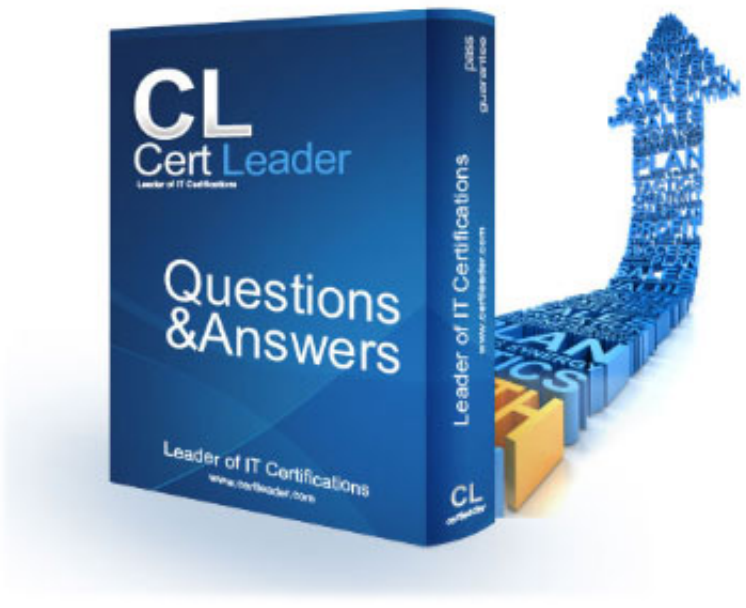
220-1102 Dumps

CompTIA A+ Certification Exam: Core 2

https://www.certleader.com/220-1102-dumps.html



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

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

Answer: C

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

NEW QUESTION 2
A 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.

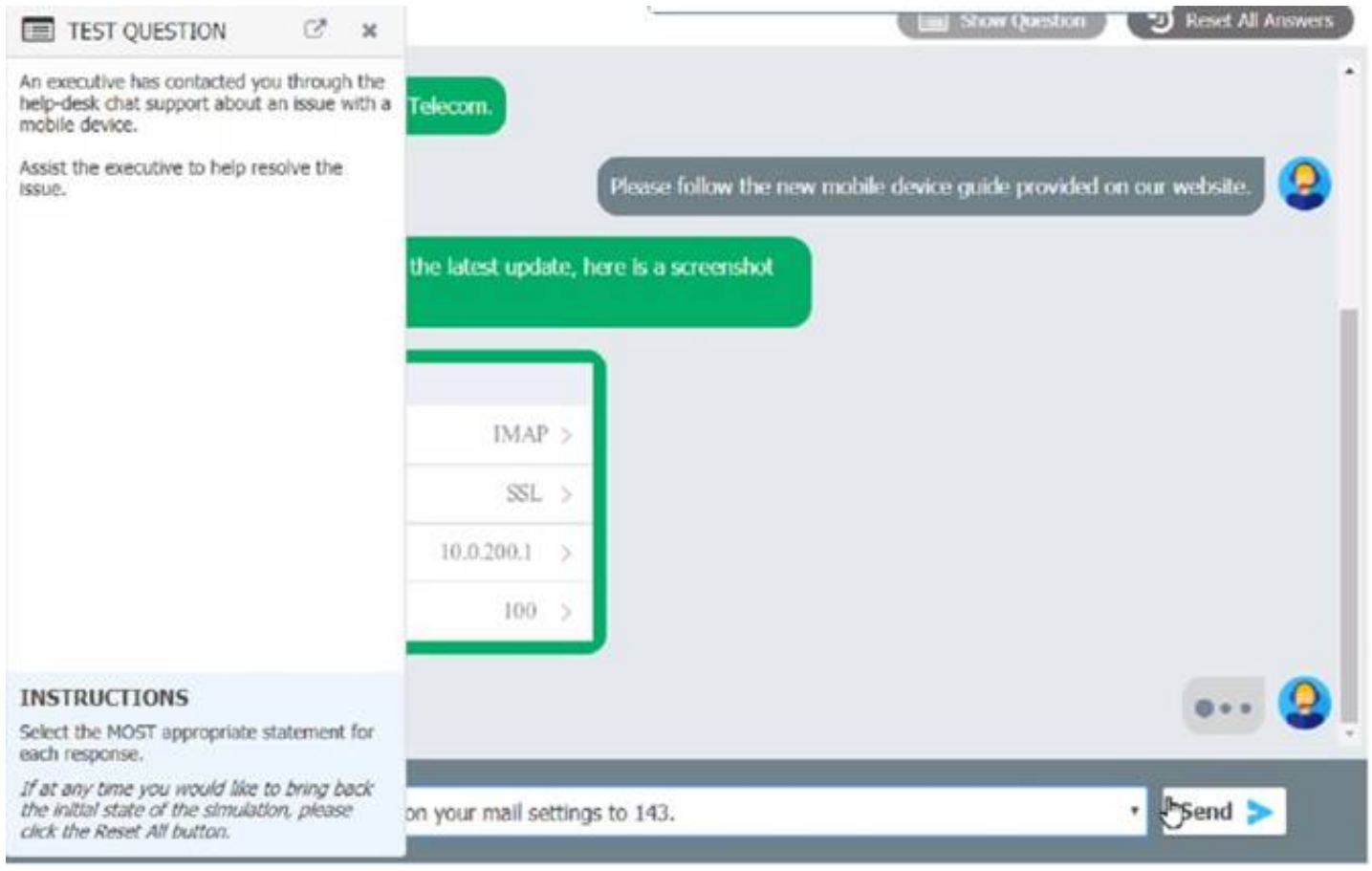
NEW QUESTION 3
Which of the following is the MOST basic version of Windows that includes BitLocker?

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 4
An executive has contacted you through the help-desk chat support about an issue with a mobile device.
Assist the executive to help resolve the issue.



Which of the following should be done NEXT?

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

Answer: A

NEW QUESTION 5
When trying to access a secure internal network, the user receives an error messaging stating, "There is a problem with this website's security certificate." The user reboots the desktop and tries to access the website again, but the issue persists. Which of the following should the user do to prevent this error from reoccurring?

A. Reimage the system and install SSL.
B. Install Trusted Root Certificate.
C. Select View Certificates and then Install Certificate.
D. Continue to access the website.

Answer: C

Explanation:
The error message indicates that the website's security certificate is not trusted by the user's device, which may prevent the user from accessing the secure internal network. To resolve this issue, the user can view the certificate details and install it on the device, which will add it to the trusted root certificate store. Reimaging the system and installing SSL, installing Trusted Root Certificate, or continuing to access the website are not recommended solutions, as they may compromise the security of the device or the network.

NEW QUESTION 6
A developer receives the following error while trying to install virtualization software on a workstation:
VTx not supported by system
Which of the following upgrades will MOST likely fix the issue?

A. Processor
B. Hard drive
C. Memory
D. Video card

Answer: A

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

NEW QUESTION 7
A systems administrator is monitoring an unusual amount of network traffic from a kiosk machine and needs to Investigate to determine the source of the traffic. Which of the following tools can the administrator use to view which processes on the kiosk machine are connecting to the internet?

A. Resource Monitor
B. Performance Monitor
C. Command Prompt
D. System Information

Answer: A

Explanation:
Resource Monitor is a tool that shows the network activity of each process on a Windows machine, including the TCP connections and the sent and received bytes. Performance Monitor is a tool that shows the performance metrics of the system, such as CPU, memory, disk and network usage. Command Prompt is a tool that allows running commands and scripts on a Windows machine. System Information is a tool that shows the hardware and software configuration of a Windows machine. Verified References:
https://www.comptia.org/blog/how-to-use-resource-monitor https://www.comptia.org/certifications/a

NEW QUESTION 8
A user reports that the pages flash on the screen two or three times before finally staying open when attempting to access banking web pages. Which of the following troubleshooting steps should the technician perform NEXT to resolve the issue?

A. Examine the antivirus logs.
B. Verify the address bar URL.
C. Test the internet connection speed.
D. Check the web service status.

Answer: B

Explanation:
The next troubleshooting step that the technician should perform to resolve the issue of pages flashing on the screen before staying open when accessing banking web pages is to verify the address bar URL. The address bar URL is the web address that appears in the browser's address bar and indicates the location of the web page being accessed. Verifying the address bar URL can help determine if the user is accessing a legitimate or malicious website, as some phishing websites may try to impersonate banking websites by using similar-looking URLs or domains.

NEW QUESTION 9
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 10
A hotel's Wi-Fi was used to steal information on a corporate laptop. A technician notes the following security log:
SRC: 192.168.1.1/secrets.zip Protocol SMB >> DST: 192.168.1.50/capture The technician analyses the following Windows firewall information:

Port	Status	Direction
1	Open	In/Out
445	Open	In/Out
25	Open	Out
110	Open	In/Out
53	Open	In/Out

Which of the following protocols most likely allowed the data theft to occur?

A. 1
B. 53
C. 110
D. 445

Answer: D

Explanation:
The protocol that most likely allowed the data theft to occur is SMB over TCP port 445. SMB is a network file sharing protocol that enables access to files, printers, and other resources on a network. Port 445 is used by SMB to communicate directly over TCP without the need for NetBIOS, which is an older and less secure protocol. The security log shows that the source IP address 192.168.1.1 sent a file named secrets.zip using SMB protocol to the destination IP address 192.168.1.50, which captured the file. The Windows firewall information shows that port 445 is enabled for inbound and outbound traffic, which means that it is not blocked by the firewall. Therefore, port 445 is the most likely port that was exploited by the attacker to steal the data from the corporate laptop.
References:
? SMB port number: Ports 445, 139, 138, and 137 explained1
? What is an SMB Port + Ports 445 and 139 Explained2
? CompTIA A+ Certification Exam Core 2 Objectives3

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 12
A Windows user recently replaced a computer The user can access the public internet on the computer; however, an internal site at https7/companyintranet.com:8888 is no longer loading. Which of the following should a technician adjust to resolve the issue?

A. Default gateway settings
B. DHCP settings
C. IP address settings
D. Firewall settings
E. Antivirus settings

Answer: D

Explanation:
The technician should adjust the firewall settings to resolve the issue of not being able to access an internal site at https://companyintranet.com:8888. The firewall settings control how the firewall filters and allows network traffic based on rules and policies. The firewall settings may be blocking or preventing the access to the internal site by mistake or by default, especially if the site uses a non-standard port number such as 8888. The technician should check and modify the firewall settings to allow the access to the internal site or its port number. Default gateway settings determine how a computer connects to other networks or the internet. Default gateway settings are not likely to cause the issue of not being able to access an internal site if the user can access the public internet. DHCP settings determine how a computer obtains its IP address and other network configuration parameters automatically from a DHCP server. DHCP settings are not likely to cause the issue of not being able to access an internal site if the user can access other network resources. IP address settings determine how a computer identifies itself and communicates with other devices on a network. IP address settings are not likely to cause the issue of not being able to access an internal site if the user can access other network resources. Antivirus settings control how the antivirus software scans and protects the computer from malware and threats. Antivirus settings are less likely to cause the issue of not being able to access an internal site than firewall settings, unless the antivirus software has its own firewall feature that may interfere with the network traffic. References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.6

NEW QUESTION 13
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 18
A user calls the help desk to report that Windows installed updates on a laptop and rebooted overnight. When the laptop started up again, the touchpad was no longer working. The technician thinks the software that controls the touchpad might be the issue. Which of the following tools should the technician use to make adjustments?

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

Answer: D

Explanation:
The technician should use devmgmt.msc tool to make adjustments for the touchpad issue after Windows installed updates on a laptop. Devmgmt.msc is a command that opens the Device Manager, which is a utility that allows users to view and manage the hardware devices and drivers installed on a computer. The technician can use the Device Manager to check the status, properties and compatibility of the touchpad device and its driver, and perform actions such as updating, uninstalling or reinstalling the driver, enabling or disabling the device, or scanning for hardware changes. Eventvwr.msc is a command that opens the Event Viewer, which is a utility that allows users to view and monitor the system logs and events. The Event Viewer may provide some information or clues about the touchpad issue, but it does not allow users to manage or troubleshoot the device or its driver directly. Perfmon.msc is a command that opens the Performance Monitor, which is a utility that allows users to measure and analyze the performance of the system

NEW QUESTION 20
A remote user is experiencing issues connecting to a corporate email account on a laptop. The user clicks the internet connection icon and does not recognize the connected Wi-Fi. The help desk technician, who is troubleshooting the issue, assumes this is a rogue access point. Which of the following is the first action the technician should take?

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

Answer: C

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

NEW QUESTION 21
A Linux technician needs a filesystem type that meets the following requirements:
. All changes are tracked.
. The possibility of file corruption is reduced.
· Data recovery is easy.
Which of the following filesystem types best meets these requirements?

A. ext3
B. FAT32
C. exFAT
D. NTFS

Answer: A

Explanation:
The ext3 file system is a Linux native file system that meets the requirements of the question. It has the following features:
? All changes are tracked. The ext3 file system uses a journaling mechanism that
records all changes to the file system metadata in a special log called the journal before applying them to the actual file system. This ensures that the file system can be restored to a consistent state in case of a power failure or system crash12.
? The possibility of file corruption is reduced. The journaling feature of ext3 also
reduces the possibility of file corruption, as it avoids the need for a full file system check after an unclean shutdown. The file system can be quickly replayed from the journal and any inconsistencies can be fixed12.
? Data recovery is easy. The ext3 file system supports undeletion of files using tools
such as ext3grep or extundelete, which can scan the file system for deleted inodes and attempt to recover the data blocks associated with them34.
References:
1: Introduction to Linux File System [Structure and Types] - MiniTool1 2: 7 Ways to Determine the File System Type in Linux (Ext2, Ext3 or Ext4) - Tecmint3 3: How to Recover Deleted Files in Linux with ext3grep 4: How to Recover Deleted Files from ext3 Partitions

NEW QUESTION 23
A user is having phone issues after installing a new application that claims to optimize performance. The user downloaded the application directly from the vendor's website and is now experiencing high network utilization and is receiving repeated security warnings. Which of the following should the technician perform FIRST to mitigate the issue?

A. Reset the phone to factory settings
B. Uninstall the fraudulent application
C. Increase the data plan limits
D. Disable the mobile hotspot.

Answer: B

Explanation:

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

NEW QUESTION 24
A technician installed a new application on a workstation. For the program to function properly, it needs to be listed in the Path Environment Variable. Which of the following Control Panel utilities should the technician use?

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

Answer: A

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

NEW QUESTION 26
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 28
Which of the following is the most likely reason a filtration system is critical for data centers?

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

Answer: B

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

NEW QUESTION 30
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 33
Which of the following macOS features can help a user close an application that has stopped responding?

A. Finder
B. Mission Control
C. System Preferences

D. Force Quit

Answer: D

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

NEW QUESTION 35
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 36
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 41
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 43

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

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

Answer: C

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

NEW QUESTION 45
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 49
A technician is creating a tunnel that hides IP addresses and secures all network traffic. Which of the following protocols is capable of enduring enhanced security?

A. DNS
B. IPS
C. VPN
D. SSH

Answer: C

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

NEW QUESTION 52
A technician is setting up a new laptop. The company's security policy states that users cannot install virtual machines. Which of the following should the technician implement to prevent users from enabling virtual technology on their laptops?

A. UEFI password
B. Secure boot
C. Account lockout
D. Restricted user permissions

Answer: B

Explanation:
A technician setting up a new laptop must ensure that users cannot install virtual machines as the company's security policy states One way to prevent users from enabling virtual technology is by implementing Secure Boot. Secure Boot is a feature of UEFI firmware that ensures the system only boots using firmware that is trusted by the manufacturer. It verifies the signature of all bootloaders, operating systems, and drivers before running them, preventing any unauthorized modifications to the boot process. This will help prevent users from installing virtual machines on the laptop without authorization.

NEW QUESTION 57
Which of the following would MOST likely be deployed to enhance physical security for a building? (Select TWO).

A. Multifactor authentication
B. Badge reader
C. Personal identification number
D. Firewall
E. Motion sensor
F. Soft token

Answer: BE

Explanation:
Badge reader and motion sensor are devices that can be deployed to enhance physical security for a building. A badge reader is a device that scans and verifies an identification card or tag that grants access to authorized personnel only. A badge reader can help prevent unauthorized entry or intrusion into a building or a restricted area. A motion sensor is a device that detects movement and triggers an alarm or an action when motion is detected. A motion sensor can help deter or alert potential intruders or trespassers in a building or an area. Multifactor authentication is a method of verifying identity using two or more factors, such as something you know, something you have or something you are. Multifactor authentication is not a device that can be deployed to enhance physical security for a building but a technique that can be used to enhance logical security for systems or services. Personal identification number is a numeric code that can be used as part of authentication or access control. Personal identification number is not a device that can be deployed to enhance physical security for a building but an example of something you know factor in multifactor authentication. Firewall is a device or software that filters network traffic based on rules and policies. Firewall is not a device that can be deployed to enhance physical security for a building but a device that can be used to enhance network security for systems or services. Soft token is an application or software that generates one-time passwords or codes for authentication purposes. Soft token is not a device that can be deployed to enhance physical security for a building but an example of something you have factor in multifactor authentication. References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 3.3

NEW QUESTION 59
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 62
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
C. Startup
D. 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 65
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 66
A systems administrator is experiencing Issues connecting from a laptop to the corporate network using PKI. Which to the following tools can the systems administrator use to help remediate the issue?

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

Answer: A

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

NEW QUESTION 68
A computer on a corporate network has a malware infection. Which of the following would be the BEST method for returning the computer to service?

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

Answer: B

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

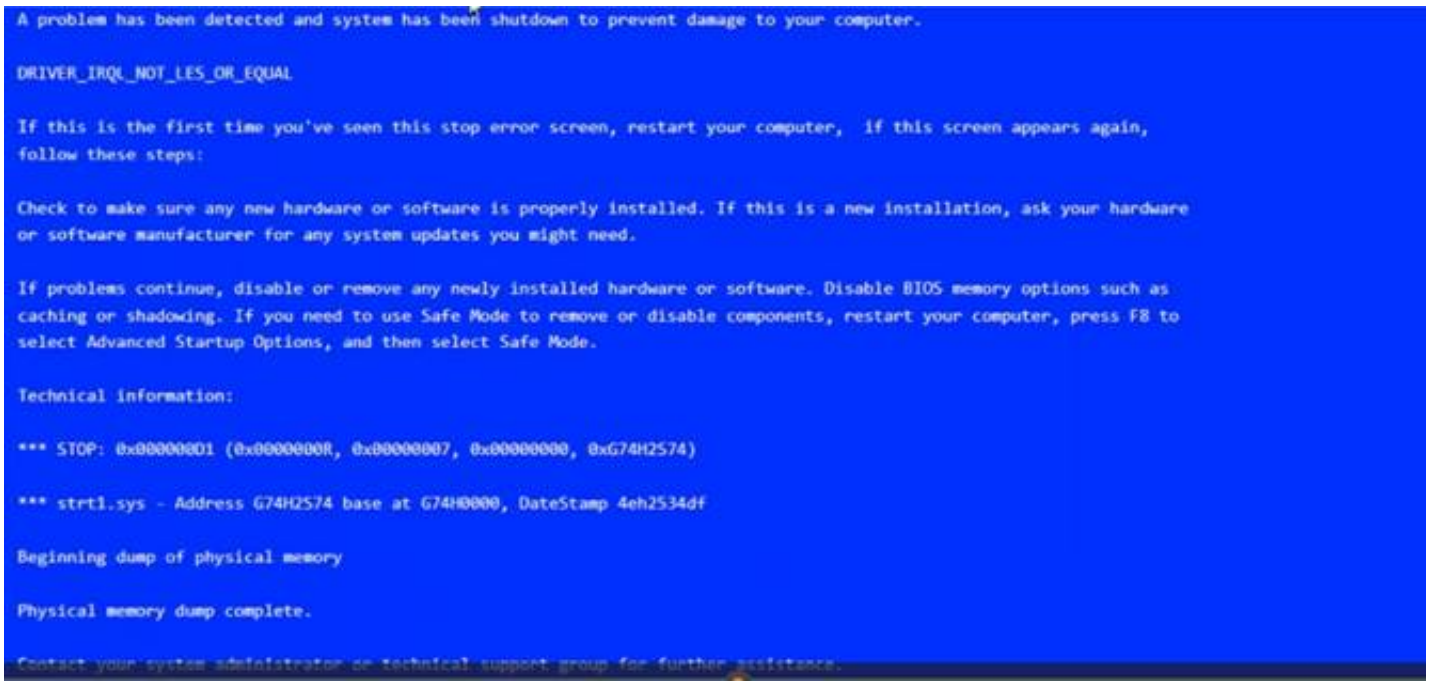
NEW QUESTION 69
A technician has verified a computer is infected with malware. The technician isolates the system and updates the anti-malware software. Which of the following should the technician do next?

A. Mastered
B. Not Mastered

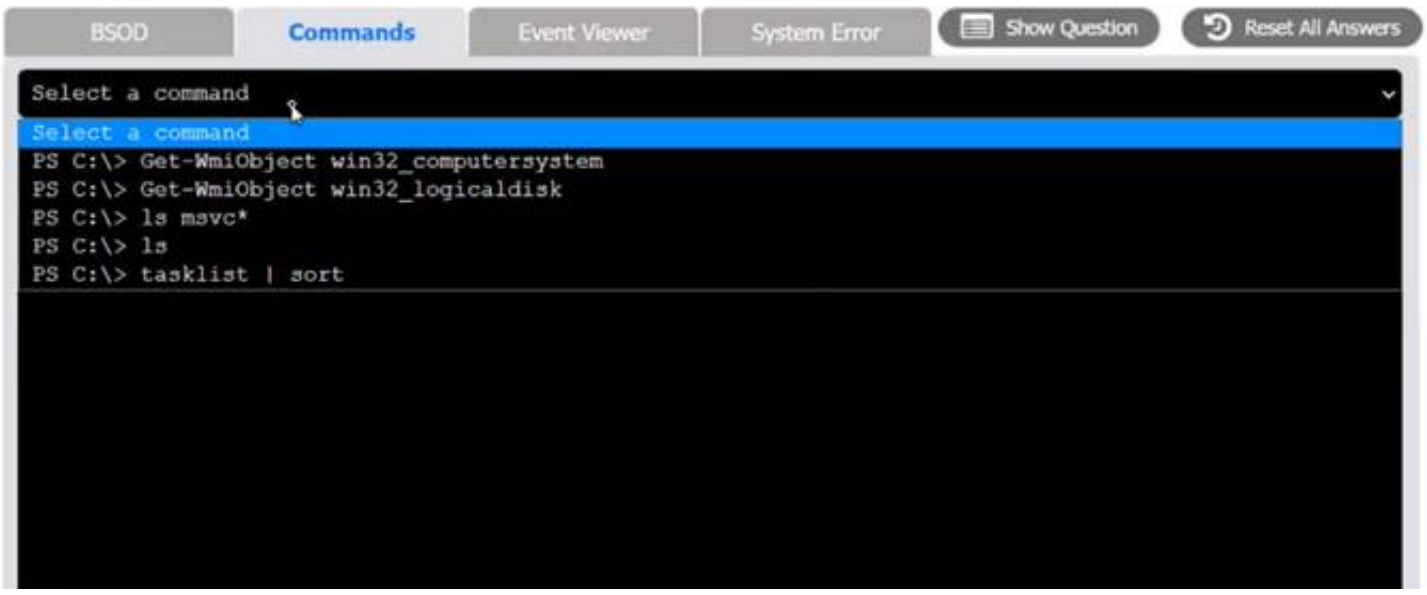
Answer: A

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.

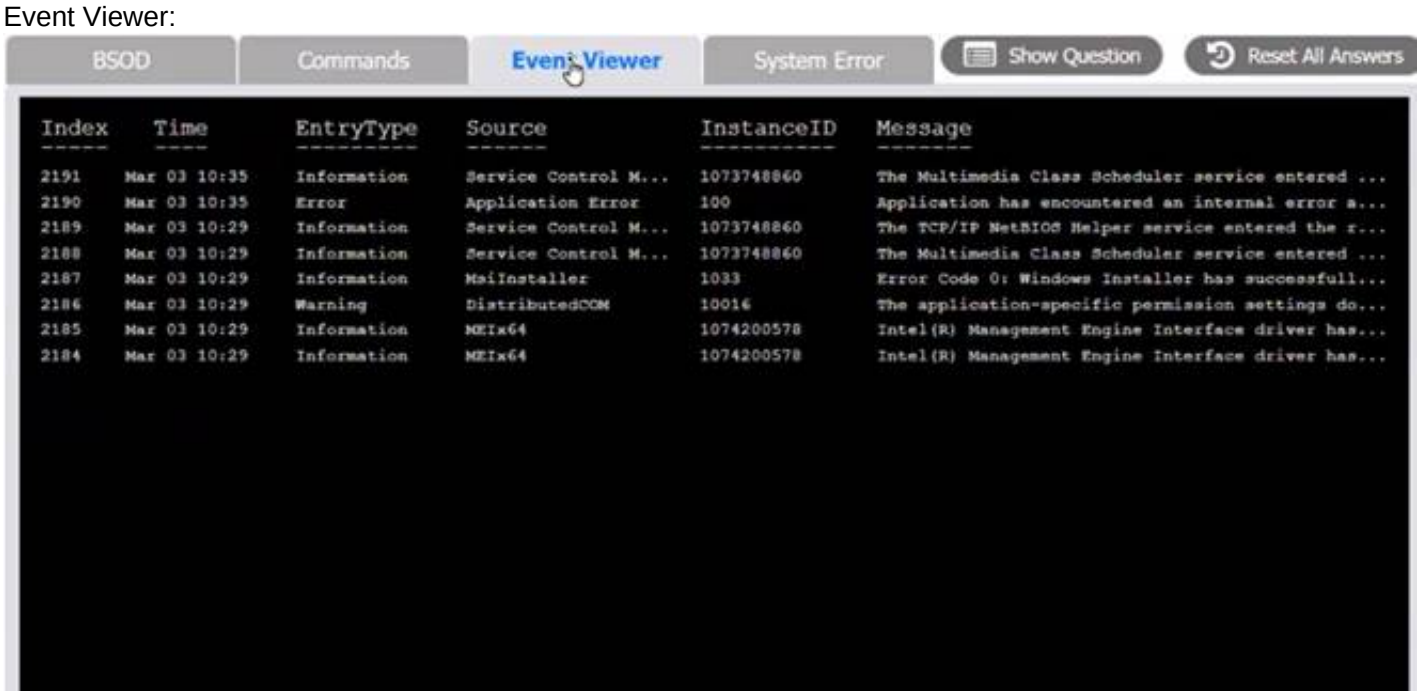
NEW QUESTION 72
SIMULATION
A user reports that after a recent software deployment to upgrade applications, the user can no longer use the Testing program.
However, other employees can successfully use the Testing program.
INSTRUCTIONS
Review the information in each tab to verify the results of the deployment 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



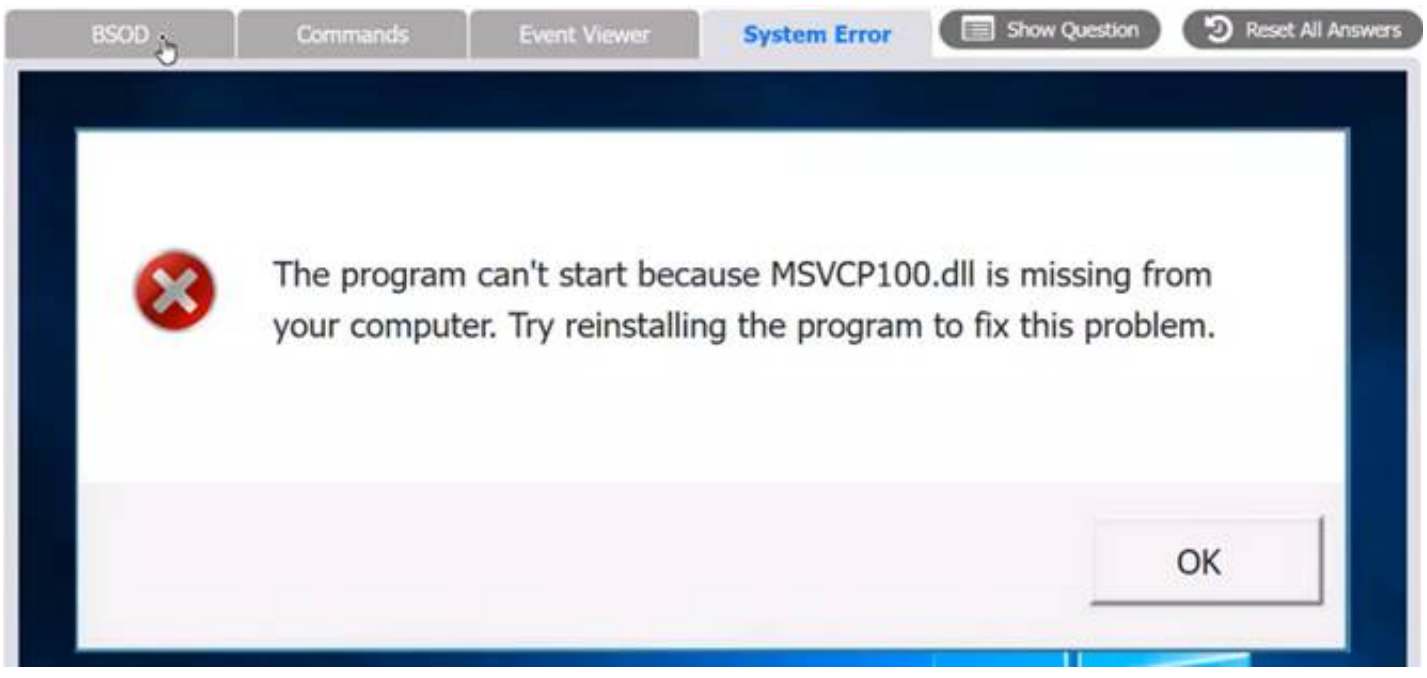
Commands:

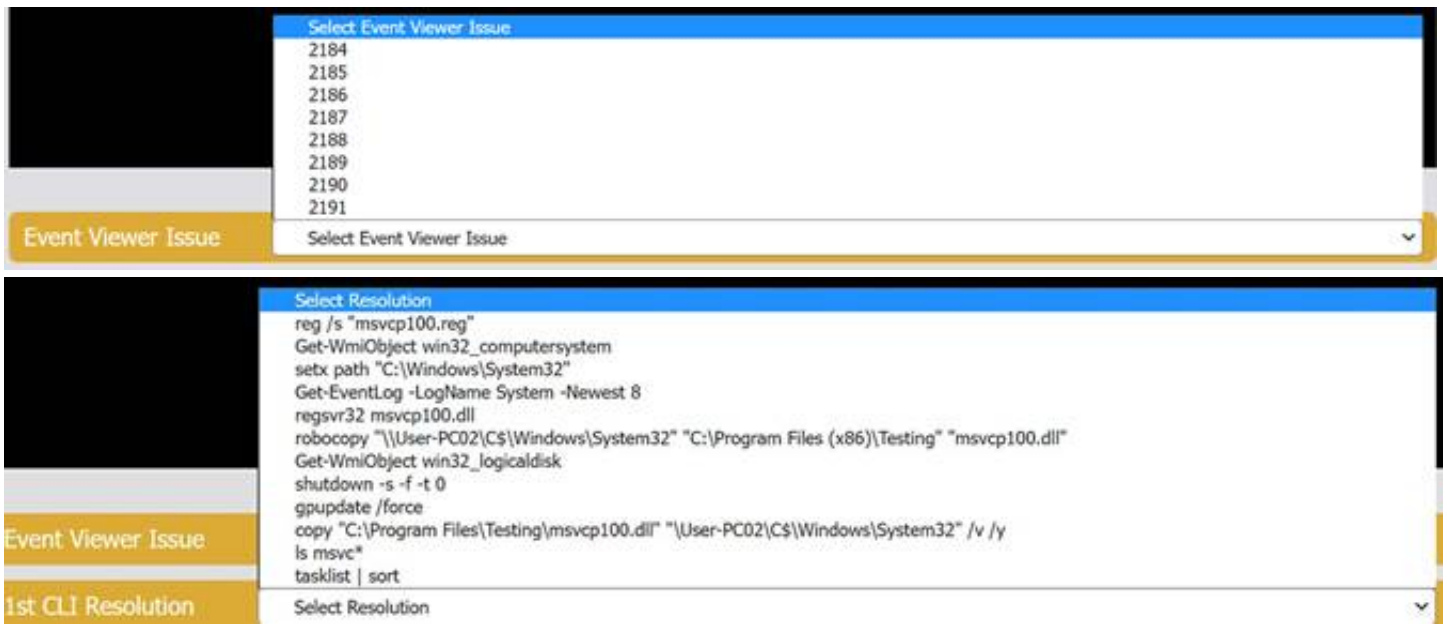


Event Viewer:



System Error:

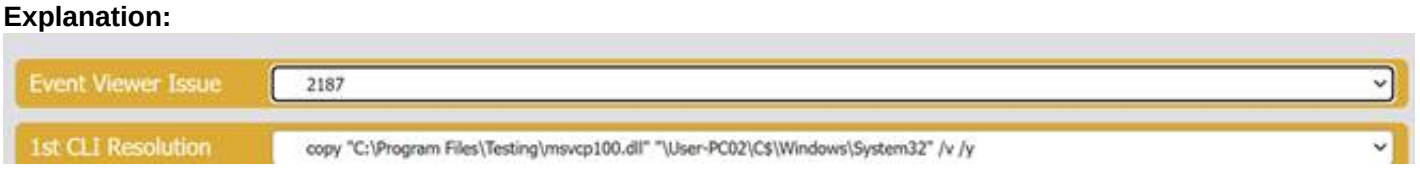




A. Mastered
B. Not Mastered

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 77
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 81
A user's mobile phone has become sluggish A systems administrator discovered several malicious applications on the device and reset the phone. The administrator installed MDM software. Which of the following should the administrator do to help secure the device against this threat in the future? (Select TWO).

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

Answer: CE

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

NEW QUESTION 83
Which of the following is also known as something you know, something you have, and something you are?

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

Answer: B

Explanation:
MFA stands for Multi-Factor Authentication, which is a method of verifying a user's identity using two or more different factors of authentication. The three factors of authentication are something you know, something you have, and something you are. These factors correspond to different types of information or evidence that only the legitimate user should possess or provide. For example:
? Something you know: a password, a PIN, a security question, etc.
? Something you have: a smart card, a token, a mobile device, etc.
? Something you are: a fingerprint, a face, an iris, etc.
MFA provides a higher level of security than single-factor authentication, which only uses one factor, such as a password. MFA reduces the risk of unauthorized access, identity theft, and data breaches, as an attacker would need to compromise more than one factor to impersonate a user. MFA is commonly used for online banking, email accounts, cloud services, and other sensitive applications

NEW QUESTION 87
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 90
While trying to repair a Windows 10 OS, a technician receives a prompt asking for a key. The technician tries the administrator password, but it is rejected. Which of the following does the technician need in order to continue the OS repair?

A. SSL key
B. Preshared key
C. WPA2 key
D. Recovery key

Answer: D

Explanation:

A recovery key is a code that can be used to unlock a BitLocker-encrypted drive when the normal authentication methods (such as password or PIN) are not available or have been forgotten. BitLocker is a feature of Windows that encrypts the entire drive to protect data from unauthorized access. If a technician is trying to repair a Windows 10 OS that has BitLocker enabled, they will need the recovery key to access the drive and continue the OS repair. SSL key, preshared key, and WPA2 key are not keys that are related to BitLocker or OS repair.

NEW QUESTION 94
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

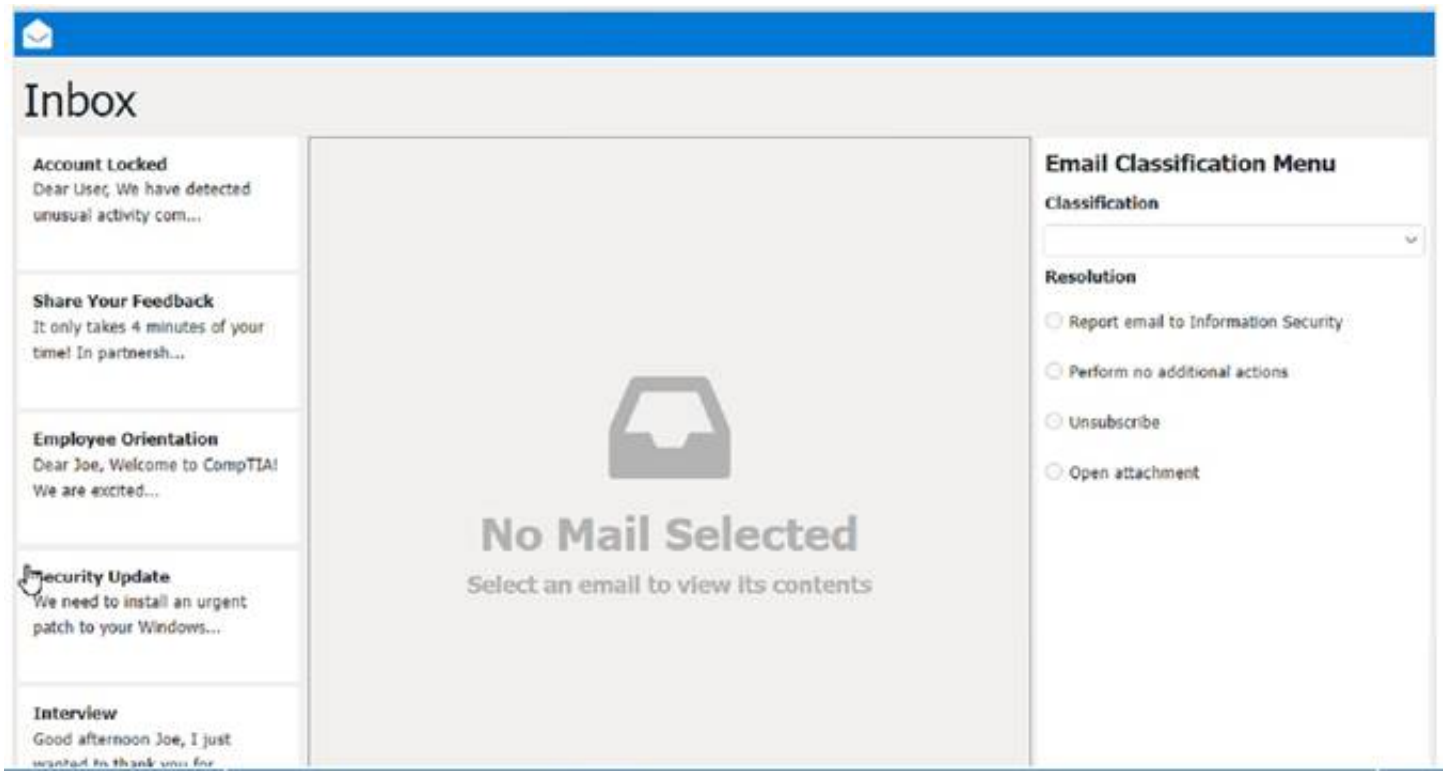
NEW QUESTION 99
A user calls the help desk to report that none of the files on a PC will open. The user also indicates a program on the desktop is requesting payment in exchange for file access A technician verifies the user's PC is infected with ransorrrware. Which of the following should the technician 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 103
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.

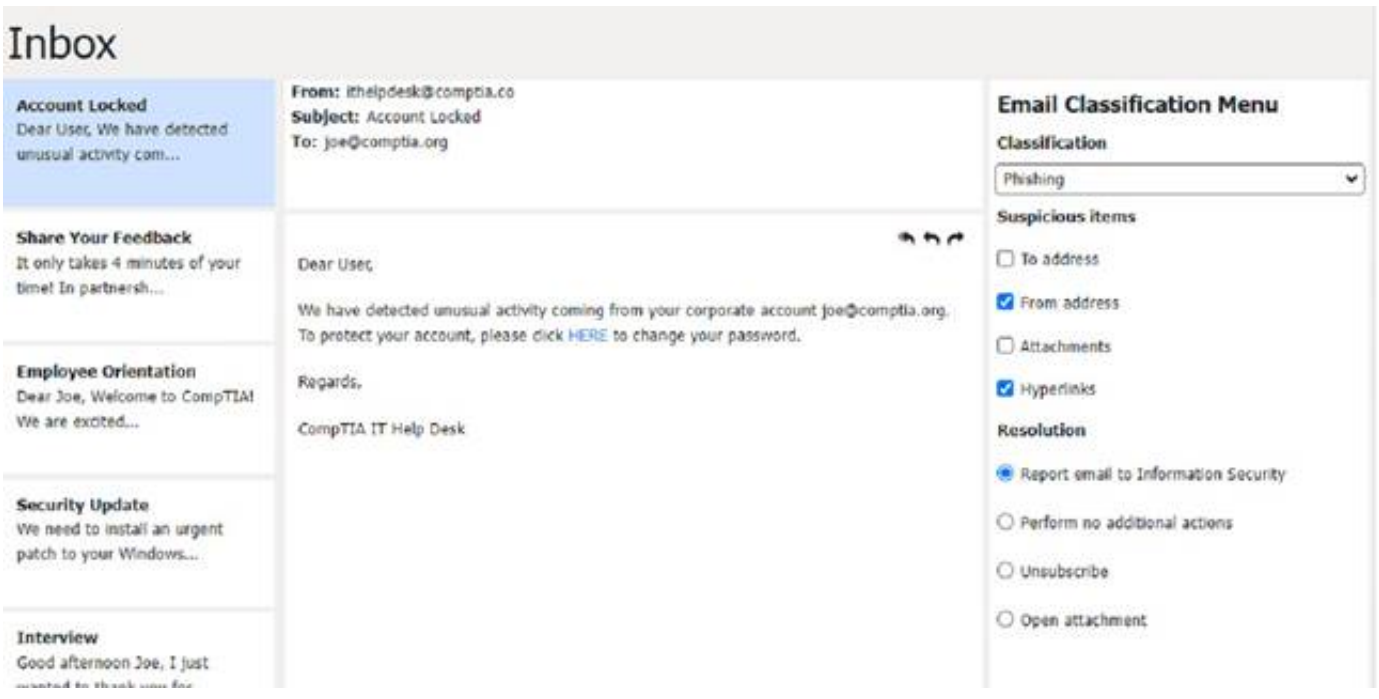
The appropriate resolution for this email is A. Report email to Information Security. The user should not click on the link, reply to the email, or provide any personal or account information. The user should forward the email to the Information Security team or use a professional email form to report 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:

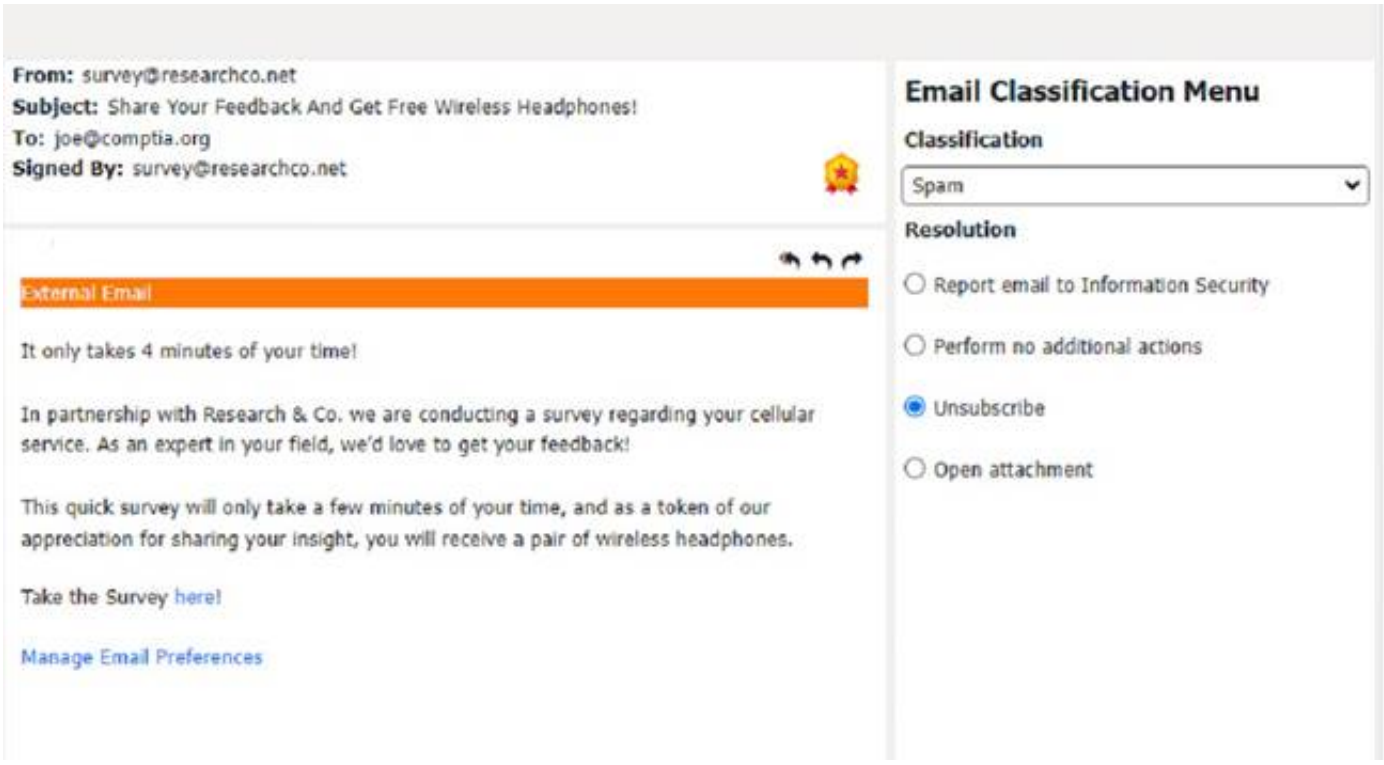
? The email offers a free wireless headphone as an incentive, which is too good to be true.

? 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.

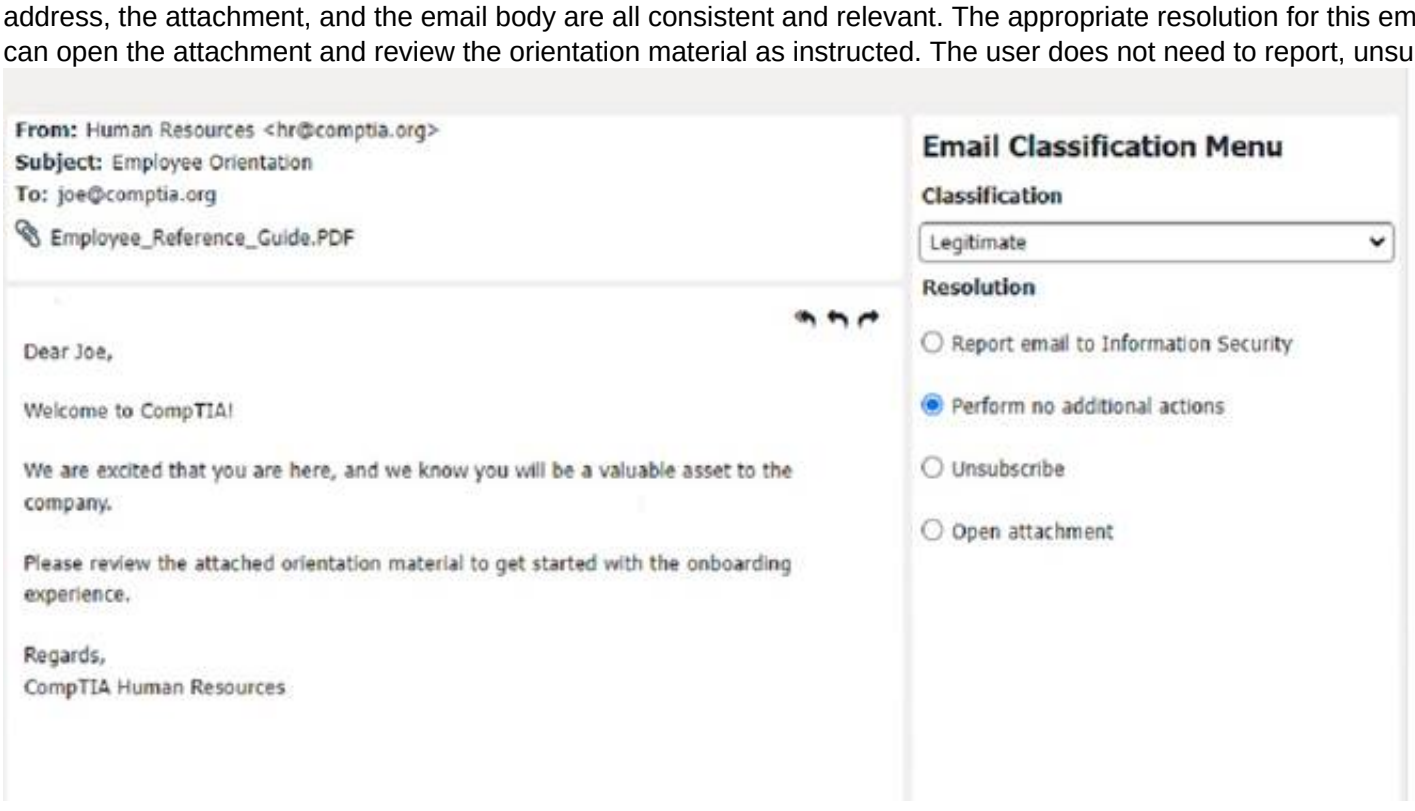
? The email does not have an unsubscribe option, which is required by law for commercial emails.

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:

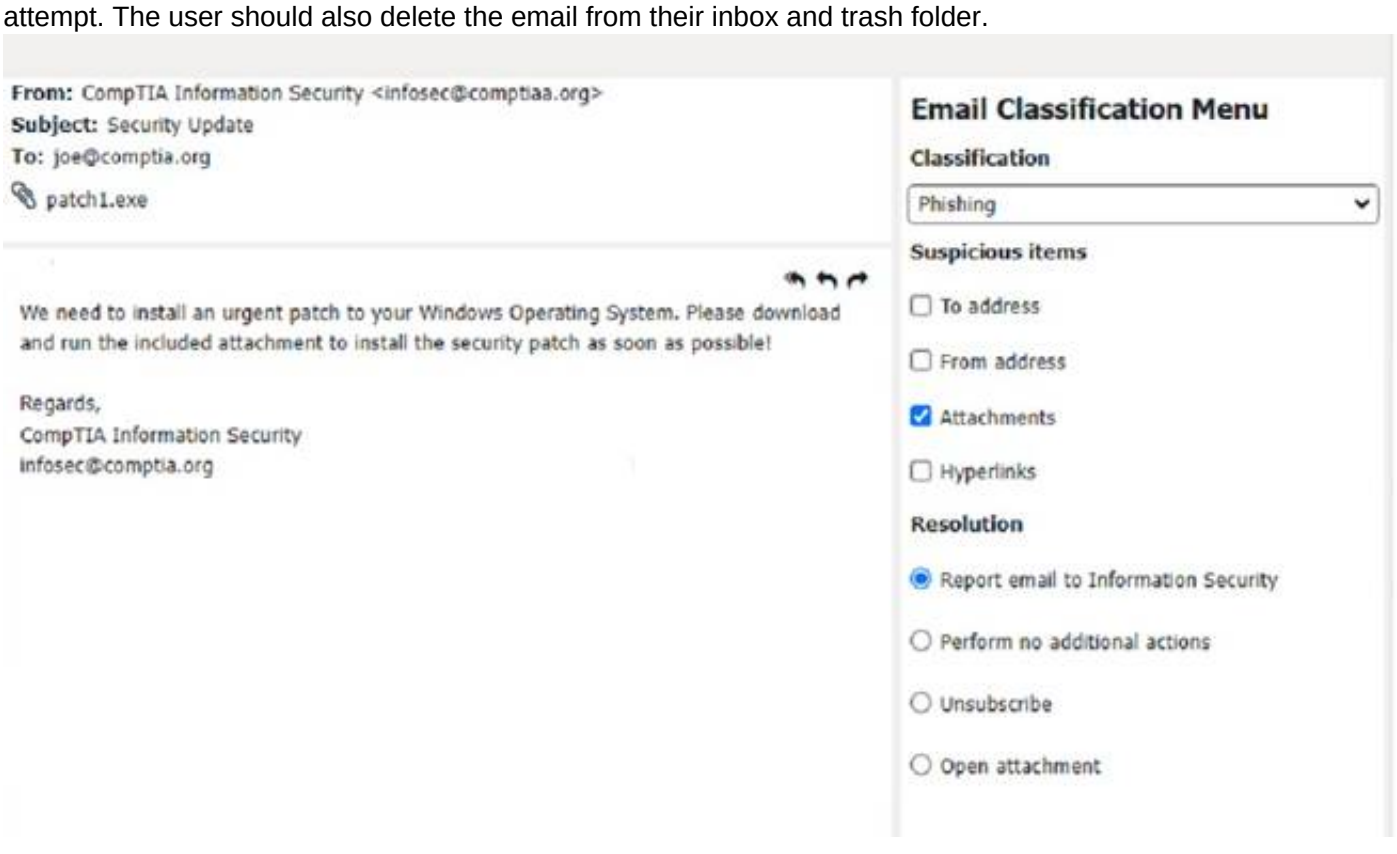
? The email has a generic greeting and does not address the user by name or username.

? The email has an urgent tone and claims that a security patch needs to be installed immediately.

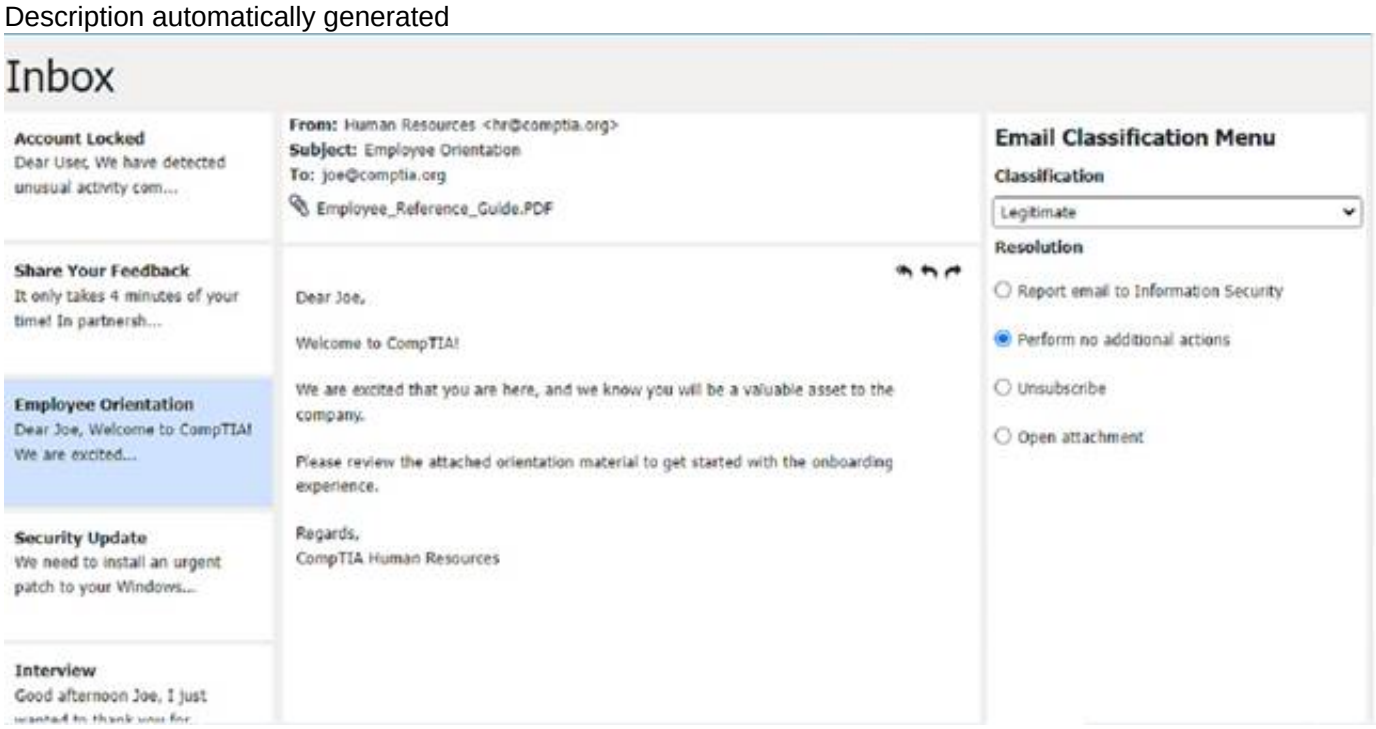
? The email has an attachment named “patch1.exe”, which is an executable file that could contain malware or ransomware.

? 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.



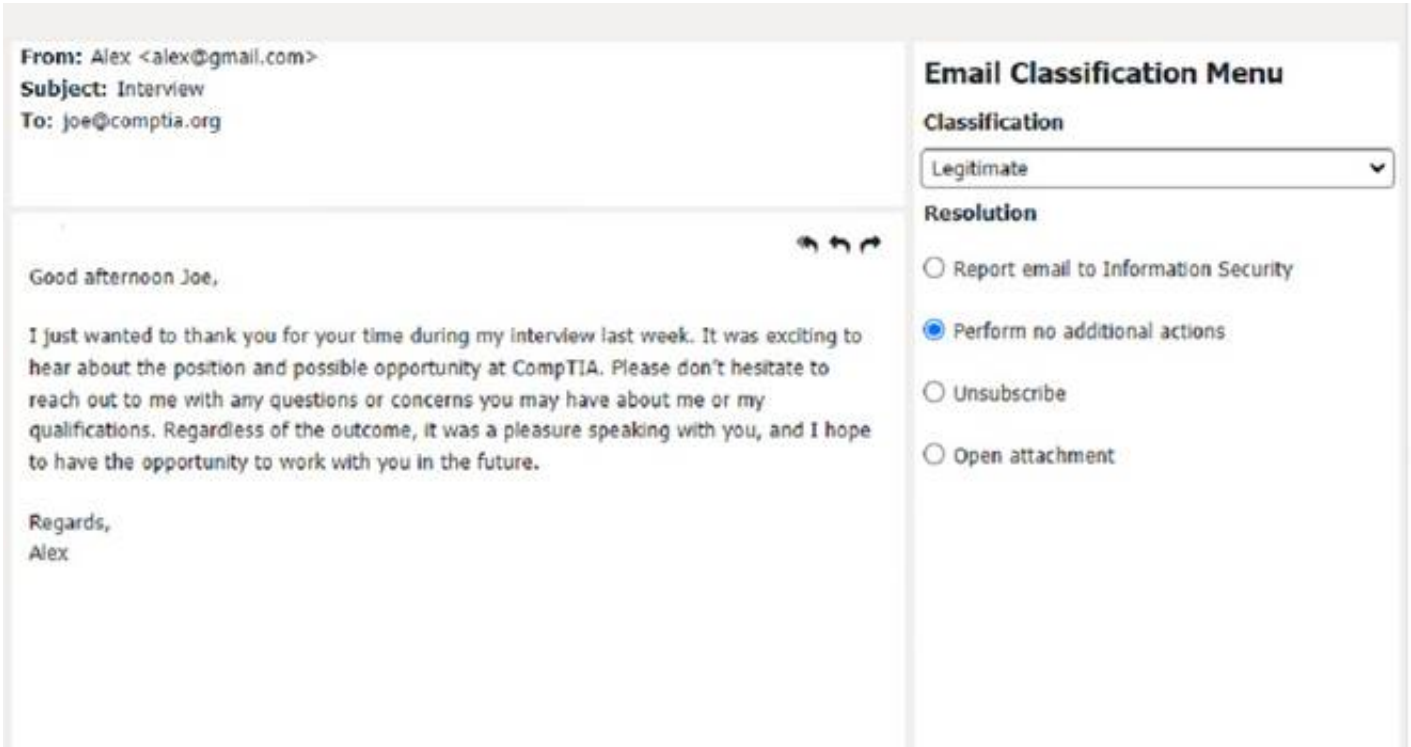
A screenshot of a computer
Description automatically generated



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 106
An IT security team is implementing a new Group Policy that will return a computer to the login after three minutes. Which of the following BEST describes the change in policy?

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

Answer: B

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

NEW QUESTION 108
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 111
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 114
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 117
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 120
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 124
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 129
The findings from a security audit indicate the risk of data loss from lost or stolen laptops is high. The company wants to reduce this risk with minimal impact to users who want to use their laptops when not on the network. Which of the following would BEST reduce this risk for Windows laptop users?

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

Answer: D

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

NEW QUESTION 133
As part of a CYOD policy a systems administrator needs to configure each user's Windows device to require a password when resuming from a period of sleep or inactivity. Which of the following paths will lead the administrator to the correct settings?

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

Answer: A

Explanation:
The systems administrator should use Settings to access Screensaver settings to configure each user's Windows device to require a password when resuming from a period of sleep or inactivity1

NEW QUESTION 136
A user's corporate phone was stolen, and the device contains company trade secrets. Which of the following technologies should be implemented to mitigate this risk? (Select TWO).

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

Answer: AC

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

NEW QUESTION 137
A hard drive that previously contained PI I needs to be repurposed for a public access workstation. Which of the following data destruction methods should a technician use to ensure data is completely removed from the hard drive?

A. Shredding
B. Degaussing

C. Low-level formatting
D. Recycling

Answer: A

Explanation:
Shredding is a data destruction method that physically destroys the hard drive by cutting it into small pieces using a machine. Shredding ensures that data is completely removed from the hard drive and cannot be recovered by any means. Shredding is suitable for hard drives that contain PII (personally identifiable information), which is any information that can be used to identify, contact, or locate an individual. Degaussing, low-level formatting, and recycling are not data destruction methods that can guarantee complete data removal from a hard drive.

NEW QUESTION 140
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 142
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 of the event, such as an application, a service, a driver, or a hardware device. By using Event Viewer, a technician can identify the root cause of the unexpected shutdown, such as a power failure, a thermal event, a driver conflict, or a malware infection.

NEW QUESTION 147
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 151
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 155
Which of the following default system tools can be used in macOS to allow the technician to view the screen simultaneously with the user?

A. Remote Assistance
B. Remote Desktop Protocol
C. Screen Sharing
D. Virtual Network Computing

Answer: C

Explanation:
Screen Sharing is the default system tool that can be used in macOS to allow the technician to view the screen simultaneously with the user. Screen Sharing is a built-in app that lets users share their Mac screen with another Mac on the network. The user can enable screen sharing in the System Preferences > Sharing pane, and then allow other users to request or enter a password to access their screen1. The technician can launch the Screen Sharing app from the Spotlight search or the Finder sidebar, and then enter the user's name, address, or Apple ID to connect to their screen2. Remote Assistance is a Windows feature that allows users to invite someone to help them with a problem on their PC3. Remote Desktop Protocol (RDP) is a protocol that allows users to connect to a remote computer over a network4. Virtual Network Computing (VNC) is a technology that allows users to share their screen with other devices using a VNC viewer app1. These are not default system tools in macOS, although they can be used with third-party software or settings.
References: 1: https://support.apple.com/guide/mac-help/share-the-screen-of-another-mac-mh14066/mac 2: https://www.howtogeek.com/449239/how-to-share-your-macs-screen-with-another-mac/ 3: https://support.microsoft.com/en-us/windows/solve-pc-problems-over-a-remote-connection-b077e31a-16f4-2529-1a47-21f6a9040bf3 4: https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/clients/remote-desktop-protocol

NEW QUESTION 157
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 162
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 increase the risk of malware infection, but it does not explain why the malware persists after a System Restore. The system updates not including the latest anti-malware definitions may reduce the effectiveness of malware detection and removal, but it does not explain why the malware persists after a System Restore. The system restore process being compromised by the malware may prevent a successful System Restore, but it does not explain why the malware persists after a System Restore. References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.3

NEW QUESTION 167
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 172
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 174
Which of the following operating systems is most commonly used in embedded systems?
A. Chrome OS
B. macOS
C. Windows
D. Linux

Answer: D

Explanation:
Linux is the most commonly used operating system in embedded systems because it is open source, free, customizable, and supports a wide range of architectures and devices. Linux also offers many advantages for embedded development, such as real- time capabilities, modularity, security, scalability, and reliability. Linux can run on embedded systems with limited resources, such as memory, storage, or power, and can be tailored to the specific needs of the application. Linux also has a large and active community of developers and users who contribute to its improvement and innovation. Some examples of embedded systems that use Linux are smart TVs, routers, drones, robots, smart watches, and IoT devices

NEW QUESTION 179
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 180
Which of the following filesystem types does macOS use?

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

Answer: D

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

NEW QUESTION 185
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 189
Which of the following defines the extent of a change?

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

Answer: A

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

NEW QUESTION 193
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 194
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 197
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 200
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 203
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 206
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 210
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 213
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 216
Which of the following helps ensure that a piece of evidence extracted from a PC is admissible in a court of law?

A. Data integrity form
B. Valid operating system license
C. Documentation of an incident
D. Chain of custody

Answer: D

Explanation:
Chain of custody is a process that helps ensure that a piece of evidence extracted from a PC is admissible in a court of law. Chain of custody refers to the documentation and tracking of who handled, accessed, modified, or transferred the evidence, when, where, why, and how. Chain of custody can help establish the authenticity, integrity, and reliability of the evidence, as well as prevent tampering, alteration, or loss of the evidence. Data integrity form, valid operating system license, and documentation of an incident are not processes that can ensure that a piece of evidence extracted from a PC is admissible in a court of law.

NEW QUESTION 220
A technician is setting up a newly built computer. Which of the following is the fastest way for the technician to install Windows 10?

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

Answer: D

Explanation:
Windows 10


The correct answer is D. Unattended installation. An unattended installation is a way of installing Windows 10 without requiring any user input or interaction. It uses a configuration file called answer file that contains the settings and preferences for the installation, such as the product key, language, partition, and network settings. An unattended installation can be performed by using a bootable USB flash drive or DVD that contains the Windows 10 installation files and the answer file1. This is the fastest way for the technician to install Windows 10 on a newly built computer, as it automates the whole process and saves time. A factory reset is a way of restoring a computer to its original state by deleting all the data and applications and reinstalling the operating system. A factory reset can be performed by using the recovery partition or media that came with the computer, or by using the Reset this PC option in Windows 10 settings2. A factory reset is not a way of installing Windows 10 on a newly built computer, as it requires an existing operating system to be present.
A system restore is a way of undoing changes to a computer's system files and settings by using a restore point that was created earlier. A system restore can be performed by using the System Restore option in Windows 10 settings or by using the Advanced Startup Options menu3. A system restore is not a way of installing Windows 10 on a newly built computer, as it requires an existing operating system and restore points to be present.
An in-place upgrade is a way of upgrading an existing operating system to a newer version without losing any data or applications. An in-place upgrade can be performed by using the Windows 10 Media Creation Tool or by running the Setup.exe file from the Windows 10 installation media. An in-place upgrade is not a way of installing Windows 10 on a newly built computer, as it requires an existing operating system to be present.

NEW QUESTION 223
An Android user reports that when attempting to open the company's proprietary mobile application it immediately doses. The user states that the issue persists, even after rebooting the phone. The application contains critical information that cannot be lost. Which of the following steps should a systems administrator attempt FIRST?

A. Mastered
B. Not Mastered

Answer: A

Explanation:
The systems administrator should clear the application cach1e2
If clearing the application cache does not work, the systems administrator should uninstall and reinstall the application12
Resetting the phone to factory settings is not necessary at this point12
Installing an alternative application with similar functionality is not necessary at this point12

NEW QUESTION 224
Which of the following Is a package management utility for PCs that are running the Linux operating system?

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

Answer: B

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

NEW QUESTION 229
An architecture firm is considering upgrading its computer-aided design (CAD) software to the newest version that forces storage of backups of all CAD files on the software's cloud server. Which of the following is MOST likely to be of concern to the IT manager?

A. All updated software must be tested with alt system types and accessories
B. Extra technician hours must be budgeted during installation of updates
C. Network utilization will be significantly increased due to the size of CAD files
D. Large update and installation files will overload the local hard drives.

Answer: C

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

NEW QUESTION 230
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 234
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 236
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.

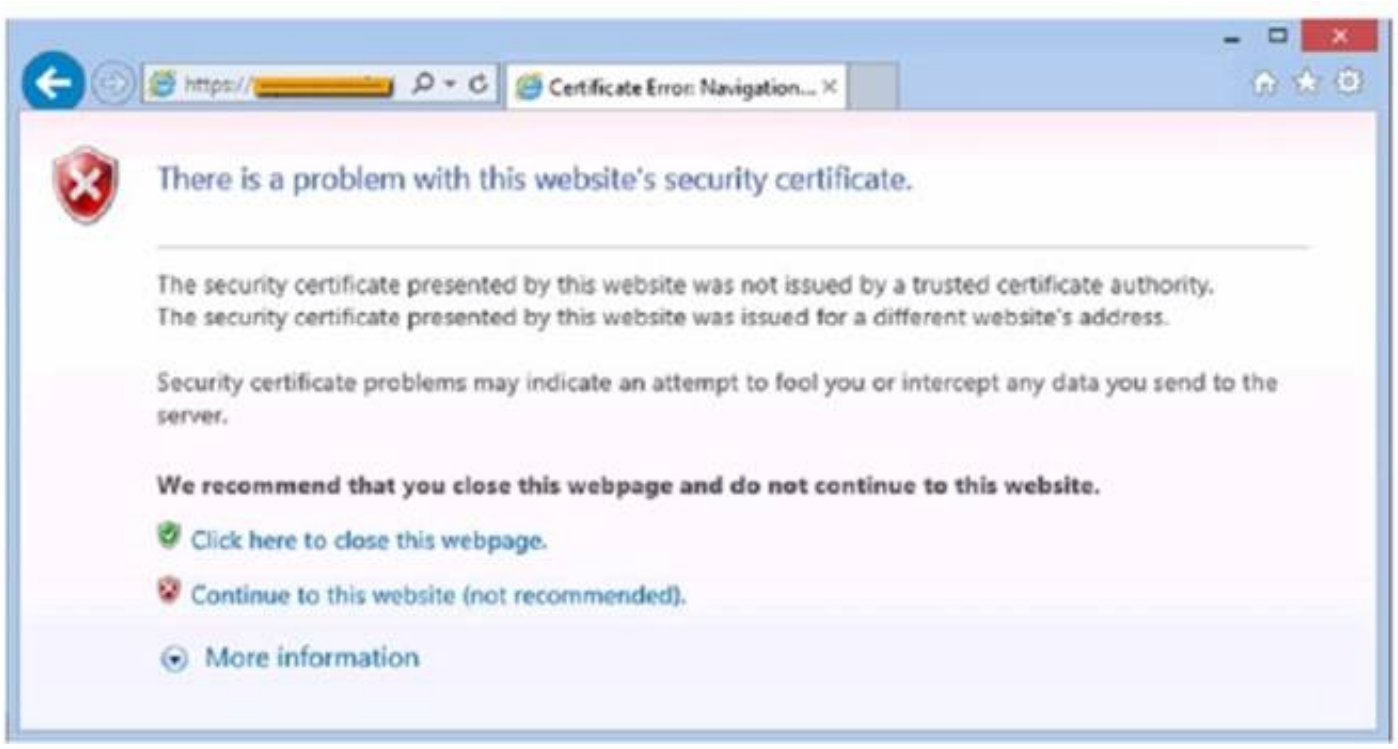
NEW QUESTION 241
A technician is troubleshooting a PC that has been performing poorly. Looking at the Task Manager, the technician sees that CPU and memory resources seem fine, but disk throughput is at 100%.
Which of the following types of malware is the system MOST likely infected with?

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 242
After clicking on a link in an email a Chief Financial Officer (CFO) received the following error:



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

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

Answer: A

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

NEW QUESTION 247
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 249
Which of the following protects a mobile device against unwanted access when it is left unattended?

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

Answer: A

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

NEW QUESTION 254
A user's antivirus software reports an infection that it is unable to remove. Which of the following is the most appropriate way to remediate the issue?

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

Answer: C

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

NEW QUESTION 255
A technician is editing the hosts file on a few PCs in order to block certain domains. Which of the following would the technician need to execute after editing the hosts file?

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

Answer: D

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

NEW QUESTION 260
A user contacted the help desk to report pop-ups on a company workstation indicating the computer has been infected with 137 viruses and payment is needed to remove them. The user thought the company-provided antivirus software would prevent this issue. The help desk ticket states that the user only receives these messages when first opening the web browser. Which of the following steps would MOST likely resolve the issue? (Select TWO)

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 263
Which of the following file types allows a user to easily uninstall software from macOS by simply placing it in the trash bin?

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

Answer: C

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

NEW QUESTION 266
A user has a computer with Windows 10 Home installed and purchased a Windows 10 Pro license. The user is not sure how to upgrade the OS. Which of the following should the technician do to apply this license?

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

Answer: B

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

NEW QUESTION 267
A customer calls a service support center and begins yelling at a technician about a feature for a product that is not working to the customer's satisfaction. This feature is not supported by the service support center and requires a field technician to troubleshoot. The customer continues to demand service. Which of the following is the BEST course of action for the support center representative to take?

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

Answer: B

Explanation:
Apologizing to the customer and escalating the issue to a manager is the best course of action for the support center representative to take. This shows empathy

and professionalism and allows the manager to handle the situation and provide the appropriate service or resolution for the customer.

NEW QUESTION 270

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your 220-1102 Exam with Our Prep Materials Via below:

https://www.certleader.com/220-1102-dumps.html