Exam Questions 220-1202

CompTIA A+ Certification Exam: Core 2

https://www.2passeasy.com/dumps/220-1202/

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
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 4
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 5
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 6
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 7
A small office reported a phishing attack that resulted in a malware infection. A technician is investigating the incident and has verified the following:
All endpoints are updated and have the newest EDR signatures.
Logs confirm that the malware was quarantined by EDR on one system. The potentially infected machine was reimaged.
Which of the following actions should the technician take next?

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

Answer: B

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

Reference:
CompTIA A+ 220-1102 Objective 2.5: Given a scenario, detect, remove, and prevent malware using appropriate tools and methods.
Study Guide Section: Incident response and user education after a security event

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

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

Answer: D

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

NEW QUESTION 9
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 10
Which of the following methods involves requesting a user's approval via a push notification to verify the user's identity?

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

Answer: B

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

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

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

Answer: A

Explanation:

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

NEW QUESTION 13
A technician is setting up a Windows server to allow remote desktop connections for multiple users. Which of the following should the technician configure on the workstation?

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

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
To allow Remote Desktop Protocol (RDP) access, the firewall must be configured to allow inbound connections on TCP port 3389. If the Windows Firewall blocks RDP, users will not be able to connect remotely even if the feature is enabled in system settings.
* B. Computer Management allows configuration of services and local users, but not network access.
* C. User Accounts is for account setup and control, but enabling remote access requires firewall configuration.
* D. Ease of Access is unrelated to remote connectivity—it??s for accessibility features. Reference:
CompTIA A+ 220-1102 Objective 2.2: Compare and contrast security measures and firewall settings.
Study Guide Section: Enabling and securing RDP via firewall settings
==========

NEW QUESTION 17
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 21
A help desk team was alerted that a company-owned cell phone has an unrecognized password-cracking application. Which of the following should the help desk team do to prevent further unauthorized installations from occurring?

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

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Mobile Device Management (MDM) is used to control, monitor, and enforce policies on mobile devices. It allows IT teams to restrict app installations, push approved apps, and monitor device compliance. Deploying MDM would prevent unauthorized applications, such as password crackers, from being installed on company-managed devices.
* A. Group Policy is for managing Windows environments and not applicable to smartphones.
* B. PAM (Privileged Access Management) controls administrative access, not app installation.
* C. Anti-malware can help detect malicious apps but doesn??t prevent their installation proactively.
Reference:
CompTIA A+ 220-1102 Objective 2.2: Compare and contrast common security measures and tools.

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

NEW QUESTION 22
A security administrator teaches all of an organization's staff members to use BitLocker To Go. Which of the following best describes the reason for this training?

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

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
BitLocker To Go is a Microsoft encryption feature specifically designed for removable drives such as USB flash drives and external hard drives. It allows users to protect the data on these devices by requiring a password to decrypt the contents, thereby preventing unauthorized access in the event the device is lost or stolen.
A is correct because BitLocker To Go is directly tied to password-protecting removable media.
B and C are unrelated to BitLocker To Go; Secure Boot and VPN encryption are entirely
different security layers.
D applies to BitLocker (not BitLocker To Go) and full disk encryption on internal drives using TPM.
Reference:
CompTIA A+ 220-1102 Objective 2.2: Compare and contrast common security measures and tools.
Study Guide Section: Encryption technologies (BitLocker, BitLocker To Go)
==========

NEW QUESTION 23
A user is attempting to open on a mobile phone a HD video that is hosted on a popular media streaming website. The user is receiving connection timeout errors. The mobile reception icon area is showing two bars next to 3G. Which of the following is the most likely cause of the issue?

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

Answer: C

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

NEW QUESTION 25
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 file types would a desktop support technician most likely use to automate tasks for a Windows user log-in?

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

Answer: A

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

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

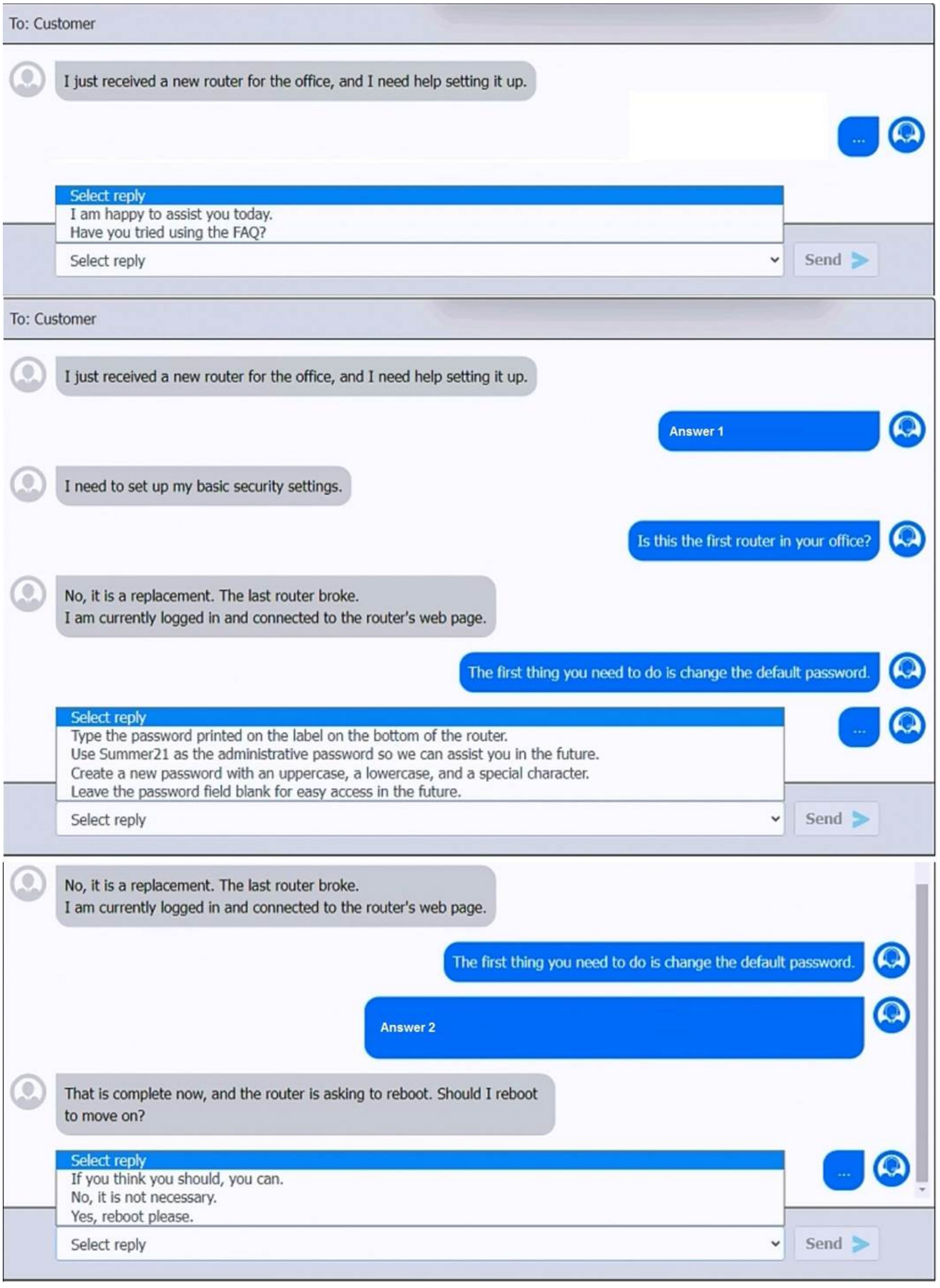
NEW QUESTION 38
A company recently transitioned to a cloud-based productivity suite and wants to secure the environment from external threat actors. Which of the following is the most effective method?

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

Answer: A

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

NEW QUESTION 40
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 41
A technician is troubleshooting an issue in which a service runs momentarily and stops at certain points in the process. The technician needs to determine the root cause of this issue. Which of the following tools should the technician use?

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

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Event Viewer is the best tool to analyze the root cause of service failures in Windows. It provides detailed logs from system processes, including errors, warnings, and crash reports related to services and applications. When a service starts and stops unexpectedly, Event Viewer will often record the cause, such as dependency failures or access violations.
* B. Task Manager shows active processes but doesn't retain logs or causes of failure.
* C. Internet Options is used for configuring browser settings, not troubleshooting services.
* D. Process Explorer is powerful but more suited for live monitoring and detailed process trees, not post-failure log analysis.
Reference:
CompTIA A+ 220-1102 Objective 3.1: Given a scenario, troubleshoot common Windows OS problems.
Study Guide Section: Log file analysis using Event Viewer
==========

NEW QUESTION 44
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 47
A technician notices that the weekly backup is taking too long to complete. The daily backups are incremental. Which of the following would most likely resolve the issue?

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

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
A synthetic full backup combines the last full backup with subsequent incremental backups to create a new full backup without re-reading data from the source system. This method significantly reduces the backup window and network impact. It is especially useful when traditional full backups are too time-consuming.
* A. Changing the backup window only shifts timing, not duration.
* B. Incremental weekly backups would lack a proper full recovery point and aren't ideal alone.

* C. Storage space isn't the bottleneck in backup speed—it??s read/write operations and network load.
Reference:
CompTIA A+ 220-1102 Objective 4.2: Summarize backup and recovery concepts.
Study Guide Section: Backup types — full, incremental, differential, and synthetic backups
==========

NEW QUESTION 48
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 49
Which of the following methods would make data unrecoverable but allow the drive to be repurposed?

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

Answer: C

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

NEW QUESTION 54
Which of the following provides information to employees, such as permitted activities when using the organization's resources?

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

Answer: A

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

NEW QUESTION 56
Technicians are failing to document user contact information, device asset tags, and a clear description of each issue in the ticketing system. Which of the following should a help desk management team implement for technicians to use on every call?

A. Service-level agreements
B. Call categories
C. Standard operating procedures

D. Knowledge base articles

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Standard Operating Procedures (SOPs) define the mandatory steps and expectations technicians must follow during support calls. This includes documentation standards such as logging user info, asset details, and issue descriptions in the ticketing system. Implementing SOPs ensures consistency and accountability.
* A. SLAs define response/resolution times but not documentation practices.
* B. Call categories organize types of issues but don't guide technician actions.
* D. Knowledge base articles provide solutions to known problems but don't ensure proper ticket documentation.
Reference:
CompTIA A+ 220-1102 Objective 4.2: Summarize best practices associated with types of documentation and support systems information.
Study Guide Section: Documentation practices, SOPs, ticketing protocols
==========

NEW QUESTION 60
Which of the following is the best reason for a network engineering team to provide a help desk technician with IP addressing information to use on workstations being deployed in a secure network segment?

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

Answer: C

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

NEW QUESTION 63
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 66
Which of the following is a Linux command that is used for administrative purposes?

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

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The su (substitute user) command is used in Linux to switch to another user account, most commonly to escalate privileges by switching to the root (administrator) account. It allows administrative tasks to be performed in a terminal session.
* A. runas is a Windows command for executing a program under another user's context.
* B. cmcl is not a valid Linux or administrative command.
* C. net user is a Windows command for managing local user accounts.
Reference:
CompTIA A+ 220-1102 Objective 1.9: Identify common features and tools of the Linux client/desktop OS.

Study Guide Section: Linux command-line tools — su, sudo
==========

NEW QUESTION 67
A technician needs to provide remote support for a legacy Linux-based operating system from their Windows laptop. The solution needs to allow the technician to see what the user is doing and provide the ability to interact with the user's session. Which of the following remote access technologies would support the use case?

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

Answer: B

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

NEW QUESTION 68
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 71
A technician needs to install an operating system on a large number of workstations. Which of the following is the fastest method?

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

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Image deployment is the fastest and most efficient method for installing operating systems on multiple machines. It involves creating a pre-configured image of an OS and deploying it across systems using tools like Windows Deployment Services (WDS) or third-party imaging solutions. This method saves time and ensures consistency across all devices.
* A. Physical media is slow and not scalable.
* B. Mountable ISOs are useful but still require manual installation.
* C. Manual installation is time-consuming and not suitable for large-scale deployment. Reference:
CompTIA A+ 220-1102 Objective 1.4: Given a scenario, use appropriate Microsoft operating system installation methods.
Study Guide Section: Deployment methods — image deployment, automation

NEW QUESTION 72
A user's new smartphone is not staying charged throughout the day. The smartphone charges fully every night. Which of the following should a technician review first to troubleshoot the issue?

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

Answer: D

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

NEW QUESTION 75
MFA for a custom web application on a user's smartphone is no longer working. The last time the user remembered it working was before taking a vacation to another country. Which of the following should the technician do first?

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

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Multi-Factor Authentication (MFA) apps, especially time-based one-time password (TOTP) apps (e.g., Google Authenticator, Authy), rely on accurate time synchronization between the device and the authentication server. If the user recently traveled internationally, the device may have incorrect date/time settings due to time zone changes or failed synchronization, leading to MFA failure.
The most logical and non-intrusive first step is to verify and correct the date and time settings. This aligns with basic troubleshooting principles—start with the simplest and most likely cause before taking more drastic action.
Reference:
CompTIA A+ 220-1102 Objective 2.6: Given a scenario, apply cybersecurity best practices to secure a workstation.
Study Guide Section: Authentication technologies and MFA troubleshooting
==========

NEW QUESTION 77
A customer wants to be able to work from home but does not want to be responsible for bringingcompany equipment back and forth. Which of the following would allow the user to remotely access and use a Windows PC at the main office? (Choose two.)

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

Answer: CD

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

NEW QUESTION 82
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 220-1202 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 220-1202 Product From:

https://www.2passeasy.com/dumps/220-1202/

Money Back Guarantee

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