CompTIA

Exam Questions 220-1102

CompTIA A+ Certification Exam: Core 2

NEW QUESTION 1
After a failed update, an application no longer launches and generates the following error message: Application needs to be repaired. Which of the following Windows 10 utilities should a technician use to address this concern?

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

Answer: D

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

NEW QUESTION 2
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 3
A user is no longer able to start the OS on a computer and receives an error message indicating there is no OS found. A technician reviews the audit logs and notes that the user's system posted a S.M.A.R.T. error just days before this issue. Which of the following is the MOST likely cause of this issue?

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

Answer: C

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

NEW QUESTION 4
Which of the following is the MOST basic version of Windows that includes BitLocker?

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

Answer: D

Explanation:
The most basic version of Windows that includes BitLocker is Windows Pro. BitLocker is a feature of Windows Pro that provides full disk encryption for all data on a storage drive [1]. It helps protect data from unauthorized access or theft and can help secure data from malicious attacks. Pro for Workstations includes this feature, as well as other features such as support for up to 6 TB of RAM and ReFS.

NEW QUESTION 5
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 6
Which of the following OS types provides a lightweight option for workstations thai need an easy-to-use browser-based interface?

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

Answer: B

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

NEW QUESTION 7
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 8
Which of the following data is MOST likely to be regulated?

A. Name in a Phone book
B. Name on a medical diagnosis
C. Name on a job application
D. Name on a employer's website

Answer: B

Explanation:
A name on a medical diagnosis (B) is most likely to be regulated. This is because it falls under the category of protected health information (PHI), which is subject to regulations such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States. These regulations aim to protect the privacy and security of individuals' health information.

NEW QUESTION 9
A user reports a computer is running slow. Which of the following tools will help a technician identity the issued

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 10
A technician at a customer site is troubleshooting a laptop A software update needs to be downloaded but the company's proxy is blocking traffic to the update site. Which of the following should the technician perform?

A. Change the DNS address to 1.1.1.1

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

Answer: C

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

NEW QUESTION 10
A BSOD appears on a user's workstation monitor. The user immediately presses the power button to shut down the PC, hoping to repair the issue. The user then restarts the PC, and the BSOD reappears, so the user contacts the help desk. Which of the following should the technician use to determine the cause?

A. Stop code
B. Event Mewer
C. Services
D. System Configuration

Answer: A

Explanation:
When a Blue Screen of Death (BSOD) appears on a Windows workstation, it indicates that there is a serious problem with the operating system. The stop code displayed on the BSOD can provide valuable information to help determine the cause of the issue. The stop code is a specific error code that is associated with the BSOD, and it can help identify the root cause of the problem.
In this scenario, the user has encountered a BSOD and has restarted the PC, only to see the BSOD reappear. This suggests that the problem is persistent and requires further investigation. By analyzing the stop code displayed on the BSOD, a technician can begin to identify the underlying issue and take appropriate actions to resolve it.

NEW QUESTION 14
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 15
A technician is in the process of installing a new hard drive on a server but is called away to another task. The drive has been unpackaged and left on a desk. Which of the following should the technician perform before leaving?

A. Ask coworkers to make sure no one touches the hard drive.
B. Leave the hard drive on the table; it will be okay while the other task is completed.
C. Place the hard drive in an antistatic bag and secure the area containing the hard drive.
D. Connect an electrostatic discharge strap to the drive.

Answer: C

Explanation:
The technician should place the hard drive in an antistatic bag and secure the area containing the hard drive before leaving. This will protect the hard drive from electrostatic discharge (ESD), dust, moisture, and physical damage. Asking coworkers to make sure no one touches the hard drive is not a reliable or secure way to prevent damage. Leaving the hard drive on the table exposes it to ESD and other environmental hazards. Connecting an electrostatic discharge strap to the drive is not enough to protect it from dust, moisture, and physical damage.

NEW QUESTION 18
A large university wants to equip all classrooms with high-definition IP videoconferencing equipment. Which of the following would most likely be impacted in this situation?

A. SAN
B. LAN
C. GPU
D. PAN

Answer: B

Explanation:
LAN is the most likely option to be impacted in this situation. LAN stands for Local Area Network, and it is a network that connects devices within a limited area,

such as a building or a campus. Installing high-definition IP videoconferencing equipment in all classrooms would require a high bandwidth and reliable LAN infrastructure to support the video and audio transmission. The LAN would also need to be configured with proper security, quality of service, and multicast protocols to ensure the optimal performance of the videoconferencing system. SAN, GPU, and PAN are not directly related to this scenario. SAN stands for Storage Area Network, and it is a network that provides access to consolidated storage devices. GPU stands for Graphics Processing Unit, and it is a hardware component that handles graphics rendering and computation. PAN stands for Personal Area Network, and it is a network that connects devices within a short range, such as Bluetooth or infrared. References:
? Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 20
? CompTIA A+ Complete Study Guide: Core 1 Exam 220-1101 and Core 2 Exam …, page 104

NEW QUESTION 22
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 attacker. A keylogger can be used to steal passwords, credit card numbers, personal information, and other sensitive data. A keylogger can be delivered through a USB drive that contains a malicious executable file, such as grabber.exe, and an output file that stores the captured keystrokes, such as output.txt. The other options are not likely to use this method of attack. References: : https://www.comptia.org/training/resources/exam-objectives/comptia-a-core-2-exam- objectives : https://www.kaspersky.com/resource-center/definitions/keylogger

NEW QUESTION 25
A user reports a PC is running slowly. The technician suspects it has a badly fragmented hard drive. Which of the following tools should the technician use?

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

Answer: C

Explanation:
The technician should use dfrgui.exe to defragment the hard drive1

NEW QUESTION 29
A technician installed Windows 10 on a workstation. The workstation only has 3.5GB of usable RAM, even though the technician installed 8GB. Which of the following is the MOST likely reason this system is not utilizing all the
available RAM?

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

Answer: B

Explanation:
The most likely reason that the system is not utilizing all the available RAM is that it is running a 32-bit OS. A 32-bit OS can only address up to 4GB of RAM, and some of that is reserved for hardware and system use1. Therefore, even if the technician installed 8GB of RAM, the system can only use around 3.5GB of usable RAM. To use the full 8GB of RAM, the technician would need to install a 64-bit OS, which can address much more memory2. The system missing updates, the system's memory failing, or the system requiring BIOS updates are not likely to cause this issue.
References: 2: https://support.microsoft.com/en-us/windows/windows-10-system-requirements-6d4e9a79-66bf-7950-467c-795cf0386715 1: https://www.makeuseof.com/tag/unlock-64gb-ram-32-bit-windows-pae-patch/

NEW QUESTION 33
After a security event, a technician removes malware from an affected laptop and disconnects the laptop from the network. Which of the following should the technician do to prevent the operating system from automatically returning to an infected state?

A. Enable System Restore.
B. Disable System Restore.
C. Enable antivirus.
D. Disable antivirus.
E. Educate the user.

Answer: B

Explanation:
System Restore is a feature that allows the user to revert the system to a previous state. However, this can also restore the malware that was removed by the technician. Disabling System Restore can prevent the operating system from automatically returning to an infected state. Enabling antivirus, educating the user, and enabling System Restore are good preventive measures, but they do not address the question. Disabling antivirus can make the system more vulnerable to malware attacks

NEW QUESTION 36

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?

APFS

A
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 39
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 44
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 49
An administrator has submitted a change request for an upcoming server deployment. Which of the following must be completed before the change can be approved?

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

Answer: A

Explanation:
Risk analysis is the process of identifying and evaluating the potential threats and impacts of a change on the system, network, or service. It is an essential step before approving a change request, as it helps to determine the level of risk, the mitigation strategies, and the contingency plans. Risk analysis also helps to prioritize the change requests based on their urgency and importance12.
References: 1 The Change Request Process and Best Practices(https://www.processmaker.com/blog/it-change-request-process-best- practices/)2 Risk Assessment and Analysis Methods: Qualitative and Quantitative(https://www.isaca.org/resources/isaca-journal/issues/2021/volume-2/risk- assessment-and-analysis-methods).

NEW QUESTION 51
A user connected a smartphone to a coffee shop's public Wi-Fi and noticed the smartphone started sending unusual SMS messages and registering strange network activity A technician thinks a virus or other malware has infected the device. Which of the following should the technician suggest the user do to best address these security and privacy concerns? (Select two).

A. Disable Wi-Fi autoconnect.
B. Stay offline when in public places.
C. Uninstall all recently installed applications.
D. Schedule an antivirus scan.
E. Reboot the device
F. Update the OS

Answer: CD

Explanation:
The best way to address the security and privacy concerns caused by a malware infection on a smartphone is to uninstall all recently installed applications and schedule an antivirus scan. Uninstalling the applications that may have introduced the malware can help remove the source of infection and prevent further damage. Scheduling an antivirus scan can help detect and remove any remaining traces of malware and restore the device's functionality. References: CompTIA A+ Core 2 (220-1102) Certification Study Guide, Chapter 5: Mobile Devices, Section 5.3: Mobile Device Security1

NEW QUESTION 52
A small-office customer needs three PCs to be configured in a network with no server. Which of the following network types is the customer's BEST choice for this environment?

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 57
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 62
A system drive is nearly full, and a technician needs lo tree up some space. Which of the following tools should the technician use?

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

Answer: A

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

NEW QUESTION 67
A technician is troubleshooting a mobile device that was dropped. The technician finds that the screen (ails to rotate, even though the settings are correctly applied. Which of the following pieces of hardware should the technician replace to resolve the issue?

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

Answer: C

Explanation:

The piece of hardware that the technician should replace to resolve the issue of the screen failing to rotate on a mobile device that was dropped is the accelerometer. The accelerometer is a sensor that detects the orientation and movement of the mobile device by measuring the acceleration forces acting on it. The accelerometer allows the screen to rotate automatically according to the position and angle of the device. If the accelerometer is damaged or malfunctioning, the screen may not rotate properly or at all, even if the settings are correctly applied. LCD stands for Liquid Crystal Display and is a type of display that uses liquid crystals and backlight to produce images on the screen. LCD is not related to the screen rotation feature but to the quality and brightness of the display. Battery is a component that provides power to the mobile device by storing and releasing electrical energy. Battery is not related to the screen rotation feature but to the battery life and performance of the device. Digitizer is a component that converts touch inputs into digital signals that can be processed by the mobile device. Digitizer is not related to the screen rotation feature but to the touch sensitivity and accuracy of the display. References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.5

NEW QUESTION 69
A user requires a drive to be mapped through a Windows command line. Which of the following command-line tools can be utilized to map the drive?

A. gpupdate
B. net use
C. hostname
D. dir

Answer: B

Explanation:
Net use is a command-line tool that can be used to map a drive in Windows. Mapping a drive means assigning a drive letter to a network location or a local folder, which allows the user to access it more easily and quickly. Net use can also be used to disconnect a mapped drive, display information about mapped drives, or connect to shared resources on another computer. Gpupdate, hostname, and dir are not command-line tools that can be used to map a drive.

NEW QUESTION 70
An office is experiencing constant connection attempts to the corporate Wi-Fi. Which of the following should be disabled to mitigate connection attempts?

A. SSID
B. DHCP
C. Firewall
D. SSD

Answer: A

Explanation:
The SSID (Service Set Identifier) is the name of a wireless network that is broadcasted by the router or the Wi-Fi base station. The SSID helps nearby devices to identify and connect to the available networks. However, broadcasting the SSID also exposes the network to potential connection attempts from unauthorized or malicious users. Therefore, disabling the SSID can mitigate connection attempts by making the network invisible or hidden to the devices that are not already connected to it. To connect to a hidden network, the user would need to know the exact SSID and enter it manually. The other options are not related to mitigating connection attempts to the corporate Wi-Fi. DHCP (Dynamic Host Configuration Protocol) is a protocol that assigns IP addresses to the devices on a network. Firewall is a software or hardware device that filters the incoming and outgoing network traffic based on predefined rules. SSD (Solid State Drive) is a type of storage device that uses flash memory to store data. Disabling any of these options would not prevent connection attempts to the Wi-Fi network, and may cause other problems or issues for the network functionality and performance.
References:
? What is SSID + how to find (and change) it1
? Choosing an SSID2
? SSID Meaning: Finding Your Network’s Name3

NEW QUESTION 75
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 78
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 79
The courts determined that a cybercrimes case could no longer be prosecuted due to the agency's handling of evidence. Which of the following was MOST likely violated during the investigation?

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

Answer: C

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

NEW QUESTION 82
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 85
A technician is modifying the default home page of all the workstations in a company. Which of the following will help to implement this change?

A. Group Policy
B. Browser extension
C. System Configuration
D. Task Scheduler

Answer: A

Explanation:
Group Policy is a feature of Windows that allows administrators to centrally manage and configure the settings of computers and users in a domain network. Group Policy can be used to modify the default home page of all the workstations in a company by creating and applying a policy that specifies the desired URL for the home page. This way, the change will be automatically applied to all the workstations that are joined to the domain and receive the policy.

NEW QUESTION 87
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 90
A user reports a virus is on a PC. The user installs additional real-lime protection antivirus software, and the PC begins performing extremely slow. Which of the following steps should the technician take to resolve the issue?

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

Answer: E

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

NEW QUESTION 94
A salesperson's computer is unable to print any orders on a local printer that is connected to the computer Which of the following tools should the salesperson use to restart the print spooler?

A. Control Panel
B. Processes
Startup
C: Services

Answer: D

Explanation:
The correct answer is D. Services. The print spooler is a service that manages the print queue and sends print jobs to the printer. To restart the print spooler, the salesperson can use the Services app, which allows them to stop and start the service. Alternatively, they can also use the Task Manager or the Command Prompt to restart the print spooler.
References and Explanation
? The Services app is a tool that displays all the services that are running on the
computer. It can be accessed by typing services.msc in the Run window or by searching for Services in the Start menu. The Services app allows users to start, stop, restart, or configure any service, including the print spooler123.
? The Task Manager is a tool that shows information about the processes,
applications, and services that are running on the computer. It can be accessed by pressing Ctrl + Shift + Esc or by right-clicking on the taskbar and selecting Task Manager. The Task Manager allows users to start, stop, or restart any service by going to the Services tab and right-clicking on the service name12.
? The Command Prompt is a tool that allows users to execute commands and
perform tasks using text input. It can be accessed by typing cmd in the Run window or by searching for Command Prompt in the Start menu. The Command Prompt allows users to start, stop, or restart any service by using the net command with the service name. For example, to restart the print spooler, users can type net stop spooler and then net start spooler1.
? The Control Panel is a tool that provides access to various settings and options for
the computer. It can be accessed by typing control panel in the Run window or by searching for Control Panel in the Start menu. The Control Panel does not allow users to restart the print spooler directly, but it can be used to access other tools such as Devices and Printers, Troubleshooting, or Administrative Tools2.
? The Processes tab is a part of the Task Manager that shows information about the
processes that are running on the computer. It can be accessed by opening the Task Manager and selecting the Processes tab. The Processes tab does not allow users to restart the print spooler directly, but it can be used to end any process that is related to printing or causing problems with the print spooler2.
? The Startup tab is a part of the Task Manager that shows information about the
programs that run automatically when the computer starts. It can be accessed by opening the Task Manager and selecting the Startup tab. The Startup tab does not allow users to restart the print spooler directly, but it can be used to disable or enable any program that affects printing or interferes with the print spooler2.

NEW QUESTION 98
A company needs employees who work remotely to have secure access to the corporate intranet. Which of the following should the company implement?

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

Answer: C

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

NEW QUESTION 103
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.

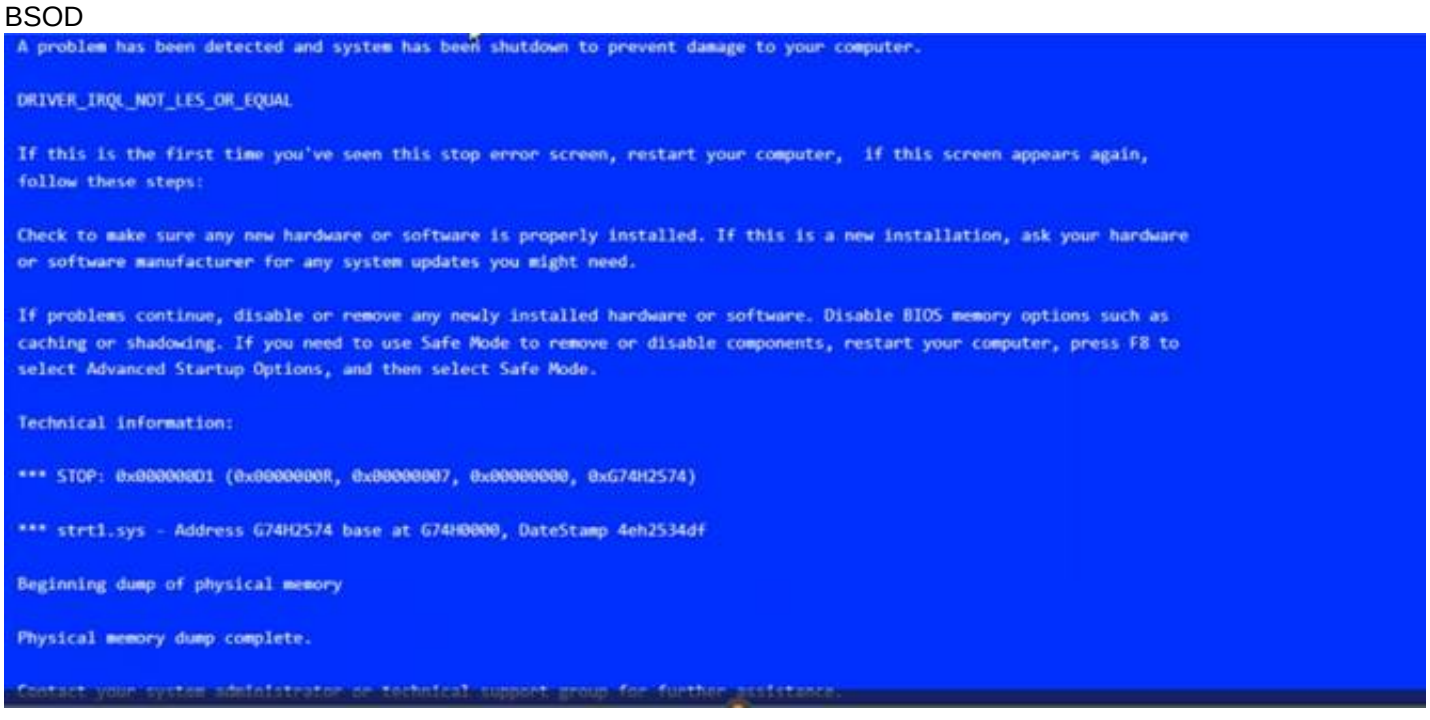
NEW QUESTION 107
A technician has verified a computer is infected with malware. The technician isolates the system and updates the anti-malware software. Which of the following should the technician do next?

A. Mastered
B. Not Mastered

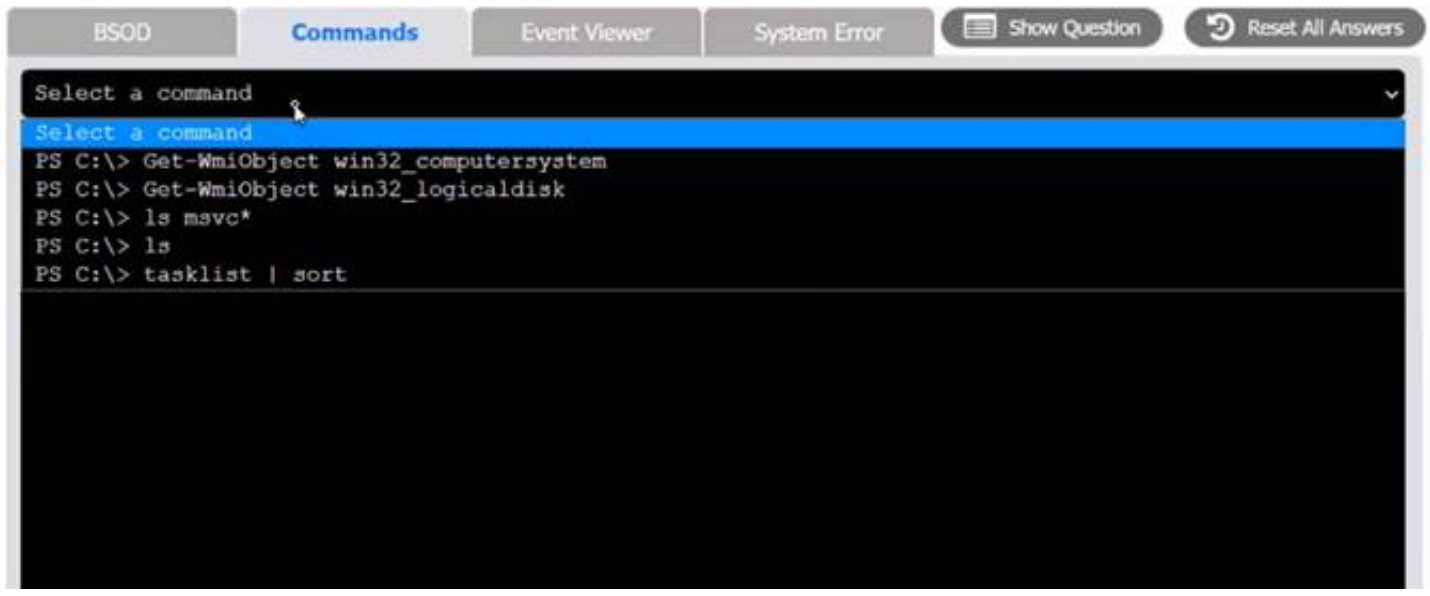
Answer: A

Explanation:
Malware is malicious software that can cause damage or harm to a computer system or network4. A technician has verified a computer is infected with malware by observing unusual behavior, such as slow performance, pop-ups, or unwanted ads. The technician isolates the system and updates the anti-malware software to prevent further infection or spread of the malware. The next step is to run repeated remediation scans until the malware is removed. A remediation scan is a scan that detects and removes malware from the system. Running one scan may not be enough to remove all traces of malware, as some malware may hide or regenerate itself.

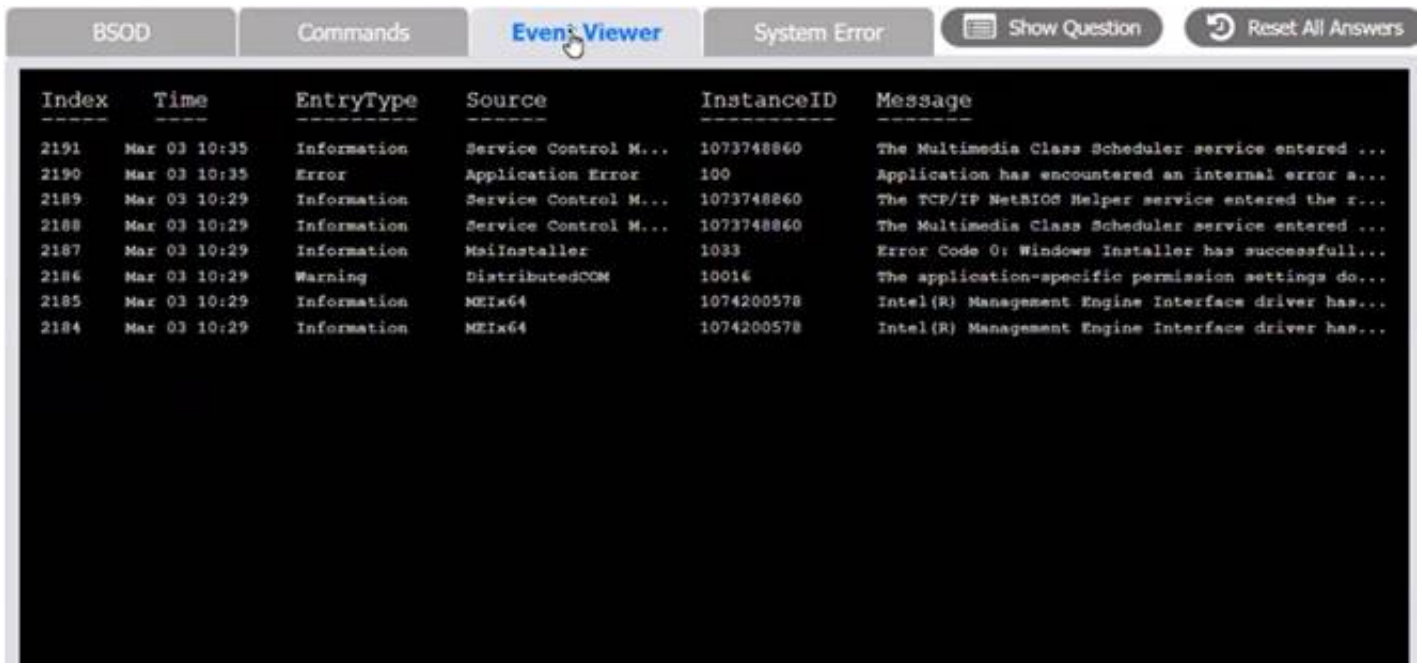
NEW QUESTION 112
SIMULATION
A user reports that after a recent software deployment to upgrade applications, the user can no longer use the Testing program. However, other employees can successfully use the Testing program.
INSTRUCTIONS
Review the information in each tab to verify the results of the deployment 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



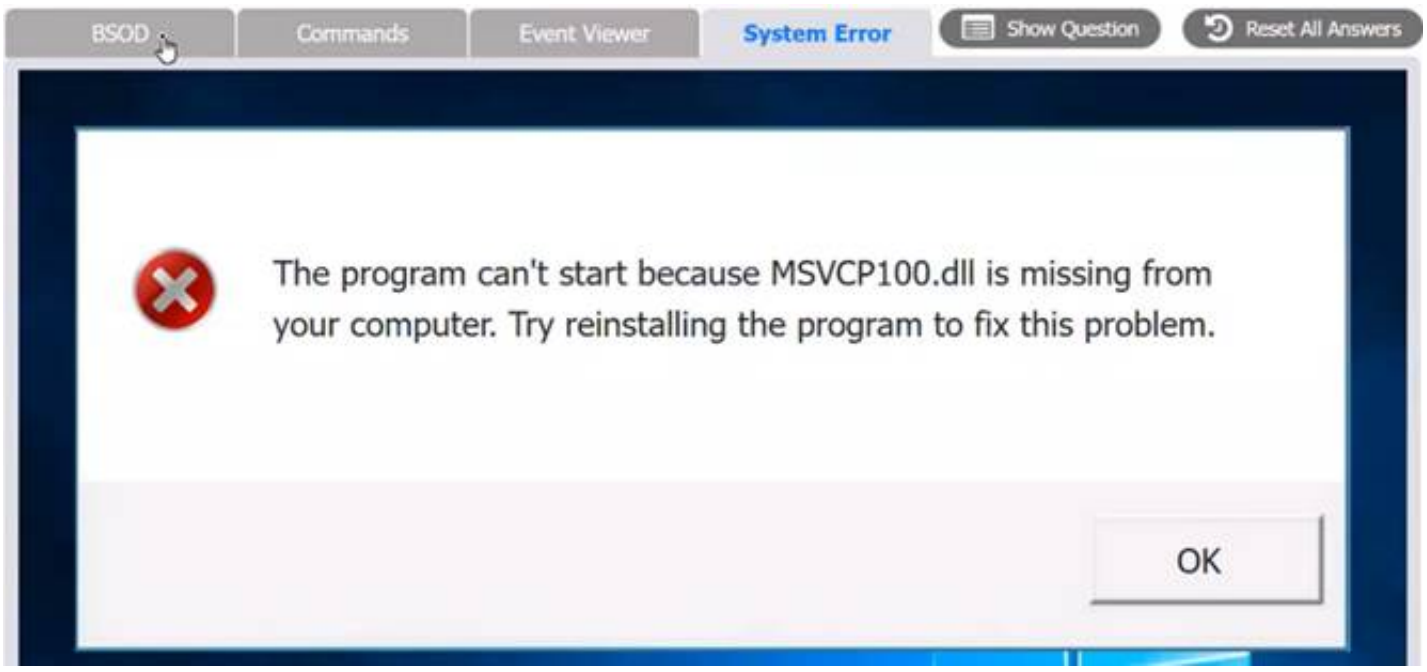
Commands:

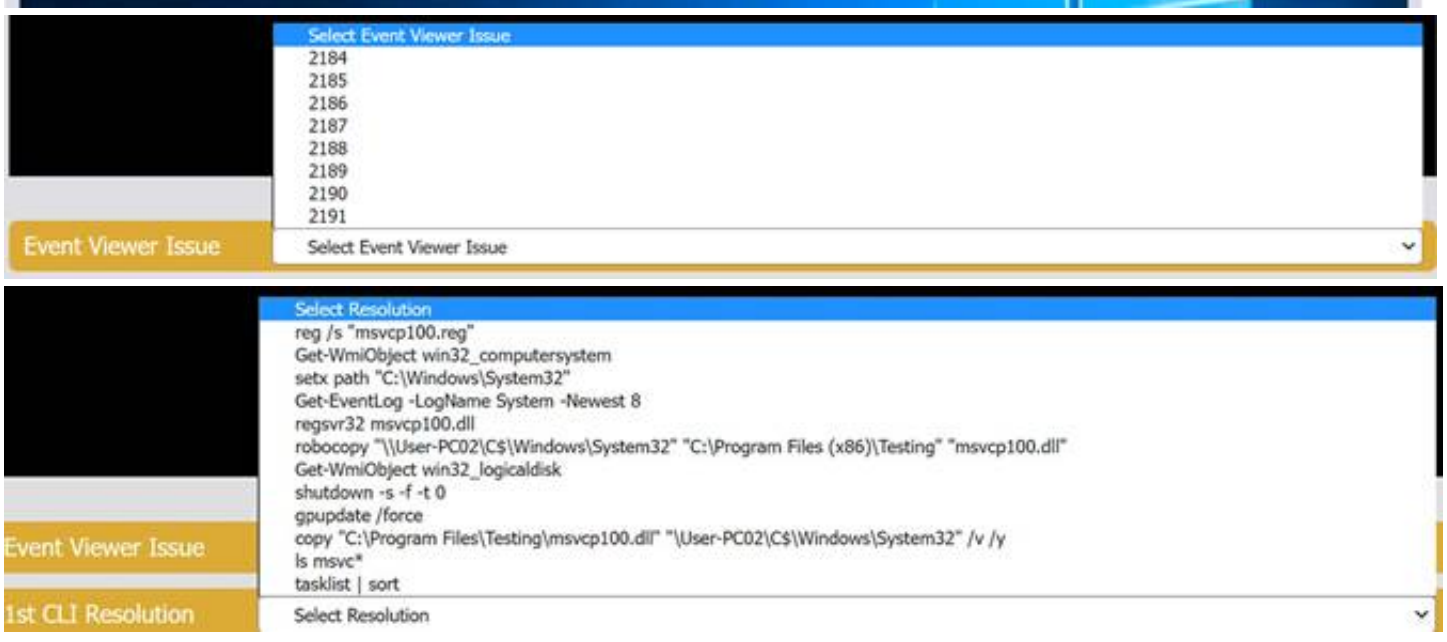


Event Viewer:



System Error:

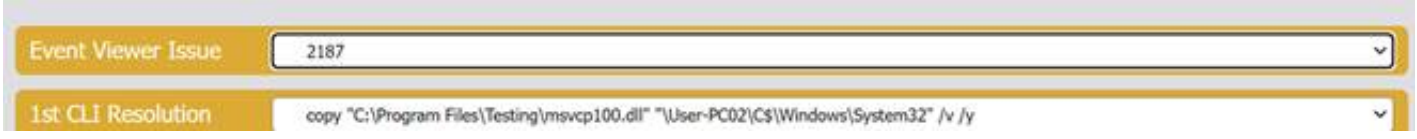




A. Mastered
B. Not Mastered

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 114
A company is looking lot a solution that provides a backup for all data on the system while providing the lowest impact to the network. Which of the following backup types will the company MOST likely select?

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

Answer: B

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

NEW QUESTION 119
A help desk technician needs to remotely access and control a customer's Windows PC by using a secure session that allows the technician the same control as the customer. Which of the following tools provides this type of access?

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

Answer: B

Explanation:
RDP stands for Remote Desktop Protocol, which is a proprietary protocol developed by Microsoft that allows a user to remotely access and control another computer over a network. RDP provides a secure session that encrypts the data between the client and the host, and allows the user to see and interact with the desktop and applications of the remote computer as if they were sitting in front of it. RDP also supports features such as audio, video, clipboard, printer, and file sharing, as well as multiple monitor support and session recording. To use RDP, the host computer must have Remote Desktop enabled and configured, and the client computer must have a Remote Desktop client software installed. The client can connect to the host by entering its IP address, hostname, or domain name, and providing the login credentials of a user account on the host. RDP is commonly used for remote administration, technical support, and remote work scenarios

NEW QUESTION 120
A desktop technician has received reports that a user's PC is slow to load programs and saved files. The technician investigates and discovers an older HDD with adequate free space. Which of the following should the technician use to alleviate the issue first?

A. Disk Management
B. Disk Defragment
C. Disk Cleanup
D. Device Manager

Answer: B

Explanation:
Disk Defragment is a tool that can be used to improve the performance of a hard disk drive (HDD). HDDs store data in sectors and clusters on spinning platters. Over time, as data is written, deleted, and moved, the data may become fragmented, meaning that it is spread across different locations on the disk. This causes the HDD to take longer to access and load data, resulting in slower performance. Disk Defragment consolidates the fragmented data and rearranges it in a contiguous manner, which reduces the seek time and increases the speed of the HDD. Disk Management, Disk Cleanup, and Device Manager are not tools that can alleviate the issue of slow HDD performance.

NEW QUESTION 124
A technician is troubleshooting application crashes on a Windows workstation. Each time the workstation user tries to open a website in a browser, the following message is displayed:
crypt32.d11 is missing not found
Which of the following should the technician attempt FIRST?

A. Rebuild Windows profiles.
B. Reimage the workstation
C. Roll back updates
D. Perform a system file check

Answer: D

Explanation:
If this file is missing or corrupted, it can cause application crashes or errors when trying to open websites in a browser. To fix this, the technician can perform a system file check, which is a utility that scans and repairs corrupted or missing system files1. To perform a system file check, the technician can follow these steps:
? Open the Command Prompt as an administrator. To do this, type cmd in the
search box on the taskbar, right-click on Command Prompt, and select Run as administrator.
? In the Command Prompt window, type sfc /scannow and hit Enter. This will start
the scanning and repairing process, which may take some time.
? Wait for the process to complete. If any problems are found and fixed, you will see a message saying Windows Resource Protection found corrupt files and successfully repaired them. If no problems are found, you will see a message saying Windows Resource Protection did not find any integrity violations.
? Restart your computer and check if the issue is resolved.

NEW QUESTION 125
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:
The best course of action for the technician is to restore the defaults and reimage the corporate OS on the device. This will remove the jailbreak and any unauthorized or malicious apps that may have been installed on the device, as well as restore the security features and policies that the company has set for its devices. This will also ensure that the device can receive the latest updates and patches from the manufacturer and the company, and prevent any data leakage or compromise from the device.
Jailbreaking is a process of bypassing the built-in security features of a device to install software other than what the manufacturer has made available for that device1. Jailbreaking allows the device owner to gain full access to the root of the operating system and access all the features1. However, jailbreaking also exposes the device to various risks, such as:
? The loss of warranty from the device manufacturers2.
? Inability to update software until a jailbroken version becomes available2.
? Increased security vulnerabilities32.
? Decreased battery life2.
? Increased volatility of the device2.
Some of the signs of a jailbroken device are:
? A high number of ads, which may indicate the presence of adware or spyware on the device3.
? Receiving data-usage limit notifications, which may indicate the device is sending or receiving data in the background without the user's knowledge or consent3.
? Experiencing slow response, which may indicate the device is running unauthorized or malicious apps that consume resources or interfere with the normal functioning of the device3.
? Finding apps or icons that the user did not install or recognize, such as Cydia, which is a storefront for jailbroken iOS devices1.
The other options are not sufficient or appropriate for dealing with a jailbroken device. Running an antivirus and enabling encryption may not detect or remove all the threats or vulnerabilities that the jailbreak has introduced, and may not restore the device to its original state or functionality. Backing up the files and doing a system restore may not erase the jailbreak or the unauthorized apps, and may also backup the infected or compromised files. Undoing the jailbreak and enabling an antivirus may not be possible or effective, as the jailbreak may prevent the device from updating or installing security software, and may also leave traces of the jailbreak or the unauthorized apps on the device.
References:
? CompTIA A+ Certification Exam Core 2 Objectives4
? CompTIA A+ Core 2 (220-1102) Certification Study Guide5
? What is Jailbreaking & Is it safe? - Kaspersky1
? Is Jailbreaking Safe? The ethics, risks and rewards involved - Comparitech3
? Jailbreaking : Security risks and moving past them2

NEW QUESTION 130
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 134
A technician downloads a validated security tool and notes the vendor hash of a58e87a2. When the download is complete, the technician again validates the hash, but the value returns as 2a876a7d3. Which of the following is the MOST likely cause of the issue?

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

Answer: C

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

NEW QUESTION 137
Which of the following filesystems replaced FAT as the preferred filesystem for Microsoft Windows OS?

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

Answer: C

Explanation:
NTFS stands for New Technology File System and it is the preferred filesystem for Microsoft Windows OS since Windows NT 3.1 in 19931. NTFS replaced FAT (File Allocation Table) as the default filesystem for Windows because it offers many advantages over FAT, such as:
? Support for larger volumes and files (up to 16 exabytes)2
? Support for file compression, encryption, and permissions2
? Support for journaling, which records changes to the filesystem and helps recover from errors2
? Support for hard links, symbolic links, and mount points2
? Support for long filenames and Unicode characters2
FAT32 is an improved version of FAT that supports larger volumes and files (up to 32 GB and 4 GB respectively) and is compatible with older versions of Windows and other operating systems3. However, FAT32 still has many limitations and drawbacks compared to NTFS, such as:
? No support for file compression, encryption, and permissions3
? No support for journaling, which makes it vulnerable to corruption and data loss3
? No support for hard links, symbolic links, and mount points3
? No support for long filenames and Unicode characters3
APFS (Apple File System) is the default filesystem for macOS, iOS, iPadOS, watchOS, and tvOS since 20174. APFS replaced HFS+ (Hierarchical File System Plus) as the preferred filesystem for Apple devices because it offers many advantages over HFS+, such as:
? Support for larger volumes and files (up to 8 zettabytes)4
? Support for file cloning, snapshots, and encryption4
? Support for space sharing, which allows multiple volumes to share the same storage pool4
? Support for fast directory sizing, which improves performance and efficiency4 ext4 (Fourth Extended Filesystem) is the default filesystem for most Linux distributions since 20085. ext4 replaced ext3 as the preferred filesystem for Linux because it offers many advantages over ext3, such as:
? Support for larger volumes and files (up to 1 exabyte and 16 terabytes respectively)5
? Support for extents, which reduce fragmentation and improve performance5
? Support for journal checksumming, which improves reliability and reduces recovery time5
? Support for delayed allocation, which improves efficiency and reduces metadata overhead5
References:
1: NTFS - Wikipedia 2: [NTFS vs FAT32 vs exFAT: What's the Difference?] 3: [FAT32 - Wikipedia] 4: [Apple File System - Wikipedia] 5: [ext4 - Wikipedia] : NTFS vs FAT32 vs exFAT: What's the Difference? : FAT32 - Wikipedia : Apple File System - Wikipedia : ext4 - Wikipedia

NEW QUESTION 140
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 142
A user calls the help desk to report that none of the files on a PC will open. The user also indicates a program on the desktop is requesting payment in exchange for file access A technician verifies the user's PC is infected with ransorrrware. Which of the following should the technician do FIRST?

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

Answer: C

Explanation:
The technician should quarantine the system first1 Reference:
CompTIA A+ Certification Exam: Core 2 Objectives Version 4.0. Retrieved from https://partners.comptia.org/docs/default-source/resources/comptia-a-220-1102-exam- objectives-(3-0)

NEW QUESTION 147
A company is deploying mobile phones on a one-to-one basis, but the IT manager is concerned that users will root/jailbreak their phones. Which of the following technologies can be implemented to prevent this issue?

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

Answer: D

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

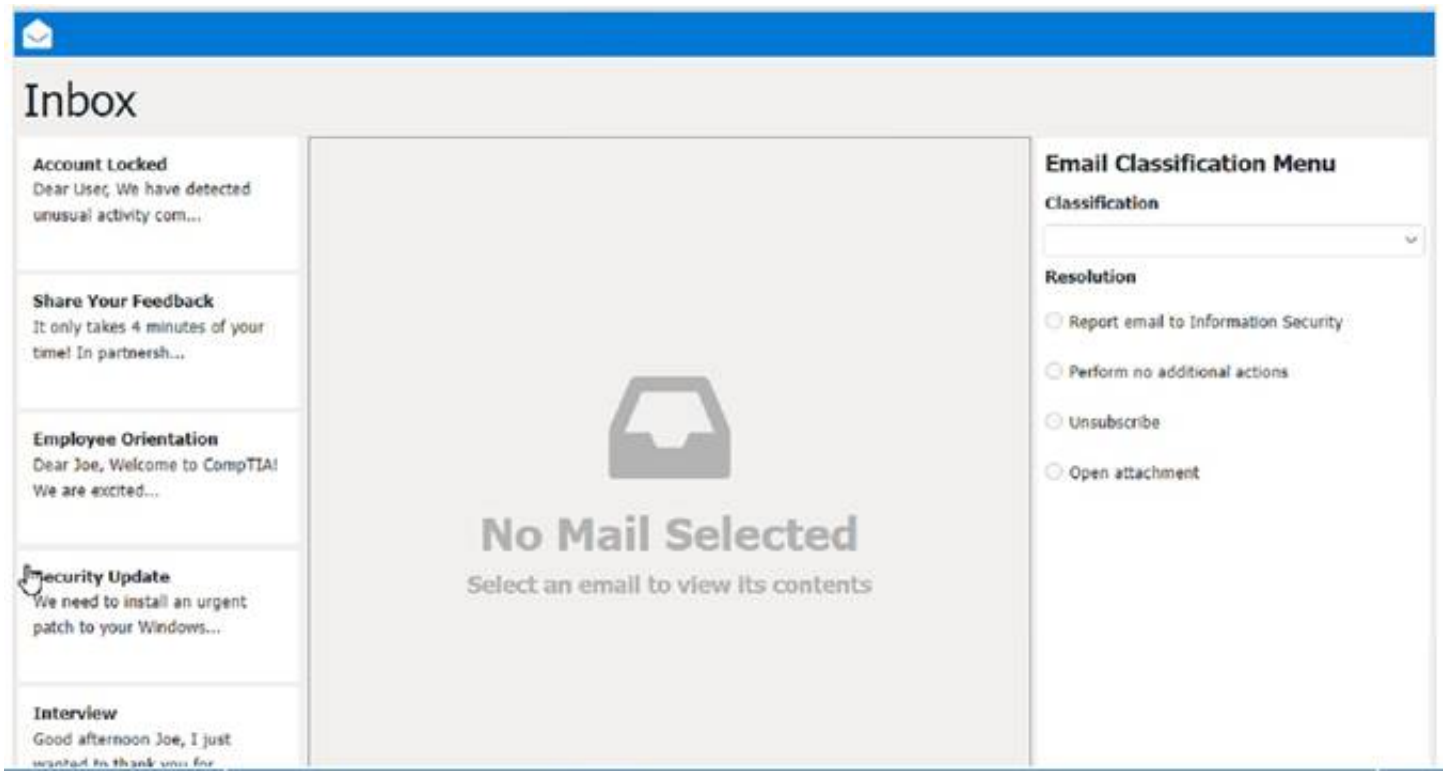
NEW QUESTION 148
A homeowner recently moved and requires a new router for the new ISP to function correctly. The internet service has been installed and has been confirmed as functional. Which of the following is the FIRST step the homeowner should take after installation of all relevant cabling and hardware?

A. Convert the PC from a DHCP assignment to a static IP address.
B. Run a speed test to ensure the advertised speeds are met.
C. Test all network sharing and printing functionality the customer uses.
D. Change the default passwords on new network devices.

Answer: D

Explanation:
When a homeowner moves and sets up a new router for the new ISP it is important to take appropriate security measures to protect their network from potential security threats. The FIRST step that the homeowner should take after installation of all relevant cabling and hardware is to change the default passwords on new network devices. Most modern routers come with default usernames and passwords that are widely known to potential attackers. If these defaults are not changed, it could make it easier for external attackers to gain unauthorized access to the network. Changing the passwords on new network devices is a simple but effective way to improve the security posture of the network.

NEW QUESTION 152
SIMULATION
As a corporate technician, you are asked to evaluate several suspect email messages on a client's computer. Corporate policy requires he following:
. All phishing attempts must be reported.
. Future spam emails to users must be prevented. INSTRUCTIONS
Review each email and perform the following within the email:
. Classify the emails
. Identify suspicious items, if applicable, in each email
. Select the appropriate resolution



Answer:

See the Full solution in Explanation below.

A. Mastered

B. Not Mastered

Answer: A

Explanation:

Classification: a) Phishing

This email is a phishing attempt, as it tries to trick the user into clicking on a malicious link that could compromise their account or personal information. Some suspicious items in this email are:

? The email has a generic greeting and does not address the user by name.

? The email has spelling errors, such as “unusal” and “Locaked”.

? The email uses a sense of urgency and fear to pressure the user into clicking on the link.

? The email does not match the official format or domain of the IT Help Desk at CompTIA.

? The email has two black bat icons, which are not related to CompTIA or IT support.

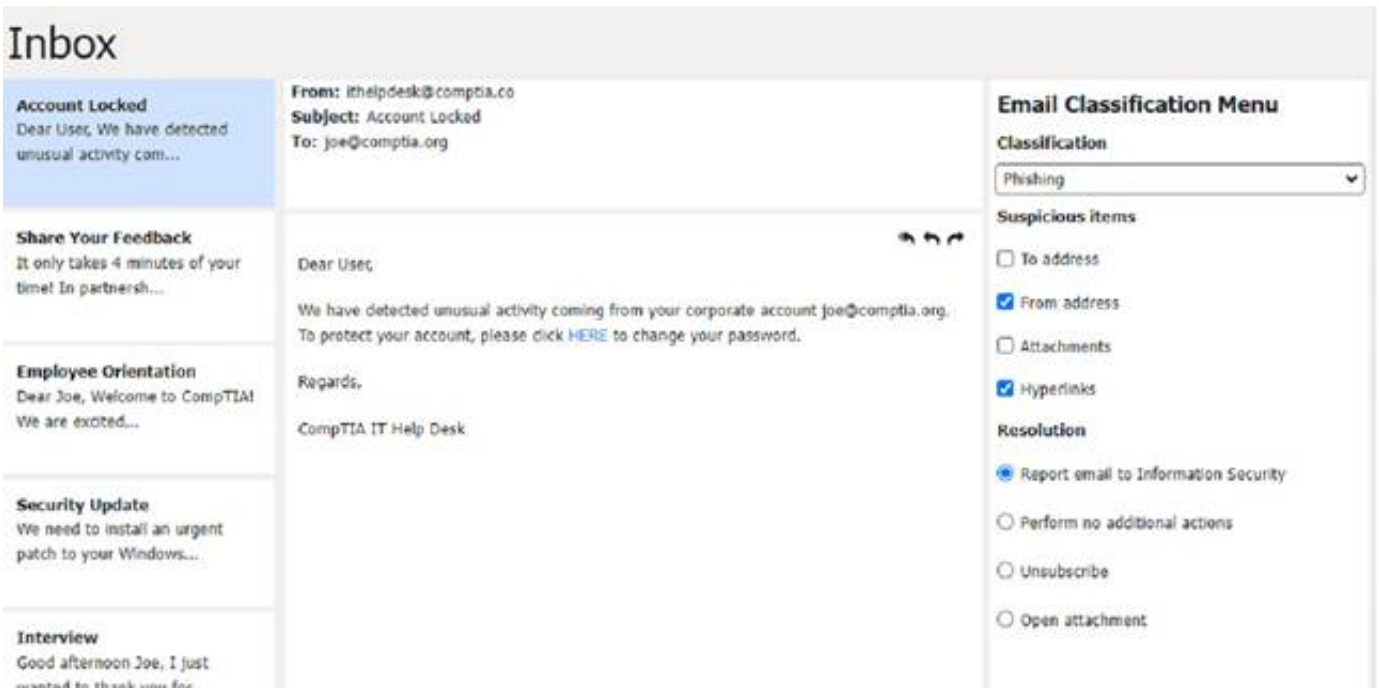
The appropriate resolution for this email is A. Report email to Information Security. The user should not click on the link, reply to the email, or provide any personal or account information. The user should forward the email to the Information Security team or use a professional email form to report the phishing attempt. The user should also delete the email from their inbox and trash folder.

The suspicious items to select are:

? b) From address

? d) Hyperlinks

These items indicate that the email is not from a legitimate source and that the link is potentially malicious. The other items are not suspicious in this case, as the to address is the user’s own email and there are no attachments.



Classification: b) Spam

This email is a spam email, as it is an unsolicited and unwanted message that tries to persuade the user to participate in a survey and claim a reward. Some suspicious items in this email are:

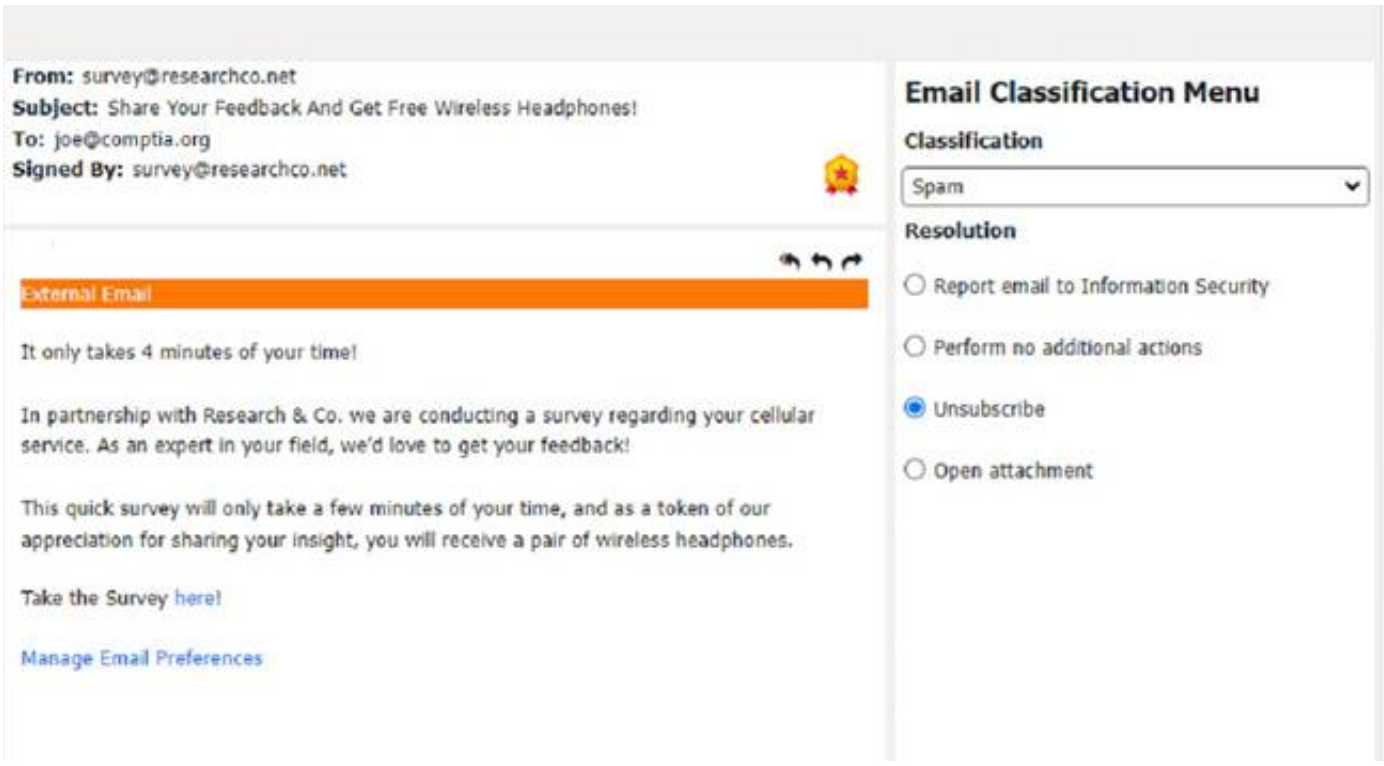
? The email offers a free wireless headphone as an incentive, which is too good to be true.

? The email does not provide any details about the survey company, such as its name, address, or contact information.

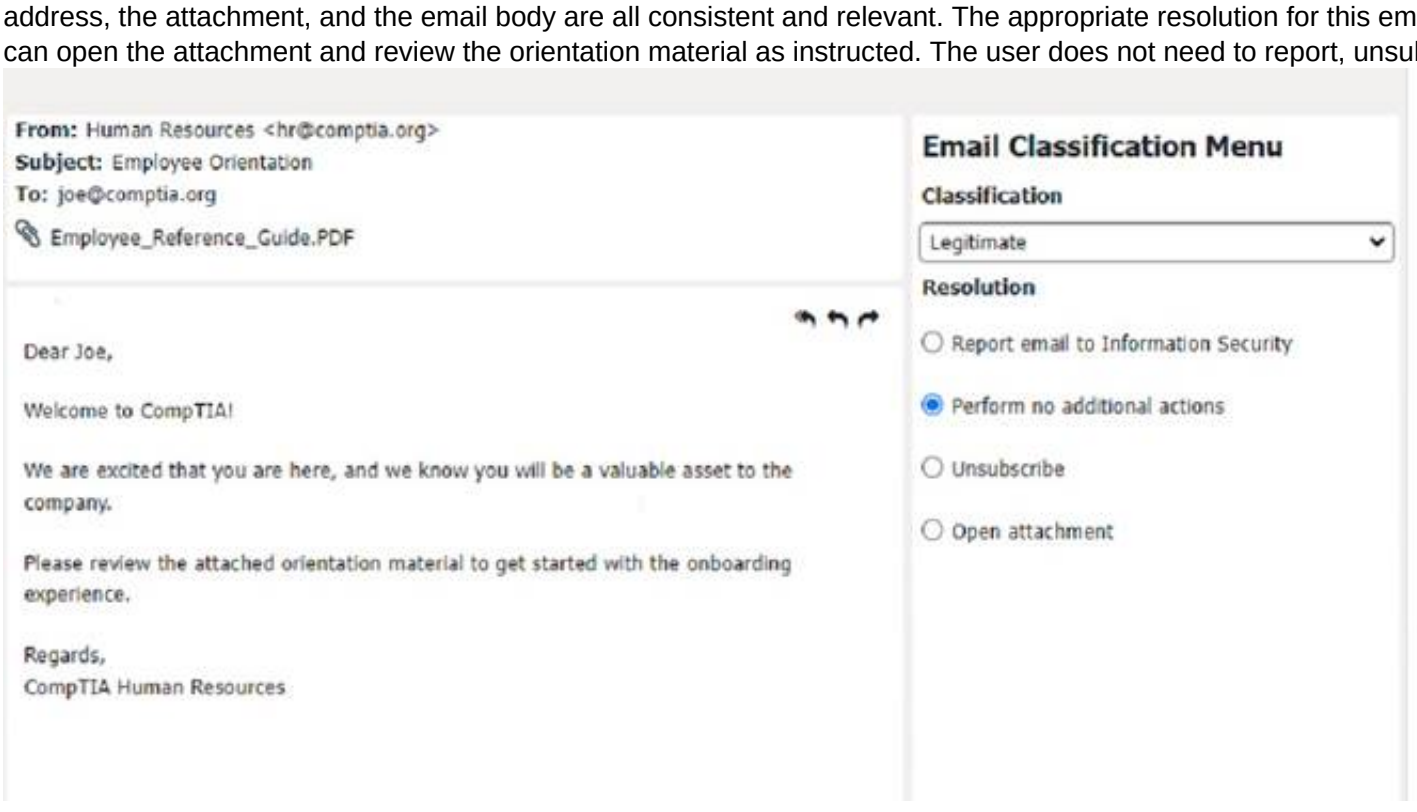
? The email contains an external survey link, which may lead to a malicious or fraudulent website.

? The email does not have an unsubscribe option, which is required by law for commercial emails.

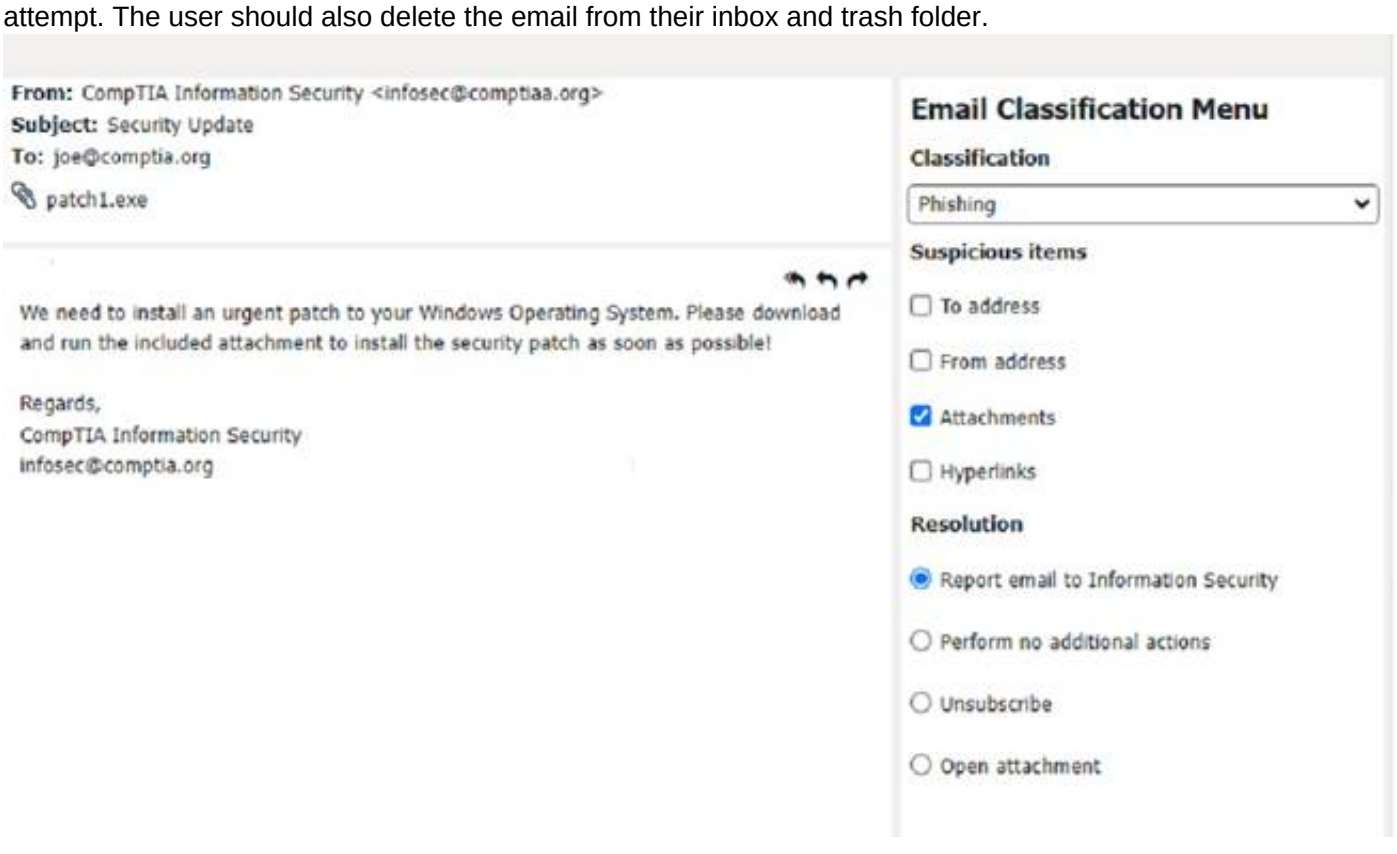
The appropriate resolution for this email is C. Unsubscribe. The user should look for an unsubscribe link or button at the bottom of the email and follow the instructions to opt out of receiving future emails from the sender. The user should also mark the email as spam or junk in their email client, which will help filter out similar emails in the future. The user should not click on the survey link, reply to the email, or provide any personal or financial information.



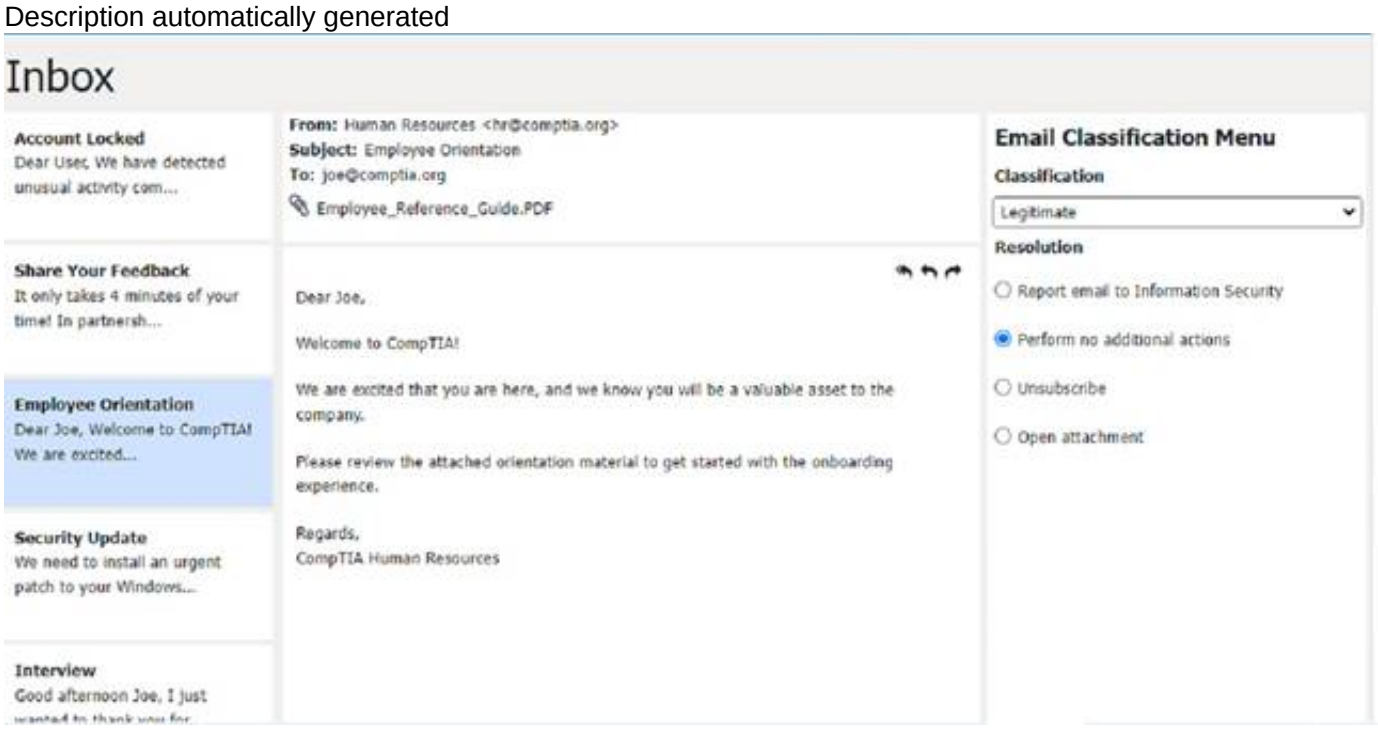
Classification: c) Legitimate
This email is a legitimate email, as it is from a trusted source and has a valid purpose. There are no suspicious items in this email, as the from address, the to address, the attachment, and the email body are all consistent and relevant. The appropriate resolution for this email is B. Perform no additional actions. The user can open the attachment and review the orientation material as instructed. The user does not need to report, unsubscribe, or delete this email.



A screenshot of a computer
Description automatically generated
Classification: a) Phishing
This email is a phishing attempt, as it tries to deceive the user into downloading and running a malicious attachment that could compromise their system or data. Some suspicious items in this email are:
? The email has a generic greeting and does not address the user by name or
username.
? The email has an urgent tone and claims that a security patch needs to be installed immediately.
? The email has an attachment named “patch1.exe”, which is an executable file that could contain malware or ransomware.
? The email does not match the official format or domain of CompTIA Information Security.
The appropriate resolution for this email is A. Report email to Information Security. The user should not open the attachment, reply to the email, or provide any personal or account information. The user should forward the email to the Information Security team or use a professional email form to report the phishing attempt. The user should also delete the email from their inbox and trash folder.



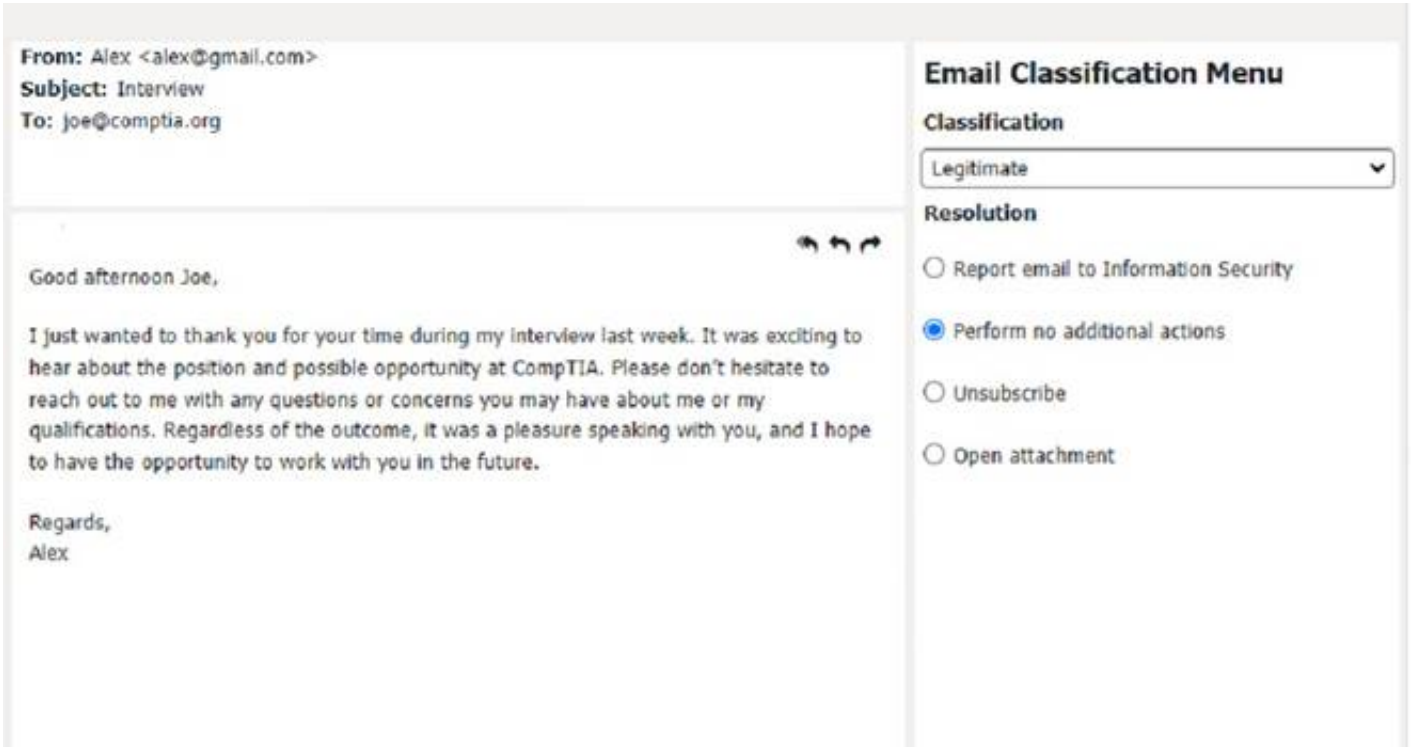
A screenshot of a computer
Description automatically generated



Classification: c) Legitimate

This email is a legitimate email, as it is from a trusted source and has a valid purpose. There are no suspicious items in this email, as the from address, the to address, and the email body are all consistent and relevant. The appropriate resolution for this email is B.

Perform no additional actions. The user can reply to the email and thank the sender for the interview opportunity. The user does not need to report, unsubscribe, or delete this email.



A screenshot of a computer
Description automatically generated

NEW QUESTION 153
A company is experiencing a DDoS attack. Several internal workstations are the source of the traffic. Which of the following types of infections are the workstations most likely experiencing? (Select two).

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

Answer: AD

Explanation:
Zombies and botnets are terms that describe the types of infections that can cause internal workstations to participate in a DDoS (distributed denial-of-service) attack. A DDoS attack is a malicious attempt to disrupt the normal functioning of a website or a network by overwhelming it with a large amount of traffic from multiple sources. Zombies are infected computers that are remotely controlled by hackers without the owners' knowledge or consent. Botnets are networks of zombies that are coordinated by hackers to launch DDoS attacks or other malicious activities. Keylogger, adware, ransomware, and spyware are not types of infections that can cause internal workstations to participate in a DDoS attack.

NEW QUESTION 154
Which of the following is MOST likely used to run .vbs files on Windows devices?

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

Answer: C

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

NEW QUESTION 159
A team of support agents will be using their workstations to store credit card data. Which of the following should the IT department enable on the workstations in order to remain compliant with common regulatory controls? (Select TWO).

A. Encryption
B. Antivirus
C. AutoRun
D. Guest accounts
E. Default passwords
F. Backups

Answer: AF

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

NEW QUESTION 160
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 165
A user reported that a laptop's screen turns off very quickly after silting for a few moments and is also very dim when not plugged in to an outlet Everything else seems to be functioning normally. Which of the following Windows settings should be configured?

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

Answer: A

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

NEW QUESTION 167
A new employee was hired recently. Which of the following documents will the new employee need to sign before being granted login access to the network?

A. Mastered
B. Not Mastered

Answer: A

Explanation:
A new employee will need to sign an AUP before being granted login access to the network. An AUP is an Acceptable Use Policy that defines the rules and guidelines for using network resources and services in an organization. An AUP typically covers topics such as security, privacy, ethics, compliance and liability issues related to network usage. An AUP helps protect the organization and its users from legal, regulatory and reputational risks associated with network activities. An MSDS is a Material Safety Data Sheet that provides information about hazardous substances and how to handle them safely. An MSDS is not related to network access or usage. A EULA is an End User License Agreement that specifies the terms and conditions for using a software product or service. A EULA is usually provided by software vendors or developers and does not apply to network access or usage in general. A UAC is a User Account Control that is a security feature that prompts users for permission or confirmation before performing certain actions that require elevated privileges or affect system settings. A UAC is not

a document that needs to be signed by users but a mechanism that helps prevent unauthorized changes or malware infections on a system. References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 5.1

NEW QUESTION 168
A user recently purchased a second monitor and wants to extend the Windows desktop to the new screen. Which of the following Control Panel options should a technician adjust to help the user?

A. Color Management
B. System
C. Troubleshooting
D. Device Manager
E. Administrative Tools

Answer: D

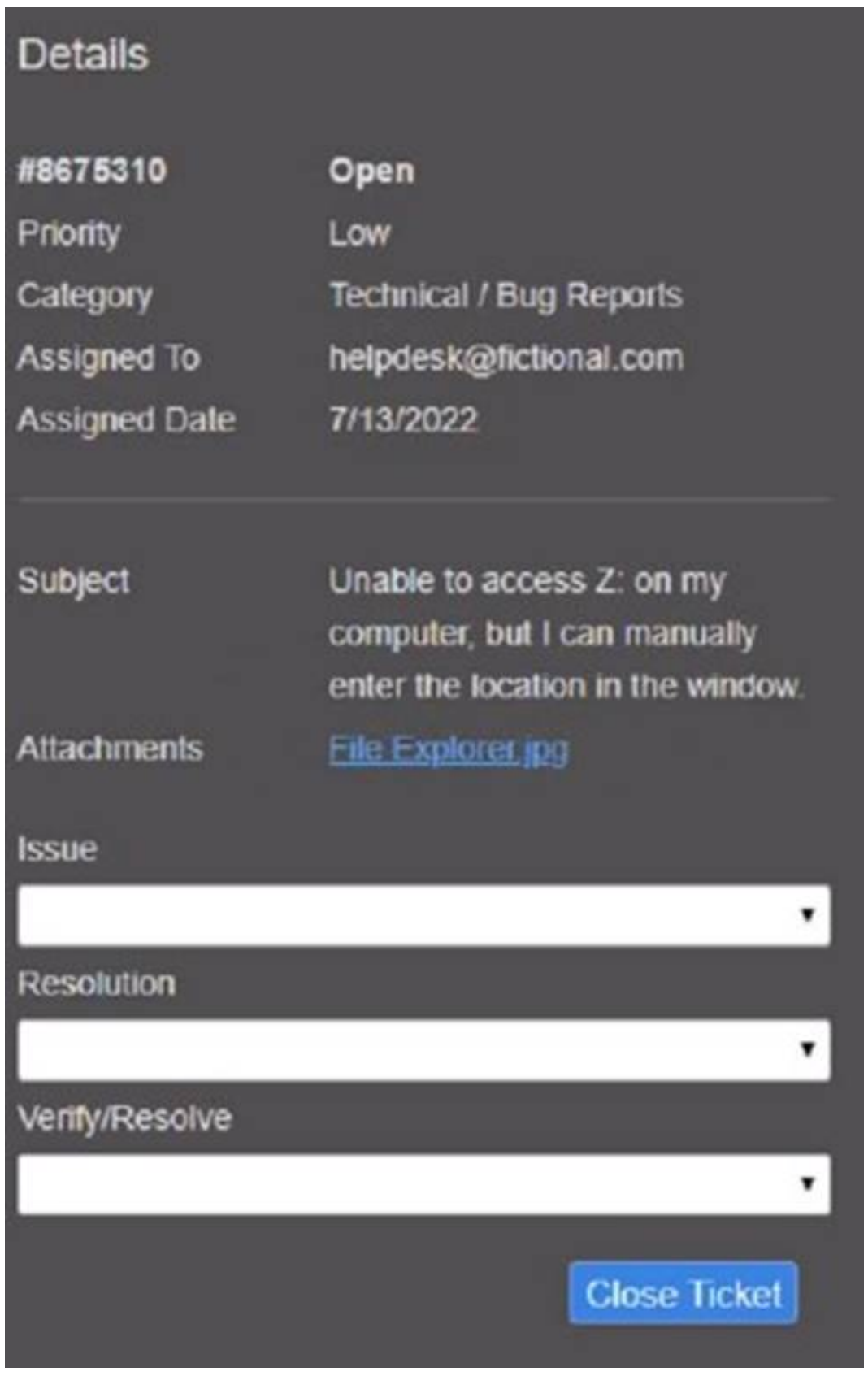
NEW QUESTION 173
A help desk technician determines a motherboard has failed. Which of the following is the most logical next step in the remediation process?

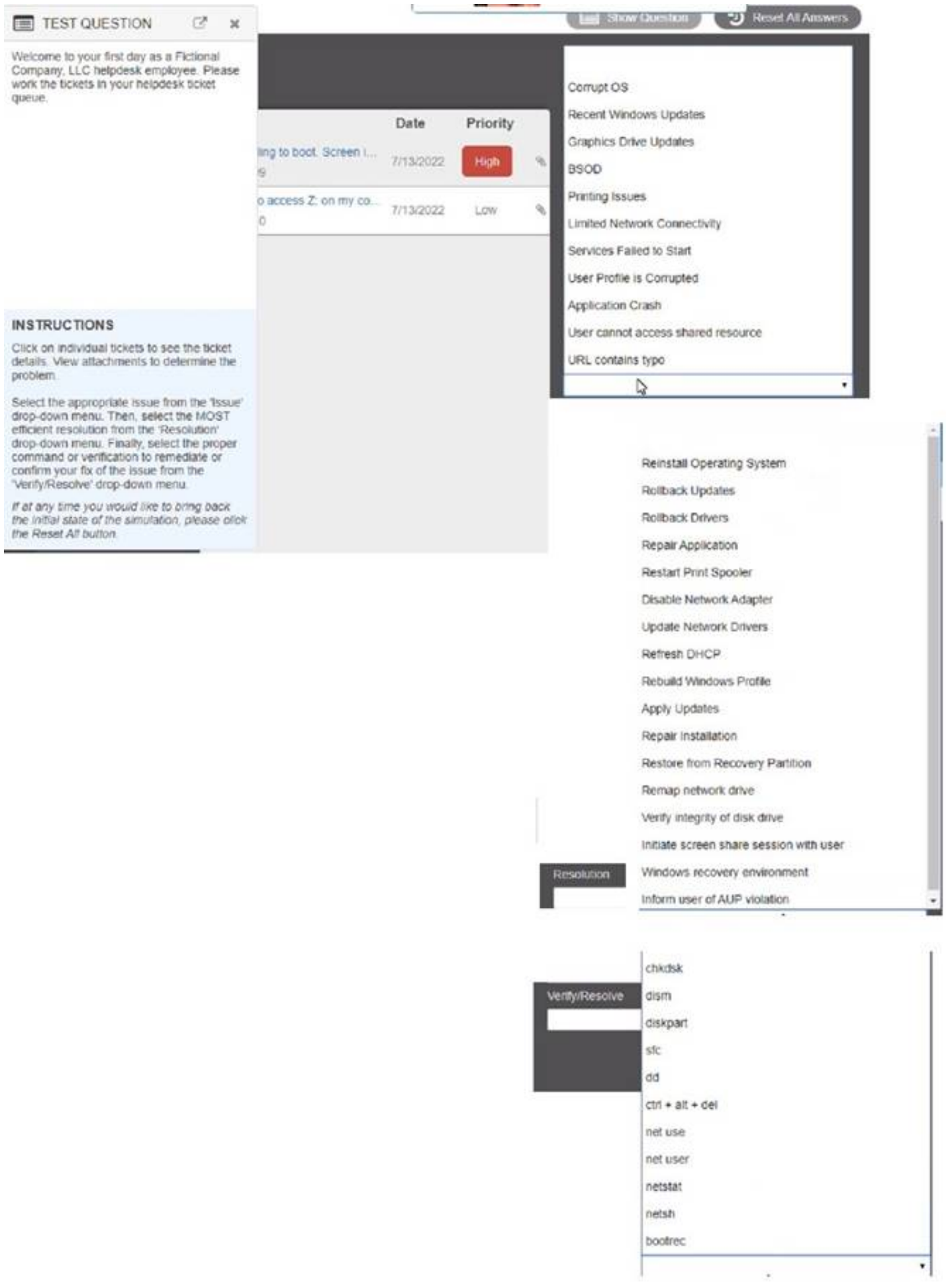
A. Escalating the issue to Tier 2
B. Verifying warranty status with the vendor
C. Replacing the motherboard
D. Purchasing another PC

Answer: B

Explanation:
Verifying warranty status with the vendor is the most logical next step in the remediation process after determining that a motherboard has failed. A warranty is a guarantee from the vendor that covers the repair or replacement of defective or faulty products within a specified period of time. Verifying warranty status with the vendor can help the technician determine if the motherboard is eligible for warranty service and what steps to take to obtain it. Escalating the issue to Tier 2, replacing the motherboard, and purchasing another PC are not the most logical next steps in the remediation process.

NEW QUESTION 177
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.

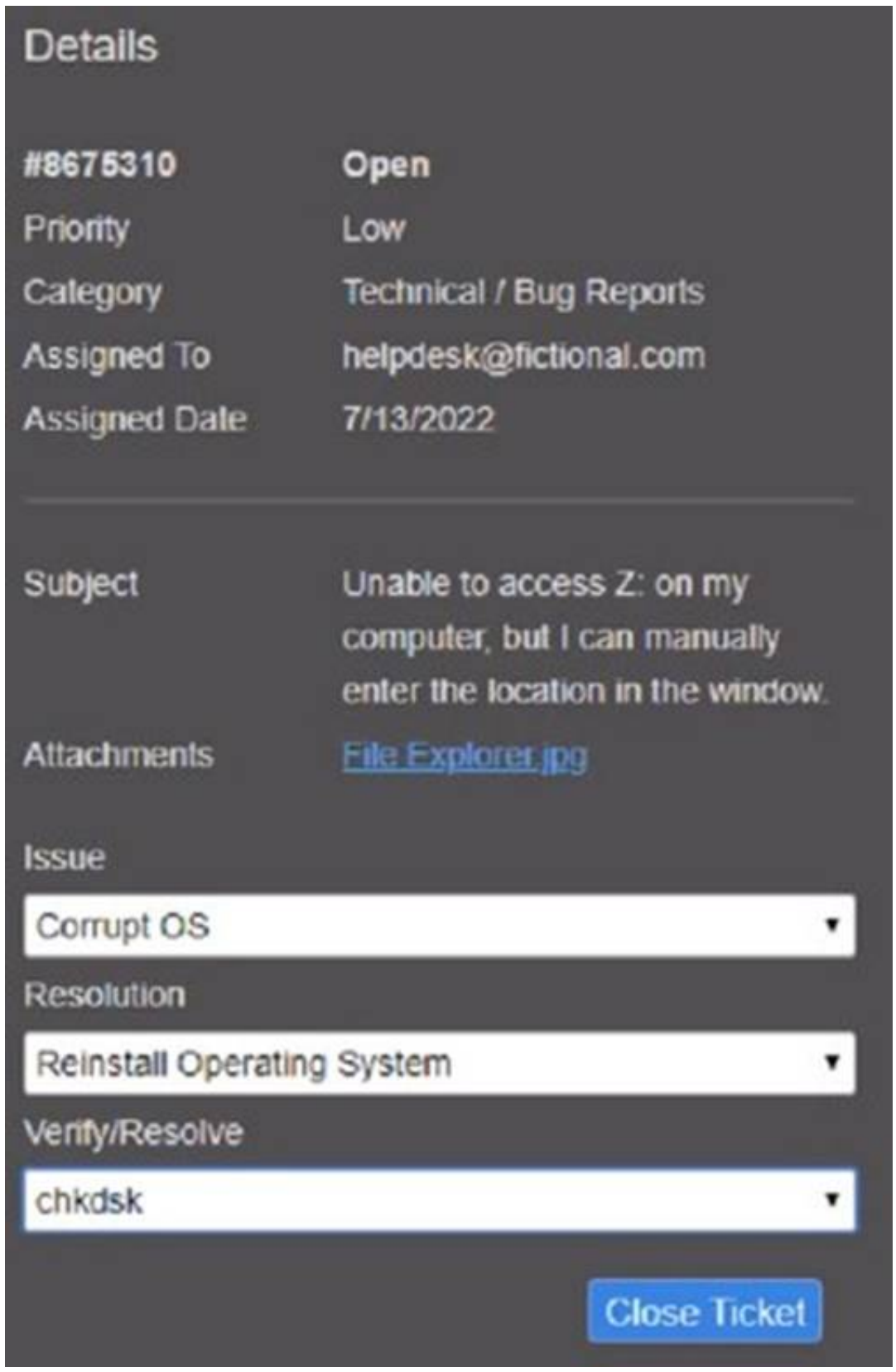

Details
#8675310
Open
Priority
Low
Category
Technical / Bug Reports
Assigned To
helpdesk@fictional.com
Assigned Date
7/13/2022
Subject
Unable to access Z: on my computer, but I can manually enter the location in the window.
Attachments
File Explorer.jpg
Issue
Resolution
Verify/Resolve
Close Ticket



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 179
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 182
A user visits a game vendor's website to view the latest patch notes, but this information is not available on the page. Which of the following should the user perform before reloading the page?

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

Answer: D

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

NEW QUESTION 184
Which of the following options should MOST likely be considered when preserving data from a hard drive for forensic analysis? (Select TWO).

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

Answer: B

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

NEW QUESTION 189
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 has taken the appropriate action by not taking the call and setting the phone to silent in order to avoid any distractions and remain focused on the task at hand. This is a good example of how to maintain focus and productivity when working on a customer's PC, and will help to ensure that the job is completed in a timely and efficient manner.

NEW QUESTION 191
A user's computer unexpectedly shut down immediately after the user plugged in a USB headset. Once the user turned the computer back on, everything was functioning properly, including the headset. Which of the following Microsoft tools would most likely be used to determine the root cause?

A. Event Viewer
B. System Configuration
C. Device Manager
D. Performance Monitor

Answer: A

Explanation:
Event Viewer is a Microsoft tool that records and displays system events, errors, warnings, and information. Event Viewer can help troubleshoot and diagnose problems, such as unexpected shutdowns, by showing the details of what happened before, during, and after the incident. Event Viewer can also show the source such as an application, a service, a driver, or a hardware device. By using Event Viewer, a technician can identify the root of the event
cause of the unexpected shutdown, such as a power failure, a thermal event, a driver conflict, or a malware infection.

NEW QUESTION 193
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 194
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 196
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 199
A user contacts a technician about an issue with a laptop. The user states applications open without being launched and the browser redirects when trying to go to certain websites. Which of the following is MOST likely the cause of the user's issue?

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

Answer: D

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

NEW QUESTION 201
A technician, who is working at a local office, has found multiple copies of home edition software installed on computers. Which of the following does this MOST likely violate?

A. EULA
B. Pll
C. DRM
D. Open-source agreement

Answer: A

Explanation:
The installation of home edition software on computers at a local office most likely violates the EULA. EULA stands for End User License Agreement and is a legal contract that specifies the terms and conditions for using a software product or service. EULA typically covers topics such as license scope, duration and limitations, rights and obligations of the parties, warranties and disclaimers, liability and indemnity clauses, and termination procedures. EULA may also restrict the use of home edition software to personal or non- commercial purposes only, and prohibit the use of home edition software in business or professional settings. Violating EULA may result in legal actions or penalties from the software vendor or developer. PII stands for Personally Identifiable Information and is any

information that can be used to identify or locate an individual, such as name, address, phone number, email address, social security number or credit card number. PII is not related to software installation or licensing but to data protection and privacy. DRM stands for Digital Rights Management and is a technology that controls or restricts the access and use of digital content, such as music, movies, books or games. DRM is not related to software installation or licensing but to content distribution and piracy prevention. Open- source agreement is a type of license that allows users to access, modify and distribute the source code of a software product or service freely and openly. Open-source agreement does not restrict the use of software to home edition only but encourages collaboration and innovation among developers and users. References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 5.1

NEW QUESTION 204
A user reports a workstation has been performing strangely after a suspicious email was opened on it earlier in the week. Which of the following should the technician perform FIRST?

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 208
A user reports that the hard drive activity light on a Windows 10 desktop computer has been steadily lit for more than an hour, and performance is severely degraded. Which of the following tabs in Task Manager would contain the information a technician would use to identify the cause of this issue?

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

Answer: B

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

NEW QUESTION 213
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 216
A technician is unable to completely start up a system. The OS freezes when the desktop background appears, and the issue persists when the system is restarted. Which of the following should the technician do next to troubleshoot the issue?

A. Disable applicable BIOS options.
B. Load the system in safe mode.
C. Start up using a flash drive OS and run System Repair.
D. Enable Secure Boot and reinstall the system.

Answer: B

Explanation:
Loading the system in safe mode is a common troubleshooting step that allows the technician to isolate the problem by disabling unnecessary drivers and services. This can help determine if the issue is caused by a faulty device, a corrupted system file, or a malware infection.

NEW QUESTION 220
A Windows workstation that was recently updated with approved system patches shut down instead of restarting. Upon reboot, the technician notices an alert stating the workstation has malware in the root OS folder. The technician promptly performs a System Restore and reboots the workstation, but the malware is still detected. Which of the following BEST describes why the system still has malware?

A. A system patch disabled the antivirus protection and host firewall.
B. The system updates did not include the latest anti-malware definitions.

C. The system restore process was compromised by the malware.
D. The malware was installed before the system restore point was created.

Answer: D

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

NEW QUESTION 222
A technician is unable to access the internet or named network resources. The technician receives a valid IP address from the DHCP server and can ping the default gateway. Which of the following should the technician check next to resolve the issue?

A. Verify the DNS server settings.
B. Turn off the Windows firewall.
C. Confirm the subnet mask is correct.
D. Configure a static IP address.

Answer: A

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

NEW QUESTION 225
A technician is creating a location on a Windows workstation for a customer to store meeting minutes. Which of the following commands should the technician use?

A. c: \minutes
B. dir
C. rmdir
D. md

Answer: D

Explanation:
The command md stands for make directory and is used to create a new directory or folder in the current location. In this case, the technician can use md minutes to create a folder named minutes in the C: drive. The other commands are not relevant for this task. c: \minutes is not a command but a path to a folder. dir is used to display a list of files and folders in the current directory. rmdir is used to remove or delete an existing directory or folder.

NEW QUESTION 229
A technician is trying to connect to a user's laptop in order to securely install updates. Given the following information about the laptop:

Hostname:	corp-laptop-222
IP Address:	192.168.0.45
Gateway:	192.168.1.1
Subnet Mask:	255.255.252.0
Open Ports:	21, 22, 80, 443

Which of the following should the technician do to connect via RDP?

A. Confirm the user can ping the default gateway.
B. Change the IP address on the user's laptop.
C. Change the subnet mask on the user's laptop.
D. Open port 3389 on the Windows firewall.

Answer: D

Explanation:
In order to connect to a user's laptop via RDP, the technician should open port 3389 on the Windows firewall. This is because RDP uses port 3389 for communication12. The other options are not necessary or relevant for establishing an RDP connection.
? Confirming the user can ping the default gateway is not required for RDP, as it only tests the network connectivity between the user's laptop and the router. RDP works over the internet, so the technician should be able to ping the user's laptop directly using its IP address3.
? Changing the IP address on the user's laptop is not needed for RDP, as long as the IP address is valid and not conflicting with another device on the network. The user's laptop has a valid IP address of 192.168.0.45, which belongs to the

same subnet as the gateway (192.168.0.1) and the subnet mask (255.255.255.0)4.
? Changing the subnet mask on the user's laptop is not required for RDP, as long as
the subnet mask matches the network configuration. The user's laptop has a correct subnet mask of 255.255.255.0, which defines a network with 254 possible hosts4.
References:
1: [What is RDP and How Does It Work? - CompTIA] 2: CompTIA A+ Certification Exam Core 2 Objectives - CompTIA 3: [Ping (networking utility) - Wikipedia] 4: [IP address - Wikipedia] : What is RDP and How Does It Work? - CompTIA : CompTIA A+ Certification Exam Core 2 Objectives - CompTIA : Ping (networking utility) - Wikipedia) : IP address - Wikipedia

NEW QUESTION 234
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 235
A user's smartphone data usage is well above average. The user suspects an installed application is transmitting data in the background. The user would like to be alerted when an application attempts to communicate with the internet. Which of the following BEST addresses the user's concern?

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

Answer: D

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

NEW QUESTION 240
A technician is installing RAM in a new workstation and needs to protect against electrostatic discharge. Which of the following will best resolve this concern?

A. Battery backup
B. Thermal paste
C. ESD strap
D. Consistent power

Answer: C

Explanation:
An ESD strap, also known as an antistatic wrist strap, is a device that prevents electrostatic discharge (ESD) from damaging sensitive electronic components such as RAM. ESD is the sudden flow of electricity between two objects with different electrical charges, which can cause permanent damage or malfunction to electronic devices. An ESD strap connects the technician's wrist to a grounded surface, such as a metal case or a mat, and equalizes the electrical potential between the technician and the device. Battery backup, thermal paste, and consistent power are not devices that can protect against ESD.

NEW QUESTION 242
A technician is concerned about a large increase in the number of whaling attacks happening in the industry. The technician wants to limit the company's risk to avoid any issues. Which of the following items should the technician implement?

A. Screened subnet
B. Firewall
C. Anti-phishing training
D. Antivirus

Answer: C

Explanation:
Anti-phishing training is a method of educating users on how to identify and avoid phishing attacks, which are attempts to trick users into revealing sensitive information or performing malicious actions by impersonating legitimate entities or persons. Whaling attacks are a specific type of phishing attack that target high-level executives or influential individuals within an organization. Anti-phishing training can help users recognize the signs of whaling attacks and prevent them from falling victim to them. Screened subnet, firewall, and antivirus are not items that can directly address the issue of whaling attacks.

NEW QUESTION 246
A company is recycling old hard drives and wants to quickly reprovision the drives for reuse. Which of the following data destruction methods should the company use?

A. Degaussing
B. Standard formatting
C. Low-level wiping
D. Deleting

Answer: C

Explanation:
Low-level wiping is the best data destruction method for recycling old hard drives for reuse. Low-level wiping is a process that overwrites every bit of data on a hard drive with zeros or random patterns, making it impossible to recover any data from the drive. Low-level wiping also restores the drive to its factory state, removing any bad sectors or errors that may have accumulated over time. Low-level wiping can be done using specialized software tools or hardware devices that connect to the drive. Degaussing, standard formatting, and deleting are not suitable data destruction methods for recycling old hard drives for reuse. Degaussing is a process that exposes a hard drive to a strong magnetic field, destroying both the data and the drive itself. Degaussing renders the drive unusable for reuse. Standard formatting is a process that erases the data on a hard drive by removing the file system structure, but it does not overwrite the data itself. Standard formatting leaves some data recoverable using forensic tools or software utilities. Deleting is a process that removes the data from a hard drive by marking it as free space, but it does not erase or overwrite the data itself. Deleting leaves most data recoverable using undelete tools or software utilities.
References:
? Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 15
? CompTIA A+ Complete Study Guide: Core 1 Exam 220-1101 and Core 2 Exam …, page 105

NEW QUESTION 247
A systems administrator needs to reset a users password because the user forgot it. The systems administrator creates the new password and wants to further protect the user's account Which of the following should the systems administrator do?

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

Answer: A

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

NEW QUESTION 251
Which of the following must be maintained throughout the forensic evidence life cycle when dealing with a piece of evidence?

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

Answer: B

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

NEW QUESTION 253
A developer's Type 2 hypervisor is performing inadequately when compiling new source code. Which of the following components should the developer upgrade to improve the hypervisor’s performance?

A. Amount of system RAM
B. NIC performance
C. Storage IOPS
D. Dedicated GPU

Answer: A

Explanation:
The correct answer is A. Amount of system RAM. A Type 2 hypervisor is a virtualization software that runs on top of a host operating system, which means it shares the system resources with the host OS and other applications. Therefore, increasing the amount of system RAM can improve the performance of the hypervisor and the virtual machines running on it. RAM is used to store data and instructions that are frequently accessed by the CPU, and having more RAM can reduce the need for swapping data to and from the storage device, which is slower than RAM.
NIC performance, storage IOPS, and dedicated GPU are not as relevant for improving the hypervisor’s performance in this scenario. NIC performance refers to the speed and quality of the network interface card, which is used to connect the computer to a network. Storage IOPS refers to the number of input/output operations per second that can be performed by the storage device, which is a measure of its speed and efficiency. Dedicated GPU refers to a separate graphics processing unit that can handle complex graphics tasks, such as gaming or video editing. These components may affect other aspects of the computer’s performance, but they are not directly related to the hypervisor’s ability to compile new source code.

NEW QUESTION 256
A manager called the help desk to ask for assistance with creating a more secure environment for the finance department- which resides in a non-domain

environment. Which of the following would be the BEST method to protect against unauthorized use?

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

Answer: B

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

NEW QUESTION 259
A technician is setting up a desktop computer in a small office. The user will need to access files on a drive shared from another desktop on the network. Which of the following configurations should the technician employ to achieve this goal?

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

Answer: A

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

NEW QUESTION 262
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 267
A user reports that a workstation is operating sluggishly Several other users operate on the same workstation and have reported that the workstation is operating normally. The systems administrator has validated that the workstation functions normally. Which of the following steps should the systems administrator most likely attempt NEXT?

A. Increase the paging file size
B. Run the chkdsk command
C. Rebuild the user's profile
D. Add more system memory.
E. Defragment the hard drive.

Answer: C

Explanation:
Since the systems administrator has validated that the workstation functions normally and other users operate on the same workstation without any issues, the next step should be to rebuild the user’s profile. This will ensure that any corrupted files or settings are removed and the user’s profile is restored to its default state.

NEW QUESTION 272
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 273
A systems administrator is creating periodic backups of a folder on a Microsoft Windows machine. The source data is very dynamic, and files are either added or deleted regularly. Which of the following utilities can be used to 'mirror the source data for the backup?

A. copy
B. xcopy
C. robocopy
D. Copy-Item

Answer: C

Explanation:
Robocopy is a command-line utility that can be used to mirror the source data for the backup. It can copy files and folders with various options, such as copying only changed files, preserving attributes and permissions, and retrying failed copies. Robocopy is more powerful and flexible than copy or xcopy, which are simpler commands that can only copy files and folders without mirroring or other advanced features. Copy-Item is a PowerShell cmdlet that can also copy files and folders, but it is not a native Windows utility and it requires PowerShell to run1.
References: 1: https://windowsreport.com/mirror-backup-software/

NEW QUESTION 277
A technician is troubleshooting a PC that has been performing poorly. Looking at the Task Manager, the technician sees that CPU and memory resources seem fine, but disk throughput is at 100%.
Which of the following types of malware is the system MOST likely infected with?

A. Keylogger
B. Rootkit
C. Ransomware
D. Trojan

Answer: C

Explanation:
Ransomware is a type of malware that encrypts the files on the victim's computer and demands a ransom for their decryption. Ransomware can cause high disk throughput by encrypting large amounts of data in a short time.

NEW QUESTION 281
Which of the following protocols supports fast roaming between networks?

A. WEP
B. WPA
C. WPA2
D. LEAP
E. PEAP

Answer: B

Explanation:
WPA2 is the only protocol among the options that supports fast roaming between
networks. Fast roaming, also known as IEEE 802.11r or Fast BSS Transition (FT), enables a client device to roam quickly in environments implementing WPA2 Enterprise security, by ensuring that the client device does not need to re-authenticate to the RADIUS server
every time it roams from one access point to another1. WEP, WPA, LEAP, and PEAP do not support fast roaming and require the client device to perform the full authentication process every time it roams, which can cause delays and interruptions in the network service.
References:
? The Official CompTIA A+ Core 2 Study Guide2, page 263.
? WiFi Fast Roaming, Simplified3

NEW QUESTION 282
A mobile phone user has downloaded a new payment application that allows payments to be made with a mobile device. The user attempts to use the device at a payment terminal but is unable to do so successfully. The user contacts a help desk technician to report the issue. Which of the following should the technician confirm NEXT as part of the troubleshooting process?

A. If airplane mode is enabled
B: If Bluetooth is disabled
C. If NFC is enabled
D. If WiFi is enabled
E. If location services are disabled

Answer: C

Explanation:
NFC stands for Near Field Communication, and it is a wireless technology that allows your phone to act as a contactless payment device, among other things2. Payment applications that allow payments to be made with a mobile device usually rely on NFC to communicate with the payment terminal1. Therefore, if NFC is disabled on the phone, the payment will not work. To enable NFC on an Android phone, you need to follow these steps3:
? On your Android device, open the Settings app.
? Select Connected devices.
? Tap on Connection preferences.
? You should see the NFC option. Toggle it on.
The other options are not directly related to using a payment application with a mobile device. Airplane mode is a setting that disables all wireless communication on the phone, including NFC4, but it also affects calls, texts, and internet access. Bluetooth is a wireless technology that allows you to connect your phone with other devices such as headphones or speakers, but it is not used for contactless payments. Wi-Fi is a wireless technology that allows you to access the internet or a local network, but it is also not used for contactless payments. Location services are a feature that allows your phone to determine your geographic location

using GPS or other methods, but they are not required for contactless payments.

NEW QUESTION 284
A user wants to acquire antivirus software for a SOHO PC. A technician recommends a licensed software product, but the user does not want to pay for a license. Which of the following license types should the technician recommend?

A. Corporate
B. Open-source
C. Personal
D. Enterprise

Answer: B

Explanation:
Open-source software is software that has its source code available for anyone to inspect, modify, and distribute. Open-source software is usually free of charge and does not require a license to use. Some examples of open-source antivirus software are ClamAV, Comodo, and Immunet12. The other license types are either not free or not suitable for a SOHO PC. Corporate and enterprise licenses are designed for large-scale organizations and networks, and they usually require a subscription fee. Personal licenses are for individual users and may have limited features or support.
References: 1 What is Open Source Software? - Definition from Techopedia(https://www.tomsguide.com/us/best-antivirus,review-2588.html). 2 7 Best Lifetime License Antivirus Tools [2023 Guide] - Windows Report(https://windowsreport.com/antivirus-with-unlimited-validity/).

NEW QUESTION 288
.....

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

100% Actual & Verified — Instant Download, Please Click
Order The 220-1102 Practice Test Here