CompTIA

Exam Questions 220-1102

CompTIA A+ Certification Exam: Core 2

NEW QUESTION 1
An employee has repeatedly contacted a technician about malware infecting a work computer. The technician has removed the malware several times, but the user's PC keeps getting infected. Which of the following should the technician do to reduce the risk of future infections?

A. Configure the firewall.
B. Restore the system from backups.
C. Educate the end user
D. Update the antivirus program.

Answer: C

Explanation:
Malware is software that infects computer systems to damage, disable or exploit the computer or network for various malicious purposes5. Malware is typically distributed via email attachments, fake internet ads, infected applications or websites, and often relies on user interaction to execute6. Therefore, one of the most effective ways to prevent malware infections is to educate the end user about the common signs and sources of malware, and how to avoid them7. Configuring the firewall, restoring the system from backups, and updating the antivirus program are also important security measures, but they do not address the root cause of the user's repeated infections, which is likely due to a lack of awareness or caution.
References5: Malware: what it is, how it works, and how to stop it - Norton6: How to Prevent Malware: 15 Best Practices for Malware Prevention7: 10 Security Tips for How to Prevent Malware Infections - Netwrix

NEW QUESTION 2
A company recently experienced a security incident in which a USB drive containing malicious software was able to covertly install malware on a workstation. Which of the following actions should be taken to prevent this incident from happening again? (Select two).

A. Install a host-based IDS.
B. Restrict log-in times.
C. Enable a BIOS password.
D. Update the password complexity.
E. Disable AutoRun.
F. Update the antivirus definitions.
G. Restrict user permissions.

Answer: EG

Explanation:
AutoRun is a feature of Windows that automatically executes a program or file when a removable media such as a USB drive is inserted into the computer. Disabling AutoRun can prevent a USB drive containing malicious software from covertly installing malware on a workstation, as it would require the user to manually open the drive and run the file. Restricting user permissions can also prevent a USB drive containing malicious software from covertly installing malware on a workstation, as it would limit the user's ability to execute or install unauthorized programs or files. Installing a host-based IDS, restricting log-in times, enabling a BIOS password, updating the password complexity, and updating the antivirus definitions are not actions that can directly prevent this incident from happening again.

NEW QUESTION 3
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

Answer: C

Explanation:
Incremental backup is a backup method that only backs up the files that have changed since the last backup, whether it was a full or an incremental backup. Incremental backup can save storage space and bandwidth, as it does not copy the same files over and over again. Incremental backup can also retain more versions of backups, as it only stores the changes made to the files. However, incremental backup can have longer restore times, as it requires restoring the last full backup and all the subsequent incremental backups in order to recover the data. The law firm is not concerned about restore times but asks the technician to retain more versions when possible, so incremental backup would be a suitable choice for them.

NEW QUESTION 4
A customer installed a new web browser from an unsolicited USB drive that the customer received in the mail. The browser is not working as expected, and internet searches are redirected to another site. Which of the following should the user do next after uninstalling the browser?

A. Delete the browser cookies and history.
B. Reset all browser settings.
C. Change the browser default search engine.
D. Install a trusted browser.

Answer: D

Explanation:
The customer's web browser is likely infected by a browser hijacker, which is a type of malware that changes the browser's settings and redirects the user to malicious websites. A browser hijacker can also steal the user's personal data, display unwanted ads, and install more malware on the device. To remove a browser hijacker, the user should first uninstall the browser

from the Control Panel, then scan the device with an antivirus or anti-malware program, and finally install a trusted browser from a legitimate source. Deleting the browser cookies and history, resetting the browser settings, or changing the browser default search engine may not be enough to get rid of the browser hijacker, as it may have embedded itself into the system or other browser components.

NEW QUESTION 5
A technician installs specialized software on a workstation. The technician then attempts to run the software. The workstation displays a message indicating the software is not authorized to run. Which of the following should the technician do to most likely resolve the issue?

A. Install the software in safe mode.
B. Attach the external hardware token.
C. Install OS updates.
D. Restart the workstation after installation.

Answer: B

Explanation:
A hardware token is a physical device that provides an additional layer of security for software authorization. Some specialized software may require a hardware token to be attached to the workstation in order to run. A hardware token may contain a cryptographic key, a password, or a one-time code that verifies the user's identity or permission. Installing the software in safe mode, installing OS updates, and restarting the workstation after installation are not likely to resolve the issue of software authorization.

NEW QUESTION 6
A technician is preparing to remediate a Trojan virus that was found on a workstation. Which of the following steps should the technician complete BEFORE removing the virus?

A. Disable System Restore.
B. Schedule a malware scan.
C. Educate the end user.
D. Run Windows Update.

Answer: A

Explanation:
Before removing a Trojan virus from a workstation, a technician should disable System Restore. System Restore is a feature that allows users to restore their system to a previous state in case of problems or errors. However, System Restore can also restore infected files or registry entries that were removed by antivirus software or manual actions. By disabling System Restore, a technician can ensure that the Trojan virus is completely removed and does not reappear after a system restore operation. Scheduling a malware scan may help detect and remove some malware but may not be effective against all types of Trojan viruses. Educating the end user may help prevent future infections but does not address the current issue of removing the Trojan virus. Running Windows Update may help patch some security vulnerabilities but does not guarantee that the Trojan virus will be removed. References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.3

NEW QUESTION 7
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.

Answer: B

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 References: https://www.comptia.org/blog/how-to- remove-a-virus https://www.comptia.org/certifications/a

NEW QUESTION 8
A remote user is experiencing issues connecting to a corporate email account on a laptop. The user clicks the internet connection icon and does not recognize the connected Wi-Fi. The help desk technician, who is troubleshooting the issue, assumes this is a rogue access point. Which of the following is the first action the technician should take?

A. Restart the wireless adapter.
B. Launch the browser to see if it redirects to an unknown site.
C. Instruct the user to disconnect the Wi-Fi.
D. Instruct the user to run the installed antivirus software.

Answer: C

Explanation:
Instructing the user to disconnect the Wi-Fi is the first action the technician should take if they suspect a rogue access point. A rogue access point is an unauthorized wireless network that could be used to intercept or manipulate network traffic, compromise security, or launch attacks. Disconnecting the Wi-Fi would prevent further exposure or damage to the user's device or data. Restarting the wireless adapter, launching the browser, or running the antivirus software are possible actions to take after disconnecting the Wi-Fi, but they are not as urgent or effective as the first step. References:
? Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 22
? CompTIA A+ Core 1 (220-1101) and Core 2 (220-1102) Cert Guide, page 456

NEW QUESTION 9
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

Answer: D

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.

NEW QUESTION 10
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

Answer: D

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.

NEW QUESTION 10
A technician needs to track evidence for a forensic investigation on a Windows computer. Which of the following describes this process?

A. Valid license
B. Data retention requirements
C. Material safety data sheet
D. Chain of custody

Answer: D

Explanation:
Chain of custody is a legal term that refers to the chronological documentation or paper trail that records the sequence of custody, control, transfer, analysis, and disposition of materials, including physical or electronic evidence1. It is important in forensic investigations to establish that the evidence is in fact related to the case, and that it has not been tampered with or contaminated. A technician needs to track evidence for a forensic investigation on a Windows computer by following the proper procedures for collecting, handling, storing, and analyzing the evidence, and documenting every step of the process on a chain of custody form23

NEW QUESTION 14
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.

Answer: D

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.

NEW QUESTION 19
A technician is investigating options to secure a small office's wireless network. One requirement is to allow automatic log-ins to the network using certificates instead of passwords. Which of the following should the wireless solution have in order to support this feature?

A. RADIUS
B. AES
C. EAP-EKE
D. MFA

Answer: A

Explanation:
RADIUS is the correct answer for this question. RADIUS stands for Remote Authentication Dial-In User Service, and it is a protocol that provides centralized authentication, authorization, and accounting for wireless networks. RADIUS can support certificate-based authentication, which allows users to log in to the network automatically without entering passwords. RADIUS also provides other benefits, such as enforcing security policies, logging user activities, and managing network access. AES, EAP-EKE, and MFA are not wireless solutions, but rather encryption algorithms, authentication methods, and security factors, respectively.
References:
? Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 23
? CompTIA A+ Core 1 (220-1101) and Core 2 (220-1102) Cert Guide, page 459

NEW QUESTION 23
Which of the following is the most likely reason a filtration system is critical for data centers?

A. Plastics degrade over time.
B. High humidity levels can rust metal.
C. Insects can invade the data center.
D. Dust particles can clog the machines.

Answer: B

Explanation:
A filtration system is critical for data centers because it can control the humidity and temperature levels in the environment. High humidity levels can cause condensation and corrosion on the metal components of the servers and other equipment, leading to malfunction and damage. A filtration system can also prevent dust, dirt, and other contaminants from entering the data center and clogging the machines or causing overheating.

NEW QUESTION 24
Which of the following macOS features can help a user close an application that has stopped responding?

A. Finder
B. Mission Control
C. System Preferences
D. Force Quit

Answer: D

Explanation:
The correct answer is D. Force Quit. Force Quit is a macOS feature that allows users to close an application that has stopped responding. To use Force Quit, users can press and hold Option (or Alt), Command, and Esc (Escape) keys together, or choose Force Quit from the Apple menu in the corner of the screen. A Force Quit window will open, where users can select the application that they want to close and click Force Quit123.
References and Explanation
? The web search results provide information about how to force an app to quit on
Mac using different methods, such as keyboard shortcuts, mouse clicks, or menu options. The results also explain what to do if the app cannot be forced to quit or if the Mac does not respond.
? The first result1 is from the official Apple Support website and provides detailed
instructions and screenshots on how to force an app to quit on Mac using the keyboard shortcut or the Apple menu. It also explains how to force quit the Finder app and how to restart or turn off the Mac if needed.
? The second result2 is from the same website but for a different region (UK). It has
the same content as the first result but with some minor differences in spelling and wording.
? The third result4 is from a website called Lifehacker that provides tips and tricks for
various topics, including technology. It compares how to close a program that is not responding on different operating systems, such as Windows, Mac, and Linux. It briefly mentions how to force quit an app on Mac using the keyboard shortcut or the mouse click.
? The fourth result3 is from a website called Parallels that provides software
solutions for running Windows on Mac. It focuses on how to force quit an app on Mac using the keyboard shortcut and provides a video tutorial and a screenshot on how to do it. It also suggests some alternative ways to close an app that is not responding, such as using Activity Monitor or Terminal commands.

NEW QUESTION 27
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

Answer: C

Explanation:
Since there are no error messages on the device, the technician should check if the battery is sufficiently charge1d
If the battery is low, the device may not have enough power to complete the update2
In 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.

NEW QUESTION 30
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

Answer: C

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.

NEW QUESTION 32
Which of the following features allows a technician to configure policies in a Windows 10 Professional desktop?

A. gpedit
B. gpmc
C. gpresult
D. gpupdate

Answer: A

Explanation:
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.
References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.6

NEW QUESTION 36
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.

Answer: C

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

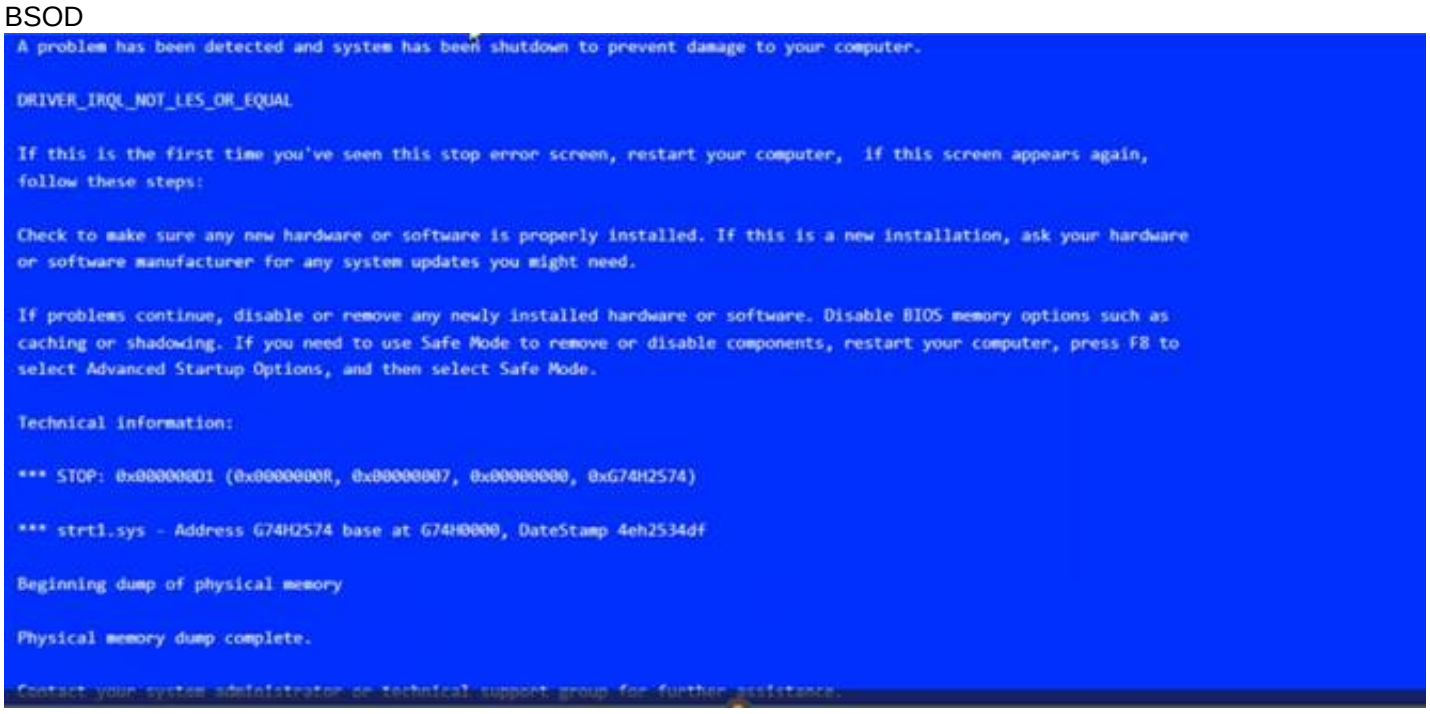
NEW QUESTION 41
A user has requested help setting up the fingerprint reader on a Windows 10 laptop. The laptop is equipped with a fingerprint reader and is joined to a domain Group Policy enables Windows Hello on all computers in the environment. Which of the following options describes how to set up 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.

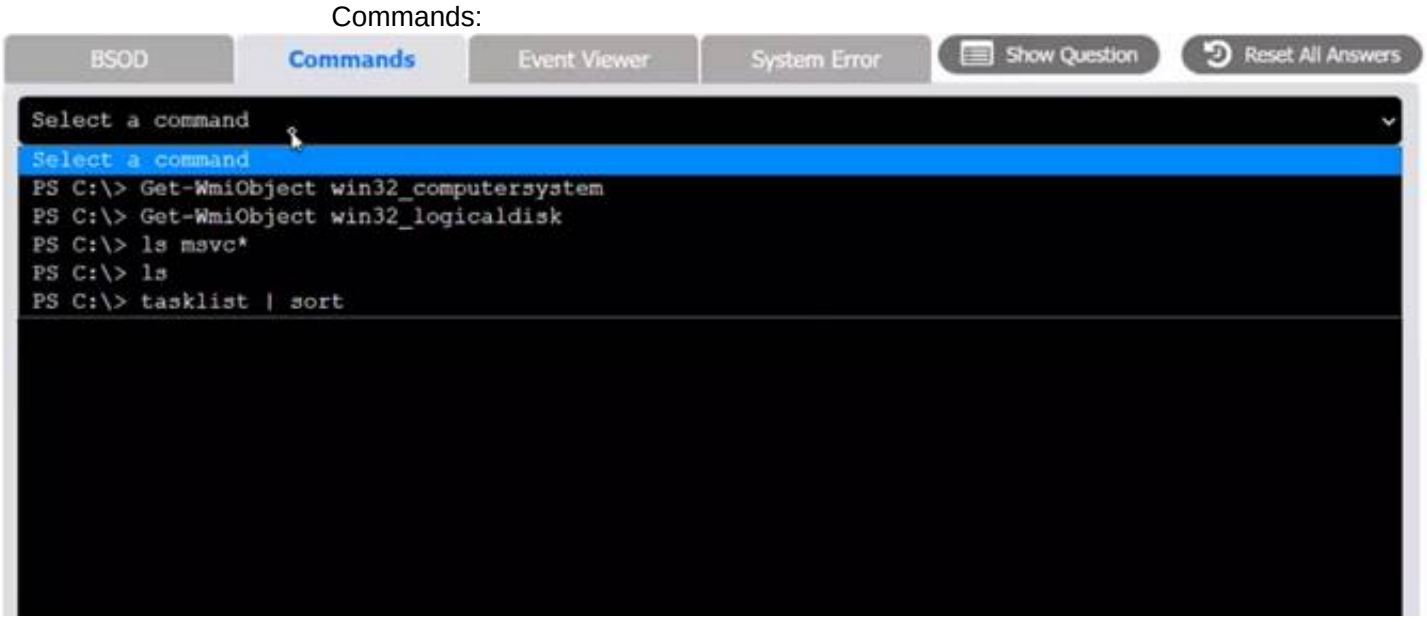
Answer: B

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.

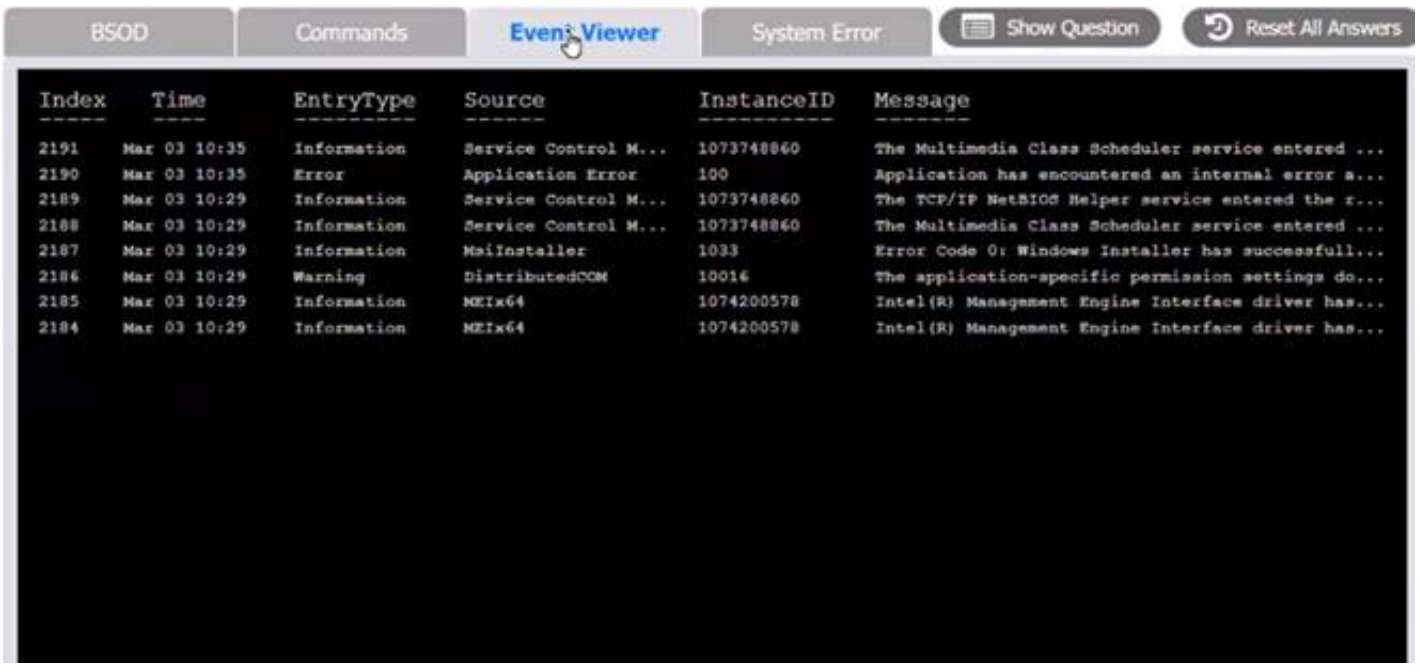
NEW QUESTION 43
SIMULATION
A user reports that after a recent software deployment to upgrade applications, the user can no longer use the Testing program. However, other employees can successfully use the Testing program.
INSTRUCTIONS
Review the information in each tab to verify the results of the deployment and resolve any issues discovered by selecting the:
? Index number of the Event Viewer issue
? First command to resolve the issue
? Second command to resolve the issue
BSOD



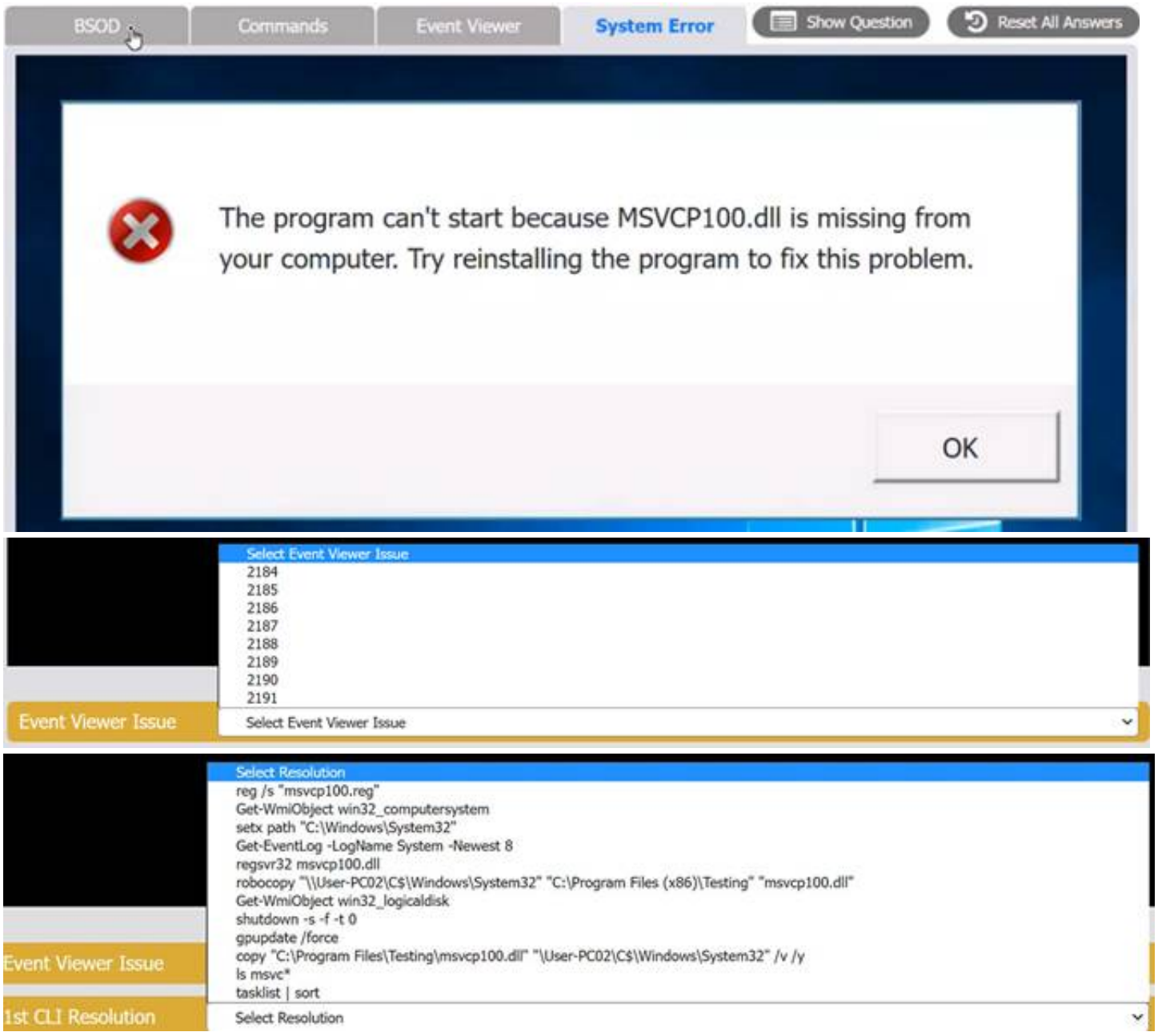
Commands:



Event Viewer:



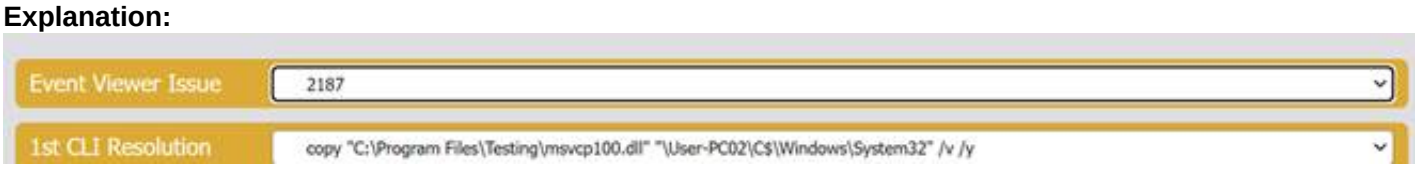
System Error:



A. Mastered
B. Not Mastered

Answer: A

Explanation:



The user is experiencing a system error that prevents them from using the Testing program. The error message indicates that the file MSVCP100.dll is missing from the computer. This file is part of the Microsoft Visual C++ 2010 Redistributable Package, which is required by some applications to run properly. The error may have occurred due to a corrupted or incomplete software deployment.
To resolve this issue, the user needs to restore the missing file and register it in the system. One possible way to do this is to copy the file from another computer that has the

Testing program installed and working, and then use the regsvr32 command to register it. The steps are as follows:
? On another computer (User-PC02) that has the Testing program installed and working, locate the file MSVCP100.dll in the folder C:\Program Files\Testing.
? Share the folder C:\Windows\System32 on User-PC02 by right-clicking on it, selecting Properties, then Sharing, then Advanced Sharing, then checking Share this folder, then clicking OK.
? On the user's computer (User-PC01), open a command prompt as an administrator by clicking Start, typing cmd, right-clicking on Command Prompt, and selecting Run as administrator.
? In the command prompt, type the following command to copy the file MSVCP100.dll from User-PC02 to User-PC01: copy "C:\Program Files\Testing\msvcp100.dll" "\\User-PC02\C$\Windows\System32"
? After the file is copied, type the following command to register it in the system: regsvr32 msvcp100.dll
? Restart the user's computer and try to run the Testing program again. Therefore, based on the instructions given by the user, the correct answers are: Select Event Viewer Issue: 2187
Select First Command: copy "C:\Program Files\Testing\msvcp100.dll" "\\User- PC02\C$\Windows\System32"
Select Second Command: regsvr32 msvcp100.dll

NEW QUESTION 45
A user's mobile phone has become sluggish A systems administrator discovered several malicious applications on the device and reset the phone. The administrator installed MDM software. Which of the following should the administrator do to help secure the device against this threat in the future? (Select TWO).

A. Prevent a device root
B. Disable biometric authentication
C. Require a PIN on the unlock screen
D. Enable developer mode
E. Block a third-party application installation
F. Prevent GPS spoofing

Answer: CE

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.

NEW QUESTION 47
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

Answer: A

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.

NEW QUESTION 51
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

Answer: D

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.

NEW QUESTION 53
Which of the following should be documented to ensure that the change management plan is followed?

A. Scope of the change
B. Purpose of the change
C. Change rollback plan
D. Change risk analysis

Answer: A

Explanation:
The scope of the change is one of the elements that should be documented to ensure that the change management plan is followed. The scope of the change defines the boundaries and limitations of the change, such as what is included and excluded, what are the deliverables and outcomes, what are the assumptions and constraints, and what are the dependencies and risks. The scope of the change helps to clarify the expectations and objectives of the change, as well as to prevent scope creep or deviation from the original plan. The scope of the change also helps to measure the progress and success of the change, as well as to communicate the change to the stakeholders and the team

NEW QUESTION 55
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.

Answer: D

Explanation:
The first step in removing a virus from a computer is to update the antivirus software with the latest virus definitions. Virus definitions are files that contain information about the characteristics and behavior of known viruses and malware. They help the antivirus software to identify and remove the malicious threats from the computer. Without the latest virus definitions, the antivirus software may not be able to detect or remove the virus that infected the user's computer. Therefore, the technician should download the latest virus definitions from the antivirus vendor's website or use the update feature in the antivirus program before scanning the computer for viruses.
References:
? How to remove malware or viruses from my Windows 10 PC, section 21
? How to Remove a Virus From a Computer in 2023, section 32
? The Official CompTIA A+ Core 2 Study Guide (220-1102), page 2193

NEW QUESTION 59
A technician suspects a rootkit has been installed and needs to be removed. Which of the following would BEST resolve the issue?

A. Mastered
B. Not Mastered

Answer: A

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 system
https://www.minitool.com/backup-tips/how-to-get-rid-of-rootkit-windows-10.html

NEW QUESTION 60
A user's corporate phone was stolen, and the device contains company trade secrets. Which of the following technologies should be implemented to mitigate this risk? (Select TWO).

A. Remote wipe
B. Firewall
C. Device encryption
D. Remote backup
E. Antivirus
F. Global Positioning System

Answer: AC

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.
References: 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)

NEW QUESTION 63
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

Answer: C

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

NEW QUESTION 66
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

Answer: D

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 the speech
recognition feature. Personalization settings can be used to customize the appearance and behavior of the PC, but they will not enable the speech recognition feature1
Open up ease of access, click on speech, then there is an on and off button for speech recognition.

NEW QUESTION 68
A user reports an issue when connecting a mobile device to Bluetooth. The user states the mobile device's Bluetooth is turned on. Which of the following steps should the technician take NEXT to resolve the issue?

A. Restart the mobile device.
B. Turn on airplane mode.
C. Check that the accessory is ready to pair.
D. Clear all devices from the phone's Bluetooth settings.

Answer: C

Explanation:
The first step in troubleshooting a Bluetooth connection issue is to check that the accessory is ready to pair with the mobile device. Some accessories may have a button or a switch that needs to be pressed or turned on to initiate pairing mode. If the accessory is not ready to pair, the mobile device will not be able to detect it.
Reference: CompTIA A+ Core 2 Exam Objectives, Section 2.4

NEW QUESTION 69
A company is experiencing a ODDS 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. Ransomvvare
F. Spyware

Answer: AD

Explanation:
The correct answers are A and D. Zombies and botnets are types of infections that allow malicious actors to remotely control infected computers and use them to launch distributed denial-of-service (DDoS) attacks against a target. A DDoS attack is a type of cyberattack that aims to overwhelm a server or a network with a large volume of traffic from multiple sources, causing it to slow down or crash.
A keylogger is a type of malware that records the keystrokes of a user and sends them to a remote server, often for the purpose of stealing passwords, credit card numbers, or other sensitive information.
Adware is a type of software that displays unwanted advertisements on a user's computer, often in the form of pop-ups, banners, or redirects. Adware can also collect user data and compromise the security and performance of the system.
Ransomware is a type of malware that encrypts the files or locks the screen of a user's computer and demands a ransom for their restoration. Ransomware can also threaten to delete or expose the user's data if the ransom is not paid.
Spyware is a type of software that covertly monitors and collects information about a user's online activities, such as browsing history, search queries, or personal data. Spyware can also alter the settings or functionality of the user's system without their consent.

NEW QUESTION 73
A technician downloaded software from the Internet that required the technician to scroll through a text box and at the end of the text box, click a button labeled Accept Which of the following agreements IS MOST likely in use?

A. Mastered
B. Not Mastered

Answer: A

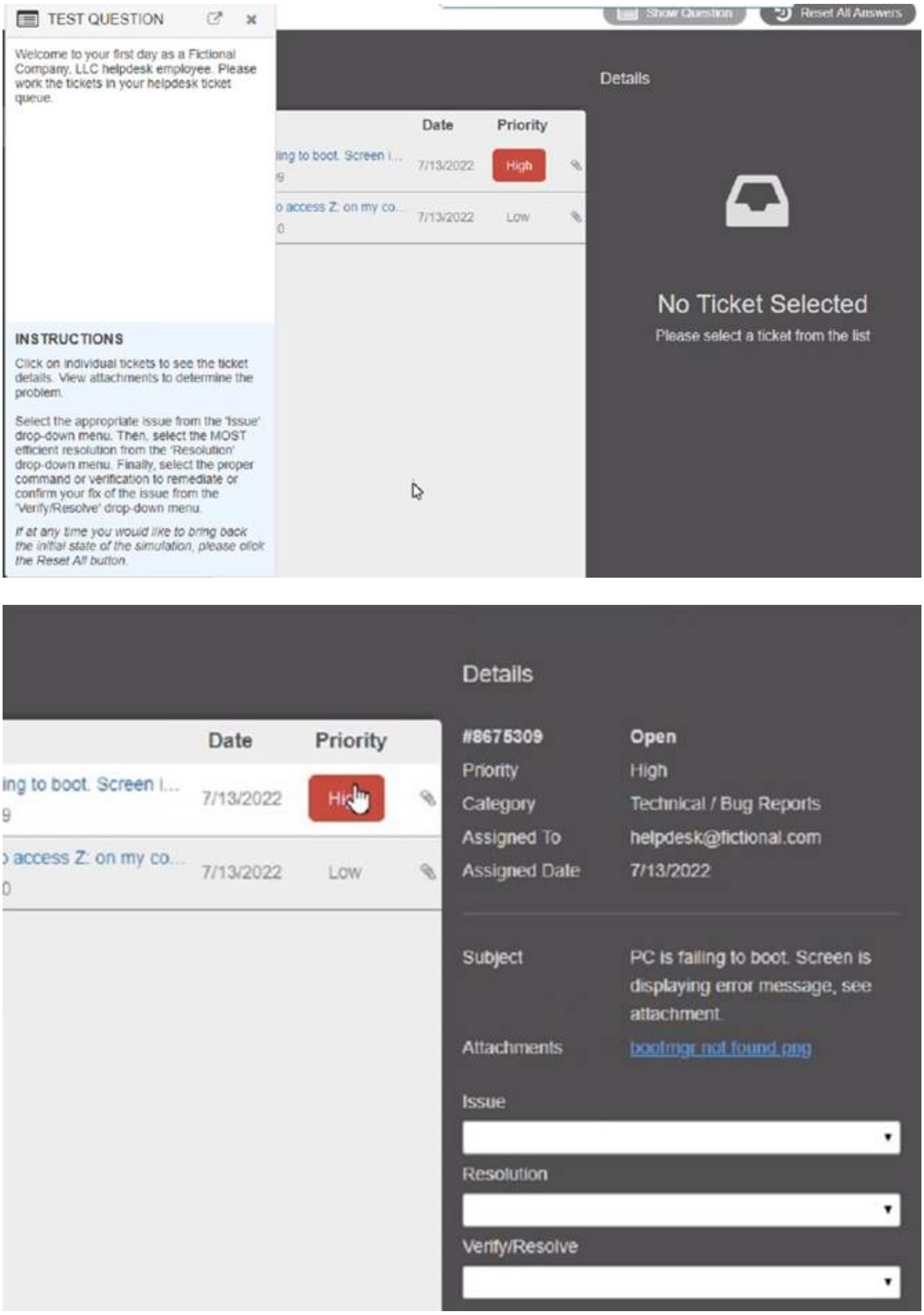
Explanation:
The most likely agreement in use here is a EULA (End User License Agreement). This is a legally binding agreement between the user and the software developer, outlining the terms and conditions that the user must agree to in order to use the software. It is important that the user understands and agrees to the EULA before they can proceed with downloading and installing the software. As stated in the CompTIA A+ Core 2 exam objectives, users should be aware of the EULA before downloading any software.

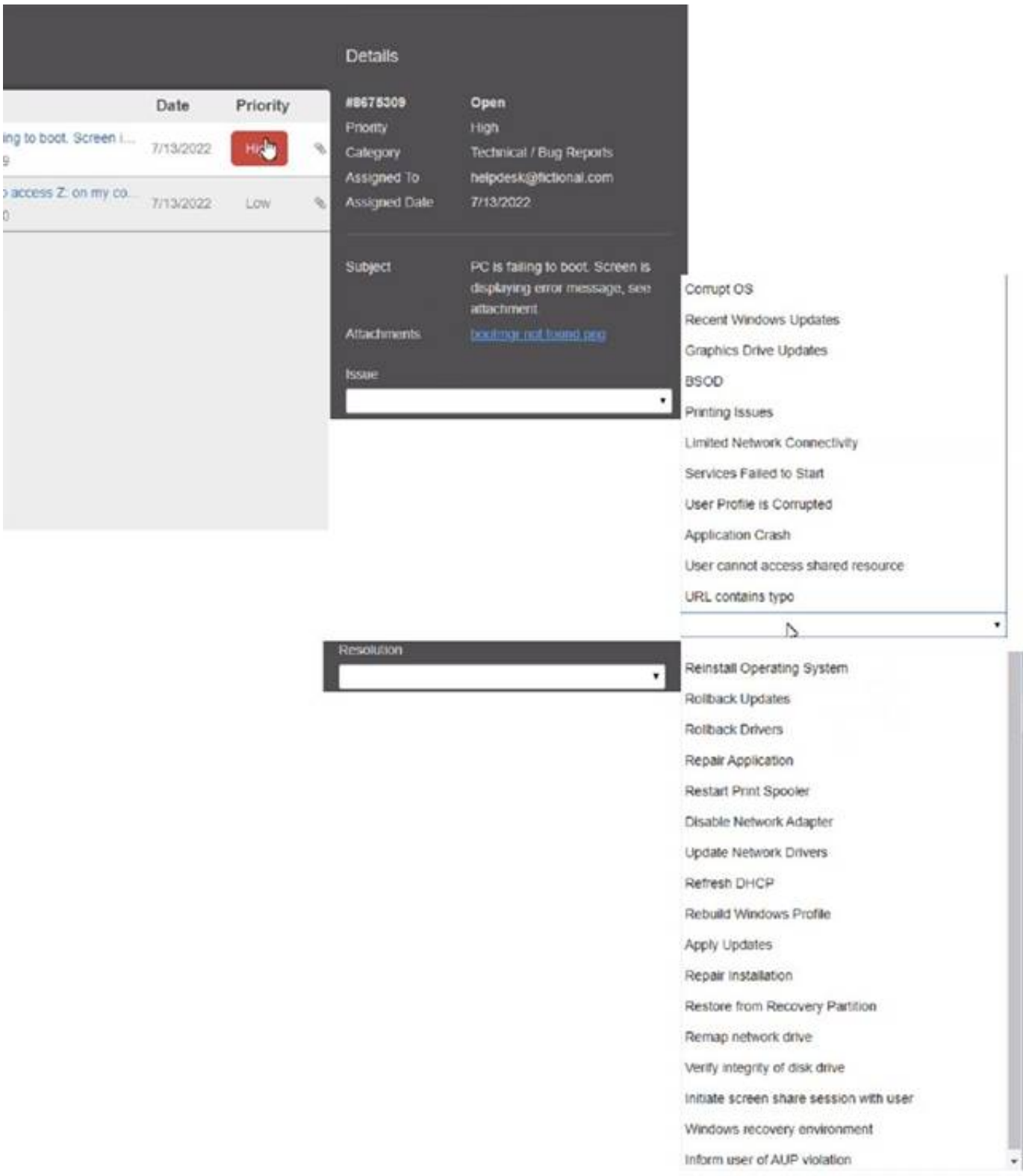
NEW QUESTION 76
A user in a corporate office reports the inability to connect to any network drives. No other users have reported this issue. Which of the following is the MOST likely reason the user is having this issue?

A. Mastered
B. Not Mastered

Answer: A

NEW QUESTION 81
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.

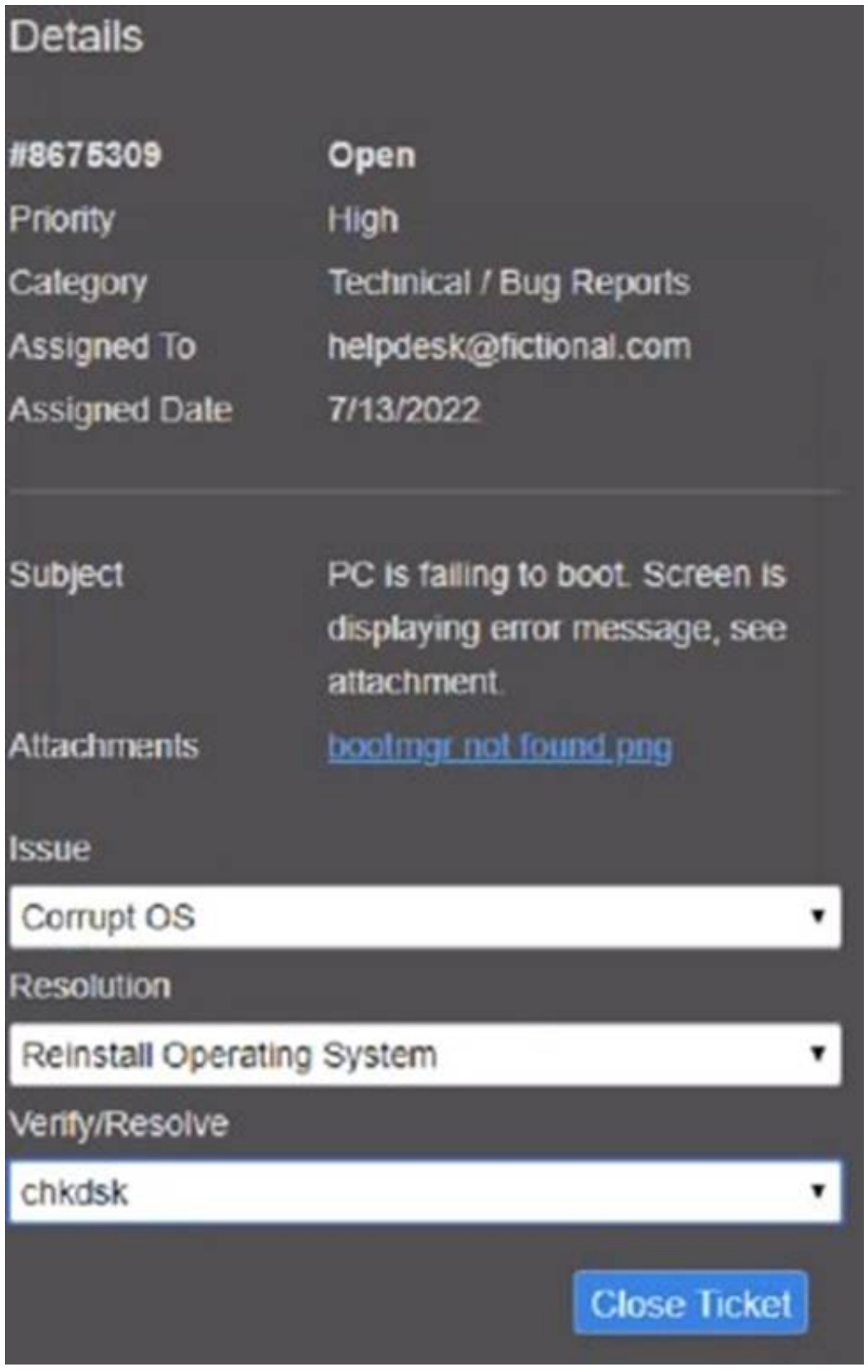

TEST QUESTION
Welcome to your first day as a Fictional Company, LLC helpdesk employee. Please work the tickets in your helpdesk ticket queue.
INSTRUCTIONS
Click on individual tickets to see the ticket details. View attachments to determine the problem.
Select the appropriate issue from the 'Issue' drop-down 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.
Show Question
Reset All Answers
Details
Date
Priority
ing to boot. Screen i...
7/13/2022
High
o access Z: on my co...
7/13/2022
Low
No Ticket Selected
Please select a ticket from the list
Details
Date
Priority
ing to boot. Screen i...
7/13/2022
Hi
access Z: on my co...
7/13/2022
Low
#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



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 83
A user's application is unresponsive. Which of the following Task Manager tabs will allow the user to address the situation?

A. Startup
B. Performance
C. Application history
D. Processes

Answer: D

Explanation:
The Processes tab in the Task Manager shows all the running processes on the computer, including applications and background services. The user can use this tab to identify the unresponsive application and end its process by right-clicking on it and selecting End task. This will free up the system resources and close the application. The other tabs in the Task Manager do not allow the user to address the situation. The Startup tab shows the programs that run when the computer starts, the Performance tab shows the system resource usage and statistics, and the Application history tab shows the resource usage of the applications over time

NEW QUESTION 84
Which of the following filesystem types does macOS use?

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

Answer: D

Explanation:
APFS stands for Apple File System and it is the default filesystem type for macOS since High Sierra (10.13) version1. APFS is optimized for flash storage and supports features such as encryption, snapshots, cloning, and space sharing1.

NEW QUESTION 89
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.

Answer: A

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.

NEW QUESTION 93
An organization is updating the monitors on kiosk machines. While performing the upgrade, the organization would like to remove physical input devices. Which of the following utilities in the Control Panel can be used to turn on the on-screen keyboard to replace the physical input devices?

A. Devices and Printers
B. Ease of Access
C. Programs and Features
Device Manager
D.

Answer: B

Explanation:
Ease of Access is a utility in the Control Panel that allows users to adjust various accessibility settings on Windows, such as the on-screen keyboard, magnifier, narrator, high contrast, etc. The on-screen keyboard can be turned on by going to Ease of Access > Keyboard and toggling the switch to On12. Alternatively, the on-screen keyboard can be opened by pressing Windows + Ctrl + O keys or by typing osk.exe in the Run dialog box3.
References: 1 Use the On-Screen Keyboard (OSK) to type(https://support.microsoft.com/en-us/windows/use-the-on-screen-keyboard-osk-to-type- ecbb5e08-5b4e-d8c8-f794-81dbf896267a)2 How to Enable or Disable the On-Screen Keyboard in Windows 10 - Lifewire(https://www.lifewire.com/enable-or-disable-on-screen-keyboard-in-windows-10-5180667)3 On-Screen Keyboard Settings, Tips and Tricks in Windows 11/10(https://www.thewindowsclub.com/windows-onscreen-keyboard).

NEW QUESTION 96
Which of the following defines the extent of a change?

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

Answer: A

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.
References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 5.2

NEW QUESTION 101
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.

Answer: C

Explanation:
being significantly increased due to the size of CAD files.
The IT manager is most likely to be concerned about network utilization
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.

NEW QUESTION 102
Which of the following is a proprietary Cisco AAA protocol?

A. TKIP
B. AES
C. RADIUS
D. TACACS+

Answer: D

Explanation:
TACACS+ is a proprietary Cisco AAA protocol

NEW QUESTION 104
A company-owned mobile device is displaying a high number of ads, receiving data-usage limit notifications, and experiencing slow response. After checking the device, a technician notices the device has been jailbroken. Which of the following should the technician do next?

A. Run an antivirus and enable encryption.
B. Restore the defaults and reimage the corporate OS.
C. Back up the files and do a system restore.
D. Undo the jailbreak and enable an antivirus.

Answer: B

Explanation:
Jailbreaking a device exposes it to various security risks, such as malware, data theft, network attacks, and service disruption1234. Running an antivirus and enabling encryption may not be enough to remove the threats and restore the device's functionality. Undoing the jailbreak may not be possible or effective, depending on the method used. Backing up the files and doing a system restore may preserve the jailbreak and the associated problems. The best option is to erase the device and reinstall the original operating system that is compatible with the corporate policies and standards. This will ensure that the device is clean, secure, and compliant25.
References: 1 What is Jailbreaking & Is it safe? - Kaspersky(https://www.kaspersky.com/resource-center/definitions/what-is- jailbreaking). 2 Jailbreak Detection: Why is jailbreaking a potential security risk? -
Cybersecurity ASEE(https://cybersecurity.asee.co/blog/what-is-jailbreaking/). 3 Jailbreaking Information for iOS Devices | University IT(https://uit.stanford.edu/service/mydevices/jailbreak)4 What does it mean to jailbreak your phone—and is it legal? - Microsoft(https://www.microsoft.com/en-us/microsoft-365-life- hacks/privacy-and-safety/what-is-jailbreaking-a-phone). 5 Resetting a corporate laptop back to a personal laptop… Enterprise vs Pro - Windows 10(https://community.spiceworks.com/topic/2196812-resetting-a-corporate-laptop-back-to-a-personal-laptop-enterprise-vs-pro).

NEW QUESTION 108
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.

Answer: D

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.

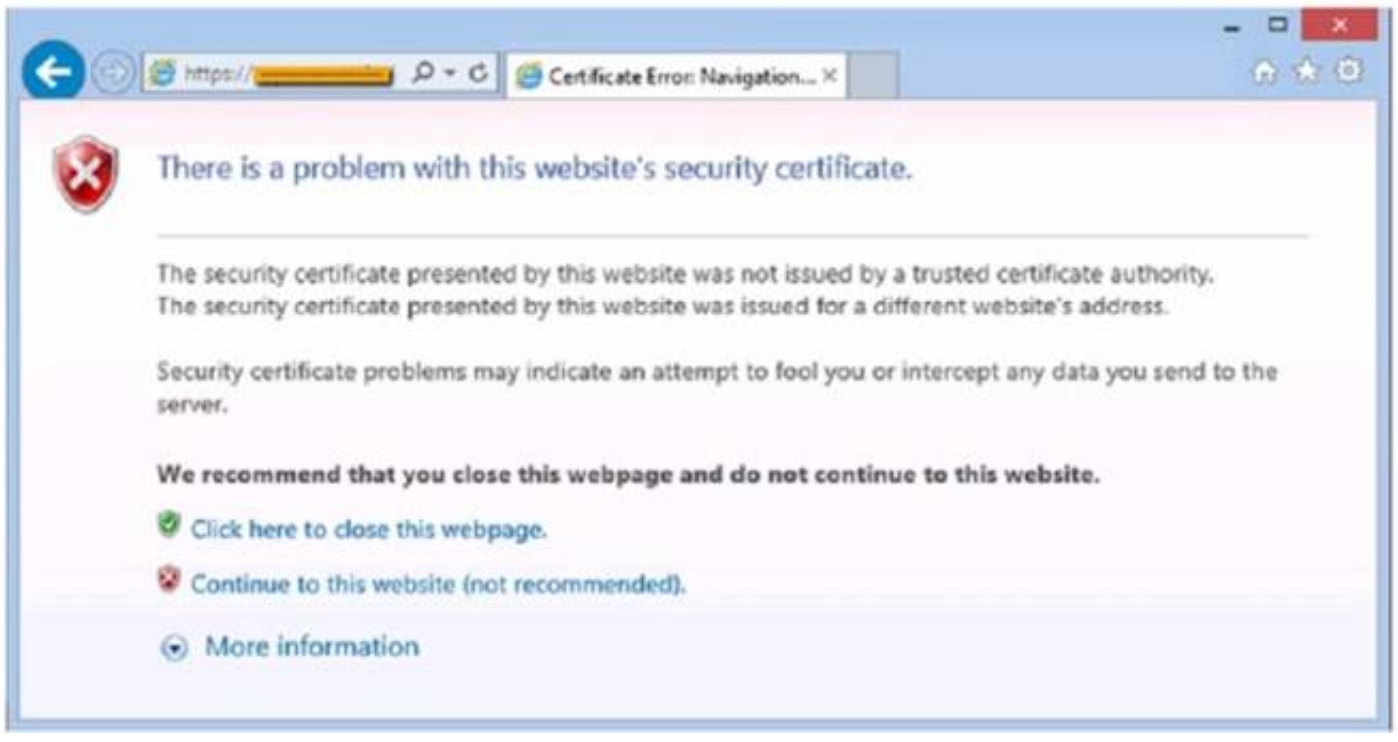
NEW QUESTION 111
A user installed a new application that automatically starts each time the user logs in to a Windows 10 system. The user does not want this to happen and has asked for this setting to be changed. Which of the following tools would the technician MOST likely use to safely make this change?

A. Mastered
B. Not Mastered

Answer: A

Explanation:
The technician would most likely use the Task Manager tool to safely make this change12
The Task Manager tool can be used to disable applications from starting automatically on Windows 10
The tool that a technician would most likely use to stop an application from automatically starting when a user logs in to a Windows 10 system is the Task Manager. The Task Manager can be used to view and manage processes, including those that are set to automatically start when a user logs in to the system.

NEW QUESTION 113
After clicking on a link in an email a Chief Financial Officer (CFO) received the following error:



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

Answer: A

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.

NEW QUESTION 115
A user's antivirus software reports an infection that it is unable to remove. Which of the following is the most appropriate way to remediate the issue?

A. Disable System Restore.
B. Utilize a Linux live disc.
C. Quarantine the infected system.
D. Update the anti-malware.

Answer: C

Explanation:
Quarantining the infected system is the most appropriate way to remediate the issue of an infection that the antivirus software cannot remove. Quarantining means isolating the system from the network and other devices to prevent the infection from spreading or causing further damage. Quarantining also allows the technician to perform further analysis and removal of the infection without risking the security of other systems or data.
Some of the steps involved in quarantining an infected system are:
? Disconnect the system from the internet and any local network connections, such as Wi-Fi, Ethernet, Bluetooth, or USB.
? Disable any file-sharing or remote access services on the system, such as Windows File Sharing, Remote Desktop, or TeamViewer.
? Use a separate device to download and update the antivirus software and any other tools that may be needed to remove the infection, such as malware scanners, rootkit removers, or bootable rescue disks.
? Transfer the updated antivirus software and tools to the infected system using a removable media, such as a CD, DVD, or USB flash drive. Scan the removable media for any infections before and after using it on the infected system.
? Run the antivirus software and tools on the infected system and follow the instructions to delete or quarantine the infection. If the infection is persistent or complex, it may require booting the system from a rescue disk or using a Linux live disc to access and clean the system files.
? After the infection is removed, restore the system to a previous clean state using
System Restore, backup, or recovery partition. Scan the system again to ensure that it is clean and secure. Reconnect the system to the network and update the system and the antivirus software.
References:
? How to Identify and Repair Malware or Virus Infected Computers, section 31
? Uninstalling Antivirus Software, the Clean Way: 40 Removal Tools & Instructions, section 22
? How to manually remove an infected file from a Windows computer3
? The Official CompTIA A+ Core 2 Study Guide (220-1102), page 2194

NEW QUESTION 118
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.

Answer: D

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.

NEW QUESTION 120
A user is trying to use proprietary software, but it crashes intermittently. The user notices that the desktop is displaying a "low memory" warning message. Upon restarting the desktop, the issue persists. Which of the following should a technician do next to troubleshoot the issue?

A. Reimage the computer.
B. Replace the system RAM.
C. Reinstall and update the failing software.
D. Decrease the page file size.

Answer: C

Explanation:
The most likely cause of the intermittent crashes is that the proprietary software is incompatible, outdated, or corrupted. Reinstalling and updating the software can fix these issues and ensure the software runs smoothly. Reimaging the computer or replacing the system RAM are too drastic and unnecessary steps. Decreasing the page file size can worsen the low memory problem and affect the performance of other applications.

NEW QUESTION 123
Which of the following file types allows a user to easily uninstall software from macOS by simply placing it in the trash bin?

A. .exe
B. .dmg
C. . app
D. . rpm
E. .pkg

Answer: C

Explanation:
app files are application bundles that contain all the necessary files and resources for a Mac app. They can be easily deleted by dragging them to the Trash or using Launchpad12. Other file types, such as .exe, .dmg, .rpm, and .pkg, are either not compatible with macOS or require additional steps to uninstall34.
References: 1 Uninstall apps on your Mac - Apple Support(https://support.apple.com/en- us/102610)2 How to Uninstall Apps on a Mac (and Make Sure Leftover Files Are
…(https://www.pcmag.com/how-to/uninstall-delete-apps-from-mac)3 How to install and uninstall software on a Mac - Laptop Mag(https://www.laptopmag.com/articles/install- unininstall-mac-software)4 How to completely uninstall an app on a Mac and delete all junk files(https://www.xda-developers.com/how-to-uninstall-app-mac/).

NEW QUESTION 128
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.

Answer: B

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 resources and slowing down the phone. The user should uninstall the application and run a malware scan on the phone1

NEW QUESTION 132
Maintaining the chain of custody is an important part of the incident response process. Which of the following reasons explains why this is important?

A. To maintain an information security policy
B. To properly identify the issue
C. To control evidence and maintain integrity
D. To gather as much information as possible

Answer: C

Explanation:
Maintaining the chain of custody is important to control evidence and maintain integrity. The chain of custody is a process that documents who handled, accessed, or modified a piece of evidence, when, where, how, and why. The chain of custody ensures that the evidence is preserved, protected, and authenticated throughout the incident response process. Maintaining the chain of custody can help prevent tampering, alteration, or loss of evidence, as well as establish its reliability and validity in legal proceedings. Maintaining an information security policy, properly identifying the issue, and gathering as much information as possible are not reasons why maintaining the chain of custody is important. Maintaining an information security policy is a general practice that defines the rules and guidelines for securing an organization’s information assets and resources. Properly identifying the issue is a step in the incident response process that

involves analyzing and classifying the incident based on its severity, impact, and scope. Gathering as much information as possible is a step in the incident response process that involves collecting and documenting relevant data and evidence from various sources, such as logs, alerts, or witnesses. References:
? Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 26

NEW QUESTION 133
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

Answer: D

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.
References: 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)

NEW QUESTION 137
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

Answer: B

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

NEW QUESTION 142
The command cac cor.ptia. 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 compti
C. txt would be displayed.
D. The contents of the text comptia.txt would be categorized in alphabetical order.
E. The contents of the text compti
F. txt would be copied to another compti
G. txt file

Answer: B

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

NEW QUESTION 146
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

Answer: B

Explanation:
Full disk encryption is a security mechanism that encrypts the entire data on a hard drive, making it unreadable without the correct decryption key or password. It can prevent the stored data from being recovered by unauthorized persons who steal or access the laptop. Biometrics, enforced strong system password and two-factor authentication are other security mechanisms, but they only protect the login access to the laptop, not the data on the hard drive. Verified References: https://www.comptia.org/blog/what-is-full-disk- encryption https://www.comptia.org/certifications/a

NEW QUESTION 148
Which of the following is used to explain issues that may occur during a change implementation?

A. Scope change
B. End-user acceptance

C. Risk analysis
D. Rollback plan

Answer: C

Explanation:
Risk analysis is used to explain issues that may occur during a change implementation. Risk analysis is a process of identifying, assessing and prioritizing potential risks that may affect a project or an activity. Risk analysis can help determine the likelihood and impact of various issues that may arise during a change implementation, such as technical errors, compatibility problems, security breaches, performance degradation or user dissatisfaction. Risk analysis can also help plan and prepare for mitigating or avoiding these issues. Scope change is a modification of the original goals, requirements or deliverables of a project or an activity. Scope change is not used to explain issues that may occur during a change implementation but to reflect changes in expectations or needs of the stakeholders. End- user acceptance is a measure of how well the users are satisfied with and adopt a new system or service. End-user acceptance is not used to explain issues that may occur during a change implementation but to evaluate the success and effectiveness of the change. Rollback plan is a contingency plan that describes how to restore a system or service to its previous state in case of a failed or problematic change implementation. Rollback plan is not used to explain issues that may occur during a change implementation but to recover from them. References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 5.2

NEW QUESTION 149
A technician is replacing the processor in a desktop computer prior to opening the computer, the technician wants to ensure the internal components are protected. Which of the following safety procedures would BEST protect the components in the PC? (Select TWO).

A. Utilizing an ESD strap
B. Disconnecting the computer from the power source
C. Placing the PSU in an antistatic bag
D. Ensuring proper ventilation
E. Removing dust from the ventilation fans
F. Ensuring equipment is grounded

Answer: AC

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

NEW QUESTION 153
A large company is selecting a new Windows operating system and needs to ensure it has built-in encryption and endpoint protection. Which of the following Windows versions will MOST likely be selected?

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

Answer: D

Explanation:
When selecting a new Windows operating system for a large company that needs built-in encryption and endpoint protection, the Enterprise edition is the most likely choice. This edition provides advanced security features such as Windows Defender Advanced Threat Protection (ATP), AppLocker, and BitLocker Drive Encryption. These features can help to protect the company's data and endpoints against malware attacks, unauthorized access, and data theft.
The Home and Pro editions of Windows do not include some of the advanced security features provided by the Enterprise edition, such as Windows Defender ATP and AppLocker. The Pro for Workstations edition is designed for high-performance and high- end hardware configurations, but it does not provide additional security features beyond those provided by the Pro edition.

NEW QUESTION 158
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.

Answer: C

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.

NEW QUESTION 159
A customer calls desktop support and begins yelling at a technician. The customer claims to have submitted a support ticket two hours ago and complains that the issue still has not been resolved. Which of the following describes how the technician should respond?

A. Place the customer on hold until the customer calms down.
B. Disconnect the call to avoid a confrontation.
C. Wait until the customer is done speaking and offer assistance.
D. Escalate the issue to a supervisor.

Answer: C

Explanation:
The best way to deal with an angry customer who is yelling at a technician is to wait until the customer is done speaking and offer assistance. This shows respect, empathy, and professionalism, and allows the technician to understand the customer's problem and find a solution. According to the CompTIA A+ Core 2 (220-1102) Certification Study Guide1, some of the steps to handle angry customers are:
? Stay calm and do not take it personally.
? Listen actively and acknowledge the customer's feelings.
? Apologize sincerely and offer to help.
? Restate the customer's issue and ask for clarification if needed.
? Explain the possible causes and solutions for the problem.
? Provide clear and realistic expectations for the resolution.
? Follow up with the customer until the issue is resolved.
The other options are not appropriate ways to deal with angry customers, as they may worsen the situation or damage the customer relationship. Placing the customer on hold may make them feel ignored or dismissed. Disconnecting the call may make them feel disrespected or abandoned. Escalating the issue to a supervisor may make them feel frustrated or powerless, unless the technician cannot resolve the issue or the customer requests to speak to a supervisor.
References:
? CompTIA A+ Certification Exam Core 2 Objectives2
? CompTIA A+ Core 2 (220-1102) Certification Study Guide1
? How To Deal with Angry Customers (With Examples and Tips)3
? 17 ways to deal with angry customers: Templates and examples4
? Six Ways to Handle Angry Customers5

NEW QUESTION 162
A user updates a mobile device's OS. A frequently used application becomes consistently unresponsive immediately after the device is launched. Which of the following troubleshooting steps should the user perform FIRST?

A. Delete the application's cache.
B. Check for application updates.
C. Roll back the OS update.
D. Uninstall and reinstall the application.

Answer: B

Explanation:
Checking for application updates is the first troubleshooting step that the user should perform, because the application may not be compatible with the new OS version and may need an update to fix the issue. Deleting the application's cache, rolling back the OS update, or uninstalling and reinstalling the application are possible solutions, but they are more time-consuming and disruptive than checking for updates. References: : https://www.comptia.org/training/resources/exam-objectives/comptia-a-core-2-exam- objectives : https://www.lifewire.com/how-to-update-apps-on-android-4173855

NEW QUESTION 163
A technician needs to ensure that USB devices are not suspended by the operating system Which of the following Control Panel utilities should the technician use to configure the setting?

A. System
B. Power Options
C. Devices and Printers
D. Ease of Access

Answer: B

Explanation:
The correct answer is B. Power Options. The Power Options utility in the Control Panel allows you to configure various settings related to how your computer uses and saves power, such as the power plan, the sleep mode, the screen brightness, and the battery status. To access the Power Options utility, you can follow these steps:
? Go to Control Panel > Hardware and Sound > Power Options.
? Click on Change plan settings for the power plan you are using.
? Click on Change advanced power settings.
? Expand the USB settings category and then the USB selective suspend setting subcategory.
? Set the option to Disabled for both On battery and Plugged in.
? Click on OK and then on Save changes.
This will prevent the operating system from suspending the USB devices to save power . System, Devices and Printers, and Ease of Access are not the utilities that should be used to configure the setting. System is a utility that provides information about your computer's hardware and software, such as the processor, memory, operating system, device manager, and system protection. Devices and Printers is a utility that allows you to view and manage the devices and printers connected to your computer, such as adding or removing devices, changing device settings, or troubleshooting problems. Ease of Access is a utility that allows you to customize your computer's accessibility options, such as the narrator, magnifier, high contrast, keyboard, mouse, and speech recognition. None of these utilities have any option to configure the USB selective suspend setting.

NEW QUESTION 166
Which of the following is the most likely to use NTFS as the native filesystem?

A. macOS
B. Linux
C. Windows
D. Android

Answer: C

Explanation:
NTFS stands for New Technology File System, which is a proprietary file system developed by Microsoft4. NTFS is the default file system for the Windows NT family of operating systems, which includes Windows 10, Windows Server 2019, and other versions5. NTFS provides features such as security, encryption, compression, journaling, and large volume support45. NTFS is not the native file system for other operating systems, such as macOS, Linux, or Android, although some of them can read or write to NTFS volumes with third-party drivers or tools

NEW QUESTION 171
A technician requires graphical remote access to various Windows, Linux, and macOS desktops on the company LAN. The security administrator asks the technician to utilize a single software solution that does not require an external internet connection. Which of the following remote access tools is the technician most likely to install?

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

Answer: A

Explanation:
VNC (Virtual Network Computing) is a remote access tool that allows the technician to access and control various Windows, Linux, and macOS desktops on the company LAN using a graphical user interface. VNC does not require an external internet connection, as it works over a local network or a VPN. VNC uses a client-server model, where the server runs on the remote desktop and the client connects to it from another device. VNC can transmit the keyboard and mouse events from the client to the server, and the screen updates from the server to the client, enabling the technician to interact with the remote desktop as if it were local12.
VNC is a better option than the other choices because:
? RMM (Remote Monitoring and Management) (B) is not a single software solution, but a category of software solutions that enable IT professionals to remotely monitor, manage, and troubleshoot multiple devices and networks. RMM software may include remote access tools, but also other features such as patch management, backup and recovery, security, reporting, and automation. RMM software may require an external internet connection, as it often relies on cloud-based services or web-based consoles34.
? RDP (Remote Desktop Protocol) © is a remote access tool that allows the technician to access and control Windows desktops on the company LAN using a graphical user interface. However, RDP is not compatible with Linux or macOS desktops, unless they have third-party software installed that can emulate or translate the RDP protocol. RDP also has some security and performance issues, such as encryption vulnerabilities, bandwidth consumption, and latency problems56.
? SSH (Secure Shell) (D) is a remote access tool that allows the technician to access and control various Windows, Linux, and macOS desktops on the company

LAN using a command-line interface. SSH does not require an external internet connection, as it works over a local network or a VPN. SSH uses encryption and authentication to secure the communication between the client and the server. However, SSH does not provide a graphical user interface, which may limit the functionality and usability of the remote desktop7 .
References:
1: What is VNC? - Definition from Techopedia1 2: How VNC Works - RealVNC2 3: What is Remote Monitoring and Management (RMM)? - Definition from Techopedia3 4: What is RMM Software? - NinjaRMM4 5: What is Remote Desktop Protocol (RDP)? - Definition from Techopedia5 6: Remote Desktop Protocol: What it is and how to secure it - CSO Online6 7: What is Secure Shell (SSH)? - Definition from Techopedia7 : How to Use SSH to Access a Remote Server in Linux or Windows - Hostinger Tutorials

NEW QUESTION 174
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

Answer: D

Explanation:
The risk analysis should be performed before it's taken to the board. The step after the board approves the change is End User Agreenment Reference: https://www.youtube.com/watch?v=Ru77iZxuElA&list=PLG49S3nxzAnna96gzhJrzkii4hH_mgW4b&index=59

NEW QUESTION 179
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

Answer: A

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.

NEW QUESTION 184
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.

Answer: A

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

NEW QUESTION 187
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

Answer: C

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.

NEW QUESTION 191
A user requires local administrative access to a workstation. Which of the following Control Panel utilities allows the technician to grant access to the user?

A. System
B. Network and Sharing Center
C. User Accounts
D. Security and Maintenance

Answer: C

Explanation:
User Accounts is 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.
References: 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)

NEW QUESTION 194
A technician received a call from a user who clicked on a web advertisement Now. every time the user moves the mouse, a pop-up display across the monitor. Which of the following procedures should the technician perform?

A. Boot into safe mode.
B. Perform a malware scan.
C. Restart the machine.
D. Reinstall the browser

Answer: AB

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 References: https://www.comptia.org/blog/how-to-boot-into-safe-mode https://www.comptia.org/certifications/a

NEW QUESTION 198
Which of the following Wi-Fi protocols is the MOST secure?

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 199
A technician successfully removed malicious software from an infected computer after running updates and scheduled scans to mitigate future risks. Which of the following should the technician do next?

A. Educate the end user on best practices for security.
B. Quarantine the host in the antivirus system.
C. Investigate how the system was infected with malware.
D. Create a system restore point.

Answer: A

Explanation:
Educating the end user on best practices for security is the next step that the technician should take after successfully removing malicious software from an infected computer. Educating the end user on best practices for security is an important part of preventing future infections and mitigating risks. The technician should explain to the end user how to avoid common sources of malware, such as phishing emails, malicious websites, or removable media. The technician should also advise the end user to use strong passwords, update software regularly, enable antivirus and firewall protection, and backup data frequently. Educating the end user on best practices for security can help the end user become more aware and responsible for their own security and reduce the likelihood of recurrence of malware infections. Quarantining the host in the antivirus system, investigating how the system was infected with malware, and creating a system restore point are not the next steps that the technician should take after successfully removing malicious software from an infected computer. Quarantining the host in the antivirus system is a step that the technician should take before removing malicious software from an infected computer. Quarantining the host in the antivirus system means isolating the infected computer from the network or other devices to prevent the spread of malware. Investigating how the system was infected with malware is a step that the technician should take during or after removing malicious software from an infected computer. Investigating how the system was infected with malware means identifying the source, type, and impact of malware on the system and documenting the findings and actions taken. Creating a system restore point is a step that the technician should take before removing malicious software from an infected computer. Creating a system restore point means saving a snapshot of the system's configuration and settings at a certain point in time, which can be used to restore the system in case of failure or corruption. References:
? Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 15
? CompTIA A+ Core 1 (220-1101) and Core 2 (220-1102) Cert Guide, page 458

NEW QUESTION 202
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.

Answer: B

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 References: https://www.comptia.org/blog/how-to-roll-back-windows-updates https://www.comptia.org/certifications/a

NEW QUESTION 204
A technician is partitioning a hard disk. The five primary partitions should contain 4TB of free space. Which of the following partition styles should the technician use to partition the device?

A. EFS
B. GPT
C. MBR
D. FAT32

Answer: B

Explanation:
GPT is the correct answer for this question. GPT stands for GUID Partition Table, and it is a partition style that supports up to 128 primary partitions and up to 18 exabytes of disk size per partition. GPT also uses a unique identifier for each partition and provides better data protection and recovery. GPT is suitable for partitioning a hard disk that has five primary partitions with 4TB of free space each. EFS, MBR, and FAT32 are not correct answers for this question. EFS stands for Encrypting File System, and it is a feature that allows encrypting files and folders on NTFS volumes. EFS is not a partition style, but rather a file system attribute. MBR stands for Master Boot Record, and it is an older partition style that supports up to four primary partitions and up to 2TB of disk size per partition. MBR cannot handle five primary partitions with 4TB of free space each. FAT32 stands for File Allocation Table 32, and it is a file system that supports up to 32GB of disk size per partition and up to 4GB of file size. FAT32 is not a partition style, but rather a file system type. References:
? Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 14
? CompTIA A+ Complete Study Guide: Core 1 Exam 220-1101 and Core 2 Exam …, page 105

NEW QUESTION 205
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

Answer: D

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 References: https://www.comptia.org/blog/what-is-an-unattended-installation https://www.comptia.org/certifications/a

NEW QUESTION 208
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

Answer: A

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.

NEW QUESTION 212
Which of the following provide the BEST way to secure physical access to a data cento server room? (Select TWO).

A. Biometric lock
B. Badge reader
C. USB token
D. Video surveillance
E. Locking rack
F. Access control vestibule

Answer: AB

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.

NEW QUESTION 213
A developer reports that a workstation's database file extensions have been changed from
.d b to .enc. The developer is also unable to open the database files manually. Which of the following is the best option for recovering the data?

A. Accessing a restore point
B. Rebooting into safe mode
C. Utilizing the backups
D. Using an AV to scan the affected files

Answer: C

Explanation:
The scenario described in the question suggests that the workstation has been infected by a ransomware, which is a type of malware that encrypts the files on the target system and demands a ransom for the decryption key12. The file extension .enc is commonly used by some ransomware variants to mark the encrypted files34. The developer is unable to open the database files manually because they are encrypted and require the decryption key, which is usually held by the attacker.
The best option for recovering the data is to utilize the backups, assuming that the backups are recent, valid, and not affected by the ransomware. Backups are copies of the data that are stored in a separate location or device, and can be used to restore the data in case of a disaster, such as a ransomware attack . By restoring the data from the backups, the developer can avoid paying the ransom and losing the data permanently.
Accessing a restore point is not a good option, because restore points are snapshots of the system settings and configuration, not the data files. Restore points can help to undo some system changes, such as installing a faulty driver or software, but they cannot recover the encrypted data files .
Rebooting into safe mode is also not a good option, because safe mode is a diagnostic mode that allows the system to run with minimal drivers and services, but it does not affect the data files. Safe mode can help to troubleshoot some system issues, such as malware infections, but it cannot decrypt the data files .
Using an AV to scan the affected files is also not a good option, because an AV is a software that can detect and remove some malware, but it cannot decrypt the data files. An AV can help to prevent or remove some ransomware infections, but it cannot recover the encrypted data files .
References1: CompTIA A+ Certification Exam Core 2 Objectives, page 10 2: CompTIA A+ Core 2 (220-1102) Complete Video Course, Lesson 26 Documentation 3: How to remove
.e nc file virus (Ransomware virus removal guide) 4: Enc File Extension - What is an .enc file and how do I open it? : CompTIA A+ Certification Exam Core 2 Objectives, page 13 : CompTIA A+ Core 2 (220-1102) Complete Video Course, Lesson 26 Documentation
: What is a restore point? : How to use System Restore on Windows 10 : [What is Safe Mode?] : [How to boot into Safe Mode on Windows 10] : CompTIA A+ Certification Exam Core 2 Objectives, page 10 : [Can antivirus software remove ransomware?]

NEW QUESTION 217
Which of the following file types would be used in the Windows Startup folder to automate copying a personal storage table (.pst file) to a network drive at log-in?

A. .bat
B. .dll
C. .ps1
D. .txt

Answer: A

Explanation:
The .bat file type would be used in the Windows Startup folder to automate copying a personal storage table (.pst) file to a network drive at log-in. A .bat file is a batch file that contains a series of commands that can be executed by the command interpreter. A .bat file can be used to perform various tasks, such as copying, moving, deleting, or renaming files or directories. A .bat file can be placed in the Windows Startup folder to run automatically when a user logs in to the system. A .bat file can use the copy command to copy a .pst file from a local drive to a network drive. A .pst file is a personal storage table file that contains email messages, contacts, calendars, and other data from Microsoft Outlook. A .pst file can be backed up to a network drive for security or recovery purposes. The .dll, .ps1, and .txt file types are not used in the Windows Startup folder to automate copying a .pst file to a network drive at log-in. A .dll file is a dynamic link library file that contains code or data that can be shared by multiple programs. A .dll file cannot be executed directly by the user or the system. A .ps1 file is a PowerShell script file that contains commands or expressions that can be executed by the PowerShell interpreter. A.ps1 file can also perform various tasks, such as copying files or directories, but it requires PowerShell to be installed and configured on the system. A .txt file is a plain text file that contains unformatted text that can be read by any text editor or word processor. A .txt file cannot contain commands or expressions that can be executed by the system.
References:
? Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 18
? CompTIA A+ Core 1 (220-1101) and Core 2 (220-1102) Cert Guide, page 459

NEW QUESTION 220
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.

Answer: B

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

NEW QUESTION 225
A large company is changing its password length requirements. The Chief Information Officer is mandating that passwords now be at least 12 characters long, instead of 10. Which of the following should be used to adjust this setting?

A. Group Policy
B. User accounts
C. Access control lists
D. Authenticator applications

Answer: A

Explanation:
Group Policy is a feature of Windows that allows administrators to manage and configure settings for computers and users on a network12. One of the settings that can be controlled by Group Policy is the password policy, which defines the rules for creating and changing passwords, such as minimum length, complexity, expiration, and history34. By using Group Policy, the Chief Information Officer can enforce the new password length requirement for all users and computers in the company's domain, without having to manually adjust each user account or device.
References1: The Official CompTIA A+ Core 2 Student Guide (Exam 220-1102), page 10-11 2: CompTIA A+ Certification Exam Core 2 Objectives, page 13 3: The Official CompTIA A+ Core 2 Instructor Guide (Exam 220-1102), page 10-12 4: CompTIA A+ Certification Exam: Core 2 (220-1102) Exam Objectives

NEW QUESTION 229
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.

Answer: B

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.

NEW QUESTION 232
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. Mastered
B. Not Mastered

Answer: A

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.

NEW QUESTION 235
A user needs assistance changing the desktop wallpaper on a Windows 10 computer. Which of the following methods will enable the user to change the wallpaper using a Windows 10 Settings tool?

A. Open Settings, select Accounts, select, Your info, click Browse, and then locate and open the image the user wants to use as the wallpaper
B. Open Settings, select Personalization, click Browse, and then locate and open the image the user wants to use as the wallpaper
C. Open Settings, select System, select Display, click Browse, and then locate and open the image the user wants to use as the wallpaper
D. Open Settings, select Apps, select Apps & features, click Browse, and then locate and open the image the user wants to use as the wallpaper.

Answer: B

Explanation:
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 image the user wants to use as the wallpape1r https://www.lifewire.com/change-desktop-background-windows-11-5190733

NEW QUESTION 237
Which of the following common security vulnerabilities can be mitigated by using input validation?

A. Brute-force attack
B. Cross-site scripting
C. SQL injection
D. Cross-site request forgery

Answer: BC

Explanation:
Cross-site scripting (XSS) and SQL injection are common security vulnerabilities that can be mitigated by using input validation. Input validation is a technique that checks the user input for any malicious or unexpected characters or commands before processing it. XSS is an attack that injects malicious scripts into web pages to steal cookies, session tokens or other sensitive information from users or web servers. SQL injection is an attack that injects malicious SQL statements into web applications to manipulate databases, execute commands or access unauthorized data. Verified References: https://www.comptia.org/blog/what-is-input-validation https://www.comptia.org/certifications/a

NEW QUESTION 240
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

Answer: A

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

NEW QUESTION 243
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

Answer: C

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.

NEW QUESTION 248
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

Answer: B

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.

NEW QUESTION 251
Malware is installed on a device after a user clicks on a link in a suspicious email. Which of the following is the best way to remove the malware?

A. Run System Restore.
B. Place in recovery mode.
C. Schedule a scan.
D. Restart the PC.

Answer: B

Explanation:
Recovery mode is a special boot option that allows the user to access advanced tools and features to troubleshoot and remove malware from the device. Recovery mode can also restore the system to a previous state or reset the device to factory settings. Running System Restore, scheduling a scan, or restarting

the PC may not be effective in removing the malware, as it may still be active or hidden in the system files.

NEW QUESTION 254
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

Answer: B

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. References: CompTIA A+ Core 2 (220-1002) Certification
Exam Objectives Version 4.0, Domain 1.1

NEW QUESTION 257
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

Answer: A

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

NEW QUESTION 259
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

Answer: B

Explanation:
To exclude an application folder from being cataloged by a Windows 10 search, the technician should use the Indexing Options uti1lity

NEW QUESTION 263
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

Answer: A

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.

NEW QUESTION 267
A PC is taking a long time to boot Which of the following operations would be best to do to resolve the issue at a minimal expense?

(Select two).

A. Installing additional RAM
B. Removing the applications from startup
C. Installing a faster SSD
D. Running the Disk Cleanup utility
E. Defragmenting the hard drive
F. Ending the processes in the Task Manager

Answer: BD

Explanation:
The best operations to do to resolve the issue of a long boot time at a minimal expense are B. Removing the applications from startup and D. Running the Disk Cleanup utility. These are two simple and effective ways to speed up your PC's boot time without spending any money on hardware upgrades.
Removing the applications from startup means preventing unnecessary programs from launching automatically when you turn on your computer. This can reduce the load on your system resources and make the boot process faster. You can do this in Windows 10 by pressing Ctrl + Alt + Esc to open the Task Manager, and going to the Startup tab. There, you can see a list of programs that start with your computer, and their impact on the startup performance. You can disable any program that you don't need by right-clicking on it and choosing Disable12.
Running the Disk Cleanup utility means deleting temporary files, system files, and other unnecessary data that may be taking up space and slowing down your computer. This can free up some disk space and improve the performance of your system. You can do this in Windows 10 by typing disk cleanup in the search box and selecting the Disk Cleanup app. There, you can choose which files you want to delete, such as Recycle Bin, Temporary Internet Files, Thumbnails, etc. You can also click on Clean up system files to delete more files, such as Windows Update Cleanup, Previous Windows installation(s), etc34.

NEW QUESTION 272
A user contacts the help desk to request assistance with a program feature. The user is in a different building but on the same network as the help desk technician. Which of the following should the technician use to assist the user?

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

Answer: C

Explanation:
RDP stands for Remote Desktop Protocol and it is a protocol that allows a user to remotely access and control another computer over a network. A technician can use RDP to assist a user who is in a different building but on the same network by connecting to the user's computer and viewing their screen, keyboard, and mouse. AAA, SSH, and VPN are not protocols that can be used to assist a user with a program feature.

NEW QUESTION 276
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

Answer: C

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.

NEW QUESTION 279
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

Answer: D

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

NEW QUESTION 280
Applications on a computer are not updating, which is preventing the user from opening certain files. Which of the following MMC snap-ins should the technician launch next to continue troubleshooting the issue?

A. gpedit.msc
B. perfmon.msc

C. devmgmt.msc

Answer: C

Explanation:
devmgmt.msc is the MMC snap-in that opens the Device Manager, a tool that allows the technician to view and manage the hardware devices and their drivers on the computer1. If the applications are not updating properly, it could be due to outdated, corrupted, or incompatible drivers that prevent the hardware from functioning normally. The technician can use the Device Manager to update, uninstall, rollback, or disable the drivers, as well as scan for hardware changes, troubleshoot problems, and view device properties2. gpedit.msc is the MMC snap-in that opens the Group Policy Editor, a tool that allows the technician to configure the local or domain group policy settings for the computer or a group of computers3. Group policy settings can affect the security, performance, and functionality of the system, but they are not directly related to the application updates or the hardware drivers.
perfmon.msc is the MMC snap-in that opens the Performance Monitor, a tool that allows the technician to monitor and analyze the performance of the system and its components, such as processor, memory, disk, network, etc4. Performance Monitor can display real- time data or collect log data for later analysis, as well as generate reports and alerts based on the performance counters5. Performance Monitor can help the technician identify and diagnose performance issues, but it does not provide a way to manage the hardware drivers.
References:
? The Official CompTIA A+ Core 2 Study Guide6, page 223, 225, 227, 228.

NEW QUESTION 283
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

220-1102 Practice Exam Features:

* 220-1102 Questions and Answers Updated Frequently

* 220-1102 Practice Questions Verified by Expert Senior Certified Staff

* 220-1102 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 220-1102 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year