CompTIA

Exam Questions 220-1202

CompTIA A+ Certification Exam: Core 2

NEW QUESTION 1
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
==========

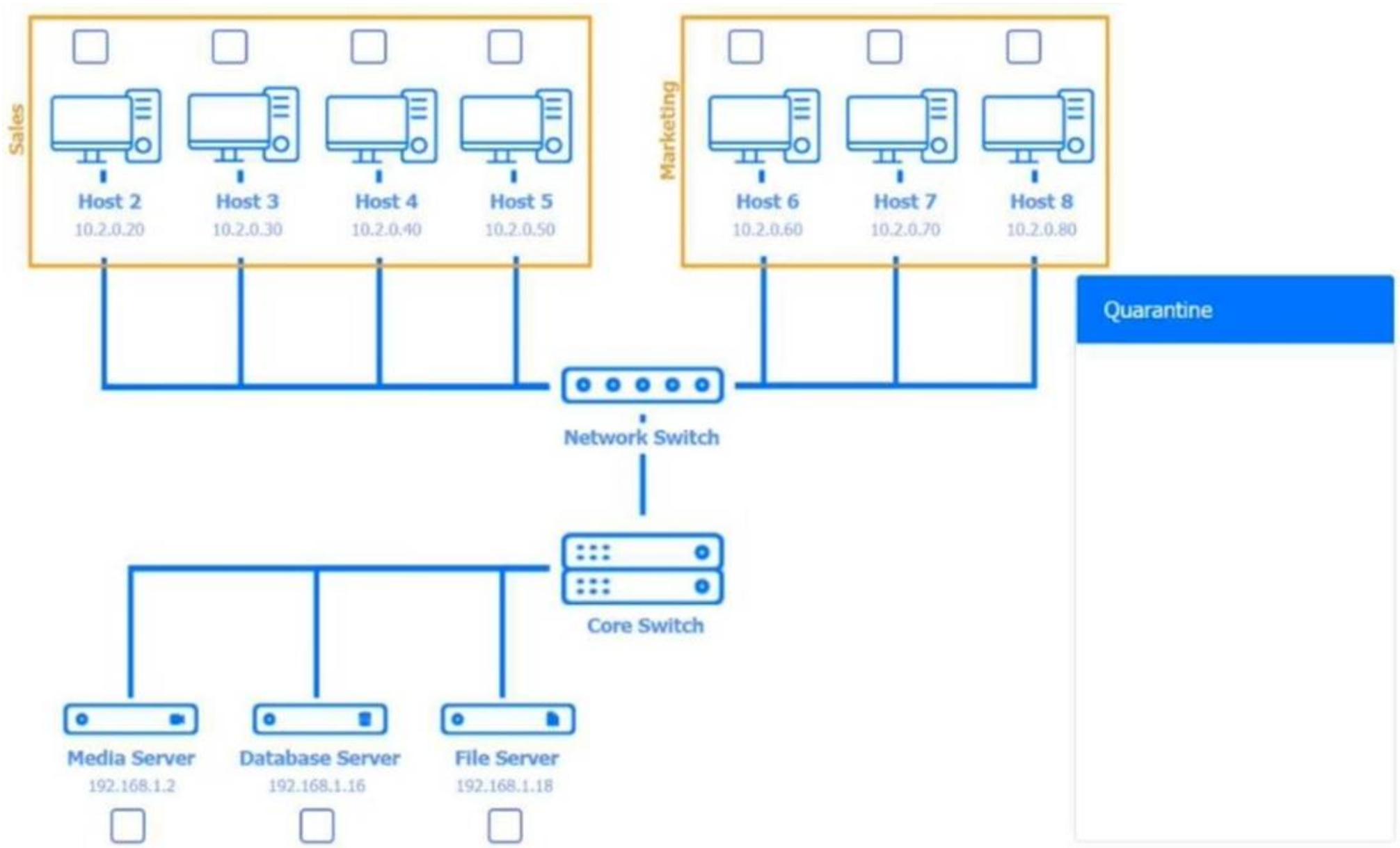
NEW QUESTION 2
The screen of a previously working computer repeatedly displays an OS Not Found error message when the computer is started. Only a USB drive, a keyboard, and a mouse are plugged into the computer. Which of the following should a technician do first?

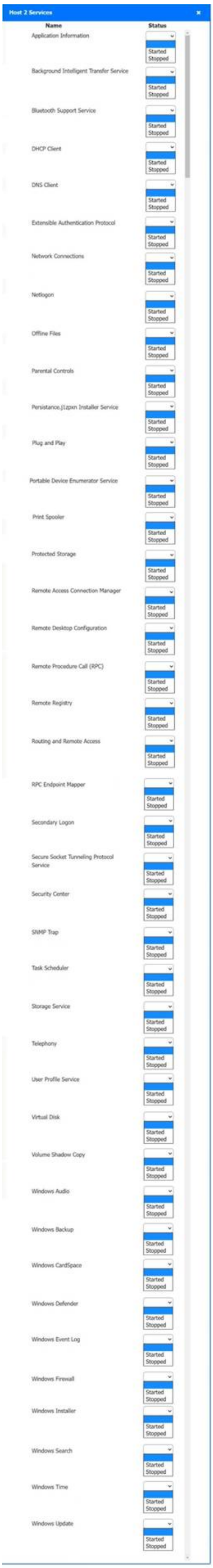
A. Run data recovery tools on the disk
B. Partition the disk using the GPT format
C. Check boot options
D. Switch from UEFI to BIOS

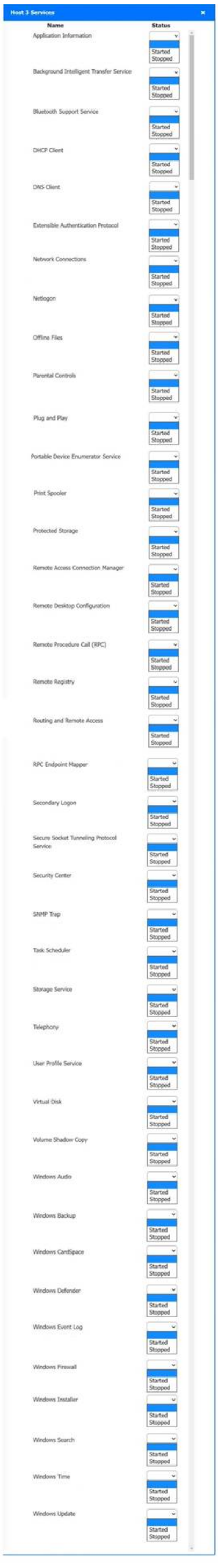
Answer: C

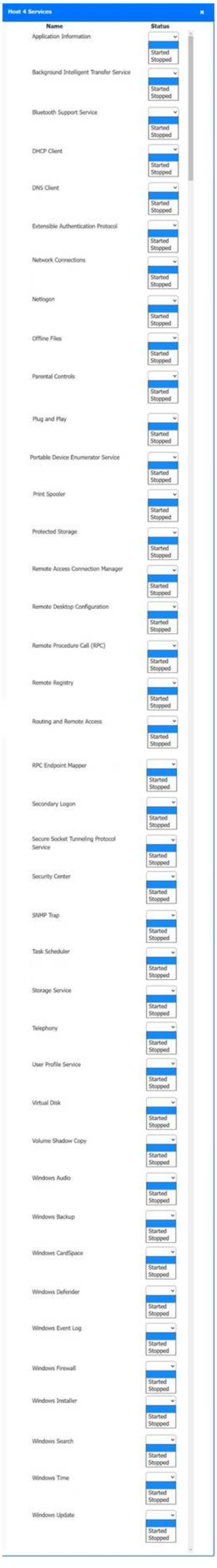
Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
An "OS Not Found" error typically indicates that the computer is attempting to boot from a drive that doesn't contain a valid operating system or bootable partition. The presence of a USB drive might be confusing the boot order.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

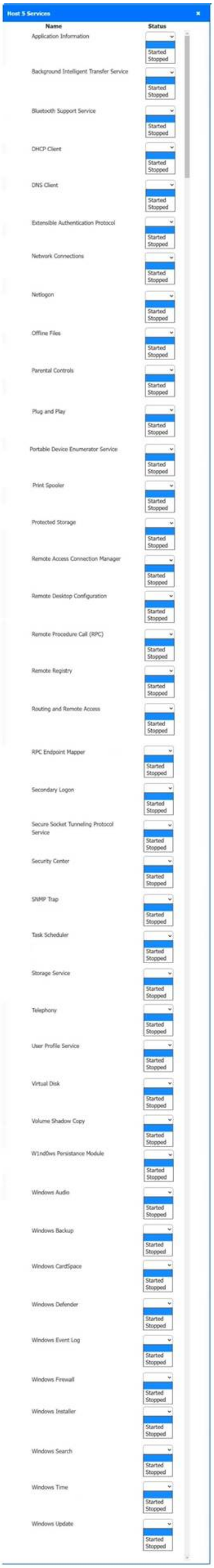
NEW QUESTION 3
SIMULATION
Multiple users are reporting audio issues as well as performance issues after downloading unauthorized software. You have been dispatched to identify and resolve any issues on the network using best practice procedures.
INSTRUCTIONS
Quarantine and configure the appropriate device(s) so that the users?? audio issues are resolved using best practice procedures.
Multiple devices may be selected for quarantine. Click on a host or server to configure services.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

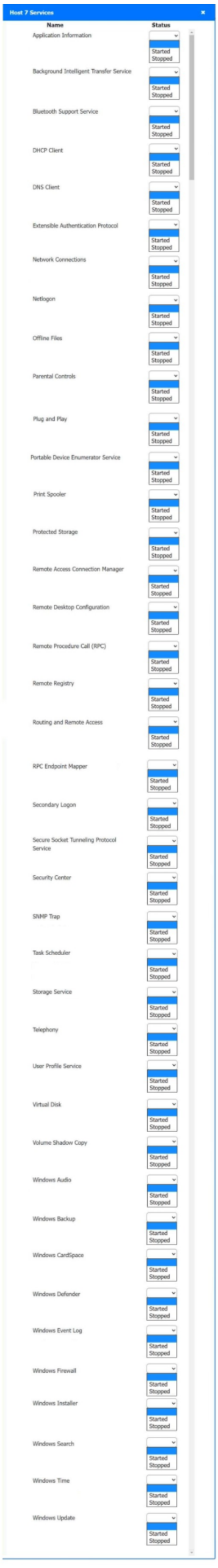

Sales
Host 2
10.2.0.20
Host 3
10.2.0.30
Host 4
10.2.0.40
Host 5
10.2.0.50
Marketing
Host 6
10.2.0.60
Host 7
10.2.0.70
Host 8
10.2.0.80
Quarantine
Network Switch
Core Switch
Media Server
192.168.1.2
Database Server
192.168.1.16
File Server
192.168.1.18

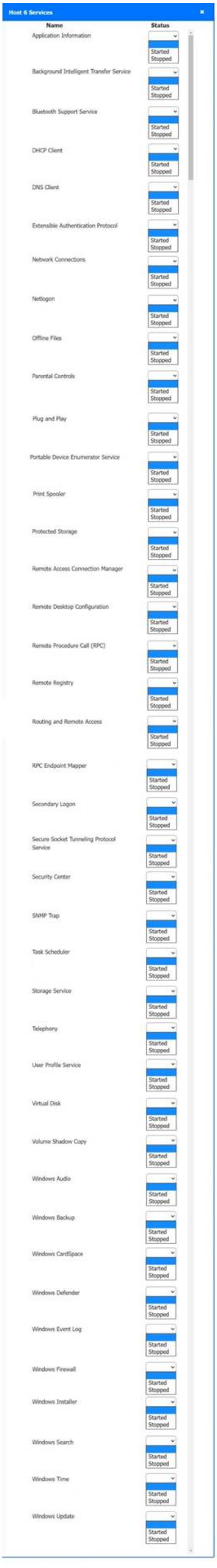

Host 2 Services
Name
Status
Application Information
Background Intelligent Transfer Service
Bluetooth Support Service
DHCP Client
DNS Client
Extensible Authentication Protocol
Network Connections
Netlogon
Offline Files
Parental Controls
Persistance.j1zpxn Installer Service
Plug and Play
Portable Device Enumerator Service
Print Spooler
Protected Storage
Remote Access Connection Manager
Remote Desktop Configuration
Remote Procedure Call (RPC)
Remote Registry
Routing and Remote Access
RPC Endpoint Mapper
Secondary Logon
Secure Socket Tunneling Protocol Service
Security Center
SNMP Trap
Task Scheduler
Storage Service
Telephony
User Profile Service
Virtual Disk
Volume Shadow Copy
Windows Audio
Windows Backup
Windows CardSpace
Windows Defender
Windows Event Log
Windows Firewall
Windows Installer
Windows Search
Windows Time
Windows Update
Started
Stopped

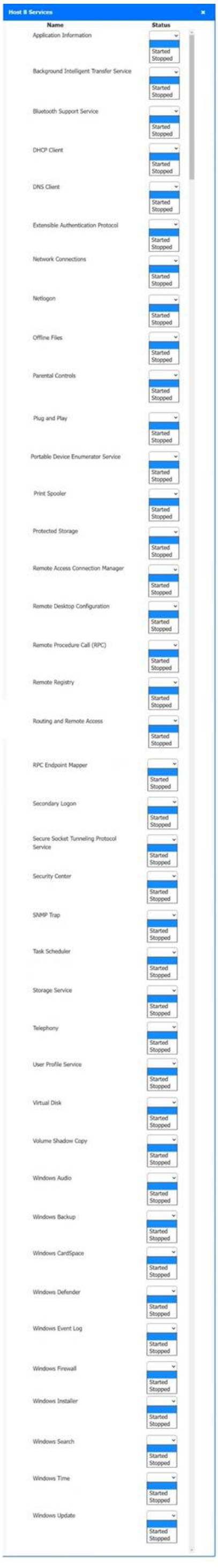

Host 3 Services
Name
Status
Application Information
Background Intelligent Transfer Service
Bluetooth Support Service
DHCP Client
DNS Client
Extensible Authentication Protocol
Network Connections
Netlogon
Offline Files
Parental Controls
Plug and Play
Portable Device Enumerator Service
Print Spooler
Protected Storage
Remote Access Connection Manager
Remote Desktop Configuration
Remote Procedure Call (RPC)
Remote Registry
Routing and Remote Access
RPC Endpoint Mapper
Secondary Logon
Secure Socket Tunneling Protocol Service
Security Center
SNMP Trap
Task Scheduler
Storage Service
Telephony
User Profile Service
Virtual Disk
Volume Shadow Copy
Windows Audio
Windows Backup
Windows CardSpace
Windows Defender
Windows Event Log
Windows Firewall
Windows Installer
Windows Search
Windows Time
Windows Update
Started
Stopped

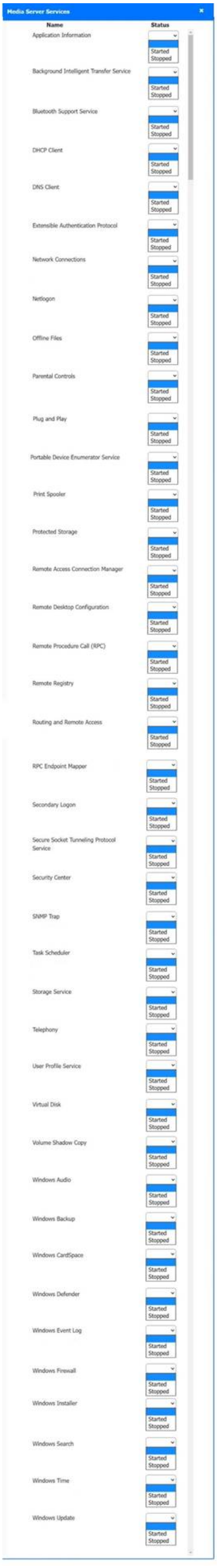

Host 4 Services
Name
Status
Application Information
Background Intelligent Transfer Service
Bluetooth Support Service
DHCP Client
DNS Client
Extensible Authentication Protocol
Network Connections
Netlogon
Offline Files
Parental Controls
Plug and Play
Portable Device Enumerator Service
Print Spooler
Protected Storage
Remote Access Connection Manager
Remote Desktop Configuration
Remote Procedure Call (RPC)
Remote Registry
Routing and Remote Access
RPC Endpoint Mapper
Secondary Logon
Secure Socket Tunneling Protocol Service
Security Center
SNMP Trap
Task Scheduler
Storage Service
Telephony
User Profile Service
Virtual Disk
Volume Shadow Copy
Windows Audio
Windows Backup
Windows CardSpace
Windows Defender
Windows Event Log
Windows Firewall
Windows Installer
Windows Search
Windows Time
Windows Update
Started
Stopped

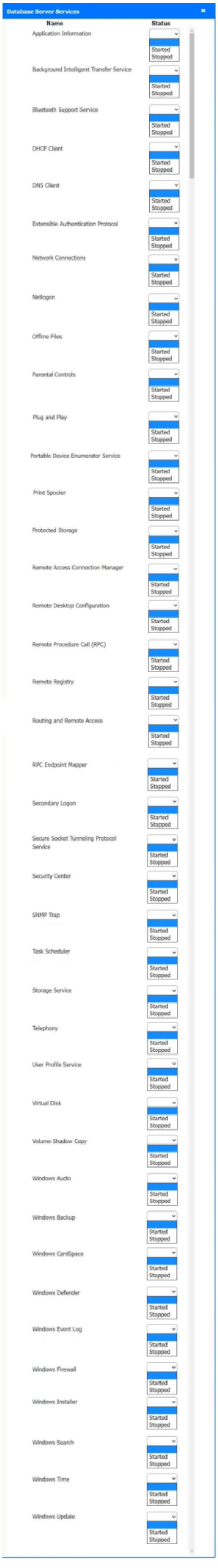

Host 5 Services
Name
Status
Application Information
Background Intelligent Transfer Service
Bluetooth Support Service
DHCP Client
DNS Client
Extensible Authentication Protocol
Network Connections
Netlogon
Offline Files
Parental Controls
Plug and Play
Portable Device Enumerator Service
Print Spooler
Protected Storage
Remote Access Connection Manager
Remote Desktop Configuration
Remote Procedure Call (RPC)
Remote Registry
Routing and Remote Access
RPC Endpoint Mapper
Secondary Logon
Secure Socket Tunneling Protocol Service
Security Center
SNMP Trap
Task Scheduler
Storage Service
Telephony
User Profile Service
Virtual Disk
Volume Shadow Copy
W1nd0ws Persistance Module
Windows Audio
Windows Backup
Windows CardSpace
Windows Defender
Windows Event Log
Windows Firewall
Windows Installer
Windows Search
Windows Time
Windows Update
Started
Stopped

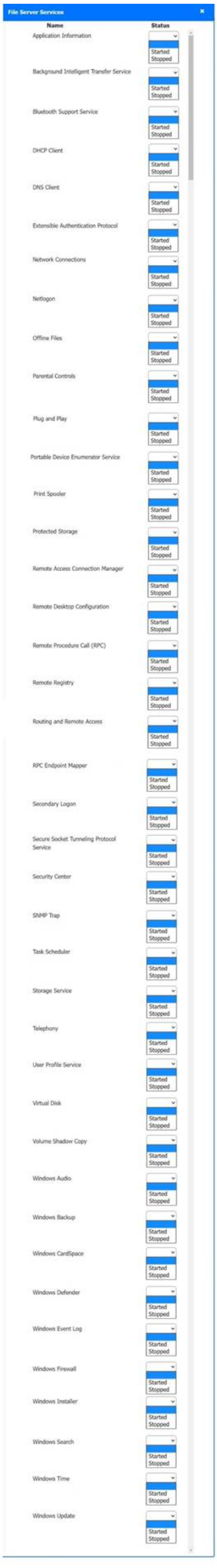

Host 7 Services
Name
Status
Application Information
Background Intelligent Transfer Service
Bluetooth Support Service
DHCP Client
DNS Client
Extensible Authentication Protocol
Network Connections
Netlogon
Offline Files
Parental Controls
Plug and Play
Portable Device Enumerator Service
Print Spooler
Protected Storage
Remote Access Connection Manager
Remote Desktop Configuration
Remote Procedure Call (RPC)
Remote Registry
Routing and Remote Access
RPC Endpoint Mapper
Secondary Logon
Secure Socket Tunneling Protocol Service
Security Center
SNMP Trap
Task Scheduler
Storage Service
Telephony
User Profile Service
Virtual Disk
Volume Shadow Copy
Windows Audio
Windows Backup
Windows CardSpace
Windows Defender
Windows Event Log
Windows Firewall
Windows Installer
Windows Search
Windows Time
Windows Update
Started
Stopped


Host 6 Services
Name
Status
Application Information
Background Intelligent Transfer Service
Bluetooth Support Service
DHCP Client
DNS Client
Extensible Authentication Protocol
Network Connections
Netlogon
Offline Files
Parental Controls
Plug and Play
Portable Device Enumerator Service
Print Spooler
Protected Storage
Remote Access Connection Manager
Remote Desktop Configuration
Remote Procedure Call (RPC)
Remote Registry
Routing and Remote Access
RPC Endpoint Mapper
Secondary Logon
Secure Socket Tunneling Protocol Service
Security Center
SNMP Trap
Task Scheduler
Storage Service
Telephony
User Profile Service
Virtual Disk
Volume Shadow Copy
Windows Audio
Windows Backup
Windows CardSpace
Windows Defender
Windows Event Log
Windows Firewall
Windows Installer
Windows Search
Windows Time
Windows Update
Started
Stopped


Host 8 Services
Name
Status
Application Information
Background Intelligent Transfer Service
Bluetooth Support Service
DHCP Client
DNS Client
Extensible Authentication Protocol
Network Connections
Netlogon
Offline Files
Parental Controls
Plug and Play
Portable Device Enumerator Service
Print Spooler
Protected Storage
Remote Access Connection Manager
Remote Desktop Configuration
Remote Procedure Call (RPC)
Remote Registry
Routing and Remote Access
RPC Endpoint Mapper
Secondary Logon
Secure Socket Tunneling Protocol Service
Security Center
SNMP Trap
Task Scheduler
Storage Service
Telephony
User Profile Service
Virtual Disk
Volume Shadow Copy
Windows Audio
Windows Backup
Windows CardSpace
Windows Defender
Windows Event Log
Windows Firewall
Windows Installer
Windows Search
Windows Time
Windows Update
Started
Stopped


Media Server Services
Name
Status
Application Information
Background Intelligent Transfer Service
Bluetooth Support Service
DHCP Client
DNS Client
Extensible Authentication Protocol
Network Connections
Netlogon
Offline Files
Parental Controls
Plug and Play
Portable Device Enumerator Service
Print Spooler
Protected Storage
Remote Access Connection Manager
Remote Desktop Configuration
Remote Procedure Call (RPC)
Remote Registry
Routing and Remote Access
RPC Endpoint Mapper
Secondary Logon
Secure Socket Tunneling Protocol Service
Security Center
SNMP Trap
Task Scheduler
Storage Service
Telephony
User Profile Service
Virtual Disk
Volume Shadow Copy
Windows Audio
Windows Backup
Windows CardSpace
Windows Defender
Windows Event Log
Windows Firewall
Windows Installer
Windows Search
Windows Time
Windows Update
Started
Stopped


Database Server Services
Name
Status
Application Information
Background Intelligent Transfer Service
Bluetooth Support Service
DHCP Client
DNS Client
Extensible Authentication Protocol
Network Connections
Netlogon
Offline Files
Parental Controls
Plug and Play
Portable Device Enumerator Service
Print Spooler
Protected Storage
Remote Access Connection Manager
Remote Desktop Configuration
Remote Procedure Call (RPC)
Remote Registry
Routing and Remote Access
RPC Endpoint Mapper
Secondary Logon
Secure Socket Tunneling Protocol Service
Security Center
SNMP Trap
Task Scheduler
Storage Service
Telephony
User Profile Service
Virtual Disk
Volume Shadow Copy
Windows Audio
Windows Backup
Windows CardSpace
Windows Defender
Windows Event Log
Windows Firewall
Windows Installer
Windows Search
Windows Time
Windows Update
Started
Stopped


File Server Services
Name
Status
Application Information
Background Intelligent Transfer Service
Bluetooth Support Service
DHCP Client
DNS Client
Extensible Authentication Protocol
Network Connections
Netlogon
Offline Files
Parental Controls
Plug and Play
Portable Device Enumerator Service
Print Spooler
Protected Storage
Remote Access Connection Manager
Remote Desktop Configuration
Remote Procedure Call (RPC)
Remote Registry
Routing and Remote Access
RPC Endpoint Mapper
Secondary Logon
Secure Socket Tunneling Protocol Service
Security Center
SNMP Trap
Task Scheduler
Storage Service
Telephony
User Profile Service
Virtual Disk
Volume Shadow Copy
Windows Audio
Windows Backup
Windows CardSpace
Windows Defender
Windows Event Log
Windows Firewall
Windows Installer
Windows Search
Windows Time
Windows Update
Started
Stopped

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Host 2, Host 3, Host 4 , Host 5 ,Host 6, Host 7, Host 8 , Media Server - Stop All unwanted and malicious service (Persistance.j1zpxn Installer Service) from all the listed host and Media servers
Refer screenshot below on the required service started/stopped on host2, same service to be started and stopped across all host servers.

NEW QUESTION 4
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
==========

NEW QUESTION 5
A company would like to deploy baseline images to new computers as they are started up on the network. Which of the following boot processes should the company use for this task?

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

Answer: D

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

NEW QUESTION 6
A technician is attempting to join a workstation to a domain but is receiving an error message stating the domain cannot be found. However, the technician is able to ping the server and access the internet. Given the following information:
? IP Address – 192.168.1.210
? Subnet Mask – 255.255.255.0
? Gateway – 192.168.1.1
? DNS1 – 8.8.8.8
? DNS2 – 1.1.1.1
? Server – 192.168.1.10
Which of the following should the technician do to fix the issue?

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

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The issue described—??domain cannot be found?? despite the ability to ping the server and access the internet—indicates aDNS resolution problem, not a network connectivity issue. The workstation is currently usingpublic DNS servers (8.8.8.8 and 1.1.1.1)which cannot resolve internal domain names, such as the ones used

in Active Directory environments. To resolve this, the technician needs tochange the DNS settings to point to the internal DNS server, which in most domain setups is thedomain controller itself (likely 192.168.1.10 in this case).
Here??s the breakdown of the incorrect options:
? B. Assign a static IP address: The IP is already assigned and functioning; the
device can ping and reach the network and internet.
? C. Configure a subnet mask: The subnet mask is appropriate for the network range (Class C /24).
? D. Update the default gateway: The gateway is valid and allows internet access; this is not the issue.
CompTIA A+ 220-1102 Core 2 Objective Reference:
Objective 1.8 – Given a scenario, use features and tools of the operating system. Under this objective, candidates must know how to troubleshoot OS-based network configurations, includingproper DNS settings in domain environments.

NEW QUESTION 7
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
==========

NEW QUESTION 8
A company wants to use a single operating system for its workstations and servers and avoid licensing fees. Which of the following operating systems would the company most likely select?

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

Answer: A

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

NEW QUESTION 9
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
==========

NEW QUESTION 10

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
==========

NEW QUESTION 10
A technician needs to map a shared drive from a command-line interface. Which of the following commands should the technician use?

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

Answer: C

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

NEW QUESTION 12
Which of the following prevents forced entry into a building?

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

Answer: D

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

NEW QUESTION 15
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

NEW QUESTION 17
Which of the following methods involves requesting a user's approval via a push notification to verify the user's identity?

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

Answer: B

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

NEW QUESTION 19
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

NEW QUESTION 22
A technician is using a credential manager to safeguard a large number of credentials. Which of the following is important for using this application?

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

Answer: B

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

NEW QUESTION 27
Which of the following is found in an MSDS sheet for a battery backup?

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

Answer: B

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

NEW QUESTION 28
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)

NEW QUESTION 32
Which of the following is used to apply corporate restrictions on an Apple device?

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

Answer: D

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

NEW QUESTION 33
A user is experiencing issues with outdated images while browsing websites. Which of the following settings should a technician use to correct this issue?

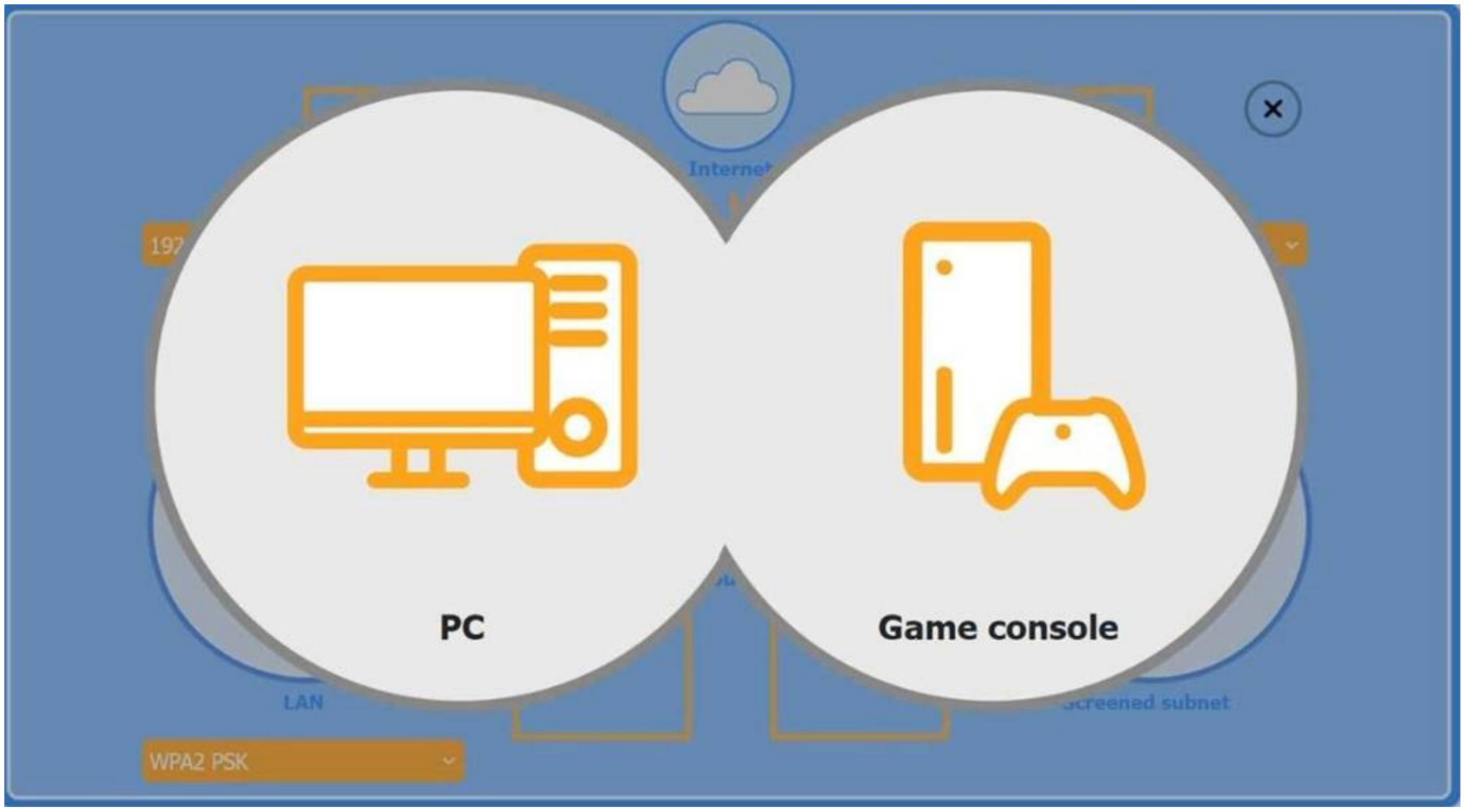
A. Administrative Tools
B. Windows Defender Firewall
C. Internet Options
D. Ease of Access

Answer: C

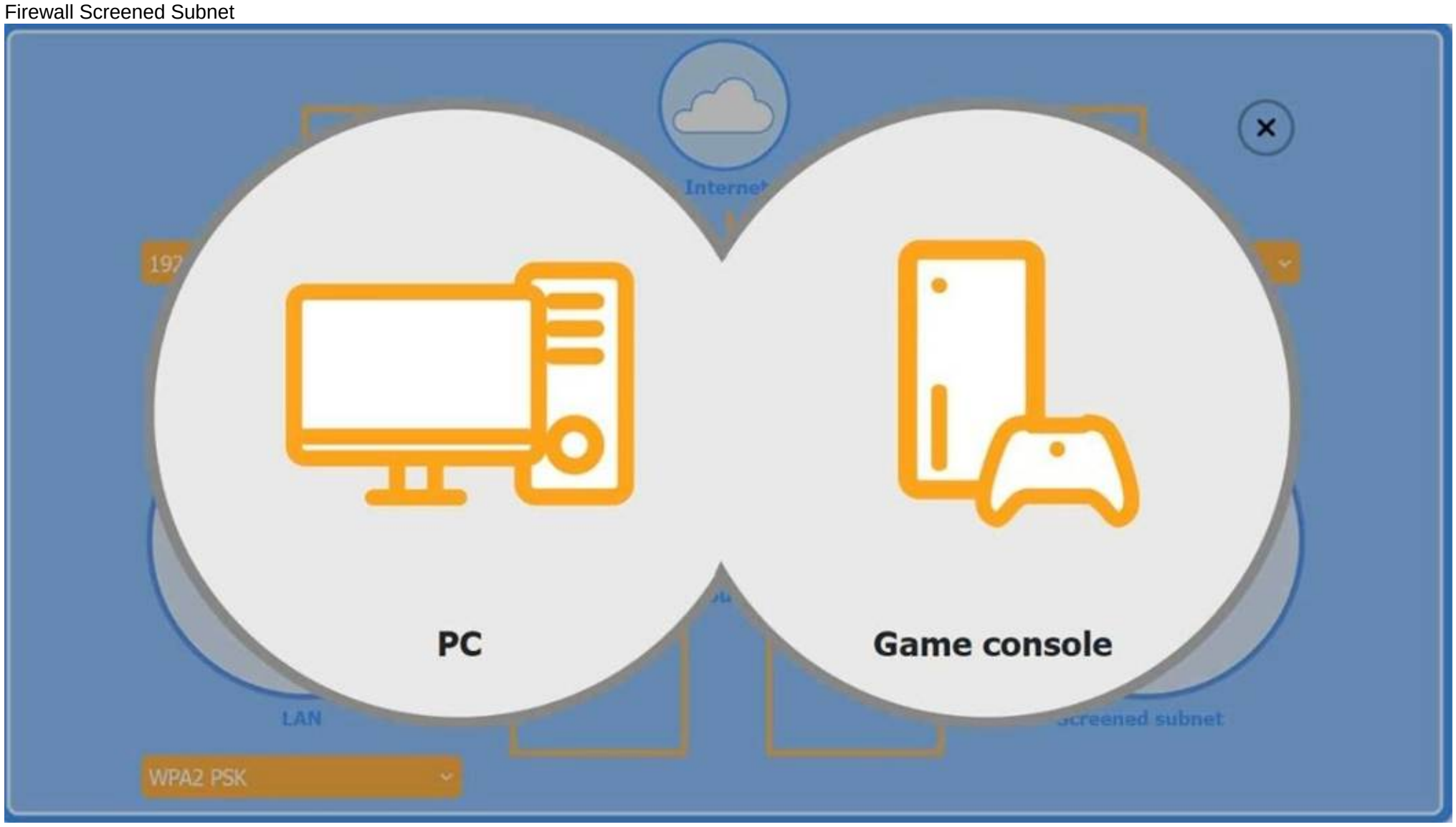
Explanation:
Comprehensive and Detailed Explanation From Exact Extract: Outdated images and website data often result from cached files in the browser. The Internet Options panel in Windows (specifically under the General tab) allows users to clear browsing history, including cached images and files, 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

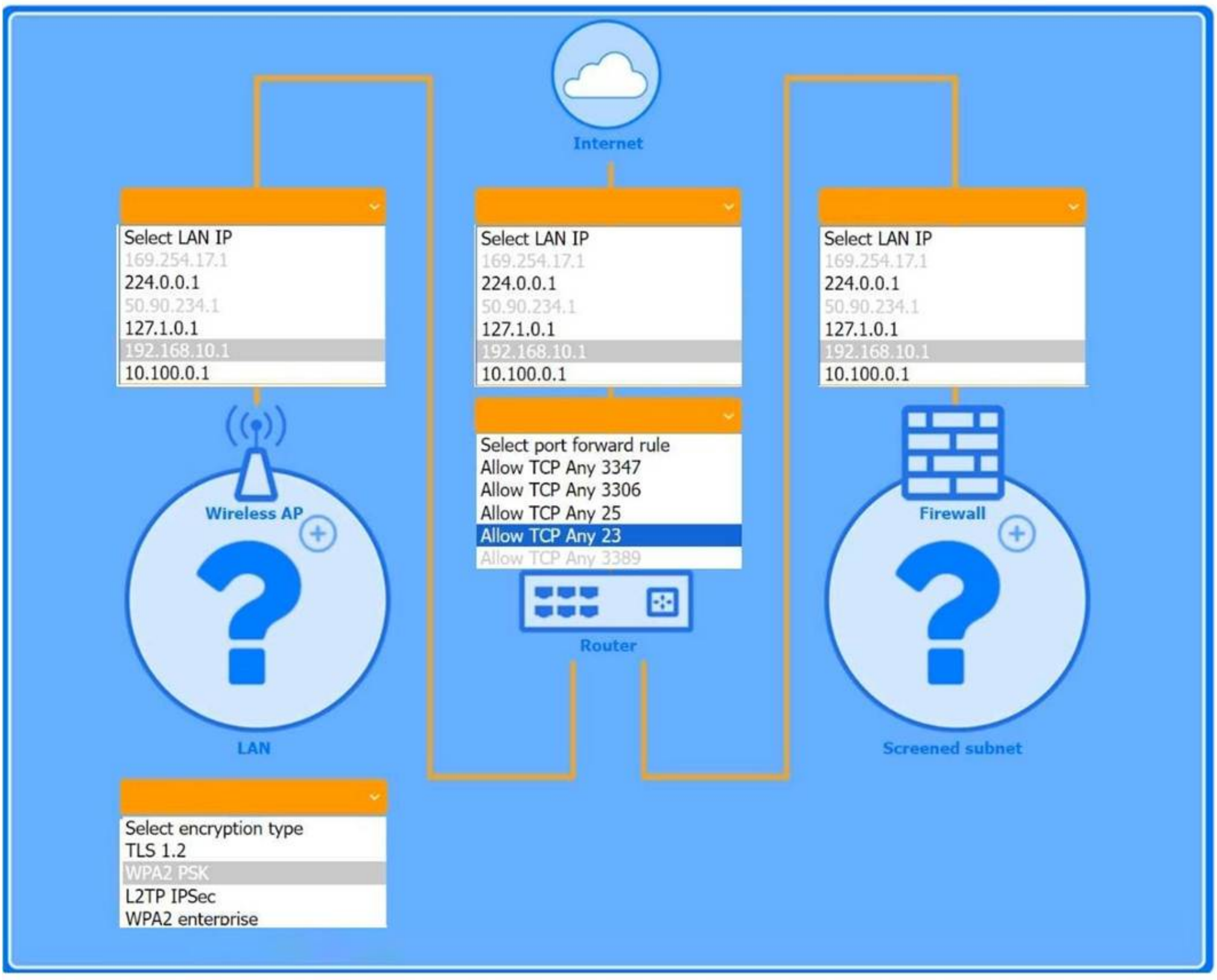
NEW QUESTION 34
SIMULATION
You are configuring a home network for a customer. The customer has requested the ability to access a Windows PC remotely, and needs all chat and optional

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





A. Mastered
B. Not Mastered

Answer: A

Explanation:
The completed configuration:
* 1. Wireless AP (LAN side) 1. LAN IP: 192.168.10.1
* 2. Encryption: WPA2 PSK
* 2. 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.
* 3. Firewall (screened subnet side) 1. LAN IP: 10.100.0.1
* 4. 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.

NEW QUESTION 36
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
==========

NEW QUESTION 40
A technician notices that the weekly backup is taking too long to complete. The daily backups are incremental. Which of the following would most likely resolve the issue?

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

Answer: D

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

NEW QUESTION 44
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)
==========

NEW QUESTION 46
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.

NEW QUESTION 50
A network technician notices that most of the company's network switches are now end-of- life and need to be upgraded. Which of the following should the technician do first?

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

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The first step in the IT change management process is to identify and propose the change. In this case, the technician notices a need (end-of-life network switches), so the
appropriate action is toformally propose a change. This proposal would be documented and submitted for approval before any planning or implementation occurs.
According to the CompTIA A+ 220-1102 objectives under Operational Procedures (Domain 4.0), the change management process follows these typical steps:
? Submit a change request (Propose the change)
? Review and approval (Approve the change)
? Planning and scheduling (Schedule the change)
? Implementation
? Documentation and review
Therefore, proposing the change is the correct first step in accordance with standard ITIL- based change management practices.
Reference:
CompTIA A+ 220-1102 Objective 4.1: Given a scenario, implement best practices associated with documentation and support systems information management.
Study Guide Section: Change Management Process
==========

NEW QUESTION 51
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)
==========

NEW QUESTION 55
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
==========

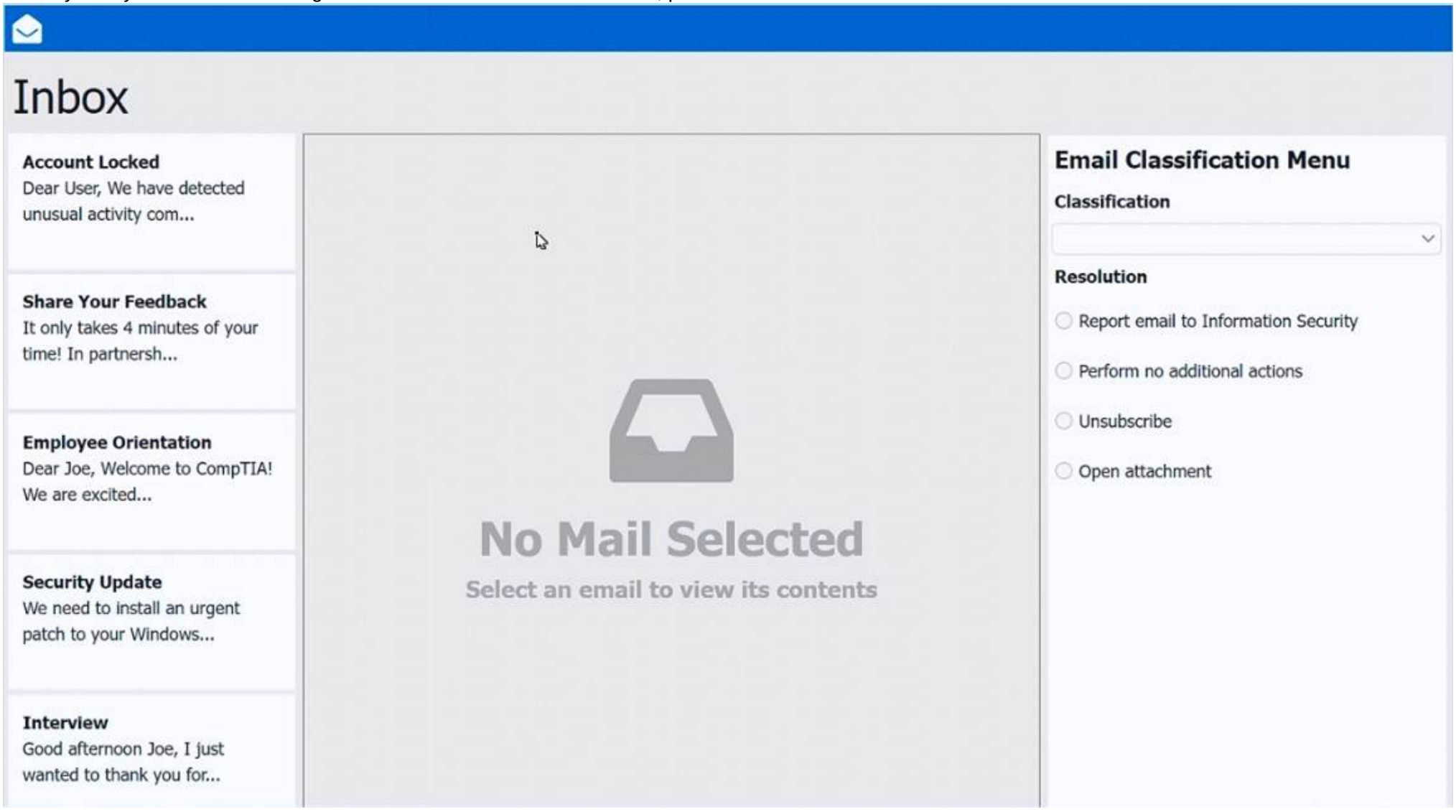
NEW QUESTION 60
A technician is preparing to replace the batteries in a rack-mounted UPS system. After ensuring the power is turned off and the batteries are fully discharged, the technician needs to remove the battery modules from the bottom of the rack. Which of the following steps should the technician take?

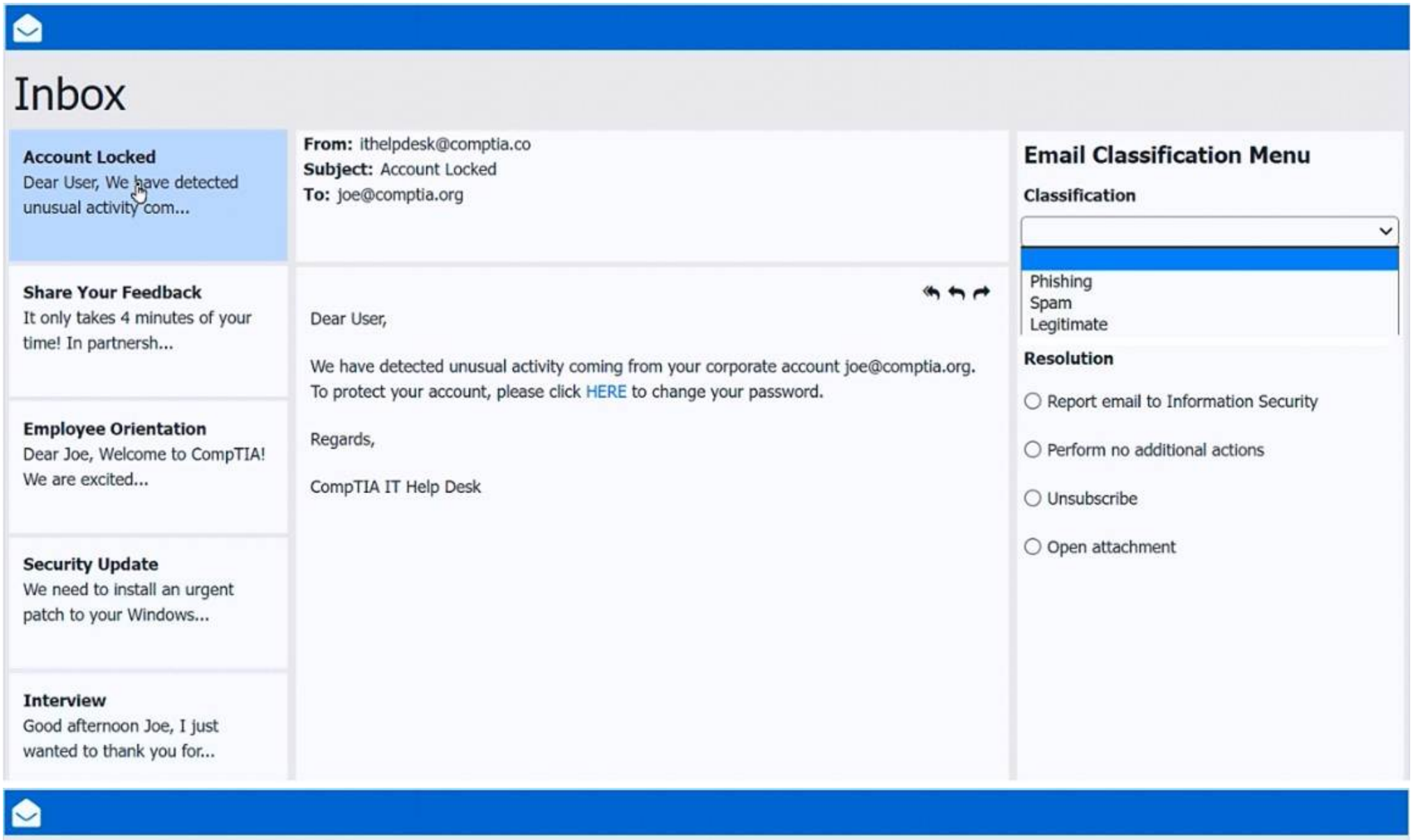
A. Ensure the fire suppression system is ready to be activated.
B. Use appropriate lifting techniques and guidelines.
C. Place the removed batteries in an antistatic bag.
D. Wear a face mask to filter out any harmful fumes.

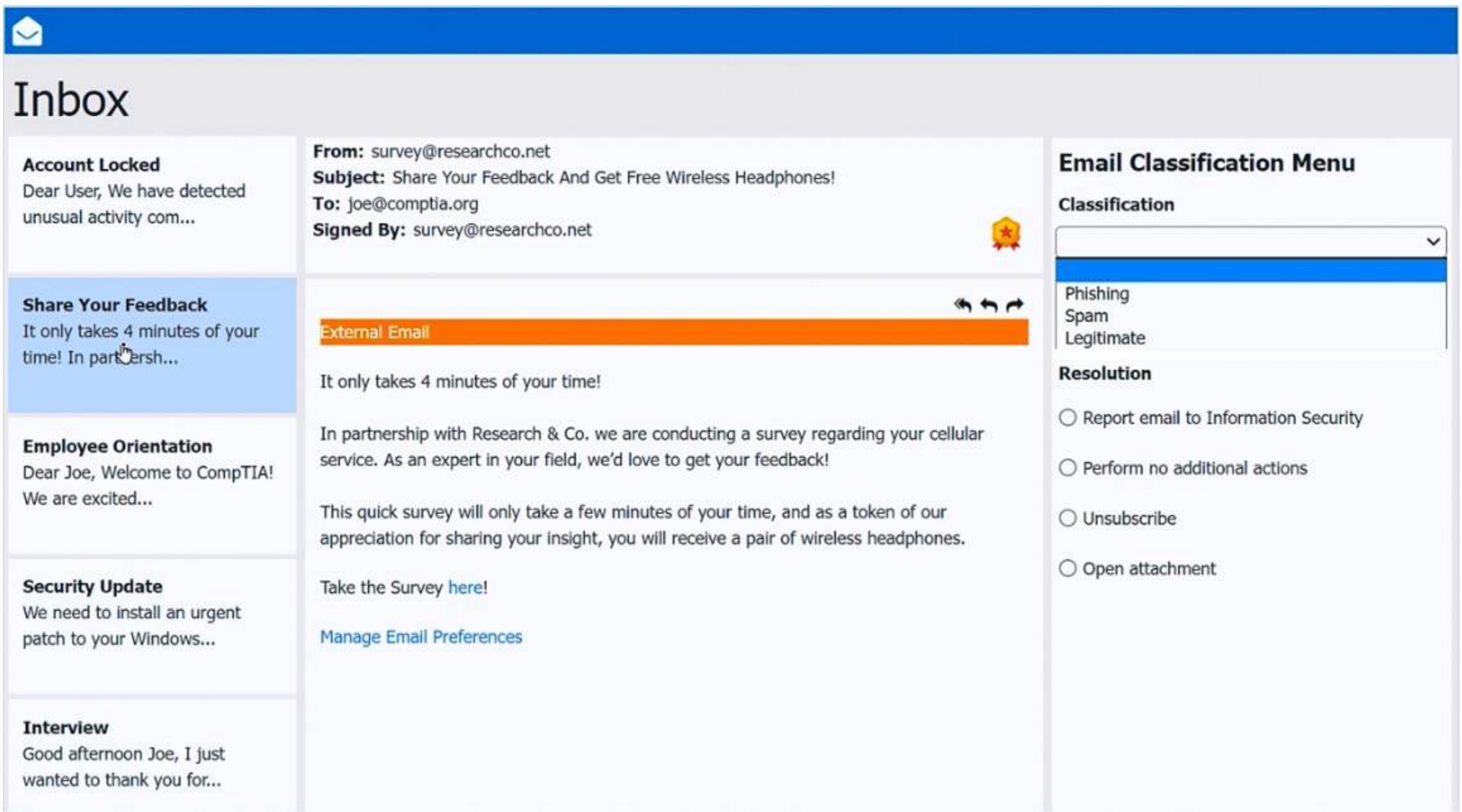
Answer: B

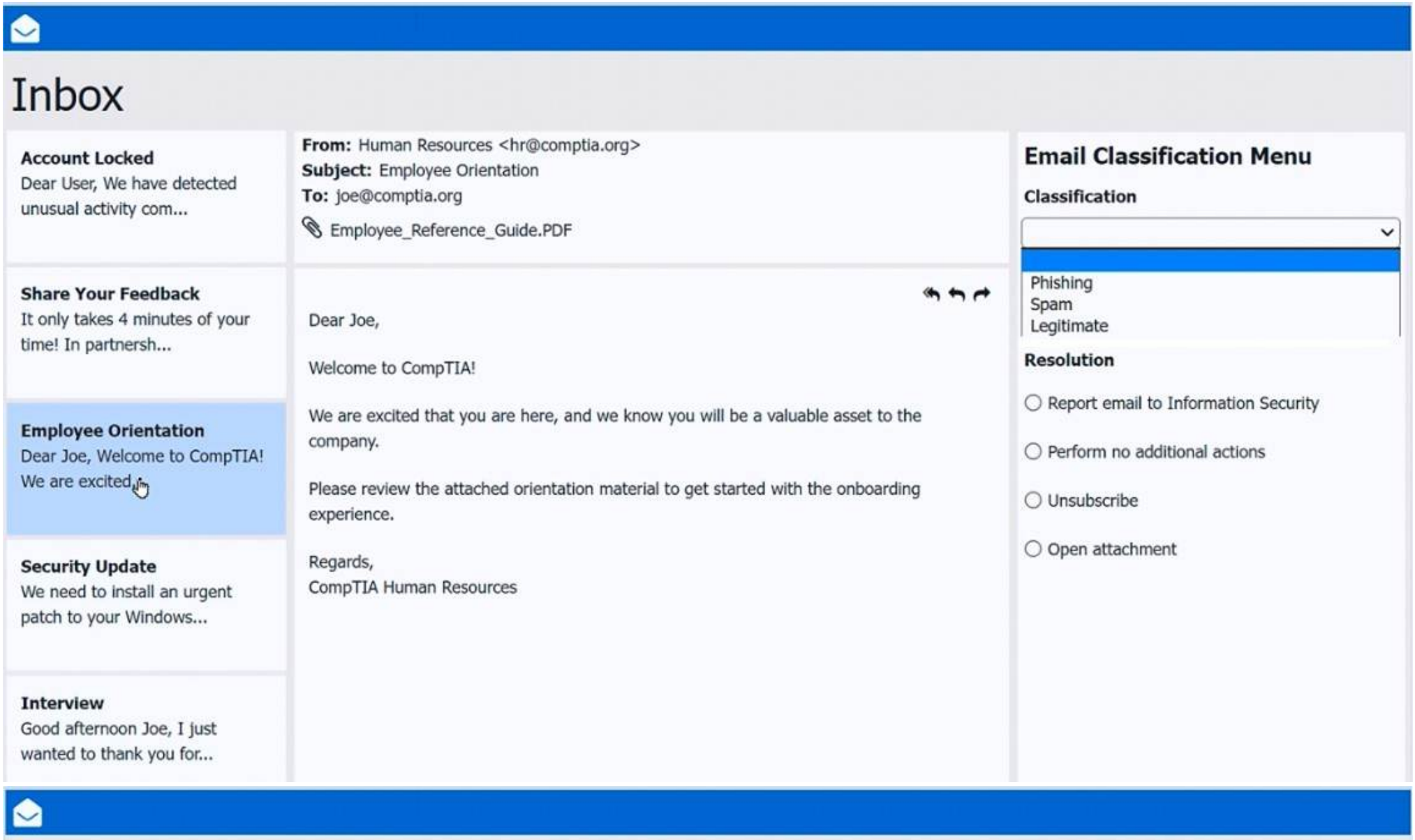
Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
UPS batteries are heavy and often located at the bottom of racks to maintain balance. Safe removal requires the use of correct lifting techniques to avoid injury.
OSHA and workplace safety standards emphasize ergonomic handling when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

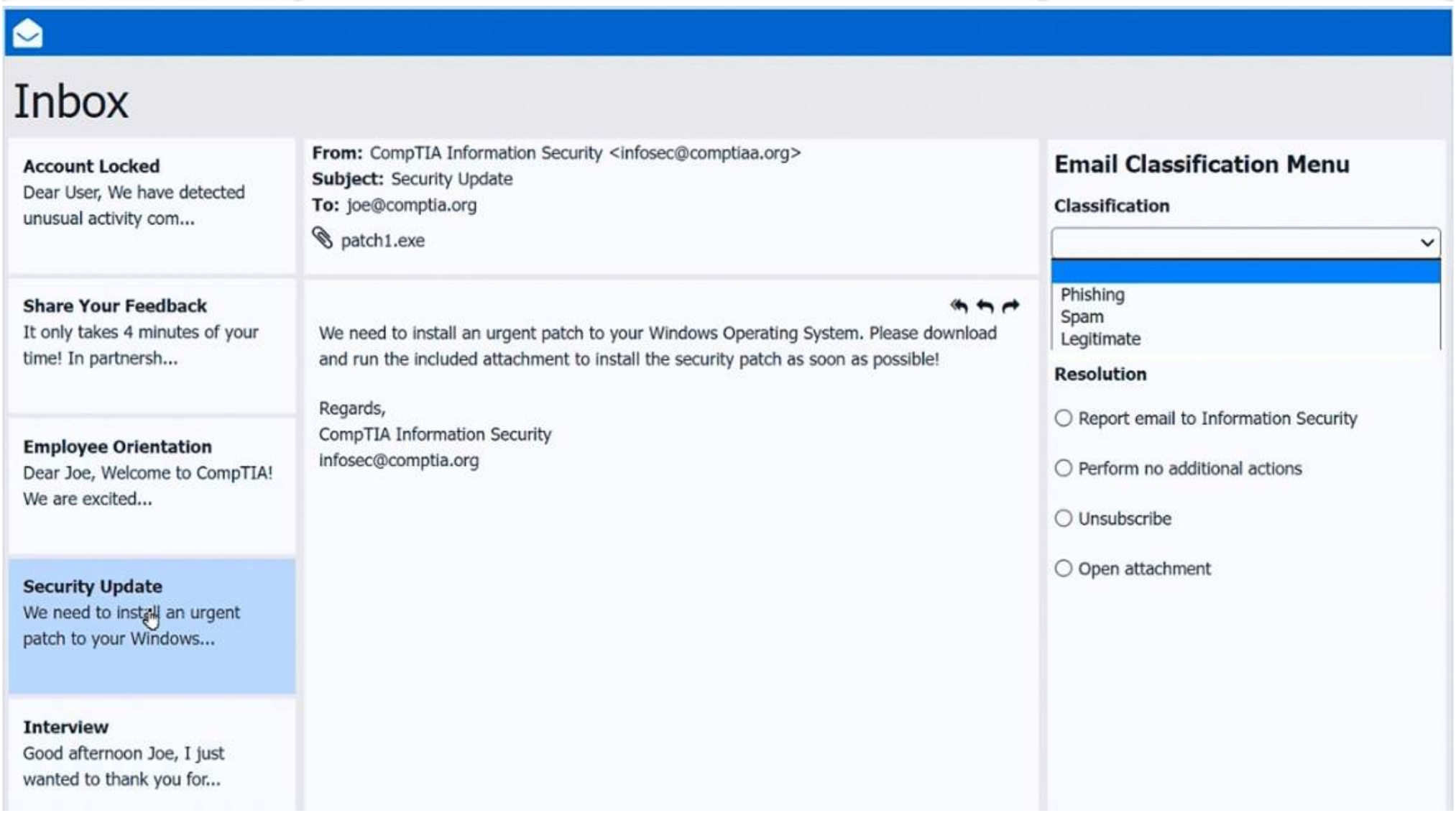
NEW QUESTION 63
SIMULATION
As a corporate technician, you are asked to evaluate several suspect email messages on a client's computer. Corporate policy requires the following:
>All phishing attempts must be reported.
>Future spam emails to users must be prevented. INSTRUCTIONS
Review each email and perform 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.

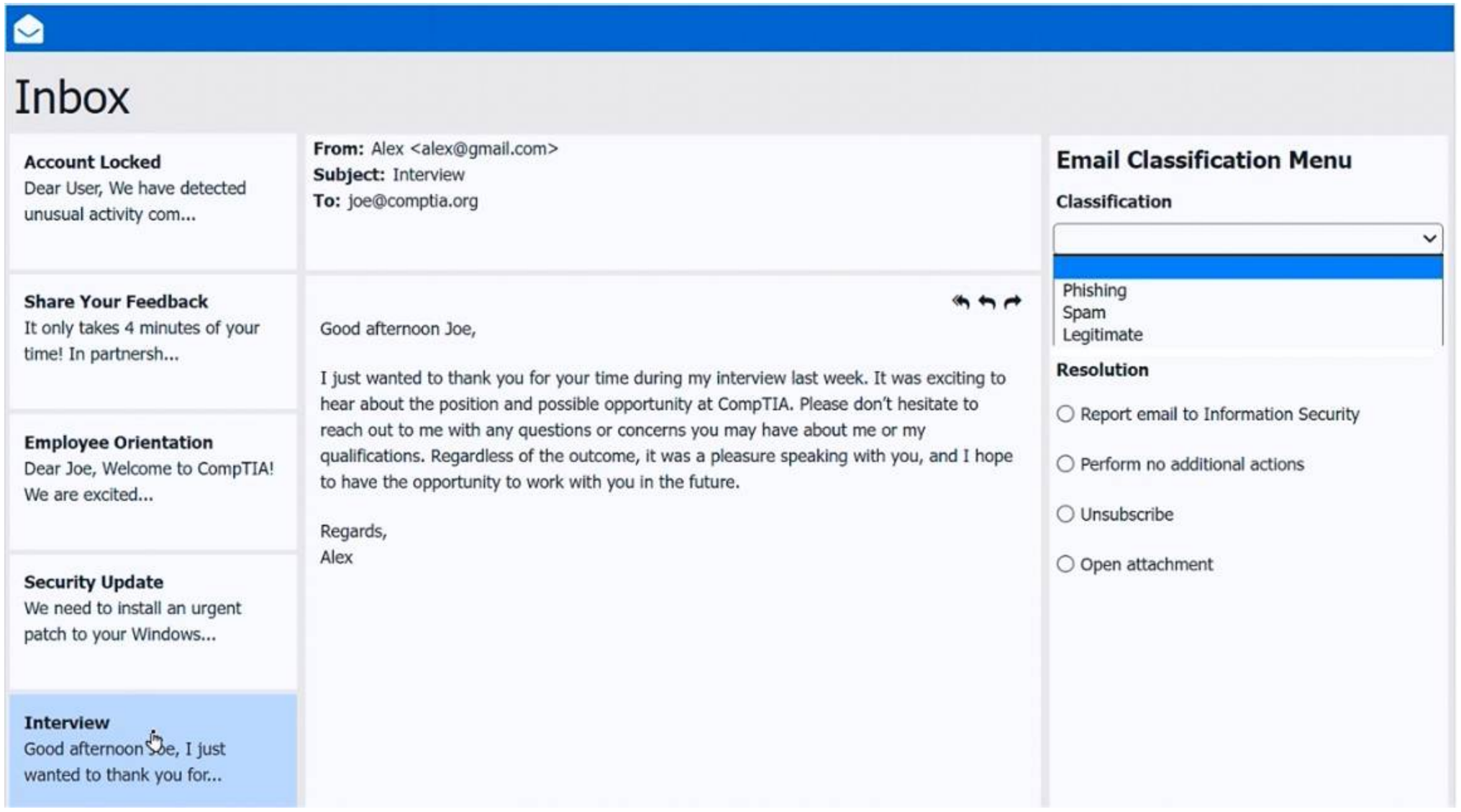



Inbox
Account Locked
Dear User, We have detected unusual activity com...
Share Your Feedback
It only takes 4 minutes of your time! In partnersh...
Employee Orientation
Dear Joe, Welcome to CompTIA! We are excited...
Security Update
We need to install an urgent patch to your Windows...
Interview
Good afternoon Joe, I just wanted to thank you for...
From: ithelpdesk@comptia.co
Subject: Account Locked
To: joe@comptia.org
Dear User,
We have detected unusual activity coming from your corporate account joe@comptia.org.
To protect your account, please click HERE to change your password.
Regards,
CompTIA IT Help Desk
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: survey@researchco.net
Subject: Share Your Feedback And Get Free Wireless Headphones!
To: joe@comptia.org
Signed By: survey@researchco.net
External Email
It only takes 4 minutes of your time!
In partnership with Research & Co. we are conducting a survey regarding your cellular service. As an expert in your field, we'd love to get your feedback!
This quick survey will only take a few minutes of your time, and as a token of our appreciation for sharing your insight, you will receive a pair of wireless headphones.
Take the Survey here!
Manage Email Preferences
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: 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



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 65
A technician is assigned to offboard a user. Which of the following are common tasks on an offboarding checklist? (Choose two.)

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

Answer: BD

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

NEW QUESTION 70
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
==========

NEW QUESTION 74
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
==========

NEW QUESTION 75
A support specialist needs to decide whether to install a 32-bit or 64-bit OS architecture on a new computer. Which of the following specifications will help the specialist determine which OS architecture to use?

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

Answer: A

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

NEW QUESTION 78
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
==========

NEW QUESTION 79
A user reports some single sign-on errors to a help desk technician. Currently, the user is able tosign 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.
==========

NEW QUESTION 82
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

220-1202 Practice Exam Features:

* 220-1202 Questions and Answers Updated Frequently

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

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

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