CompTIA.220-1102.vJul-2024.by.Onmotokia.304q

Number: 220-1102
Passing Score: 800
Time Limit: 120
File Version: 13.0

Exam Code: 220-1102
Exam Name: CompTIA A+ Certification Exam: Core 2

Exam A

QUESTION 1
While browsing a website, a staff member received a message that the website could not be trusted.
Shortly afterward, several other colleagues reported the same issue across numerous other websites. Remote users who were not connected to corporate resources did not have any issues.
Which of the following is MOST likely the cause of this issue?

A. A bad antivirus signature update was installed.
B. A router was misconfigured and was blocking traffic.
C. An upstream internet service provider was flapping.
D. The time or date was not in sync with the website.

Correct Answer: D
Section:
Explanation:

QUESTION 2
Security software was accidentally uninstalled from all servers in the environment. After requesting the same version of the software be reinstalled, the security analyst learns that a change request will need to be filled out.
Which of the following is the BEST reason to follow the change management process in this scenario?

A. Owners can be notified a change is being made and can monitor it for performance impact. Most Voted
B. A risk assessment can be performed to determine if the software is needed.
C. End users can be aware of the scope of the change.
D. A rollback plan can be implemented in case the software breaks an application.

Correct Answer: A
Section:
Explanation:
change management process can help ensure that owners are notified of changes being made and can monitor them for performance impact (A). This can help prevent unexpected issues from arising.

QUESTION 3
Which of the following should be done NEXT?

A. Send an email to Telecom to inform them of the issue and prevent reoccurrence.
B. Close the ticket out.
C. Tell the user to take time to fix it themselves next time.
D. Educate the user on the solution that was performed.

Correct Answer: D
Section:
Explanation:
educating the user on the solution that was performed is a good next step after resolving an issue.This can help prevent similar issues from happening again and empower users to solve problems on their own.

QUESTION 4
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

Correct Answer: C
Section:
Explanation:
User Accounts is a Control Panel utility that allows the technician to manage user accounts and groups on a local computer. The technician can use this utility to add a user to the local administrators group, which grants the user local administrative access to the workstation. The other
options are not relevant for this task. Reference: : https://docs.microsoft.com/en-us/windowsserver/identity/ad-fs/operations/manage-user-accounts-and-groups

QUESTION 5
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

Correct Answer: B, E
Section:
Explanation:
Drilling and incinerating are physical destruction methods that make the data on hard drives unrecoverable. Standard formatting, erasing and low-level formatting are logical methods that can be reversed with data recovery tools. Recycling is not a destruction method at all. Verified Reference:
https://www.comptia.org/blog/what-is-a-certificate-of-destruction
https://www.comptia.org/certifications/a

QUESTION 6
A small-office customer needs three PCs to be configured in a network with no server. Which of the following network types is the customer's BEST choice for this environment?

A. Workgroup network
B. Public network
C. Wide area network
D. Domain network

Correct Answer: A
Section:
Explanation:
A workgroup network is a peer-to-peer network where each PC can share files and resources with other PCs without a central server. A public network is a network that is accessible to anyone on the internet. A wide area network is a network that spans a large geographic area, such as a country or a continent. A domain network is a network where a server controls the access and security of the PCs.
Verified Reference: https://www.comptia.org/blog/network-types
https://www.comptia.org/certifications/a

QUESTION 7

A technician is creating a tunnel that hides IP addresses and secures all network traffic. Which of the following protocols is capable of enduring enhanced security?

A. DNS

B. IPS

C. VPN

D. SSH

Correct Answer: C

Section:

Explanation:

A VPN (virtual private network) is a protocol that creates a secure tunnel between two devices over the internet, hiding their IP addresses and encrypting their traffic. DNS (domain name system) is a protocol that translates domain names to IP addresses. IPS (intrusion prevention system) is a device that monitors and blocks malicious network traffic. SSH (secure shell) is a protocol that allows remote access and command execution on another device. Verified Reference:

https://www.comptia.org/blog/what-is-a-vpn https://www.comptia.org/certifications/a

QUESTION 8

A systems administrator is monitoring an unusual amount of network traffic from a kiosk machine and needs to Investigate to determine the source of the traffic. Which of the following tools can the administrator use to view which processes on the kiosk machine are connecting to the internet?

A. Resource Monitor

B. Performance Monitor

C. Command Prompt

D. System Information

Correct Answer: A

Section:

Explanation:

Resource Monitor is a tool that shows the network activity of each process on a Windows machine, including the TCP connections and the sent and received bytes. Performance Monitor is a tool that shows the performance metrics of the system, such as CPU, memory, disk and network usage.

Command Prompt is a tool that allows running commands and scripts on a Windows machine.

System Information is a tool that shows the hardware and software configuration of a Windows machine. Verified Reference: https://www.comptia.org/blog/how-to-use-resource-monitor

https://www.comptia.org/certifications/a

QUESTION 9

A developer receives the following error while trying to install virtualization software on a workstation:

VTx not supported by system Which of the following upgrades will MOST likely fix the issue?

A. Processor

B. Hard drive

C. Memory

D. Video card

Correct Answer: A

Section:

Explanation:

The processor is the component that determines if the system supports virtualization technology (VTx), which is required for running virtualization software. The hard drive, memory and video card are not directly related to VTx support, although they may affect the performance of the virtual machines. Verified Reference: https://www.comptia.org/blog/what-is-virtualization https://www.comptia.org/certifications/a

QUESTION 10
A user's iPhone was permanently locked after several tailed login attempts. Which of the following will restore access to the device?

A. Fingerprint and pattern
B. Facial recognition and PIN code
C. Primary account and password
D. Secondary account and recovery code

Correct Answer: D
Section:
Explanation:
A secondary account and recovery code are used to reset the primary account and password on an iPhone after it has been locked due to failed login attempts. Fingerprint, pattern, facial recognition and PIN code are biometric or numeric methods that can be used to unlock an iPhone, but they are not helpful if the device has been permanently locked. Verified Reference:
https://support.apple.com/en-us/HT204306 https://www.comptia.org/certifications/a

QUESTION 11
An Internet cafe has several computers available for public use. Recently, users have reported the computers are much slower than they were the previous week. A technician finds the CPU is at 100%utilization, and antivirus scans report no current infection. Which of the following is MOST likely causing the issue?

A. Spyware is redirecting browser searches.
B. A cryptominer is verifying transactions.
C. Files were damaged from a cleaned virus infection.
D. A keylogger is capturing user passwords.

Correct Answer: B
Section:
Explanation:
A cryptominer is a malicious program that uses the CPU resources of a computer to generate cryptocurrency, such as Bitcoin or Ethereum. This can cause the CPU to run at 100% utilization and slow down the system. Spyware, virus and keylogger are other types of malware, but they do not necessarily cause high CPU usage. Verified Reference: https://www.comptia.org/blog/what-iscryptomining
https://www.comptia.org/certifications/a

QUESTION 12
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

Correct Answer: A, E
Section:
Explanation:
The correct answers are E. Windows Defender and A. File Explorer. Windows Defender is a built-in antivirus program that can detect and remove malicious software from a workstation. File Explorercan be used to locate and delete files associated with the malicious software

QUESTION 13
A technician has just used an anti-malware removal tool to resolve a user's malware issue on a corporate laptop. Which of the following BEST describes what the technician should do before returning the laptop to the user?

A. Educate the user on malware removal.
B. Educate the user on how to reinstall the laptop OS.
C. Educate the user on how to access recovery mode.
D. Educate the user on common threats and how to avoid them.

Correct Answer: D
Section:
Explanation:
educating the user on common threats and how to avoid them (D) would be a good step before returning the laptop to the user. This can help prevent similar issues from happening again

QUESTION 14
A technician is upgrading the backup system for documents at a high-volume law firm. The current backup system can retain no more than three versions of full backups before failing. The law firm is not concerned about restore times but asks the technician to retain more versions when possible.
Which of the following backup methods should the technician MOST likely implement?

A. Full
B. Mirror
C. Incremental
D. Differential

Correct Answer: C
Section:
Explanation:
The law firm wants to retain more versions of the backups when possible, so the best backup method for the technician to implement in this scenario would be Incremental backup. Incremental backups only save the changes made since the last backup, which allows for more frequent backups and minimizes the amount of storage required. This would allow the law firm to retain more than three versions of backups without risking backup failure.To retain more versions of backups, the technician should implement an Incremental backup method12An incremental backup method only backs up the data that has changed since the last backup, so it requires less storage space than a full backup

QUESTION 15
Which of the following is the MOST basic version of Windows that includes BitLocker?

A. Home
B. pro
C. Enterprise
D. Pro for Workstations

Correct Answer: B
Section:
Explanation:

QUESTION 16
A user receives a notification indicating the data plan on the user's corporate phone has reached its limit. The user has also noted the performance of the phone is abnormally slow. A technician discovers a third-party GPS application was installed on the phone. Which of the following is the MOST likely cause?

A. The GPS application is installing software updates.

B. The GPS application contains malware.

C. The GPS application is updating its geospatial map data.

D. The GPS application is conflicting with the built-in GPS.

Correct Answer: B
Section:
Explanation:
The GPS application contains malware. The third-party GPS application is likely the cause of the slow performance of the phone. The application may contain malware that is using up system resourcesand slowing down the phone. The user should uninstall the application and run a malware scan on the phone1

QUESTION 17
A change advisory board did not approve a requested change due to the lack of alternative actions if implementation failed. Which of the following should be updated before requesting approval again?

A. Scope of change

B. Risk level

C. Rollback plan

D. End user acceptance

Correct Answer: C
Section:
Explanation:
The rollback plan should be updated before requesting approval again. A rollback plan is a plan for undoing a change if it causes problems, and it is an important part of any change management process. If the change advisory board did not approve the requested change due to the lack of alternative actions if implementation failed, then updating the rollback plan would be the best way to address this concern.

QUESTION 18
A user is having phone issues after installing a new application that claims to optimize performance.
The user downloaded the application directly from the vendor's website and is now experiencing high network utilization and is receiving repeated security warnings. Which of the following should the technician perform FIRST to mitigate the issue?

A. Reset the phone to factory settings

B. Uninstall the fraudulent application

C. Increase the data plan limits

D. Disable the mobile hotspot.

Correct Answer: B
Section:
Explanation:
Installing applications directly from a vendor's website can be risky, as the application may be malicious or fraudulent. Uninstalling the application can help mitigate the issue by removing the source of the problem

QUESTION 19
A user enabled a mobile device's screen lock function with pattern unlock. The user is concerned someone could access the mobile device by repeatedly attempting random patterns to unlock the device. Which of the following features BEST addresses the user's concern?

A. Remote wipe

B. Anti-maIware

C. Device encryption

D. Failed login restrictions

Correct Answer: A
Section:
Explanation:
The feature that BEST addresses the user's concern is remote wipe. This is because remote wipeallows the user to erase all data on the mobile device if it is lost or stolen, which will prevent unauthorized access to the device1.

QUESTION 20
When a user calls in to report an issue, a technician submits a ticket on the user's behalf. Which of the following practices should the technician use to make sure the ticket is associated with the correct user?

A. Have the user provide a callback phone number to be added to the ticket
B. Assign the ticket to the department's power user
C. Register the ticket with a unique user identifier
D. Provide the user with a unique ticket number that can be referenced on subsequent calls.

Correct Answer: D
Section:
Explanation:
The technician should provide the user with a unique ticket number that can be referenced on subsequent calls to make sure the ticket is associated with the correct user. This is becauseregistering the ticket with a unique user identifier, having the user provide a callback phone number to be added to the ticket, or assigning the ticket to the department's power user will not ensure that the ticket is associated with the correct user2.

QUESTION 21
Which of the following is the MOST cost-effective version of Windows 10 that allows remote access through Remote Desktop?

A. Home
B. Pro for Workstations
C. Enterprise
D. Pro

Correct Answer: D
Section:
Explanation:
The most cost-effective version of Windows 10 that allows remote access through Remote Desktop is Windows 10 Pro. Windows 10 Pro includes Remote Desktop, which allows users to connect to a remote computer and access its desktop, files, and applications. Windows 10 Home does not includeRemote Desktop, while Windows 10 Pro for Workstations and Windows 10 Enterprise are more expensive versions of Windows 10 that include additional features for businesses

QUESTION 22
Once weekly a user needs Linux to run a specific open-source application that is not available for the currently installed Windows platform. The user has limited bandwidth throughout the day. Which of the following solutions would be the MOST efficient, allowing for parallel execution of the Linux application and Windows applications?

A. Install and run Linux and the required application in a PaaS cloud environment
B. Install and run Linux and the required application as a virtual machine installed under the Windows OS
C. Use a swappable drive bay for the boot drive and install each OS with applications on its own drive Swap the drives as needed
D. Set up a dual boot system by selecting the option to install Linux alongside Windows

Correct Answer: B
Section:
Explanation:
The user should install and run Linux and the required application as a virtual machine installed under the Windows OS. This solution would allow for parallel execution of the Linux application and Windows applications2.
The MOST efficient solution that allows for parallel execution of the Linux application and Windows applications is to install and run Linux and the required application as a virtual machine installedunder the Windows OS. This is because it allows you to run both Linux and Windows together without the need to keep the Linux portion confined to a VM window3.

QUESTION 23
A technician at a customer site is troubleshooting a laptop A software update needs to be downloaded but the company's proxy is blocking traffic to the update site. Which of the following should the technician perform?

A. Change the DNS address to 1.1.1.1
B. Update Group Policy
C. Add the site to the client's exceptions list
D. Verity the software license is current.

Correct Answer: C
Section:
Explanation:
The technician should add the update site to the client’s exceptions list to bypass the proxy. This can be done through the client’s web browser settings, where the proxy settings can be configured. By adding the update site to the exceptions list, the client will be able to access the site and download the software update.

QUESTION 24
A technician is installing new software on a macOS computer. Which of the following file types will the technician MOST likely use?

A. .deb
B. .vbs
C. .exe
D. .app

Correct Answer: D
Section:
Explanation:
The file type that the technician will MOST likely use when installing new software on a macOScomputer is .app. This is because .app is the file extension for applications on macOS1.

QUESTION 25
Which of the following is the MOST important environmental concern inside a data center?

A. Battery disposal
B. Electrostatic discharge mats
C. Toner disposal
D. Humidity levels

Correct Answer: D
Section:
Explanation:
One of the most important environmental concerns inside a data center is the level of humidity. High levels of humidity can cause condensation, which can result in corrosion of components and other equipment. Low levels of humidity can cause static electricity to build up, potentially leading to electrostatic discharge (ESD) and damage to components. Therefore, it is crucial to maintain a relative humidity range of 40-60% in a data center to protect the equipment and ensure proper operation.

QUESTION 26
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

Correct Answer: B
Section:
Explanation:
The account access level the user will need to access advanced features and configuration settings for several applications while adhering to corporate policy requiring a least privilege environment isa standard account. This is because a standard account allows the user to access advanced features and configuration settings for several applications while adhering to corporate policy requiring a least privilege environment1.

QUESTION 27
A change advisory board just approved a change request. Which of the following is the MOST likely next step in the change process?

A. End user acceptance
B. Perform risk analysis
C. Communicate to stakeholders
D. Sandbox testing

Correct Answer: A
Section:
Explanation:

QUESTION 28
A user reports that the hard drive activity light on a Windows 10 desktop computer has been steadily lit for more than an hour, and performance is severely degraded. Which of the following tabs in Task Manager would contain the information a technician would use to identify the cause of this issue?

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

Correct Answer: B
Section:
Explanation:
Processes tab in Task Manager would contain the information a technician would use to identify the cause of this issue. The Processes tab in Task Manager displays all the processes running on the computer, including the CPU and memory usage of each process. The technician can use this tab toidentify the process that is causing the hard drive activity light to remain lit and the performance degradation1

QUESTION 29
A user contacted the help desk to report pop-ups on a company workstation indicating the computer has been infected with 137 viruses and payment is needed to remove them. The user thought the company-provided antivirus software would prevent this issue. The help desk ticket states that the user only receives these messages when first opening the web browser. Which of the following steps would MOST likely resolve the issue? (Select TWO)

A. Scan the computer with the company-provided antivirus software
B. Install a new hard drive and clone the user's drive to it
C. Deploy an ad-blocking extension to the browser.
D. Uninstall the company-provided antivirus software
E. Click the link in the messages to pay for virus removal
F. Perform a reset on the user's web browser

Correct Answer: C, F
Section:
Explanation:
The most likely steps to resolve the issue are to deploy an ad-blocking extension to the browser and perform a reset on the user's web browser. Ad-blocking extensions can help to prevent pop-ups and other unwanted content from appearing in the browser, and resetting the browser can help to remove any malicious extensions or settings that may be causing the issue.

QUESTION 30
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

Correct Answer: A, F
Section:
Explanation:
The best ways to limit the bank's risk are to enable multifactor authentication for each support account and enforce account lockouts after five bad password attempts. Multifactor authentication adds an extra layer of security to the login process, making it more difficult for attackers to gain access to systems. Account lockouts after five bad password attempts can help to prevent brute force attacks by locking out accounts after a certain number of failed login attempts.

QUESTION 31
A technician is asked to resize a partition on the internal storage drive of a computer running macOS.
Which of the followings tools should the technician use to accomplish this task?

A. Consoltf
B. Disk Utility
C. Time Machine
D. FileVault

Correct Answer: B
Section:
Explanation:
The technician should use Disk Utility to resize a partition on the internal storage drive of a computer running macOS. Disk Utility is a built-in utility that allows users to manage disks, partitions, and volumes on a Mac. It can be used to resize, create, and delete partitions, as well as to format disks and volumes.

QUESTION 32
A technician is working with a company to determine the best way to transfer sensitive personal information between offices when conducting business. The company currently uses USB drives and is resistant to change. The company's compliance officer states that all media at rest must be encrypted. Which of the following would be the BEST way to secure the current workflow?

A. Deploy a secondary hard drive with encryption on the appropriate workstation
B. Configure a hardened SFTP portal for file transfers between file servers
C. Require files to be individually password protected with unique passwords
D. Enable BitLocker To Go with a password that meets corporate requirements

Correct Answer: D
Section:
Explanation:
The BEST way to secure the current workflow of transferring sensitive personal information between offices when conducting business is to enable BitLocker To Go with a password that meets corporate requirements. This is because BitLocker To Go is a full-disk encryption feature that encrypts all data on a USB drive, which is what the company currently uses, and requires a password to access the data

QUESTION 33
A technician is configuring a new Windows laptop Corporate policy requires that mobile devices make use of full disk encryption at all limes Which of the following encryption solutions should the technician choose?

A. Encrypting File System
B. FileVault
C. BitLocker
D. Encrypted LVM

Correct Answer: A
Section:
Explanation:
The encryption solution that the technician should choose when configuring a new Windows laptop and corporate policy requires that mobile devices make use of full disk encryption at all times is BitLocker. This is because BitLocker is a full-disk encryption feature that encrypts all data on a hard drive and is included with Window

QUESTION 34
Which of the following must be maintained throughout the forensic evidence life cycle when dealing with a piece of evidence?

A. Acceptable use
B. Chain of custody
C. Security policy
D. Information management

Correct Answer: B
Section:
Explanation:
The aspect of forensic evidence life cycle that must be maintained when dealing with a piece of evidence is chain of custody. This is because chain of custody is the documentation of the movement of evidence from the time it is collected to the time it is presented in court, and it is important to maintain the integrity of the evidence

QUESTION 35
A technician is troubleshooting a customer's PC and receives a phone call. The technician does not take the call and sets the phone to silent. Which of the following BEST describes the technician's actions?

A. Avoid distractions
B. Deal appropriately with customer's confidential material
C. Adhere to user privacy policy
D. Set and meet timelines

Correct Answer: A
Section:
Explanation:
The technician has taken the appropriate action by not taking the call and setting the phone to silent in order to avoid any distractions and remain focused on the task at hand. This is a good example of how to maintain focus and productivity when working on a customer's PC, and will help to ensure that the job is completed in a timely and efficient manner.

QUESTION 36
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 alt 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.

Correct Answer: C
Section:
Explanation:
The IT manager is most likely to be concerned about network utilization being significantly increased due to the size of CAD files. Backing up all CAD files to the software's cloud server can result in a large amount of data being transferred over the network, which can cause network congestion and slow down other network traffic.

QUESTION 37
A wireless network is set up, but it is experiencing some interference from other nearby SSIDs.
Which of the following can BEST resolve the interference?

A. Changing channels
B. Modifying the wireless security
C. Disabling the SSIO broadcast
D. Changing the access point name

Correct Answer: A
Section:
Explanation:
Changing channels can best resolve interference from other nearby SSIDs. Wireless networks operate on different channels, and changing the channel can help to avoid interference from other nearby networks.

QUESTION 38
A technician suspects a rootkit has been installed and needs to be removed. Which of the following would BEST resolve the issue?

A. Application updates
B. Anti-malware software
C. OS reinstallation
D. File restore

Correct Answer: C
Section:
Explanation:
If a rootkit has caused a deep infection, then the only way to remove the rootkit is to reinstall the operating system. This is because rootkits are designed to be difficult to detect and remove, and they can hide in the operating system's kernel, making it difficult to remove them without reinstalling the operating systemhttps://www.minitool.com/backup-tips/how-to-get-rid-of-rootkit-windows-10.html

QUESTION 39
A customer reported that a home PC with Windows 10 installed in the default configuration is having issues loading applications after a reboot occurred in the middle of the night. Which of the following is the FIRST step in troubleshooting?

A. Install alternate open-source software in place of the applications with issues

B. Run both CPU and memory tests to ensure that all hardware functionality is normal
C. Check for any installed patches and roll them back one at a time until the issue is resolved
D. Reformat the hard drive, and then reinstall the newest Windows 10 release and all applications.

Correct Answer: C
Section:
Explanation:
The first step in troubleshooting is to check for any installed patches and roll them back one at a time until the issue is resolved. This can help to identify any patches that may be causing the issue and allow them to be removed.

QUESTION 40
A technician has been tasked with installing a workstation that will be used tor point-of-sale transactions. The point-of-sale system will process credit cards and loyalty cards. Which of the following encryption technologies should be used to secure the workstation in case of theft?

A. Data-in-transit encryption
B. File encryption
C. USB drive encryption
D. Disk encryption

Correct Answer: D
Section:
Explanation:
Disk encryption should be used to secure the workstation in case of theft. Disk encryption can help to protect data on the hard drive by encrypting it so that it cannot be accessed without the correct encryption key

QUESTION 41
A company installed a new backup and recovery system. Which of the following types of backups should be completed FIRST?

A. Full
B. Non-parity
C. Differential
D. Incremental

Correct Answer: A
Section:
Explanation:
The type of backup that should be completed FIRST after installing a new backup and recovery system is a full backup. This is because a full backup is a complete backup of all data and is the foundation for all other backups. After a full backup is completed, other types of backups, such as differential and incremental backups, can be performed.

QUESTION 42
A call center technician receives a call from a user asking how to update Windows Which of the following describes what the technician should do?

A. Have the user consider using an iPad if the user is unable to complete updates
B. Have the user text the user's password to the technician.
C. Ask the user to click in the Search field, type Check for Updates, and then press the Enter key
D. Advise the user to wait for an upcoming, automatic patch

Correct Answer: C
Section:
Explanation:

The technician should guide the user to update Windows through the built-in "Check for Updates" feature. This can be done by having the user click in the Search field, type "Check for Updates", and then press the Enter key. This will bring up the Windows Update function, which will search for any available updates and give the user the option to install them.

QUESTION 43
Someone who is fraudulently claiming to be from a reputable bank calls a company employee. Which of the following describes this incident?

A. Pretexting
B. Spoofing
C. Vishing
D. Scareware

Correct Answer: C
Section:
Explanation:
Vishing is a type of social engineering attack where a fraudulent caller impersonates a legitimate entity, such as a bank or financial institution, in order to gain access to sensitive information. The caller will typically use a variety of techniques, such as trying to scare the target or providing false information, in order to get the target to provide the information they are after. Vishing is often used to gain access to usernames, passwords, bank account information, and other sensitive data.

QUESTION 44
A company is Issuing smartphones to employees and needs to ensure data is secure if the devices are lost or stolen. Which of the following provides the BEST solution?

A. Anti-malware
B. Remote wipe
C. Locator applications
D. Screen lock

Correct Answer: B
Section:
Explanation:
This is because remote wipe allows the data on the smartphone to be erased remotely, which helps to ensure that sensitive data does not fall into the wrong hands.

QUESTION 45
A technician is setting up a SOHO wireless router. The router is about ten years old. The customer would like the most secure wireless network possible. Which of the following should the technician configure?

A. WPA2 with TKIP
B. WPA2withAES
C. WPA3withAES-256
D. WPA3 with AES-128

Correct Answer: B
Section:
Explanation:
This is because WPA2 with AES is the most secure wireless network configuration that is available on a ten-year-old SOHO wireless router.

QUESTION 46
A technician has been tasked with using the fastest and most secure method of logging in to laptops.
Which of the following log-in options meets these requirements?

A. PIN
B. Username and password
C. SSO
D. Fingerprint

Correct Answer: A
Section:
Explanation:
This is because a PIN is a fast and secure method of logging in to laptops, and it is more secure than a password because it is not susceptible to keyloggers.

QUESTION 47
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

Correct Answer: A, B
Section:
Explanation:
The two safety procedures that would best protect the components in the PC are: Utilizing an ESD strap Placing the PSU in an antistatic bag https://www.professormesser.com/free-a-plus-training/220-902/computer-safety-procedures-2/
https://www.skillsoft.com/course/comptia-a-core-2-safety-procedures-environmental-impacts- cbdf0f2c-61c0-4f4a-a659-dc98f1f00158

QUESTION 48
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

Correct Answer: C, E
Section:
Explanation:
To help secure the device against this threat in the future, the administrator should require a PIN on the unlock screen and block a third-party application installation. Requiring a PIN on the unlock screen can help to prevent unauthorized access to the device, while blocking third-party application installation can help to prevent malicious applications from being installed on the device.

QUESTION 49
A company wants to remove information from past users' hard drives in order to reuse the hard drives Witch of the following is the MOST secure method

A. Reinstalling Windows
B. Performing a quick format
C. Using disk-wiping software
D. Deleting all files from command-line interface

Correct Answer: C
Section:
Explanation:
Using disk-wiping software is the most secure method for removing information from past users’ hard drives in order to reuse the hard drives. Disk-wiping software can help to ensure that all data on the hard drive is completely erased and cannot be recovered.

QUESTION 50
A technician is configuring a SOHO device Company policy dictates that static IP addresses cannot be used. The company wants the server to maintain the same IP address at all times. Which of the following should the technician use?

A. DHCP reservation
B. Port forwarding
C. DNS A record
D. NAT

Correct Answer: A
Section:
Explanation:
The technician should use DHCP reservation to maintain the same IP address for the server at all times. DHCP reservation allows the server to obtain an IP address dynamically from the DHCP server, while ensuring that the same IP address is assigned to the server each time it requests an IP address.

QUESTION 51
A user is unable to use any internet-related functions on a smartphone when it is not connected to Wi-Fi When the smartphone is connected to Wi-Fi the user can browse the internet and send and receive email. The user is also able to send and receive text messages and phone calls when the smartphone is not connected to Wi-Fi. Which of the following is the MOST likely reason the user is unable to use the internet on the smartphone when it is not connected to Wi-Fi?

A. The smartphone's line was not provisioned with a data plan
B. The smartphone's SIM card has failed
C. The smartphone's Bluetooth radio is disabled.
D. The smartphone has too many applications open

Correct Answer: A
Section:
Explanation:
The smartphone’s line was not provisioned with a data plan. The user is unable to use any internet- related functions on the smartphone when it is not connected to Wi-Fi because the smartphone’sline was not provisioned with a data plan. The user can send and receive text messages and phone calls when the smartphone is not connected to Wi-Fi because these functions do not require an internet connection1

QUESTION 52
Which of the following Wi-Fi protocols is the MOST secure?

A. WPA3
B. WPA-AES

C. WEP
D. WPA-TKIP

Correct Answer: A
Section:
Explanation:

QUESTION 53
A user attempts to open some files, but a message appears stating that the files are encrypted. The user was able to access these files before without receiving this message and no changes have been made within the company. Which of the following has infected the computer?

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

Correct Answer: C
Section:
Explanation:
Ransomware is malicious software that encrypts files on a computer, making them inaccessible until a ransom is paid. In this case, the user was able to access the files before without issue, and no changes have been made within the company, so it is likely that the computer was infected with ransomware.

QUESTION 54
A help desk technician is troubleshooting a workstation in a SOHO environment that is running above normal system baselines. The technician discovers an unknown executable with a random string name running on the system. The technician terminates the process, and the system returns to normal operation. The technician thinks the issue was an infected file, but the antivirus is not detecting a threat. The technician is concerned other machines may be infected with this unknown virus. Which of the following is the MOST effective way to check other machines on the network for this unknown threat?

A. Run a startup script that removes files by name.
B. Provide a sample to the antivirus vendor.
C. Manually check each machine.
D. Monitor outbound network traffic.

Correct Answer: C
Section:
Explanation:
The most effective way to check other machines on the network for this unknown threat is to manually check each machine. This can help to identify any other machines that may be infected with the unknown virus and allow them to be cleaned.

QUESTION 55
A user reports that a PC seems to be running more slowly than usual. A technician checks system resources, but disk, CPU, and memory usage seem to be fine. The technician sees that GPU temperature is extremely high. Which of the following types of malware is MOST likely to blame?

A. Spyware
B. Cryptominer
C. Ransormvare
D. Boot sector virus

Correct Answer: B
Section:
Explanation:
The type of malware that is most likely to blame for a PC running more slowly than usual and having an extremely high GPU temperature is a “cryptominer”. Cryptominers are a type of malware that use the resources of a computer to mine cryptocurrency. This can cause the computer to run more slowly than usual and can cause the GPU temperature to rise. Spyware is a type of malware that is used to spy on a user’s activities, but it does not typically cause high GPU temperatures. Ransomware is a type of malware that encrypts a user’s files and demands payment to unlock them, but it does nottypically cause high GPU temperatures. Boot sector viruses are a type of malware that infects the boot sector of a hard drive, but they do not typically cause high GPU temperatures12

QUESTION 56
Upon downloading a new ISO, an administrator is presented with the following string:
59d15a16ce90cBcc97fa7c211b767aB Which of the following BEST describes the purpose of this string?

A. XSS verification
B. AES-256 verification
C. Hash verification
D. Digital signature verification

Correct Answer: C
Section:
Explanation:
Hash verification is a process that verifies the integrity of a file by comparing the hash value of the downloaded file to the hash value provided by the source1

QUESTION 57
Which of the following OS types provides a lightweight option for workstations thai need an easy-touse browser-based interface?

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

Correct Answer: B
Section:
Explanation:
Chrome OS provides a lightweight option for workstations that need an easy-to-use browser-based interface1

QUESTION 58
Following the latest Windows update PDF files are opening in Microsoft Edge instead of Adobe Reader. Which of the following utilities should be used to ensure all PDF files open in Adobe Reader?

A. Network and Sharing Center
B. Programs and Features
C. Default Apps
D. Add or Remove Programs

Correct Answer: C
Section:
Explanation:
Default Apps should be used to ensure all PDF files open in Adobe Reader

QUESTION 59
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

Correct Answer: A, B
Section:
Explanation:
A biometric lock requires an authorized user to provide a unique biometric identifier, such as a fingerprint, in order to gain access to the server room. A badge reader requires an authorized user to swipe an access card in order to gain access. Both of these methods ensure that only authorized personnel are able to access the server room. Additionally, video surveillance and access control vestibules can be used to further secure the server room. Finally, a locking rack
can be used to physically secure the servers, so that they cannot be accessed without the appropriate key.

QUESTION 60
During a recent flight an executive unexpectedly received several dog and cat pictures while trying to watch a movie via in-flight Wi-Fi on an iPhone. The executive has no records of any contacts sending pictures like these and has not seen these pictures before. To BEST resolve this issue, the executive should:

A. set AirDrop so that transfers are only accepted from known contacts
B. completely disable all wireless systems during the flight
C. discontinue using iMessage and only use secure communication applications
D. only allow messages and calls from saved contacts

Correct Answer: A
Section:
Explanation:
To best resolve this issue, the executive should set AirDrop so that transfers are only accepted from known contacts (option A). AirDrop is a feature on iOS devices that allows users to share files, photos, and other data between Apple devices. By setting AirDrop so that it only accepts transfers from known contacts, the executive can ensure that unwanted files and photos are not sent to their device. Additionally, the executive should ensure that the AirDrop setting is only enabled when it is necessary, as this will protect their device from any unwanted files and photos.

QUESTION 61
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

Correct Answer: B
Section:
Explanation:

The technician should not proceed with initiating a full scan and removal of the viruses using the presented interface or call the phone number displayed in the interface of the antivirus removal tool12Shutting down the infected computer and swapping it with another computer is not necessary at this point12The technician should not immediately assume that the message is legitimate or perform any actions without knowing what the interface is and what triggered it to pop up. It is important to investigate the issue further, including checking the legitimacy of the antivirus program and the message it is displaying.

QUESTION 62
The command cac cor.pti a. txt was issued on a Linux terminal. Which of the following results should be expected?

A. The contents of the text comptia.txt will be replaced with a new blank document
B. The contents of the text comptia. txt would be displayed.
C. The contents of the text comptia.txt would be categorized in alphabetical order.
D. The contents of the text comptia. txt would be copied to another comptia. txt file

Correct Answer: B
Section:
Explanation:
The command cac cor.ptia. txt was issued on a Linux terminal. This command would display the contents of the text comptia.txt.

QUESTION 63
A user's smarlphone data usage is well above average. The user suspects an installed application is transmitting data in the background The user would like to be alerted when an application attempts to communicate with the internet.
Which of the following BEST addresses the user's concern?

A. Operating system updates
B. Remote wipe
C. Antivirus
D. Firewall

Correct Answer: D
Section:
Explanation:
A firewall is a security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. In this scenario, the user is concerned about an installed application transmitting data in the background, so a firewall would be the best solution to address their concern. By installing and configuring a firewall, the user can block unauthorized connections to and from the device, and receive alerts whenever an application tries to access the internet.

QUESTION 64
A technician is unable to join a Windows 10 laptop to a domain Which of the following is the MOST likely reason?

A. The domain's processor compatibility is not met
B. The laptop has Windows 10 Home installed
C. The laptop does not have an onboard Ethernet adapter
D. The Laptop does not have all current Windows updates installed

Correct Answer: B
Section:
Explanation:
https://partners.comptia.org/docs/default-source/resources/comptia-a-220-1102-exam-objectives- (3-0)

QUESTION 65
A technician is troubleshooting an issue involving programs on a Windows 10 machine that are loading on startup but causing excessive boot times. Which of the following should the technician do to selectively prevent

programs from loading?

A. Right-click the Windows button, then select Run entering shell startup and clicking OK, and then move items one by one to the Recycle Bin

B. Remark out entries listed HKEY_LOCAL_MACHINE>SOFTWARE>Microsoft>Windows>CurrentVersion>Run

C. Manually disable all startup tasks currently listed as enabled and reboot checking for issue resolution at startup

D. Open the Startup tab and methodically disable items currently listed as enabled and reboot, checking for issue resolution at each startup.

Correct Answer: D
Section:
Explanation:
This is the most effective way to selectively prevent programs from loading on a Windows 10 machine. The Startup tab can be accessed by opening Task Manager and then selecting the Startup tab. From there, the technician can methodically disable items that are currently listed as enabled, reboot the machine, and check for issue resolution at each startup. If the issue persists, the technician can then move on to disabling the next item on the list.

QUESTION 66
A desktop specialist needs to prepare a laptop running Windows 10 for a newly hired employee.
Which of the following methods should the technician use to refresh the laptop?

A. Internet-based upgrade

B. Repair installation

C. Clean install

D. USB repair

E. In place upgrade

Correct Answer: C
Section:
Explanation:
The desktop specialist should use a clean install to refresh the laptop. A clean install will remove all data and applications from the laptop and install a fresh copy of Windows 10, ensuring that the laptop is ready for the newly hired employee.

QUESTION 67
A technician found that an employee is mining cryptocurrency on a work desktop. The company has decided that this action violates its guidelines. Which of the following should be updated to reflect this new requirement?

A. MDM

B. EULA

C. IRP

D. AUP

Correct Answer: D
Section:
Explanation:
AUP (Acceptable Use Policy) should be updated to reflect this new requirement. The AUP is a document that outlines the acceptable use of technology within an organization. It is a set of rules that employees must follow when using company resources. The AUP should be updated to include a policy on cryptocurrency mining on work desktops

QUESTION 68
A user calls the help desk to report that none of the files on a PC will open. The user also indicates a program on the desktop is requesting payment in exchange for file access A technician verifies the user's PC is infected with ransorrrware.
Which of the following should the technician do FIRST?

A. Scan and remove the malware
B. Schedule automated malware scans
C. Quarantine the system
D. Disable System Restore

Correct Answer: C
Section:
Explanation:
The technician should quarantine the system first1Reference:CompTIA A+ Certification Exam: Core 2 Objectives Version 4.0. Retrieved from https://partners.comptia.org/docs/default-source/resources/comptia-a-220-1102-exam-objectives- (3-0)

QUESTION 69
A user has requested help setting up the fingerprint reader on a Windows 10 laptop. The laptop is equipped with a fingerprint reader and is joined to a domain Group Policy enables Windows Hello on all computers in the environment. Which of the following options describes how to set up Windows Hello Fingerprint for the user?

A. Navigate to the Control Panel utility, select the Security and Maintenance submenu, select Change Security and Maintenance settings, select Windows Hello Fingerprint, and have the user place a fingerprint on the fingerprint reader repeatedly until Windows indicates setup is complete
B. Navigate to the Windows 10 Settings menu, select the Accounts submenu, select Sign in options, select Windows Hello Fingerprint, and have the user place a fingerprint on the fingerprint reader repeatedly until Windows indicates setup is complete.
C. Navigate to the Windows 10 Settings menu, select the Update & Security submenu select Windows Security, select Windows Hello Fingerprint and have the user place a fingerprint on the fingerprint reader repeatedly until Windows indicates setup is complete
D. Navigate to the Control Panel utility, select the Administrative Tools submenu, select the user account in the list, select Windows Hello Fingerprint, and have the user place a fingerprint on the fingerprint reader repeatedly until Windows indicates setup is complete.

Correct Answer: B
Section:
Explanation:
Navigate to the Windows 10 Settings menu, select the Accounts submenu, select Sign in options, select Windows Hello Fingerprint, and have the user place a fingerprint on the fingerprint reader repeatedly until Windows indicates setup is complete. Windows Hello Fingerprint can be set up by navigating to the Windows 10 Settings menu, selecting the Accounts submenu, selecting Sign in options, and then selecting Windows Hello Fingerprint. The user will then be asked to place a fingerprint on the fingerprint reader repeatedly until Windows indicates that setup is complete.Windows Hello Fingerprint allows the user to log into the laptop using just their fingerprint, providing an additional layer of security.

QUESTION 70
A user reports a PC is running slowly. The technician suspects it has a badly fragmented hard drive.
Which of the following tools should the technician use?

A. resmon exe
B. msconfig.extf
C. dfrgui exe
D. msmfo32.exe

Correct Answer: C
Section:
Explanation:
The technician should use dfrgui.exe to defragment the hard drive1

QUESTION 71
A user reports a computer is running stow. Which of the following tools will help a technician identify the issue?

A. Disk Cleanup
B. Group Policy Editor
C. Disk Management
D. Resource Monitor

Correct Answer: D
Section:
Explanation:

QUESTION 72
A user is unable to log in to the domain with a desktop PC, but a laptop PC is working properly on the same network. A technician logs in lo the desktop PC with a local account but is unable to browse to the secure intranet site to get troubleshooting tools. Which of the following is the MOST likely cause of the issue?

A. Time drift
B. Dual in-line memory module failure
C. Application crash
D. Filesystem errors

Correct Answer: A
Section:
Explanation:
The most likely cause of the issue is a “time drift”. Time drift occurs when the clock on a computer is not synchronized with the clock on the domain controller. This can cause authentication problemswhen a user tries to log in to the domain. The fact that the technician is unable to browse to the secure intranet site to get troubleshooting tools suggests that there may be a problem with the network connection or the firewall settings on the desktop PC12

QUESTION 73
Which of the following could be used to implement secure physical access to a data center?

A. Geofence
B. Alarm system
C. Badge reader
D. Motion sensor

Correct Answer: C
Section:
Explanation:
Badge readers are used to implement secure physical access to a data center. They are used to readthe identification information on an employee’s badge and grant access to the data center if the employee is authorized2.This system requires individuals to have an access badge that contains their identification information or a unique code that can be scanned by a reader. After the badge is scanned, the system compares the information on the badge with the authorized personnel database to authenticate if the individual has the required clearance to enter that area. The other options listed, such as a geofence, alarm system, or motion sensor are security measures that may be used in conjunction with badge readers, but do not provide identification and authentication features.

QUESTION 74
A user wants to set up speech recognition on a PC In which of the following Windows Settings tools can the user enable this option?

A. Language
B. System

C. Personalization
D. Ease of Access

Correct Answer: D
Section:
Explanation:
The user can enable speech recognition on a PC in the Ease of Access settings tool. To set up Speech Recognition on a Windows PC, the user should open Control Panel, click on Ease of Access, click on Speech Recognition, and click the Start Speech Recognition link. Language settings can be used to change the language of the speech recognition feature, but they will not enable the feature. System settings can be used to configure the hardware and software of the PC, but they will not enable thespeech recognition feature. Personalization settings can be used to customize the appearance and behavior of the PC, but they will not enable the speech recognition feature1Open up ease of access, click on speech, then there is an on and off button for speech recognition.

QUESTION 75
A user is experiencing frequent malware symptoms on a Windows workstation. The user has tried several times to roll back the state but the malware persists. Which of the following would MOST likely resolve the issue?

A. Quarantining system files
B. Reimaging the workstation
C. Encrypting the hard drive
D. Disabling TLS 1.0 support

Correct Answer: C
Section:
Explanation:
Since Windows systems support FAT32 and NTFS "out of the box" and Linux supports a whole range of them including FAT32 and NTFS, it is highly recommended to format the partition or disk you want to share in either FAT32 or NTFS, but since FAT32 has a file size limit of 4.2 GB, if you happen to work with huge files, then it is better you use NTFS

QUESTION 76
A technician needs lo formal a USB drive to transfer 20GB of data from a Linux computer to a Windows computer. Which of the following filesystems will the technician MOST likely use?

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

Correct Answer: D
Section:
Explanation:

QUESTION 77
A technician is setting up a desktop computer in a small office. The user will need to access files on a drive shared from another desktop on the network. Which of the following configurations should the technician employ to achieve this goal?

A. Configure the network as private
B. Enable a proxy server
C. Grant the network administrator role to the user
D. Create a shortcut to public documents

Correct Answer: A

Section:
Explanation:
The technician should configure the network as private to allow the user to access files on a drive shared from another desktop on the network1

QUESTION 78
A technician needs to transfer a large number of files over an unreliable connection. The technician should be able to resume the process if the connection is interrupted. Which of the following tools can be used?

A. afc
B. ehkdsk
C. git clone
D. zobocopy

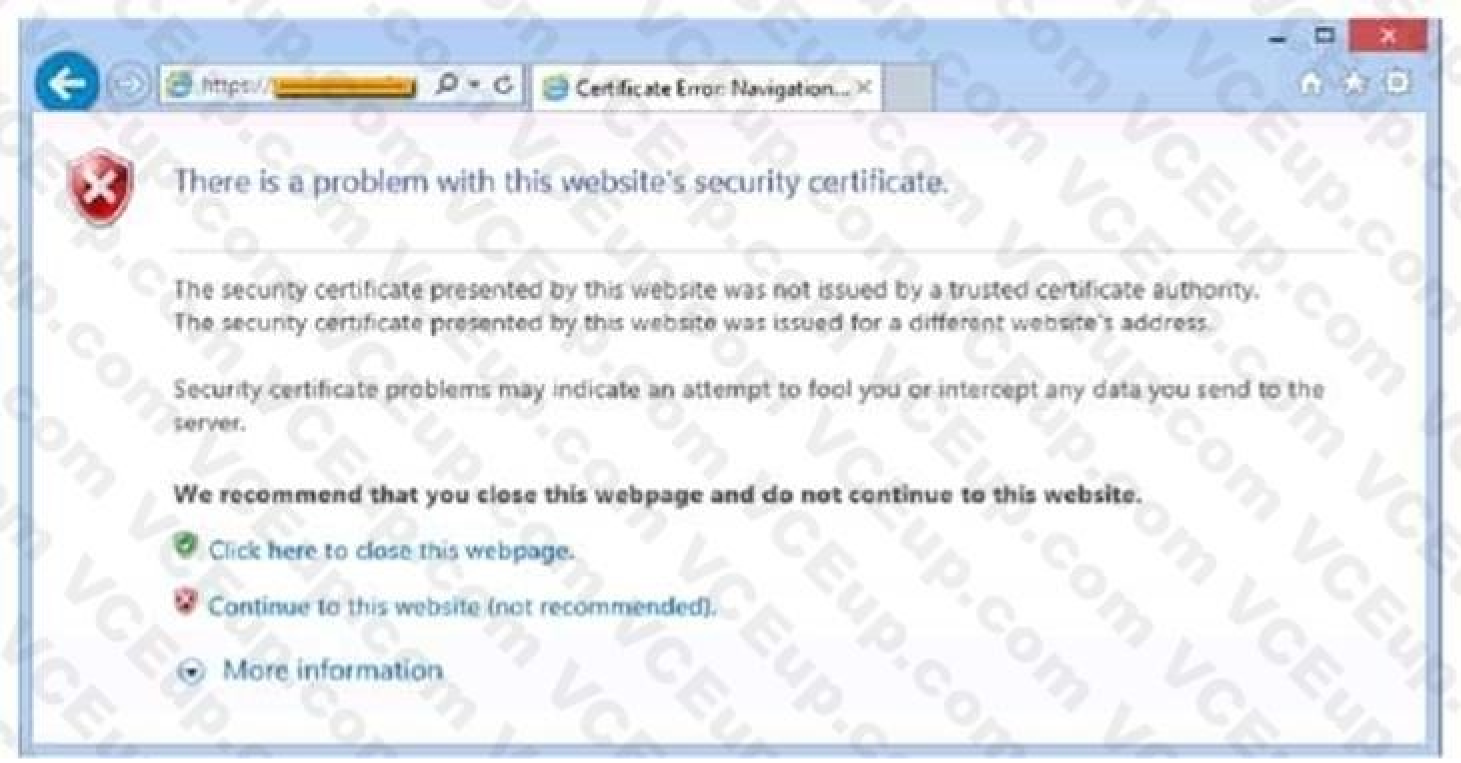
Correct Answer: A
Section:
Explanation:
The technician should use afc to transfer a large number of files over an unreliable connection and be able to resume the process if the connection is interrupted1

QUESTION 79
An incident handler needs to preserve evidence for possible litigation. Which of the following will the incident handler MOST likely do to preserve the evidence?

A. Encrypt the files
B. Clone any impacted hard drives
C. Contact the cyber insurance company
D. Inform law enforcement

Correct Answer: B
Section:
Explanation:
The incident handler should clone any impacted hard drives to preserve evidence for possible litigation1

QUESTION 80
After clicking on a link in an email a Chief Financial Officer (CFO) received the following error:



There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

More information

The CFO then reported the incident to a technician. The link is purportedly to the organization's bank. Which of the following should the technician perform FIRST?

A. Update the browser's CRLs
B. File a trouble ticket with the bank.
C. Contact the ISP to report the CFCs concern
D. Instruct the CFO to exit the browser

Correct Answer: A
Section:
Explanation:
The technician should update the browser’s CRLs first. The error message indicates that the certificate revocation list (CRL) is not up to date. Updating the CRLs will ensure that the browser can verify the authenticity of the bank’s website.

QUESTION 81
A technician has spent hours trying to resolve a computer issue for the company's Chief Executive Officer (CEO). The CEO needs the device returned as soon as possible. Which of the following steps should the technician take NEXT?

A. Continue researching the issue
B. Repeat the iterative processes
C. Inform the CEO the repair will take a couple of weeks
D. Escalate the ticket

Correct Answer: D
Section:
Explanation:
The technician should escalate the ticket to ensure that the CEO’s device is returned as soon as possible1

QUESTION 82
A technician needs to exclude an application folder from being cataloged by a Windows 10 search.
Which of the following utilities should be used?

A. Privacy
B. Indexing Options
C. System
D. Device Manager

Correct Answer: B
Section:
Explanation:
To exclude an application folder from being cataloged by a Windows 10 search, the technician should use the Indexing Options utility1

QUESTION 83
The network was breached over the weekend System logs indicate that a single user's account was successfully breached after 500 attempts with a dictionary attack. Which of the following would BEST mitigate this threat?

A. Encryption at rest
B. Account lockout
C. Automatic screen lock
D. Antivirus

Correct Answer: B
Section:
Explanation:
Account lockout would best mitigate the threat of a dictionary attack

QUESTION 84
As part of a CYOD policy a systems administrator needs to configure each user's Windows device to require a password when resuming from a period of sleep or inactivity. Which of the following paths will lead the administrator to the correct settings?

A. Use Settings to access Screensaver settings
B. Use Settings to access Screen Timeout settings
C. Use Settings to access General
D. Use Settings to access Display.

Correct Answer: A
Section:
Explanation:
The systems administrator should use Settings to access Screensaver settings to configure each user’s Windows device to require a password when resuming from a period of sleep or inactivity

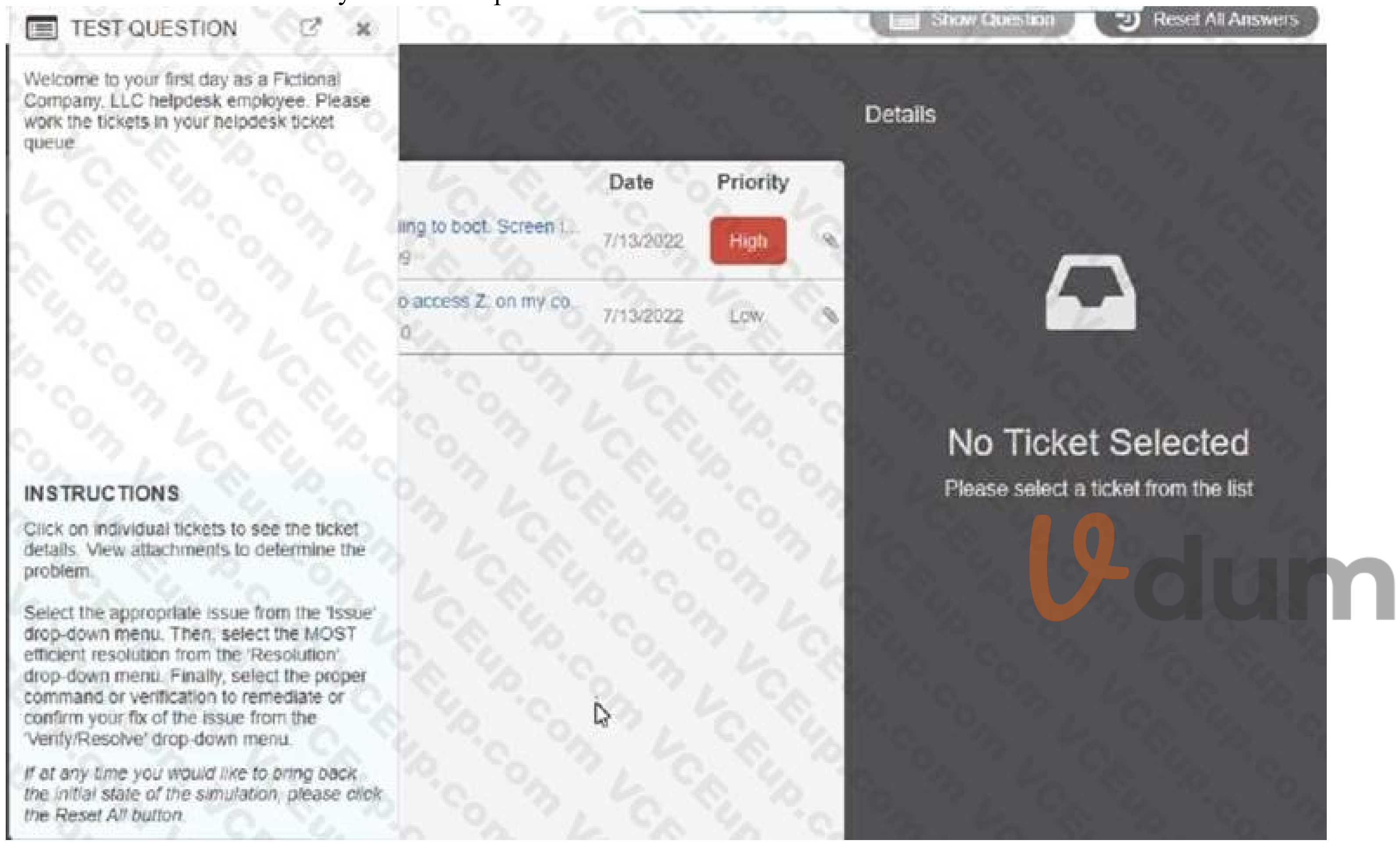
QUESTION 85
A user is configuring a new SOHO Wi-Fi router for the first time. Which of the following settings should the user change FIRST?

A. Encryption
B. Wi-Fi channel
C. Default passwords
D. Service set identifier

Correct Answer: C
Section:

Explanation:
the user should change the default passwords first when configuring a new SOHO Wi-Fi router1

QUESTION 86
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.



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

	Date	Priority
ling to boot. Screen i... 9	7/13/2022	High
o access Z: on my co... 0	7/13/2022	Low

No Ticket Selected

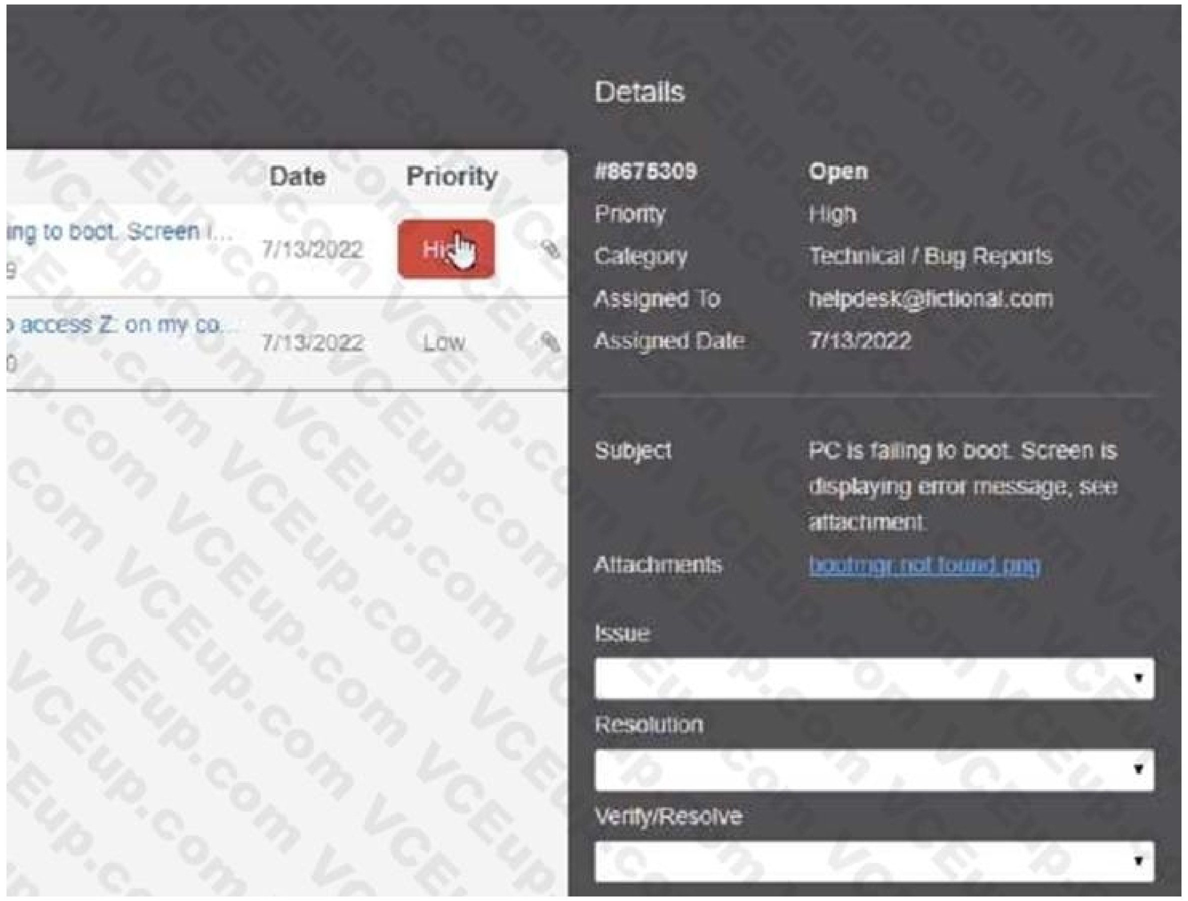
Please select a ticket from the list

INSTRUCTIONS

Click on individual tickets 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.

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



	Date	Priority
ing to boot. Screen i... 9	7/13/2022	High
access Z: on my co... 0	7/13/2022	Low

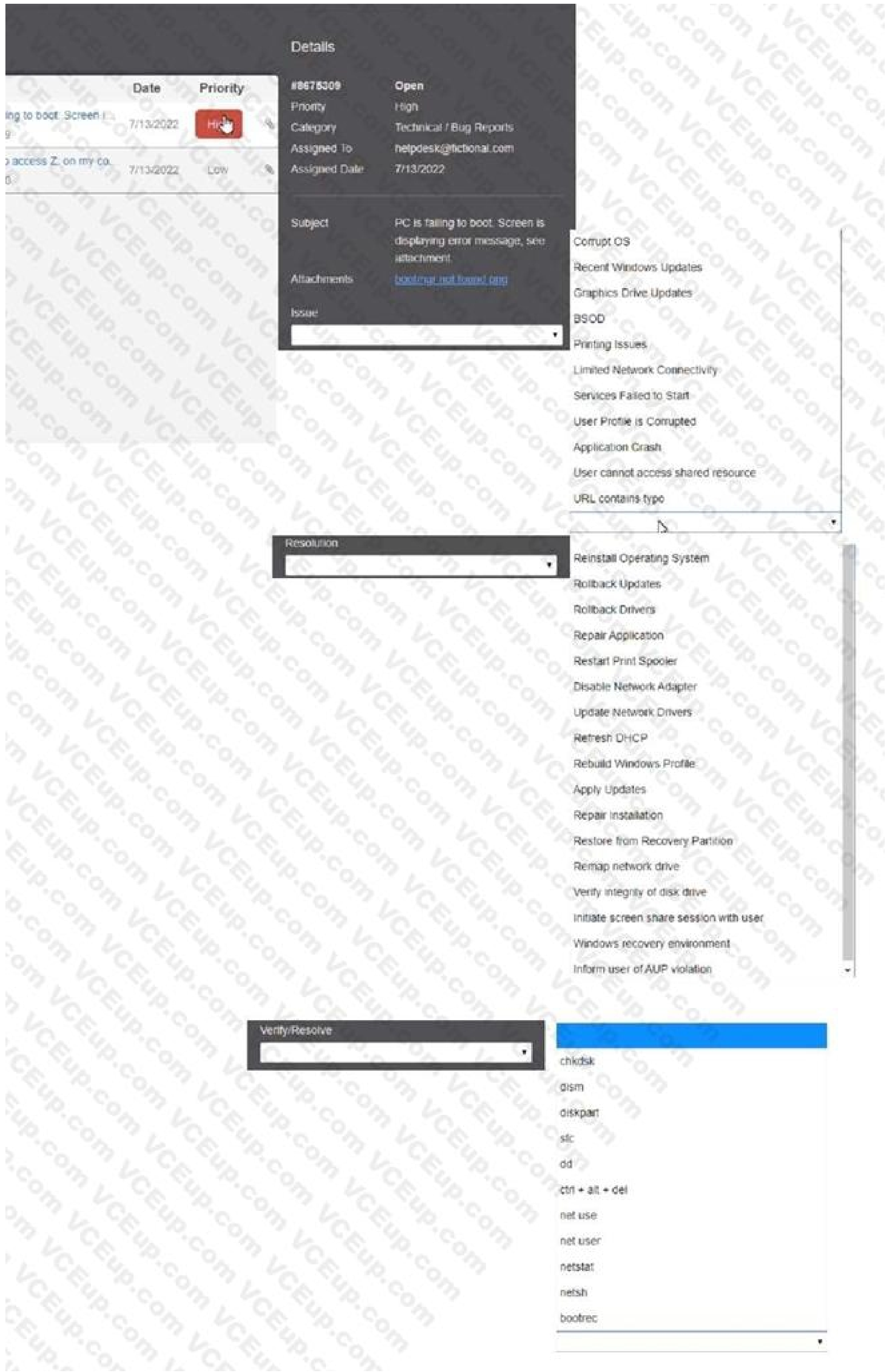
Details

#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



Details

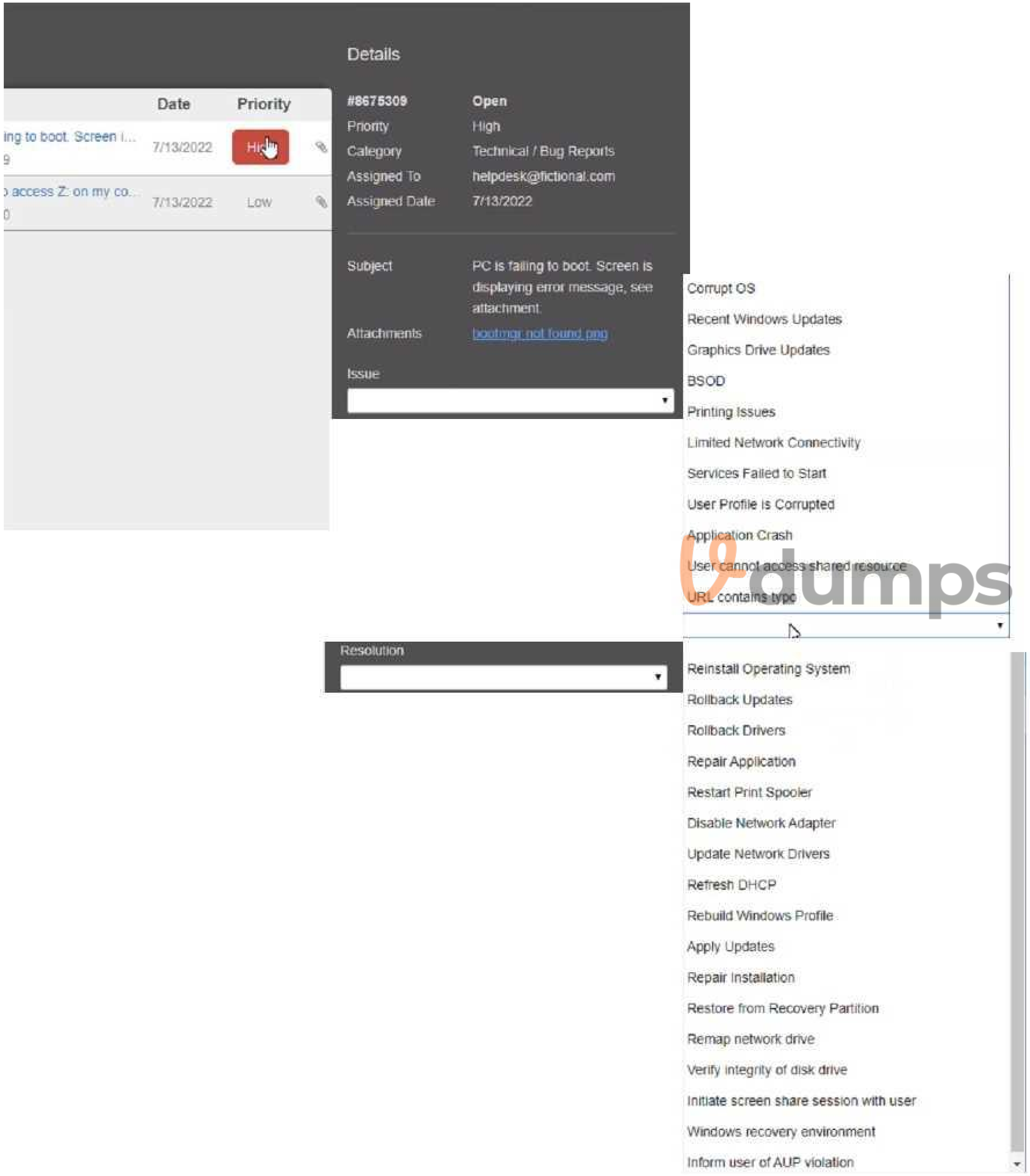
#8675309	Open
Priority	High
Category	Technical / Bug Reports
Assigned To	helpdesk@fictional.com
Assigned Date	7/13/2022
Subject	PC is failing to boot. Screen is displaying error message, see attachment
Attachments	bootmgr not found.png

Issue

Resolution

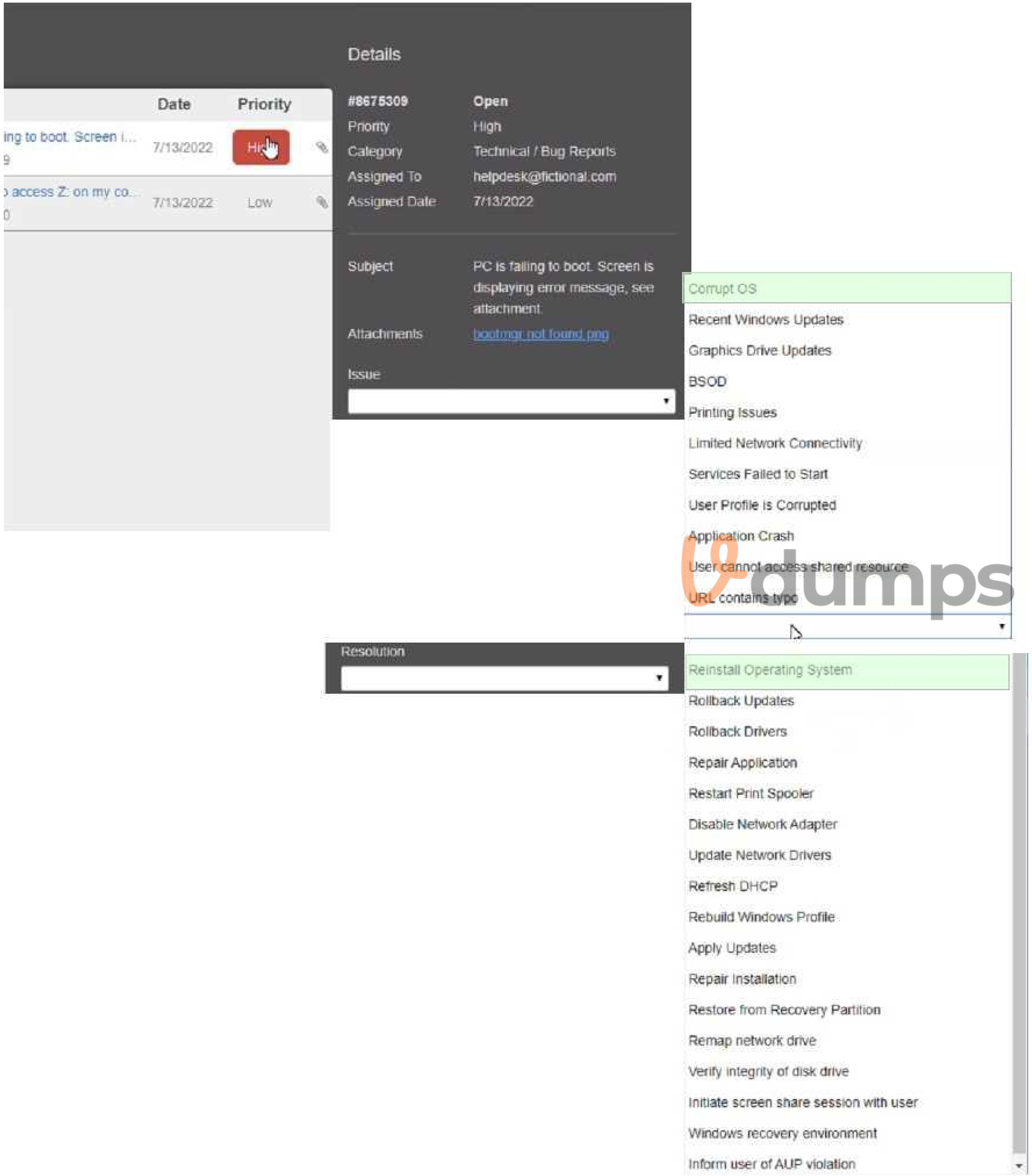
Verify/Resolve

Hot Area:



#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

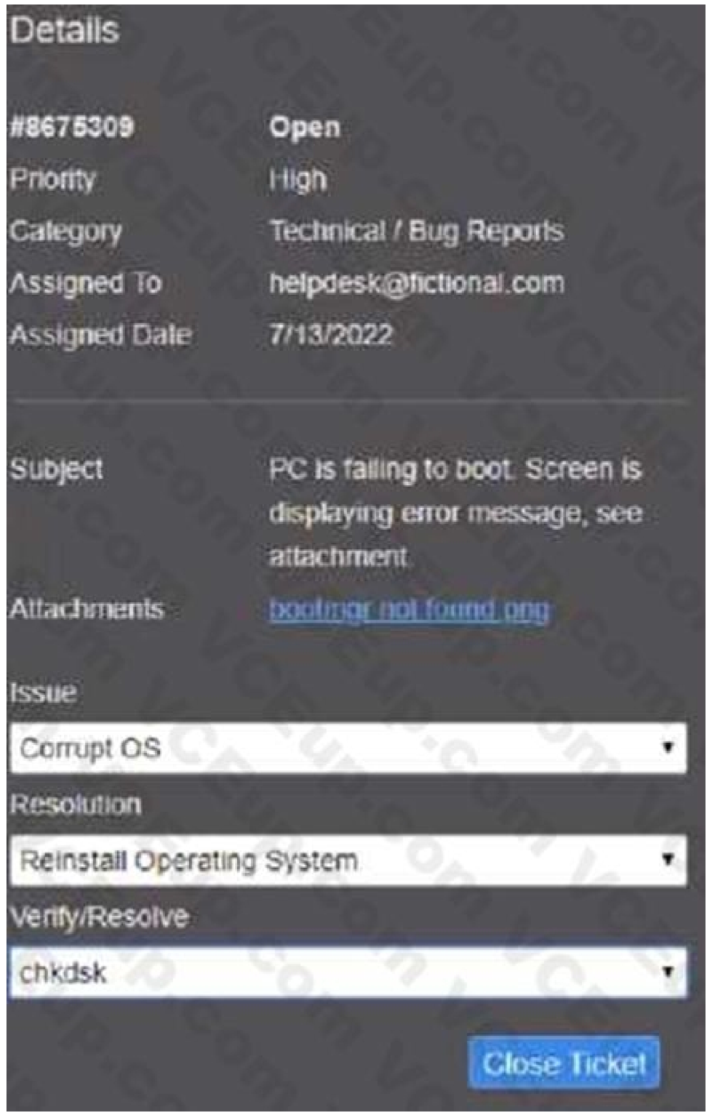
Answer Area:



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

Section:
Explanation:
Answer: A
Explanation:



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: Corrupt OS

Resolution: Reinstall Operating System

Verify/Resolve: chkdsk

QUESTION 87
A user reports a computer is running slow. Which of the following tools will help a technician identity the issued

A. Disk Cleanup
B. Group Policy Editor
C. Disk Management
D. Resource Monitor

Correct Answer: D
Section:
Explanation:
Resource Monitor will help a technician identify the issue when a user reports a computer is running slow1

QUESTION 88
An Android user contacts the help desk because a company smartphone failed to complete a tethered OS update A technician determines there are no error messages on the device Which of the following should the technician

do NEXT?

A. Verify all third-party applications are disabled
B. Determine if the device has adequate storage available.
C. Check if the battery is sufficiently charged
D. Confirm a strong internet connection is available using Wi-Fi or cellular data

Correct Answer: C
Section:
Explanation:
Since there are no error messages on the device, the technician should check if the battery is sufficiently charged1If the battery is low, the device may not have enough power to complete the update2In this scenario, the technician has already determined that there are no error messages on the device. The next best step would be to check if the battery is sufficiently charged. If the battery is low, it could be preventing the device from completing the update process.Verifying that third-party applications are disabled, determining if the device has adequate storage available, and confirming a strong internet connection are all important steps in troubleshooting issues with mobile devices.
However, since the problem in this scenario is related to a failed OS update, it is important to first check the battery level before proceeding with further troubleshooting steps.

QUESTION 89
A user reports that text on the screen is too small. The user would like to make the text larger and easier to see. Which of the following is the BEST way for the user to increase the size of text, applications, and other items using the Windows 10 Settings tool?

A. Open Settings select Devices, select Display, and change the display resolution to a lower resolution option
B. Open Settings, select System, select Display, and change the display resolution to a lower resolution option.
C. Open Settings Select System, select Display, and change the Scale and layout setting to a higher percentage.
D. Open Settings select Personalization, select Display and change the Scale and layout setting to a higher percentage

Correct Answer: C
Section:
Explanation:
Open Settings, select System, select Display, and change the Scale and layout setting to a higher percentage123 Reference: 4. How to Increase the Text Size on Your Computer. Retrieved from https://www.laptopmag.com/articles/
increase-text-size-computer 5. How to Change the Size of Text in Windows 10. Retrieved from https://www.howtogeek.com/370055/how-to-change-the-size-of- text-in-windows-10/ 6. Change the size of text in Windows. Retrieved from
https://support.microsoft.com/en-us/windows/change-the-size-of-text-in-windows-1d5830c3-eee3- 8eaa-836b-abcc37d99b9a

QUESTION 90
A technician is installing new network equipment in a SOHO and wants to ensure the equipment is secured against external threats on the Internet. Which of the following actions should the technician do FIRST?

A. Lock all devices in a closet.
B. Ensure all devices are from the same manufacturer.
C. Change the default administrative password.
D. Install the latest operating system and patches

Correct Answer: C
Section:
Explanation:
The technician should change the default administrative password FIRST to ensure the network equipment is secured against external threats on the Internet. Changing the default administrative password is a basic security measure that can help prevent unauthorized access to the network equipment. Locking all devices in a closet is a physical security measure that can help prevent theft or damage to the devices, but it does not address external threats on the Internet.
Ensuring all devices are from the same manufacturer is not a security measure and does not address externalthreats on the Internet. Installing the latest operating system and patches is important for maintaining the security of

the network equipment, but it is not the first action the technician should take1

QUESTION 91
Which of the following Linux commands would be used to install an application?

A. yum
B. grep
C. Is
D. sudo

Correct Answer: D
Section:
Explanation:
The Linux command used to install an application is sudo. The sudo command allows users to run programs with the security privileges of another user, such as the root user. This is necessary toinstall applications because it requires administrative privileges1

QUESTION 92
A technician suspects the boot disk of a user's computer contains bad sectors. Which of the following should the technician verify in the command prompt to address the issue without making any changes?

A. Run sfc / scannow on the drive as the administrator.
B. Run clearnmgr on the drive as the administrator
C. Run chkdsk on the drive as the administrator.
D. Run dfrgui on the drive as the administrator.

Correct Answer: C
Section:
Explanation:
The technician should verify bad sectors on the user's computer by running chkdsk on the drive as the administrator. Chkdsk (check disk) is a command-line utility that detects and repairs disk errors, including bad sectors. It runs a scan of the disk and displays any errors that are found

QUESTION 93
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.

Correct Answer: B
Section:
Explanation:
To change the desktop wallpaper on a Windows 10 computer using a Windows 10 Settings tool, the user should open Settings, select Personalization, click Browse, and then locate and open the imagethe user wants to use as the wallpaper1 https://www.lifewire.com/change-desktop-background-windows-11-5190733

QUESTION 94
A technician wants to enable BitLocker on a Windows 10 laptop and is unable to find the BitLocker Drive Encryption menu item in Control Panel. Which of the following explains why the technician unable to find this menu item?

A. The hardware does not meet BitLocker's minimum system requirements.

B. BitLocker was renamed for Windows 10.

C. BitLocker is not included on Windows 10 Home.

D. BitLocker was disabled in the registry of the laptop

Correct Answer: C
Section:
Explanation:
BitLocker is only available on Windows 10 Pro, Enterprise, and Education editions1. Therefore, the technician is unable to find the BitLocker Drive Encryption menu item in Control Panel because it is not included in the Windows 10 Home edition1.

QUESTION 95
A user receives a notification indicating the antivirus protection on a company laptop is out of date. A technician is able to ping the user's laptop. The technician checks the antivirus parent servers and sees the latest signatures have been installed. The technician then checks the user's laptop and finds the antivirus engine and definitions are current. Which of the following has MOST likely occurred?

A. Ransomware

B. Failed OS updates

C. Adware

D. Missing system files

Correct Answer: B
Section:
Explanation:
The most likely reason for the antivirus protection on a company laptop being out of date is failed OSupdates1. Antivirus software relies on the operating system to function properly. If the operatingsystem is not up-to-date, the antivirus software may not function properly and may not be able to receive the latest virus definitions and updates2. Therefore, it is important to keep the operating system up-to-date to ensure the antivirus software is functioning properly2

QUESTION 96
Which of the following is a proprietary Cisco AAA protocol?

A. TKIP

B. AES

C. RADIUS

D. TACACS+

Correct Answer: D
Section:
Explanation:
TACACS+ is a proprietary Cisco AAA protocol

QUESTION 97
A technician needs to interconnect two offices to the main branch while complying with good practices and security standards. Which of the following should the technician implement?

A. MSRA

B. VNC

C. VPN

D. SSH

Correct Answer: C
Section:
Explanation:
A technician needs to interconnect two offices to the main branch while complying with good practices and security standards. The technician should implement VPN

QUESTION 98
A Chief Executive Officer has learned that an exploit has been identified on the web server software, and a patch is not available yet. Which of the following attacks MOST likely occurred?

A. Brute force
B. Zero day
C. Denial of service
D. On-path

Correct Answer: B
Section:
Explanation:
A zero-day attack is an attack that exploits a previously unknown vulnerability in a computer application, meaning that the attack occurs on “day zero” of awareness of the vulnerabilityConfiguring AAA Services. Retrieved from https:// www.cisco.com/c/en/us/td/docs/routers/crs/software/crs_r4- 0/security/configuration/guide/sc40crsbook_chapter1.html

QUESTION 99
A technician needs to format a USB drive to transfer 20GB of data from a Linux computer to a Windows computer. Which of the following filesystems will the technician MOST likely use?

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

Correct Answer: D
Section:
Explanation:
exFAT is a file system that is supported by both Linux and Windows and can handle large files1.

QUESTION 100
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

Correct Answer: C
Section:
Explanation:
4. Chrome OS. Retrieved from https://en.wikipedia.org/wiki/Chrome_OS 5. What is Chrome OS?Retrieved from https://www.google.com/chromebook/chrome-os/A netbook with a web-based, proprietary operating system is most likely running Chrome OS.Chrome OS is a web-based operating system developed by Google that is designed to work with web applications and cloud storage. It is optimized for netbooks and other low-power devices and is designed to be fast, secure, and easy to use.

QUESTION 101

An Android user reports that when attempting to open the company's proprietary mobile application it immediately doses. The user states that the issue persists, even after rebooting the phone. The application contains critical information that cannot be lost. Which of the following steps should a systems administrator attempt FIRST?

A. Uninstall and reinstall the application
B. Reset the phone to factory settings
C. Install an alternative application with similar functionality
D. Clear the application cache.

Correct Answer: D
Section:
Explanation:
The systems administrator should clear the application cache12 If clearing the application cache does not work, the systems administrator should uninstall and reinstall the application12Resetting the phone to factory settings is not necessary at this point12 Installing an alternative application with similar functionality is not necessary at this point12

QUESTION 102
A technician needs to document who had possession of evidence at every step of the process. Which of the following does this process describe?

A. Rights management
B. Audit trail
C. Chain of custody
D. Data integrity

Correct Answer: C
Section:
Explanation:
The process of documenting who had possession of evidence at every step of the process is called chain of custody

QUESTION 103
A user calls the help desk to report potential malware on a computer. The anomalous activity began after the user clicked a link to a free gift card in a recent email The technician asks the user to describe any unusual activity, such as slow performance, excessive pop-ups, and browser redirections. Which of the following should the technician do NEXT?

A. Advise the user to run a complete system scan using the OS anti-malware application
B. Guide the user to reboot the machine into safe mode and verify whether the anomalous activities are still present
C. Have the user check for recently installed applications and outline those installed since the link in the email was clicked
D. Instruct the user to disconnect the Ethernet connection to the corporate network.

Correct Answer: D
Section:
Explanation:
First thing you want to do is quarantine/disconnect the affected system from the network so whatever malicious software doesn't spread

QUESTION 104
A company needs to securely dispose of data stored on optical discs. Which of the following is the MOST effective method to accomplish this task?

A. Degaussing
B. Low-level formatting
C. Recycling
D. Shredding

Correct Answer: D
Section:
Explanation:
Shredding is the most effective method to securely dispose of data stored on optical discs12 Reference: 4. How Can I Safely Destroy Sensitive Data CDs/DVDs? - How-To Geek. Retrieved from https://www.howtogeek.com/174307/how- can-i-safely-destroy-sensitive-data-cdsdvds/ 5. Disposal — UK Data Service. Retrieved from https://ukdataservice.ac.uk/learning-hub/research-data-management/store-your-data/disposal/

QUESTION 105
A network administrator is deploying a client certificate lo be used for Wi-Fi access for all devices m an organization The certificate will be used in conjunction with the user's existing username and password Which of the following BEST describes the security benefits realized after this deployment?

A. Multifactor authentication will be forced for Wi-Fi
B. All Wi-Fi traffic will be encrypted in transit
C. Eavesdropping attempts will be prevented
D. Rogue access points will not connect

Correct Answer: A
Section:
Explanation:
Multifactor authentication will be forced for Wi-Fi after deploying a client certificate to be used for Wi-Fi access for all devices in an organization
Reference:CompTIA Security+ (Plus) Practice Test Questions | CompTIA. Retrieved from https://www.comptia.org/training/resources/comptia-security-practice-tests

QUESTION 106
A bank would like to enhance building security in order to prevent vehicles from driving into the building while also maintaining easy access for customers. Which of the following BEST addresses this need?

A. Guards
B. Bollards
C. Motion sensors
D. Access control vestibule

Correct Answer: B
Section:
Explanation:
Bollards are the best solution to enhance building security in order to prevent vehicles from driving into the building while also maintaining easy access for customers4Reference: 2. Bollards. Retrieved from https://en.wikipedia.org/wiki/
Bollard

QUESTION 107
A technician is working to resolve a Wi-Fi network issue at a doctor's office that is located next to an apartment complex. The technician discovers that employees and patients are not the only people on the network. Which of the following should the technician do to BEST minimize this issue?

A. Disable unused ports.
B. Remove the guest network
C. Add a password to the guest network
D. Change the network channel.

Correct Answer: D
Section:

Explanation:
Changing the network channel is the best solution to minimize the issue of employees and patients not being the only people on the Wi-Fi network5Reference: 3. Sample CompTIA Security+ exam questions and answers. Retrieved from
https://www.techtarget.com/searchsecurity/quiz/Sample-CompTIA-Security-exam-questions-and- answers

QUESTION 108
A technician just completed a Windows 10 installation on a PC that has a total of 16GB of RAM. The technician notices the Windows OS has only 4GB of RAM available for use. Which of the following explains why the OS can only access 46B of RAM?

A. The UEFI settings need to be changed.
B. The RAM has compatibility issues with Windows 10.
C. Some of the RAM is defective.
D. The newly installed OS is x86.

Correct Answer: D
Section:
Explanation:
The newly installed OS is x86. The x86 version of Windows 10 can only use up to 4GB of RAM. Thex64 version of Windows 10 can use up to 2TB of RAM1.

QUESTION 109
Which of the following is a data security standard for protecting credit cards?

A. PHI
B. NIST
C. PCI
D. GDPR

Correct Answer: C
Section:
Explanation:

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that ALL companies that accept, process, store or transmit credit card information maintain a secure environment.

QUESTION 110
Which of the following should be used to control security settings on an Android phone in a domain environment?

A. MDM
B. MFA
C. ACL
D. SMS

Correct Answer: A
Section:
Explanation:
The best answer to control security settings on an Android phone in a domain environment is to use “Mobile Device Management (MDM)”. MDM is a type of software that is used to manage and secure mobile devices such as smartphones and tablets. MDM can be used to enforce security policies, configure settings, and remotely wipe data from devices. In a domain environment, MDM can beused to manage Android phones and enforce security policies such as password requirements, encryption, and remote wipe capabilities12

QUESTION 111
A user is being directed by the help desk to look up a Windows PC's network name so the help desk can use a remote administration tool to assist the user. Which of the following commands would allow the user to give the technician the correct information? (Select TWO).

A. ipconfig /all
B. hostname
C. netstat /?
D. nslookup localhost
E. arp —a
F. ping :: 1

Correct Answer: A, B
Section:
Explanation:
The user can use the following commands to give the technician the correct information: ipconfig /all and hostname 1. The ipconfig /all command displays the IP address, subnet mask, and default gateway for all adapters on the computer 1. The hostname command displays the name of the computer 1.

QUESTION 112
A user created a file on a shared drive and wants to prevent its data from being accidentally deleted by others. Which of the following applications should the technician use to assist the user with hiding the file?

A. Device Manager
B. Indexing Options
C. File Explorer
D. Administrative Tools

Correct Answer: C
Section:
Explanation:
The technician should use the File Explorer application to assist the user with hiding the file 1. Theuser can right-click the file and select Properties. In the Properties dialog box, select the Hiddencheck box, and then click OK 1.

QUESTION 113
A developer is creating a shell script to automate basic tasks in Linux. Which of the following file types are supported by default?

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

Correct Answer: D
Section:
Explanation:

https://www.educba.com/shell-scripting-in-linux/

QUESTION 114
Before leaving work, a user wants to see the traffic conditions for the commute home. Which of the following tools can the user employ to schedule the browser to automatically launch a traffic website at 4:45 p.m.?

A. taskschd.msc

B. perfmon.msc

C. lusrmgr.msc

D. Eventvwr.msc

Correct Answer: A
Section:
Explanation:
The user can use the Task Scheduler (taskschd.msc) to schedule the browser to automatically launch a traffic website at 4:45 p.m. The Task Scheduler is a tool in Windows that allows users to schedule tasks to run automatically at specified times or in response to certain events.

QUESTION 115
A technician is installing a new business application on a user's desktop computer. The machine is running Windows 10 Enterprise 32-bit operating system. Which of the following files should the technician execute in order to complete the installation?

A. Installer_x64.exe

B. Installer_Files.zip

C. Installer_32.msi

D. Installer_x86.exe

E. Installer_Win10Enterprise.dmg

Correct Answer: D
Section:
Explanation:
The 32-bit operating system can only run 32-bit applications, so the technician should execute the 32-bit installer. The "x86" in the file name refers to the 32-bit architecture. https://www.digitaltrends.com/computing/32-bit-vs-64-bit-operating- systems/

QUESTION 116
A user is having issues with document-processing software on a Windows workstation. Other users that log in to the same device do not have the same issue.
Which of the following should a technician do to remediate the issue?

A. Roll back the updates.

B. Increase the page file.

C. Update the drivers.

D. Rebuild the profile.

Correct Answer: D
Section:
Explanation:
The issue is specific to the user's profile, so the technician should rebuild the profile. Rebuilding theprofile will create a new profile and transfer the user's data to the new profile1

QUESTION 117
A call center handles inquiries into billing issues for multiple medical facilities. A security analyst notices that call center agents often walk away from their workstations, leaving patient data visible for anyone to see. Which of the following should a network administrator do to BEST prevent data theft within the call center?

A. Encrypt the workstation hard drives.

B. Lock the workstations after five minutes of inactivity.

C. Install privacy screens.

D. Log off the users when their workstations are not in use.

Correct Answer: B
Section:
Explanation:
The BEST solution for preventing data theft within the call center in this scenario would be to lock the workstations after a period of inactivity. This would prevent unauthorized individuals from accessing patient data if call center agents were
to step away from their workstations without logging out.

QUESTION 118
A technician is setting up a backup method on a workstation that only requires two sets of tapes to restore. Which of the following would BEST accomplish this task?

A. Differential backup
B. Off-site backup
C. Incremental backup
D. Full backup

Correct Answer: D
Section:
Explanation:
To accomplish this task, the technician should use a Full backup method1 A full backup only requires two sets of tapes to restore because it backs up all the data from theworkstation. With a differential backup, the backups need to be taken multiple times over a period of time, so more tapes would be needed to restore the data

QUESTION 119
A help desk team lead contacts a systems administrator because the technicians are unable to log in to a Linux server that is used to access tools. When the administrator tries to use remote desktop to log in to the server, the administrator sees the GUI is crashing. Which of the following methods can the administrator use to troubleshoot the server effectively?

A. SFTP
B. SSH
C. VNC
D. MSRA

Correct Answer: B
Section:
Explanation:

QUESTION 120
A user turns on a new laptop and attempts to log in to specialized software, but receives a message stating that the address is already in use. The user logs on to the old desktop and receives the same message. A technician checks the account and sees a comment that the user requires a specifically allocated address before connecting to the software. Which of the following should the technician do to MOST likely resolve the issue?

A. Bridge the LAN connection between the laptop and the desktop.
B. Set the laptop configuration to DHCP to prevent conflicts.
C. Remove the static IP configuration from the desktop.
D. Replace the network card in the laptop, as it may be defective.

Correct Answer: C
Section:
Explanation:

The new laptop was set up with the static IP it needs to connect to the software. The old desktop is still configured with that IP, hence the conflict.

QUESTION 121
A technician is upgrading the backup system for documents at a high-volume law firm. The current backup system can retain no more than three versions of full backups before failing. The law firm is not concerned about restore times but asks the technician to retain more versions when possible.
Which of the following backup methods should the technician MOST likely implement?

A. Full
B. Mirror
C. Incremental
D. Differential

Correct Answer: C
Section:

QUESTION 122
A company discovered that numerous computers from multiple geographic locations are sending a very high number of connection requests which is causing the company's web server to become unavailable to the general public. Which of the following attacks is occurring?

A. Zero day
B. SOL injection
C. Cross-site scripting
D. Distributed denial of service

Correct Answer: D
Section:
Explanation:
The company is experiencing a distributed denial of service (DDoS) attack. A DDoS attack is a type of cyber attack in which multiple compromised systems are used to target a single system, causing a denial of service for users of the targeted system.

QUESTION 123
A technician is setting up a backup method on a workstation that only requires two sets of tapes to restore. Which of the following would BEST accomplish this task?

A. Differential backup
B. Off-site backup
C. Incremental backup
D. Full backup

Correct Answer: D
Section:
Explanation:
A full backup involves creating a copy of all data on the workstation, including system files and usercreated data, and storing it on a set of tapes. This ensures that all data is backed up, and ensures that the data can be restored in the event of a system failure or data loss.

QUESTION 124
A technician is troubleshooting a lack of outgoing audio on a third-party Windows 10 VoIP application, The PC uses a USB microphone connected to a powered hub. The technician verifies the microphone works on the PC using Voice Recorder. Which of the following should the technician do to solve the issue?

A. Remove the microphone from the USB hub and plug it directly into a USB port on the PC.

B. Enable the microphone under Windows Privacy settings to allow desktop applications to access it.

C. Delete the microphone from Device Manager and scan for new hardware,

D. Replace the USB microphone with one that uses a traditional 3.5mm plug.

Correct Answer: B
Section:
Explanation:
In Windows 10, there are privacy settings that control access to certain devices, such as microphones, cameras, and other input devices. If the microphone is not enabled under these privacy settings, the VoIP application may not have access to it, causing a lack of outgoing audio.
The technician can go to the Windows 10 Settings menu, select the Privacy submenu, and under App permissions, select Microphone. The technician should then turn on the toggle switch for the VoIP application to allow it to access the microphone.
Removing the microphone from the USB hub and plugging it directly into a USB port on the PC may or may not solve the issue, as the issue could be related to the privacy settings. Deleting the microphone from Device Manager and scanning for new hardware may also not solve the issue, as the issue could be related to the privacy settings. Replacing the USB microphone with one that uses a traditional 3.5 mm plug is not recommended, as it would require purchasing a new microphone and may not solve the issue.

QUESTION 125
A technician is setting up a new laptop for an employee who travels, Which of the following is the BEST security practice for this scenario?

A. PIN-based login

B. Quarterly password changes

C. Hard drive encryption

D. A physical laptop lock

Correct Answer: C
Section:
Explanation:
Encrypting the laptop's hard drive will ensure that any sensitive data stored on the laptop is secure, even if the laptop is lost or stolen. Encryption ensures that the data cannot be accessed by anyone without the correct encryption key. This is an important security measure for any laptop used by an employee who travels, as it helps to protect the data stored on the laptop from unauthorized access.

QUESTION 126
A user in a corporate office reports the inability to connect to any network drives. No other users have reported this issue. Which of the following is the MOST likely reason the user is having this issue?

A. The user is not connected to the VPN.

B. The file server is offline.

C. A low battery is preventing the connection.

D. The log-in script failed.

Correct Answer: D
Section:

QUESTION 127
A user received the following error upon visiting a banking website:
The security presented by website was issued a different website' s address .
A technician should instruct the user to:

A. clear the browser cache and contact the bank.

B. close out of the site and contact the bank.

C. continue to the site and contact the bank.

D. update the browser and contact the bank.

Correct Answer: A
Section:
Explanation:
The technician should instruct the user to clear the browser cache and contact the bank (option A).
This error indicates that the website the user is visiting is not the correct website and is likely due to a cached version of the website being stored in the user's browser. Clearing the browser cache should remove any stored versions of the website and allow the user to access the correct website.
The user should also contact the bank to confirm that they are visiting the correct website and to report the error.

QUESTION 128
A user is attempting to browse the internet using Internet Explorer. When trying to load a familiar web page, the user is unexpectedly redirected to an unfamiliar website. Which of the following would MOST likely solve the issue? (Choose Correct Answer and provide from Comptia A+ Core2 Study guide or manual from Comptia.org)

A. Updating the operating system

B. Changing proxy settings

C. Reinstalling the browser

D. Enabling port forwarding

Correct Answer: C
Section:
Explanation:
Reinstalling the browser would most likely solve the issue. This would remove any malicious software or add-ons that may be causing the issue and restore the browser to its default settings.

QUESTION 129
Which of the following is a consequence of end-of-lite operating systems?

A. Operating systems void the hardware warranty.

B. Operating systems cease to function.

C. Operating systems no longer receive updates.

D. Operating systems are unable to migrate data to the new operating system.

Correct Answer: C
Section:
Explanation:
End-of-life operating systems are those which have reached the end of their life cycle and are no longer supported by the software developer. This means that the operating system will no longer receive updates, security patches, or other new features. This can leave users vulnerable to security threats, as the system will no longer be protected against the latest threats. Additionally, this can make it difficult to migrate data to a newer operating system, as the old system is no longer supported.

QUESTION 130
Which of the following data is MOST likely to be regulated?

A. Name in a Phone book

B. Name on a medical diagnosis

C. Name on a job application

D. Name on a employer's website

Correct Answer: B
Section:

QUESTION 131
An organization's Chief Financial Officer (CFO) is concerned about losing access to very sensitive, legacy unmaintained PII on a workstation if a ransomware outbreak occurs. The CFO has a regulatory requirement to retain this data for many years. Which of the following backup methods would BEST meet the requirements?

A. A daily, incremental backup that is saved to the corporate file server
B. An additional, secondary hard drive in a mirrored RAID configuration
C. A full backup of the data that is stored of site in cold storage
D. Weekly, differential backups that are stored in a cloud-hosting provider

Correct Answer: C
Section:
Explanation:
According to CompTIA A+ Core 2 objectives, a full backup stored off-site provides the greatest protection against data loss in the event of a ransomware attack or other data disaster. By storing the backup in a separate physical location, it is less likely to be affected by the same event that could cause data loss on the original system. Cold storage is a term used for data archiving, which typically refers to a long-term storage solution that is used for retaining data that is infrequently accessed, but still needs to be kept for regulatory or compliance reasons.

QUESTION 132
A technician connects an additional monitor to a PC using a USB port. The original HDMI monitor is mounted to the left of the new monitor. When moving the mouse to the right from the original monitor to the new monitor, the mouse stops at the end of the screen on the original monitor. Which of the following will allow the mouse to correctly move to the new monitor?

A. Rearranging the monitor's position in display settings
B. Swapping the cables for the monitors
C. Using the Ctrl+AIt+> to correct the display orientation
D. Updating the display drivers for the video card

Correct Answer: B
Section:
Explanation:
The correct answer is B. Swapping the cables for the monitors. When the second monitor is connected with the HDMI port, it is necessary to swap the cables for the monitors so that the mouse can move from the original monitor to the new monitor. This is because the HDMI port is designed to only support one monitor, and the mouse will not be able to move from one to the other without the cables being swapped.
According to CompTIA A+ Core 2 documents, "When connecting multiple displays to a system, the cables used to connect the displays must be swapped between the displays. For example, if a monitor is connected to a system using a VGA cable, the VGA cable must be moved to the next display to allow the mouse to move between the two displays."

QUESTION 133
A technician receives a call from a user who is on vacation. The user provides the necessary credentials and asks the technician to log in to the users account and read a critical email that the user has been expecting. The technician refuses because this is a violation of the:

A. acceptable use policy.
B. regulatory compliance requirements.
C. non-disclosure agreement
D. incident response procedures

Correct Answer: A
Section:
Explanation:
Logging into a user's account without their explicit permission is a violation of the acceptable use policy, which outlines the rules and regulations by which a user must abide while using a computer system. By logging into the

user's account without their permission, the technician would be violating this policy. Additionally, this action could be seen as a breach of confidentiality, as the technician would have access to information that should remain confidential.

QUESTION 134

A new service desk is having a difficult time managing the volume of requests. Which of the following is the BEST solution for the department?

A. Implementing a support portal
B. Creating a ticketing system
C. Commissioning an automated callback system
D. Submitting tickets through email

Correct Answer: A
Section:
Explanation:

A support portal is an online system that allows customers to access customer service tools, submit requests and view status updates, as well as access information such as how-to guides, FAQs, and other self-service resources. This would be the best solution for the service desk, as it would allow them to easily manage the volume of requests by allowing customers to submit their own requests and view the status of their requests. Additionally, the portal would provide customers with selfservice resources that can help them resolve their own issues, reducing the amount of tickets that need to be handled by the service desk.

QUESTION 135

An IT services company that supports a large government contract replaced the Ethernet cards on several hundred desktop machines to comply With regulatory requirements. Which of the following disposal methods for the non-compliant cards is the MOST environmentally friendly?

A. incineration
B. Resale
C. Physical destruction
D. Dumpster for recycling plastics

Correct Answer: D
Section:
Explanation:

When disposing of non-compliant Ethernet cards, the most environmentally friendly option is to use a dumpster for recycling plastics. This method is the most effective way to reduce the amount of waste that is sent to landfills, and it also helps to reduce the amount of energy used in the production of new materials. Additionally, recycling plastics helps to reduce the amount of toxic chemicals that can be released into the environment. According to CompTIA A+ Core 2 documents, "The most environmentally friendly disposal method for non-compliant Ethernet cards is to use a dumpster for recycling plastics. This method is the most effective way to reduce the amount of waste that is sent to landfills, and it also helps to reduce the amount of energy used in the production of new materials."

QUESTION 136

A technician has verified that a user's computer has a virus, and the antivirus software is out Of date.
Which of the following steps should the technician take NEXT?

A. Quarantine the computer.
B. use a previous restore point,
C. Educate the end user about viruses
D. Download the latest virus definitions

Correct Answer: D
Section:
Explanation:

This will ensure that the antivirus software is up-to-date, and can detect any new viruses that may have been released since the last virus definition update.
The CompTIA A+ Core 2 220-1002 exam covers this topic in the following domains:

1.3 Explain the importance of security awareness and 2.2 Given a scenario, use secure data management and disaster recovery principles.

QUESTION 137
A systems administrator needs to reset a users password because the user forgot it. The systems administrator creates the new password and wants to further protect the user's account Which of the following should the systems administrator do?

A. Require the user to change the password at the next log-in.
B. Disallow tie user from changing the password.
C. Disable the account
D. Choose a password that never expires.

Correct Answer: A
Section:
Explanation:
This will ensure that the user is the only one who knows their password, and that the new password is secure.
The CompTIA A+ Core 2 220-1002 exam covers this topic in the domain 1.4 Given a scenario, use appropriate data destruction and disposal methods.

QUESTION 138
A technician received a call stating that all files in a user's documents folder appear to be Changed, and each of the files now has a look file extension Which pf the following actions is the FIRST step the technician should take?

A. Runa live disk clone.
B. Run a full antivirus scan.
C. Use a batch file to rename the files-
D. Disconnect the machine from the network

Correct Answer: D
Section:
Explanation:
The CompTIA A+ Core 2 220-1002 exam covers this topic in the following domains: 1.2 Given a scenario, use appropriate resources to support users and 1.3 Explain the importance of security awareness.

QUESTION 139
An analyst needs GUI access to server software running on a macOS server. Which of the following options provides the BEST way for the analyst to access the macOS server from the Windows workstation?

A. RDP through RD Gateway
B. Apple Remote Desktop
C. SSH access with SSH keys
D. VNC with username and password

Correct Answer: B
Section:
Explanation:

Apple Remote Desktop is a remote access solution that allows a user to access and control another macOS computer from their Windows workstation. It provides a graphical user interface so that the analyst can easily access the server software running on the macOS server. Apple Remote Desktop also supports file transfers, so the analyst can easily transfer files between the two computers.
Additionally, Apple Remote Desktop supports encryption, so data is secure during transmission.

QUESTION 140
The findings from a security audit indicate the risk of data loss from lost or stolen laptops is high. The company wants to reduce this risk with minimal impact to users who want to use their laptops when not on the network.

Which of the following would BEST reduce this risk for Windows laptop users?

A. Requiring strong passwords
B. Disabling cached credentials
C. Requiring MFA to sign on
D. Enabling BitLocker on all hard drives

Correct Answer: D
Section:
Explanation:
BitLocker is a disk encryption tool that can be used to encrypt the hard drive of a Windows laptop.
This will protect the data stored on the drive in the event that the laptop is lost or stolen, and will help to reduce the risk of data loss. Additionally, BitLocker can be configured to require a PIN or other authentication in order to unlock the drive, providing an additional layer of security.

QUESTION 141
A technician has been asked to set up a new wireless router with the best possible security. Which of the following should the technician implement?

A. WPS
B. TKIP
C. WPA3
D. WEP

Correct Answer: C
Section:
Explanation:
WPA3 (Wi-Fi Protected Access version 3) is the latest version of Wi-Fi security and offers the highest level of protection available. It is designed to protect against brute force password attempts and protect against eavesdropping and man- in-the-middle attacks. WPA3 also supports the use of stronger encryption algorithms, such as the Advanced Encryption Standard (AES), which provides additional protection for wireless networks. WPA3 should be implemented in order to ensure the best possible security for the new wireless router.

QUESTION 142
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.

Correct Answer: D
Section:
Explanation:
The workstations and the authentication server have a system clock difference. If a Group Policy setting is applied that forces the workstations to use a specific SNTP server, but the system clock on the workstations and the authentication
server are out of sync, then this can cause authentication issues and users will be unable to log in. In this case, the most likely cause of the issue is a difference in system clocks and the technician should ensure that the clocks on the workstations and the authentication server are in sync.

QUESTION 143
A desktop support technician is tasked with migrating several PCs from Windows 7 Pro to Windows 10 Pro, The technician must ensure files and user preferences are retained, must perform the operation locally, and should migrate one station at a time. Which of the following methods would be MOST efficient?

A. Golden image
B. Remote network install
C. In-place upgrade
D. Clean install

Correct Answer: C
Section:
Explanation:
An in-place upgrade is the most efficient method for migrating from Windows 7 Pro to Windows 10 Pro, as it will retain all user files and preferences, can be done locally, and can be done one station at a time. An in-place upgrade involves installing the new version of Windows over the existing version, and can be done quickly and easily.

QUESTION 144
A suite of security applications was installed a few days ago on a user's home computer. The user reports that the computer has been running slowly since the installation. The user notices the hard drive activity light is constantly solid.
Which of the following should be checked FIRST?

A. Services in Control Panel to check for overutilization
B. Performance Monitor to check for resource utilization
C. System File Checker to check for modified Windows files
D. Event Viewer to identify errors

Correct Answer: C
Section:
Explanation:
System File Checker to check for modified Windows files. System File Checker (SFC) is a Windows utility that can be used to scan for and restore corrupt Windows system files. SFC can be used to detect and fix any modified or corrupted system files on a computer, and thus should be checked first when a user reports that their computer has been running slowly since the installation of security applicationsÂ [1][2]. By checking SFC, any modified or corrupted system files can be identified and fixed, potentially improving the overall performance of the computer.

QUESTION 145
A Windows user reported that a pop-up indicated a security issue. During inspection, an antivirus system identified malware from a recent download, but it was unable to remove the malware. Which of the following actions would be BEST to remove the malware while also preserving the user's files?

A. Run the virus scanner in an administrative mode.
B. Reinstall the operating system.
C. Reboot the system in safe mode and rescan.
D. Manually delete the infected files.

Correct Answer: C
Section:
Explanation:
Rebooting the system in safe mode will limit the number of programs and processes running, allowing the antivirus system to more effectively identify and remove the malware. Rescanning the system will allow the antivirus system to identify and remove the malware while preserving the user's files.

QUESTION 146
A macOS user reports seeing a spinning round cursor on a program that appears to be frozen. Which of the following methods does the technician use to force the program to close in macOS?

A. The technician presses the Ctrl+Alt+Del keys to open the Force Quit menu, selects the frozen application in the list, and clicks Force Quit.

B. The technician clicks on the frozen application and presses and holds the Esc key on the keyboard for 10 seconds Which causes the application to force quit.

C. The technician opens Finder, navigates to the Applications folder, locates the application that is frozen in the list, right-clicks on the application, and selects the Force Quit option.

D. The technician opens the Apple icon menu, selects Force Quit, selects the frozen application in the list, and clicks Force Quit.

Correct Answer: D
Section:
Explanation:
The technician opens the Apple icon menu, selects Force Quit, selects the frozen application in the list, and clicks Force Quit. This is the most common method of force quitting a program in macOS.
This can be done by clicking on the Apple icon in the top left of the screen, selecting Force Quit, selecting the frozen application in the list, and then clicking Force Quit. This will force the application to quit and the spinning round cursor will disappear.

QUESTION 147
A technician is tasked with configuring a computer for a visually impaired user. Which of the following utilities should the technician use?

A. Device Manager

B. System

C. Ease of Access Center

D. Programs and Features

Correct Answer: C
Section:
Explanation:
The Ease of Access Center is a built-in utility in Windows that provides tools and options for making a computer easier to use for individuals with disabilities, including the visually impaired. In the Ease of Access Center, the technician can turn on options like high contrast display, screen magnification, and screen reader software to help the user better interact with the computer.

QUESTION 148
While assisting a customer with an issue, a support representative realizes the appointment is taking longer than expected and will cause the next customer meeting to be delayed by five minutes. Which of the following should the support representative do NEXT?

A. Send a quick message regarding the delay to the next customer.

B. Cut the current customer's lime short and rush to the next customer.

C. Apologize to the next customer when arriving late.

D. Arrive late to the next meeting without acknowledging the lime.

Correct Answer: A
Section:
Explanation:
The support representative should send a quick message regarding the delay to the next customer.This will help the next customer understand the situation and adjust their schedule accordingly.

QUESTION 149
An administrator has received approval for a change request for an upcoming server deployment.
Which of the following steps should be completed NEXT?

A. Perform a risk analysis.

B. Implement the deployment.

C. Verify end user acceptance

D. Document the lessons learned.

Correct Answer: A
Section:
Explanation:
Before making any changes to the system, it is important to assess the risks associated with the change and determine whether it is worth implementing. Risk analysis involves identifying potential risks, assessing their likelihood and impact, and determining what steps can be taken to mitigate them. It is important to perform this step before making any changes, as this allows the administrator to make an informed decision about whether or not the change should be implemented. Once the risks have been assessed and the administrator has decided to go ahead with the change, the next step is to implement the deployment.

QUESTION 150
A technician is troubleshooting a customer's PC and receives a phone call. The technician does not take the call and sets the phone to silent. Which of the following BEST describes the technician's actions?

A. Avoid distractions
B. Deal appropriately with customer's confidential material .
C. Adhere to user privacy policy
D. Set and meet timelines

Correct Answer: A
Section:
Explanation:
The technician's action of setting the phone to silent while troubleshooting the customer's PC is an example of avoiding distractions. By setting the phone to silent, the technician is ensuring that they are able to focus on the task at hand without any distractions that could potentially disrupt their workflow. This is an important practice when handling customer's confidential material, as it ensures that the technician is able to focus on the task and not be distracted by any external sources.
Furthermore, it also adheres to user privacy policies, as the technician is not exposing any confidential information to any external sources.

QUESTION 151
A manager reports that staff members often forget the passwords to their mobile devices and applications. Which of the following should the systems administrator do to reduce the number of help desk tickets submitted?

A. Enable multifactor authentication.
B. Increase the failed log-in threshold.
C. Remove complex password requirements.
D. Implement a single sign-on with biometrics.

Correct Answer: D
Section:
Explanation:

QUESTION 152
A laptop user is visually impaired and requires a different cursor color. Which of the following OS utilities is used to change the color of the cursor?

A. Keyboard
B. Touch pad
C. Ease of Access Center
D. Display settings

Correct Answer: C
Section:
Explanation:
The OS utility used to change the color of the cursor in Windows is Ease of Access Center12 The user can change the cursor color by opening the Settings app, selecting Accessibility in the left sidebar, selecting Mouse pointer and touch under Vision, and choosing one of the cursor options.

The user can select Custom to pick a color and use the Size slider to make the cursor larger or smaller12 The Ease of Access Center in the Windows OS provides accessibility options for users with disabilities or impairments. One of these options allows the user to change the color and size of the cursor, making it more visible and easier to locate on the screen. The Keyboard and Touchpad settings do not offer the option to change cursor color, and Display Settings are used to adjust the resolution and other properties of the display. Therefore, C is the best answer. This information is covered in the Comptia A+ Core2 documents/guide under the Accessibility section.

QUESTION 153
A user is attempting to make a purchase at a store using a phone. The user places the phone on the payment pad, but the device does not recognize the phone. The user attempts to restart the phone but still has the same results. Which of the following should the user do to resolve the issue?

A. Turn off airplane mode while at the register.
B. Verify that NFC is enabled.
C. Connect to the store's Wi-Fi network.
D. Enable Bluetooth on the phone.

Correct Answer: B
Section:
Explanation:
The user should verify that NFC is enabled on their phone. NFC is a technology that allows two devices to communicate with each other when they are in close proximity2.
NFC (Near Field Communication) technology allows a phone to wirelessly communicate with a payment terminal or other compatible device. In order to use NFC to make a payment or transfer information, the feature must be enabled on the phone. Therefore, the user should verify that NFC is enabled on their phone before attempting to make a payment with it. The other options, such as turning off airplane mode, connecting to Wi-Fi, or enabling Bluetooth, do not pertain to the NFC feature and are unlikely to resolve the issue. This information is covered in the Comptia A+ Core2 documents/guide under the Mobile Devices section.

QUESTION 154
A junior administrator is responsible for deploying software to a large group of computers in an organization. The administrator finds a script on a popular coding website to automate this distribution but does not understand the scripting language. Which of the following BEST describes the risks in running this script?

A. The instructions from the software company are not being followed.
B. Security controls will treat automated deployments as malware.
C. The deployment script is performing unknown actions.
D. Copying scripts off the internet is considered plagiarism.

Correct Answer: C
Section:
Explanation:
The risks in running this script are that the deployment script is performing unknown actions. Running the script blindly could cause unintended actions, such as deploying malware or deleting important files, which could negatively impact the organization's network and data1.

QUESTION 155
An administrator has submitted a change request for an upcoming server deployment. Which of the following must be completed before the change can be approved?

A. Risk analysis
B. Sandbox testing
C. End user acceptance
D. Lessons learned

Correct Answer: A
Section:
Explanation:
A risk analysis must be completed before a change request for an upcoming server deployment can be approved Risk analysis is an important step in the change management process because it helps identify and mitigate potential risks before changes are implemented. Once the risks have been analyzed and the appropriate measures have been taken to minimize them, the change can be approved and implemented.

QUESTION 156
A user reports a workstation has been performing strangely after a suspicious email was opened on it earlier in the week. Which of the following should the technician perform FIRST?

A. Escalate the ticket to Tier 2.
B. Run a virus scan.
C. Utilize a Windows restore point.
D. Reimage the computer.

Correct Answer: B
Section:
Explanation:
https://partners.comptia.org/docs/default-source/resources/comptia-a-220-1102-exam-objectives(3-0) When a user reports that their workstation is behaving strangely after opening a suspicious email, the first step a technician should take is to run a virus scan on the computer. This is because opening a suspicious email is a common way for viruses and malware to infect a computer. Running a virus scan can help identify and remove any infections that may be causing the computer to behave strangely.

QUESTION 157
Each time a user tries to go to the selected web search provider, a different website opens. Which of the following should the technician check FIRST?

A. System time
B. IP address
C. DNS servers
D. Windows updates

Correct Answer: C
Section:
Explanation:
When a user experiences unexpected or erratic behavior while browsing the internet, it could be caused by the DNS servers. DNS translates human-readable domain names (like google.com) into IP addresses, which computers can use to communicate with web servers. If the DNS servers are not functioning correctly or have been compromised, it can result in the browser being redirected to unintended websites.

QUESTION 158
Which of the following is the STRONGEST wireless configuration?

A. WPS
B. WPA3
C. WEP
D. WMN

Correct Answer: B
Section:
Explanation:
The strongest wireless configuration is B. WPA3. WPA3 is the most up-to-date wireless encryption protocol and is the most secure choice. It replaces PSK with SAE, a more secure way to do the initial key exchange. At the same time, the session key size of WPA3 increases to 128-bit in WPA3-Personal mode and 192-bit in WPA3-Enterprise, which makes the password harder to crack than the previous Wi-Fi security standards
https://www.makeuseof.com/tag/wep-wpa-wpa2-wpa3-explained/

QUESTION 159
A technician has an external SSD. The technician needs to read and write to an external SSD on both Macs and Windows PCs. Which of the following filesystems is supported by both OS types?

A. NTFS

B. APFS

C. ext4

D. exFAT

Correct Answer: D
Section:
Explanation:
The filesystem that is supported by both Macs and Windows PCs is D. exFAT. exFAT is a file system that is designed to be used on flash drives like USB sticks and SD cards. It is supported by both Macs and Windows PCs, and it can handle large files and volumes
https://www.diskpart.com/articles/file-system-for-mac-and-windows-0310.html

QUESTION 160
A user's system is infected with malware. A technician updates the anti-malware software and runs a scan that removes the malware. After the user reboots the system, it once again becomes infected with malware. Which of the following will MOST likely help to permanently remove the malware?

A. Enabling System Restore

B. Educating the user

C. Booting into safe mode

D. Scheduling a scan

Correct Answer: B
Section:
Explanation:
Although updating the anti-malware software and running scans are important steps in removing malware, they may not be sufficient to permanently remove the malware if the user keeps engaging in behaviors that leave the system vulnerable, such as downloading unknown files or visiting malicious websites. Therefore, educating the user on safe computing practices is the best way to prevent future infections and permanently remove the malware.
Enabling System Restore, Booting into safe mode, and scheduling a scan are not the most efficient ways to permanently remove the malware. Enabling System Restore and Booting into safe mode may help in some cases, but they may not be sufficient to permanently remove the malware. Scheduling a scan is also important for detecting and removing malware, but it may not be sufficient to prevent future infections.
https://partners.comptia.org/docs/default-source/resources/comptia-a-220-1102-exam-objectives(3-0)

QUESTION 161
A user connected a laptop to a wireless network and was tricked into providing login credentials for a website. Which of the following threats was used to carry out the attack?

A. Zero day

B. Vishing

C. DDoS

D. Evil twin

Correct Answer: D
Section:
Explanation:

QUESTION 162
Which of the following change management documents includes how to uninstall a patch?

A. Purpose of change

B. Rollback plan

C. Scope of change

D. Risk analysis

Correct Answer: B
Section:
Explanation:
The change management document that includes how to uninstall a patch is called the "rollback plan". The rollback plan is a document that outlines the steps that should be taken to undo a change that has been made to a system. In the case of a patch, the rollback plan would include instructions on how to uninstall the patch if it causes problems or conflicts with other software12

QUESTION 163
A network administrator is deploying a client certificate to be used for Wi-Fi access for all devices in an organization. The certificate will be used in conjunction with the user's existing username and password. Which of the following BEST describes the security benefits realized after this deployment?

A. Multifactor authentication will be forced for Wi-Fi.

B. All Wi-Fi traffic will be encrypted in transit.

C. Eavesdropping attempts will be prevented.

D. Rogue access points will not connect.

Correct Answer: A
Section:
Explanation:

QUESTION 164
In which of the following scenarios would remote wipe capabilities MOST likely be used? (Select TWO).

A. A new IT policy requires users to set up a lock screen PIN.

B. A user is overseas and wants to use a compatible international SIM Card.

C. A user left the phone at home and wants to prevent children from gaining access to the phone.

D. A user traded in the company phone for a cell carrier upgrade by mistake.

E. A user cannot locate the phone after attending a play at a theater.

F. A user forgot the phone in a taxi, and the driver called the company to return the device.

Correct Answer: E, F
Section:
Explanation:
Remote wipe capabilities are used to erase all data on a mobile device remotely. This can be useful in situations where a device is lost or stolen, or when sensitive data needs to be removed from a device. Remote wipe capabilities are most likely to be used in the following scenarios:
1. A user cannot locate the phone after attending a play at a theater. F. A user forgot the phone in a taxi, and the driver called the company to return the device1 In scenario E, remote wipe capabilities would be used to prevent unauthorized access to the device and to protect sensitive data. In scenario F, remote wipe capabilities would be used to erase all data on the device before it is returned to the user.

QUESTION 165
Sensitive data was leaked from a user's smartphone. A technician discovered an unapproved application was installed, and the user has full access to the device's command shell. Which of the following is the NEXT step the technician should take to find the cause of the leaked data?

A. Restore the device to factory settings.

B. Uninstall the unapproved application.

C. Disable the ability to install applications from unknown sources.

D. Ensure the device is connected to the corporate WiFi network.

Correct Answer: B
Section:
Explanation:
The technician should disable the user's access to the device's command shell. This will prevent the user from accessing sensitive data and will help to prevent further data leaks. The technician should then investigate the unapproved application to determine if it is the cause of the data leak. If the application is found to be the cause of the leak, the technician should uninstall the application and restore the device to factory settings. If the application is not the cause of the leak, the technician should investigate further to determine the cause of the leak. Disabling the ability to install applications from unknown sources can help to prevent future data leaks, but it is not the next step the technician should take in this scenario. Ensuring the device is connected to the corporate WiFi network is not relevant to this scenario1

QUESTION 166
A technician is attempting to mitigate micro power outages, which occur frequently within the area of operation. The outages are usually short, with the longest occurrence lasting five minutes. Which of the following should the technician use to mitigate this issue?

A. Surge suppressor
B. Battery backup
C. CMOS battery
D. Generator backup

Correct Answer: B
Section:
Explanation:
A battery backup, also known as an uninterruptible power supply (UPS), is a device that provides backup power during a power outage. When the power goes out, the battery backup provides a short amount of time (usually a few minutes up to an hour, depending on the capacity of the device) to save any work and safely shut down the equipment.

QUESTION 167
A user has a license for an application that is in use on a personal home laptop. The user approaches a systems administrator about using the same license on multiple computers on the corporate network. Which of the following BEST describes what the systems administrator should tell the user?

A. Use the application only on the home laptop because it contains the initial license.
B. Use the application at home and contact the vendor regarding a corporate license.
C. Use the application on any computer since the user has a license.
D. Use the application only on corporate computers.

Correct Answer: B
Section:
Explanation:
Use the application at home and contact the vendor regarding a corporate license. The user should use the application only on the home laptop because it contains the initial license. The user should contact the vendor regarding a corporate license if they want to use the application on multiple computers on the corporate network1

QUESTION 168
A macOS user needs to create another virtual desktop space. Which of the following applications will allow the user to accomplish this task?

A. Dock
B. Spotlight
C. Mission Control
D. Launchpad

Correct Answer: C
Section:
Explanation:
application that will allow a macOS user to create another virtual desktop space is Mission Control Mission Control lets you create additional desktops, called spaces, to organize the windows of your apps. You can create a space by entering Mission Control and clicking the Add button in the Spaces bar1. You can also assign apps to specific spaces and move between them easily1.

QUESTION 169
A technician is troubleshooting a computer with a suspected short in the power supply. Which of the following is the FIRST step the technician should take?

A. Put on an ESD strap
B. Disconnect the power before servicing the PC.
C. Place the PC on a grounded workbench.
D. Place components on an ESD mat.

Correct Answer: B
Section:
Explanation:
The first step a technician should take when troubleshooting a computer with a suspected short in the power supply is B. Disconnect the power before servicing the PC. This is to prevent any electrical shock or damage to the components. A power supply can be dangerous even when unplugged, as capacitors can maintain a line voltage charge for a long time1. Therefore, it is important to disconnect the power cord and press the power button to discharge any residual power before opening the case2. The other steps are also important for safety and proper diagnosis, but they should be done after disconnecting the power.

QUESTION 170
A team of support agents will be using their workstations to store credit card dat a. 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

Correct Answer: A, F
Section:
Explanation:
Encryption is a way of protecting cardholder data by transforming it into an unreadable format that can only be decrypted with a secret key1. Backups are a way of ensuring that cardholder data is not lost or corrupted in case of a disaster or system failure2. Both encryption and backups are part of the PCI DSS requirements that apply to any entity that stores, processes, or transmits cardholder data1. The other options are not directly related to credit card data security or compliance.

QUESTION 171
A user is unable to log in to the network. The network uses 802.1X with EAP-TLS to authenticate on the wired network. The user has been on an extended leave and has not logged in to the computer in several months. Which of the following is causing the login issue?

A. Expired certificate
B. OS update failure
C. Service not started
D. Application crash

E. Profile rebuild needed

Correct Answer: A
Section:
Explanation:
EAP-TLS is a method of authentication that uses certificates to establish a secure tunnel between the client and the server3. The certificates have a validity period and must be renewed before they expire1. If the user has been on an extended leave and has not logged in to the computer in several months, it is possible that the certificate on the client or the server has expired and needs to be renewed2. The other options are not directly related to EAP-TLS authentication or 802.1X network access.

QUESTION 172
A company is deploying mobile phones on a one-to-one basis, but the IT manager is concerned that users will root/jailbreak their phones. Which of the following technologies can be implemented to prevent this issue?

A. Signed system images
B. Antivirus
C. SSO
D. MDM

Correct Answer: D
Section:
Explanation:
MDM stands for Mobile Device Management, and it is a way of remotely managing and securing mobile devices that are used for work purposes1. MDM can enforce policies and restrictions on the devices, such as preventing users from installing unauthorized apps, modifying system settings, or accessing root privileges2. MDM can also monitor device status, wipe data, lock devices, or locate lost or stolen devices1.

QUESTION 173
A technician is troubleshooting an issue that requires a user profile to be rebuilt. The technician is unable to locate Local Users and Groups in the Mtv1C console. Which of the following is the NEXT step the technician should take to resolve the issue?

A. Run the antivirus scan.
B. Add the required snap-in.
C. Restore the system backup
D. use the administrator console.

Correct Answer: B
Section:
Explanation:
Local Users and Groups is a Microsoft Management Console (MMC) snap-in that allows you to manage user accounts or groups on your computer1. If you cannot find it in the MMC console, you can add it manually by following these steps2:
Press Windows key + R to open the Run dialog box, or open the Command Prompt. Type mmc and hit Enter. This will open a blank MMC console.
Click File and then Add/Remove Snap-in.
In the Add or Remove Snap-ins window, select Local Users and Groups from the Available snap-ins list, and click Add.
In the Select Computer window, choose Local computer or Another computer, depending on which computer you want to manage, and click Finish.
Click OK to close the Add or Remove Snap-ins window. You should now see Local Users and Groups in the MMC console.

QUESTION 174
Which of the following only has a web browser interface?

A. Linux
B. Microsoft Windows

C. iOS
D. Chromium

Correct Answer: D
Section:
Explanation:
Chromium is an operating system that only has a web browser interface. Chromium is an open- source project that provides the source code and framework for Chrome OS, which is a Linux-based operating system developed by Google. Chromium and Chrome OS are designed to run web applications and cloud services through the Chrome web browser, which is the only user interface available on the system. Chromium and Chrome OS are mainly used on devices such as Chromebooks, Chromeboxes and Chromebits. Linux is an operating system that does not only have a web browser interface but also a graphical user interface and a command-line interface. Linux is an open-source and customizable operating system that can run various applications and services on different devices and platforms. Linux can also support different web browsers, such as Firefox, Opera and Chromium. Microsoft Windows is an operating system that does not only have a web browser interface but also a graphical user interface and a command-line interface. Microsoft Windows is a proprietary and popular operating system that can run various applications and services on different devices and platforms. Microsoft Windows can also support different web browsers, such as Edge, Internet Explorer and Chrome. iOS is an operating system that does not only have a web browser interface but also a graphical user interface and a voice-based interface. iOS is a proprietary and mobile operating system developed by Apple that can run various applications and services on devices such as iPhone, iPad and iPod Touch. iOS can also support different web browsers, such as Safari, Firefox and Chrome. Reference: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.1

QUESTION 175
A kiosk, which is running Microsoft Windows 10, relies exclusively on a numeric keypad to allow customers to enter their ticket numbers but no other information. If the kiosk is idle for four hours, the login screen locks. Which of the following sign-on options would allow any employee the ability to unlock the kiosk?

A. Requiring employees to enter their usernames and passwords
B. Setting up facial recognition for each employee
C. Using a PIN and providing it to employees
D. Requiring employees to use their fingerprints

Correct Answer: C
Section:
Explanation:
The best sign-on option that would allow any employee the ability to unlock the kiosk that relies exclusively on a numeric keypad is to use a PIN and provide it to employees. A PIN is a Personal Identification Number that is a numeric code that can be used as part of authentication or access control. A PIN can be entered using only a numeric keypad and can be easily shared with employees who need to unlock the kiosk. Requiring employees to enter their usernames and passwords may not be feasible or convenient if the kiosk only has a numeric keypad and no other input devices. Setting up facial recognition for each employee may not be possible or secure if the kiosk does not have a camera or biometric sensor. Requiring employees to use their fingerprints may not be possible or secure if the kiosk does not have a fingerprint scanner or biometric sensor. Reference: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 3.3

QUESTION 176
A user calls the help desk to report that Windows installed updates on a laptop and rebooted overnight. When the laptop started up again, the touchpad was no longer working. The technician thinks the software that controls the touchpad might be the issue. Which of the following tools should the technician use to make adjustments?

A. eventvwr.msc
B. perfmon.msc
C. gpedic.msc
D. devmgmt.msc

Correct Answer: D
Section:
Explanation:
The technician should use devmgmt.msc tool to make adjustments for the touchpad issue after Windows installed updates on a laptop. Devmgmt.msc is a command that opens the Device Manager, which is a utility that allows users to view and manage the hardware devices and drivers installed on a computer. The technician can use the Device Manager to check the status, properties and compatibility of the touchpad device and its driver, and perform actions such as updating, uninstalling or reinstalling the driver, enabling or disabling the device, or scanning for hardware changes. Eventvwr.msc is a command that opens the Event Viewer, which is a utility that

allows users to view and monitor the system logs and events. The Event Viewer may provide some information or clues about the touchpad issue, but it does not allow users to manage or troubleshoot the device or its driver directly. Perfmon.msc is a command that opens the Performance Monitor, which is a utility that allows users to measure and analyze the performance of the system

QUESTION 177
A technician installed Windows 10 on a workstation. The workstation only has 3.5GB of usable RAM, even though the technician installed 8GB. Which of the following is the MOST likely reason this system is not utilizing all the available RAM?

A. The system is missing updates.
B. The system is utilizing a 32-bit OS.
C. The system's memory is failing.
D. The system requires BIOS updates

Correct Answer: B
Section:
Explanation:
The most likely reason that the system is not utilizing all the available RAM is that the system is utilizing a 32-bit OS. A 32-bit OS is an operating system that uses 32 bits to address memory locations and perform calculations. A 32-bit OS can only support up to 4GB of RAM, and some of that RAM may be reserved for hardware devices or system functions, leaving less than 4GB of usable RAM for applications and processes. A 32-bit OS cannot recognize or utilize more than 4GB of RAM, even if more RAM is installed on the system. To utilize all the available RAM, the system needs to use a 64- bit OS, which can support much more RAM than a 32-bit OS. The system missing updates may cause some performance or compatibility issues, but it does not affect the amount of usable RAM on the system. The system's memory failing may cause some errors or crashes, but it does not affect the amount of usable RAM on the system. The system requiring BIOS updates may cause some configuration or compatibility issues, but it does not affect the amount of usable RAM on the system.
Reference: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.1

QUESTION 178
A Windows workstation that was recently updated with approved system patches shut down instead of restarting. Upon reboot, the technician notices an alert stating the workstation has malware in the root OS folder. The technician promptly performs a System Restore and reboots the workstation, but the malware is still detected. Which of the following BEST describes why the system still has malware?

A. A system patch disabled the antivirus protection and host firewall.
B. The system updates did not include the latest anti-malware definitions.
C. The system restore process was compromised by the malware.
D. The malware was installed before the system restore point was created.

Correct Answer: D
Section:
Explanation:
The best explanation for why the system still has malware after performing a System Restore is that the malware was installed before the system restore point was created. A system restore point is a snapshot of the system settings and configuration at a certain point in time. A System Restore is a feature that allows users to restore their system to a previous state in case of problems or errors. However, a System Restore does not affect personal files or folders, and it may not remove malware that was already present on the system before the restore point was created. A system patch disabling the antivirus protection and host firewall may increase the risk of malware infection, but it does not explain why the malware persists after a System Restore. The system updates not including the latest anti-malware definitions may reduce the effectiveness of malware detection and removal, but it does not explain why the malware persists after a System Restore. The system restore process being compromised by the malware may prevent a successful System Restore, but it does not explain why the malware persists after a System Restore. Reference: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.3

QUESTION 179
Which of the following is the default GUI and file manager in macOS?

A. Disk Utility
B. Finder
C. Dock
D. FileVault

Correct Answer: B
Section:
Explanation:
Finder is the default GUI and file manager in macOS. Finder is an application that allows users to access and manage files and folders on their Mac computers. Finder also provides features such as Quick Look, Spotlight, AirDrop and iCloud Drive. Finder uses a graphical user interface that consists of icons, menus, toolbars and windows to display and interact with files and folders. Disk Utility is a utility that allows users to view and manage disk drives and partitions on their Mac computers. Disk Utility is not a GUI or a file manager but a disk management tool. Dock is a feature that allows users to access and launch applications on their Mac computers. Dock is not a GUI or a file manager but an application launcher. FileVault is a feature that allows users to encrypt and protect their data on their Mac computers. FileVault is not a GUI or a file manager but an encryption tool.
Reference: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.1

QUESTION 180
A technician needs to add an individual as a local administrator on a Windows home PC. Which of the following utilities would the technician MOST likely use?

A. Settings &gt; Personalization
B. Control Panel &gt; Credential Manager
C. Settings &gt; Accounts &gt; Family and Other Users
D. Control Panel &gt; Network and Sharing Center

Correct Answer: C
Section:
Explanation:
The technician would most likely use Settings &gt; Accounts &gt; Family and Other Users to add an individual as a local administrator on a Windows home PC. Settings &gt; Accounts &gt; Family and Other Users allows users to add and manage other user accounts on their Windows PC. The technician can add an individual as a local administrator by selecting Add someone else to this PC under Other users and following the steps to create a new user account with administrator privileges. Settings &gt; Personalization allows users to customize the appearance and behavior of their desktop, such as themes, colors, backgrounds, lock screen and screensaver. Settings &gt; Personalization is not related to adding an individual as a local administrator on a Windows home PC but to configuring desktop settings and preferences. Control Panel &gt; Credential Manager allows users to view and manage their web credentials and Windows credentials stored on their Windows PC. Control Panel &gt; Credential Manager is not related to adding

QUESTION 181
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

Correct Answer: A
Section:
Explanation:
The feature that allows a technician to configure policies in a Windows 10 Professional desktop is gpedit. Gpedit is a command that opens the Local Group Policy Editor, which is a utility that allows users to view and modify local group policies on their Windows PC. Local group policies are a set of rules and settings that control the behavior and configuration of the system and its users. Local group policies can be used to configure policies such as security, network, software installation and user rights. Gpmc is a command that opens the Group Policy Management Console, which is a utility that allows users to view and modify domain-based group policies on a Windows Server. Domain-based group policies are a set of rules and settings that control the behavior and configuration of the computers and users in a domain. Domain-based group policies are not available on a Windows 10 Professional desktop. Gpresult is a command that displays the result of applying group policies on a Windows PC. Gpresult can be used to troubleshoot or verify group policy settings but not to configure them. Gpupdate is a command that updates or refreshes the group policy settings on a Windows PC. Gpupdate can be used to apply new or changed group policy settings but not to configure them. Reference: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.6

QUESTION 182
Which of the following defines the extent of a change?

A. Scope
B. Purpose
C. Analysis
D. Impact

Correct Answer: A
Section:
Explanation:
The term that defines the extent of a change is scope. Scope is a measure of the size, scale and boundaries of a project or an activity. Scope defines what is included and excluded in the project or activity, such as goals, requirements, deliverables, tasks and resources. Scope helps determine the feasibility, duration and cost of the project or activity. Scope also helps manage the expectations and needs of the stakeholders involved in the project or activity. Purpose is the reason or objective for doing a project or an activity. Purpose defines why the project or activity is important or necessary, such as solving a problem, meeting a need or achieving a goal. Purpose helps provide direction, motivation and justification for the project or activity. Analysis is the process of examining, evaluating and interpreting data or information related to a project or an activity. Analysis helps identify, understand and prioritize issues, risks, opportunities and solutions for the project or activity. Impact is the effect or outcome of a project or an activity on something or someone else. Impact defines how the project or activity affects or influences other factors, such as performance, quality, satisfaction or value. Impact helps measure the success and effectiveness of the project or activity.
Reference: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 5.2

QUESTION 183
Which of the following filesystem formats would be the BEST choice to ensure read and write compatibility of USB flash drives across several generations of Microsoft operating systems?

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

Correct Answer: D
Section:
Explanation:
The best filesystem format to ensure read and write compatibility of USB flash drives across several generations of Microsoft operating systems is FAT32. FAT32 stands for File Allocation Table 32-bit and is a filesystem format that organizes and manages files and folders on storage devices using 32-bit clusters. FAT32 is compatible with most Microsoft operating systems since Windows 95 OSR2, as well as other operating systems such as Linux and Mac OS X. FAT32 can support storage devices up to 2TB in size and files up to 4GB in size. APFS stands for Apple File System and is a filesystem format that organizes and manages files and folders on storage devices using encryption, snapshots and cloning features. APFS is compatible with Mac OS X 10.13 High Sierra and later versions but not with Microsoft operating systems natively. Ext4 stands for Fourth Extended File System and is a filesystem format that organizes and manages files and folders on storage devices using journaling, extents and delayed allocation features. Ext4 is compatible with Linux operating systems but not with Microsoft operating systems natively.

QUESTION 184
A technician is troubleshooting a mobile device that was dropped. The technician finds that the screen (ails to rotate, even though the settings are correctly applied. Which of the following pieces of hardware should the technician replace to resolve the issue?

A. LCD
B. Battery
C. Accelerometer
D. Digitizer

Correct Answer: C
Section:
Explanation:
The piece of hardware that the technician should replace to resolve the issue of the screen failing to rotate on a mobile device that was dropped is the accelerometer. The accelerometer is a sensor that detects the orientation and movement of the mobile device by measuring the acceleration forces acting on it. The accelerometer allows the screen to rotate automatically according to the position and angle of the device. If the accelerometer is

damaged or malfunctioning, the screen may not rotate properly or at all, even if the settings are correctly applied. LCD stands for Liquid Crystal Display and is a type of display that uses liquid crystals and backlight to produce images on the screen. LCD is not related to the screen rotation feature but to the quality and brightness of the display. Battery is a component that provides power to the mobile device by storing and releasing electrical energy. Battery is not related to the screen rotation feature but to the battery life and performance of the device. Digitizer is a component that converts touch inputs into digital signals that can be processed by the mobile device. Digitizer is not related to the screen rotation feature but to the touch sensitivity and accuracy of the display. Reference: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.5

QUESTION 185

A technician downloads a validated security tool and notes the vendor hash of a58e87a2. When the download is complete, the technician again validates the hash, but the value returns as 2a876a7d3. Which of the following is the MOST likely cause of the issue?

A. Private-browsing mode
B. Invalid certificate
C. Modified file
D. Browser cache

Correct Answer: C
Section:
Explanation:

The most likely cause of the issue of having different hash values for a downloaded security tool is a modified file. A hash value is a unique and fixed-length string that is generated from an algorithm that processes data or files. A hash value can be used to verify the integrity and authenticity of data or files by comparing it with a known or expected value. If the hash values do not match, it means that the data or file has been altered or corrupted in some way. A modified file may result from intentional or unintentional changes, such as editing, encryption, compression or malware infection. Private-browsing mode is a feature that allows users to browse the web without storing any browsing history, cookies or cache on their browser. Private-browsing mode does not affect the hash value of a downloaded file but only how the browser handles user data. Invalid certificate is an error that occurs when a website or a server does not have a valid or trusted digital certificate that proves its identity and secures its communication. Invalid certificate does not affect the hash value of a downloaded file but only how the browser verifies the website or server's credibility. Browser cache is a temporary storage that stores copies of web pages, images and other content that users have visited on their browser.

QUESTION 186

An implementation specialist is replacing a legacy system at a vendor site that has only one wireless network available. When the specialist connects to Wi-Fi. the specialist realizes the insecure network has open authentication. The technician needs to secure the vendor's sensitive dat a. Which of the following should the specialist do FIRST to protect the company's data?

A. Manually configure an IP address, a subnet mask, and a default gateway.
B. Connect to the vendor's network using a VPN.
C. Change the network location to private.
D. Configure MFA on the network.

Correct Answer: B
Section:
Explanation:

The first thing that the specialist should do to protect the company's data on an insecure network with open authentication is to connect to the vendor's network using a VPN. A VPN stands for Virtual Private Network and is a technology that creates a secure and encrypted connection over a public or untrusted network. A VPN can protect the company's data by preventing eavesdropping, interception or modification of the network traffic by unauthorized parties. A VPN can also provide access to the company's internal network and resources remotely. Manually configuring an IP address, a subnet mask and a default gateway may not be necessary or possible if the vendor's network uses DHCP to assign network configuration parameters automatically. Manually configuring an IP address, a subnet mask and a default gateway does not protect the company's data from network attacks or threats. Changing the network location to private may not be advisable or effective if the vendor's network is a public or untrusted network. Changing the network location to private does not protect the company's data from network attacks or threats. Configuring MFA on the network may not be feasible or sufficient if the vendor's network has open authentication and does not support or require MFA. Configuring MFA on the network does not protect the company's data from network attacks or threats. Reference: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 3.3

QUESTION 187

A user contacts a technician about an issue with a laptop. The user states applications open without being launched and the browser redirects when trying to go to certain websites. Which of the following is MOST likely the cause of the user's issue?

A. Keylogger
B. Cryptominers
C. Virus
D. Malware

Correct Answer: D
Section:
Explanation:
The most likely cause of the user’s issue of applications opening without being launched and browser redirects when trying to go to certain websites is malware. Malware is a general term that refers to any software or code that is malicious or harmful to a computer or system. Malware can perform various unwanted or unauthorized actions on a computer or system, such as opening applications, redirecting browsers, displaying ads, stealing data, encrypting files or damaging hardware. Malware can infect a computer or system through various means, such as email attachments, web downloads, removable media or network connections. Keylogger is a type of malware that records and transmits the keystrokes made by a user on a keyboard. Keylogger can be used to steal personal or sensitive information, such as passwords, credit card numbers or chat messages. Keylogger does not typically open applications or redirect browsers but only captures user inputs. Cryptominers are a type of malware that use the computing resources of a computer or system to mine cryptocurrency, such as Bitcoin or Ethereum. Cryptominers can degrade the performance and increase the power consumption of a computer or system. Cryptominers do not typically open applications or redirect browsers but only consume CPU or GPU cycles. Virus is a type of malware that infects and replicates itself on other files or programs on a computer or system.

QUESTION 188
A technician is finalizing a new workstation for a user. The user's PC will be connected to the internet but will not require the same private address each time. Which of the following protocols will the technician MOST likely utilize?

A. DHCP
B. SMTP
C. DNS
D. RDP

Correct Answer: A
Section:
Explanation:
DHCP stands for Dynamic Host Configuration Protocol and it is used to assign IP addresses and other network configuration parameters to devices on a network automatically. This is useful for devices that do not require the same private address each time they connect to the internet.

QUESTION 189
A user is no longer able to start the OS on a computer and receives an error message indicating there is no OS found. A technician reviews the audit logs and notes that the user's system posted a S.M.A.R.T. error just days before this issue. Which of the following is the MOST likely cause of this issue?

A. Boot order
B. Malware
C. Drive failure
D. Windows updates

Correct Answer: C
Section:
Explanation:
A S.M.A.R.T. error is a warning that a hard drive is about to fail or has failed. This means that the OS cannot be loaded from the drive and the user will see an error message indicating there is no OS found. The most likely cause of this issue is drive failure.

QUESTION 190
A manager called the help desk to ask for assistance with creating a more secure environment for the finance department- which resides in a non-domain environment. Which of the following would be the BEST method to

protect against unauthorized use?

A. Implementing password expiration
B. Restricting user permissions
C. Using screen locks
D. Disabling unnecessary services

Correct Answer: B
Section:
Explanation:
Restricting user permissions is a method of creating a more secure environment for the finance department in a non-domain environment. This means that users will only have access to the files and resources that they need to perform their tasks and will not be able to modify or delete other files or settings that could compromise security or functionality.

QUESTION 191
Which of the following options should MOST likely be considered when preserving data from a hard drive for forensic analysis? (Select TWO).

A. Licensing agreements
B. Chain of custody
C. Incident management documentation
D. Data integrity
E. Material safety data sheet
F. Retention requirements

Correct Answer: B
Section:
Explanation:
Chain of custody and data integrity are two options that should most likely be considered when preserving data from a hard drive for forensic analysis. Chain of custody refers to the documentation and tracking of who has access to the data and how it is handled, stored, and transferred. Data integrity refers to the assurance that the data has not been altered, corrupted, or tampered with during the preservation process

QUESTION 192
A customer calls a service support center and begins yelling at a technician about a feature for a product that is not working to the customer's satisfaction. This feature is not supported by the service support center and requires a field technician to troubleshoot. The customer continues to demand service. Which of the following is the BEST course of action for the support center representative to take?

A. Inform the customer that the issue is not within the scope of this department.
B. Apologize to the customer and escalate the issue to a manager.
C. Ask the customer to explain the issue and then try to fix it independently.
D. Respond that the issue is something the customer should be able to fix.

Correct Answer: B
Section:
Explanation:
Apologizing to the customer and escalating the issue to a manager is the best course of action for the support center representative to take. This shows empathy and professionalism and allows the manager to handle the situation and provide the appropriate service or resolution for the customer.

QUESTION 193
All the desktop icons on a user's newly issued PC are very large. The user reports that the PC was working fine until a recent software patch was deployed. Which of the following would BEST resolve the issue?

A. Rolling back video card drivers
B. Restoring the PC to factory settings
C. Repairing the Windows profile
D. Reinstalling the Windows OS

Correct Answer: A
Section:
Explanation:
Rolling back video card drivers is the best way to resolve the issue of large desktop icons on a user’s newly issued PC. This means restoring the previous version of the drivers that were working fine before the software patch was deployed. The software patch may have caused compatibility issues or corrupted the drivers, resulting in display problems

QUESTION 194
A technician is installing a program from an ISO file. Which of the following steps should the technician take?

A. Mount the ISO and run the installation file.
B. Copy the ISO and execute on the server.
C. Copy the ISO file to a backup location and run the ISO file.
D. Unzip the ISO and execute the setup.exe file.

Correct Answer: A
Section:
Explanation:
Mounting the ISO and running the installation file is the correct way to install a program from an ISO file. An ISO file is an image of a disc that contains all the files and folders of a program. Mounting the ISO means creating a virtual drive that can access the ISO file as if it were a physical disc. Running the installation file means executing the setup program that will install the program on the computer

QUESTION 195
Which of the following would MOST likely be used to change the security settings on a user's device in a domain environment?

A. Security groups
B. Access control list
C. Group Policy
D. Login script

Correct Answer: C
Section:
Explanation:
Group Policy is the most likely tool to be used to change the security settings on a user’s device in a domain environment. Group Policy is a feature of Windows that allows administrators to manage and configure settings for multiple devices and users in a centralized way. Group Policy can be used to enforce security policies such as password complexity, account lockout, firewall rules, encryption settings, etc.

QUESTION 196
While staying at a hotel, a user attempts to connect to the hotel Wi-Fi but notices that multiple SSIDs have very similar names. Which of the following social-engineering attacks is being attempted?

A. Evil twin
B. Impersonation
C. Insider threat
D. Whaling

Correct Answer: A
Section:
Explanation:
An evil twin is a type of social-engineering attack that involves setting up a rogue wireless access point that mimics a legitimate one. The attacker can then intercept or modify the traffic of the users who connect to the fake SSID. The attacker may also use phishing or malware to steal credentials or personal information from the users

QUESTION 197
Which of the following is used to integrate Linux servers and desktops into Windows Active Directory environments?

A. apt-get
B. CIFS
C. Samba
D. greP

Correct Answer: C
Section:
Explanation:
Samba is a software suite that allows Linux servers and desktops to integrate with Windows Active Directory environments. Samba can act as a domain controller, a file server, a print server, or a client for Windows networks. Samba can also provide authentication and authorization services for Linux users and devices using Active Directory.

QUESTION 198
A technician installed a new application on a workstation. For the program to function properly, it needs to be listed in the Path Environment Variable. Which of the following Control Panel utilities should the technician use?

A. System
B. Indexing Options
C. Device Manager
D. Programs and Features

Correct Answer: A
Section:
Explanation:
System is the Control Panel utility that should be used to change the Path Environment Variable. The Path Environment Variable is a system variable that specifies the directories where executable files are located. To edit the Path Environment Variable, the technician should go to System &gt; Advanced system settings &gt; Environment Variables and then select Path from the list of system variables and click Edit.

QUESTION 199
An organization implemented a method of wireless security that requires both a user and the user's computer to be in specific managed groups on the server in order to connect to Wi-Fi. Which of the following wireless security methods BEST describes what this organization implemented?

A. TKIP
B. RADIUS
C. WPA2
D. AES

Correct Answer: B
Section:
Explanation:
RADIUS stands for Remote Authentication Dial-In User Service and it is a protocol that provides centralized authentication, authorization, and accounting for network access. RADIUS can be used to implement a method of wireless security that requires both a user and the user’s computer to be in specific managed groups on the server in order to connect to Wi-Fi. This is also known as 802.1X authentication or EAP-TLS authentication

QUESTION 200
A company acquired a local office, and a technician is attempting to join the machines at the office to the local domain. The technician notes that the domain join option appears to be missing. Which of the following editions of Windows is MOST likely installed on the machines?

A. Windows Professional
B. Windows Education
C. Windows Enterprise
D. Windows Home

Correct Answer: D
Section:
Explanation:
Windows Home is the most likely edition of Windows installed on the machines that do not have the domain join option. Windows Home is a consumer-oriented edition that does not support joining a domain or using Group Policy. Only Windows Professional, Education, and Enterprise editions can join a domain

QUESTION 201
Which of the following macOS features provides the user with a high-level view of all open windows?

A. Mission Control
B. Finder
C. Multiple Desktops
D. Spotlight

Correct Answer: A
Section:
Explanation:
Mission Control is the macOS feature that provides the user with a high-level view of all open windows. Mission Control allows the user to see and switch between multiple desktops, full-screen apps, and windows in a single screen. Mission Control can be accessed by swiping up with three or four fingers on the trackpad, pressing F3 on the keyboard, or moving the cursor to a hot corner

QUESTION 202
Which of the following should be used to secure a device from known exploits?

A. Encryption
B. Remote wipe
C. Operating system updates
D. Cross-site scripting

Correct Answer: C
Section:
Explanation:
Operating system updates are used to secure a device from known exploits. Operating system updates are patches or fixes that are released by the vendor to address security vulnerabilities, bugs, or performance issues. Operating system updates can also provide new features or enhancements to the device. It is important to keep the operating system updated to prevent attackers from exploiting known flaws or weaknesses.

QUESTION 203
The audio on a user's mobile device is inconsistent when the user uses wireless headphones and moves around. Which of the following should a technician perform to troubleshoot the issue?

A. Verify the Wi-Fi connection status.

B. Enable the NFC setting on the device.
C. Bring the device within Bluetooth range.
D. Turn on device tethering.

Correct Answer: C
Section:
Explanation:
Bringing the device within Bluetooth range is the best way to troubleshoot the issue of inconsistent audio when using wireless headphones and moving around. Bluetooth is a wireless technology that allows devices to communicate over short distances, typically up to 10 meters or 33 feet. If the device is too far from the headphones, the Bluetooth signal may be weak or interrupted, resulting in poor audio quality or loss of connection.

QUESTION 204
A technician is editing the hosts file on a few PCs in order to block certain domains. Which of the following would the technician need to execute after editing the hosts file?

A. Enable promiscuous mode.
B. Clear the browser cache.
C. Add a new network adapter.
D. Reset the network adapter.

Correct Answer: D
Section:
Explanation:
Resetting the network adapter is the best way to apply the changes made to the hosts file on a few PCs. The hosts file is a text file that maps hostnames to IP addresses and can be used to block certain domains by redirecting them to invalid or local addresses. Resetting the network adapter will clear the DNS cache and force the PC to use the new entries in the hosts file.

QUESTION 205
A data center is required to destroy SSDs that contain sensitive information. Which of the following is the BEST method to use for the physical destruction of SSDs?

A. Wiping
B. Low-level formatting
C. Shredding
D. Erasing

Correct Answer: C
Section:
Explanation:
Shredding is the best method to use for the physical destruction of SSDs because it reduces them to small pieces that cannot be recovered or accessed. Wiping, low-level formatting, and erasing are not effective methods for destroying SSDs because they do not physically damage the flash memory chips that store data1.

QUESTION 206
After a failed update, an application no longer launches and generates the following error message:
Application needs to be repaired. Which of the following Windows 10 utilities should a technician use to address this concern?

A. Device Manager
B. Administrator Tools
C. Programs and Features
D. Recovery

Correct Answer: D
Section:
Explanation:
Recovery is a Windows 10 utility that can be used to address the concern of a failed update that prevents an application from launching. Recovery allows the user to reset the PC, go back to a previous version of Windows, or use advanced startup options to troubleshoot and repair the system2. Device Manager, Administrator Tools, and Programs and Features are not Windows 10 utilities that can fix a failed update.

QUESTION 207
A technician receives a call (rom a user who is having issues with an application. To best understand the issue, the technician simultaneously views the user's screen with the user. Which of the following would BEST accomplish this task?

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

Correct Answer: C
Section:
Explanation:
VNC (Virtual Network Computing) is a protocol that allows a technician to simultaneously view and control a user's screen remotely. VNC uses a server-client model, where the user's computer runs a VNC server and the technician's computer runs a VNC client. VNC can work across different platforms and operating systems3. SSH (Secure Shell) is a protocol that allows a technician to access a user's command-line interface remotely, but not their graphical user interface. VPN (Virtual Private Network) is a technology that creates a secure and encrypted connection over a public network, but does not allow screen sharing. RDP (Remote Desktop Protocol) is a protocol that allows a technician to access a user's desktop remotely, but not simultaneously with the user.

QUESTION 208
A computer on a corporate network has a malware infection. Which of the following would be the BEST method for returning the computer to service?

A. Scanning the system with a Linux live disc, flashing the BIOS, and then returning the computer to service
B. Flashing the BIOS, reformatting the drive, and then reinstalling the OS
C. Degaussing the hard drive, flashing the BIOS, and then reinstalling the OS
D. Reinstalling the OS. flashing the BIOS, and then scanning with on-premises antivirus

Correct Answer: B
Section:
Explanation:
Flashing the BIOS, reformatting the drive, and then reinstalling the OS is the best method for returning a computer with a malware infection to service. Flashing the BIOS updates the firmware of the motherboard and can remove any malware that may have infected it. Reformatting the drive erases all data on it and can remove any malware that may have infected it. Reinstalling the OS restores the system files and settings to their original state and can remove any malware that may have modified them. Scanning the system with a Linux live disc may not detect or remove all malware infections. Degaussing the hard drive is an extreme method of destroying data that may damage the drive beyond repair. Reinstalling the OS before flashing the BIOS or scanning with antivirus may not remove malware infections that persist in the BIOS or other files.

QUESTION 209
A technician needs to access a Windows 10 desktop on the network in a SOHO using RDP. Although the connection is unsuccessful, the technician is able to ping the computer successfully. Which of the following is MOST likely preventing the connection?

A. The Windows 10 desktop has Windows 10 Home installed.
B. The Windows 10 desktop does not have DHCP configured.
C. The Windows 10 desktop is connected via Wi-Fi.
D. The Windows 10 desktop is hibernating.

Correct Answer: A
Section:
Explanation:
The Windows 10 desktop has Windows 10 Home installed, which does not support RDP (Remote Desktop Protocol) as a host. Only Windows 10 Pro, Enterprise, and Education editions can act as RDP hosts and allow remote access to their desktops1. The Windows 10 desktop does not have DHCP configured, is connected via Wi-Fi, or is hibernating are not likely to prevent the RDP connection if the technician is able to ping the computer successfully.

QUESTION 210
Which of the following often uses an SMS or third-party application as a secondary method to access a system?

A. MFA
B. WPA2
C. AES
D. RADIUS

Correct Answer: A
Section:
Explanation:
MFA (Multi-Factor Authentication) is a security measure that often uses an SMS or third-party application as a secondary method to access a system. MFA requires the user to provide two or more pieces of evidence to prove their identity, such as something they know (e.g., password), something they have (e.g., phone), or something they are (e.g., fingerprint)2. WPA2 (Wi-Fi Protected Access 2) is a security protocol for wireless networks that does not use SMS or third-party applications. AES (Advanced Encryption Standard) is a symmetric encryption algorithm that does not use SMS or third- party applications. RADIUS (Remote Authentication Dial-In User Service) is a network protocol that provides centralized authentication and authorization for remote access clients, but does not use SMS or third-party applications.

QUESTION 211
A company needs employees who work remotely to have secure access to the corporate intranet. Which of the following should the company implement?

A. Password-protected Wi-Fi
B. Port forwarding
C. Virtual private network
D. Perimeter network

Correct Answer: C
Section:
Explanation:
A virtual private network (VPN) is a technology that creates a secure and encrypted connection over a public network, such as the internet. A VPN allows remote employees to access the corporate intranet as if they were physically connected to the local network3. Password-protected Wi-Fi is a security measure for wireless networks that does not provide access to the corporate intranet. Port forwarding is a technique that allows external devices to access services on a private network through a router, but does not provide access to the corporate intranet. A perimeter network is a network segment that lies between an internal network and an external network, such as the internet, and provides an additional layer of security, but does not provide access to the corporate intranet.

QUESTION 212
A systems administrator is creating a new document with a list of the websites that users are allowed to access. Which of the following types of documents is the administrator MOST likely creating?

A. Access control list
B. Acceptable use policy
C. Incident report
D. Standard operating procedure

Correct Answer: A

Section:
Explanation:
An access control list (ACL) is a list of permissions associated with a system resource (object), such as a website. An ACL specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects1. A systems administrator can create an ACL to define the list of websites that users are allowed to access.
Reference: 1: Access-control list - Wikipedia (https://en.wikipedia.org/wiki/Access-control_list)

QUESTION 213
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

Correct Answer: A, C
Section:
Explanation:
Remote wipe is a feature that allows data to be deleted from a device or system remotely by an administrator or owner1. It is used to protect data from being compromised if the device is lost, stolen, or changed hands1. Device encryption is a feature that helps protect the data on a device by making it unreadable to unauthorized users2. It requires a key or a password to access the data2. Both features can help mitigate the risk of losing company trade secrets if a corporate phone is stolen.
Reference: 1: How to remote wipe Windows laptop (https://www.thewindowsclub.com/remote- wipe-windows-10) 2: Device encryption in Windows (https://support.microsoft.com/en- us/windows/device-encryption-in-windows-ad5dcf4b-dbe0-2331-228f-7925c2a3012d)

QUESTION 214
A user receives the following error while attempting to boot a computer.
BOOTMGR is missing
press Ctrl+Alt+Del to restart
Which of the following should a desktop engineer attempt FIRST to address this issue?

A. Repair Windows.
B. Partition the hard disk.
C. Reimage the workstation.
D. Roll back the updates.

Correct Answer: A
Section:
Explanation:
The error “BOOTMGR is missing” indicates that the boot sector is damaged or missing1. The boot sector is a part of the hard disk that contains the code and information needed to start Windows1. To fix this error, one of the possible methods is to run Startup Repair from Windows Recovery Environment (WinRE)1. Startup Repair is a tool that can automatically diagnose and repair problems with the boot process2.
Reference: 1: “Bootmgr is missing Press Ctrl+Alt+Del to restart” error when you start Windows (https://support.microsoft.com/en-us/topic/-bootmgr-is-missing-press-ctrl-alt-del-to-restart- when-you-start-windows-8bc1b94b-d243-1027-5410-aeb04d5cd5e2) 2: Startup Repair: frequently asked questions (https://support.microsoft.com/en-us/windows/startup-repair-frequently-asked- questions-f5f412a0-19c4-8e0a-9f68-bb0f17f3daa0)

QUESTION 215
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

Correct Answer: C
Section:
Explanation:
User Accounts is a Control Panel utility that allows the technician to manage user accounts and groups on a workstation1. The technician can use User Accounts to grant local administrative access to a user by adding the user to the Administrators group1. The Administrators group has full control over the workstation and can perform tasks such as installing software, changing system settings, and accessing all files.
Reference: 1: User Accounts (Control Panel) (https://docs.microsoft.com/en- us/windows/win32/shell/user-accounts) : Local Users and Groups (https://docs.microsoft.com/en- us/windows-server/identity/ad-ds/plan/security-best-practices/local-users-and-groups)

QUESTION 216
A user receives an error message from an online banking site that states the following:
Your connection is not private. Authority invalid.
Which of the following actions should the user take NEXT?

A. Proceed to the site.

B. Use a different browser.

C. Report the error to the bank.

D. Reinstall the browser.

Correct Answer: C
Section:
Explanation:
The error message “Your connection is not private. Authority invalid.” means that the web browser cannot verify the identity or security of the website’s SSL certificate. This could indicate that the website has been compromised, has a configuration error, or has an expired or invalid certificate. The user should not proceed to the site or use a different browser, as this could expose their sensitive information to potential attackers. The user should also not reinstall the browser, as this is unlikely to fix the error and could cause data loss. The best action for the user to take is to report the error to the bank and wait for them to resolve it.
Reference: : How to Fix “Your Connection Is Not Private” Errors (https://www.howtogeek.com/874436/how-to-fix-your-connection-is-not-private-errors/) : Fix connection errors (https://support.google.com/chrome/answer/6098869?hl=en)

QUESTION 217
A user notices a small USB drive is attached to the user's computer after a new vendor visited the office. The technician notices two files named grabber.exe and output.txt. Which of the following attacks is MOST likely occurring?

A. Trojan

B. Rootkit

C. Cryptominer

D. Keylogger

Correct Answer: D
Section:
Explanation:
A keylogger is a type of malware that records the keystrokes of a user and sends them to a remote attacker1. The attacker can use the captured information to steal passwords, credit card numbers, or other sensitive data. A keylogger can be installed on a computer by attaching a small USB drive that contains a malicious executable file, such as grabber.exe2. The output.txt file may contain the recorded keystrokes. The user should remove the USB drive and scan the computer for malware.
Reference: 2: What is grabber.exe? (https://www.freefixer.com/library/file/grabber.exe-55857/) 1:
What is a keylogger? (https://www.kaspersky.com/resource-center/definitions/keylogger)

QUESTION 218
A SOHO client is having trouble navigating to a corporate website. Which of the following should a technician do to allow access?

A. Adjust the content filtering.
B. Unmap port forwarding.
C. Disable unused ports.
D. Reduce the encryption strength

Correct Answer: A
Section:
Explanation:
Content filtering is a process that manages or screens access to specific emails or webpages based on their content categories1. Content filtering can be used by organizations to control content access through their firewalls and enforce corporate policies around information system management2. A SOHO client may have content filtering enabled on their network and may need to adjust it to allow access to a corporate website that is blocked by default. The client can use a software program, a hardware device, or a subscription service to configure the content filtering settings and whitelist the desired website2.
Reference: 1: Web content filtering (https://learn.microsoft.com/en-us/microsoft- 365/security/defender-endpoint/web-content-filtering?view=o365-worldwide) 2: What is Content Filtering? Definition and Types of Content Filters (https://www.fortinet.com/resources/cyberglossary/content-filtering)

QUESTION 219
Which of the following is used as a password manager in the macOS?

A. Terminal
B. FileVault
C. Privacy
D. Keychain

Correct Answer: D
Section:
Explanation:
Keychain is a feature of macOS that securely stores passwords, account numbers, and other confidential information for your Mac, apps, servers, and websites1. You can use the Keychain Access app on your Mac to view and manage your keychains and the items stored in them1. Keychain can also sync your passwords and other secure information across your devices using iCloud Keychain1. Keychain can be used as a password manager in macOS to help you keep track of and protect your passwords.
Reference: 1: Manage passwords using keychains on Mac (https://support.apple.com/guide/mac- help/use-keychains-to-store-passwords-mchlf375f392/mac)

QUESTION 220
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

Correct Answer: C
Section:
Explanation:
Robocopy is a command-line utility that can be used to mirror the source data for the backup. It can copy files and folders with various options, such as copying only changed files, preserving attributes and permissions, and retrying failed copies. Robocopy is more powerful and flexible than copy or xcopy, which are simpler commands that can only copy files and folders without mirroring or other advanced features. Copy-Item is a PowerShell cmdlet that can also copy files and folders, but it is not a native Windows utility and it requires PowerShell to run1.

Reference: 1: https://windowsreport.com/mirror-backup-software/

QUESTION 221
A change advisory board authorized a setting change so a technician is permitted to implement the change. The technician successfully implemented the change. Which of the following should be done NEXT?

A. Document the date and time of change.
B. Document the purpose of the change.
C. Document the risk level.
D. Document findings of the sandbox test.

Correct Answer: A
Section:
Explanation:
After implementing a change authorized by the change advisory board (CAB), the technician should document the date and time of change as part of the post-implementation review. This helps to track the change history, verify the success of the change, and identify any issues or incidents caused by the change1. Documenting the purpose of the change, the risk level, and the findings of the sandbox test are all part of the pre-implementation activities that should be done before submitting the change request to the CAB2.
Reference: 2: https://www.manageengine.com/products/service-desk/itil-change-management/cab- change-advisory-board.html 1: https://www.servicenow.com/content/dam/servicenow- assets/public/en-us/doc-type/success/quick-answer/change-advisory-board-setup.pdf

QUESTION 222
A company implemented a BYOD policy and would like to reduce data disclosure caused by malware that may infect these devices. Which of the following should the company deploy to address these concerns?

A. UAC
B. MDM
C. LDAP
D. SSO

Correct Answer: B
Section:
Explanation:
MDM stands for mobile device management, which is a type of software solution that allows remote management and security of mobile devices. MDM can help a company reduce data disclosure caused by malware that may infect these devices by enforcing security policies, such as encryption,
password protection, antivirus software, and remote wipe. MDM can also monitor and control the access of personal devices to corporate data and networks. UAC stands for user account control, which is a feature of Windows that prompts users for permission or an administrator password before making changes that affect the system. UAC may not be effective in preventing malware infection or data disclosure on personal devices. LDAP stands for lightweight directory access protocol, which is a protocol for accessing and managing information stored in a directory service,
such as user names and passwords. LDAP does not directly address the issue of malware infection or data disclosure on personal devices. SSO stands for single sign-on, which is a feature that allows users to access multiple applications or services with one set of credentials. SSO may not prevent
malware infection or data disclosure on personal devices, and may even increase the risk if the credentials are compromised.
https://www.nist.gov/news-events/news/2021/03/mobile-device-security-bring-your-own-devicebyod-draft-sp-1800-22

QUESTION 223
A technician is working on a way to register all employee badges and associated computer IDs. Which of the following options should the technician use in order to achieve this objective?

A. Database system
B. Software management
C. Active Directory description
D. Infrastructure as a Service

Correct Answer: A
Section:
Explanation:
A database system is a software application that allows storing, organizing, and managing data in a structured way. A database system can be used to register all employee badges and associated computer IDs by creating a table or a record for each employee that contains their badge number,
computer ID, name, and other relevant information. A database system can also facilitate searching, updating, and deleting data as needed. Software management is a general term that refers to the process of planning, developing, testing, deploying, and maintaining software applications. It does
not directly address the issue of registering employee badges and computer IDs. Active Directory description is a field in Active Directory that can be used to store additional information about an object, such as a user or a computer. It is not a software application that can be used to register
employee badges and computer IDs by itself. Infrastructure as a Service (IaaS) is a cloud computing model that provides servers, storage, networking, and software over the internet. It does not directly address the issue of registering employee badges and computer IDs either.
https://www.idcreator.com/
https://www.alphacard.com/photo-id-systems/card-type/employee-badges

QUESTION 224
An IT security team is implementing a new Group Policy that will return a computer to the login after three minutes. Which of the following BEST describes the change in policy?

A. Login times
B. Screen lock
C. User permission
D. Login lockout attempts

Correct Answer: B
Section:
Explanation:
Screen lock is a feature that returns a computer to the login screen after a period of inactivity,
requiring the user to enter their credentials to resume their session. Screen lock can be configured using Group Policy settings, such as Screen saver timeout and Interactive logon: Machine inactivity limit. Screen lock can help prevent unauthorized access to a computer when the user is away from
their desk. Login times are not a feature that returns a computer to the login screen, but a measure of how long it takes for a user to log in to a system. User permission is not a feature that returns a computer to the login screen, but a set of rights and privileges that determine what a user can do on a system. Login lockout attempts are not a feature that returns a computer to the login screen, but a security policy that locks out a user account after a number of failed login attempts.
https://woshub.com/windows-lock-screen-after-idle-via-gpo/

QUESTION 225
A technician needs to transfer a file to a user's workstation. Which of the following would BEST accomplish this task utilizing the workstation's built-in protocols?

A. VPN
B. SMB
C. RMM
D. MSRA

Correct Answer: B
Section:
Explanation:
SMB stands for Server Message Block, which is a network file sharing protocol that allows applications on a computer to read and write to files and to request services from server programs in a computer network. SMB is a built-in protocol in Windows operating systems and can be used to
transfer files between computers over a network. The technician can use SMB to access a file share on the user's workstation and copy the file to or from it. VPN stands for virtual private network, which is a technology that creates a secure and encrypted connection over a public network. VPN is
not a built-in protocol in Windows operating systems and does not directly transfer files between computers. RMM stands for remote monitoring and management, which is a type of software solution that allows remote

management and monitoring of devices and networks. RMM is not a
built-in protocol in Windows operating systems and does not directly transfer files between computers. MSRA stands for Microsoft Remote Assistance, which is a feature that allows a user to invite another user to view or control their computer remotely. MSRA is not a protocol, but an application that uses Remote Desktop Protocol (RDP) to establish a connection. MSRA does not directly transfer files between computers.
https://www.pcmag.com/picks/the-best-desktop-workstations

QUESTION 226
A customer called the help desk to report that a machine that was recently updated is no longer working. The support technician checks the latest logs to see what updates were deployed, but nothing was deployed in more than three weeks. Which of the following should the support technician do to BEST resolve the situation?

A. Offer to wipe and reset the device for the customer.
B. Advise that the help desk will investigate and follow up at a later date.
C. Put the customer on hold and escalate the call to a manager.
D. Use open-ended questions to further diagnose the issue.

Correct Answer: D
Section:
Explanation:
Open-ended questions are questions that require more than a yes or no answer and encourage the customer to provide more details and information. Using open-ended questions can help the support technician to understand the problem better, identify the root cause, and find a suitable solution.
Some examples of open-ended questions are:
What exactly is not working on your machine?
When did you notice the problem?
How often does the problem occur?
What were you doing when the problem happened?
What have you tried to fix the problem?
Offering to wipe and reset the device for the customer is not a good option, as it may result in data loss and inconvenience for the customer. It should be used as a last resort only if other troubleshooting steps fail. Advising that the help desk will investigate and follow up at a later date is
not a good option, as it may leave the customer unsatisfied and frustrated. It should be used only if the problem requires further research or escalation and cannot be resolved on the first call. Putting the customer on hold and escalating the call to a manager is not a good option, as it may waste time
and resources. It should be used only if the problem is beyond the support technician's scope or authority and requires managerial intervention.

QUESTION 227
Which of the following is MOST likely used to run .vbs files on Windows devices?

A. winmgmt.exe
B. powershell.exe
C. cscript.exe
D. explorer.exe

Correct Answer: C
Section:
Explanation:
A .vbs file is a Virtual Basic script written in the VBScript scripting language. It contains code that can be executed within Windows via the Windows-based script host (Wscript.exe), to perform certain admin and processing functions1. Cscript.exe is a command-line version of the Windows Script Host
that provides command-line options for setting script properties. Therefore, cscript.exe is most likely used to run .vbs files on Windows devices. Reference: 1: https://fileinfo.com/extension/vbs :
https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/cscript

QUESTION 228
Which of the following physical security controls can prevent laptops from being stolen?

A. Encryption
B. LoJack
C. Multifactor authentication
D. Equipment lock
E. Bollards

Correct Answer: D
Section:
Explanation:
An equipment lock is a physical security device that attaches a laptop to a fixed object, such as a desk or a table, with a cable and a lock. This can prevent the laptop from being stolen by unauthorized persons. Encryption, LoJack, multifactor authentication and bollards are other security measures, but they do not physically prevent theft. Verified Reference: https://www.comptia.org/blog/physicalsecurity
https://www.comptia.org/certifications/a

QUESTION 229
A user attempts to install additional software and receives a UAC prompt. Which of the following is the BEST way to resolve this issue?

A. Add a user account to the local administrator's group.
B. Configure Windows Defender Firewall to allow access to all networks.
C. Create a Microsoft account.
D. Disable the guest account.

Correct Answer: A
Section:
Explanation:
A user account that belongs to the local administrator's group has the permission to install software on a Windows machine. If a user receives a UAC (user account control) prompt when trying to install software, it means the user does not have enough privileges and needs to enter an administrator's password or switch to an administrator's account. Adding the user account to the local administrator's group can resolve this issue. Configuring Windows Defender Firewall, creating a
Microsoft account and disabling the guest account are not related to this issue. Verified Reference:
https://www.comptia.org/blog/user-account-control https://www.comptia.org/certifications/a

QUESTION 230
Which of the following wireless security features can be enabled lo allow a user to use login credentials to attach lo available corporate SSIDs?

A. TACACS+
B. Kerberos
C. Preshared key
D. WPA2/AES

Correct Answer: D
Section:
Explanation:
WPA2/AES (Wi-Fi Protected Access 2/Advanced Encryption Standard) is a wireless security standard that supports enterprise mode, which allows a user to use login credentials (username and password) to authenticate to available corporate SSIDs (service set identifiers). TACACS+ (Terminal Access Controller Access-Control System Plus) and Kerberos are network authentication protocols, but they are not wireless security features. Preshared key is another wireless security feature, but it does not use login credentials. Verified Reference: https://www.comptia.org/blog/wireless-securitystandards
https://www.comptia.org/certifications/a

QUESTION 231

Which of the following Is a package management utility for PCs that are running the Linux operating system?

A. chmod
B. yum
C. man
D. grep

Correct Answer: B
Section:
Explanation:
yum (Yellowdog Updater Modified) is a package management utility for PCs that are running the Linux operating system. It can be used to install, update and remove software packages from repositories. chmod (change mode) is a command that changes the permissions of files and directories in Linux. man (manual) is a command that displays the documentation of other commands in Linux. grep (global regular expression print) is a command that searches for patterns in text files in Linux. Verified Reference: https://www.comptia.org/blog/linux-package-management
https://www.comptia.org/certifications/a

QUESTION 232
A malicious file was executed automatically when a flash drive was plugged in. Which of the following features would prevent this type of incident?

A. Disabling UAC
B. Restricting local administrators
C. Enabling UPnP
D. Turning off AutoPlay

Correct Answer: D
Section:
Explanation:
AutoPlay is a feature that automatically runs programs or files when a removable media device, such as a flash drive, is plugged in. This can be exploited by malware authors who place malicious files on flash drives that execute automatically when inserted into a computer. Turning off AutoPlay can prevent this type of incident by requiring the user to manually open or run files from removable media devices. Disabling UAC (user account control), restricting local administrators and enabling UPnP (universal plug and play) are not effective ways to prevent this type of incident. Verified Reference: https://www.comptia.org/blog/autoplay-security-risk
https://www.comptia.org/certifications/a

QUESTION 233
Which of the following protects a mobile device against unwanted access when it is left unattended?

A. PIN code
B. OS updates
C. Antivirus software
D. BYOD policy

Correct Answer: A
Section:
Explanation:
A PIN code is a numeric password that protects a mobile device against unwanted access when it is left unattended. It requires the user to enter the correct code before unlocking the device. OS updates, antivirus software and BYOD policy are other security measures for mobile devices, but they do not prevent unauthorized access when the device is left unattended. Verified Reference:
https://www.comptia.org/blog/mobile-device-security https://www.comptia.org/certifications/a

QUESTION 234
A user is unable to access a web-based application. A technician verifies the computer cannot access any web pages at all. The computer obtains an IP address from the DHCP server. Then, the technician verifies the user can

ping localhost. the gateway, and known IP addresses on the interne! and receive a response. Which of the following Is the MOST likely reason tor the Issue?

A. A firewall is blocking the application.
B. The wrong VLAN was assigned.
C. The incorrect DNS address was assigned.
D. The browser cache needs to be cleared

Correct Answer: C
Section:
Explanation:
DNS (domain name system) is a protocol that translates domain names to IP addresses. If the computer has an incorrect DNS address assigned, it will not be able to resolve the domain names of web-based applications and access them. A firewall, a VLAN (virtual local area network) and a browser cache are not the most likely reasons for the issue, since the computer can ping known IP addresses on the internet and receive a response. Verified Reference:
https://www.comptia.org/blog/what-is-dns https://www.comptia.org/certifications/a

QUESTION 235
A technician is trying to encrypt a single folder on a PC. Which of the following should the technician use to accomplish this task?

A. FAT32
B. exFAT
C. BitLocker
D. EFS

Correct Answer: D
Section:
Explanation:
EFS (Encrypting File System) is a feature that allows a user to encrypt a single folder or file on a Windows PC. It uses a public key encryption system to protect the data from unauthorized access.
FAT32 and exFAT are file system formats that do not support encryption. BitLocker is a feature that encrypts the entire drive, not a single folder or file. Verified Reference:
https://www.comptia.org/blog/what-is-efs https://www.comptia.org/certifications/a

QUESTION 236
A technician removed a virus from a user's device. The user returned the device a week later with the same virus on it. Which of the following should the technician do to prevent future infections?

A. Disable System Restore.
B. Educate the end user.
C. Install the latest OS patches.
D. Clean the environment reinstallation.

Correct Answer: B
Section:
Explanation:
Educating the end user is the best way to prevent future infections by viruses or other malware. The technician should teach the user how to avoid risky behaviors, such as opening suspicious attachments, clicking on unknown links, downloading untrusted software, etc. Disabling System Restore, installing the latest OS patches and performing a clean installation are possible ways to remove existing infections, but they do not prevent future ones. Verified Reference:
https://www.comptia.org/blog/how-to-prevent-malware https://www.comptia.org/certifications/a

QUESTION 237
A customer calls the help desk asking for instructions on how to modify desktop wallpaper. Which of the following Windows 10 settings should the technician recommend?

A. Personalization
B. Apps
C. Updates
D. Display

Correct Answer: A
Section:
Explanation:
Personalization is a Windows 10 setting that allows a user to modify the desktop wallpaper, as well as other aspects of the appearance and behavior of the desktop, such as colors, themes, sounds, etc.
Apps is a Windows 10 setting that allows a user to manage the installed applications and their features. Updates is a Windows 10 setting that allows a user to check for and install the latest updates for the OS and other components. Display is a Windows 10 setting that allows a user to adjust the screen resolution, brightness, orientation, etc. Verified Reference:
https://www.comptia.org/blog/windows-10-settings https://www.comptia.org/certifications/a

QUESTION 238
A systems administrator installed the latest Windows security patch and received numerous tickets reporting slow performance the next day. Which of the following should the administrator do to resolve this issue?

A. Rebuild user profiles.
B. Roll back the updates.
C. Restart the services.
D. Perform a system file check.

Correct Answer: B
Section:
Explanation:

Rolling back the updates is the best way to resolve the issue of slow performance caused by installing the latest Windows security patch. This can be done by using the System Restore feature or by uninstalling the specific update from the Control Panel. Rebuilding user profiles, restarting the services and performing a system file check are not likely to fix the issue, since they do not undo the changes made by the update. Verified Reference:
https://www.comptia.org/blog/how-to-roll-backwindows-updates https://www.comptia.org/certifications/a

QUESTION 239
A corporation purchased new computers for a school. The computers are the same make and model and need to have the standard image loaded. Which of the following orchestration tools should a desktop administrator use tor wide-scale deployment?

A. USB drive
B. DVD Installation media
C. PXE boot
D. Recovery partition

Correct Answer: C
Section:
Explanation:
PXE (Preboot eXecution Environment) boot is an orchestration tool that allows a desktop administrator to deploy a standard image to multiple computers over a network. It requires a PXE server that hosts the image and a PXE client that boots from the network interface card (NIC). USB drive and DVD installation media are not orchestration tools, but manual methods of installing an image on each computer individually. Recovery partition is not an orchestration tool, but a hidden partition on the hard drive that contains an image of the factory settings. Verified Reference:
https://www.comptia.org/blog/what-is-pxe-boot https://www.comptia.org/certifications/a

QUESTION 240
Every time a user tries to open the organization's proprietary application on an Android tablet, the application immediately closes. Other applications are operating normally. Which of the following troubleshooting actions

would MOST likely resolve the Issue? (Select TWO).

A. Uninstalling the application
B. Gaining root access to the tablet
C. Resetting the web browser cache
D. Deleting the application cache
E. Clearing the application storage
F. Disabling mobile device management

Correct Answer: A, E
Section:
Explanation:
Uninstalling and reinstalling the application can resolve the issue of it crashing immediately on an
Android tablet, as it can fix any corrupted or missing files or settings. Clearing the application storage can also resolve the issue, as it can free up space and remove any conflicting data. Gaining root access to the tablet, resetting the web browser cache, deleting the application cache and disabling mobile device management are not likely to resolve the issue, as they do not affect how the application runs. Verified Reference:
https://www.comptia.org/blog/how-to-fix-android-appscrashing
https://www.comptia.org/certifications/a

QUESTION 241
A user's permissions are limited to read on a shared network folder using NTFS security settings.
Which of the following describes this type of security control?

A. SMS
B. MFA
C. ACL
D. MDM

Correct Answer: C
Section:
Explanation:
ACL (access control list) is a security control that describes what permissions a user or group has on a shared network folder using NTFS (New Technology File System) security settings. It can be used to grant or deny read, write, modify, delete or execute access to files and folders. SMS (short message service), MFA (multifactor authentication), MDM (mobile device management) are not security controls that apply to shared network folders.
Verified Reference:
https://www.comptia.org/blog/what-is-an-acl https://www.comptia.org/certifications/a

QUESTION 242
A company is looking lot a solution that provides a backup for all data on the system while providing the lowest impact to the network. Which of the following backup types will the company MOST likely select?

A. Off-site
B. Synthetic
C. Full
D. Differential

Correct Answer: B
Section:
Explanation:
A synthetic backup is a backup type that provides a backup for all data on the system while providing the lowest impact to the network. It combines a full backup with one or more incremental backups to create a single backup set, without requiring access to the original data source. Off-site is a backup location, not a backup type. Full and differential are backup types, but they have a higher impact on the network than synthetic. Verified

Reference: https://www.comptia.org/blog/what-is-a-syntheticbackup
https://www.comptia.org/certifications/a

QUESTION 243
A system drive is nearly full, and a technician needs lo tree up some space. Which of the following tools should the technician use?

A. Disk Cleanup
B. Resource Monitor
C. Disk Defragment
D. Disk Management

Correct Answer: A
Section:
Explanation:
Disk Cleanup is a tool that can free up some space on a system drive that is nearly full. It can delete temporary files, cached files, recycle bin files, old system files and other unnecessary data. Resource Monitor is a tool that shows the network activity of each process on a Windows machine. Disk Defragment is a tool that optimizes the performance of a hard drive by rearranging the data into contiguous blocks. Disk Management is a tool that allows creating, formatting, resizing and deleting partitions on a hard drive. Verified Reference: https://www.comptia.org/blog/how-to-use-diskcleanup
https://www.comptia.org/certifications/a

QUESTION 244
A technician needs to establish a remote access session with a user who has a Windows workstation.
The session must allow for simultaneous viewing of the workstation by both the user and technician.
Which of the following remote access technologies should be used?

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

Correct Answer: D
Section:
Explanation:
MSRA (Microsoft Remote Assistance) is a remote access technology that allows a technician to establish a session with a user who has a Windows workstation. The session allows for simultaneous viewing of the workstation by both the user and technician, as well as remote control and file transfer capabilities. RDP (remote desktop protocol) is another remote access technology, but it does not allow simultaneous viewing by default. VPN (virtual private network) and SSH (secure shell) are protocols that create secure tunnels between two devices over the internet, but they do not allow remote access sessions. Verified Reference: https://www.comptia.org/blog/what-is-msra
https://www.comptia.org/certifications/a

QUESTION 245
A technician is selling up a newly built computer. Which of the following is the FASTEST way for the technician to install Windows 10?

A. Factory reset
B. System Restore
C. In-place upgrade
D. Unattended installation

Correct Answer: D
Section:

Explanation:

An unattended installation is the fastest way to install Windows 10 on a newly built computer. It uses an answer file that contains all the configuration settings and preferences for the installation, such as language, product key, partition size, etc. It does not require any user interaction or input during the installation process. Factory reset, System Restore and in-place upgrade are not methods of installing Windows 10 on a new computer, but ways of restoring or updating an existing Windows installation.

Verified Reference: https://www.comptia.org/blog/what-is-an-unattended-installation

https://www.comptia.org/certifications/a

QUESTION 246

A systems administrator notices that a server on the company network has extremely high CPU utilization. Upon further inspection, the administrator sees that the server Is consistently communicating with an IP address that is traced back to a company that awards digital currency for solving hash algorithms. Which of the following was MOST likely used to compromise the server?

A. Keylogger
B. Ransomware
C. Boot sector virus
D. Cryptomining malware

Correct Answer: D
Section:
Explanation:

Cryptomining malware is a type of malicious program that uses the CPU resources of a compromised server to generate cryptocurrency, such as Bitcoin or Ethereum. It can cause extremely high CPU utilization and network traffic to the IP address of the cryptocurrency service. Keylogger, ransomware and boot sector virus are other types of malware, but they do not cause the same symptoms as cryptomining malware. Verified Reference: https://www.comptia.org/blog/what-is-cryptomining

https://www.comptia.org/certifications/a

QUESTION 247

A user opened a ticket regarding a corporate-managed mobile device. The assigned technician notices the OS Is several versions out of date. The user Is unaware the OS version is not current because auto-update is turned on. Which of the following is MOST likely the cause of the Issue?

A. The device does not have enough free space lo download the OS updates.
B. The device needs domain administrator confirmation to update to a major release.
C. The device is not compatible with the newest version of the OS.
D. The device is restricted from updating due to a corporate security policy.

Correct Answer: D
Section:
Explanation:

A corporate security policy can restrict a corporate-managed mobile device from updating its OS automatically, even if the auto-update feature is turned on. This can be done to prevent compatibility issues, security risks or performance problems caused by untested or unwanted updates. The device administrator can control when and how the updates are applied to the device.

The device not having enough free space, needing domain administrator confirmation or being incompatible with the newest version of the OS are not likely causes of the issue, since the user would receive an error message or a notification in those cases. Verified Reference:

https://www.comptia.org/blog/mobile-device-management

https://www.comptia.org/certifications/a

QUESTION 248

A user is receiving repeated pop-up advertising messages while browsing the internet. A malware scan Is unable to locate the source of an infection. Which of the following should the technician check NEXT?

A. Windows updates
B. DNS settings

C. Certificate store
D. Browser plug-ins

Correct Answer: D
Section:
Explanation:
Browser plug-ins are software components that add functionality to a web browser, such as playing videos, displaying animations, etc. However, some browser plug-ins can also be malicious or compromised and cause unwanted pop-up advertising messages while browsing the internet. A malware scan may not be able to locate the source of the infection if it is hidden in a browser plug-in.
Windows updates, DNS settings and certificate store are not likely sources of pop-up advertising messages. Verified Reference: https://www.comptia.org/blog/browser-security
https://www.comptia.org/certifications/a

QUESTION 249
Which of The following refers to the steps to be taken if an Issue occurs during a change Implementation?

A. Testing
B. Rollback
C. Risk
D. Acceptance

Correct Answer: B
Section:
Explanation:
Rollback refers to the steps to be taken if an issue occurs during a change implementation. It means restoring the system to its previous state before the change was applied, using backup data or configuration files. It can minimize the impact and downtime caused by a failed change. Testing refers to the steps to be taken before a change implementation, to verify that the change works as expected and does not cause any errors or conflicts. Risk refers to the potential negative consequences of a change implementation, such as data loss, security breach, performance degradation, etc. Acceptance refers to the steps to be taken after a change implementation, to confirm that the change meets the requirements and expectations of the stakeholders. Verified Reference: https://www.comptia.org/blog/change-management-process
https://www.comptia.org/certifications/a

QUESTION 250
A user reported that a laptop's screen turns off very quickly after silting for a few moments and is also very dim when not plugged in to an outlet Everything else seems to be functioning normally.
Which of the following Windows settings should be configured?

A. Power Plans
B. Hibernate
C. Sleep/Suspend
D. Screensaver

Correct Answer: A
Section:
Explanation:
Power Plans are Windows settings that allow a user to configure how a laptop's screen behaves when plugged in or running on battery power. They can adjust the screen brightness and the time before the screen turns off due to inactivity. Hibernate, Sleep/Suspend and Screensaver are other Windows settings that affect how a laptop's screen behaves, but they do not allow changing the screen brightness or turning off time. Verified Reference: https://www.comptia.org/blog/windowspower-plans https://www.comptia.org/certifications/a

QUESTION 251
Which of the following security methods supports the majority of current Wi-Fi-capable devices without sacrificing security?

A. WPA3

B. MAC filleting
C. RADIUS
D. TACACS+

Correct Answer: A
Section:
Explanation:
WPA3 (Wi-Fi Protected Access 3) is a wireless security method that supports the majority of current
Wi-Fi-capable devices without sacrificing security. It is backward compatible with WPA2 devices and offers enhanced encryption and authentication features. MAC filtering is another wireless security method, but it can be easily bypassed by spoofing MAC addresses. RADIUS (Remote Authentication Dial-In User Service) and TACACS+ (Terminal Access Controller Access-Control System Plus) are network authentication protocols, but they are not wireless security methods by themselves.
Verified Reference: https://www.comptia.org/blog/wireless-security-standards
https://www.comptia.org/certifications/a

QUESTION 252
A technician is setting up a newly built computer. Which of the following is the fastest way for the technician to install Windows 10?

A. Factory reset
B. System Restore
C. In-place upgrade
D. Unattended installation

Correct Answer: D
Section:
Explanation:
An unattended installation is a method of installing Windows 10 that does not require any user input or interaction during the installation process. An unattended installation can be performed by using an answer file, which is a file that contains all the configuration settings and preferences for the installation, such as the product key, the language, the partition size, and the user accounts. An unattended installation can be the fastest way to install Windows 10, as it automates and streamlines the installation process. Factory reset, System Restore, and in-place upgrade are not methods of installing Windows 10.

QUESTION 253
Which of the following allows access to the command line in macOS?

A. PsExec
B. command.com
C. Terminal
D. CMD

Correct Answer: C
Section:
Explanation:
Terminal is an application that allows access to the command line in macOS. The command line is an interface that allows users to interact with the operating system and perform various tasks by typing commands and arguments. Terminal can be used to launch programs, manage files and folders, configure settings, troubleshoot issues, and run scripts in macOS. PsExec, command.com, and CMD are not applications that allow access to the command line in macOS.

QUESTION 254
A user visits a game vendor's website to view the latest patch notes, but this information is not available on the page. Which of the following should the user perform before reloading the page?

A. Synchronize the browser data.

B. Enable private browsing mode.
C. Mark the site as trusted.
D. Clear the cached file.

Correct Answer: D
Section:
Explanation:
Clearing the cached file is an action that can help resolve the issue of not seeing the latest patch notes on a game vendor's website. A cached file is a copy of a web page or file that is stored locally on the user's browser or device for faster loading and offline access. However, sometimes a cached file may become outdated or corrupted and prevent the user from seeing the most recent or accurate version of a web page or file. Clearing the cached file can force the browser to download and display the latest version from the server instead of using the old copy from the cache.
Synchronizing the browser data, enabling private browsing mode, and marking the site as trusted are not actions that can help resolve this issue.

QUESTION 255
An administrator responded to an incident where an employee copied financial data to a portable hard drive and then left the company with the dat a. The administrator documented the movement of the evidence. Which of the following concepts did the administrator demonstrate?

A. Preserving chain of custody
B. Implementing data protection policies
C. Informing law enforcement
D. Creating a summary of the incident

Correct Answer: A
Section:
Explanation:
Preserving chain of custody is a concept that refers to the documentation and tracking of who handled, accessed, modified, or transferred a piece of evidence, when, where, why, and how.
Preserving chain of custody can help establish the authenticity, integrity, and reliability of the evidence, as well as prevent tampering, alteration, or loss of the evidence. An administrator who documented the movement of the evidence demonstrated the concept of preserving chain of custody. Implementing data protection policies, informing law enforcement, and creating a summary of the incident are not concepts that describe the action of documenting the movement of the evidence.

QUESTION 256
Which of the following threats will the use of a privacy screen on a computer help prevent?

A. Impersonation
B. Shoulder surfing
C. Whaling
D. Tailgating

Correct Answer: B
Section:
Explanation:
Shoulder surfing is a threat that involves someone looking over another person's shoulder to observe their screen, keyboard, or other sensitive information. Shoulder surfing can be used to steal passwords, personal identification numbers (PINs), credit card numbers, or other confidential data.
The use of a privacy screen on a computer can help prevent shoulder surfing by limiting the viewing angle of the screen and making it harder for someone to see the screen from the side or behind.
Impersonation, whaling, and tailgating are not threats that can be prevented by using a privacy screen on a computer.

QUESTION 257
Users access files in the department share. When a user creates a new subfolder, only that user can access the folder and Its files. Which of the following will MOST likely allow all users to access the new folders?

A. Assigning share permissions
B. Enabling inheritance
C. Requiring multifactor authentication
D. Removing archive attribute

Correct Answer: B
Section:
Explanation:
Enabling inheritance is a method that allows new subfolders to inherit the permissions and settings from their parent folder. If users can access files in the department share, but not in the new subfolders created by other users, it may indicate that inheritance is disabled and that each new subfolder has its own permissions and settings that restrict access to only the creator. Enabling inheritance can help resolve this issue by allowing all users to access the new subfolders with the same permissions and settings as the department share. Assigning share permissions, requiring multifactor authentication, and removing archive attribute are not methods that can most likely allow all users to access the new folders.

QUESTION 258
A user has a computer with Windows 10 Home installed and purchased a Windows 10 Pro license.
The user is not sure how to upgrade the OS. Which of the following should the technician do to apply this license?

A. Copy the c:\Wlndows\wlndows.lie file over to the machine and restart.
B. Redeem the included activation key card for a product key.
C. Insert a Windows USB hardware dongle and initiate activation.
D. Activate with the digital license included with the device hardware.

Correct Answer: B
Section:
Explanation:
Redeeming the included activation key card for a product key is the correct way to apply a Windows 10 Pro license to a computer that has Windows 10 Home installed. The activation key card is a physical or digital card that contains a 25-digit code that can be used to activate Windows 10 Pro online or by phone. Copying the windows.lie file, inserting a Windows USB hardware dongle and activating with the digital license are not valid methods of applying a Windows 10 Pro license.
Verified Reference: https://www.comptia.org/blog/how-to-upgrade-windows-10-home-to-pro
https://www.comptia.org/certifications/a

QUESTION 259
A user is unable to access files on a work PC after opening a text document. The text document was labeled "URGENT PLEASE READ.txt - In active folder, .txt file titled urgent please read". Which of the following should a support technician do FIRST?

A. Quarantine the host in the antivirus system.
B. Run antivirus scan tor malicious software.
C. Investigate how malicious software was Installed.
D. Reimage the computer.

Correct Answer: B
Section:
Explanation:
Running an antivirus scan for malicious software is the first step that a support technician should do when a user reports a virus on a PC. The antivirus scan can detect and remove the virus, as well as prevent further damage or infection. Quarantining the host, investigating how the malware was installed and reimaging the computer are possible steps that can be done after running the antivirus scan, depending on the situation and the results of the scan. Verified Reference:
https://www.comptia.org/blog/how-to-remove-a-virus https://www.comptia.org/certifications/a

QUESTION 260
Which of the following Is used to identify potential issues with a proposed change poor lo implementation?

A. Request form
B. Rollback plan
C. End-user acceptance
D. Sandbox testing

Correct Answer: D
Section:
Explanation:
Sandbox testing is a method of identifying potential issues with a proposed change prior to implementation. It involves creating a simulated or isolated environment that mimics the real system and applying the change to it. This can help to verify that the change works as expected and does not cause any errors or conflicts. Request form, rollback plan and end-user acceptance are other components of a change management process, but they do not involve identifying issues with a change. Verified Reference: https://www.comptia.org/blog/what-is-sandbox-testing
https://www.comptia.org/certifications/a

QUESTION 261
Which of the following operating systems is considered closed source?

A. Ubuntu
B. Android
C. CentOS
D. OSX

Correct Answer: D
Section:
Explanation:
OSX (now macOS) is an operating system that is considered closed source, meaning that its source code is not publicly available or modifiable by anyone except its developers. It is owned and maintained by Apple Inc. Ubuntu, Android and CentOS are operating systems that are considered open source, meaning that their source code is publicly available and modifiable by anyone who wants to contribute or customize them. Verified Reference: https://www.comptia.org/blog/opensource-vs-closed-source-software https://www.comptia.org/certifications/a

QUESTION 262
The courts determined that a cybercrimes case could no longer be prosecuted due to the agency's handling of evidence. Which of the following was MOST likely violated during the investigation?

A. Open-source software
B. EULA
C. Chain of custody
D. AUP

Correct Answer: C
Section:
Explanation:
Chain of custody is a process that documents how evidence is collected, handled, stored and transferred during a cybercrime investigation. It ensures that the evidence is authentic, reliable and admissible in court. If the chain of custody is violated during an investigation, it can compromise the integrity of the evidence and lead to the case being dismissed. Open-source software, EULA (enduser license agreement) and AUP (acceptable use policy) are not related to cybercrime investigations or evidence handling. Verified Reference: https://www.comptia.org/blog/what-is-chain-of-custody
https://www.comptia.org/certifications/a

QUESTION 263

A remote user is having issues accessing an online share. Which of the following tools would MOST likely be used to troubleshoot the Issue?

A. Screen-sharing software
B. Secure shell
C. Virtual private network
D. File transfer software

Correct Answer: A
Section:
Explanation:
Screen-sharing software is a tool that allows a technician to remotely view and control a user's screen over the internet. It can be used to troubleshoot issues with accessing an online share, as well as other problems that require visual inspection or guidance. Secure shell (SSH) is a protocol that allows remote access and command execution on another device, but it does not allow screensharing.
Virtual private network (VPN) is a protocol that creates a secure tunnel between two devices over the internet, but it does not allow remote troubleshooting. File transfer software is a tool that allows transferring files between two devices over the internet, but it does not allow screen-sharing.
Verified Reference: https://www.comptia.org/blog/what-is-screen-sharing-software
https://www.comptia.org/certifications/a

QUESTION 264
A user reports a virus is on a PC. The user installs additional real-lime protection antivirus software, and the PC begins performing extremely slow. Which of the following steps should the technician take to resolve the issue?

A. Uninstall one antivirus software program and install a different one.
B. Launch Windows Update, and then download and install OS updates
C. Activate real-time protection on both antivirus software programs
D. Enable the quarantine feature on both antivirus software programs.
E. Remove the user-installed antivirus software program.

Correct Answer: E
Section:
Explanation:
Removing the user-installed antivirus software program is the best way to resolve the issue of extremely slow performance caused by installing additional real-time protection antivirus software on a PC. Having more than one antivirus software program running at the same time can cause conflicts, resource consumption and performance degradation. Uninstalling one antivirus software program and installing a different one, activating real-time protection on both antivirus software programs, enabling the quarantine feature on both antivirus software programs and launching Windows Update are not effective ways to resolve the issue. Verified Reference:
https://www.comptia.org/blog/why-you-shouldnt-run-multiple-antivirus-programs-at-the-sametime
https://www.comptia.org/certifications/a

QUESTION 265
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

Correct Answer: A, B
Section:
Explanation:
Booting into safe mode and performing a malware scan are the steps that a technician should perform when troubleshooting an issue with pop-up advertising messages on a PC. Safe mode is a diagnostic mode that starts the

PC with minimal drivers and services, which can prevent the pop-up malware from running. Malware scan is a tool that can detect and remove the pop-up malware, as well as prevent further infection or damage. Investigating how the malware was installed, reinstalling the browser and restarting the machine are possible steps that can be done after booting into safe mode and performing a malware scan, depending on the situation and the results of the scan.
Verified Reference: https://www.comptia.org/blog/how-to-boot-into-safe-mode
https://www.comptia.org/certifications/a

QUESTION 266
A systems administrator is experiencing Issues connecting from a laptop to the corporate network using PKI. Which to the following tools can the systems administrator use to help remediate the issue?

A. certmgr.msc
B. msconfig.exe
C. lusrmgr.msc
D. perfmon.msc

Correct Answer: A
Section:
Explanation:
certmgr.msc is a tool that can be used to troubleshoot issues with PKI (public key infrastructure) on a Windows machine. It allows a system administrator to view, manage and import certificates, as well as check their validity, expiration and revocation status. msconfig.exe, lusrmgr.msc and perfmon.msc are other tools that can be used for different purposes on a Windows machine, but they are not related to PKI. Verified Reference:
https://www.comptia.org/blog/what-is-certmgr-msc
https://www.comptia.org/certifications/a

QUESTION 267
An application user received an email indicating the version of the application currently in use will no longer be sold. Users with this version of the application will no longer receive patches or updates either. Which of the following indicates a vendor no longer supports a product?

A. AUP
B. EULA
C. EOL
D. UAC

Correct Answer: C
Section:
Explanation:
EOL (end-of-life) is a term that indicates a vendor no longer supports a product. It means that the product will no longer be sold, updated or patched by the vendor, and that the users should migrate to a newer version or alternative product. AUP (acceptable use policy), EULA (end-user license agreement) and UAC (user account control) are not terms that indicate a vendor no longer supports a product. Verified Reference:
https://www.comptia.org/blog/what-is-end-of-life
https://www.comptia.org/certifications/a

QUESTION 268
A user called the help desk lo report an Issue with the internet connection speed on a laptop. The technician thinks that background services may be using extra bandwidth. Which of the following tools should the technician use to investigate connections on the laptop?

A. nslookup
B. net use
C. netstat
D. net user

Correct Answer: C
Section:
Explanation:
netstat is a tool that can be used to investigate connections on a Windows machine. It displays information about the active TCP connections, listening ports, routing tables, network statistics, etc.
nslookup is a tool that can be used to query DNS servers and resolve domain names to IP addresses.
net use is a tool that can be used to connect or disconnect network drives or printers. net user is a tool that can be used to create or modify user accounts on a Windows machine. Verified Reference:
https://www.comptia.org/blog/what-is-netstat https://www.comptia.org/certifications/a

QUESTION 269
A remote user is experiencing issues with Outlook settings and asks a technician to review the settings. Which of the following can the technician use to access the user's computer remotely?

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

Correct Answer: B
Section:
Explanation:
One of the possible ways to access the user's computer remotely is to use RDP, which stands for Remote Desktop Protocol. RDP is a protocol that allows a user to connect to another computer over a network and use its graphical interface. RDP is commonly used for remote desktop software, such as Microsoft Remote Desktop Connection1. To use RDP, the user's computer must run RDP server software, and the technician must run RDP client software. The technician can then enter the user's IP address or hostname, and provide the appropriate credentials to log in to the user's computer.
Once connected, the technician can view and control the user's desktop, and review the Outlook settings.

QUESTION 270
A workstation is displaying a message indicating that a user must exchange cryptocurrency for a decryption key. Which of the following is the best way for a technician to return the device to service safely?

A. Run an AV scan.
B. Reinstall the operating system
C. Install a software firewall.
D. Perform a system restore.
E. Comply with the on-screen instructions.

Correct Answer: B
Section:
Explanation:
The best way for a technician to return the device to service safely is to reinstall the operating system. This is because the device is infected by ransomware, which is a form of malware that encrypts files and demands payment for decryption. Reinstalling the operating system will erase the ransomware and restore the device to its original state. However, this will also delete any data that was not backed up before the infection. Therefore, it is important to have regular backups of critical data and protect them from ransomware attacks1.
The other options are not effective or safe for ransomware recovery. Running an AV scan may not detect or remove the ransomware, especially if it is a new or unknown variant. Installing a software firewall may prevent future attacks, but it will not help with the current infection. Performing a system restore may not work if the ransomware has corrupted or deleted the restore points.
Complying with the on-screen instructions is not advisable, as it will encourage the attackers and there is no guarantee that they will provide the decryption key after receiving the payment.
To prevent and recover from ransomware attacks, it is recommended to follow some best practices, such as234:
Use strong passwords and multifactor authentication for all accounts and devices.
Keep all software and firmware updated with the latest security patches.
Avoid opening suspicious or unsolicited emails and attachments.
Educate users and staff on how to recognize and report phishing and social engineering attempts.
Use antivirus software and enable real-time protection.

Enable network segmentation and firewall rules to limit the spread of ransomware.
Implement a Zero Trust security model to verify all requests and devices before granting access.
Create and test backups of critical data and store them offline or in a separate network.
Recover safely by isolating the infected devices, identifying the ransomware variant, and restoring data from backups.
Report any ransomware incidents to law enforcement agencies and seek help from experts.

QUESTION 271
A customer has a USB-only printer attached to a computer. A technician is configuring an arrangement that allows other computers on the network to use the printer. In which of the following locations on the customer's desktop should the technician make this configuration?

A. Printing Preferences/Advanced tab
B. Printer Properties/Sharing tab
C. Printer Properties/Security tab
D. Printer Properties/Ports tab

Correct Answer: B
Section:
Explanation:
The correct answer is B. Printer Properties/Sharing tab. This is the location where the technician can enable printer sharing and assign a share name for the USB printer. This will allow other computers on the network to access the printer by using the share name or the IP address of the computer that has the printer attached1.
1: CompTIA A+ Certification Exam: Core 2 Objectives, page 15, section 1.9.

QUESTION 272
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
Disabling local administrator accounts

Correct Answer: D, E
Section:
Explanation:
The correct answers are D. Restricting log-in times and E. Enabling a screen lock. These are the security measures that can be used to prevent the computers from being accessed by unsupervised contractors in the building. Restricting log-in times means setting a policy that allows users to log in only during certain hours, such as the regular working hours of the company. This will prevent unauthorized access by contractors who work at night1. Enabling a screen lock means setting a policy that requires users to enter a password or a PIN to unlock their screens after a period of inactivity. This will prevent unauthorized access by contractors who might try to use the computers when the users are away2.
1: CompTIA A+ Certification Exam: Core 2 Objectives, page 19, section 2.3. 2: CompTIA A+ Certification Exam: Core 2 Objectives, page 20, section 2.4.

QUESTION 273
A technician is unable to access the internet or named network resources. The technician receives a valid IP address from the DHCP server and can ping the default gateway. Which of the following should the technician check next to resolve the issue?

A. Verify the DNS server settings.
B. Turn off the Windows firewall.

C. Confirm the subnet mask is correct.
D. Configure a static IP address.

Correct Answer: A
Section:
Explanation:
The correct answer is
A. Verify the DNS server settings. This is because the DNS server is responsible for resolving domain names to IP addresses, which is necessary for accessing the internet or named network resources. If the DNS server settings are incorrect or the DNS server is down, the technician will not be able to access these resources even if they have a valid IP address and can ping the default gateway1.
1: CompTIA A+ Certification Exam: Core 2 Objectives, page 16, section 1.10.

QUESTION 274
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

Correct Answer: B, E
Section:
Explanation:
The correct answers are B. Removing the applications from startup and E. Defragmenting the hard drive. These are the operations that would be best to do to resolve the issue of a slow boot at a minimal expense.
Removing the applications from startup means disabling the programs that run automatically when the PC is turned on. This will reduce the load on the CPU and RAM and speed up the boot process1.
Defragmenting the hard drive means rearranging the files on the disk so that they are stored in contiguous blocks. This will improve the disk performance and reduce the time it takes to read and write data2.
1: CompTIA A+ Certification Exam: Core 2 Objectives, page 23, section 3.1. 2: CompTIA A+ Certification Exam: Core 2 Objectives, page 24, section 3.2.

QUESTION 275
The screen on a user's mobile device is not autorotating even after the feature has been enabled and the device has been restarted. Which of the following should the technician do next to troubleshoot the issue?

A. Calibrate the phone sensors.
B. Enable the touch screen.
C. Reinstall the operating system.
D. Replace the screen.

Correct Answer: A
Section:
Explanation:
Calibrating the phone sensors is a step that can troubleshoot the issue of screen not autorotating on a mobile device. Screen autorotation is a feature that automatically adjusts the screen orientation based on the device's position and movement. Screen autorotation relies on sensors such as accelerometer and gyroscope to detect the device's tilt and rotation. Calibrating the phone sensors can help fix any errors or inaccuracies in the sensor readings that may prevent screen autorotation from working properly. Enabling the touch screen, reinstalling the operating system, and replacing the screen are not steps that should be done next to troubleshoot this issue.

QUESTION 276
Which of the following would most likely be used to extend the life of a device?

A. Battery backup
B. Electrostatic discharge mat
C. Proper ventilation
D. Green disposal

Correct Answer: C
Section:
Explanation:
Proper ventilation is a factor that can extend the life of a device by preventing overheating and thermal damage to the device's components. Proper ventilation means ensuring that there is enough airflow around and inside the device to dissipate heat and maintain a suitable temperature for optimal performance. Proper ventilation can be achieved by using fans, heat sinks, vents, or liquid cooling systems, as well as avoiding placing the device near heat sources or in enclosed spaces. Battery backup, electrostatic discharge mat, and green disposal are not factors that can extend the life of a device.

QUESTION 277
A company is experiencing a DDoS attack. Several internal workstations are the source of the traffic.
Which of the following types of infections are the workstations most likely experiencing? (Select two).

A. Zombies
B. Keylogger
C. Adware
D. Botnet
E. Ransomware
F. Spyware

Correct Answer: A, D
Section:
Explanation:
Zombies and botnets are terms that describe the types of infections that can cause internal workstations to participate in a DDoS (distributed denial-of-service) attack. A DDoS attack is a malicious attempt to disrupt the normal functioning of a website or a network by overwhelming it with a large amount of traffic from multiple sources. Zombies are infected computers that are remotely controlled by hackers without the owners' knowledge or consent. Botnets are networks of zombies that are coordinated by hackers to launch DDoS attacks or other malicious activities.
Keylogger, adware, ransomware, and spyware are not types of infections that can cause internal workstations to participate in a DDoS attack.

QUESTION 278
A help desk technician determines a motherboard has failed. Which of the following is the most logical next step in the remediation process?

A. Escalating the issue to Tier 2
B. Verifying warranty status with the vendor
C. Replacing the motherboard
D. Purchasing another PC

Correct Answer: B
Section:
Explanation:
Verifying warranty status with the vendor is the most logical next step in the remediation process after determining that a motherboard has failed. A warranty is a guarantee from the vendor that covers the repair or replacement of defective or faulty products within a specified period of time.
Verifying warranty status with the vendor can help the technician determine if the motherboard is eligible for warranty service and what steps to take to obtain it. Escalating the issue to Tier 2, replacing the motherboard, and purchasing another PC are not the most logical next steps in the remediation process.

QUESTION 279
Which of the following helps ensure that a piece of evidence extracted from a PC is admissible in a court of law?

A. Data integrity form
B. Valid operating system license
C. Documentation of an incident
D. Chain of custody

Correct Answer: D
Section:
Explanation:
Chain of custody is a process that helps ensure that a piece of evidence extracted from a PC is admissible in a court of law. Chain of custody refers to the documentation and tracking of who handled, accessed, modified, or transferred the evidence, when, where, why, and how. Chain of custody can help establish the authenticity, integrity, and reliability of the evidence, as well as prevent tampering, alteration, or loss of the evidence. Data integrity form, valid operating system license, and documentation of an incident are not processes that can ensure that a piece of evidence extracted from a PC is admissible in a court of law.

QUESTION 280
A user installed a new computer game. Upon starting the game, the user notices the frame rates are low. Which of the following should the user upgrade to resolve the issue?

A. Hard drive
B. Graphics card
C. Random-access memory
D. Monitor

Correct Answer: B
Section:
Explanation:
A graphics card, also known as a video card or a GPU (graphics processing unit), is a component that can affect the performance of a computer game. A graphics card is responsible for rendering and displaying graphics on the screen, such as images, animations, and effects. A computer game may require a high level of graphics processing power to run smoothly and achieve high frame rates, which are the number of frames per second (FPS) that the game can display. Upgrading to a better graphics card can improve the performance of a computer game by increasing its graphics quality and frame rates. Hard drive, random-access memory, and monitor are not components that can directly improve the performance of a computer game.

QUESTION 281
A company would like to implement multifactor authentication for all employees at a minimal cost.
Which of the following best meets the company's requirements?

A. Biometrics
B. Soft token
C. Access control lists
D. Smart card

Correct Answer: B
Section:
Explanation:
A soft token, also known as a software token or an OTP (one-time password) app, is a type of multifactor authentication that generates a temporary code or password on a user's device, such as a smartphone or a tablet. The user must enter this code or password along with their username and password to access their account or service. A soft token can help improve security by adding an extra layer of verification and preventing unauthorized access even if the user's credentials are compromised. A soft token can also be implemented at a minimal cost, as it does not require any additional hardware or infrastructure. Biometrics, access control lists, and smart card are not types of multifactor authentication that can be implemented at a minimal cost.

QUESTION 282
A technician is setting up a new laptop. The company's security policy states that users cannot install virtual machines. Which of the following should the technician implement to prevent users from enabling virtual technology on their laptops?

A. UEFI password
B. Secure boot
C. Account lockout
D. Restricted user permissions

Correct Answer: B
Section:
Explanation:
A technician setting up a new laptop must ensure that users cannot install virtual machines as the company's security policy states One way to prevent users from enabling virtual technology is by implementing Secure Boot. Secure Boot is a feature of UEFI firmware that ensures the system only boots using firmware that is trusted by the manufacturer. It verifies the signature of all bootloaders, operating systems, and drivers before running them, preventing any unauthorized modifications to the boot process. This will help prevent users from installing virtual machines on the laptop without authorization.

QUESTION 283
The web browsing speed on a customer's mobile phone slows down every few weeks and then returns to normal after three or four days. Restarting the device does not usually restore performance. Which of the following should a technician check FIRST to troubleshoot this issue?

A. Data usage limits
B. Wi-Fi connection speed
C. Status of airplane mode
D. System uptime

Correct Answer: B
Section:
Explanation:
The technician should check the Wi-Fi connection speed first to troubleshoot this issue. Slow web browsing speed on a mobile phone can be caused by a slow Wi-Fi connection. The technician should check the Wi-Fi connection speed to ensure that it is fast enough to support web browsing. If the WiFi connection speed is slow, the technician should troubleshoot the Wi-Fi network to identify and resolve the issue.

QUESTION 284
Following a recent power outage, several computers have been receiving errors when booting. The technician suspects file corruption has occurred. Which of the following steps should the technician try FIRST to correct the issue?

A. Rebuild the Windows profiles.
B. Restore the computers from backup.
C. Reimage the computers.
D. Run the System File Checker.

Correct Answer: D
Section:
Explanation:
The technician should run the System File Checker (SFC) first to correct file corruption errors on computers after a power outage. SFC is a command-line utility that scans for and repairs corrupted system files. It can be run from the command prompt or from the Windows Recovery Environment. Rebuilding the Windows profiles, restoring the computers from backup, and reimaging the computers are more drastic measures that should be taken only if SFC fails to correct the issue1

QUESTION 285
A user is unable to access a website, which is widely used across the organization, and receives the following error message:

The security certificate presented by this website has expired or is not yet valid.
The technician confirms the website works when accessing it from another computer but not from the user's computer. Which of the following should the technician perform NEXT to troubleshoot the issue?

A. Reboot the computer.
B. Reinstall the OS.
C. Configure a static 12
D. Check the computer's date and time.

Correct Answer: D
Section:
Explanation:
The error message indicates that the security certificate presented by the website has either expired or is not yet valid. This can happen if the computer's clock has the wrong date or time, as SSL/TLS certificates have a specific validity period. If the clock is off by too much, it may cause the certificate to fail to validate. Therefore, the technician should check the computer's date and time and ensure that they are correct.

QUESTION 286
A company has just refreshed several desktop PCs. The hard drives contain PII. Which of the following is the BEST method to dispose of the drives?

A. Drilling
B. Degaussing
C. Low-level formatting
D. Erasing/wiping

Correct Answer: D
Section:
Explanation:
Erasing/wiping the hard drives is the best method to dispose of the drives containing PII

QUESTION 287
After a company installed a new SOHO router customers were unable to access the company-hosted public website. Which of the following will MOST likely allow customers to access the website?

A. Port forwarding
B. Firmware updates
C. IP filtering
D. Content filtering

Correct Answer: B
Section:
Explanation:
If customers are unable to access the company-hosted public website after installing a new SOHO router, the company should check for firmware updates1. Firmware updates can fix bugs and compatibility issues that may be preventing customers from accessing the website1. The company should also ensure that the router is properly configured to allow traffic to the website1. If the router is blocking traffic to the website, the company should configure the router to allow traffic to the website1.

QUESTION 288
A new spam gateway was recently deployed at a small business However; users still occasionally receive spam. The management team is concerned that users will open the messages and potentially infect the network systems. Which of the following is the MOST effective method for dealing with this Issue?

A. Adjusting the spam gateway
B. Updating firmware for the spam appliance

C. Adjusting AV settings
D. Providing user training

Correct Answer: D
Section:
Explanation:
The most effective method for dealing with spam messages in a small business is to provide user training1. Users should be trained to recognize spam messages and avoid opening them1. They should also be trained to report spam messages to the IT department so that appropriate action can be taken1. In addition, users should be trained to avoid clicking on links or downloading attachments from unknown sources1. By providing user training, the management team can reduce the risk of users opening spam messages and potentially infecting the network systems1.

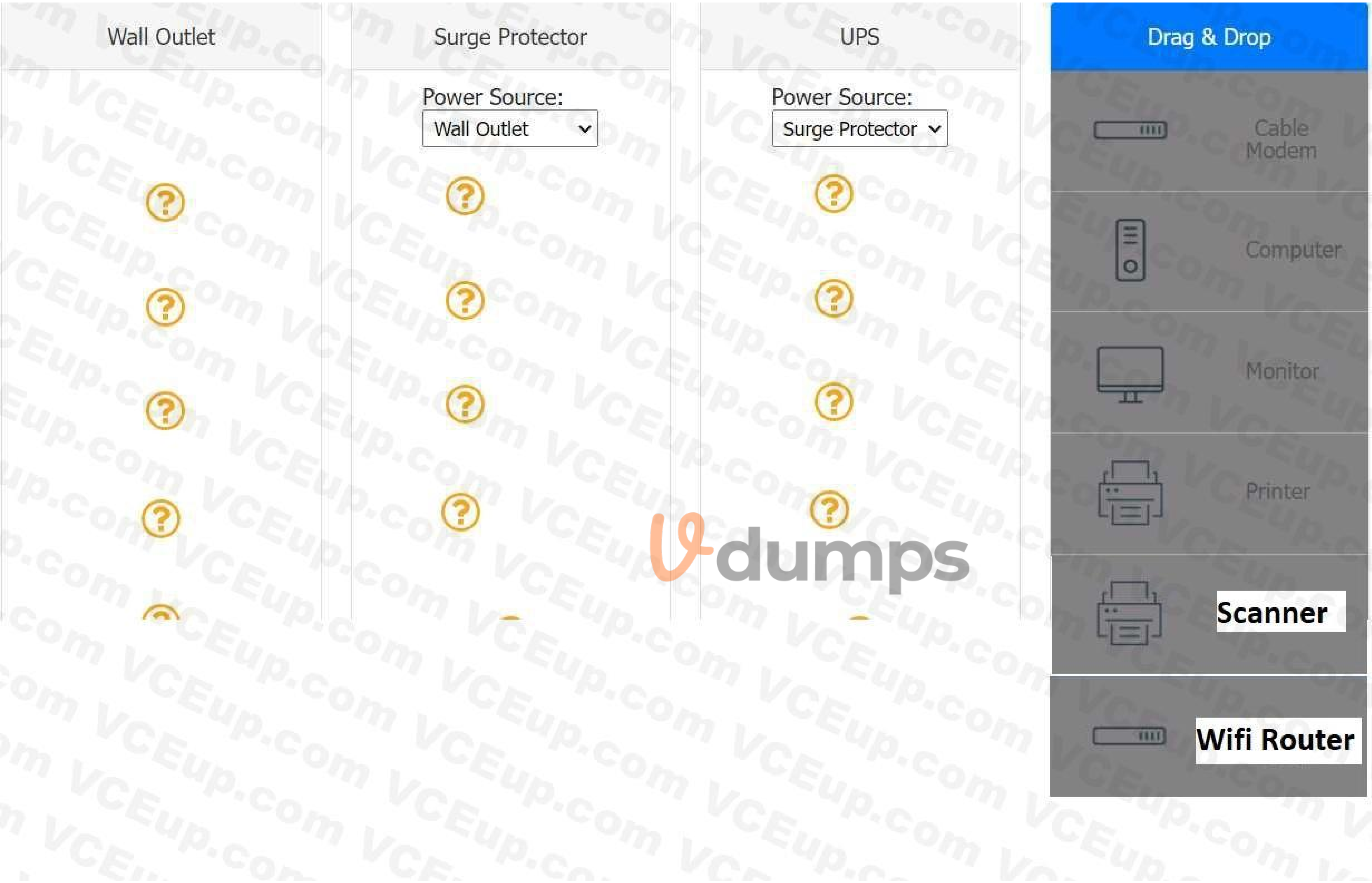
QUESTION 289
A user reports a PC is running slowly. The technician suspects high disk I/O. Which of the following should the technician perform NEXT?

A. resmon_exe
B. dfrgui_exe
C. msinf032exe
D. msconfig_exe

Correct Answer: A
Section:
Explanation:
If a technician suspects high disk I/O, the technician should use the Resource Monitor (resmon.exe) to identify the process that is causing the high disk I/O1. Resource Monitor provides detailed information about the system's resource usage, including disk I/O1. The technician can use this information to identify the process that is causing the high disk I/O and take appropriate action1.

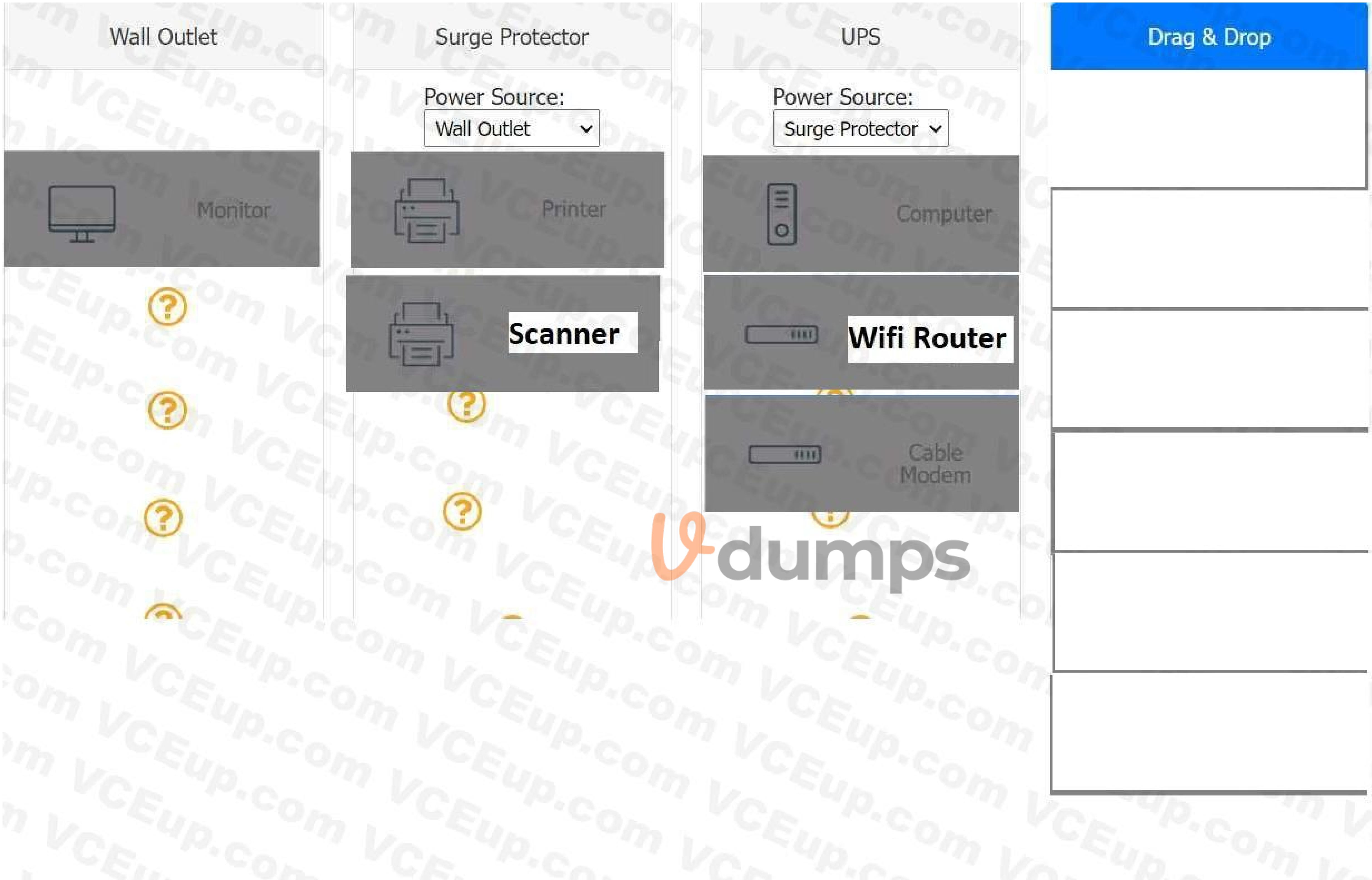
QUESTION 290
DRAG DROP
A customer recently experienced a power outage at a SOHO. The customer does not think the components are connected properly. A print job continued running for several minutes after the power failed, but the customer was not able to interact with the computer. Once the UPS stopped 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.

Select and Place:



Wall Outlet	Surge Protector	UPS
	Power Source: Wall Outlet	Power Source: Surge Protector

Correct Answer:



Section:
Explanation:

QUESTION 291
During a network outage, a technician discovers a new network switch that was not listed in the support documentation. The switch was installed during a recent change window when a new office was added to the environment. Which of the following would most likely prevent this type of mismatch after next month's change window?

A. Performing annual network topology reviews
B. Requiring all network changes include updating the network diagrams

C. Allowing network changes once per year
D. Routinely backing up switch configuration files

Correct Answer: B
Section:

QUESTION 292
A technician is in the process of installing a new hard drive on a server but is called away to another task. The drive has been unpackaged and left on a desk. Which of the following should the technician perform before leaving?

A. Ask coworkers to make sure no one touches the hard drive.
B. Leave the hard drive on the table; it will be okay while the other task is completed.
C. Place the hard drive in an antistatic bag and secure the area containing the hard drive.
D. Connect an electrostatic discharge strap to the drive.

Correct Answer: C
Section:
Explanation:
The technician should place the hard drive in an antistatic bag and secure the area containing the hard drive before leaving. This will protect the hard drive from electrostatic discharge (ESD), dust, moisture, and physical damage. Asking coworkers to make sure no one touches the hard drive is not a reliable or secure way to prevent damage. Leaving the hard drive on the table exposes it to ESD and other environmental hazards. Connecting an electrostatic discharge strap to the drive is not enough to protect it from dust, moisture, and physical damage.

QUESTION 293
A technician installed Windows 10 on a workstation. The workstation only has 3.5GB of usable RAM, even though the technician installed 8GB. Which of the following is the MOST likely reason this system is not utilizing all the available RAM?

A. The system is missing updates.
B. The systems utilizing a 32-bit OS.
C. The system's memory is failing.
D. The system requires BIOS updates.

Correct Answer: B
Section:
Explanation:
The most likely reason that the system is not utilizing all the available RAM is that it is running a 32- bit OS. A 32-bit OS can only address up to 4GB of RAM, and some of that is reserved for hardware and system use1. Therefore, even if the technician installed 8GB of RAM, the system can only use around 3.5GB of usable RAM. To use the full 8GB of RAM, the technician would need to install a 64- bit OS, which can address much more memory2. The system missing updates, the system’s memory failing, or the system requiring BIOS updates are not likely to cause this issue.
Reference: 2: https://support.microsoft.com/en-us/windows/windows-10-system-requirements- 6d4e9a79-66bf-7950-467c-795cf0386715 1: https://www.makeuseof.com/tag/unlock-64gb-ram-32- bit-windows-pae-patch/

QUESTION 294
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.

Correct Answer: D
Section:
Explanation:
The technician should perform a rollback of the Windows update that caused the issue with the locally attached devices. A rollback is a process of uninstalling an update and restoring the previous version of the system. This can help to fix any compatibility or performance issues caused by the update1. To rollback an update, the technician can use the Settings app, the Control Panel, or the System Restore feature. The technician should also check for any device driver updates that might be needed after rolling back the update. Disabling the Windows Update service is not a good practice, as it can prevent the system from receiving important security and feature updates. Checking for updates might not fix the issue, as the update that caused the issue might still be installed. Restoring hidden updates is not relevant, as it only applies to updates that have been hidden by the user to prevent them from being installed2.
Reference: 1: https://www.windowscentral.com/how-uninstall-and-reinstall-updates-windows-10 2:
https://support.microsoft.com/en-us/windows/show-or-hide-updates-in-windows-10-9c9f0a4f- 9a6e-4c8e-8b44-afbc6b33f3cf

QUESTION 295
A macOS user is installing a new application. Which of the following system directories is the software MOST likely to install by default?

A. /etc/services
B. /Applications
C. /usr/bin
D. C:\Program Files

Correct Answer: B
Section:
Explanation:
The software is most likely to install by default in the /Applications directory, which is the standard location for macOS applications. This directory can be accessed from the Finder sidebar or by choosing Go &gt; Applications from the menu bar. The /Applications directory contains all the applications that are available to all users on the system1. Some applications might also offer the option to install in the ~/Applications directory, which is a personal applications folder for a single user2. The /etc/services directory is a system configuration file that maps service names to port numbers and protocols3. The /usr/bin directory is a system directory that contains executable binaries for various commands and utilities4. The C:\Program Files directory is a Windows directory that does not exist on macOS.

QUESTION 296
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.

Correct Answer: B
Section:
Explanation:
The user can change the wallpaper using a Windows 10 Settings tool by following these steps12:
Open Settings by pressing the Windows key and typing Settings, or by clicking the gear icon in the Start menu.
Select Personalization from the left navigation menu.
On the right side of the window, click Background.
In the Background settings, click the drop-down menu and select Picture as the background type. Click Browse and then locate and open the image the user wants to use as the wallpaper. The other options are incorrect because they do not lead to the Background settings or they do not allow the user to browse for an image. Accounts, System, and Apps are not related to personalization settings. Your info, Display, and Apps & features are not related to wallpaper settings.
Reference: 1: https://support.microsoft.com/en-us/windows/change-your-desktop-background- image-175618be-4cf1-c159-2785-ec2238b433a8 2:
https://www.computerhope.com/issues/ch000592.htm

QUESTION 297

Which of the following default system tools can be used in macOS to allow the technician to view the screen simultaneously with the user?

A. Remote Assistance
B. Remote Desktop Protocol
C. Screen Sharing
D. Virtual Network Computing

Correct Answer: C
Section:
Explanation:
Screen Sharing is the default system tool that can be used in macOS to allow the technician to view the screen simultaneously with the user. Screen Sharing is a built-in app that lets users share their Mac screen with another Mac on the network. The user can enable screen sharing in the System Preferences &gt; Sharing pane, and then allow other users to request or enter a password to access their screen1. The technician can launch the Screen Sharing app from the Spotlight search or the Finder sidebar, and then enter the user's name, address, or Apple ID to connect to their screen2. Remote Assistance is a Windows feature that allows users to invite someone to help them with a problem on their PC3. Remote Desktop Protocol (RDP) is a protocol that allows users to connect to a remote computer over a network4. Virtual Network Computing (VNC) is a technology that allows users to share their screen with other devices using a VNC viewer app1. These are not default system tools in macOS, although they can be used with third-party software or settings.
Reference: 1: https://support.apple.com/guide/mac-help/share-the-screen-of-another-macmh14066/mac 2: https://www.howtogeek.com/449239/how-to-share-your-macs-screen-withanother-mac/ 3: https://support.microsoft.com/en-us/windows/solve-pc-problems-over-a-remoteconnection-b077e31a-16f4-2529-1a47-21f6a9040bf3 4: https://docs.microsoft.com/en-us/windowsserver/remote/remote-desktop-services/clients/remote-desktop-protocol

QUESTION 298
A user's corporate laptop with proprietary work Information was stolen from a coffee shop. The user togged in to the laptop with a simple password. and no other security mechanisms were in place.
Which of the following would MOST likely prevent the stored data from being recovered?

A. Biometrics
B. Full disk encryption
C. Enforced strong system password
D. Two-factor authentication

Correct Answer: B
Section:
Explanation:

QUESTION 299
An administrator's change was approved by the change management review board. Which of the following should the administrator do next?

A. Perform risk analysis.
B. Assign a change coordinator.
C. Implement the change.
D. Verify testing results.

Correct Answer: C
Section:
Explanation:
Once a change has been approved by the change management review board, the next step is to:
Implement the change: This involves carrying out the approved change in the system or environment according to the change plan.
Perform risk analysis: This should be done before the change is approved to assess potential impacts.
Assign a change coordinator: This role should be designated earlier in the process to oversee the change implementation.

Verify testing results: This should have been done before seeking approval from the review board.
CompTIA A+ 220-1102 Exam Objectives, Section 4.2: Explain basic change-management best practices.
Change management process documentation.

QUESTION 300
When a user is in the office, web pages are loading slowly on the user's phone. Which of the following best explains this issue?

A. Exceeded the data usage limit
B. Sluggish response time
C. Degraded network service
D. High network traffic

Correct Answer: D
Section:
Explanation:
When a user experiences slow web page loading on their phone while in the office, the most likely cause is:
High network traffic: In an office environment, many devices are often connected to the network simultaneously, which can lead to congestion and slow internet speeds. High network traffic means more devices are competing for the same bandwidth, causing delays.
Exceeded the data usage limit: This typically applies to cellular data plans, not Wi-Fi in an office setting.
Sluggish response time: This is a symptom rather than a cause and can result from high network traffic.
Degraded network service: While this could be a factor, it is broader and less specific than high network traffic, which is more directly related to the user's experience.
CompTIA A+ 220-1102 Exam Objectives, Section 2.7: Given a scenario troubleshoot problems with wired and wireless networks.
Network performance troubleshooting documentation.

QUESTION 301
A customer needs to purchase a desktop capable of rendering video. Which of the following should the customer prioritize?

A. NIC
B. USB
C. GPU
D. HDMI

Correct Answer: C
Section:
Explanation:
For rendering video, the most critical component a customer should prioritize in a desktop is:
GPU (Graphics Processing Unit): The GPU is specifically designed to handle complex graphics and video rendering tasks. A powerful GPU will significantly improve performance in video rendering applications.
NIC (Network Interface Card): Important for network connectivity but irrelevant for video rendering.
USB: Useful for peripherals but does not impact video rendering capabilities.
HDMI: An important output interface for connecting monitors but not crucial for the rendering process itself.
CompTIA A+ 220-1102 Exam Objectives, Section 1.8: Explain common OS types and their purposes, including hardware components for specific tasks.
GPU importance in video rendering documentation.

QUESTION 302
Users report that a network printer intermittently goes offline during the day. Which of the following commands should the technician use to confirm whether the printer has connectivity issues?

A. ping
B. netstat

C. net
D. nslookup

Correct Answer: A
Section:
Explanation:
To confirm whether a network printer has connectivity issues, the technician should use:
ping: This command checks the connectivity to the printer by sending packets and measuring the response time. It helps determine if the printer is reachable on the network.
netstat: Provides statistics and current network connections but does not directly confirm connectivity to a specific device.
net: Used for network resources management but not specifically for checking connectivity.
nslookup: Used for querying DNS to obtain domain name or IP address mapping, not for checking connectivity.
CompTIA A+ 220-1102 Exam Objectives, Section 2.8: Given a scenario, use networking tools.
Network troubleshooting commands documentation.

QUESTION 303
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.

Correct Answer: A
Section:
Explanation:
When a user reports slow performance, a changed home page, and pop-up ads, these are classic signs of malware infection. The first step should be:
Update the antivirus program and run a full system scan: This helps identify and remove any malware present on the system, addressing the root cause of the issues.
Uninstall the suspicious search engine and reset the home page: This addresses the symptom but not the underlying cause, which is likely malware.
Install the latest updates for the operating system: Important for security but secondary to removing malware.
Block the pop-up ads using the web browser settings: Again, addresses the symptom but not the root cause.
CompTIA A+ 220-1102 Exam Objectives, Section 3.3: Given a scenario use best practice procedures for malware removal.
Malware identification and removal documentation.

QUESTION 304
A user is attempting to access a shared drive from a company-issued laptop while working from home. The user is unable to access any files and notices a red X next to each shared drive. Which of the following needs to be configured in order to restore the user's access to the shared drives?

A. IPv6
B. VPN
C. IPS
D. DNS

Correct Answer: B
Section:

Explanation:
When a user is unable to access shared drives from a company-issued laptop while working from home, the likely requirement is:
VPN (Virtual Private Network): A VPN allows secure access to the company's network from a remote location. Without a VPN connection, the user cannot access network resources such as shared drives.
IPv6: Involves IP addressing and is not directly related to accessing shared drives.
IPS (Intrusion Prevention System): Provides network security but does not facilitate access to shared drives.
DNS: Manages domain name resolution and is not typically the issue when specific shared drives are inaccessible.
CompTIA A+ 220-1102 Exam Objectives, Section 2.7: Explain common methods for securing mobile and embedded devices.
VPN configuration and remote access documentation.