PassQueen
a.k.a dumpsqueen.com

CompTIA A+ Certification Core 2 Exam

CompTIA 220-1102

Version Demo

Total Demo Questions: 84

Total Premium Questions: 843

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Operating Systems	255
Topic 2, Security	311
Topic 3, Software Troubleshooting	119
Topic 4, Operational Procedures	152
Topic 5, Mix Questions	6
Total	843

QUESTION NO: 1

A technician needs to create a security and compliance policy for backup requirements. The backups are required to:

Have the least possible impact on users.

Minimize additional expenses.Which of the following are the best options for the technician to include? (Select two).

A. Configuring the backup to run when the user logs in

B. Configuring the backup to run after peak hours

C. Installing the backup software on the servers

D. Installing the backup software on the workstations

E. Using the built-in Windows backup utility

F. Configuring the backup job to run every hour

ANSWER: B E

Explanation:

Configuring the backup to run after peak hours directly reduces disruption to normal business activity. Backup operations can consume processor capacity, disk input/output resources, and network bandwidth, particularly when copying large data sets or performing full backups. Scheduling those jobs outside the organization's busiest periods helps preserve workstation and server responsiveness for users while still ensuring that protected data is captured on a defined schedule. This is a practical policy control because it aligns backup timing with operational requirements rather than requiring new infrastructure.

Using the built-in Windows backup utility also supports the requirement to minimize additional expenses. When its available features meet the organization's recovery, retention, and scheduling requirements, a built-in tool avoids licensing and deployment costs for separate backup products. Windows Backup can create backups and system images and can be scheduled through supported Windows tools, allowing an organization to implement a basic backup policy with software already included in the operating system. The policy should still document backup scope, retention, storage location, testing, and recovery responsibilities. See Microsoft Support: Backup and Restore in Windows and Microsoft Learn: wbadmin.

QUESTION NO: 2

A user reports receiving repeated calendar invitations from unknown external senders. Several invitations contain links to unfamiliar websites. Which of the following should the user do to help prevent a security incident? (Select TWO).

A. Report the messages to the security team

B. Do not open the links

C. Accept the invitations to review the meeting details

D. Reply with a request for sender verification

E. Forward the invitations to external contacts

ANSWER: A B

Explanation:

Report the messages to the security team and **Do not open the links** are the appropriate actions. Unexpected calendar invitations can be used for phishing or social-engineering attacks. Reporting the messages allows the organization to investigate the sender, block malicious domains, identify other affected users, and adjust filtering controls if necessary.

The user should not open links or attachments from an untrusted invitation. A malicious link can lead to a credential-harvesting site, initiate an unwanted download, or direct the user to other fraudulent content. The user should instead verify

any unexpected meeting request through a known, trusted communication method. CISA provides guidance for recognizing and reporting phishing attempts in its phishing guidance.

QUESTION NO: 3

A user reports the following issues:

•Their computer is constantly running slowly.

•The default home page of the web browser has changed to a suspicious search engine.

•They have been receiving pop-up ads on the screen.

Which of the following should a technician do first to address these issues?

A. Update the antivirus program and run a full system scan.

B. Uninstall the suspicious search engine and reset the home page.

C. Install the latest updates for the operating system.

D. Block the pop-up ads using the web browser settings.

ANSWER: A

Explanation:

Update the antivirus program and run a full system scan. Persistent slow performance, an unauthorized browser-home-page change, and unexpected pop-up advertisements are common indicators of a potentially unwanted program, adware, browser hijacker, or other malware. Updating the antivirus or anti-malware definitions first is important because detection tools depend on current signatures, heuristics, and threat intelligence to recognize recently identified threats. A full system scan then examines files, installed applications, browser-related components, startup items, and other locations where malicious or unwanted software may persist.

This action directly investigates and remediates the likely underlying security incident rather than merely changing a visible browser setting. The scan results also give the technician evidence needed to determine the scope of cleanup and whether additional remediation steps are needed afterward, such as removing detected items, checking browser extensions, or applying security updates. CompTIA's Core 2 objectives include identifying malware symptoms and following a structured malware-removal process, including updating anti-malware software and scanning the system. Microsoft likewise recommends keeping security intelligence current and performing scans when malware is suspected. See the CompTIA exam objectives and Microsoft Windows Security guidance.

QUESTION NO: 4

Which of the following operating systems is most commonly used in embedded systems?

A. Chrome OS

B. macOS

C. Windows

D. Linux

ANSWER: D

Explanation:

Linux is the most commonly used operating system in embedded systems because it can be tailored to run efficiently on devices with limited storage, memory, processing power, or specialized hardware. Its open-source licensing model allows device manufacturers and developers to inspect, modify, and redistribute a customized operating-system image without

relying on a proprietary desktop operating system. This flexibility supports a wide range of embedded products, including routers, network appliances, smart televisions, industrial controllers, automotive systems, point-of-sale terminals, and Internet of Things devices.

An embedded Linux deployment commonly uses a reduced kernel configuration, only the required device drivers, and a minimal root file system. Developers can cross-compile the system for the device's processor architecture and build a compact image containing just the applications and services required for the product. The Linux kernel also has broad hardware-platform support and an established ecosystem of embedded build systems, packages, and vendor tools. These characteristics make Linux a practical and widely adopted platform when supporting purpose-built computing devices, consistent with the operating-system concepts covered by the CompTIA A+ Core 2 objectives. See the Linux Kernel Archives and the CompTIA exam objectives resource page for authoritative background.

QUESTION NO: 5

A systems administrator is creating periodic backups of a folder on a Microsoft Windows machine. The source data is very dynamic, and files are either added or deleted regularly. Which of the following utilities can be used to 'mirror the source data for the backup?

A. copy

B. xcopy

C. robocopy

D. Copy-Item

ANSWER: C

Explanation:

`robocopy` is the appropriate Windows utility because it includes a mirror mode designed to make a destination directory match a source directory. When used with the `/MIR` switch, Robocopy copies new and changed files and directories from the source and removes destination files and directories that no longer exist in the source. This behavior directly addresses a dynamic source folder in which content is regularly added and deleted, allowing each periodic run to synchronize the backup location with the current source state.

Robocopy is built into supported Windows versions and is intended for robust file-copy operations, including recurring jobs. It provides operational controls useful for administrative backup workflows, such as retry behavior, logging, restartable copying, and preservation of relevant file metadata through appropriate switches. Administrators should use mirror mode carefully because deletion propagation is intentional: a file deleted from the source will also be deleted from the mirror destination at the next run. Microsoft documents `/MIR` as equivalent to combining directory-tree copying with purging of destination items that are no longer present in the source. See the Microsoft Robocopy command reference and Microsoft's documentation for the Robocopy /MIR parameter.

QUESTION NO: 6

A user installed a new application that automatically starts each time the user logs in to a Windows 10 system. The user does not want this to happen and has asked for this setting to be changed. Which of the following tools would the technician MOST likely use to safely make this change?

A. Registry Editor

B. Task Manager

C. Event Viewer

D. Local Users and Groups

ANSWER: B

Explanation:

Task Manager is the appropriate tool because Windows 10 provides a dedicated Startup tab in Task Manager for reviewing and controlling applications that launch when a user signs in. A technician can open Task Manager, select the Startup tab, identify the newly installed application, and choose Disable. This changes the application's startup status without uninstalling the program or altering its normal ability to run when the user opens it manually.

Using Task Manager is a safe, direct approach because it exposes the startup impact and enabled/disabled status of listed applications in a standard Windows management interface. It also limits the change to the user's stated requirement: preventing automatic launch at logon. If the user later needs the application to start automatically again, the technician can return to the same Startup tab and enable it. Microsoft documents that startup applications can be managed through Task Manager in Windows, including enabling or disabling individual startup entries. See Microsoft Support: Configure startup applications in Windows and Microsoft Learn: Manage Windows startup apps.

QUESTION NO: 7

Which of the following would most likely be used in a small office environment?

A. Print server

B. Virtualization

C. Domain access

D. Workgroup

ANSWER: D

Explanation:

Workgroup is the most likely choice for a small office because it is a peer-to-peer network model designed for straightforward local resource sharing without the infrastructure and administration required by a centralized domain. In a workgroup, each computer maintains its own local user accounts, security settings, and shared resources. Users can share folders and printers directly among a limited number of systems, making this model practical when the organization has only a few devices and does not require centralized identity management, policy enforcement, or a dedicated server.

Windows supports workgroup networking for devices that need to discover and access shared resources on the same local network. A technician configuring such an environment would typically ensure appropriate network discovery and file/printer sharing settings are enabled, then configure local permissions on each system hosting a shared resource. This approach fits the limited scale and simpler administrative requirements commonly associated with a small office. Microsoft describes workgroups as collections of computers that share resources while remaining independently administered, whereas domains provide centralized administration for larger or more managed environments. See Microsoft Learn: Understanding Active Directory and Microsoft Support: File sharing over a network in Windows.

QUESTION NO: 8

A systems administrator is tasked with configuring desktop systems to use a new proxy server that the organization has added to provide content filtering. Which of the following Windows utilities IS the BEST choice for accessing the necessary configuration to complete this goal?

A. Security and Maintenance

B. Network and Sharing Center

C. Windows Defender Firewall

D. Internet Options

ANSWER: D

Explanation:

Internet Options is the best choice because it provides the Windows user-interface path to configure a proxy server for the current user's internet connections. In Internet Options, the administrator can open the *Connections* tab and select *LAN settings*, where they can enable use of a proxy server and specify its address and port. This is the traditional Windows configuration interface for a manually configured forward proxy, including a proxy used to enforce organizational web-content filtering policies. These settings are used by applications that rely on the Windows/WinINet proxy configuration, such as legacy desktop applications and components that use the system internet settings. The same configuration is also surfaced in modern Windows Settings under Network & internet > Proxy, but Internet Options is the named Windows utility that directly exposes the required LAN proxy controls. In a managed enterprise, an administrator might deploy the settings centrally with Group Policy or mobile-device management rather than configure each system manually; however, Internet Options remains the appropriate utility for accessing and validating the underlying desktop proxy configuration. Microsoft documents the Windows proxy settings and the supported manual proxy-server configuration process at Use a proxy server in Windows and describes related policy management in Microsoft Proxy Policy CSP documentation.

QUESTION NO: 9

A technician installed a known-good, compatible motherboard on a new laptop. However, the motherboard is not working on the laptop. Which of the following should the technician MOST likely have done to prevent damage?

A. Removed all jewelry

B. Completed an inventory of tools before use

C. Practiced electrical fire safety

D. Connected a proper ESD strap

ANSWER: A D

Explanation:

Connected a proper ESD strap is essential when handling or installing a laptop motherboard. Motherboards contain static-sensitive integrated circuits, and an electrostatic discharge can damage components immediately or cause latent failures that appear only after installation. A correctly used wrist strap keeps the technician at the same electrical potential as the grounded work surface or approved grounding point, minimizing the chance that a static charge will discharge through the board. This is a core hardware-handling practice covered in the CompTIA A+ objectives under safety procedures and proper use of electrostatic discharge equipment. See the CompTIA exam objectives for the current objective resources.

Removed all jewelry is also an appropriate damage-prevention measure during laptop service. Rings, watches, bracelets, and necklaces can contact exposed circuitry, connectors, or battery terminals while the device is open. Removing these conductive items reduces the risk of accidental bridging or short circuits and prevents jewelry from snagging delicate components. Combined with ESD protection, a clean, grounded workspace and removal of conductive personal items provide safer conditions for motherboard installation. General electrical-safety guidance likewise recommends removing conductive jewelry before working around electrical equipment; see OSHA electrical safety guidance.

QUESTION NO: 10

Which of the following file extensions are commonly used to install applications on a macOS machine? (Select THREE).

A. .mac

B. .Pkg

C. .deb

D. .dmg

E. .msi

F. .appx

G. .app

ANSWER: B D G

Explanation:

`.pkg`, `.dmg`, and `.app` are common macOS application-distribution formats. A `.pkg` file is an installer package handled by the macOS Installer utility. It can install an application and related components, such as support files, scripts, configuration data, or system-wide resources, to appropriate locations on the Mac. Apple documents that software packages can be installed with the system installer tools, reflecting the standard role of package files in macOS deployment workflows.

A `.dmg` file is a disk image. Users commonly download an application in a disk image, open it to mount a virtual disk on the desktop or in Finder, and then copy the included application to the Applications folder. This is a widely used distribution method for standalone macOS software.

A `.app` represents an application bundle: Finder presents the bundle as a single application even though it contains the executable and associated resources internally. An application may be copied directly from a mounted disk image, archive, network share, or external media into Applications and then opened. Apple's guidance on opening apps and installer packages supports these standard macOS application installation and execution methods. See Apple: Open apps on Mac and Apple: Install software packages.

QUESTION NO: 11

A user purchased a netbook that has a web-based, proprietary operating system. Which of the following operating systems is MOST likely installed on the netbook?

A. macOS

B. Linux

C. Chrome OS

D. Windows

ANSWER: C

Explanation:

Chrome OS is the most likely operating system because it was designed by Google as a proprietary, cloud-centric platform for lightweight laptop devices, including the netbooks and low-cost notebooks commonly called Chromebooks. Its user experience centers on the Chrome browser, web applications, and online services, while also supporting Android and Linux applications on compatible devices. Chrome OS is optimized for fast startup, straightforward administration, automatic updates, and security features such as sandboxing and verified boot. These characteristics make it well suited to systems intended primarily for internet access, web-based productivity, and cloud storage rather than traditional locally installed desktop software. Google describes ChromeOS as an operating system built for speed, simplicity, and security, with integrated Google services and browser-based workflows. Although ChromeOS is based on open-source ChromiumOS components, the Chrome OS product installed on commercial Chromebooks includes proprietary Google features and licensing. This precisely matches the description of a web-based, proprietary operating system installed on a netbook. See Google's ChromeOS overview and its Chromebook help documentation for details about ChromeOS features and operation.

QUESTION NO: 12

A user reports that a system is performing unusually and is sending requests to an unfamiliar IP address every five minutes. Which of the following should the technician check first to troubleshoot the issue?

A. Application logs

B. Running processes

C. Antivirus scans

D. Recent system updates

ANSWER: B

Explanation:

Running processes should be checked first because recurring outbound requests to an unfamiliar IP address, combined with unusual system performance, can indicate that an unauthorized or malicious program is executing. Reviewing active processes lets the technician identify unexpected executables, unusually resource-intensive programs, or processes running under an inappropriate user or system context. The technician can then correlate a suspicious process with its executable path, publisher, command line, process ID, and associated network activity. This rapidly establishes whether a currently running program is responsible for the repeated connection and supports the CompTIA troubleshooting approach of identifying symptoms and determining the probable cause before making changes. In Windows, Task Manager can provide an initial view of active processes and resource usage; more detailed investigation can use tools such as Resource Monitor or command-line network utilities to associate connections with process IDs. Microsoft documents process monitoring in Task Manager at Microsoft Support and explains how to inspect TCP/IP connections with Netstat at Microsoft Learn. Once the responsible process is identified, the technician can proceed with appropriate containment, malware remediation, or software investigation.

QUESTION NO: 13

A technician needs to configure a backup solution that will have the least additional expenses and impact on users. Which of the following steps should the technician complete? (Select two.)

A. Configure the backup to run when the user logs in

B. Configure the backup to run after peak hours

C. Use third-party licensed backup software

D. Use the built-in OS backup utility

E. Configure the backup job to run every hour

F. Use an external storage device for the backup

ANSWER: B D

Explanation:

“Configure the backup to run after peak hours” is appropriate because backup operations can consume processor time, disk I/O, network bandwidth, and storage resources. Scheduling the job outside normal business activity reduces the likelihood that users will experience slow application response, delayed file access, or network congestion. A scheduled backup also provides a predictable, repeatable process that can be monitored and adjusted to fit the organization’s operating hours.

“Use the built-in OS backup utility” best supports the requirement for the least additional expense. Operating systems commonly include backup, file-history, recovery, or related data-protection capabilities that can be configured without purchasing a separate backup-software license. Using an included tool lets the technician establish a baseline backup solution while retaining funds for storage media, retention needs, and recovery testing. Microsoft documents built-in Windows backup and restore capabilities, including backup options available through Windows settings and recovery tools. Effective backups should still be verified through periodic restore testing, because a backup is valuable only when the needed data can be recovered successfully. See Microsoft Support: Back up and restore your PC and Microsoft Learn: Windows Server Backup.

QUESTION NO: 14

A user ' s new laptop, which was advertised as gaming-ready, is performing slowly when the user is playing a modern game. However, when the user is playing a less resource-demanding game, the user does not see any lag. Which of the following should a technician do to resolve the issue?

A. Overclock the RAM

B. Enable NIC teaming

C. Select dedicated graphics

D. Activate CPU hyperthreading

ANSWER: C

Explanation:

Select dedicated graphics is correct because a gaming-ready laptop commonly includes both integrated graphics and a discrete, high-performance graphics processor. Integrated graphics prioritize battery life and routine desktop workloads, but may not provide the processing capability or dedicated video memory needed by a current, resource-intensive game. The fact that less-demanding games run without lag is consistent with the laptop being able to handle light graphical workloads while struggling with a title that needs the dedicated graphics processor.

A technician should configure the game or the operating system's per-application graphics preference to use the high-performance dedicated graphics processor. In Windows, this can be configured through Graphics settings for a specific application, selecting the High performance preference. The laptop must also be connected to AC power when appropriate, since some systems limit graphics performance on battery power. Microsoft documents how Windows assigns graphics preferences to individual applications at Graphics settings in Windows. NVIDIA also documents selecting the preferred graphics processor for a program in its control panel at How to select the preferred graphics processor for an application.

QUESTION NO: 15

A technician needs to reimage a desktop in an area without network access. Which of the following should the technician use? (Select two).

A. USB

B. PXE

C. Optical media

D. Partition

E. Boot record

F. SMB

ANSWER: A C

Explanation:

USB and optical media are appropriate because they let the technician perform an offline reimage without requiring access to a network service or shared deployment location. A bootable USB flash drive can contain a Windows installation image, recovery environment, or an imaging utility and image file. The technician can connect the drive, select it from the system's boot menu or configure boot priority in UEFI/BIOS, and start the recovery or operating-system deployment process locally. Optical media provides the same essential capability when the desktop has a compatible optical drive: a bootable DVD can contain installation or recovery files and can be used independently of network connectivity. These removable-media methods are particularly useful for isolated work areas, systems that cannot reach enterprise deployment infrastructure, and bare-metal recovery scenarios. Microsoft documents creating Windows installation media on either a USB flash drive or a DVD, both of which can be used to install or reinstall Windows. Microsoft also documents booting a PC from external installation or recovery media when local recovery is needed. See Create installation media for Windows and Recovery options in Windows.

QUESTION NO: 16

Which of the following is the best way to limit the loss of confidential data if an employee ' s company smartphone is lost or stolen?

A. Installing a VPN

B. Implementing location tracking

C. Configuring remote wipe

D. Enabling backups

ANSWER: C

Explanation:

Configuring remote wipe is the best measure because it enables an authorized administrator or device owner to remotely erase corporate data from a smartphone that is lost or stolen. This directly limits exposure of confidential information by removing locally stored email, files, application data, saved credentials, and organizational settings before an unauthorized person can access them. In a business environment, remote wipe is commonly administered through mobile device management (MDM) or endpoint management tooling. Organizations can use a full-device wipe for company-owned devices or a selective wipe to remove only work accounts and managed corporate data from a personally owned device. The feature is most effective when paired with device enrollment, reliable connectivity, screen-lock controls, and encryption, but its key purpose in this scenario is data removal after loss or theft. CompTIA's Core 2 objectives include remote wipe as a method for securing mobile devices. Microsoft also documents remote wiping as an action available for managed mobile devices, including options to remove company data where supported. See the CompTIA exam objectives and Microsoft Intune remote device actions documentation.

QUESTION NO: 17

A technician is responding to a suspected malware infection on a workstation. The device is displaying unauthorized advertisements and attempting connections to unknown internet addresses. Which of the following should the technician do FIRST? (Select TWO).

A. Disconnect the workstation from the network

B. Document the symptoms

C. Continue using the workstation to monitor the issue

D. Disable all security software

E. Immediately delete all user files

F. Connect removable media to copy unknown files

ANSWER: A B

Explanation:

Disconnect the workstation from the network and **Document the symptoms** are the best initial actions. Disconnecting the workstation from wired and wireless networks helps contain the potential infection. This reduces the chance that malware can communicate with a command-and-control server, spread to other systems, or transmit sensitive information while the technician investigates.

Documenting symptoms preserves useful information, including the time of discovery, observed pop-ups, affected applications, error messages, and suspicious network behavior. This information supports incident handling, escalation, and later verification that remediation was successful. After containment and documentation, the technician can follow organizational procedures for malware scanning, removal, recovery, and user notification. NIST incident-response guidance includes containment and documentation as key activities in handling computer security incidents. See NIST SP 800-61 Rev. 2.

QUESTION NO: 18

A customer who uses a Linux OS called the help desk to request assistance in locating a missing file. The customer does not know the exact name of the file but can provide a partial file name. Which of the following tools should the technician use? (Select two).

A. cat

B. df

C. grep

D. ps

E. dig

F. find

G. top

ANSWER: C F

Explanation:

`find` is the primary Linux utility for locating files within a directory hierarchy. A technician can search using the `-name` test and shell wildcard characters around the known portion of the filename, such as `find /home -name '*partial-name*'`. This approach directly evaluates file and directory names and can be scoped to a likely location, which makes it practical for troubleshooting a missing user file. GNU documents the available name tests and wildcard matching behavior in its find manual.

`grep` is also appropriate when used with a command that produces a list of filenames, such as `find` or `ls`. It filters that output for the partial name or pattern supplied by the customer. For example, a technician could run `find /home -type f | grep 'partial-name'` to narrow a file list to matching paths. This is especially useful when the search criteria require filtering or when filename results need to be refined further. The GNU grep manual describes grep as a utility for selecting lines that match a pattern, which supports this filename-list filtering workflow.

QUESTION NO: 19

A company recently outsourced its night-shift cleaning service. A technician is concerned about having unsupervised contractors in the building. Which of the following security measures can be used to prevent the computers from being accessed? (Select two).

A. Implementing data-at-rest encryption

B. Disabling AutoRun

C. Restricting user permissions

D. Restricting log-in times

E. Enabling a screen lock

F. Disabling local administrator accounts

ANSWER: D E

Explanation:

Restricting log-in times and **Enabling a screen lock** are appropriate controls for reducing the risk that night-shift contractors can interact with company computers. Restricting log-in times, also called logon-hours enforcement, lets an administrator limit when a user account may authenticate. For example, standard employee accounts can be permitted only during the organization's normal business hours. This adds a time-based access control that prevents those accounts from being used during the cleaning shift, even if credentials were otherwise obtained. Microsoft documents the use of account logon-hours settings through the `net user` command: Microsoft Learn: net user.

Enabling a screen lock protects an already signed-in workstation whenever its user is away. A password-protected lock screen requires successful authentication before the existing desktop session can be resumed, preventing an unsupervised person from using applications, files, network resources, or the employee's active credentials. Organizations should configure automatic locking after a short inactivity interval and require a password when the device wakes. Windows supports locking a device manually with Windows key + L and through security policies; see Microsoft Support: Lock your Windows device.

QUESTION NO: 20

A desktop engineer is deploying a master image. Which of the following should the desktop engineer consider when building the master image? (Select TWO).

A. Device drivers

B. Keyboard backlight settings

C. Installed application license keys

D. Display orientation

E. Target device power supply

F. Disabling express charging

ANSWER: A C

Explanation:

When building a master image, the desktop engineer should consider **Device drivers** and **Installed application license keys**. A master image is intended to be deployed repeatedly, so it must include or support the drivers needed for the target hardware. Engineers commonly use a hardware-neutral approach where possible, ensure essential drivers are available, and plan to inject model-specific drivers during deployment. This helps deployed systems correctly recognize components such as storage controllers, network adapters, chipsets, and graphics devices.

Application licensing also requires deliberate planning because cloning an image can duplicate application activation data or license information across many endpoints. The engineer must confirm that licenses permit the intended deployment method and should use volume licensing, subscription licensing, device-based activation, or deployment-time activation where appropriate. Microsoft notes that volume-activation technologies are designed to activate systems at scale, rather than relying on a unique manually installed product key in each cloned installation. Careful driver and licensing planning makes the image portable, supportable, and compliant after it is deployed. See Microsoft documentation on customizing Windows images and Microsoft Volume Activation overview.

QUESTION NO: 21

A user reports that an air-gapped computer may have been infected with a virus after the user transferred files from a USB drive. The technician runs a computer scan with Windows Defender but does not find an infection. Which of the following actions should the technician take next? (Select two).

A. Examine the event logs.

B. Connect to the network.

C. Document the findings.

D. Update the definitions.

E. Reimage the computer.

F. Enable the firewall.

ANSWER: A D

Explanation:

Examine the event logs. is an appropriate next step because Windows Event Viewer can provide evidence of suspicious logons, process failures, application crashes, removable-media activity, or security events that may help establish whether the USB transfer caused unusual system behavior. Reviewing relevant Windows and Microsoft Defender logs gives the technician additional evidence when an initial scan does not detect malware. Microsoft documents that Event Viewer provides access to application, security, setup, system, and forwarded-event logs for troubleshooting and investigation.

Update the definitions. is also appropriate because an antivirus scan is only as effective as its security intelligence and detection signatures. Since the device is air-gapped, the technician should obtain current Microsoft Defender security intelligence updates through an approved clean, offline method, such as downloading the appropriate update package on a trusted system and transferring it using controlled media. After updating the definitions, the technician can run another thorough scan with improved detection coverage for newer threats. Microsoft provides current Defender update packages and guidance at Microsoft Defender updates. For Windows logging and Event Viewer information, see Microsoft Learn: Event Viewer.

QUESTION NO: 22

A malicious user was able to export an entire website's user database by entering specific commands into a field on the company's website. Which of the following did the malicious user most likely exploit to extract the data?

A. Cross-site scripting

B. SQL injection

C. Brute-force attack

D. DDoS attack

ANSWER: B

Explanation:

SQL injection is correct because it occurs when an attacker supplies crafted SQL syntax through an application input field that is subsequently incorporated into a database query. If the website does not properly validate input or use parameterized queries, the attacker may alter the query's intended logic. This can allow unauthorized reading of database records, including an entire user table, rather than limiting the query to the data the application was designed to display. The clue is that the malicious user entered specific commands into a website field and then exported database information: the injected commands were interpreted by the backend database system. Preventing this issue requires treating input as data rather than executable query syntax, primarily by using parameterized queries (prepared statements), along with appropriate input validation and least-privilege database accounts. OWASP describes SQL injection as an application accepting untrusted input that can change the meaning of a query or command, potentially exposing sensitive data. The CompTIA A+ Core 2 objectives include recognizing SQL injection as a common attack vector and identifying its effects. See the OWASP SQL Injection overview and CompTIA exam objectives resource.

QUESTION NO: 23

A PC is taking a long time to boot Which of the following operations would be best to do to resolve the issue at a minimal expense? (Select two).

A. Installing additional RAM

B. Removing the applications from startup

C. Installing a faster SSD

D. Running the Disk Cleanup utility

E. Defragmenting the hard drive

F. Ending the processes in the Task Manager

ANSWER: B D

Explanation:

Removing the applications from startup is an appropriate no-cost first step because each enabled startup application can consume processor time, memory, and storage activity during sign-in. Reviewing the Startup apps list lets a technician disable nonessential software while retaining applications that are needed for security, device functionality, or the user's workflow. Microsoft documents managing these entries through the Task Manager Startup apps section or Windows Settings: Configure startup applications in Windows.

Running the Disk Cleanup utility is also a minimal-expense maintenance action. It removes unnecessary temporary files and other reclaimable data, increasing available storage capacity. A system drive that is short on free space has less room for temporary files, paging activity, updates, and normal operating-system housekeeping, all of which can contribute to poor overall responsiveness during startup. Disk Cleanup can remove selected file categories without requiring new hardware, and it can also be run with elevated privileges to identify additional system files that can be removed. Microsoft's command reference describes the Clean Manager utility and its cleanup options: cleanmgr. Together, limiting unnecessary startup workloads and reclaiming disk space are sensible, low-cost actions before considering hardware upgrades.

QUESTION NO: 24

Which of the following features can be used to ensure a user can access multiple versions of files?

A. Multiple desktops

B. Remote Disc

C. Time Machine

D. FileVault

ANSWER: C

Explanation:

Time Machine is correct because it is the built-in macOS backup feature designed to retain historical copies of data, allowing a user to browse and restore files from earlier backup points. After Time Machine is configured with an appropriate backup destination, such as an external drive, network storage, or another supported disk, it automatically performs backups and preserves versions according to its available storage and retention process. A user can enter the Time Machine interface from Finder, navigate through the timeline of saved backups, select a prior version of a file or folder, and restore it without needing to recover the entire computer. This makes it useful when a document has been overwritten, changed unintentionally, or deleted and an earlier copy is needed. Time Machine can also restore a complete Mac from a backup when necessary, but its file-level historical recovery capability directly addresses access to multiple file versions. Apple describes how to restore individual items using Time Machine in its Time Machine restore guide and provides configuration details in its Back up your Mac with Time Machine guide.

QUESTION NO: 25

A technician is setting up a conference room computer with a script that boots the application on login. Which of the following would the technician use to accomplish this task? (Select TWO).

A. File Explorer

B. Startup Folder

C. System Information

D. Programs and Features

E. Task Scheduler

F. Device Manager

ANSWER: B E

Explanation:

The **Startup Folder** is an appropriate choice because Windows automatically launches shortcuts, applications, or scripts placed in the applicable Startup folder when a user signs in. For a conference-room computer that needs to start a presentation, meeting, or room-control application immediately after login, the technician can place a shortcut to the script in the Startup folder. This provides a straightforward per-user or all-users startup mechanism.

Task Scheduler is also appropriate because it can create a task that runs a program or script using an *At log on* trigger. It provides more administrative control than the Startup folder, including the ability to select a specific user or any user, delay startup, run with elevated privileges when needed, configure retry behavior, and set conditions for execution. This makes it especially useful when the startup script requires controlled timing or permissions. Microsoft documents the Startup-folder behavior in its startup-app management guidance and documents logon-triggered tasks in Task Scheduler guidance: Configure startup applications in Windows and Task Scheduler task triggers.

QUESTION NO: 26

A Windows 10 computer is not installing updates and continues to receive errors even during manual update installations. Which of the following should a technician do to fix the issues? (Select two).

A. Ensure that the Windows Update Utility is the latest version.

B. Refresh local WSUS settings on the computer.

C. Delete the Windows Update cache.

D. Run the System check to verify system files.

E. Reimage the operating system while retaining user files.

F. Reset WMI and re-register system .dlls.

ANSWER: B C

Explanation:

Refreshing local WSUS settings on the computer and deleting the Windows Update cache are appropriate initial remediation steps when a Windows 10 device repeatedly fails to install updates, including updates installed manually. In an organization that uses Windows Server Update Services, the client receives its update-server configuration through local policy and related Windows Update settings. Refreshing those settings forces the device to obtain the current configuration and can restore proper communication with the approved update service. Microsoft describes WSUS client troubleshooting and the importance of validating client configuration and reporting in its WSUS client-agent troubleshooting guidance.

Deleting the Windows Update cache removes locally downloaded update payloads and metadata that may be incomplete or corrupted. Windows can then rebuild its update datastore and download clean copies of required files during the next scan. This is a standard targeted repair before disruptive recovery actions are considered. Microsoft's Windows Update troubleshooting guidance includes resetting update components and clearing update-related cached data when update servicing fails. Together, these actions address both the update source configuration and the local files used by the Windows Update service.

QUESTION NO: 27

A systems administrator is setting up a Windows computer for a new user Corporate policy requires a least privilege environment. The user will need to access advanced features and configuration settings for several applications. Which of the following BEST describes the account access level the user will need?

A. Power user account

B. Standard account

C. Guest account

D. Administrator account

ANSWER: A

Explanation:

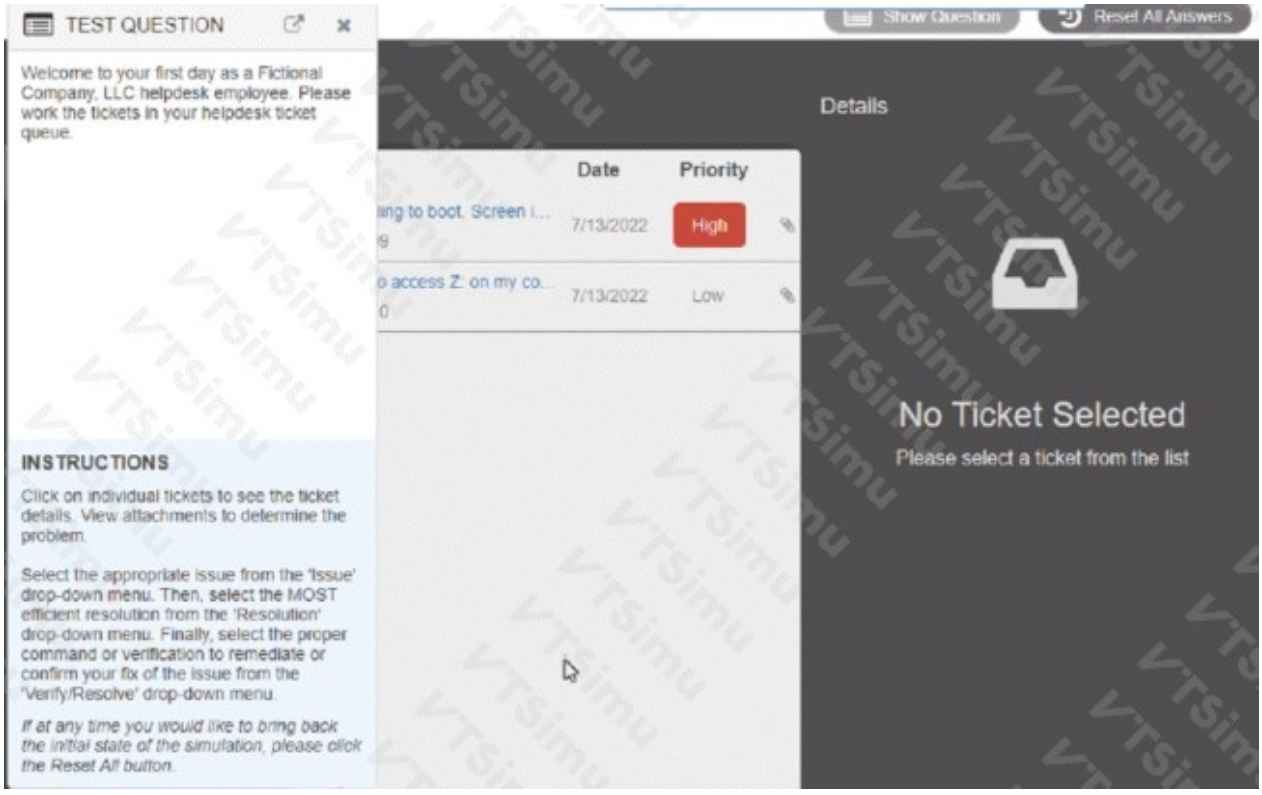
Power user account is the best fit because it provides elevated capabilities for users who must work with advanced application features and selected configuration settings, without assigning the unrestricted privileges associated with a full administrator account. This follows the principle of least privilege: the user receives only the additional access needed to perform assigned duties. In Windows environments, permissions should be granted through the appropriate account type and group membership rather than by making users local administrators by default. Microsoft notes that the built-in Power Users group is a legacy local group and that its permissions can vary by operating-system version and configuration; therefore, an administrator should validate the exact application and system permissions required before using it in a production environment. Where possible, privileges should be scoped to the specific application, folder, or management task required. For the account-level choices in this question, however, a power user level most closely matches the stated need for advanced capabilities while preserving a least-privilege posture. See Microsoft's documentation on Power Users and its guidance on Windows security groups.

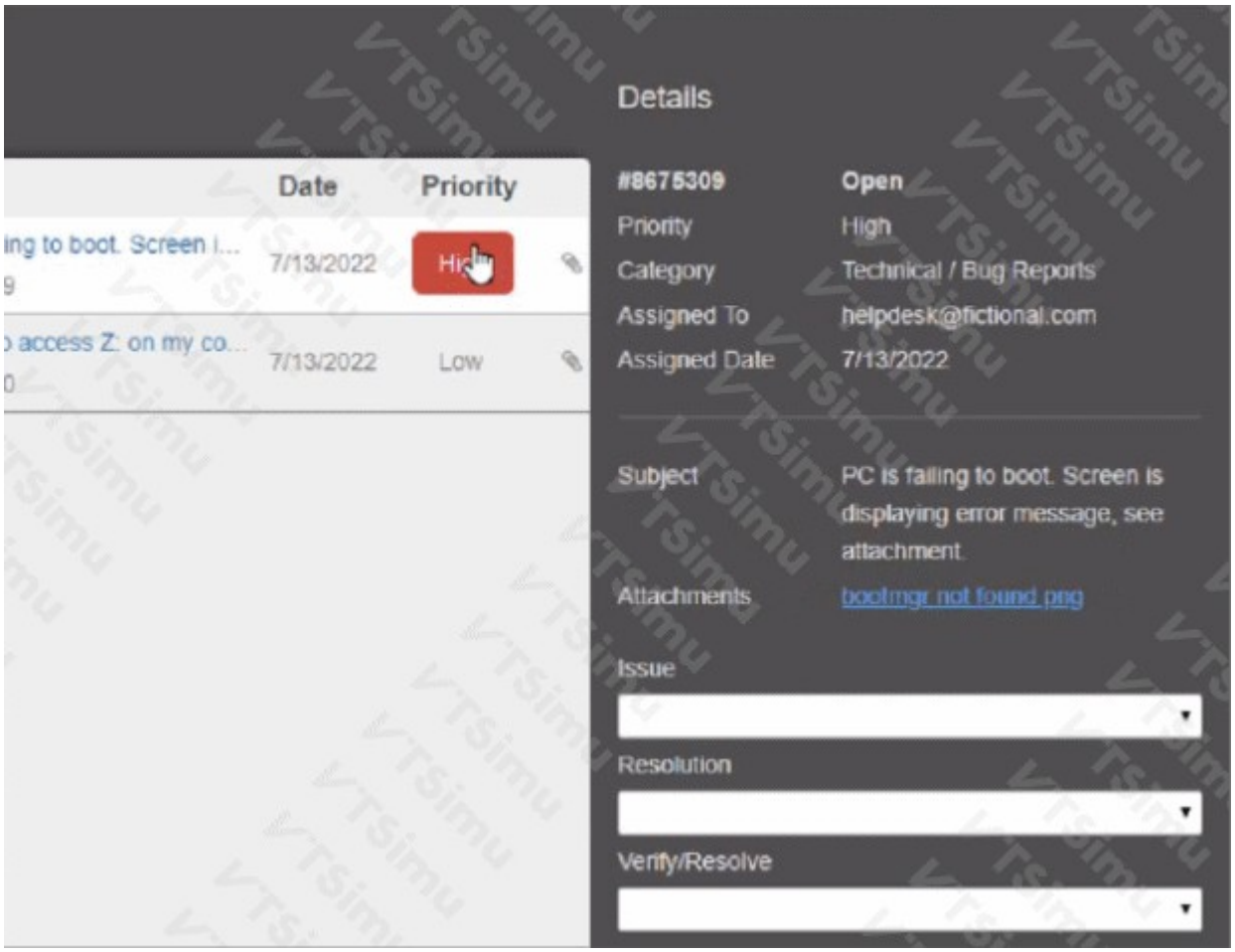
QUESTION NO: 28 - (HOTSPOT)

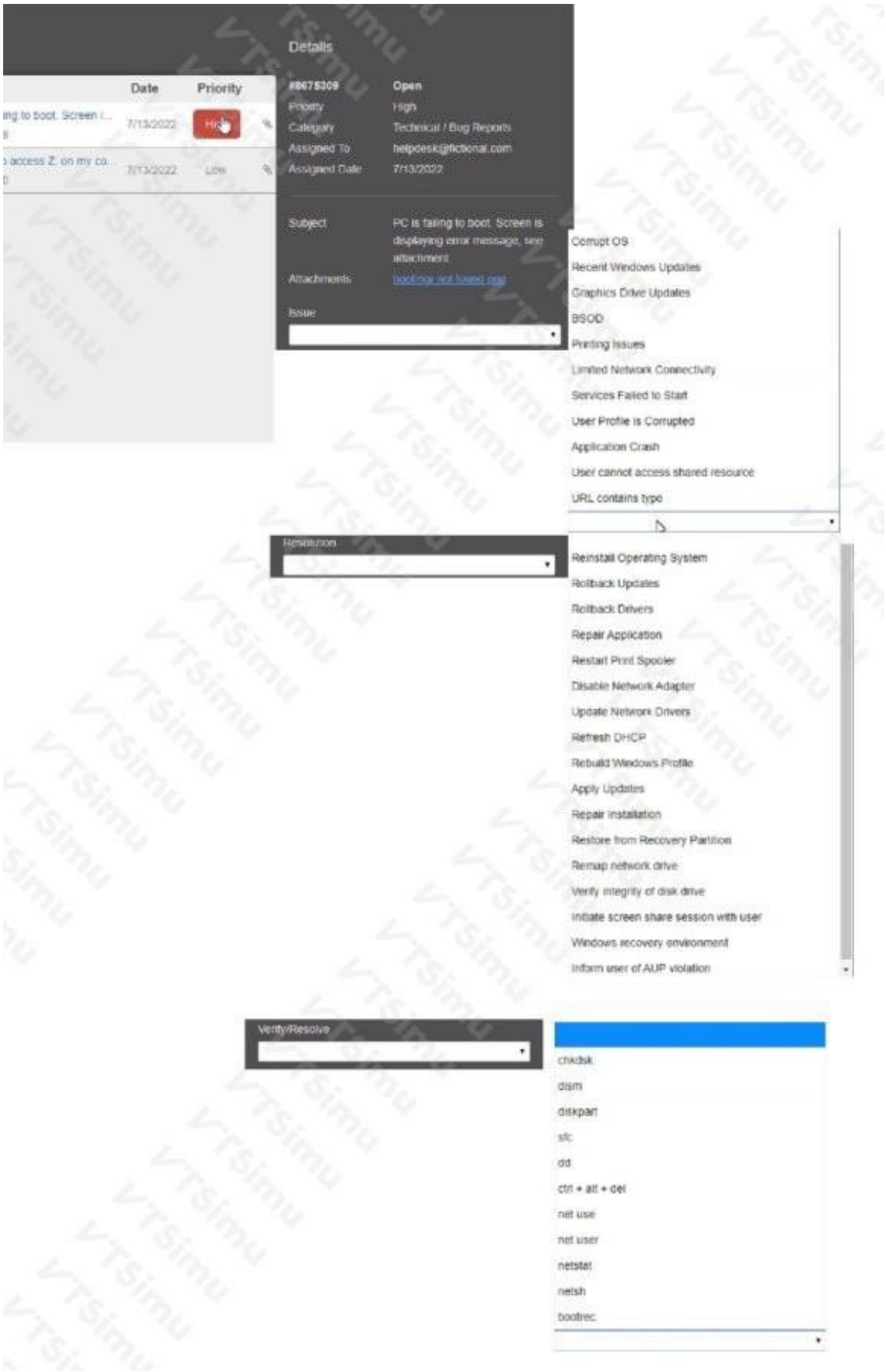
Welcome to your first day as a Fictional Company. LLC helpdesk employee. Please work the tickets in your helpdesk ticket queue.

Click on individual tickers to see the ticket details. View attachments to determine the problem.

Select the appropriate issue from the 'issue' drop-down menu. Then, select the MOST efficient resolution from the 'Resolution' drop-down menu. Finally, select the proper command or verification to remediate or confirm your fix of the issue from the Verify Resolve drop-down menu.




Date
Priority
ing to boot. Screen i...
9
7/13/2022
Hi
access Z: on my co...
0
7/13/2022
Low
Details
#8675309
Open
Priority
High
Category
Technical / Bug Reports
Assigned To
helpdesk@fictional.com
Assigned Date
7/13/2022
Subject
PC is failing to boot. Screen is displaying error message, see attachment.
Attachments
bootmgr not found.png
Issue
Resolution
Verify/Resolve


Date
Priority
Details
#8678309
Open
Priority
High
Category
Technical / Bug Reports
Assigned To
helpdesk@fictional.com
Assigned Date
7/13/2022
Subject
PC is failing to boot. Screen is displaying error message, see attachment
Attachments
bootmgr not found.png
Issue
Corrupt OS
Recent Windows Updates
Graphics Drive Updates
BSOD
Printing Issues
Limited Network Connectivity
Services Failed to Start
User Profile is Corrupted
Application Crash
User cannot access shared resource
URL contains typo
Resolution
Reinstall Operating System
Rollback Updates
Rollback Drivers
Repair Application
Restart Print Spooler
Disable Network Adapter
Update Network Drivers
Refresh DHCP
Rebuild Windows Profile
Apply Updates
Repair Installation
Restore from Recovery Partition
Remap network drive
Verify integrity of disk drive
Initiate screen share session with user
Windows recovery environment
Inform user of AUP violation
Verify/Resolve
chkdsk
dism
diskpart
sfc
dd
ctrl + alt + del
net use
net user
netstat
netsh
bootrec

ANSWER:


Details
Date
Priority
#8675309
Open
Priority
High
Category
Technical / Bug Reports
Assigned To
helpdesk@fictional.com
Assigned Date
7/13/2022
Subject
PC is failing to boot. Screen is displaying error message, see attachment
Attachments
bootrec not fixed.jpg
Issue
Corrupt OS
Recent Windows Updates
Graphics Drive Updates
BSOD
Printing Issues
Limited Network Connectivity
Services Failed to Start
User Profile is Corrupted
Application Crash
User cannot access shared resource
URL contains typo
Resolution
Reinstall Operating System
Rollback Updates
Rollback Drivers
Repair Application
Restart Print Spooler
Disable Network Adapter
Update Network Drivers
Refresh DHCP
Rebuild Windows Profile
Apply Updates
Repair Installation
Restore from Recovery Partition
Remap network drive
Verify integrity of disk drive
Initiate screen share session with user
Windows recovery environment
Inform user of AUP violation
Verify/Resolve
chkdsk
dism
diskpart
sfc
dd
ctrl + alt + del
net use
net user
netstat
net use
net user
netstat
nelsh
bootrec

Explanation:

The correct issue selection is **Corrupt OS**. The ticket describes a computer that cannot complete startup and points to a boot-related attachment, which indicates that Windows system or startup components are damaged or unavailable. The efficient next step is **Repair Installation**. A repair installation is intended to restore a working Windows environment while preserving the existing installation, user profiles, data, and applications as much as possible. This follows the troubleshooting principle of using the least destructive effective remediation before replacing the operating system completely.

For Verify/Resolve, use **bootrec**. The Bootrec tool is designed for Windows Recovery Environment startup repair tasks. It can repair the master boot record, write a new boot sector, scan for Windows installations, and rebuild the Boot Configuration Data store. Those functions directly address a Windows machine that fails at the boot stage because its startup configuration or boot records have been corrupted. Microsoft documents Bootrec and its startup-repair switches at Repair the Windows boot menu. Microsoft also describes recovery options, including methods used to repair an existing installation, at Recovery options in Windows. This selection set identifies the boot failure correctly, preserves the user's environment through repair rather than replacement, and uses the appropriate startup-recovery utility to restore boot capability.

QUESTION NO: 29

Which of the following features allows a technician to configure policies in a Windows 10 Professional desktop?

A. gpedit

B. gpmc

C. gpresult

D. gpupdate

ANSWER: A

Explanation:

gpedit is the appropriate choice because it launches the Local Group Policy Editor on supported Windows editions, including Windows 10 Professional. Local Group Policy Editor provides a graphical administrative interface for configuring policy settings that apply to the local computer and its local users. A technician can use it to manage settings in areas such as security configuration, Windows components, administrative templates, user environment behavior, startup and logon behavior, and system restrictions. These policies are stored locally and are useful when a device is not managed through an Active Directory domain or when a local setting is needed for that individual PC. In practice, the editor is commonly started from the Run dialog, Command Prompt, or Start search using `gpedit.msc`; "gpedit" identifies this Group Policy editing function in the answer choices. Group Policy is a core Windows administrative technology used to centrally or locally define and enforce configuration settings. Microsoft describes Group Policy and its policy-processing model in its Group Policy overview. The CompTIA A+ objectives also include use of Windows administrative tools and command-line utilities relevant to system configuration and troubleshooting; see the official CompTIA exam objectives.

QUESTION NO: 30

Which of the following ensures proprietary information on a lost or stolen mobile device cannot be accessed while the device is offline?

A. Remote wipe

B. Mandatory screen locks

C. Location applications

D. Device data encryption

ANSWER: D

Explanation:

Device data encryption is correct because it protects data stored locally on the mobile device even when the device has no network connection. Encryption converts the proprietary information into unreadable ciphertext, and it can be decrypted only with the appropriate key, typically protected by the user's PIN, password, biometrics, or a hardware-backed security component. Therefore, if a lost or stolen device is offline, an unauthorized person cannot simply remove or browse its storage to view the organization's files. This is particularly important for mobile devices because offline status prevents cloud-based management systems from immediately sending commands or reporting the device's location. Full-device or file-based encryption provides protection at rest independently of connectivity, so it is the control that directly meets the requirement. Microsoft explains that device encryption helps protect data by encrypting the drive and requiring authorized credentials to access it: Microsoft Support: Device encryption in Windows. Android also documents that file-based encryption protects user data through cryptographic keys tied to user authentication: Android Open Source Project: File-based encryption.

QUESTION NO: 31

A user requires local administrative access to a workstation. Which of the following Control Panel utilities allows the technician to grant access to the user?

A. System

B. Network and Sharing Center

C. User Accounts

D. Security and Maintenance

ANSWER: C

Explanation:

User Accounts is the appropriate Control Panel utility because it provides the interface for managing local user account settings, including changing a local account's type. A technician can open User Accounts, select the applicable account, and change its account type to Administrator. This grants the user membership-level administrative privileges on that workstation, allowing the account to perform elevated tasks such as installing approved software, modifying protected system settings, and managing other local accounts when required.

This approach is appropriate when the user needs administrative rights specifically on a standalone or locally managed Windows workstation. The change should be made according to the organization's authorization and least-privilege policies, since administrative accounts have broad control of the device. Microsoft documents that account types determine whether users can make system-wide changes, and that an administrator account can make changes affecting other users and system security. For more information, see Microsoft Support: Manage user accounts in Windows and Microsoft Learn: User Account Control architecture.

QUESTION NO: 32

Which of the following provide the BEST way to secure physical access to a data cento server room? (Select TWO).

A. Biometric lock

B. Badge reader

C. USB token

D. Video surveillance

E. Locking rack

F. Access control vestibule

ANSWER: A B

Explanation:

Biometric lock and Badge reader are the best selections because they are direct physical access-control mechanisms for the server-room entrance. A biometric lock validates a unique physical characteristic, such as a fingerprint, before permitting entry. This provides strong assurance that the person requesting access is an authorized individual and reduces the risk associated with a lost or shared credential. A badge reader enforces access based on an issued credential and can be centrally managed: administrators can grant access only to approved personnel, apply time-based permissions, and promptly revoke access when an employee changes roles or leaves the organization. Badge systems also commonly create access logs that support auditing and incident investigations. Used together, badge-based access and biometric verification provide layered authentication at the point of entry, helping ensure that access to sensitive server infrastructure is limited to authorized staff. This approach aligns with NIST physical access-control guidance, which calls for controlling physical access to systems and facilities and maintaining records of physical access. See NIST SP 800-53, Physical and Environmental Protection controls and CISA Physical Security guidance.

QUESTION NO: 33

Which of the following languages is used for scripting the creation of Active Directory accounts?

A. Bash

B. Structured Query Language

C. Hypertext Preprocessor

D. PowerShell

ANSWER: D

Explanation:

PowerShell is the appropriate scripting language for automating the creation and management of Active Directory accounts in Windows environments. With the Active Directory module installed, an administrator can use cmdlets such as `New-ADUser` to create user objects, set account properties, assign organizational units, and configure credentials in a repeatable script. For example, a PowerShell script can import employee details from a CSV file and create corresponding directory accounts consistently, making it especially useful for onboarding many users or applying standardized account settings. This capability aligns with the administrative automation tasks expected of an IT support professional working with Windows domains. The ActiveDirectory PowerShell module is available on domain controllers and can also be installed through Remote Server Administration Tools on supported administrative workstations. Microsoft documents the `New-ADUser` cmdlet, including its required identity and account-property parameters, at Microsoft Learn: New-ADUser. Guidance for installing and using Windows Server Remote Server Administration Tools is available at Microsoft Learn: Remote Server Administration Tools.

QUESTION NO: 34

A user receives an email that appears to be from the company payroll department. The email requests the user's username, password, and multifactor authentication code to correct a direct-deposit issue. Which of the following should the user do? (Select TWO).

A. Report the message to the security team

B. Contact the payroll department using a known phone number

C. Reply to the message with the requested code

D. Open the attached form to verify the request

E. Forward the message to personal email for review

ANSWER: A B

Explanation:

Report the message to the security team is appropriate because the message is a likely phishing attempt that requests credentials and an MFA code. Reporting enables the organization to investigate the sender, block related messages, and warn other users before additional accounts are targeted.

Contact the payroll department using a known phone number is also appropriate. The user should independently verify the request using trusted contact information rather than replying to the suspicious email or using its links. The FTC advises users not to click links or provide information in unexpected messages and to verify requests independently at How to recognize and avoid phishing scams.

QUESTION NO: 35

A technician is upgrading the Microsoft Windows 10 OS. Which of the following are required for the technician to safely upgrade the OS? (Select two).

A. Release notes

B. Antivirus software

C. Backup of critical data

D. Device drivers

E. Word processing software

F. Safe boot mode

ANSWER: C D

Explanation:

A **Backup of critical data** is required before an operating-system upgrade because upgrades modify core system files, settings, and the boot environment. Although an in-place upgrade is designed to retain user files, a failed installation, disk issue, unexpected power interruption, or rollback problem can make data unavailable. A verified backup provides a recovery path and is a fundamental safety step before making major system changes. Microsoft specifically recommends backing up files before installing or reinstalling Windows so important information can be restored if needed.

Device drivers are also an essential upgrade consideration. The upgraded operating system must have compatible drivers for hardware such as storage controllers, network adapters, graphics hardware, chipsets, printers, and input devices. A technician should confirm driver availability and compatibility before beginning the upgrade and obtain current versions from the device or system manufacturer. This helps ensure that the computer remains usable after the upgrade, including maintaining network connectivity needed for activation, updates, and post-upgrade support. These preparations align with CompTIA's operating-system upgrade considerations and Microsoft's guidance for preparing for Windows installation.

References: Microsoft Support: Back up and restore; Microsoft Learn: Windows drivers.

QUESTION NO: 36

A systems administrator is troubleshooting network performance issues in a large corporate office. The end users report that traffic to certain internal environments is not stable and often drops. Which of the following command-line tools can provide the most detailed information for investigating the issue further?

A. ipconfig

B. arp

C. nslookup

D. pathping

ANSWER: D

Explanation:

pathping is the appropriate tool because it combines route discovery with repeated packet-loss and latency testing at each hop between the local computer and the destination. This is especially useful when connectivity to internal environments is intermittent, because the administrator needs more than confirmation that a host is currently reachable. Pathping first identifies the route, then sends multiple probes over time and calculates statistics for the links and routers involved. Its output can reveal packet loss and delay patterns associated with a particular point along the route, helping narrow the investigation to a network segment, router, or path where instability is occurring. The command is available in Windows and is designed for diagnosing the effect of packet loss and network latency on routed paths. Because the reported symptom is traffic that drops unpredictably, collecting per-hop loss information over a test interval provides detailed evidence for escalation or corrective action. Microsoft documents PathPing syntax, parameters, and its packet-loss reporting behavior at PathPing | Microsoft Learn. Microsoft's network troubleshooting guidance also describes using pathping to identify latency and packet loss across network hops: Troubleshoot network connectivity | Microsoft Learn.

QUESTION NO: 37 - (SIMULATION)

Ann, a CEO, has purchased a new consumer-class tablet for personal use, but she is unable to connect it to the companyâ€™s wireless network. All the corporate laptops are connecting without issue. She has asked you to assist with getting the device online.

INSTRUCTIONS

Review the network diagrams and device configurations to determine the cause of the problem and resolve any discovered issues.

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

ANSWER: See the explanation for the answer

Explanation:

Configure Ann's tablet for the company's **BYOD** wireless network rather than the corporate laptop network.

SSID: `BYOD`
Frequency/Band: `2.4 GHz`
Wireless security mode: `WPA-PSK`
Pre-shared key/password: `TotallySecret`

Do not use the `CORP` SSID, 5 GHz, or WPA2 settings intended for corporate laptops. The consumer tablet must join the BYOD network using its compatible 2.4 GHz WPA-PSK configuration.

QUESTION NO: 38

Which of the following environmental factors are most important to consider when planning the configuration of a data center? (Select two).

A. Temperature levels

B. Location of the servers

C. Humidity levels

D. Noise levels

E. Lighting levels

F. Cable management

ANSWER: A C

Explanation:

Temperature levels and **Humidity levels** are fundamental environmental considerations for a data center because both directly affect the reliable operation and service life of IT hardware. Servers, storage systems, network equipment, and power equipment generate substantial heat. Maintaining an appropriate equipment-inlet temperature with adequate cooling capacity and airflow prevents thermal throttling, unexpected shutdowns, and accelerated component degradation. Data-center thermal planning therefore includes rack layout, hot- and cold-aisle airflow design, cooling systems, and continuous environmental monitoring.

Humidity must also remain within an appropriate operating range. Air that is too dry increases the likelihood of electrostatic discharge, which can damage sensitive electronic components. Conversely, excessive humidity can lead to condensation and corrosion. Effective environmental controls monitor both temperature and humidity throughout the room, particularly near equipment air intakes, and alert staff when conditions approach thresholds. These controls support equipment availability, help prevent hardware failures, and contribute to predictable cooling and operational performance. ASHRAE provides thermal guidance for data-processing environments, and the U.S. Environmental Protection Agency describes airflow and environmental-management practices for efficient data centers. See ASHRAE Technical Committee 9.9 and ENERGY STAR Data Center Equipment.

QUESTION NO: 39

The Chief Executive Officer at a bark recently saw a news report about a high-profile cybercrime where a remote-access tool that the bank uses for support was also used in this crime. The report stated that attackers were able to brute force passwords to access systems. Which of the following would BEST limit the bark's risk? (Select TWO)

A. Enable multifactor authentication for each support account

B. Limit remote access to destinations inside the corporate network

C. Block all support accounts from logging in from foreign countries

D. Configure a replacement remote-access tool for support cases.

E. Purchase a password manager for remote-access tool users

F. Enforce account lockouts after five bad password attempts

ANSWER: A F

Explanation:

Enable multifactor authentication for each support account is appropriate because access requires more than a password, such as a time-based verification code, hardware security key, or biometric factor. Even if an attacker successfully guesses or obtains a support-account password, the additional authentication factor helps prevent the attacker from completing the remote-access login. Multifactor authentication is particularly important for privileged or support accounts because those accounts may provide broad access to systems and sensitive data. NIST identifies phishing-resistant authenticators and multi-factor authentication as important protections for authentication systems: NIST SP 800-63B.

Enforce account lockouts after five bad password attempts directly reduces the feasibility of password brute-forcing by limiting the number of consecutive failed authentication attempts an attacker can make against an account. A lockout or equivalent rate-limiting control forces delays or administrative intervention before further guesses are accepted, substantially increasing the time and effort required to guess credentials at scale. Microsoft recommends account lockout policies as a means to help mitigate password-guessing attacks and provides guidance for configuring thresholds and durations: Microsoft account lockout threshold guidance. Used together, these controls protect both against password guessing and against the use of a compromised password.

QUESTION NO: 40

A technician is installing software on a user's workstation. The installation fails due to incompliance with the HCL. Which of the following components is most likely causing the installation to fail? (Select two).

A. NIC

B. CPU

C. PSU

D. KVM

E. RAM

F. DVI

ANSWER: B E

Explanation:

CPU and RAM are the components most likely to prevent a software installation when the workstation does not meet the supported hardware requirements. Software installers commonly validate the processor architecture and supported instruction set, as well as the amount of available memory, before allowing installation to continue. For example, an application may require a 64-bit processor, a particular processor generation or feature, and a stated minimum amount of RAM. If the installed processor is unsupported, or if memory does not satisfy the product's requirements, the device is not an appropriate hardware platform for that software and installation can fail or be blocked. Reviewing the software vendor's hardware compatibility information and minimum system requirements before deployment confirms whether the workstation configuration is supported. Microsoft similarly publishes processor and memory requirements for its operating systems, illustrating why these platform components are central compatibility checks during installation. See Microsoft's Windows processor requirements and Microsoft's Windows memory limits.

QUESTION NO: 41

Which of the following file types should be used to install software on a macOS computer? (Select two).

A. .yum

B. .pkg

C. .msi

D. .ps1

E. .exe

F. .dmg

ANSWER: B F

Explanation:

`.pkg` and `.dmg` are standard file types used to distribute and install software on macOS. A `.pkg` file is an installer package handled by the macOS Installer app. It can place application files in appropriate locations and may execute approved installation or configuration scripts as part of the installation process. Organizations commonly use signed package installers for managed software deployments because they provide a structured installation workflow. Apple documents the `installer` utility as the command-line tool for installing macOS installer packages: macOS installer command reference.

A `.dmg` file is a macOS disk image. Opening it mounts the image like a removable volume in Finder, exposing its contents. Many application vendors distribute apps in a disk image that contains an application bundle and, commonly, a shortcut to the Applications folder; the user installs the app by copying it there. Disk images can also contain a `.pkg` installer, documentation, or other installation resources. Apple's Disk Utility documentation describes disk images as files that can be opened and mounted to access their contents: Create a disk image using Disk Utility.

QUESTION NO: 42

A technician is configuring a Linux workstation that will be shared by several developers. The developers need to create and modify files in a common project directory, but other local users must not be able to access the directory. Which of the following should the technician configure? (Select TWO).

A. A shared group

B. Group read, write, and execute permissions

C. World read and execute permissions

D. The root account for each developer

E. Full control permissions for all local users

ANSWER: A B

Explanation:

A shared group should be configured so the authorized developers can be assigned membership that grants access to the project directory. Group-based permissions are preferable to assigning permissions individually because access can be managed consistently as developers join or leave the team.

Group read, write, and execute permissions should also be applied to the directory. Read permission permits listing directory contents, write permission permits creating and removing entries, and execute permission permits accessing the directory and its contents. Permissions for other users should remain restricted. Red Hat documents Linux file permissions and ownership at Managing file system permissions.

QUESTION NO: 43

An employee has been using the same password for multiple applications and websites for the past several years. Which of the following would be best to prevent security issues?

A. Configuring firewall settings

B. Implementing expiration policies

C. Defining complexity requirements

D. Updating antivirus definitions

E. Implementing a password manager and using a unique password for every application and website

ANSWER: E

Explanation:

Implementing a password manager and using a unique password for every application and website is the best solution because it directly addresses password reuse. When one reused password is exposed through a phishing attack, credential-stuffing attack, or third-party data breach, an attacker can try that same credential pair against the employee's other accounts. Unique, long passwords limit the impact of a compromise to the affected service rather than allowing one leaked password to expose multiple accounts.

A password manager makes this practical by generating and securely storing strong, distinct passwords, so the employee does not need to memorize numerous credentials. It also supports better day-to-day password hygiene by reducing the temptation to reuse simple, memorable passwords. Current NIST guidance emphasizes screening passwords against known compromised values and does not recommend requiring periodic password changes without evidence of compromise; the priority is resistant, unique authentication secrets. See NIST SP 800-63B and CISA's guidance on using strong passwords.

QUESTION NO: 44

A user is trying to use a third-party USB adapter but is experiencing connection issues. Which of the following tools should the technician use to resolve this issue?

A. taskschd.msc

B. eventvwr.msc

C. devmgmt.msc

D. diskmgmt.msc

ANSWER: C

Explanation:

devmgmt.msc is the appropriate tool because it opens Windows Device Manager, the primary console for diagnosing and managing hardware devices and their drivers. For a third-party USB adapter with connection problems, a technician can use Device Manager to determine whether Windows detects the adapter, inspect its device status and error codes, and review the installed driver details. Device Manager also supports practical remediation steps that directly address common adapter failures, including updating the driver, rolling back a problematic driver update, uninstalling the device so Windows can reinstall it, enabling a disabled device, and scanning for hardware changes after reconnecting the adapter. This is especially useful with third-party peripherals because compatibility, unsigned or outdated drivers, and failed driver installations can prevent normal operation even when the USB port itself is functional. Microsoft describes Device Manager as the tool used to view and control installed hardware and manage device drivers. Additional driver-management guidance is available in Microsoft Support: Open Device Manager and Microsoft Learn: Device and driver installation overview.

QUESTION NO: 45

A company is retiring old workstations and needs a certificate of destruction for all hard drives. Which of the following would be BEST to perform on the hard drives to ensure the data is unrecoverable? (Select TWO).

A. Standard formatting

B. Drilling

C. Erasing

D. Recycling

E. Incinerating

F. Low-level formatting

ANSWER: B E

Explanation:

Drilling and **Incinerating** are appropriate physical-destruction techniques for hard disk drives when the objective is to render stored information unrecoverable before disposal. Drilling damages the drive's platters—the media that holds magnetic data—so that the drive cannot operate normally and data extraction is substantially prevented. For effective destruction, the process should damage all platters rather than only the external casing. Incinerating exposes the storage media to destructive heat, permanently damaging the platters and magnetic layer. These are media-destruction approaches rather than simple logical deletion methods.

Because the organization needs a certificate of destruction, the work should be performed or documented through an approved disposal process, commonly by a qualified IT asset-disposition or media-destruction provider. The certificate should identify the assets or media processed, the destruction method, the date, and the responsible provider or custodian to support audit and compliance requirements. NIST SP 800-88 Rev. 1 identifies destruction as a sanitization method and describes physical techniques, including disintegration and incineration, that make media unusable and information recovery infeasible. See NIST SP 800-88 Rev. 1, Guidelines for Media Sanitization and CompTIA's overview of certificates of destruction.

QUESTION NO: 46

A technician is on-site dealing with an angry customer. The customer thinks the issues have not been addressed, while the technician thinks that the issue has been correctly resolved. Which of the following should the technician do to handle the situation?

A. Insist that the customer is correct and document the concern.

B. Listen to the customer and do not speak at all.

C. Escalate the issue to the next tier.

D. Apologize and ask what would help resolve the issue.

ANSWER: D

Explanation:

“Apologize and ask what would help resolve the issue.” is the most appropriate response because it applies the customer-service and communication practices expected of an IT support professional. The immediate goal is to de-escalate the customer’s frustration, acknowledge that their experience matters, and gain enough information to identify what they believe remains unresolved. An apology in this context expresses empathy for the inconvenience and dissatisfaction; it does not require the technician to prematurely accept an inaccurate technical conclusion. Asking what would resolve the issue shifts the interaction toward a collaborative, solution-focused discussion and gives the customer an opportunity to clarify unmet expectations, remaining symptoms, or business impact. The technician can then verify the reported concern, explain the current status in clear language, and agree on appropriate next steps. This approach preserves professionalism, builds trust, and supports effective resolution while maintaining a respectful on-site interaction. CompTIA’s A+ materials identify communication and professionalism as core skills for IT support roles; see the CompTIA A+ certification overview and the CompTIA exam objectives resource page.

QUESTION NO: 47

A technician needs to update the software on several hundred Mac laptops. Which of the following is the best method to complete the task?

A. SSH

B. MDM

C. RDP

D. SFTP

ANSWER: B

Explanation:

MDM is the best method because it provides centralized, scalable administration for a large fleet of Apple devices. An organization can enroll Mac laptops in an MDM service and use that service to deploy software, schedule or enforce operating-system updates, apply configuration profiles, monitor deployment status, and report on device compliance without requiring a technician to work on each laptop individually. This approach is particularly suited to several hundred systems because policies can be targeted to groups of devices and updates can be staged to reduce disruption and bandwidth demand. Apple’s device-management framework supports declarative device management and software-update controls, allowing administrators to manage update availability and installation across supervised organizational devices. In practice, an MDM platform also provides inventory, security-policy enforcement, remote management, and audit capabilities alongside software deployment, making it an appropriate operational solution rather than merely a remote-access method. Apple describes the management capabilities and deployment workflow in its Apple Platform Deployment guide. For additional detail on managing updates through MDM, see Apple’s Manage software updates documentation.

QUESTION NO: 48

An administrator needs to copy files to a Linux server at another office location so multiple users can access the files. Which of the following is the best for the administrator to use?

A. SFTP

B. RDP

C. DHCP

D. RMM

ANSWER: A

Explanation:

SFTP is the appropriate choice because it is designed specifically for securely transferring files to and from a remote host. SFTP operates as a subsystem of Secure Shell (SSH), typically using TCP port 22, so the administrator can authenticate to the Linux server and copy files through an encrypted connection. Encryption protects both credentials and file contents from interception while data travels between office locations, which is essential when files are transferred across an untrusted network such as the internet or a WAN. Linux servers commonly include an SSH server implementation, making SFTP a standard, interoperable method for administrative file transfers. After the administrator uploads the files to an appropriate shared directory and configures the required server-side permissions or sharing service, authorized users can access them. The key requirement in this scenario is the secure remote copy operation, and SFTP directly supplies that capability without requiring an interactive graphical desktop session. SSH documentation describes SFTP as a secure file-transfer protocol running over the SSH transport: OpenSSH Manuals. For additional protocol background, see the IETF SSH File Transfer Protocol specification: IETF Internet-Draft.

QUESTION NO: 49 - (SIMULATION)

A user reports that after a recent software deployment to upgrade applications, the user can no longer use the Testing program.

However, other employees can successfully use the Testing program.

INSTRUCTIONS

Review the information in each tab to verify the results of the deployment and resolve any issues discovered by selecting the:

Index number of the Event Viewer issue

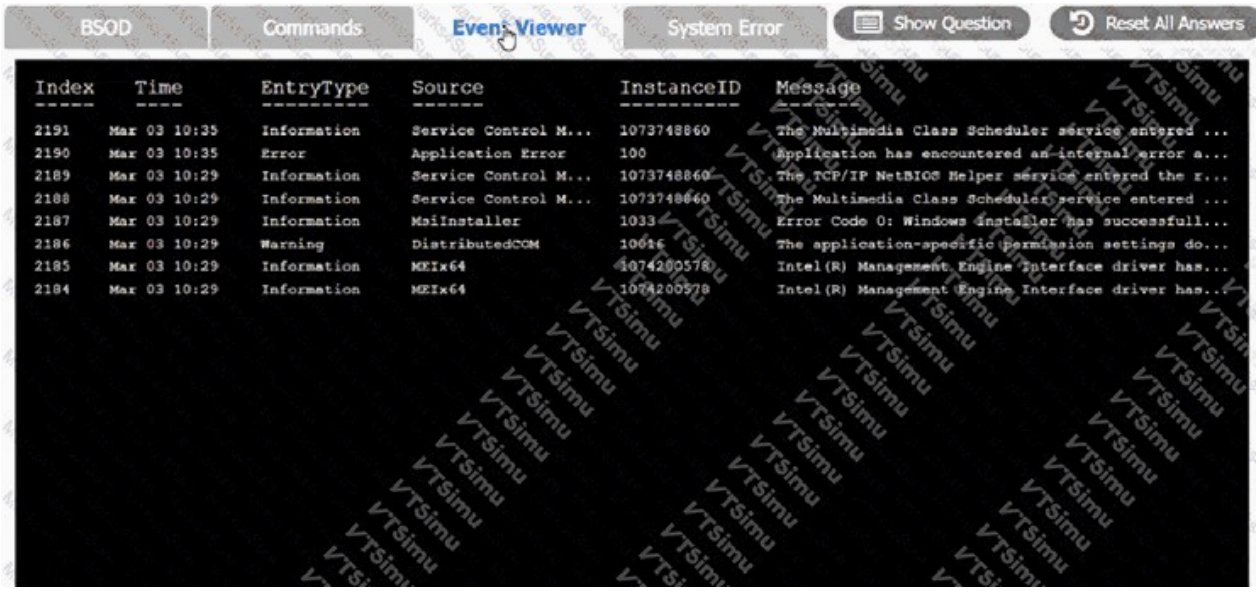
First command to resolve the issue

Second command to resolve the issue

BSOD

Commands:

Event Viewer:



System Error:

ANSWER: See the explanation for the answer

Explanation:

Event Viewer index: `2190`.

This is the relevant entry because it is the only **Error** entry and its source is *Application Error*. Index `2187` is informational and indicates that Windows Installer completed successfully, so it is not the failure to select.

If the System Error tab reports that `MSVCP100.dll` is missing, the proper repair is to reinstall or repair the **Microsoft Visual C++ 2010 Redistributable** required by the Testing application (or repair/reinstall the Testing application). Do **not** copy an arbitrary DLL from another computer and do not use `regsvr32` on `MSVCP100.dll`; it is a Visual C++ runtime library, not a self-registering COM DLL.

The supplied image does not show the available command choices or the BSOD tab, so the exact two command selections and the BSOD selection cannot be verified from the provided material.

QUESTION NO: 50

A technician is replacing the rack mount UPS. Which of the following should the technician consider?

A. Determining the availability of compressed air

B. Getting assistance to lift the hardware

C. Checking local low-voltage regulations

D. Testing the fire suppression system

ANSWER: B

Explanation:

Getting assistance to lift the hardware is the appropriate consideration because rack-mounted UPS units can be very heavy, particularly models with internal battery packs. Their size, weight, and position in a rack create a meaningful risk of back injury, crushed fingers, or damage to rack equipment if one person attempts to remove or install the unit alone. Before beginning the replacement, the technician should evaluate the UPS weight, use the manufacturer's handling instructions, and arrange for another trained person or suitable lifting equipment when needed. The unit should also be supported correctly during removal and installation so it does not shift unexpectedly or place excessive strain on rack rails. This reflects the CompTIA A+ emphasis on following safety procedures and using appropriate lifting techniques when servicing computer

equipment. UPS systems also involve stored electrical energy and batteries, so careful, controlled handling helps protect both personnel and equipment while the unit is being replaced. OSHA's material-handling guidance recommends planning lifts and obtaining help or using mechanical assistance for heavy or awkward loads. See OSHA Manual Material Handling and CompTIA Exam Objectives.

QUESTION NO: 51

A user recently downloaded a free game application on an Android device. The device then began crashing frequently and quickly losing its battery charge. Which of the following should the technician recommend be done first to remediate these issues? (Select two).

A. Uninstall the game application.

B. Perform a factory reset of the device.

C. Connect the device to an external charger.

D. Install the latest security patches.

E. Clear the application's cache.

F. Enable the device's built-in anti-malware protection.

ANSWER: A D

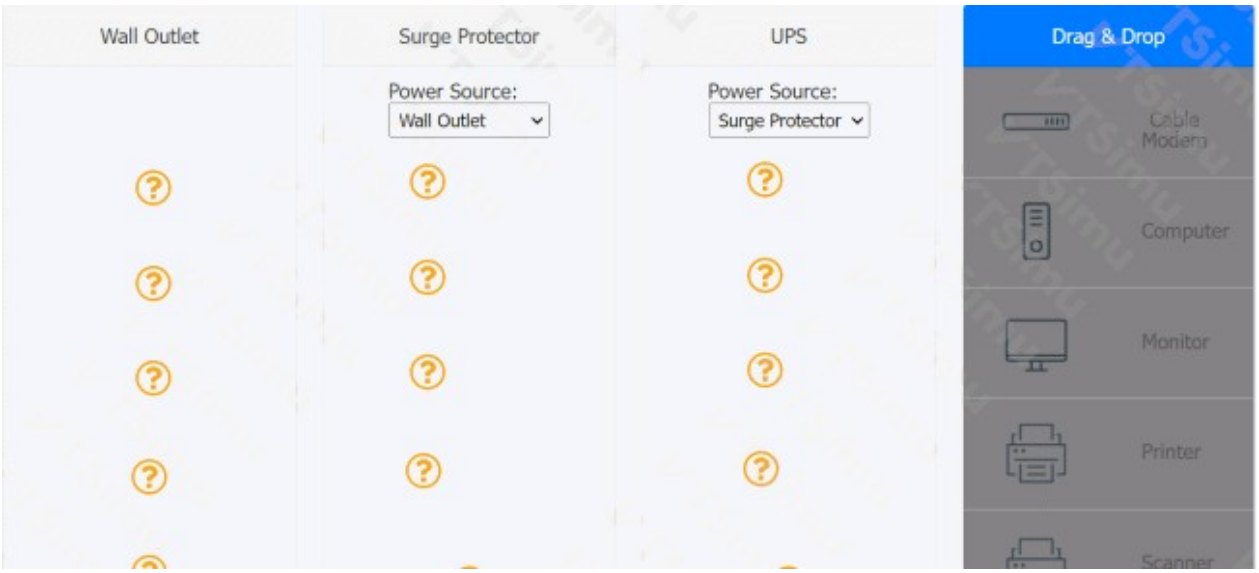
Explanation:

"Uninstall the game application." is an appropriate first remediation step because the crashes and accelerated battery depletion began immediately after that application was installed. Removing the recently added application stops it from continuing to execute, consume battery-intensive resources in the background, or cause instability. The user can remove an Android application through the device's app-management settings, as described in Google's Android Help guidance for deleting apps.

"Install the latest security patches." should also be recommended promptly. Android security and system updates provide fixes for known vulnerabilities, bugs, and stability issues. Applying available updates helps ensure the device has current protections and platform fixes after an application with potentially unsafe or poorly coded behavior has been encountered. Updates should be obtained through the device's normal system-update mechanism and from the device manufacturer or carrier when applicable. Google explains how to check for and install Android updates in its Android system update documentation. Together, removing the suspected source of the symptoms and bringing the operating system's security level current are proportionate initial remediation actions.

QUESTION NO: 52 - (DRAG DROP)

A customer recently experienced a power outage at a SOHO. The customer does not think the components are connected properly. A print job continued running for several minutes after the power failed, but the customer was not able to interact with the computer. Once the UPS stopped beeping, all functioning devices also turned off. In case of a future power failure, the customer wants to have the most time available to save cloud documents and shut down the computer without losing any data.



ANSWER:

Explanation:

A UPS is intended to provide temporary battery power during an outage, allowing a user to save work and perform an orderly shutdown rather than losing data when electricity disappears. For this situation, the UPS should be connected directly to the wall outlet so its battery runtime is available to the equipment that matters most: the computer and monitor, plus the cable modem and Wi-Fi router. Keeping the modem and router powered is important because the customer is working with cloud documents; the network connection can remain available long enough to save outstanding changes before shutting down. APC explains that a UPS provides battery backup power during an outage and is used to keep critical equipment operating long enough for a safe shutdown: APC UPS FAQ.

The printer and scanner should connect to a surge protector that is also plugged directly into the wall outlet. These peripherals do not need battery backup for the customer to save cloud work, and printers can draw substantial power while operating. Reserving the UPS battery capacity for the computer, display, and network equipment increases the time available to save documents and shut down cleanly. A surge protector is appropriate for reducing the risk of damage from voltage spikes, while it does not supply battery power during a blackout. The National Institute of Standards and Technology describes the importance of surge protection for electronic equipment in its surge protective devices guidance.

The resulting layout uses two direct wall connections: one for the UPS and one for the surge protector. The UPS-backed group contains the computer, monitor, cable modem, and Wi-Fi router. The surge-protected group contains the printer and scanner. This arrangement preserves battery runtime for essential work and connectivity while still giving the noncritical peripherals surge protection.

QUESTION NO: 53

Which of the following should be enabled on a mobile device to prevent unauthorized access to data in case the device is lost or stolen? (Select two).

A. Biometric authentication

B. Remote wipe

C. Encryption

D. Device tracking

E. Antivirus software

F. VPN access

ANSWER: A C

Explanation:

Biometric authentication and **Encryption** provide complementary protection for data on a lost or stolen mobile device. Biometric authentication, such as fingerprint or facial recognition, is a device-lock authentication control that helps ensure the device can be unlocked only by its authorized user. This prevents someone who merely possesses the device from accessing applications, files, saved credentials, and other locally available information.

Encryption protects the confidentiality of data stored on the device. When device storage is encrypted, the underlying information is converted into an unreadable form and requires the appropriate decryption key, typically protected by the user's lock-screen credentials or hardware-backed security. Therefore, even if an attacker attempts to remove storage or access the device through unauthorized means, the data remains protected rather than being available in plain text. Together, biometric authentication limits access through the normal user interface, while encryption protects the stored data itself. This layered approach follows standard mobile-device security practice. See Google's overview of Android encryption and Apple's documentation on data protection and encryption.

QUESTION NO: 54

A user reports that antivirus software indicates a computer is infected with viruses. The user thinks this happened white browsing the internet. The technician does not recognize the interface with which the antivirus message is presented. Which of the following is the NEXT step the technician should take?

A. Shut down the infected computer and swap it with another computer

B. Investigate what the interface is and what triggered it to pop up

C. Proceed with initiating a full scan and removal of the viruses using the presented interface

D. Call the phone number displayed in the interface of the antivirus removal tool

ANSWER: B

Explanation:

Investigate what the interface is and what triggered it to pop up is the appropriate next step because an unfamiliar antivirus warning that appears while browsing may be a browser-based scareware or technical-support scam rather than a legitimate alert from the installed security product. The technician should first determine whether the message originated from the web browser, a notification permission, an installed application, or the organization's known antivirus software. This includes identifying the browser tab or process involved, checking the name and publisher of the purported security application, and confirming whether the device's legitimate endpoint-protection console reports an actual detection.

This cautious verification prevents the technician from interacting with a potentially malicious or deceptive prompt. Fraudulent alerts often imitate trusted antivirus products and use alarming language to pressure users into taking immediate action. Establishing the source and trigger supports the CompTIA troubleshooting methodology: identify the problem and

question the user before implementing a remediation plan. Microsoft provides guidance on recognizing and responding to pop-up and technical-support scams in its technical-support scam protection guidance. The CISA malware guidance also emphasizes verifying suspicious activity and using trusted security tools.

QUESTION NO: 55

A technician needs to troubleshoot a user's computer while the user is connected to the system. The technician must also connect to the user's system using remote access tools built in to Windows Which of the following is the best option to troubleshoot the user's computer?

A. Screen share

B. MSRA

C. Virtual network computer

D. RDP

ANSWER: B

Explanation:

MSRA is the correct choice because it is the Microsoft Remote Assistance feature built into Windows and is designed for interactive support of an active user. A technician can initiate or accept a Remote Assistance invitation, view the user's desktop, communicate with the user during the session, and—when the user grants permission—request control of the desktop and input devices. This makes it well suited to troubleshooting an issue while the user remains signed in, can describe the symptoms, and can observe or participate in the repair process. Remote Assistance also emphasizes user consent: the user controls whether to allow the support connection and whether to grant control, which is appropriate for a technician assisting an end user on a live system. Microsoft describes Remote Assistance as a feature that enables a helper to view or control another user's computer remotely with the user's permission. This directly satisfies both requirements: the remote capability is included with Windows, and it supports a connected user during troubleshooting. See Microsoft's Remote Assistance documentation and Remote Assistance support guidance.

QUESTION NO: 56

Which of the following can be used for multifactor authentication when logging in to a computer system? (Select two).

A. Mobile application

B. Video surveillance

C. Access control list

D. Door locks

E. Login script

F. Short Message Service

ANSWER: A F

Explanation:

Mobile application and Short Message Service can be used as an additional authentication factor during a computer-system login. An authenticator mobile application, installed on a registered smartphone, can generate time-based one-time passwords or receive an approval prompt. The user proves possession of the enrolled device by entering the current code or approving the request, in addition to providing a password or another independent factor. Short Message Service can similarly deliver a one-time verification code to a phone number associated with the account. Entering that code demonstrates access to the registered phone and provides a possession-based factor alongside the password. MFA is effective only when it combines credentials from independent factor categories, such as something the user knows and something the user has. These methods are widely implemented for account and operating-system sign-in workflows,

although authenticator apps are generally preferred over SMS where available because they avoid some risks associated with telephone-number attacks. Microsoft describes authentication methods, including authenticator apps and SMS, at Microsoft Entra authentication methods. NIST also discusses out-of-band authentication and verifier-generated one-time codes in NIST SP 800-63B.

QUESTION NO: 57

A company wants to ensure employees are using strong passwords. Which of the following should the company use to enforce password security?

A. Complexity requirement

B. Security questions

C. Account lockout policy

D. Expiration policy

E. Two-factor authentication

ANSWER: A

Explanation:

Complexity requirement is the appropriate control because it directly enforces the characteristics that make a password stronger. Password-complexity settings can require a minimum length and a mix of character types, such as uppercase and lowercase letters, numbers, and symbols. They can also prevent users from choosing passwords that contain their account name or other easily guessed values. By applying these requirements centrally through an operating system, directory service, or identity provider, the company ensures that employees must create passwords meeting the organization's baseline policy rather than relying on voluntary user behavior.

Strong password requirements reduce the likelihood that attackers can successfully guess or crack passwords through common password lists, dictionary attacks, and brute-force attempts. Modern guidance also emphasizes prioritizing password length and screening against known compromised passwords, because long, unique passwords or passphrases provide meaningful resistance to guessing attacks. Password policy controls are a core administrative security measure and can be consistently applied to all relevant employee accounts. For password guidance, see NIST SP 800-63B: Digital Identity Guidelines and Microsoft password policy settings documentation.

QUESTION NO: 58

A user reports that a VPN connection is not working. A technician does not find any internal documentation about this issue. Which of the following should the technician do once the issue is resolved? (Select two).

A. Replace the user's computer to avoid future issues.

B. Note the resolution in the ticket closure message.

C. Create a KB article about the error and share it with the team.

D. Report the error to the user's supervisor.

E. Escalate the ticket to the engineering team for investigation.

F. Update local digital certificates on the user's workstation.

ANSWER: B C

Explanation:

Once the VPN problem has been resolved, the technician should **note the resolution in the ticket closure message** and **create a KB article about the error and share it with the team**. Complete ticket documentation records the symptoms,

troubleshooting performed, root cause when known, and final resolution. This gives the user and support organization an accurate service record, supports accountability, and supplies useful context if the issue recurs. Because no internal documentation existed for this particular VPN issue, creating a knowledge-base article converts the newly discovered solution into a reusable support resource. The article should describe the observed problem, applicable environment, resolution steps, and any validation needed after the repair. Sharing it with the support team improves consistency, reduces time to resolve similar incidents, and helps technicians avoid repeating the same investigation. These actions align with CompTIA A+ operational procedures that emphasize documenting findings, actions, outcomes, and lessons learned after troubleshooting is complete. Microsoft also recommends documenting incident resolution and maintaining knowledge articles so support personnel can apply established solutions to recurring issues. See Microsoft Learn: Knowledge articles and CISA: Incident response.

QUESTION NO: 59

An employee calls the help desk regarding an issue with a laptop PC. After a Windows update, the user can no longer use certain locally attached devices, and a reboot has not fixed the issue. Which of the following should the

technician perform to fix the issue?

A. Disable the Windows Update service.

B. Check for updates.

C. Restore hidden updates.

D. Rollback updates.

ANSWER: D

Explanation:

Rollback updates is the appropriate corrective action because the failure began immediately after a Windows update and persists after restarting the laptop. This timing establishes the update as the most likely recent change responsible for disrupting communication with the locally attached devices. Rolling back, or uninstalling, the problematic update returns the system to the previously working update state, restoring the drivers, services, and compatibility behavior that existed before the issue appeared. In Windows, a technician can remove a recently installed quality update through the recovery or Windows Update history interfaces; if the affected installation was a major feature update, Windows also provides a limited rollback period through Recovery settings. This approach follows standard troubleshooting practice: identify the most recent relevant change, reverse it when it caused a service failure, and then verify that the affected devices function normally. After service is restored, the technician should monitor Windows Update and apply a later corrected update when it becomes available, so the device remains protected while avoiding the known problematic release. Microsoft provides guidance for recovering from update-related device issues and for uninstalling Windows updates at Devices not working after a major Windows update and How to uninstall a Windows update.

QUESTION NO: 60

A technician reports that a SOHO wireless network was compromised by an attacker who brute forced a password to gain access. The attacker was able to modify the DNS settings on the router and spread malware to the entire network. Which of the following configurations would most likely have allowed the attack to take place? (Select two).

A. Guest network

B. TKIP

C. WPS

D. Default login

E. WEP

F. AES

ANSWER: C D

Explanation:

WPS is correct because its PIN-based enrollment mechanism has historically been susceptible to brute-force attacks. The design of the PIN validation process can allow an attacker to test the PIN in sections rather than needing to guess every digit at once, substantially reducing the effort needed to obtain access to the wireless network. Once connected, an attacker may be able to reach the router's management interface, especially when management is available from the local network.

Default login is also correct because unchanged factory-default router administrator credentials are widely known, easily discovered, and commonly targeted by automated tools. An attacker who obtains administrative access to the router can change its DNS server settings, redirecting users to malicious sites or interfering with name resolution. This router-level control can expose every device using that router to malware delivery or phishing activity, which matches the reported network-wide impact. Best practice is to disable WPS when it is not required and replace all default administrative credentials with a unique, strong password; router firmware should also be kept current. NIST's wireless-network guidance discusses securing wireless access and management controls in NIST SP 800-153. CISA also provides practical guidance for protecting home-network routers at Securing Your Home Network.

QUESTION NO: 61

A technician is replacing the processor in a desktop computer prior to opening the computer, the technician wants to ensure the internal components are protected. Which of the following safety procedures would BEST protect the components in the PC? (Select TWO).

A. Utilizing an ESD strap

B. Disconnecting the computer from the power source

C. Placing the PSU in an antistatic bag

D. Ensuring proper ventilation

E. Removing dust from the ventilation fans

F. Ensuring equipment is grounded

ANSWER: A B

Explanation:

Utilizing an ESD strap and disconnecting the computer from the power source are the best procedures to perform before opening a desktop system for processor replacement. An electrostatic discharge strap equalizes the technician's electrical potential with the computer chassis or a properly grounded ESD point. This minimizes the chance that a static charge accumulated on the technician's body will discharge through sensitive semiconductor components, such as the processor, memory, or motherboard circuitry. The strap should be worn against the skin and connected to an appropriate grounding point in accordance with the organization's ESD procedures.

Disconnecting the computer from the power source removes incoming mains power before internal work begins. This protects components by preventing accidental electrical damage while connectors, the processor, or other internal parts are handled. After unplugging the system, a technician should allow stored power to dissipate and follow the device manufacturer's disassembly instructions before servicing. These steps address the two key risks present before opening the case: electrostatic discharge and electrical power. Microsoft's guidance on safe hardware servicing is available through Technician guidelines for servicing computers, and Intel provides processor installation and handling resources at Intel processor installation support.

QUESTION NO: 62

An architecture firm is considering upgrading its computer-aided design (CAD) software to the newest version that forces storage of backups of all CAD files on the software's cloud server. Which of the following is MOST likely to be of concern to the IT manager?

A. All updated software must be tested with all system types and accessories

B. Extra technician hours must be budgeted during installation of updates

C. Network utilization will be significantly increased due to the size of CAD files

D. Large update and installation files will overload the local hard drives.

ANSWER: C

Explanation:

Network utilization will be significantly increased due to the size of CAD files is the primary concern because CAD projects often contain large drawings, models, reference files, renderings, and version histories. A mandatory cloud-backup feature can require substantial outbound WAN bandwidth, especially during the initial upload of the existing file repository. Thereafter, frequent saves, revisions, and synchronization of large project files can continue to consume internet capacity. If the firm's available upload bandwidth is limited, cloud backup traffic can compete with normal business services such as video conferencing, VoIP, web applications, client file transfers, and access to cloud-hosted resources. The IT manager should therefore evaluate the ISP connection's upload capacity, data-transfer limits, backup scheduling, synchronization behavior, and whether quality-of-service controls or bandwidth throttling are available. Microsoft's cloud migration guidance specifically identifies network bandwidth and transfer duration as important planning factors for moving data to cloud storage. Cloud computing also depends on broad network access, making the organization's network connection a key operational dependency. See Microsoft Cloud Adoption Framework: Plan for data transfer and NIST SP 800-145: The NIST Definition of Cloud Computing.

QUESTION NO: 63

A user is unable to print to a network printer. Other users can print successfully, and the technician confirms the user's workstation can communicate with the printer. The print job remains in a status of Printing but never completes. Which of the following should the technician do NEXT?

A. Restart the Print Spooler service

B. Replace the printer toner cartridge

C. Change the workstation's default gateway

D. Reset the printer to factory settings

ANSWER: A

Explanation:

Restart the Print Spooler service is the best next step because the workstation has network connectivity and other users can use the printer, which indicates the issue is likely local to the affected computer. The Print Spooler service manages print jobs sent from Windows to printers. Restarting the service clears its active processing state and can resolve stalled jobs.

If the problem continues, the technician can remove the stuck job and verify the local printer driver and queue configuration. Microsoft documents the Print Spooler service and printer troubleshooting guidance at Fix printer connection and printing problems in Windows.

QUESTION NO: 64

A technician is documenting resolution of a service ticket after replacing a failed laptop battery. Which of the following information should be included in the ticket? (Select TWO).

A. The actions performed

B. The replacement part information

C. The technician's personal phone number

D. The user's account password

E. Unrelated issues reported by other users

ANSWER: A B

Explanation:

The actions performed should be documented so future technicians can understand the troubleshooting and repair steps that were completed. This information supports continuity of service if the issue recurs.

The replacement part information should also be included. Recording the battery model, serial number when applicable, and warranty information supports asset tracking, inventory management, and future warranty claims. Accurate ticket notes are an important part of professional support procedures and establish a useful service history. CompTIA includes documentation and ticketing procedures in its A+ exam objectives, available at CompTIA exam objectives.

QUESTION NO: 65

A company needs to securely and remotely access network devices. Which of the following will allow the company to access these devices?

A. Telnet

B. TKIP

C. RDP

D. SSH

ANSWER: D

Explanation:

SSH is the appropriate protocol for securely administering network devices remotely. Secure Shell establishes an encrypted connection between the administrator's client and the device, protecting credentials, commands, and management traffic from interception or alteration while it crosses an untrusted network. This makes SSH a standard method for command-line configuration, monitoring, and troubleshooting of managed switches, routers, firewalls, servers, and similar devices. In practice, an administrator enables an SSH service on the device, connects using an SSH client, authenticates with a username and password or—preferably—public-key authentication, and then performs authorized management tasks through the encrypted session. SSH also supports integrity protections and strong modern cryptographic algorithms, helping ensure that the administrator is communicating with the intended device and that the session's contents have not been modified in transit. For secure remote device administration, use SSH version 2 and disable obsolete or insecure remote-management services when possible. The SSH protocol is defined in RFC 4251, and Microsoft provides practical guidance for using SSH in its OpenSSH overview.

QUESTION NO: 66

Which of the following operating systems were designed for smartphones? (Select two).

A. Ubuntu

B. CentOS

C. macOS

D. Chrome OS

E. iOS

F. Android

ANSWER: E F

Explanation:

iOS and Android are operating systems specifically designed to power smartphones. Apple develops iOS for the iPhone, integrating the operating system tightly with Apple's mobile hardware, touchscreen interface, cellular capabilities, application ecosystem, and device-management features. Apple describes iOS as the operating system that runs on iPhone and provides the core platform for its mobile features and apps. See Apple's iOS overview.

Android is a mobile operating system used by smartphones from many manufacturers. It is designed around mobile-device requirements such as touch input, wireless networking, telephony support, battery-aware operation, sensors, notifications, and installation of mobile applications. Android's official documentation identifies Android as an open-source software stack for a broad range of devices, including phones, and its platform architecture supports the core services needed by smartphone hardware and applications. See the Android Open Source Project documentation.

Both iOS and Android therefore meet the requirement of being purpose-built smartphone operating systems, making them the two correct selections.

QUESTION NO: 67

Which of the following best describes XFS?

A. A filesystem used by the Linux OS

B. A filesystem used by iOS

C. A filesystem used by the Windows OS

D. A filesystem used by macOS

ANSWER: A

Explanation:

XFS is a high-performance, 64-bit journaling filesystem primarily used on Linux systems. Originally developed by Silicon Graphics for IRIX, it was later ported to Linux and is designed to scale well for large filesystems, very large files, and workloads involving high-throughput I/O. Its journaling capability records filesystem metadata changes, helping support consistency and recovery after an unclean shutdown. XFS is commonly selected in enterprise Linux environments because it handles large storage volumes and parallel I/O efficiently. For example, Red Hat Enterprise Linux supports XFS and uses it as the default filesystem in several releases and deployment scenarios. Therefore, "A filesystem used by the Linux OS" is the best description, since XFS is a Linux filesystem type rather than the native filesystem associated with Apple or Microsoft operating systems. See the Red Hat Enterprise Linux filesystem overview and the Linux kernel XFS documentation for details on its Linux implementation and features.

QUESTION NO: 68

Which of the following would MOST likely be deployed to enhance physical security for a building? (Select TWO).

A. Multifactor authentication

B. Badge reader

C. Personal identification number

D. Firewall

E. Motion sensor

F. Soft token

ANSWER: B E

Explanation:

Badge reader and **motion sensor** are physical-security controls commonly deployed in and around buildings. A badge reader is an access-control device that validates an authorized credential before permitting entry through a controlled door, gate, or other restricted access point. It supports the principle of limiting facility access to approved personnel and can provide an audit trail of access attempts when integrated with an access-control system. A motion sensor detects movement in a monitored area and can trigger an alarm, activate lighting or cameras, or notify security personnel. This helps identify potential unauthorized activity, particularly when a building or restricted area is unoccupied. Both technologies directly protect physical premises, equipment, and personnel rather than solely protecting accounts, software, or network traffic. CompTIA's current A+ Core 2 objectives include physical security measures such as badge readers and motion sensors within the security domain. See the CompTIA exam objectives resource page. For practical guidance on facility access control and monitoring as part of physical security, consult CISA Physical Security.

QUESTION NO: 69

A team of support agents will be using their workstations to store credit card data. Which of the following should the IT department enable on the workstations in order to remain compliant with common regulatory controls? (Select TWO).

A. Encryption

B. Antivirus

C. AutoRun

D. Guest accounts

E. Default passwords

F. Backups

ANSWER: A B

Explanation:

Encryption and antivirus are appropriate controls for workstations that store credit card data. PCI DSS requires stored account data to be protected, including by rendering primary account numbers unreadable wherever they are stored. Strong encryption is a common method for meeting this requirement because it protects the confidentiality of cardholder data if a workstation, drive, or stored file is accessed without authorization. Effective implementation also requires secure encryption-key management, since encryption is only as protective as the controls over the keys.

Antivirus is also required as part of the malware-protection controls applicable to systems that are commonly affected by malicious software, including user workstations. The organization should deploy anti-malware protection, keep it current, and ensure it is actively operating so that malware capable of stealing payment-card data can be detected or prevented. These safeguards address two core goals of payment-card compliance: protecting stored data from disclosure and protecting systems from compromise. PCI Security Standards Council guidance is available at PCI SSC Document Library, and Microsoft summarizes relevant PCI DSS considerations at Microsoft PCI DSS offering documentation.

QUESTION NO: 70

A technician recently installed a new router for a small business. Afterwards, the technician completed an external port scan and generated the following information:

Name	Port	Status
SSH	22	Open
Web	80	Open
Secure Web	443	Open
DNS	53	Open

Which of the following should the technician perform next in order to follow best practices?

A. Migrate to UPnP.

B. Implement IP filtering.

C. Disable any unwanted services.

D. Utilize NAT.

ANSWER: C

Explanation:

Disable any unwanted services is the appropriate next step because an external port scan identifies services that are reachable from outside the business network. Each open and listening service expands the router's attack surface: it may expose an administrative interface, a remote-access protocol, or an application that does not need to be available to internet hosts. The technician should compare the scan results with documented business requirements, retain only explicitly required services, and disable unnecessary router management features, port-forwarding rules, and externally accessible services. This follows the security principle of least functionality, which calls for systems to provide only essential capabilities and to limit unnecessary network services. After making the changes, the technician should repeat the external scan to verify that only intended ports remain exposed and document the approved configuration. NIST guidance for firewalls and boundary protection emphasizes restricting inbound traffic to authorized services and maintaining rules that support the organization's security policy. See the NIST Guidelines on Firewalls and Firewall Policy and the NIST SP 800-53 least functionality control.

QUESTION NO: 71

A technician is configuring remote access to a Linux server in a cloud environment for administration through a terminal window. Which of the following should the technician use to configure remote access?

A. RDP

B. VPN

C. SSH

D. RMM

ANSWER: C

Explanation:

SSH is the appropriate tool for remotely administering a Linux server through a terminal window. Secure Shell provides an encrypted client-server connection that lets an administrator authenticate to the server and execute shell commands, manage files, edit configuration files, install updates, and perform other command-line administrative tasks without exposing the session contents or credentials in plaintext. On Linux systems, this is commonly provided by the OpenSSH server service, `sshd`, which listens on TCP port 22 by default. In a cloud deployment, the technician would typically install and enable the SSH service, permit the required inbound connection in the cloud security group or firewall, and use secure authentication—preferably an SSH key pair rather than a password. SSH is designed specifically for secure terminal-based remote access and is a core administrative protocol for Linux hosts. The OpenSSH project documents SSH as a secure remote-login and command-execution protocol, while Red Hat provides guidance for configuring and using OpenSSH services on Linux. See OpenSSH and Red Hat OpenSSH documentation.

QUESTION NO: 72

A user needs assistance changing the desktop wallpaper on a Windows 10 computer. Which of the following methods will enable the user to change the wallpaper using a Windows 10 Settings tool?

A. Open Settings, select Accounts, select, Your info, click Browse, and then locate and open the image the user wants to use as the wallpaper

B. Open Settings, select Personalization, click Browse, and then locate and open the image the user wants to use as the wallpaper

C. Open Settings, select System, select Display, click Browse, and then locate and open the image the user wants to use as the wallpaper

D. Open Settings, select Apps, select Apps & features, click Browse, and then locate and open the image the user wants to use as the wallpaper.

ANSWER: B

Explanation:

Open Settings, select Personalization, click Browse, and then locate and open the image the user wants to use as the wallpaper is correct because Windows 10 manages desktop background choices through the Personalization settings category. From the Background page, the user can choose Picture as the background type and use the Browse button to select an image file stored locally. After the image is selected, Windows applies it as the desktop wallpaper and also provides display-fit settings, such as Fill, Fit, Stretch, Tile, Center, and Span, to control how the image appears across one or more displays. This is the supported Settings-based workflow for configuring the desktop background in Windows 10. Microsoft documents that users can change their desktop background through the Personalization area and select a picture from available images or browse to another image file. See Microsoft Support: Change your desktop background image. The Settings app and its Personalization controls are also covered in Microsoft Support: Personalize your Windows device.

QUESTION NO: 73

Which of the following best describes when to use the YUM command in Linux?

A. To add functionality

B. To change folder permissions

C. To show documentation

D. To list file contents

ANSWER: A

Explanation:

To add functionality is correct because YUM is a package-management command used on Red Hat Enterprise Linux–family distributions to obtain and manage software from configured repositories. Installing a package adds the program, libraries, services, commands, or other components needed to provide a new capability on the system. For example, an administrator could use `yum install httpd` to install the Apache HTTP Server package, thereby adding web-server functionality. YUM also manages package dependencies, so it identifies and installs required supporting packages automatically when available through the enabled repositories. Beyond initial installation, YUM can update installed software, remove packages, search repositories, and display package information. In newer releases of Red Hat Enterprise Linux, `yum` is provided as a compatibility command backed by DNF, but it continues to be used in many administrative procedures and exam contexts. Package management is therefore the relevant use case when the goal is to extend a Linux system with software-based features. Red Hat documents installing software with YUM/DNF and managing repositories in its software installation guidance. The YUM project also provides command and package-management documentation at yum.baseurl.org.

QUESTION NO: 74

A user's mobile phone has become sluggish A systems administrator discovered several malicious applications on the device and reset the phone. The administrator installed MDM software. Which of the following should the administrator do to help secure the device against this threat in the future? (Select TWO).

A. Prevent a device root

B. Disable biometric authentication

C. Require a PIN on the unlock screen

D. Enable developer mode

E. Block a third-party application installation

F. Prevent GPS spoofing

ANSWER: A E

Explanation:

Preventing a device root and blocking third-party application installation directly reduce the likelihood of malicious applications being installed or gaining elevated control on the mobile device. MDM can enforce policies that identify rooted devices and deny them access to organizational resources or require remediation. Rooting bypasses the operating system's normal security boundaries, potentially allowing malicious software to obtain privileged access, alter protected settings, and evade management controls. Maintaining the manufacturer-supported security model helps preserve application sandboxing, verified boot protections, and the ability to receive security updates.

Blocking third-party application installation restricts users from sideloading apps from unapproved sources. Instead, the organization can require applications to come from an approved enterprise catalog or official managed app store, where applications can be reviewed and distributed under policy. This gives the administrator meaningful control over which software is allowed on enrolled devices and helps prevent recurrence of the malicious-app issue described. Android Enterprise documents that device-management policies can control application installation and unknown sources, while Microsoft documents using mobile application management policies to protect managed devices and apps. See Android Enterprise managed configurations and Microsoft Intune app protection policies.

QUESTION NO: 75

A technician is troubleshooting a userâ€™s PC that is running slowly and displaying frequent pop-ups. The technician thinks malware may be causing the issues, but before the issues began the user installed anti-malware software in response to a pop-up window Which of the following is the most likely cause of these issues'?

A. Expired certificate

B. False alert

C. Missing system files

D. OS update failure

ANSWER: B

Explanation:

False alert is correct because the user acted on an unsolicited pop-up that prompted installation of purported anti-malware software. This is a common social-engineering and malware-delivery technique: a deceptive warning claims that the computer is infected or at risk, then directs the user to install a tool that is actually unwanted or malicious. Such rogue security software may continually generate alarming notifications, display advertisements, consume CPU and memory resources, change browser settings, or install additional malware. Those behaviors directly fit the reported combination of degraded performance and frequent pop-ups beginning after the software installation.

The key diagnostic detail is the sequence of events: the symptoms started after the user responded to a pop-up and installed software, rather than after a normal operating-system maintenance action. A technician should treat unexpected security warnings and software obtained through them as untrusted, isolate the system as appropriate, and follow an approved malware-removal process. Microsoft identifies fake virus alerts and unsolicited pop-ups as scams that can attempt to persuade users to download unsafe software. See Microsoft Support: Protect yourself from tech support scams and CISA: Avoiding social engineering and phishing attacks.

QUESTION NO: 76

A user connected a smartphone to a coffee shop's public Wi-Fi and noticed the smartphone started sending unusual SMS messages and registering strange network activity A technician thinks a virus or other malware has infected the device. Which of the following should the technician suggest the user do to best address these security and privacy concerns? (Select two).

A. Disable Wi-Fi autoconnect.

B. Stay offline when in public places.

C. Uninstall all recently installed applications.

D. Schedule an antivirus scan.

E. Reboot the device

F. Update the OS

ANSWER: C D

Explanation:

“Uninstall all recently installed applications” and “Schedule an antivirus scan” are the most direct actions to remediate a suspected smartphone malware infection. Unusual outgoing SMS messages and unexplained network traffic are common indicators that a malicious application may be running on the device, abusing messaging permissions, communicating with a command-and-control service, or attempting to spread further. Removing recently installed applications is an appropriate first containment and remediation step because a newly installed app is a likely infection source, particularly if it was obtained shortly before the symptoms began. The user should prioritize apps from unknown publishers, apps installed outside the official app store, and apps granted broad permissions.

Scheduling an antivirus scan provides an additional layer of detection and cleanup. A reputable mobile security product can identify known malicious files, apps, and behaviors that remain after suspicious applications are removed. This combination addresses both the probable source of the compromise and possible residual malware. As follow-up hygiene, the user should review application permissions and change passwords from a known-clean device if sensitive accounts may have been exposed. Google provides mobile-security guidance at Google Play Protect Help, and the U.S. Cybersecurity and Infrastructure Security Agency discusses practical mobile-device security measures at Secure Your Mobile Device.

QUESTION NO: 77

Which of the following Windows 10 editions is the most appropriate for a single user who wants to encrypt a hard drive with BitLocker?

A. Professional

B. Home

C. Enterprise

D. Embedded

ANSWER: A

Explanation:

Professional is the most appropriate Windows 10 edition for a single user who specifically needs to encrypt a hard drive with BitLocker. BitLocker Drive Encryption provides full-volume encryption, helping protect data if a computer or its drive is lost, stolen, or accessed offline. It can use a TPM to safeguard encryption keys and can also be configured with startup authentication methods such as a PIN or recovery key. Windows 10 Professional includes the BitLocker management features needed to enable, administer, suspend, and recover BitLocker-protected operating-system and fixed data drives. This makes it a practical fit for an individual, small-business user, or power user who needs business-grade security without purchasing an organizational volume-license edition. Microsoft documents that BitLocker is available on supported Pro,

Enterprise, and Education Windows editions, and it describes BitLocker as a protection mechanism for the operating system, fixed drives, and removable drives. For a single user, Professional delivers the required capability in the most suitable edition among the listed choices. See Microsoft's BitLocker overview and device encryption guidance.

QUESTION NO: 78

A technician needs to perform after-hours service starting at 10:00 p.m. The technician is currently 20 minutes late. The customer will also be late. Which of the following should the technician do considering proper communication techniques and professionalism?

Do not notify the customer if arriving before the customer.

A. Dismiss the customer and proceed with the after-hours work.

B. Contact the customer if the technician is arriving late.

C. Disclose the experience via social media.

ANSWER: B

Explanation:

Contact the customer if the technician is arriving late. is the appropriate professional response because the technician has missed the agreed service start time. Promptly communicating the delay sets accurate expectations, respects the customer's schedule, and gives the customer an opportunity to confirm whether the appointment can still proceed or needs to be rescheduled. This remains important even when the customer has stated that they will also be late: their anticipated arrival time may differ from the technician's, and the technician should not assume that the customer does not need an update.

Professional communication in a support role includes notifying affected parties about schedule changes, providing a concise status update, and confirming the next steps through an appropriate approved contact method. The technician should state that they are delayed, provide a revised estimated arrival time if known, and avoid sharing unnecessary details. This approach demonstrates accountability and helps preserve customer trust during an after-hours engagement. CompTIA's Core 2 exam objectives include professionalism and communication as required workplace skills; see the CompTIA exam objectives resource and the CompTIA A+ certification page.

QUESTION NO: 79

A technician received a call from a user who clicked on a web advertisement Now. every time the user moves the mouse, a pop-up display across the monitor. Which of the following procedures should the technician perform?

A. Boot into safe mode.

B. Perform a malware scan.

C. Restart the machine.

D. Reinstall the browser

ANSWER: A B

Explanation:

"Boot into safe mode." and "Perform a malware scan." are appropriate procedures because unexpected, persistent pop-ups after a user clicks an advertisement are a common symptom of adware or other potentially unwanted software. Safe Mode starts Windows with a limited set of drivers and startup services. This limits the ability of many nonessential applications, including malicious processes configured to run at startup, to load and interfere with diagnosis or removal. Microsoft describes Safe Mode as a troubleshooting environment intended to help isolate problems caused by normal startup software and drivers.

Once the system is in a controlled state, the technician should run an updated anti-malware scan. A scan can identify malicious files, browser-related adware components, unwanted extensions, and persistence mechanisms, then quarantine or remove detected threats. This follows the CompTIA A+ malware-remediation approach of using security tools to remediate an infection after identifying the symptoms. The technician should ensure security definitions are current before scanning and confirm the system is clean after remediation. See Microsoft's Safe Mode guidance and CompTIA's exam objectives resources for relevant troubleshooting and malware-removal concepts.

QUESTION NO: 80

A company recently experienced a security incident in which a USB drive containing malicious software was able to covertly install malware on a workstation. Which of the following actions should be taken to prevent this incident from happening again? (Select two).

A. Install a host-based IDS.

B. Restrict log-in times.

C. Enable a BIOS password.

D. Update the password complexity.

E. Disable AutoRun.

F. Update the antivirus definitions.

G. Restrict user permissions.

ANSWER: E G

Explanation:

Disabling AutoRun prevents Windows from automatically launching content when removable media is connected. This reduces the opportunity for a malicious USB device to trigger an executable or installation routine merely by being inserted. Microsoft documents that AutoRun behavior can be controlled through policy settings, allowing organizations to disable or restrict it for removable drives as part of endpoint hardening: Microsoft AutoPlay documentation.

Restricting user permissions applies the principle of least privilege. Standard users should not have administrative rights that allow software installation, system-wide configuration changes, driver installation, or modification of protected operating-system locations. If malicious code runs from a removable drive under a standard user account, these permission boundaries can prevent or substantially limit an attempted system-level installation. Administrative credentials should be used only when a legitimate task requires elevated access, rather than assigned to everyday workstation accounts. This approach is consistent with Microsoft guidance to minimize privileged access and use standard user accounts for normal work: Microsoft least-privilege guidance.

QUESTION NO: 81

A user's corporate phone was stolen, and the device contains company trade secrets. Which of the following technologies should be implemented to mitigate this risk? (Select TWO).

A. Remote wipe

B. Firewall

C. Device encryption

D. Remote backup

E. Antivirus

F. Global Positioning System

ANSWER: A C

Explanation:

Remote wipe and **Device encryption** provide complementary protection for confidential corporate data when a managed phone is stolen. Remote wipe, normally delivered through a mobile-device-management platform, enables the organization to send a command that removes corporate data from the device after it has been reported missing. This capability limits the period during which sensitive files, application data, saved credentials, and other business information remain available on the lost endpoint. It is especially valuable because the organization can act without needing physical possession of the phone.

Device encryption protects the data while it remains on the phone. Proper full-device encryption makes locally stored information unreadable without successful device authentication and the associated cryptographic keys. Consequently, even before a wipe command can be received or completed, someone who possesses the stolen phone is substantially less able to extract trade secrets from its storage. Organizations should enable encryption before an incident occurs and use strong screen-lock authentication so the encryption keys remain protected. Together, encryption provides immediate protection at rest, while remote wipe provides a response mechanism to remove organizational data after loss or theft. See Google Workspace Admin Help: Wipe a managed mobile device and Apple Platform Security: Data protection overview.

QUESTION NO: 82

A user calls the help desk and reports a workstation is infected with malicious software. Which of the following tools should the help desk technician use to remove the malicious software? (Select TWO).

A. File Explorer

B. User Account Control

C. Windows Backup and Restore

D. Windows Firewall

E. Windows Defender

F. Network Packet Analyzer

ANSWER: A E

Explanation:

Windows Defender is an appropriate primary tool because it is Microsoft's built-in anti-malware solution. A technician can update its security intelligence, run a full or offline scan when necessary, detect malicious files or processes, and quarantine or remove identified threats. This supports a controlled remediation process rather than relying solely on a user's report or manually guessing which files are malicious. Microsoft documents how Defender Antivirus scans and remediates detected threats at Microsoft Defender Antivirus.

File Explorer can also be used as part of removal after the malicious item has been identified by an anti-malware scan or other validated evidence. It enables the technician to locate affected files, review their locations, and delete remaining known malicious files or unwanted artifacts that were not automatically removed. File Explorer also provides access to locations where malware may persist, such as user profile folders, download folders, and startup-related paths. Microsoft describes file-management actions, including deleting files, in its Windows file deletion guidance. Used together, Windows Defender provides detection and remediation, while File Explorer supports removal of confirmed residual files.

QUESTION NO: 83

A company is allowing employees to use personal smartphones for corporate email. Which of the following controls would BEST protect company data while preserving the employees' personal data? (Select TWO).

A. A work profile

B. Selective wipe

C. Full device wipe for every policy violation

D. Disable all personal applications

E. Require the user to share a personal cloud-storage password

ANSWER: A B

Explanation:

A work profile separates managed corporate applications and data from personal applications and data on a personally owned device. This separation enables the organization to apply policies to business resources without controlling unrelated personal content.

Selective wipe enables the administrator to remove organizational accounts, applications, and data when an employee leaves the company or a device is lost, while preserving the employee's personal content. Android Enterprise documents work profiles and management of work data at Android Enterprise overview. Microsoft also documents selective removal of organizational data from managed devices at Intune remote device actions.

QUESTION NO: 84

A field technician applied a Group Policy setting to all the workstations in the network. This setting forced the workstations to use a specific SNTP server. Users are unable to log in now. Which of the following is the MOST likely cause of this issue?

A. The SNTP server is offline.

B. A user changed the time zone on a local machine.

C. The Group Policy setting has disrupted domain authentication on the system,

D. The workstations and the authentication server have a system clock difference.

ANSWER: D

Explanation:

The workstations and the authentication server have a system clock difference. is correct because Active Directory domain logons normally use Kerberos authentication, which depends on synchronized time between the client device and the domain controller/authentication service. Kerberos includes timestamps in authentication requests and tickets to help prevent replay attacks. If the newly assigned SNTP server causes workstation clocks to differ substantially from the authentication server’s clock, Kerberos validation can fail and users may be unable to sign in.

In Windows domains, the default maximum tolerance for computer clock synchronization is five minutes. A technician should verify the time, time zone, and synchronization status on affected workstations and the domain controller, then ensure that the configured SNTP/NTP source is reachable, authoritative, and providing accurate UTC time. Domain members should ultimately synchronize through the domain time hierarchy, with the forest-root PDC emulator synchronized to a reliable external time source. Microsoft documents the Kerberos clock-tolerance policy at Maximum tolerance for computer clock synchronization and provides time-service troubleshooting guidance at Windows Time service tools and settings.