CompTIA

Exam Questions 220-1202

CompTIA A+ Certification Exam: Core 2

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

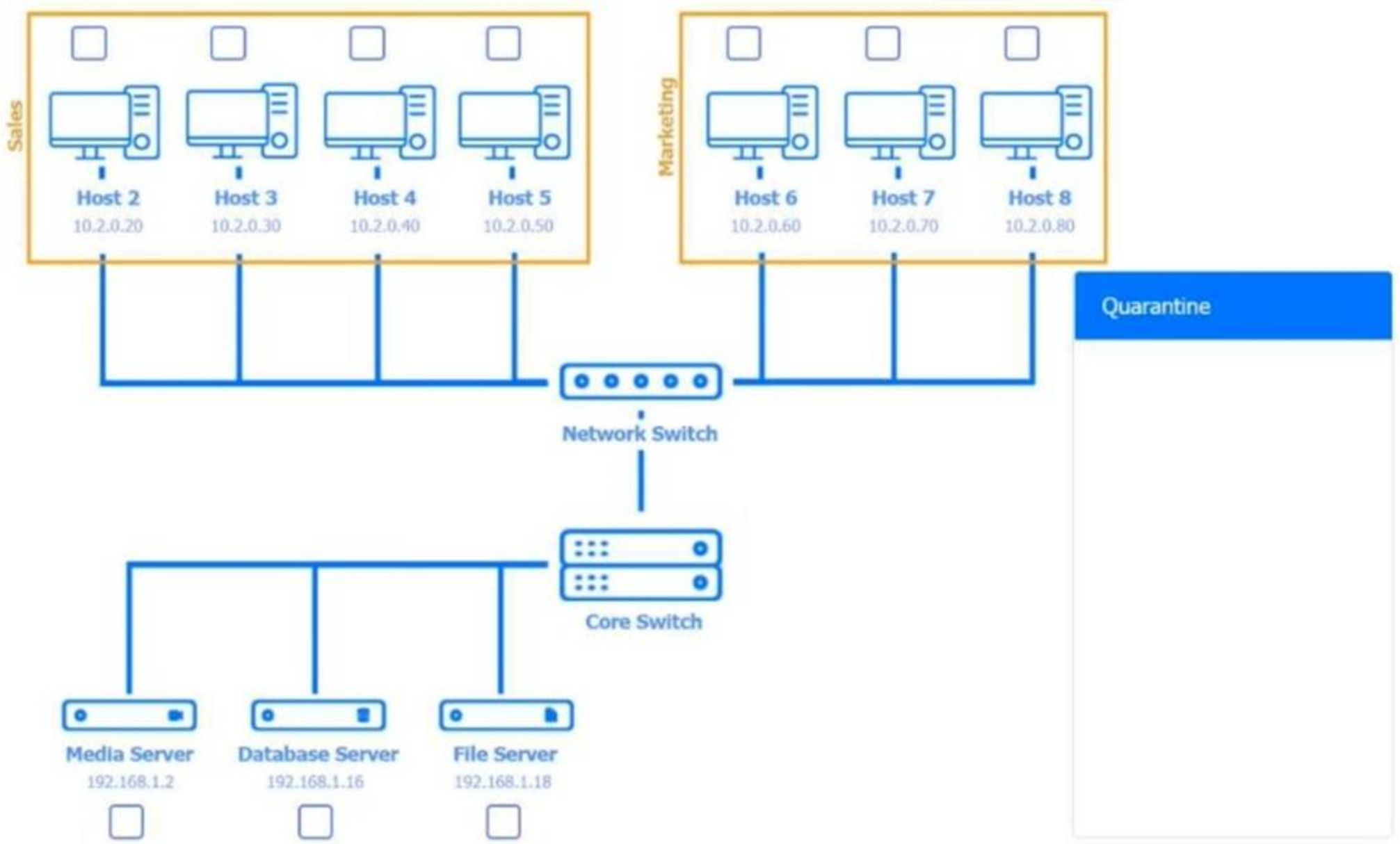
* 100% Pass Rate

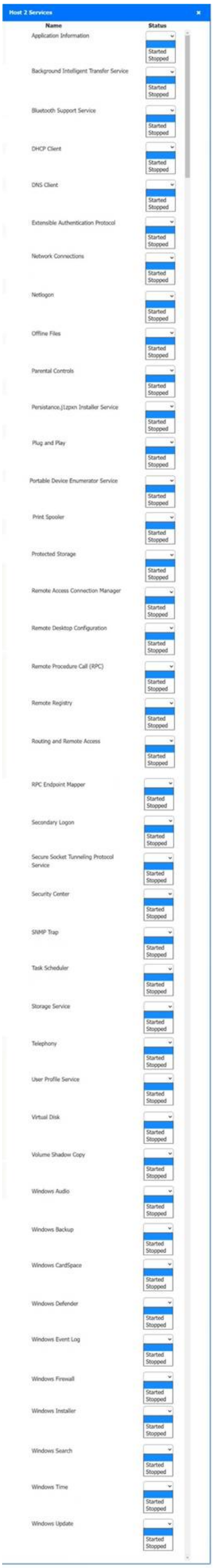
Our guarantee that you will pass the exam.

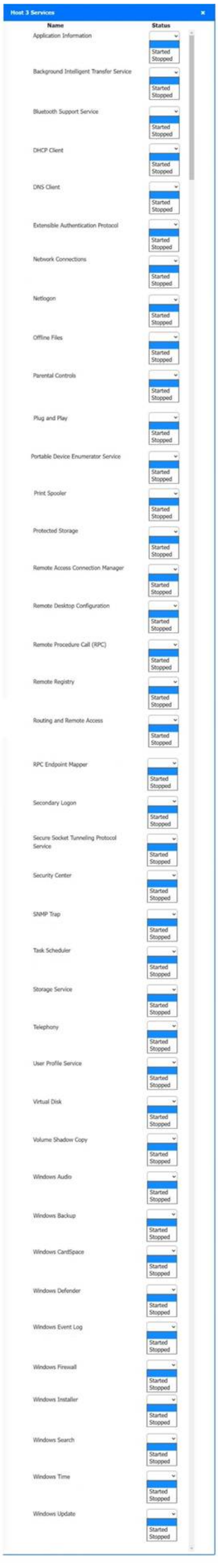
* Unique Gurantee

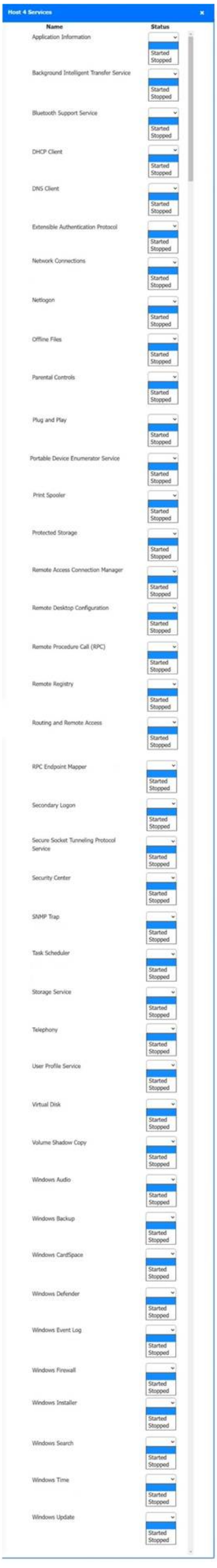
If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

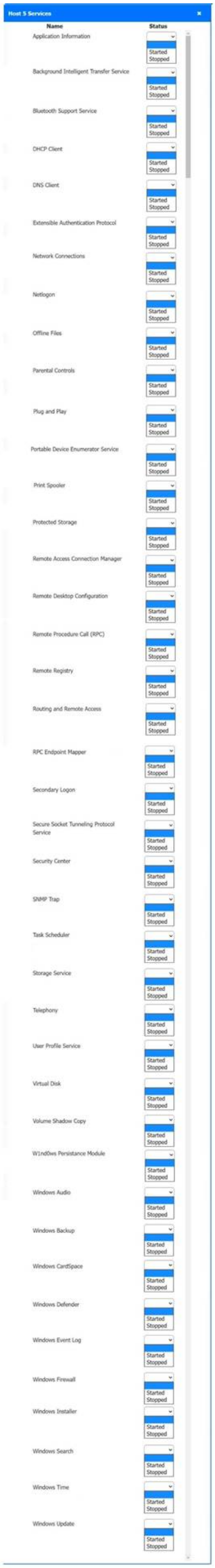
NEW QUESTION 1
SIMULATION
Multiple users are reporting audio issues as well as performance issues after downloading unauthorized software. You have been dispatched to identify and resolve any issues on the network using best practice procedures.
INSTRUCTIONS
Quarantine and configure the appropriate device(s) 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.

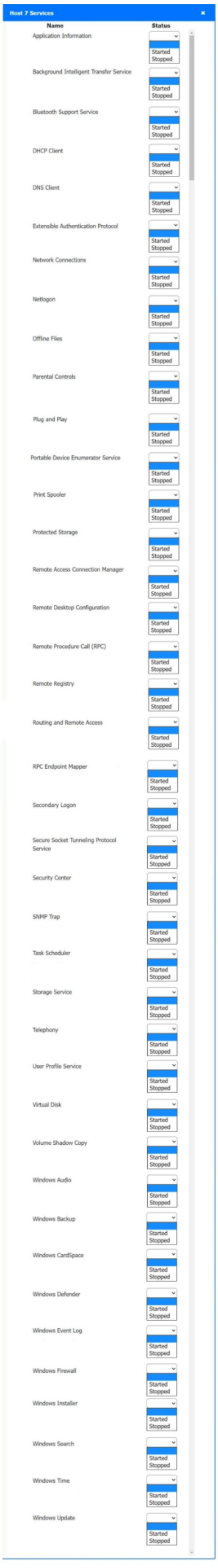


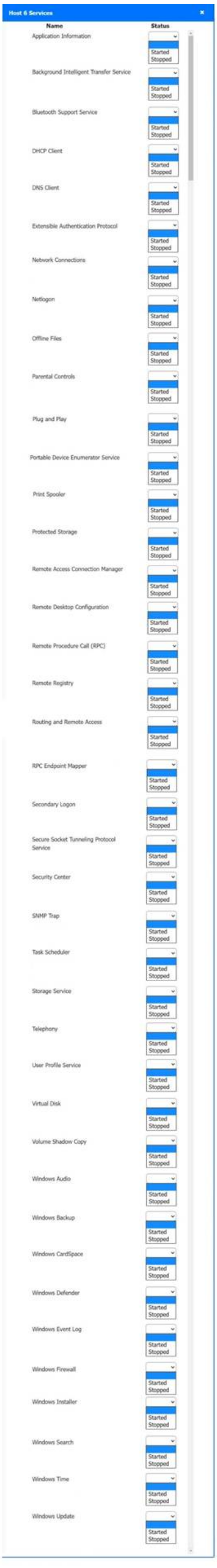

Host 2 Services
Name
Status
Application Information
Background Intelligent Transfer Service
Bluetooth Support Service
DHCP Client
DNS Client
Extensible Authentication Protocol
Network Connections
Netlogon
Offline Files
Parental Controls
Persistance.j1zpxn Installer Service
Plug and Play
Portable Device 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

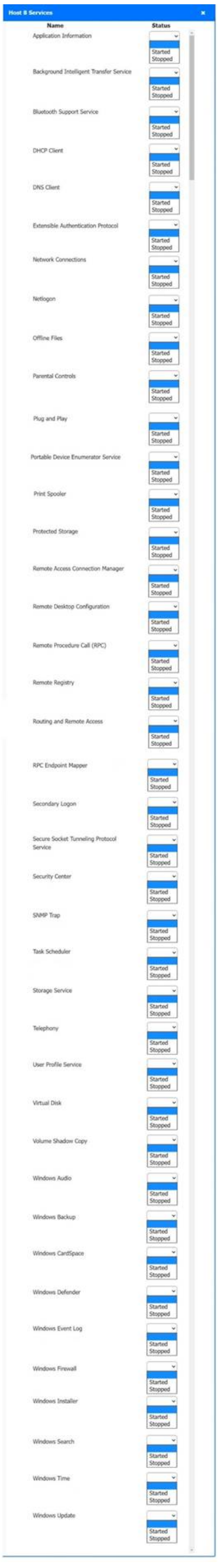

Host 3 Services
Name
Status
Application Information
Background Intelligent Transfer Service
Bluetooth Support Service
DHCP Client
DNS Client
Extensible Authentication Protocol
Network Connections
Netlogon
Offline Files
Parental Controls
Plug and Play
Portable Device Enumerator Service
Print Spooler
Protected 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

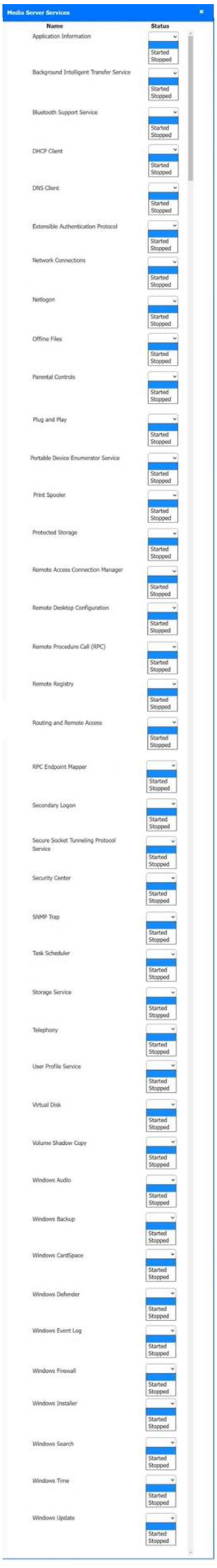

Host 4 Services
Name
Status
Application Information
Background Intelligent Transfer Service
Bluetooth Support Service
DHCP Client
DNS Client
Extensible Authentication Protocol
Network Connections
Netlogon
Offline Files
Parental Controls
Plug and Play
Portable Device Enumerator Service
Print Spooler
Protected 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

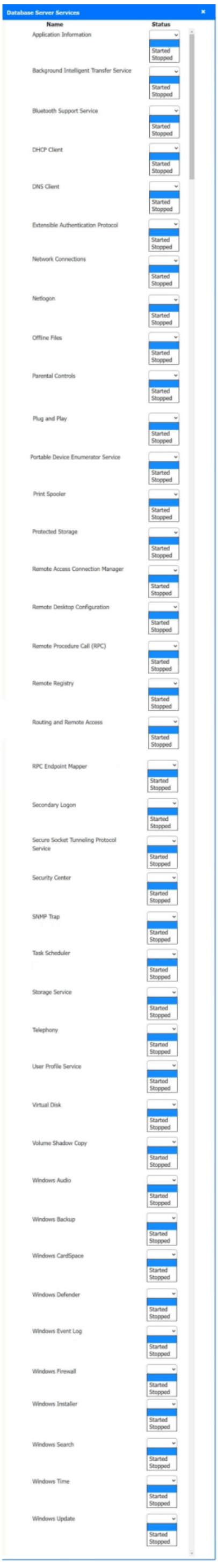

Host S Services
Name
Status
Application Information
Background Intelligent Transfer Service
Bluetooth Support Service
DHCP Client
DNS Client
Extensible Authentication Protocol
Network Connections
Netlogon
Offline Files
Parental Controls
Plug and Play
Portable Device Enumerator Service
Print Spooler
Protected 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

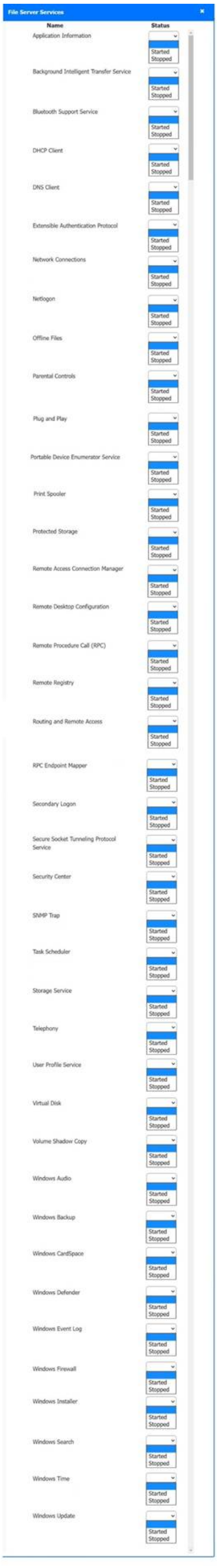

Host 7 Services
Name
Status
Application Information
Background Intelligent Transfer Service
Bluetooth Support Service
DHCP Client
DNS Client
Extensible Authentication Protocol
Network Connections
Netlogon
Offline Files
Parental Controls
Plug and Play
Portable Device Enumerator Service
Print Spooler
Protected 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 2
A technician uses AI to draft a proposal about the benefits of new software. When reading the draft, the technician notices that the draft contains factually incorrect information. Which of the following best describes this scenario?

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

Answer: B

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

NEW QUESTION 3
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 4
A technician thinks that an application a user downloaded from the internet may not be the legitimate one, even though the name is the same. The technician needs to confirm whether the application is legitimate. Which of the following should the technician do?

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

Answer: A

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

NEW QUESTION 5
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 6
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)

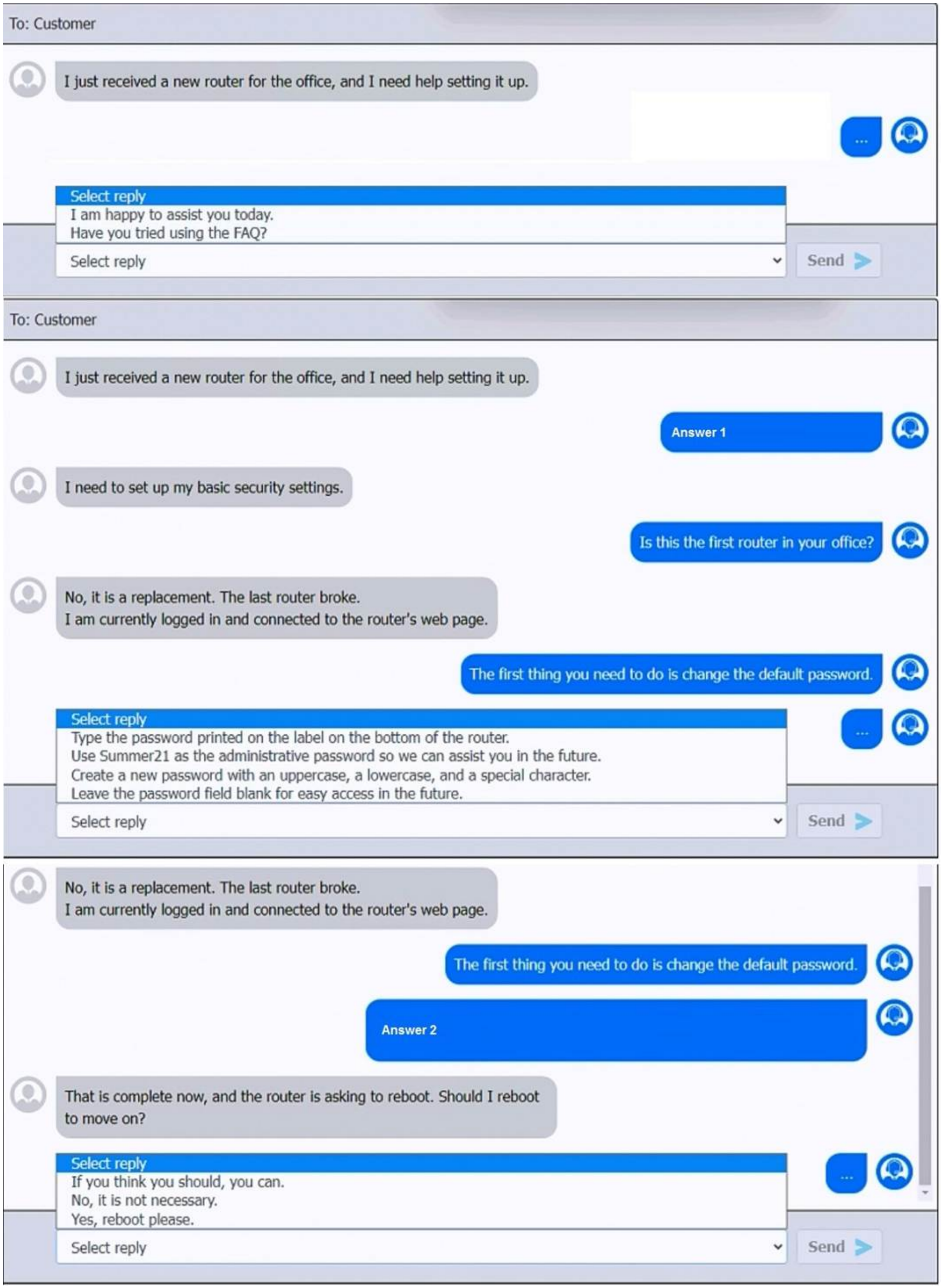
NEW QUESTION 7
A customer is unable to open some files on their system. Each time the customer attempts to open a file, the customer receives a message that the file is encrypted. Which of the following best describes this issue?

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

Answer: B

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

NEW QUESTION 8
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.



A. Mastered
B. Not Mastered

Answer: A

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.

NEW QUESTION 9
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 10
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
==========

NEW QUESTION 10
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

NEW QUESTION 13
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 14
Which of the following is the quickest way to move from Windows 10 to Windows 11 without losing data?

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

Answer: D

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

NEW QUESTION 17
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 19
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 24
A computer technician is implementing a solution to support a new internet browsing policy for a customer's business. The policy prohibits users from accessing unauthorized websites based on categorization. Which of the following should the technician configure on the SOHO router?

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

Answer: C

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

NEW QUESTION 28
Which of the following types of social engineering attacks sends an unsolicited text message to a user's mobile device?

A. Impersonation
B. Vishing
C. Spear phishing
D. Smishing

Answer: D

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

NEW QUESTION 32
A help desk technician needs to remove RAM from retired workstations and upgrade other workstations that have applications that use more memory with this RAM. Which of the following actions would the technician most likely take?

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

Answer: B

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

NEW QUESTION 37
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 39
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
==========

NEW QUESTION 41
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 46
.....

Relate Links

100% Pass Your 220-1202 Exam with Exambible Prep Materials

https://www.exambible.com/220-1202-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/