containment.

D . Updating and scanning should occur after the system is quarantined to prevent further infection or spread.

Reference:

CompTIA A+ 220-1102 Objective 2.5: Given a scenario, detect, remove, and prevent malware using appropriate tools and methods.

Study Guide Section: Malware removal best practices — Step 2: Quarantine the infected system

Question: 15

Which of the following is a Linux command that is used for administrative purposes?

A. runas
B. cmcl
C. net user
D. su

Answer: D

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

The su (substitute user) command is used in Linux to switch to another user account, most commonly to escalate privileges by switching to the root (administrator) account. It allows administrative tasks to be performed in a terminal session.

A . runas is a Windows command for executing a program under another user's context.

B . cmcl is not a valid Linux or administrative command.

C . net user is a Windows command for managing local user accounts.

Reference:

CompTIA A+ 220-1102 Objective 1.9: Identify common features and tools of the Linux client/desktop OS.
Study Guide Section: Linux command-line tools — su, sudo

Question: 16

A user recently installed an application that accesses a database from a local server. When launching the application, it does not populate any information. Which of the following command-line tools is the best to troubleshoot the issue?

A. ipconfig
B. nslookup
C. netstat
D. curl

Answer: D

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

The scenario involves an application that should retrieve data from a local database server but is failing to do so. This likely indicates a problem in communication between the application and the database server (such as a network issue, port misconfiguration, or service unavailability). The correct troubleshooting approach involves testing the network/service connectivity between the client and the database.

Let's examine the options:

A . ipconfig:This command displays IP configuration details for Windows systems, such as IP address, subnet mask, and default gateway. While useful for diagnosing general network issues, it does not test service connectivity or the availability of a specific application port/service.

B . nslookup:Used to query DNS servers to resolve domain names to IP addresses. However, since the question references a local server (likely accessed via IP or static hostname), DNS is probably not involved. Also, it does not test application/service availability.

C . netstat:Displays active TCP connections, listening ports, and routing tables. It helps determine whether the local system is listening for or maintaining any network connections, but it does not initiate a connection to test availability. It's diagnostic but not interactive for service testing.

D . curl:This is the most appropriate tool for this scenario. curl is used to test connectivity to services over protocols like HTTP, HTTPS, FTP, and more. If the application retrieves data via a web interface or API (common in database-driven applications), curl can be used to test if the application can successfully reach and retrieve data from the server. It provides immediate, testable feedback on whether the server and service are available and responsive.

Example usage:

curlhttp://localhost:8080/api/data

This command would test whether a local server's application programming interface (API) is available and responding on port 8080.

CompTIA A+ 220-1102 Reference Points:

Objective 2.4: Given a scenario, use appropriate tools to troubleshoot and support Windows OS issues.
Objective 3.3: Use appropriate tools to troubleshoot and resolve issues.

The CompTIA A+ Core 2 study guide references curl as a useful command-line utility for testing connectivity and troubleshooting application access to services.

Question: 17

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

Question: 18

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

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.

Reference:

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: 19

SIMULATION

You have been contacted through the help desk chat application. A user is setting up a replacement SOHO router. Assist the user with setting up the router.

INSTRUCTIONS

Select the most appropriate statement for each response. Click the send button after each response to continue the chat.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

To: Customer

I just received a new router for the office, and 1 need help setting it up.

Select reply
I am happy to assist you today.
Have you tried using the FAQ?

Select reply

Send

To: Customer

I just received a new router for the office, and 1 need help setting it up.

Answer 1

I need to set up my basic security settings.

Is this the first router in your office?

No, it is a replacement. The last router broke.

The first thing you need to do Is change the default password

Select reply
Type the password printed on the label on the b
Use Summer21 as the administrative password
Create a new password with an uppercase, a lo
leave the password field blank for easy access i

Select reply

Send

No, it is a replacement. The last router broke.

The first thing you need to do is change the default password.

Answer 2

That is complete now, and the router is asking to move on?

Select reply
If you think you should, you can.
No, it is not necessary.
Yes, reboot please.
Select reply

Send

Answer: See explanation below.

Explanation:

First Chat Response:When the user mentions setting up a new router, the best initial response to maintain a helpful and professional tone is:
>Select reply:"I am happy to assist you today."

Second Chat Response:When the user states that they need to set up basic security settings:
>Select reply:"Is this the first router in your office?"

Third Chat Response:After learning it's a replacement router and the user is logged into the router's web page:
>Select reply:"The first thing you need to do is change the default password."

Fourth Chat Response:For the response about password settings:
>Select reply:"Create a new password with an uppercase, a lowercase, and a special character."

Fifth Chat Response:When the router prompts to reboot:
>Select reply:"Yes, reboot please."

Study Guide Reference: The CompTIA A+ Core 2 guide highlights the importance of changing default credentials and using strong password policies, particularly in SOHO environments where routers are often targeted.

Question: 20

A help desk technician is setting up speech recognition on a Windows system. Which of the following settings should the technician use?

A. Time and Language
B. Personalization
C. System
D. Ease of Access

Answer: D

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
In Windows, accessibility tools such as speech recognition are found under the Ease of Access settings. This section includes options for users who require assistive technologies, including screen readers, magnifiers, and voice control interfaces like speech recognition. Setting up speech recognition allows users to control the system and input text using voice commands.
A . Time and Language is for setting regional preferences and language packs.
B . Personalization adjusts themes, backgrounds, and colors.
C . System includes display, storage, notifications, and power settings, but not accessibility tools. Reference:
CompTIA A+ 220-1102 Objective 1.3: Given a scenario, use appropriate Microsoft operating system features and tools.
Study Guide Section: Accessibility tools and system configuration

Question: 21

A user receives a new personal computer but is unable to run an application. An error displays saying that .NET Framework 3.5 is required and not found. Which of the following actions is the best way to resolve this issue?

A. Resolve the dependency through the 'Turn Windows features on or off' menu.
B. Download the dependency via a third-party repository.
C. Ignore the dependency and install the latest version 4 instead.
D. Forward the trouble ticket to the SOC team because the issue poses a great security risk.

Answer: A

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
NET Framework versions are often required for applications to run. If an older app requires .NET Framework 3.5, it must be explicitly installed as it is not included by default in newer versions of Windows. The best method to do this safely is through the built-in "Turn Windows features on or off" utility, which downloads and installs it via official Microsoft services.
B . Using third-party repositories is unsafe and not recommended.
C . Installing .NET 4 does not include 3.5; versions are not fully backward compatible.
D . The issue is technical, not a security incident for the SOC team.
Reference:
CompTIA A+ 220-1102 Objective 3.3: Troubleshoot common software, application, and OS security issues.
Study Guide Section: Managing application dependencies (e.g., .NET Framework, Java)

Question: 22

An employee is using a photo editing program. Certain features are disabled and require a log-in, which the employee does not have. Which of the following is a way to resolve this issue?

A. License assignment
B. VPN connection
C. Application repair
D. Program reinstallation

Answer: A

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
Many modern commercial software applications (including photo editors like Adobe Photoshop) offer tiered features based on user subscriptions or license levels. If certain features are locked and prompt for a login, the issue is likely due to a missing or unassigned software license. Assigning the correct license through a centralized license management system (such as Adobe Admin Console or Microsoft 365 portal) will enable those features.
B . VPN connection does not affect local software licensing.
C . Repairing the application does not resolve license entitlement.
D . Reinstalling the software won't help unless the license is assigned.

Reference:
CompTIA A+ 220-1102 Objective 3.3: Troubleshoot common software and application issues.
Study Guide Section: Troubleshooting licensing and access control for applications

Question: 23

A technician is deploying mobile devices and needs to prevent access to sensitive data if the devices are lost. Which of the following is the best way to prevent unauthorized access if the user is unaware that the phone is lost?

A. Encryption
B. Remote wipe
C. Geofencing
D. Facial recognition

Answer: B

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
Remote wipe is the best option to prevent unauthorized access to data when a mobile device is lost or stolen—especially if the user is unaware of the loss. It allows administrators or mobile device management (MDM) systems to remotely erase all data on the device, rendering it unusable for unauthorized users.
A . Encryption protects the data, but if the device remains powered and logged in, it may still be accessible.
C . Geofencing can restrict features based on location but does not erase data.
D . Facial recognition helps secure access but can be bypassed in some cases or fail in practical situations.
Reference:
CompTIA A+ 220-1102 Objective 2.2: Compare and contrast security measures and tools.

Study Guide Section: Mobile device security (remote wipe, lockout, MDM tools)

Question: 24

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

Question: 25

Technicians are failing to document user contact information, device asset tags, and a clear description of each issue in the ticketing system. Which of the following should a help desk management team implement for technicians to use on every call?

A. Service-level agreements
B. Call categories
C. Standard operating procedures
D. Knowledge base articles

Answer: C

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

Standard Operating Procedures (SOPs) define the mandatory steps and expectations technicians must follow during support calls. This includes documentation standards such as logging user info, asset details, and issue descriptions in the ticketing system. Implementing SOPs ensures consistency and accountability.

A . SLAs define response/resolution times but not documentation practices.

B . Call categories organize types of issues but don't guide technician actions.

D . Knowledge base articles provide solutions to known problems but don't ensure proper ticket documentation.

Reference:

CompTIA A+ 220-1102 Objective 4.2: Summarize best practices associated with types of documentation and support systems information.

Study Guide Section: Documentation practices, SOPs, ticketing protocols

Question: 26

An application's performance is degrading over time. The application is slowing, but it never gives an error and does not crash. Which of the following tools should a technician use to start troubleshooting?

A. Reliability history
B. Computer management
C. Resource monitor
D. Disk

Answer: C

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
Resource Monitor provides real-time monitoring of system performance and resource usage, including CPU, memory, disk, and network usage. It helps technicians identify performance bottlenecks (e.g., high memory or CPU usage) that can cause slowdowns in applications over time without producing crash errors.
A . Reliability history logs application crashes or errors — not helpful if the app doesn't crash.
B . Computer Management is a broad utility with limited real-time monitoring capability.
D . Disk is too vague — tools like CHKDSK can help with disk errors but not general performance degradation.
Reference:
CompTIA A+ 220-1102 Objective 3.2: Given a scenario, troubleshoot common personal computer issues.
Study Guide Section: System performance tools — Resource Monitor, Task Manager

Question: 27

Which of the following filesystem types does the Linux OS use?

A. exFAT
B. APFS
C. ext4
D. NTFS

Answer: C

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
The ext4 (Fourth Extended Filesystem) is the most widely used default filesystem in modern Linux distributions. It is designed for high performance, scalability, and reliability, and is supported by all mainstream Linux kernels.
A . exFAT is used for cross-platform external drives, not native Linux systems.
B . APFS is Apple's proprietary filesystem for macOS and iOS.
D . NTFS is the default filesystem for Windows, not Linux.
Reference:
CompTIA A+ 220-1102 Objective 1.9: Identify common features and tools of the Linux client/desktop OS.
Study Guide Section: Filesystem types in Linux — ext3, ext4, and their characteristics

Question: 28

Which of the following methods would make data unrecoverable but allow the drive to be repurposed?

A. Deleting the partitions
B. Implementing EFS
C. Performing a low-level format
D. Degaussing the device

Answer: C

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
A low-level format (also referred to as a zero-fill or full format) writes over every sector on a storage device, effectively destroying the existing data and making recovery nearly impossible. Unlike degaussing, which renders the drive unusable, a low-level format maintains the integrity of the device, allowing it to be repurposed or reused.
A . Deleting partitions does not fully erase data; it only removes references in the partition table.
B . EFS (Encrypting File System) encrypts files but does not securely wipe them.
D. Degaussing destroys the magnetic structure of a drive, making it inoperable and not reusable. Reference:
CompTIA A+ 220-1102 Objective 4.3: Given a scenario, implement basic change management best practices.
Study Guide Section: Drive sanitation methods — low-level format vs. degaussing vs. deletion

Question: 29

After a recent mobile OS upgrade to a smartphone, a user attempts to access their corporate email, but the application does not open. A technician restarts the smartphone, but the issue persists.
Which of the following is the most likely way to resolve the issue?

A. Updating the failed software
B. Registering the smartphone with an MDM solution
C. Installing a third-party client
D. Clearing the cache partition

Answer: A

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
Mobile OS updates can sometimes cause compatibility issues with specific apps, including corporate email clients. The most likely resolution is to check for and apply an update to the affected application, especially if it hasn't been updated to support the latest OS version.
B . Registering with MDM might be required for access but wouldn't address app crashes due to incompatibility.
C . A third-party client might help, but it's not the best first step if the default app is expected to work.
D . Clearing the cache can help resolve some minor issues, but updating the app directly addresses compatibility concerns.
Reference:
CompTIA A+ 220-1102 Objective 3.3: Troubleshoot mobile OS and application issues.
Study Guide Section: App compatibility and mobile software updates

Question: 30

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

Question: 31

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

Question: 32

Recently, the number of users sharing smartphone passcodes has increased. The management team wants a technician to deploy a more secure screen lock method. Which of the following technologies should the technician use?

A. Pattern lock
B. Facial recognition
C. Device encryption
D. Multifactor authentication

Answer: B

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
Facial recognition is a biometric authentication method that ties access to a unique physical feature of the user. Unlike passcodes or pattern locks—which can be easily shared—facial recognition provides a more secure and non-transferable form of access. It also enhances user convenience and is widely supported by modern smartphones.
A . Pattern locks can still be shared and are less secure.
C . Device encryption protects data but does not prevent screen access if a passcode is shared.
D . Multifactor authentication typically applies to app or account access, not basic phone unlocking. Reference:
CompTIA A+ 220-1102 Objective 2.2: Compare and contrast common security measures and authentication technologies.
Study Guide Section: Biometric screen lock technologies (e.g., facial recognition, fingerprint)

Question: 33

An end user's laptop is having network drive connectivity issues in the office. The end user submits a help desk ticket, and a support technician is able to establish a remote connection and fix the issue. The following day, however, the network drive is disconnected again. Which of the following should the technician do next?

A. Connect remotely to the user's computer to see whether the network drive is still connected.
B. Send documentation about how to fix the issue in case it reoccurs.
C. Escalate the ticket to the next level.
D. Keep the ticket open until next day, then close the ticket.

Answer: C

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
Since the issue has recurred after a temporary fix, it is likely a deeper or persistent configuration or server issue. Escalating the ticket to the next tier of support (e.g., network or system administrator) ensures further investigation and permanent resolution. Escalation is part of the standard support protocol when issues reoccur despite initial troubleshooting.
A . Rechecking remotely may confirm the issue, but doesn't resolve it long term.
B . Providing documentation helps the user but doesn't solve the root cause.
D . Keeping the ticket open is passive and doesn't address the recurring issue.
Reference:
CompTIA A+ 220-1102 Objective 4.1: Given a scenario, implement best practices associated with documentation and support systems information.
Study Guide Section: Escalation procedures and ticket management

Question: 34

Which of the following provides information to employees, such as permitted activities when using the organization's resources?

A. AUP
B. MNDA
C. DRM
D. EULA

Answer: A

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
An Acceptable Use Policy (AUP) outlines the rules and guidelines for employees or users regarding the appropriate use of company systems, resources, and internet access. It defines permitted and prohibited activities, helping to mitigate security risks and establish clear behavioral expectations. B . MNDA (Mutual Non-Disclosure Agreement) deals with confidentiality, not usage guidelines.
C . DRM (Digital Rights Management) controls access to copyrighted content.
D . EULA (End User License Agreement) pertains to software licensing, not internal policies. Reference:
CompTIA A+ 220-1102 Objective 4.3: Explain common safety and environmental impacts and procedures.
Study Guide Section: Organizational policies — AUP, security best practices

Question: 35

A technician needs to install an operating system on a large number of workstations. Which of the following is the fastest method?

A. Physical media
B. Mountable ISO
C. Manual installation
D. Image deployment

Answer: D

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
Image deployment is the fastest and most efficient method for installing operating systems on multiple machines. It involves creating a pre-configured image of an OS and deploying it across systems using tools like Windows Deployment Services (WDS) or third-party imaging solutions. This method saves time and ensures consistency across all devices.

A . Physical media is slow and not scalable.

B . Mountable ISOs are useful but still require manual installation.

C . Manual installation is time-consuming and not suitable for large-scale deployment.

Reference:
CompTIA A+ 220-1102 Objective 1.4: Given a scenario, use appropriate Microsoft operating system installation methods.
Study Guide Section: Deployment methods — image deployment, automation

Question: 36

A user is working from home and is unable to access work files on a company laptop. Which of the following should a technician configure to fix the network access issue?

A. Wide-area network
B. Wireless network
C. Proxy network settings
D. Virtual private network

Answer: D

Explanation:

A VPN creates a secure tunnel from the user's home network into the corporate network, providing the necessary routing and access controls for the laptop to reach internal file servers. Without a VPN, the device remains outside the corporate LAN and cannot directly reach protected resources.

A VPN creates a secure tunnel from the user's home network into the corporate network, providing the necessary routing and access controls for the laptop to reach internal file servers. Without a VPN, the device remains outside the corporate LAN and cannot directly reach protected resources.

Question: 37

A technician is troubleshooting an issue in which a service runs momentarily and stops at certain points in the process. The technician needs to determine the root cause of this issue. Which of the following tools should the technician use?

A. Event Viewer
B. Task Manager
C. Internet Options
D. Process Explorer

Answer: A

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
Event Viewer is the best tool to analyze the root cause of service failures in Windows. It provides detailed logs from system processes, including errors, warnings, and crash reports related to services and applications. When a service starts and stops unexpectedly, Event Viewer will often record the cause, such as dependency failures or access violations.

B . Task Manager shows active processes but doesn't retain logs or causes of failure.

C . Internet Options is used for configuring browser settings, not troubleshooting services.

D . Process Explorer is powerful but more suited for live monitoring and detailed process trees, not post-failure log analysis.

Reference:
CompTIA A+ 220-1102 Objective 3.1: Given a scenario, troubleshoot common Windows OS problems.
Study Guide Section: Log file analysis using Event Viewer

Question: 38

Which of the following is an example of an application publisher including undisclosed additional software in an installation package?

A. Virus
B. Ransomware
C. Potentially unwanted program
D. Trojan

Answer: C

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
A Potentially Unwanted Program (PUP) is software that a user may not have knowingly installed. It often gets bundled with legitimate software and installs without full disclosure. PUPs can affect performance, change system settings, or display unwanted ads but are not necessarily malicious like viruses or ransomware.

A . Viruses replicate and spread; they are generally more harmful and not "bundled" in the same way.

B . Ransomware encrypts files for payment and is deliberately malicious.

D . A Trojan disguises itself as legitimate software to perform malicious actions but is not typically pre-bundled by legitimate publishers.

Reference:
CompTIA A+ 220-1102 Objective 2.5: Given a scenario, detect, remove, and prevent malware using appropriate tools and methods.
Study Guide Section: Types of malware — PUPs and bundled software

Question: 39

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

Question: 40

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?

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. Reference:

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: 41

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

Question: 42

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

Question: 43

A technician is setting up a surveillance system for a customer. The customer wants access to the system's web interface on the LAN via the system's IP address. Which of the following should the technician use to prevent external log-in attempts from the internet?

A. Port mapping
B. Subnetting
C. Static IP
D. Content filtering

Answer: A

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
To prevent external access, the technician should avoid exposing the surveillance system's port to the public internet. Port mapping (also known as port forwarding) is the method used to control which internal devices and ports are accessible from the outside. By not configuring port forwarding for the device, external login attempts are effectively blocked.
B . Subnetting organizes IP addresses but doesn't directly restrict access.
C . A static IP ensures consistent addressing but does not secure access.
D . Content filtering is used to restrict web content, not to block access to a web interface.
Reference:
CompTIA A+ 220-1102 Objective 2.2: Compare and contrast security measures and tools.
Study Guide Section: SOHO router security — port forwarding and blocking external access

Question: 44

A technician needs to configure laptops so that only administrators can enable virtualization technology if needed. Which of the following should the technician configure?

A. BIOS password
B. Guest account
C. Screen lock
D. AutoRun setting

Answer: A

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
Virtualization settings are typically found within the BIOS/UEFI firmware configuration. To prevent unauthorized users from changing these settings, the technician should set a BIOS password. This ensures only administrators with the password can access or modify BIOS settings, including virtualization support.
B . The guest account is a user-level feature in Windows and doesn't control BIOS access.
C . A screen lock prevents casual access to the desktop but doesn't protect firmware settings.
D . AutoRun controls how media and devices behave when inserted — unrelated to BIOS security.
Reference:
CompTIA A+ 220-1102 Objective 2.2: Compare and contrast security measures and administrative controls.
Study Guide Section: BIOS/UEFI settings protection — password implementation

Question: 45

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

Question: 46

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

Question: 47

Which of the following describes an attack in which an attacker sets up a rogue AP that tricks users into connecting to the rogue AP instead of the legitimate network?

A. Stalkerware
B. Evil twin
C. Tailgating
D. Shoulder surfing

Answer: B

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

An evil twin is a rogue wireless access point set up to mimic a legitimate Wi-Fi network. Unsuspecting users may connect to it, giving attackers the opportunity to intercept traffic, steal credentials, or install malware. The evil twin often uses the same SSID as the real network to fool users.

A . Stalkerware is spyware installed to track user activity, typically on personal devices.

C . Tailgating is a physical security breach involving unauthorized entry behind someone with access. D . Shoulder surfing involves observing a person entering confidential data, such as PINs or passwords.

Reference:

CompTIA A+ 220-1102 Objective 2.3: Compare and contrast social engineering and wireless attacks.

Study Guide Section: Wireless threats — rogue APs and evil twin scenarios

Question: 48

A user is experiencing issues with outdated images while browsing websites. Which of the following settings should a technician use to correct this issue?

A. Administrative Tools
B. Windows Defender Firewall
C. Internet Options
D. Ease of Access

Answer: C

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
Outdated images and website data often result from cached files in the browser. The Internet Options panel in Windows (specifically under the General tab) allows users to clear browsing history, including cached images and files, which forces the browser to load the most current versions of web content.
A . Administrative Tools is used for advanced system management, not browser settings.
B . Windows Defender Firewall controls network traffic and security rules, not caching.
D . Ease of Access provides accessibility features for users with disabilities — unrelated to web browsing issues.
Reference:
CompTIA A+ 220-1102 Objective 3.3: Troubleshoot common software and application issues.
Study Guide Section: Internet Options and browser cache clearing for display issues

Question: 49

Every time a user loads a specific spreadsheet, their computer is temporarily unresponsive. The user also notices that the title bar indicates the application is not responding. Which of the following would a technician most likely inspect?

A. Anti-malware logs
B. Workstation repair options
C. Bandwidth status as reported in the Task Manager
D. File size and related memory utilization

Answer: D

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
If a system becomes unresponsive while opening a specific spreadsheet, the issue is likely tied to the file's size or the complexity of its content (e.g., embedded formulas, macros, or graphics). High

memory utilization caused by the file can lead to temporary freezing or application "Not Responding" messages.
Checking the spreadsheet's file size and monitoring system memory in Task Manager will help isolate performance bottlenecks.

A . Anti-malware logs are important for security troubleshooting but less likely relevant to spreadsheet-related performance issues.

B . Workstation repair is for system-wide problems and not necessary for a single-file issue.

C . Bandwidth relates to network usage and wouldn't impact opening a local file.

Reference:

CompTIA A+ 220-1102 Objective 3.3: Troubleshoot common application issues.

Study Guide Section: Troubleshooting application slowness and performance using Task Manager and resource monitoring tools

Question: 50

A user frequently misplaces their Windows laptop and is concerned about it being stolen. The user would like additional security controls on their laptop. Which of the following is a built-in technology that a technician can use to enable full drive encryption?

A. Active Directory
B. New Technology File System
C. Encrypting File System
D. BitLocker

Answer: D

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

BitLocker is Microsoft's full disk encryption technology built into Windows Pro and Enterprise editions. It encrypts the entire drive, protecting data if the device is lost or stolen. BitLocker can use TPM (Trusted Platform Module) and can be configured with PINs or USB keys for added security.

A . Active Directory is for centralized user and policy management in domains.

B . NTFS is the file system format and doesn't provide encryption by itself.

C . EFS (Encrypting File System) encrypts individual files or folders, not the entire drive.

Reference:

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

Study Guide Section: Encryption options — BitLocker vs. EFS

Question: 51

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)

Question: 52

A user's new smartphone is not staying charged throughout the day. The smartphone charges fully every night. Which of the following should a technician review first to troubleshoot the issue?

A. Storage usage
B. End of software support
C. Charger wattage
D. Background applications

Answer: D

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
Background applications can significantly drain a smartphone's battery, even when the device is idle. A technician should first review which apps are running in the background and consuming power through the battery usage section of the OS. Disabling or restricting power-hungry apps often resolves poor battery life.
A . Storage usage doesn't significantly affect battery life.
B . End of software support is unrelated to battery performance unless it's causing inefficient processes, which would still be secondary.
C . Charger wattage affects charging speed, not battery life after charging.
Reference:
CompTIA A+ 220-1102 Objective 3.3: Troubleshoot common mobile OS and application issues.
Study Guide Section: Diagnosing battery and app performance issues on mobile devices

Question: 53

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

Question: 54

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?

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.

Reference:
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: 55

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

Question: 56

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

Question: 57

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: B,D

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

Question: 58

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

Question: 59

A user has been adding data to the same spreadsheet for several years. After adding a significant amount of data, they are now unable to open the file. Which of the following should a technician do to resolve the issue?

A. Revert the spreadsheet to the last restore point.
B. Increase the amount of RAM.
C. Defragment the storage drive.
D. Upgrade the network connection speed.

Answer: B

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
When a spreadsheet becomes very large, opening and processing it requires more memory (RAM). If the system doesn't have sufficient memory, it may fail to load the file properly. Upgrading or increasing the available RAM can resolve performance and loading issues with very large files.
A . Restore points roll back system settings, not individual file content.
C . Defragmentation optimizes disk performance but won’t help with memory issues.
D . Network speed has no effect if the file is stored and opened locally.
Reference:
CompTIA A+ 220-1102 Objective 3.3: Troubleshoot common application and performance issues.
Study Guide Section: Troubleshooting large-file performance and system resource limitations

Question: 60

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

Question: 61

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

Question: 62

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

Question: 63

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

Question: 64

A customer wants to be able to work from home but does not want to be responsible for bringing company 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: C,D

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 enduser 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

Question: 65

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

Question: 66

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

Question: 67

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

Question: 68

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

Question: 69

A customer's computer does not have an active connection to the network. A technician goes through a few troubleshooting steps but is unable to resolve the issue. The technician has exhausted their knowledge. The customer expresses frustration at the time taken to resolve this issue. Which of the following should the technician do?

A. Escalate the issue to a senior team member and provide next steps to the customer.
B. Dismiss the customer and reschedule another troubleshooting session at a later date.
C. Interrupt the customer and express that troubleshooting support tickets can take time.
D. Maintain a positive attitude and continue to ask questions regarding the scope of the issue.

Answer: A

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
When a technician exhausts all troubleshooting steps within their knowledge and the issue remains unresolved, the best practice is to escalate the issue to a higher-level technician or team.
Additionally, the technician should clearly communicate the next steps to the customer to maintain transparency and reduce frustration. This ensures continuity of support and upholds customer satisfaction.
B . Dismissing the customer is unprofessional and violates proper customer service protocols.
C . Interrupting the customer and providing excuses escalates the tension and is inappropriate.
D . Continuing to ask questions without new troubleshooting steps wastes time and increases frustration.
Reference:
CompTIA A+ 220-1102 Objective 4.1: Given a scenario, implement best practices associated with documentation and support systems information.
Study Guide Section: Customer service best practices — escalation and communication

Question: 70

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

Question: 71

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

Question: 72

SIMULATION

As a corporate technician, you are asked to evaluate several suspect email messages on a client's computer.

Corporate policy requires the following:

>All phishing attempts must be reported.

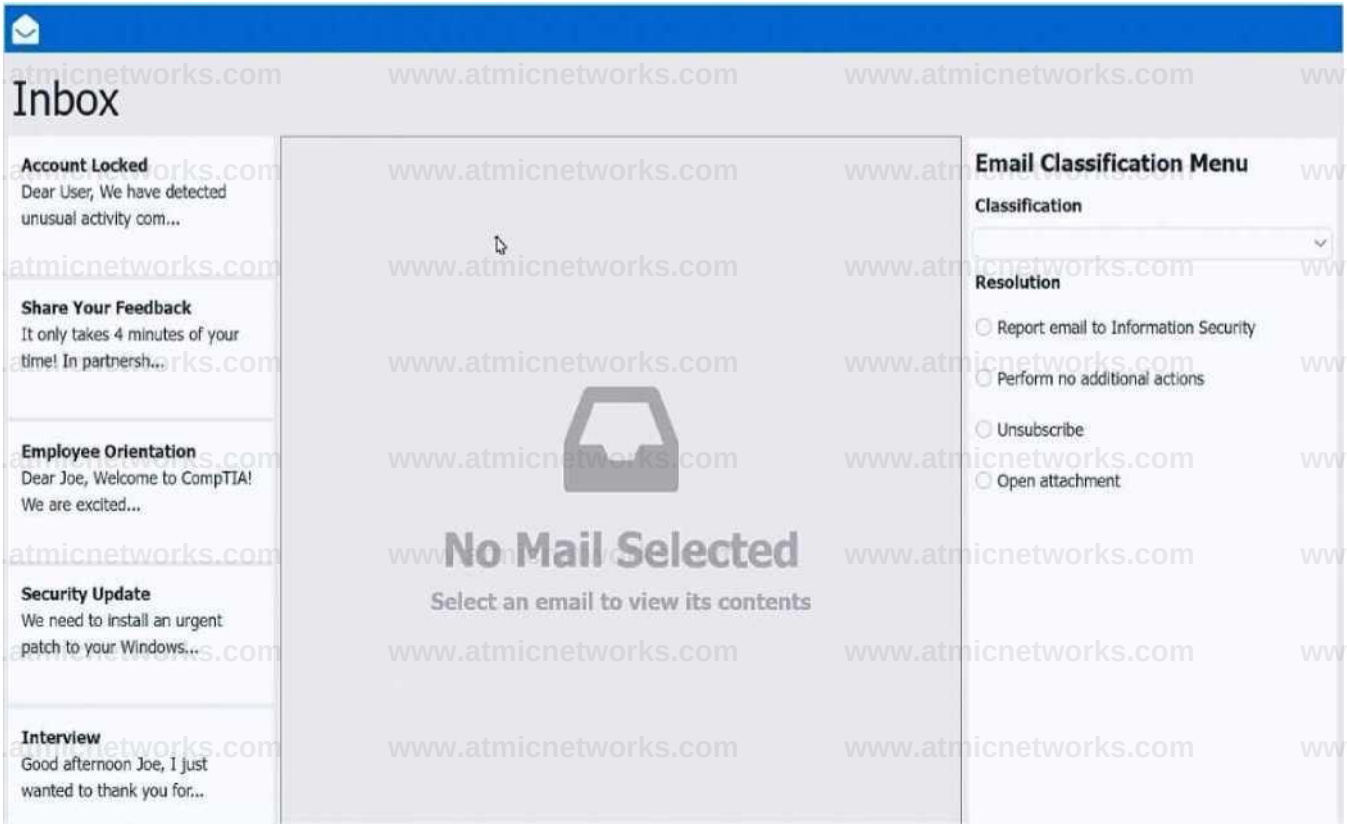
>Future spam emails to users must be prevented.

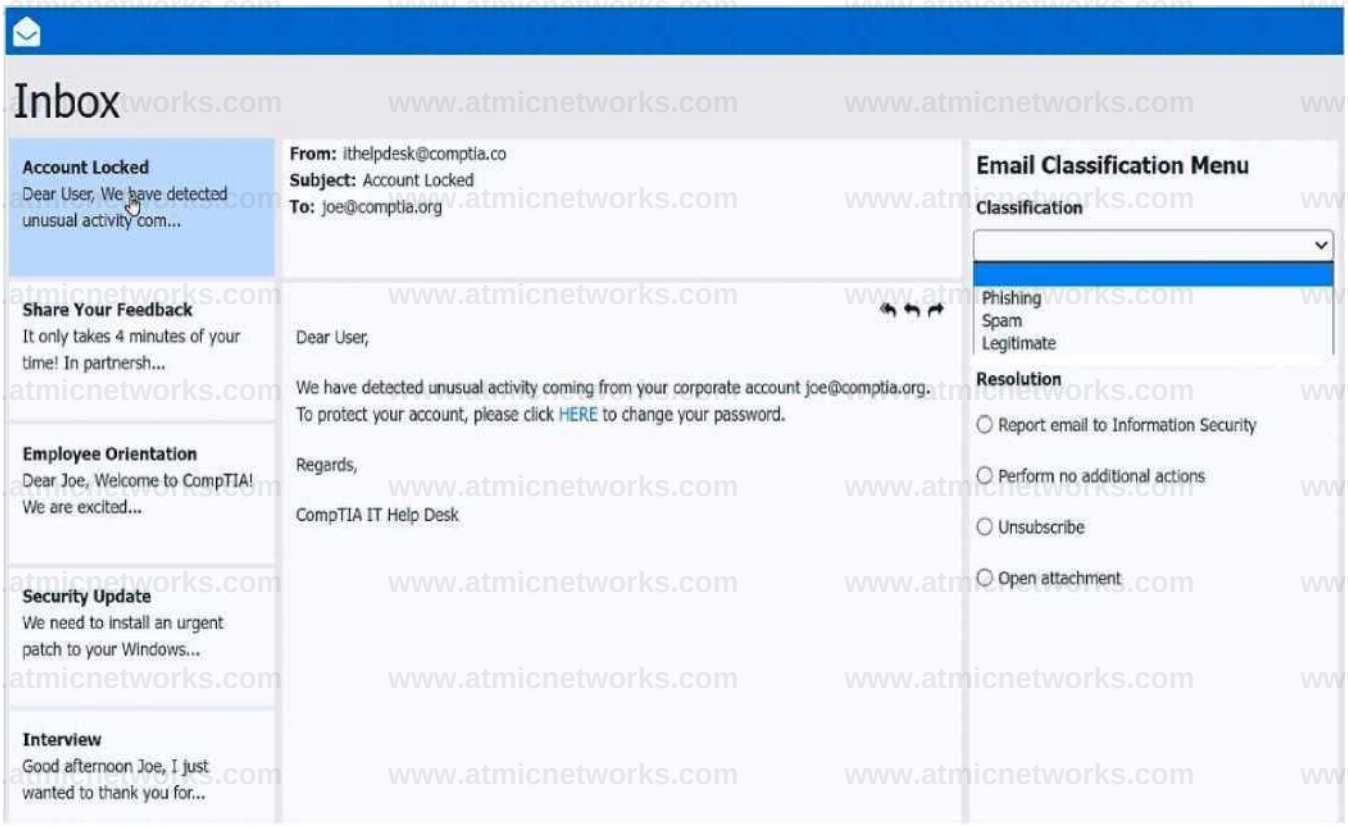
INSTRUCTIONS

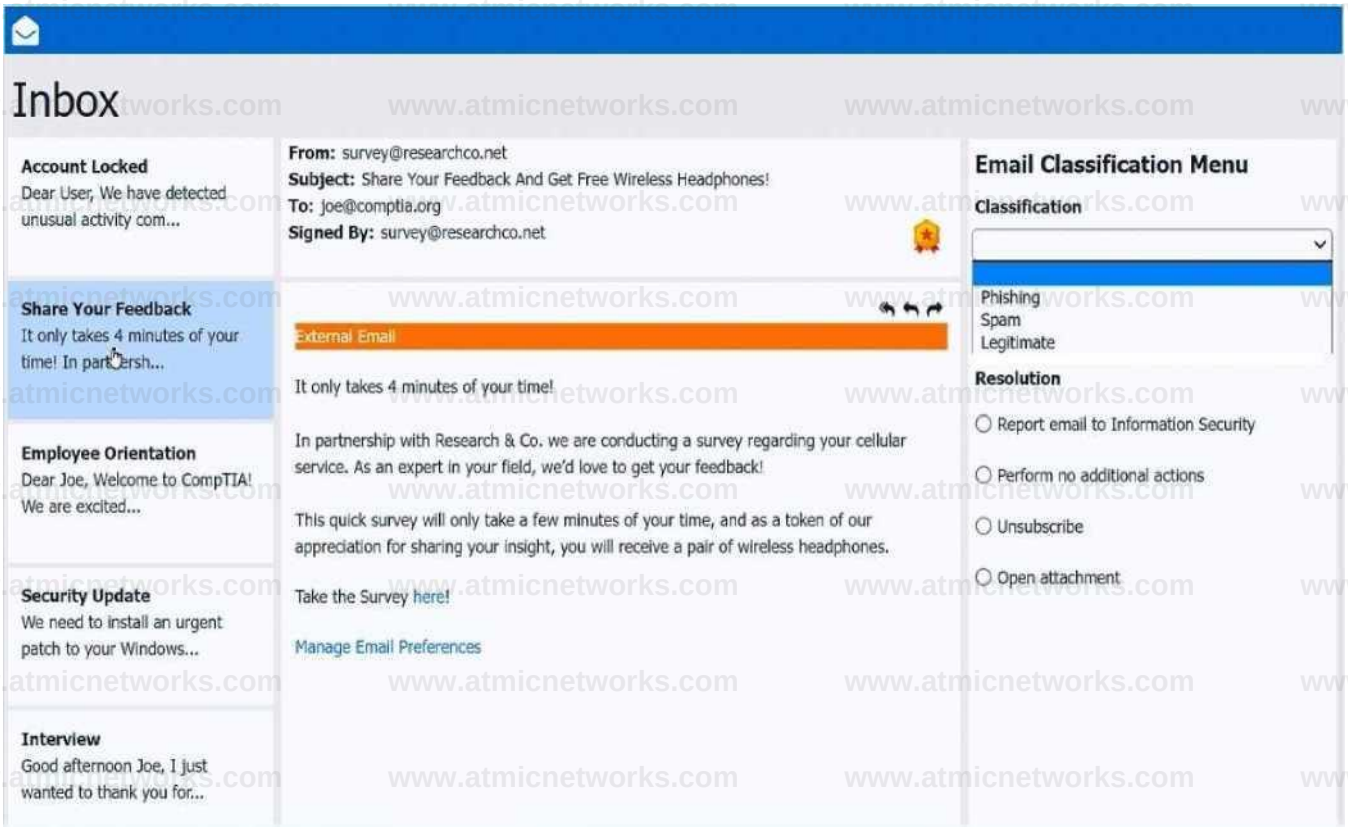
Review each email and perform the following within the email:

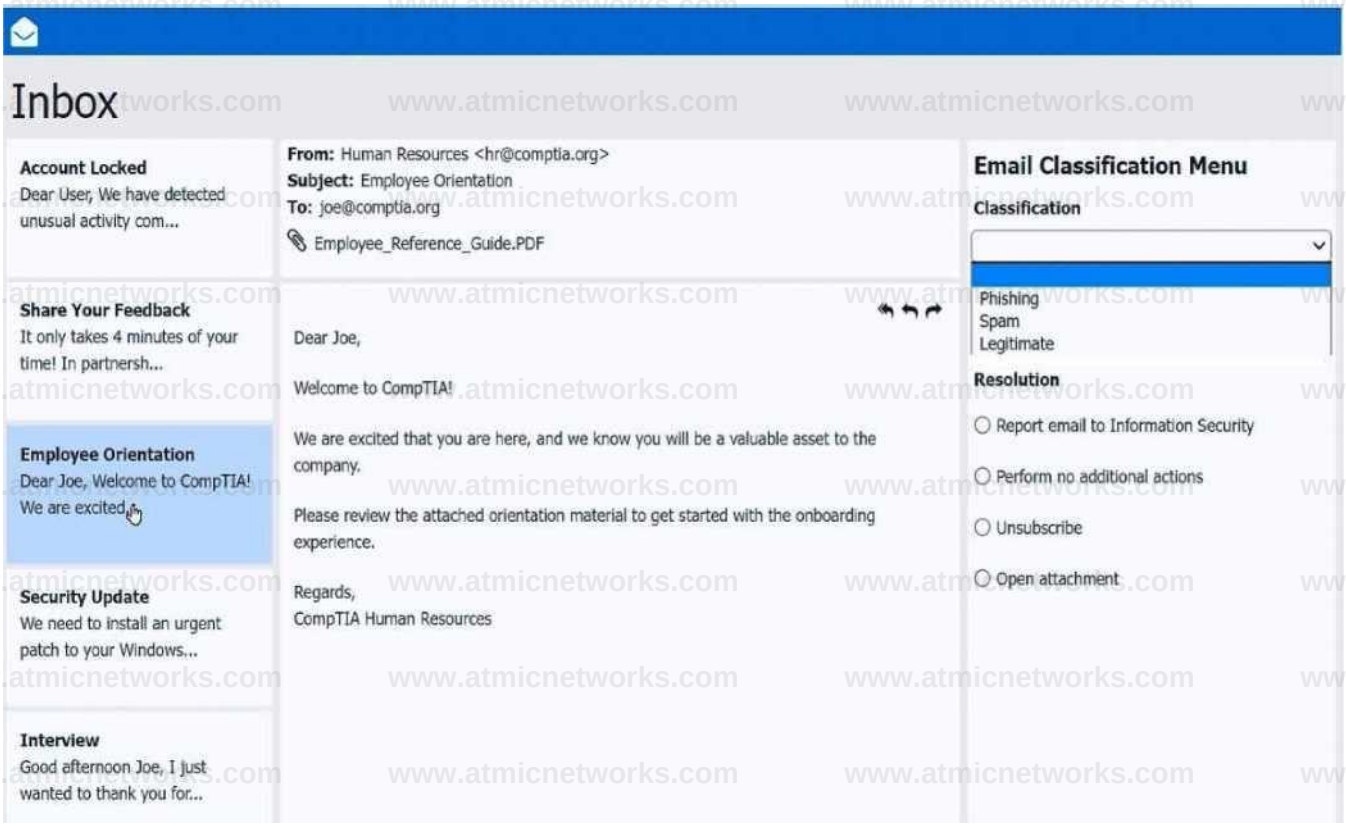
>Classify the emails
>Identify suspicious items, if applicable, in each email
>Select the appropriate resolution

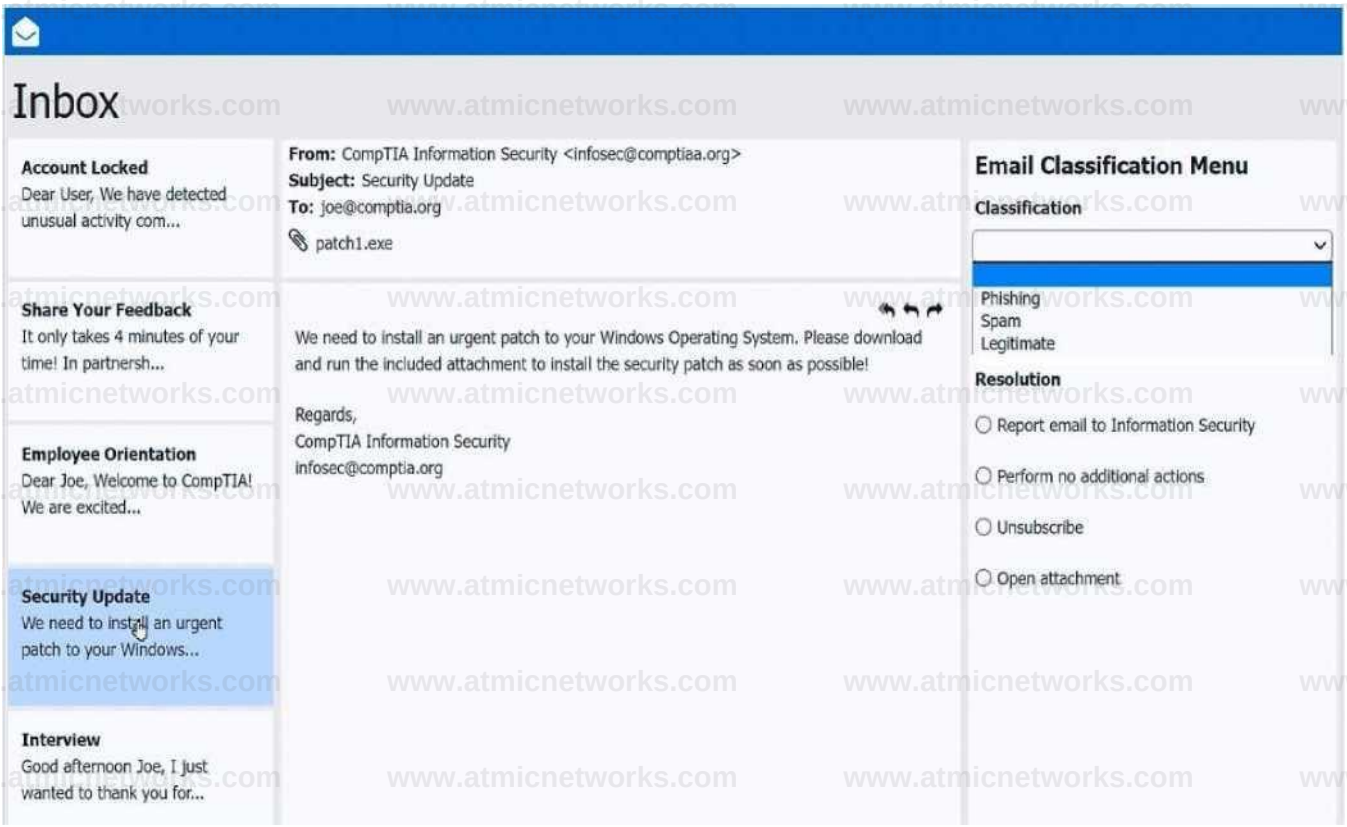
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

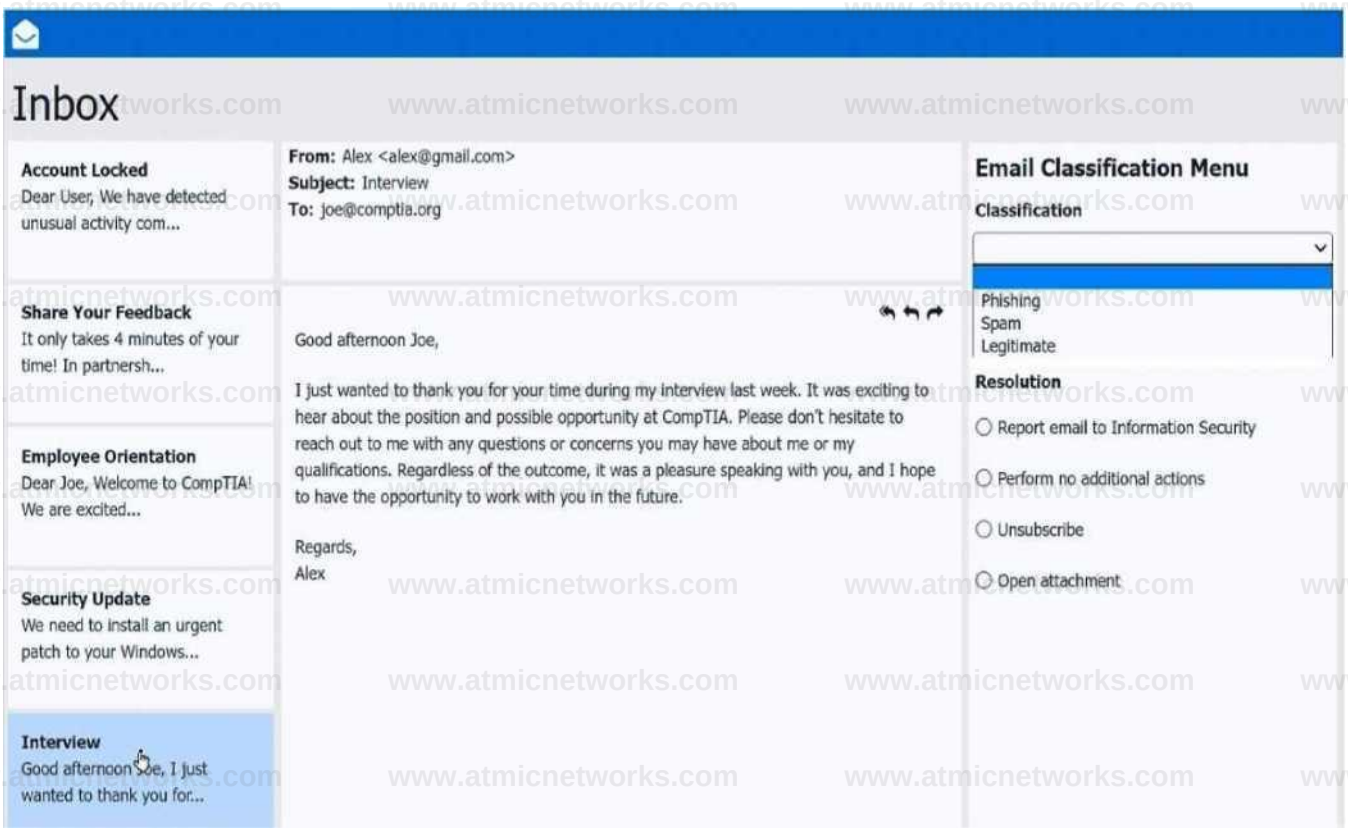







Inbox
Account Locked
Dear User, We have detected unusual activity com...
Share Your Feedback
It only takes 4 minutes of your time! In partnersh...
Employee Orientation
Dear Joe, Welcome to CompTIA! We are excited...
Security Update
We need to install an urgent patch to your Windows...
Interview
Good afternoon Joe, I just wanted to thank you for...
From: Human Resources <hr@comptia.org>
Subject: Employee Orientation
To: joe@comptia.org
Employee_Reference_Guide.PDF
Dear Joe,
Welcome to CompTIA!
We are excited that you are here, and we know you will be a valuable asset to the company.
Please review the attached orientation material to get started with the onboarding experience.
Regards,
CompTIA Human Resources
Email Classification Menu
Classification
Phishing
Spam
Legitimate
Resolution
Report email to Information Security
Perform no additional actions
Unsubscribe
Open attachment


Inbox
Account Locked
Dear User, We have detected unusual activity com...
Share Your Feedback
It only takes 4 minutes of your time! In partnersh...
Employee Orientation
Dear Joe, Welcome to CompTIA! We are excited...
Security Update
We need to install an urgent patch to your Windows...
Interview
Good afternoon Joe, I just wanted to thank you for...
From: CompTIA Information Security <infosec@comptiaa.org>
Subject: Security Update
To: joe@comptia.org
patch1.exe
We need to install an urgent patch to your Windows Operating System. Please download and run the included attachment to install the security patch as soon as possible!
Regards,
CompTIA Information Security
infosec@comptia.org
Email Classification Menu
Classification
Phishing
Spam
Legitimate
Resolution
Report email to Information Security
Perform no additional actions
Unsubscribe
Open attachment



Answer: See explanation below.

Explanation:

Inbox mail 1 -Account Locked- Phishing - Report email to Information Security Inbox mail 2 -Share your feedback - Legitimate - Perform no additional actions Inbox mail 3 –Employee orientation - Legitimate - Perform no additional actions Inbox mail 4 –Security Update – Spam - Report email to Information Security Inbox mail 5 –Interview - Legitimate - Perform no additional actions

Question: 73

A user reports getting a BSOD (Blue Screen of Death) error on their computer at least twice a day.
Which of the following should the technician use to determine the cause?

A. Event Viewer
B. Performance Monitor
C. System Information
D. Device Manager

Answer: A

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
Event Viewer is the primary tool used to investigate system-level errors and logs, including BSODs.
When a BSOD occurs, Windows logs the error codes and associated system behavior under “System” logs in Event

Viewer. This allows the technician to review crash events, identify error codes (e.g., STOP codes), and pinpoint hardware or driver issues.

B . Performance Monitor is used for real-time performance tracking and trend analysis, not crash logs.

C . System Information displays system specs but not crash logs or events.

D . Device Manager shows device status and driver issues but doesn't retain error logs related to BSODs.

Reference:

CompTIA A+ 220-1102 Objective 3.1: Given a scenario, troubleshoot common Windows OS problems.

Study Guide Section: Troubleshooting BSODs using Event Viewer and system logs

Question: 74

A technician is setting up a Windows server to allow remote desktop connections for multiple users. Which of the following should the technician configure on the workstation?

A. Firewall
B. Computer Management
C. User Accounts
D. Ease of Access

Answer: A

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

To allow Remote Desktop Protocol (RDP) access, the firewall must be configured to allow inbound connections on TCP port 3389. If the Windows Firewall blocks RDP, users will not be able to connect remotely even if the feature is enabled in system settings.

B . Computer Management allows configuration of services and local users, but not network access. C . User Accounts is for account setup and control, but enabling remote access requires firewall configuration.

D . Ease of Access is unrelated to remote connectivity—it's for accessibility features. Reference:

CompTIA A+ 220-1102 Objective 2.2: Compare and contrast security measures and firewall settings.

Study Guide Section: Enabling and securing RDP via firewall settings

Question: 75

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

Question: 77

An administrator is investigating a technical outage. The management team wants information that includes the summary of the outage and actions taken. Which of the following documentation should the administrator provide to the management team?

A. Knowledge base article
B. Non-disclosure agreement
C. Incident report
D. Standard operating procedure

Answer: C

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

An incident report documents key details such as the cause of the outage, steps taken to resolve it, and measures to prevent recurrence. It is a post-mortem analysis often shared with stakeholders to improve future response.

According to the Quentin Docter – CompTIA A+ Complete Study Guide:

"An incident report provides a summary of an event that disrupted normal operations and includes a timeline of what occurred, how the issue was diagnosed and fixed, and who was involved in the resolution".

This is reaffirmed in Travis Everett's All-in-One Guide:

"Documentation after an incident helps technical teams and management review the situation and learn from it. This is formalized in an incident report".

Question: 78

A user has rooted their corporate phone to load unapproved software. Which of the following tools should the company use to prevent access to the corporate network?

A. Mobile device management
B. Encryption
C. Geofencing
D. Lock screen

Answer: A

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

Mobile Device Management (MDM) allows an organization to enforce security policies, such as denying network access to jailbroken/rooted devices.

From the All-in-One Exam Guide by Travis Everett and Andrew Hutz:

"MDM software allows administrators to monitor, manage, and secure mobile devices connected to enterprise networks. One key feature is the detection and denial of access for rooted or jailbroken devices".

Quentin Docter also confirms:

"An MDM solution can check if a device has been rooted and prevent it from accessing the network, ensuring compliance with corporate security standards".

Question: 79

An administrator received an email stating that the OS they are currently supporting will no longer be issued security updates and patches. Which of the following is most likely the reason the administrator received this message?

A. Support from the computer's manufacturer is expiring
B. The OS will be considered end of life
C. The built-in security software is being removed from the next OS version
D. A new version of the OS will be released soon

Answer: B

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

When an OS reaches its end of life (EOL), it no longer receives updates or support, including critical security patches.

From the Quentin Docter Study Guide:

"End-of-life means the manufacturer no longer supports the OS with updates or security patches, which exposes systems to vulnerabilities unless upgraded".

All-in-One Exam Guide adds:

"End-of-life notifications serve as a final warning that continued use of the OS will be insecure and unsupported. It's crucial for administrators to plan migration".

Question: 80

Which of the following are system folders on macOS? (Select two)

A. Applications

B. Spotlight
C. Time Machine
D. Library
E. FileVault
F. iCloud

Answer: A,D

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
ApplicationsandLibraryare core system directories in macOS. TheApplicationsfolder contains installed applications. TheLibraryfolder contains support files, preferences, and other system-related files. From theQuentin Docter – CompTIA A+ Complete Study Guide:
"macOS organizes system and user files into several key folders. Among them, Applications and Library are standard system folders where apps and related files are stored."

Question: 81

After using a third-party disk optimization software package, a technician restarts a laptop and receives the message "No operating system found." The technician verifies that the BIOS properly recognizes the SSD. Which of the following should the technician do next?

A. Update BitLocker settings in the BIOS
B. Replace the CMOS battery
C. Boot from installation media and repair the MBR
D. Isolate the system from the corporate network

Answer: C

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
A corruptedMaster Boot Record (MBR)is a common issue after disk manipulation. Booting from installation media and using tools like bootrec to repair the MBR can resolve the problem.
Travis Everett – All-in-One Exam Guideexplains:
"A damaged MBR may result in the OS not loading. Booting from recovery or installation media and selecting startup repair or running bootrec commands can restore functionality."

Question: 82

After completing malware removal steps, what is the next step the technician should take?

A. Perform a secondary antivirus scan
B. Educate the end user
C. Reimage the computer
D. Review system logs

Answer: B

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

End-user education is crucial after malware removal to prevent recurrence. Teaching safe browsing habits and security awareness completes the remediation cycle.

Mark Soper – Mike Meyers' Lab Manualstates:

"Educating the user after malware remediation is part of the CompTIA malware response methodology. This includes training on phishing and safe practices."

Question: 83

Which of the following is used to store passwords in macOS?

A. FileVault
B. Keychain
C. Accessibility
D. Mission Control

Answer: B

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

Keychainis the built-in macOS utility that manages and stores credentials, including passwords and certificates.

According toQuentin Docter – CompTIA A+ Complete Study Guide:

"Keychain Access in macOS is used for managing and storing passwords securely, similar to credential managers in Windows."

Question: 84

An end user wants to have a sales printer added to their computer. The printer is on the domain. Which of the following is the best method for the technician to add the printer?

A. Go to the print server and select the printer name
B. Connect the laptop to the printer via USB
C. Connect to the printer via Bluetooth
D. Go to Local Users and Groups to add the printer

Answer: A

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

In a domain environment, printers are typically deployed via a print server. Users can browse available printers on the server

and install them directly.

All-in-One Exam Guidementions:

"In a corporate domain, printers are managed via a centralized print server. Users can select the desired printer from the server's shared list."

Question: 85

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, such as Google Authenticator or Microsoft Authenticator, can be configured to sendpush notificationsto users for approval when logging in. This is a form of multi-factor authentication.

FromAll-in-One Exam Guide:

"Push-based two-factor authentication uses an authenticator app to send a notification to a mobile device. The user must approve the login attempt in real time, ensuring the request is valid."

Question: 86

Various alerts on a user's Windows 11 laptop are continually interrupting the user during videoconference calls. Which of the following should a support technician recommend to best solve the issue?

A. Use multiple sound output devices for the various source applications
B. Disable all notifications in different applications in the order they appear
C. Configure the Sounds option in Control Panel to be set to No Sounds
D. Set Windows Notifications settings to Do Not Disturb

Answer: D

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

Windows 11 features a"Do Not Disturb"mode under Notification settings, which is designed to suppress interruptions during tasks like videoconferencing.

FromQuentin Docter – CompTIA A+ Complete Study Guide:

"Windows 11 introduces Do Not Disturb and Focus Assist under notification settings, enabling users to mute alerts during

presentations or calls."

Question: 87

A Windows 11 Home device is receiving constant pop-ups about an urgent need to update antivirus software to remove a detected threat. The user has been clicking the "X" button in the window frame but it always reappears. The pop-up includes an "OK" button to install the update and remove the threat. Which of the following should the user do next?

A. Click the "OK" button to install the update
B. Reinstall the Windows Operating System
C. Run System File Checker
D. Verify the current status and settings of protection measures

Answer: D

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
This is likely arogue antivirusor scareware tactic. The user shouldnot click "OK"and instead check Windows Security (or third-party antivirus) status and ensure real-time protection is enabled. FromMark Soper – Mike Meyers' Lab Manual:
"Users should verify security center settings if receiving suspicious pop-ups. Clicking unknown software updates can install malware. It's safer to validate protection through legitimate system tools."

Question: 88

Performance on a user's smartphone is degrading. Applications take a long time to start, and switching between windows also takes a long time. Which of the following diagnostic steps should a mobile technician take first?

A. Restore the phone to factory settings
B. Restart the phone
C. Check the phone's battery state
D. Uninstall unneeded applications

Answer: B

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
Thefirst stepin troubleshooting degraded mobile performance is typically arestart. This clears RAM and stops background processes that might be causing issues.
FromAll-in-One Exam Guide:
"Before taking invasive measures like a factory reset, always restart the device. A reboot clears temporary files and can significantly improve responsiveness."

Question: 89

A user takes an iOS-based smartphone that is performing slowly to a repair shop. A shop technician finds the following information:

Battery charge: 25%
Battery health: 90%
Hotspot: On
Mobile reception: |||
Roaming: Off
Used space: 63.76GB/64GB
Which of the following is the cause of the issue?

A. The device is running out of free space
B. The battery health is low
C. The phone is not sufficiently charged
D. The hotspot is degrading the performance
E. Too many applications are open

Answer: A

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
When an iOS device approaches full storage capacity, performance can be significantly impacted. iOS requires a buffer of free space to perform background processes efficiently.
From theAll-in-One Exam Guide:
"iOS devices need several gigabytes of free space to maintain optimal performance. Near-full storage can cause sluggish operation and failures in updates or background tasks."

Question: 90

After a user installs a mobile application from an advertisement, the phone's battery dies a few hours later, and it is hot to the touch, even when not in use. Which of the following should a technician do first?

A. Check for unauthorized device administrators
B. Contact the software developer
C. Run a mobile malware scan on the phone
D. Ensure appropriate MDM policies are applied

Answer: C

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
These symptoms strongly suggest malware activity—likely from the newly installed app. The first action should be torun a malware scanto detect and isolate malicious software.
FromQuentin Docter – CompTIA A+ Study Guide:

"Signs of malware infection include rapid battery drain and overheating. The first step should be a malware scan using trusted mobile antivirus apps."

Question: 91

A user decides to switch to Windows from Linux and is trying to migrate data using an external USB hard disk. However, when the user connects the cable to the Windows machine, an error message appears stating the device must be formatted before it can be used. The hard disk works as expected when connected to the Linux machine. Which of the following should the user do to resolve this issue?

A. Configure Windows firewall to allow data from Linux systems
B. Replace the cable with Windows-supported hardware
C. Apply a firmware update from the PC manufacturer
D. Update the file allocation system to exFAT

Answer: D

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
The Linux machine likely formatted the drive in a file system like ext4, which Windows cannot natively read. Reformatting the drive toexFATallows cross-platform compatibility.
FromAll-in-One Exam Guide:
"When migrating data between OSes, using a file system like exFAT ensures compatibility. Windows cannot read Linux-native file systems such as ext4 without third-party tools."

Question: 92

A Microsoft OS laptop user requests an alternative log-in authentication method because they have forgotten their password multiple times. Which of the following should a technician enable to satisfy this request?

A. Single sign-on
B. Windows Hello
C. BitLocker
D. User Account Control

Answer: B

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
Windows Helloprovides alternative sign-in options including facial recognition, fingerprint scans, and
PINs, reducing dependence on passwords.
FromAll-in-One Exam Guide:
"Windows Hello offers a range of biometric and PIN-based login methods designed to simplify access while enhancing security."
"It can be used in place of a password, ideal for users who frequently forget credentials."

Question: 93

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 of the following would a technician most likely do to resolve the issue?

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: 94

A secretary receives an email from the company's chief executive officer with a request to pay a vendor immediately. After the payment is made, the CEO informs the secretary that they never sent that email. Which of the following social engineering tactics best describes this type of attack?

A. Evil twin
B. Impersonation
C. Whaling
D. Spear phishing

Answer: C

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
Whalingis a form of phishing that targets high-profile individuals or involves pretending to be them (e.g., CEOs) to trick lower-level employees into transferring funds or sensitive data.

FromQuentin Docter – CompTIA A+ Study Guide:

"Whaling is a phishing tactic targeting executives or masquerading as one. The attacker crafts emails that exploit authority and urgency to manipulate recipients."

Question: 95

The battery on a user's smartphone discharges quickly when the user travels. The smartphone was replaced two weeks ago. Which of the following should a technician do first?

A. Replace the battery with a higher capacity option
B. Provide an external battery to extend the usage time
C. Ensure that the charging port is working as expected
D. Look for applications that are reporting the highest utilization

Answer: D

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

High battery drain is often due to apps running in the background or using GPS during travel. Thefirst stepshould always be tocheck battery usage statisticsto see if an application is misbehaving.

FromAll-in-One Exam Guide:

"Travel conditions can increase app activity, especially navigation or social media. Check app battery usage before assuming hardware faults."

Question: 96

A technician is reviewing an organization's current incident management policy. The organization uses a third-party vendor to protect the organization's assets with multiple tools. Which of the following service types is the organization using?

A. PaaS
B. EDR
C. MDR
D. XDR

Answer: C

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

MDR (Managed Detection and Response)provides outsourced threat monitoring and response using multiple tools. The use of athird-party providerfor protection and incident handling confirms MDR. FromQuentin Docter – CompTIA A+ Study Guide:

"MDR provides 24/7 threat detection and response through outsourced experts using advanced tools across client environments."

Question: 97

An employee is trying to connect their company laptop to an airport's Wi-Fi during a business trip. Once the network is connected, a pop-up window appears with the airport logo, which the employee quickly closes. The internet connection is not working properly. Which of the following should a help desk technician suggest?

A. Look for a wall socket with RJ45 and try to connect the laptop to it
B. Contact the airport IT department
C. Tell the employee that company policy prohibits connection to public Wi-Fi
D. Reconnect to the network and read the pop-up carefully

Answer: D

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
Most public Wi-Fi networks requireinteraction with a captive portal(e.g., terms of use or login).
Dismissing it prevents the user from gaining internet access. Reconnecting and completing the portal page is essential.
FromAll-in-One Exam Guide:
"Many public hotspots require user acknowledgment or login via a captive portal. Skipping this step results in no internet access."

Question: 98

A technician needs to disable guest log-ins on domain-joined desktop machines. Which of the following should the technician use?

A. Group Policy
B. Firewall
C. Microsoft Management Control
D. MSConfig

Answer: A

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
Group Policyis the standard administrative tool for enforcing security and configuration settings across domain-joined systems, including disabling guest accounts.
FromQuentin Docter – CompTIA A+ Study Guide:
"Disabling guest accounts and applying consistent security policies across multiple machines is best achieved through Group Policy on a Windows domain."

Question: 99

A user is unable to upload files to the corporate servers from their mobile phone when outside the office, but uploading files works without issue in the office. The user saw an error notification but dismissed it. Which of the following should a technician do to determine the root cause?

A. Check the data usage limit
B. Enable airplane mode
C. Verify the last device reboot
D. Enable Bluetooth connectivity

Answer: A

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
The user's issue likely stems from amobile data restriction or cap, especially since uploads work on Wi-Fi but not cellular. Checkingdata usage limitswill help determine if mobile uploads are blocked. FromAll-in-One Exam Guide:

"When data-intensive functions fail on mobile networks but not on Wi-Fi, it's often due to data caps or metered connection limits."

Question: 100

A user logs in to a computer each morning and tries to print a daily report, but it will not print. The help desk resolves the issue each day temporarily. To fix this permanently, which of the following should the technician do? (Select two)

A. Set the print spooler to have no dependencies
B. Set the print spooler recovery to take no action
C. Start the printer extensions and notifications service
D. Start the print spooler service
E. Set the print spooler to Automatic
F. Set the print spooler log-on to the user's account

Answer: D,E

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
The recurring print issue suggests theprint spooler service is not set to start automatically, causing it to stop between sessions. Ensuring it is set tostart automaticallyand manuallystarting the servicewill resolve the issue.
FromMark Soper – Mike Meyers' Lab Manual:
"The print spooler is essential for print services. If it isn't configured to start automatically, users may experience recurring failures."
"Manually starting the service or setting it to 'Automatic' in the Services panel resolves persistent print availability problems."

Question: 101

A technician completes the installation of an OS that appears to be successful. However, when the technician removes the USB drive that was used for the installation and restarts the system, the error "No boot device found" appears. Which of the following should the technician do next to resolve the issue?

A. Reinstall the OS from a new ISO
B. Enable UEFI devices in the BIOS
C. Restart in recovery mode and troubleshoot
D. Install storage drivers for the motherboard
E. Reseat the SATA cable

Answer: B

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
If the system fails to boot after removing the USB installation media, it often means the BIOS is not pointing to the correct boot device. This typically involves an issue with the BIOS settings—such as UEFI being disabled when the OS was installed in UEFI mode.
FromAll-in-One Exam Guideby Travis Everett:
"One of the most common post-installation issues is failing to configure the boot mode correctly in BIOS. If an OS is installed in UEFI mode, the UEFI boot must be enabled, otherwise the system won't detect the bootloader."

Question: 102

A user's application only works with a legacy version of the OS. The OS is reaching its end-of-life date. For security reasons, the company is migrating to the current version of the OS. Which of the following is the most efficient way to complete the migration while maintaining accessibility to the application?

A. Terminal server
B. Bare-metal server
C. Multiboot
D. Virtualization

Answer: D

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
Virtualizationallows the legacy OS to be run in a virtual machine (VM) on top of the newer OS. This method provides backward compatibility without requiring outdated operating systems on physical hardware.
FromQuentin Docter – CompTIA A+ Complete Study Guide:
"Using virtualization is a preferred method when legacy applications are needed after migrating to newer operating systems. It allows legacy environments to exist securely within a modern OS framework."

Question: 103

A Chief Executive Officer wants to meet with remote employees in a way that will allow for communication and training. Which of the following software technologies is the best for this situation?

A. Videoconferencing
B. Screen sharing
C. Remote Desktop
D. Virtual desktop infrastructure

Answer: A

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
Videoconferencingplatforms allow real-time face-to-face communication and are ideal for collaborative training sessions involving remote employees.
FromQuentin Docter – CompTIA A+ Complete Study Guide:
"Videoconferencing tools such as Zoom or Microsoft Teams are specifically designed for real-time communication and training, making them ideal for executive or large-group meetings."

Question: 104

When a corporate laptop is connected to the company network, it can reach external websites. However, it cannot reach any internal websites, displaying the error message "Cannot reach this page." Which of the following should a technician configure?

A. Subnet mask
B. DNS settings
C. Default gateway
D. DHCP

Answer: B

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
If internal resources (such as intranet or internal apps) can't be accessed but external sites work, this often points to aDNS issue, where the system isn't resolving internal domain names correctly.
FromAll-in-One Exam Guide:
"When internet access is functional but internal sites fail to load, the issue usually lies with DNS resolution. Internal resources often require internal DNS servers, which may not be configured correctly."

Question: 105

An international traveler is concerned about others accessing the contents of their smartphone if it is lost or stolen. The traveler has enabled biometrics. Which of the following additional security measures further reduces the risk of unauthorized data access?

A. Remote backups
B. Location tracking
C. PIN code screen lock
D. Device encryption

Answer: D

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

Device encryptionensures that even if someone bypasses biometrics or has physical access to the phone, they cannot read the stored data without the encryption key.

FromQuentin Docter – CompTIA A+ Complete Study Guide:

"Encryption is the most effective way to protect data at rest. Even if the device is lost or stolen, encryption ensures the data remains inaccessible without the correct key or passcode."

Question: 106

Which of the following is a protocol that provides AAA for network services?

A. RADIUS
B. Kerberos
C. TKIP
D. WPA3

Answer: A

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

RADIUS (Remote Authentication Dial-In User Service)provides centralized Authentication, Authorization, and Accounting (AAA) for users who connect and use a network service.

FromQuentin Docter – CompTIA A+ Complete Study Guide:

"RADIUS is a widely used protocol for implementing AAA in network environments, allowing centralized control over user access and accounting."

Question: 107

A customer's laptop will not turn on. The customer is distraught and panicking because the laptop contains family pictures that can never be replaced. Which of the following communication techniques is most important for the technician to demonstrate in this situation?

A. The technician should provide the customer with the appropriate SLA
B. The technician should inform the customer about replacement options for an increased cost
C. The technician should project confidence and maintain a positive attitude
D. The technician should be dressed in appropriate business casual attire

Answer: C

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

In emotionally sensitive situations, it is critical that the technicianprojects confidenceand maintains a calm, positive demeanor to reassure the customer.

FromAll-in-One Exam Guide:

"Confidence and empathy are key when working with distressed users. Demonstrating competence can help ease the customer's anxiety."

Question: 108

A technician is 3-D printing high-strength, carbon fiber-based filament parts for a customer order. Which of the following is the most important for the technician to use?

A. Steel-toed boots
B. Air filter mask
C. ESD mat
D. Antistatic bags

Answer: B

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

Carbon fiber filamentcan producefine particles or fumesduring printing, which may be harmful when inhaled. Wearing anair filter maskis essential to protect the respiratory system.

FromQuentin Docter – CompTIA A+ Complete Study Guide:

"When working with advanced materials like carbon fiber, always use appropriate personal protective equipment such as air filter masks to prevent inhalation of dangerous particles."

Question: 109

A client reports that their browser's home page changed. Every time they run an internet search, the results are returned from unfamiliar websites. Which of the following actions should a technician take first to resolve the issue? (Select two)

A. Clear the browsing history
B. Run operating system updates
C. Check the system date and time
D. Uninstall malicious extensions
E. Reset browser startup page
F. Restart the user's machine

Answer: D,E

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
The symptoms suggest abrowser hijacker. Thefirst stepsshould be toremove any malicious extensionsandreset the startup pageto restore normal behavior.
FromAll-in-One Exam Guide:
"Browser hijackers often install as extensions and change homepage settings. Removing these extensions and resetting the startup configuration typically resolves the issue."

Question: 110

A user reports that their corporate mobile phone is lost. Which of the following protects the data locally on the phone from unauthorized access?

A. Password manager
B. Degaussing
C. Remote wipe
D. Antivirus

Answer: C

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
Remote wipeis a mobile device management (MDM) feature that allows administrators to erase data remotely if a device is lost or stolen, preventing unauthorized access to corporate or personal information.
FromQuentin Docter – CompTIA A+ Complete Study Guide:
"Remote wipe features enable a device to be cleared of all sensitive data if it is lost or stolen. This is one of the most effective ways to prevent unauthorized access to corporate resources."

Question: 111

A technician is troubleshooting a print spooler that fails to start on a Windows 11 desktop computer. The technician determines the root cause is that required dependencies are failing to run. Which of the following tools is the technician using?

A. Process
B. Services
C. Startup
D. Performance

Answer: B

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
TheServicestool in Windows allows a technician to view service dependencies and status. If the print spooler can't start due to a dependency, Services is the correct tool to inspect and manage them. FromAll-in-One Exam Guide:
"The Services console allows technicians to view, start, and configure system services, including setting recovery actions and viewing dependencies."

Question: 112

Which of the following filesystems supports read and write operations for Windows, macOS, and Linux?

A. exFAT
B. ReFS
C. NTFS
D. APFS
E. ext4

Answer: A

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
exFATis the only listed file system that supports both read and write access across Windows, macOS, and Linux (with appropriate drivers). It's optimized for flash storage and external drives.
FromAll-in-One Exam Guide:
"exFAT is a lightweight file system with cross-platform read/write support, ideal for use on removable drives when compatibility is essential."

Question: 113

A technician installs a Bluetooth headset for a user. During testing, the sound still comes from the speaker on the computer. The technician verifies the headset shows up in Device Manager. Which of the following would the technician most likely do to fix this issue?

A. Update the drivers for the wireless headset
B. Replace the battery on the headset and try again later
C. Verify that the sound is not muted in the control panel
D. Change the headset as the default device in sound settings

Answer: D

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
Just recognizing the device isn't enough—audio output must be routed to it manuallyby setting it as the default playback device

in sound settings.

FromMark Soper – Mike Meyers' Lab Manual:

"If audio is still playing through the internal speaker, verify that the Bluetooth headset is set as the default playback device. This can be configured under Windows Sound Settings."

Question: 114

Which of the following authentication methods is the best way to prevent users from frequently entering their credentials?

A. Access control list
B. Single sign-on
C. Multifactor authentication
D. One-time password

Answer: B

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

Single sign-on (SSO)allows users to authenticate once and gain access to multiple systems without reentering credentials, which significantly enhances user convenience while maintaining security.

FromQuentin Docter – CompTIA A+ Complete Study Guide:

"Single sign-on streamlines authentication by allowing users to log in once and access all authorized resources, reducing credential fatigue and improving security."

Question: 115

A user wants to use a USB to move a 4.57GB .pst file from one Windows computer to another. Which of the following filesystems should the USB be formatted with?

A. ext4
B. NTFS
C. FAT32
D. APFS

Answer: B

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

FAT32cannot support files larger than 4GB.NTFSsupports large file sizes and is compatible across

Windows systems, making it the correct choice for transferring a 4.57GB file.

FromAll-in-One Exam Guide:

"NTFS is the preferred file system for large file transfers within Windows. FAT32 has a 4GB file size limit, which makes it

unsuitable for modern use cases involving large files."

Question: 116

An administrator is investigating a technical outage. The management team wants information that includes the summary of the outage and actions taken. Which of the following documentation should the administrator provide?

A. Knowledge base article
B. Non-disclosure agreement
C. Incident report
D. Standard operating procedure

Answer: C

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

Anincident reportsummarizes what happened during an outage, the timeline, the actions taken, and the resolution, which is exactly what management typically requests post-incident.

FromQuentin Docter – CompTIA A+ Complete Study Guide:

"Incident reports document the events of an IT issue or outage, including detection, response, and resolution. They are crucial for post-incident review and management accountability."

Question: 117

An administrator received an email stating that the OS they are currently supporting will no longer receive security updates and patches. Which of the following is the most likely reason?

A. Support from the computer's manufacturer is expiring
B. The OS will be considered end of life
C. The built-in security software is being removed from the next OS version
D. A new version of the OS will be released soon

Answer: B

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

When an OS is no longer receiving updates, it is generally because it has reachedend of life (EOL), meaning the vendor has ceased support.

FromQuentin Docter – CompTIA A+ Complete Study Guide:

"End-of-life refers to the point when an OS vendor no longer issues updates or support. Systems at EOL pose security risks and must be upgraded or isolated."

Question: 118

After using a third-party disk optimization software package, a technician restarts a laptop and receives the message “No operating system found.” The technician verifies that the BIOS properly recognizes the SSD. Which of the following should the technician do next?

A. Update BitLocker settings in the BIOS
B. Replace the CMOS battery
C. Boot from installation media and repair the MBR
D. Isolate the system from the corporate network

Answer: C

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

Disk optimization tools can sometimes corrupt theMaster Boot Record (MBR). If BIOS sees the drive but can't boot, repairing the MBR using installation media is the correct next step.

FromAll-in-One Exam Guide:

“When BIOS recognizes the drive but no OS is found, the issue is often with the boot record. Use installation media to access recovery tools and repair the MBR or boot loader.”

Question: 119

What is the next step a technician should take after completing malware cleanup?

A. Perform a secondary antivirus scan
B. Educate the end user
C. Reimage the computer
D. Review system logs

Answer: B

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

Once the system is cleaned, the next priority is toeducate the useron safe practices to prevent recurrence.

FromQuentin Docter – CompTIA A+ Complete Study Guide:

“Post-malware remediation should include user education to prevent reinfection and identify how the malware was introduced.”

Question: 120

A user wants to dispose of a failed hard drive in a way that ensures the data is unrecoverable. Which of the following is the best at-home method?

A. Standard formatting
B. Low-level formatting
C. Shredding
D. Degaussing
E. Drilling

Answer: C

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
Shreddingphysically destroys the platters, making data recovery virtually impossible. It's more effective and accessible than degaussing or low-level formatting.
FromQuentin Docter – CompTIA A+ Complete Study Guide:
"Physical destruction methods like shredding are the most secure options for ensuring data on failed drives cannot be recovered."

Question: 121

Various alerts on a user's Windows 11 laptop are continually interrupting videoconference calls.
Which of the following should a support technician recommend to best solve the issue?

A. Use multiple sound output devices for the various source applications
B. Disable all notifications in different applications in the order they appear
C. Configure the Sounds option in Control Panel to be set to No Sounds
D. Set Windows Notifications settings to Do Not Disturb

Answer: D

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
TheDo Not Disturbsetting in Windows Notification settings allows users to suppress all notification banners and sounds during presentations or video calls.
FromTravis Everett – All-in-One Exam Guide:
"Use Windows 'Do Not Disturb' to prevent notifications from interrupting full-screen apps like video conferencing."

Question: 122

A Windows 11 Home device is receiving constant pop-ups about an urgent need to update antivirus software in order to remove a detected threat. The user has been clicking the "X" button but the window keeps reappearing. The pop-up includes an "OK" button to install the update. What should the user do next?

A. Click the "OK" button to install the update
B. Reinstall the Windows Operating System
C. Run System File Checker
D. Verify the current status and settings of protection measures

Answer: D

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
Persistent pop-ups urging antivirus updates are likelyscareware or adware. The correct approach is toverify existing antivirus settings, run a trusted security scan, and avoid interacting with unknown pop-ups.
FromQuentin Docter – CompTIA A+ Complete Study Guide:
"Users should verify antivirus status using trusted tools before responding to alerts. Fake updates are common vectors for malware."

Question: 123

Performance on a user's smartphone is degrading. Applications take a long time to start, and switching between apps is slow. Which of the following diagnostic steps should a mobile technician take first?

A. Restore the phone to factory settings
B. Restart the phone
C. Check the phone's battery state
D. Uninstall unneeded applications

Answer: D

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
One of the most common causes for performance degradation on smartphones isstorage or memory overloaddue to excessive apps.Uninstalling unused appsis a basic but effective first diagnostic step. FromTravis Everett – All-in-One Exam Guide:
"Start troubleshooting sluggish smartphones by clearing unused apps and files before performing advanced diagnostics or resets."

Question: 124

A user takes an iOS-based smartphone to a repair shop due to performance issues. The technician observes:
Battery charge: 25%
Battery health: 90%
Hotspot: On
Used space: 63.76GB / 64GB
Which of the following is the most likely cause of the performance issue?

A. The device is running out of free space
B. The battery health is low
C. The phone is not sufficiently charged
D. The hotspot is degrading the performance
E. Too many applications are open

Answer: A

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
Running atnear full storage capacitysignificantly slows down smartphones. iOS in particular requires space for caching and temporary files. Performance improves when storage is cleared.
FromMike Meyers' Lab Manual:
“Lack of free space causes mobile operating systems to struggle with temp files and updates. Performance improves significantly with adequate storage.”

Question: 125

After a user installs a mobile application from an advertisement, the phone's battery dies a few hours later and becomes hot to touch, even when not in use. Which of the following should a technician do first?

A. Check for unauthorized device administrators
B. Contact the software developer
C. Run a mobile malware scan on the phone
D. Ensure appropriate MDM policies are applied

Answer: C

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
These symptoms strongly indicatemalware infectionor a malicious app running in the background.
The first action should be torun a malware scanto identify and remove malicious components.
FromQuentin Docter – CompTIA A+ Complete Study Guide:
“If a mobile device is overheating and the battery drains rapidly after installing an app, this could point to malware. Begin by scanning the device with a mobile anti-malware application.”

Question: 126

A user switches from Linux to Windows and tries to migrate data using an external USB drive.
Windows prompts that the device must be formatted. It works fine on Linux. What should the user do?

A. Configure Windows firewall to allow data from Linux systems
B. Replace the cable with Windows-supported hardware
C. Apply a firmware update from the PC manufacturer
D. Update the file allocation system to exFAT

Answer: D

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

Windows doesn't natively support many Linux file systems (like ext4).Reformatting to exFATmakes the drive readable/writable on both Linux and Windows.

FromAll-in-One Exam Guide:

"For cross-platform compatibility, exFAT is recommended as it supports large files and is recognized by Windows, macOS, and Linux (with exFAT drivers)."

Question: 127

Which of the following malware types typically has very high computing resource usage?

A. Rootkit
B. Cryptominer
C. Boot sector virus
D. Trojan

Answer: B

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

Cryptominersexploit system resources to mine cryptocurrency, often without user consent, leading to high CPU and GPU usage.

FromQuentin Docter – CompTIA A+ Complete Study Guide:

"Cryptomining malware can cause significant performance degradation by monopolizing system resources like CPU and GPU to mine digital currency."

Question: 128

A Microsoft OS laptop user frequently forgets their password. Which alternative login method should a technician enable?

A. Single sign-on
B. Windows Hello
C. BitLocker
D. User Account Control

Answer: B

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

Windows Helloallows biometric and PIN-based login, which are easier and more user-friendly than passwords.

FromQuentin Docter – CompTIA A+ Complete Study Guide:

"Windows Hello supports biometric authentication and PINs, providing easier and secure access especially for users who have trouble remembering passwords."

Question: 129

A user's computer is running slowly. Task Manager shows:
Disk: 2%
Network: 12%
GPU: 15%
CPU: 70%
Memory: 97%
Which of the following would a technician most likely do to resolve the issue?

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:

Memory usage is critically high, suggesting many applications or background processes. Closing unnecessary programs will immediately free up RAM.

FromTravis Everett – All-in-One Exam Guide:

"High memory usage with moderate CPU load usually means too many applications are open. Close unnecessary apps or use Task Manager to end processes."

Question: 130

Which of the following concepts should a technician consider when discussing confidential work projects with individuals outside the company?

A. EULA
B. EOL
C. SLA
D. NDA

Answer: D

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

AnNDA (Non-Disclosure Agreement)is used to ensure confidentiality of sensitive company information, especially when interacting with external parties.

FromQUENTIN DOCTER - COMPTIA A+ COMPLETE study GUIDE:

"An NDA ensures that confidential information is not disclosed to unauthorized individuals, especially important in external communications."

Question: 131

Technicians are failing to document user contact information, device asset tags, and a clear description of each issue in the ticketing system. What should the help desk management implement?

A. Service-level agreements
B. Call categories
C. Standard operating procedures
D. Knowledge base articles

Answer: C

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

Standard Operating Procedures (SOPs)guide technicians through consistent and complete processes, including documentation.

FromTravis Everett – All-in-One Exam Guide:

"SOPs ensure that all required steps—such as data collection and issue description—are followed in every support interaction."

Question: 132

A secretary receives an email from the CEO requesting immediate vendor payment. Later, the CEO says they never sent it. Which social engineering tactic is this?

A. Evil twin
B. Impersonation
C. Whaling
D. Spear phishing

Answer: D

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

Spear phishingtargets a specific individual using personalized tactics, as seen in emails impersonating a CEO to deceive a secretary.

FromQUENTIN DOCTER - COMPTIA A+ COMPLETE study GUIDE:

"Spear phishing targets specific individuals or roles within an organization using tailored messages to increase success rates."

Question: 133

The battery on a user's smartphone discharges quickly during travel. The phone was replaced two weeks ago. What should the technician do first?

A. Replace the battery with a higher capacity option

B. Provide an external battery
C. Ensure the charging port is working
D. Look for applications that are reporting the highest utilization

Answer: D

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

Apps like GPS or roaming services often drain battery during travel.Checking app utilizationhelps identify battery drain sources.

FromQUENTIN DOCTER - COMPTIA A+ COMPLETE study GUIDE:

"Monitoring app activity can reveal high-power usage apps running in the background, especially when mobile data or GPS is active."

Question: 134

A technician reviews an organization's incident management policy. The organization uses a third-party vendor with multiple tools to protect its assets. What service type is this?

A. PaaS
B. EDR
C. MDR
D. XDR

Answer: C

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

Managed Detection and Response (MDR)involves outsourcing security monitoring to a third-party that uses multiple tools and analytics.

FromTravis Everett – All-in-One Exam Guide:

"MDR providers handle threat detection and response using a combination of advanced tools, analytics, and expert personnel."

Question: 135

An employee is trying to connect their company laptop to airport Wi-Fi. A pop-up with the airport logo appeared and was closed quickly. The internet does not work. What should a help desk technician suggest?

A. Look for a wall socket with RJ45 and try to connect
B. Contact the airport IT department
C. Tell the employee that company policy prohibits connection to public Wi-Fi
D. Reconnect to the network and read the pop-up carefully

Answer: D

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
Public Wi-Fi networks often usecaptive portals, which require accepting terms or authenticating via the pop-up page before full access is granted. Closing it prematurely stops full connection.
FromTravis Everett – All-in-One Exam Guide:
"Captive portals intercept the first HTTP request and present a login or acknowledgment screen. Without completing it, access is denied."

Question: 136

A technician needs to disable guest log-ins on domain-joined desktop machines. Which of the following should be used?

A. Group Policy
B. Firewall
C. Microsoft Management Console
D. MSConfig

Answer: A

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
Group Policyis the standard administrative tool for setting user permissions across domain-joined systems.
FromQUENTIN DOCTER – COMPLETE Study Guide:
"Use Group Policy to enforce user rights, including disabling guest account access on domain computers."

Question: 137

A user cannot upload files to corporate servers from their mobile device when outside the office, but uploads work fine in-office. What should a technician do to determine the root cause?

A. Check the data usage limit
B. Enable airplane mode
C. Verify the last device reboot
D. Enable Bluetooth connectivity

Answer: A

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
If uploading fails only offsite,mobile data limits or restrictionsare the likely cause. Data caps or network management can

interfere with uploads.

FromTravis Everett – All-in-One Exam Guide:

"When mobile users experience network issues, always check if the device has reached a data cap or roaming restriction."

Question: 138

A user logs in daily and cannot print a report. Help desk fixes it each day, but the issue recurs. What should be done so the issue doesn't recur? (Select two)

A. Set the print spooler to have no dependencies
B. Set the print spooler recovery to take no action
C. Start the printer extensions and notifications service
D. Start the print spooler service
E. Set the print spooler to Automatic
F. Set the print spooler log-on to the user's account

Answer: D,E

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

For persistent printing issues due to spooler service, ensure theprint spooler is started and set to Automatic. This maintains print capability across reboots.

FromMike Meyers' Lab Manual:

"If users lose printing capabilities on reboot, the print spooler service must be configured to start automatically and be confirmed as running."

Question: 139

A technician is installing a cloud-based productivity suite and gets an error saying the installation is unavailable. What should be tried first?

A. Reinstall the productivity suite
B. Download an open-source alternative
C. Check the license device limit
D. Update the device OS

Answer: C

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

Cloud-based software often enforcesdevice limitsper license. Before reinstallation or switching software, checking license allocations is the most logical first step.

FromQuentin Docter – CompTIA A+ Complete Study Guide:

"Many cloud apps enforce user or device count restrictions. When an install fails, check licensing before troubleshooting other areas."

Question: 140

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

A. Implement the change
B. Approve the change
C. Document the change
D. Schedule the change

Answer: C

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

Before any change is implemented, it must bedocumentedas part of change management procedures. This ensures transparency, review, and tracking.

FromQuentin Docter – CompTIA A+ Complete Study Guide:

"Documenting a change is the first step in change management. This includes defining the scope, purpose, impact, and implementation plan before approval or scheduling."

Question: 141

After installing new webcam software, a PC experiences BSOD during videoconference calls. What should the technician do next?

A. Update the anti-malware signature and scan the system
B. File a warranty claim with the manufacturer
C. Start in Safe Mode and roll back the device driver
D. Reconnect the webcam to the computer

Answer: C

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

BSOD after driver installation suggests a compatibility issue.Safe Mode allows rollback of driversthat may be causing the crash.

FromTravis Everett – CompTIA A+ All-in-One Exam Guide:

"If a BSOD occurs after a driver update, boot into Safe Mode and roll back to the previous driver version to restore system stability."

Question: 142

A technician needs to change hibernation settings on a Windows computer via a batch file. Domain policies are unavailable. Which is the best method?

A. Use Power Options in Control Panel
B. Update the computer's firmware
C. Run gpupdate from command prompt
D. Use the powercfg command in PowerShell

Answer: D

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

Thepowercfg commandis a built-in utility for controlling power settings including hibernation. It can be used in scripts and does not require domain access.

FromQUENTIN DOCTER - COMPTIA A+ COMPLETE study GUIDE:

"The powercfg command provides granular control of power settings, useful for scripting and configuring systems without Group Policy access."

Question: 143

A user is unable to use the latest version of an app on a legacy tablet. What is the most likely reason?

A. The OS is end-of-life
B. Space is inadequate
C. MDM is blocking updates
D. The tablet is infected with malware

Answer: A

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

Older tablets may not support newer app versions due toincompatible or unsupported operating systems. App developers often drop support for outdated OS versions.

FromTravis Everett – CompTIA A+ All-in-One Exam Guide:

"When an app won't install on an older device, check the OS version. Most apps require a minimum OS level for compatibility and security."

Question: 144

A desktop technician is mapping a remote Windows share \\WinNAS\shared as local drive Z:. Which command should the technician run?

A. nslookup -opt 3: \WinNAS\shared
B. net use 3: \WinNAS\shared
C. chkdsk /R 2: \WinNAS\shared
D. sfc /offwindir 3: \WinNAS\shared

Answer: A,B,C,D

Explanation:

The correct syntax for mapping a network drive in Windows is:

net use Z: \\WinNAS\shared
This command connects the specified network share and maps it as drive Z:.
FromTravis Everett – CompTIA A+ All-in-One Exam Guide:
"Use net use followed by the desired drive letter and the UNC path to map network shares."

Question: 145

A technician uses AI to draft a document about new software benefits. Upon reading, the technician sees factually incorrect info. What term best describes this?

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

Answer: B

Explanation:

In AI terminology,hallucinationrefers to generated output that appears plausible but is factually incorrect.
FromQuentin Docter – CompTIA A+ Complete Study Guide:
"AI hallucination describes output that is fluent and coherent but includes information that is entirely fabricated or inaccurate."

Question: 146

A technician needs to download and install a new web browser on a desktop. Which attribute should be used to verify the installer's authenticity?

A. Date B. Hash C. Size
D. Name

Answer: B

Explanation:

Hash values(like SHA256) are published by vendors to verify file integrity. A match confirms the file hasn't been tampered with.
FromTravis Everett – CompTIA A+ All-in-One Exam Guide:
"Use hash values to ensure downloaded software matches the vendor's published version and hasn't been modified."

Question: 147

A town clerk wants to work from home and access documents on a town hall server. What should a technician set up?

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

Answer: C

Explanation:

AVPN (Virtual Private Network)creates a secure tunnel between the clerk's home device and the town server, ensuring private and authenticated access.
FromQuentin Docter – CompTIA A+ Complete Study Guide:
"VPNs are essential for remote access to internal resources, providing secure connections over public networks."

Question: 148

A technician follows proper malware removal procedures but cannot remove all malware. They decide to reload the OS. What should they select?

A. Version upgrade
B. System restore
C. OS repair
D. Clean install

Answer: D

Explanation:

Aclean installensures all malware is eliminated by completely wiping and reinstalling the OS. System restore or repair may leave traces.
FromQUENTIN DOCTER - COMPTIA A+ COMPLETE study GUIDE:
"If malware cannot be completely removed, perform a clean installation of the operating system.

This ensures no remnants remain on the machine."

Question: 149

What is found in an MSDS (Material Safety Data Sheet) for a battery backup?

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

Answer: B

Explanation:

An MSDS providessafety and emergency procedures, such as what to do if a battery leaks or catches fire. It is not a technical or setup guide.

FromTravis Everett – CompTIA A+ All-in-One Exam Guide:

"An MSDS contains safety information, including handling, storage, and emergency procedures related to potentially hazardous components like UPS batteries."

Question: 150

A technician is securing a newly deployed workstation. Only authorized users should access it. Which actions should the technician take? (Select two)

A. Defragment the hard drive
B. Enable SSH
C. Enable screensaver locks
D. Disable iCloud integration
E. Enable the firewall
F. Apply the BIOS password

Answer: C,F

Explanation:

Screensaver lockshelp protect unattended workstations.

BIOS passwordsprevent unauthorized changes at startup or during boot.

FromQUENTIN DOCTER - COMPTIA A+ COMPLETE study GUIDE:

"Applying a BIOS password adds a pre-boot security layer. Screensaver locks help protect logged-in sessions during idle times."

Question: 151

A user reports that the time on their computer does not match the time on their VoIP phone. What should a technician do?

A. Confirm the user is logging in to the domain.
B. Manually set the time on the phone to match the computer.
C. Download and install the latest BIOS update.
D. Configure access to an available NTP server.

Answer: D

Explanation:

This scenario involves a mismatch in device time settings, which can affect synchronization and authentication across the network. Using a Network Time Protocol (NTP) server ensures all networked devices maintain accurate and synchronized clocks.
From Travis Everett – All-in-One Exam Guide:
"NTP servers keep all devices on a network in sync. This prevents time drift, which can cause authentication issues with domain logins, certificates, and applications." .

Question: 152

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

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: 153

An administrator must rename the administrator account on a Windows desktop. Which tool is best for this?

A. lusrmgr.msc
B. devmgmt.msc
C. gpedit.msc

D. eventvwr.msc

Answer: A

Explanation:

The Local Users and Groups Manager (lusrmgr.msc) is the utility for managing user accounts, including renaming the default Administrator.

From Quentin Docter – Complete Study Guide:

"The lusrmgr.msc snap-in allows renaming and managing local user accounts, including the default administrator." .

Question: 154

Multiple users clicked a phishing link from a compromised email account. The security team isolates and removes the threat. Then, the management team provides security awareness training to the company. What step is this?

A. Provide user education.
B. Compile lessons learned.
C. Update the antivirus software.
D. Perform additional scans.

Answer: A

Explanation:

This is part of the user education step after a security incident to prevent future occurrences.

From Quentin Docter – Complete Study Guide:

"User education and awareness is a crucial part of preventing phishing attacks. After an incident, it is vital to train users on recognizing suspicious messages." .

Question: 155

An administrator is investigating a zero-day vulnerability. If left unpatched, it could severely impact business. The patch requires downtime. What should the administrator do?

A. Create a standard change request.
B. Implement an emergency change.
C. Immediately freeze all changes.
D. Continue operations until the next change interval.

Answer: B

Explanation:

A zero-day vulnerability demands an emergency change to quickly secure the system, even if downtime is needed.

From Mike Meyers' Lab Manual:
"Emergency changes bypass standard scheduling to quickly address critical vulnerabilities that pose immediate risks." .

Question: 156

An organization sees unauthorized apps installed and licensing prompts. What should the security team do?

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:

Removing users from the local admin group prevents them from installing unauthorized software.
From Quentin Docter – Complete Study Guide:
"Local admin privileges allow users to install unauthorized apps. Removing them from this group restricts installations and helps prevent malware." .

Question: 157

Why would a network engineering team provide a help desk technician with IP addresses for a wired network segment?

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

Answer: C

Explanation:

When DHCP isn't enabled, static IPs must be assigned manually, so the engineering team provides the IP details.
From Travis Everett – All-in-One Exam Guide:
"If DHCP is unavailable, technicians need the static IP configuration to connect devices to the network." .