CompTIA

Exam Questions 220-1102

CompTIA A+ Certification Exam: Core 2

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

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

Answer: C

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

NEW QUESTION 2
A 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
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 4
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 5
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 6
A user reports a computer is running slow. Which of the following tools will help a technician identity the issued

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 7
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 8
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 9
A technician is in the process of installing a new hard drive on a server but is called away to another task. The drive has been unpackaged and left on a desk. Which of the following should the technician perform before leaving?

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

Answer: C

Explanation:

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

NEW QUESTION 10
A large university wants to equip all classrooms with high-definition IP videoconferencing equipment. Which of the following would most likely be impacted in this situation?

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

Answer: B

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

NEW QUESTION 10
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 11
A technician is preparing to remediate a Trojan virus that was found on a workstation. Which of the following steps should the technician complete BEFORE removing the virus?

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

Answer: A

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

NEW QUESTION 14
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 16
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 21
Which of the following filesystem formats would be the BEST choice to ensure read and write compatibility of USB flash drives across several generations of Microsoft operating systems?

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

Answer: D

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

NEW QUESTION 26
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 29
A new spam gateway was recently deployed at a small business However; users still occasionally receive spam. The management team is concerned that users will open the messages and potentially

infect the network systems. Which of the following is the MOST effective method for dealing with this Issue?

A. Adjusting the spam gateway
B. Updating firmware for the spam appliance
C. Adjusting AV settings
D. Providing user training

Answer: D

Explanation:
The most effective method for dealing with spam messages in a small business is to provide user training1. Users should be trained to recognize spam messages and avoid opening them1. They should also be trained to report spam messages to the IT department so that appropriate action can be taken1. In addition, users should be trained to avoid clicking on links or downloading attachments from unknown sources1. By providing user training, the management team can reduce the risk of users opening spam messages and potentially infecting the network systems1.

NEW QUESTION 31
An administrator has submitted a change request for an upcoming server deployment. Which of the following must be completed before the change can be approved?

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

Answer: A

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

NEW QUESTION 32
A user connected a smartphone to a coffee shop's public Wi-Fi and noticed the smartphone started sending unusual SMS messages and registering strange network activity A technician thinks a virus or other malware has infected the device. Which of the following should the technician suggest the user do to best address these security and privacy concerns? (Select two).

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

Answer: CD

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

NEW QUESTION 33
A technician is securing a new Windows 10 workstation and wants to enable a Screensaver lock. Which of the following options in the Windows settings should the technician use?

A. Ease of Access
B. Privacy
C. Personalization
D. Update and Security

Answer: C

Explanation:
The technician should use the Personalization option in the Windows settings to enable a Screensaver lock. The Personalization option allows users to customize the appearance and behavior of their desktop, such as themes, colors, backgrounds, lock screen and screensaver. The technician can enable a Screensaver lock by choosing a screensaver from the drop-down menu, setting a wait time in minutes and checking the box that says “On resume, display logon screen”. This will lock the computer and require a password or PIN to log back in after the screensaver is activated. Ease of Access is an option in the Windows settings that allows users to adjust accessibility features and settings, such as narrator, magnifier, high contrast and keyboard shortcuts. Ease of Access is not related to enabling a Screensaver lock. Privacy is an option in the Windows settings that allows users to manage privacy and security settings, such as location, camera, microphone and app permissions. Privacy is not related to enabling a Screensaver lock. Update and Security is an option in the Windows settings that allows users to check and install updates, troubleshoot problems, backup files and restore system. Update and Security is not related to enabling a Screensaver lock. References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.7

NEW QUESTION 37
A technician is investigating options to secure a small office's wireless network. One requirement is to allow automatic log-ins to the network using certificates instead of passwords. Which of the following should the wireless solution have in order to support this feature?

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

Answer: A

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

NEW QUESTION 38
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 39
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 43
Which of the following is used as a password manager in the macOS?

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

Answer: D

Explanation:
Keychain is a feature of macOS that securely stores passwords, account numbers, and other confidential information for your Mac, apps, servers, and websites1.

You can use the Keychain Access app on your Mac to view and manage your keychains and the items stored in them1. Keychain can also sync your passwords across your devices using iCloud Keychain1. Keychain can be used as a password manager in macOS to help you keep track of and protect your passwords. References: 1: Manage passwords using keychains on Mac (https://support.apple.com/guide/mac-help/use-keychains-to-store-passwords- mchlf375f392/mac)

and other secure information

NEW QUESTION 47
Which of the following features allows a technician to configure policies in a Windows 10 Professional desktop?

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

Answer: A

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

NEW QUESTION 50
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 55
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 56
A technician suspects the boot disk of a user's computer contains bad sectors. Which of the following should the technician verify in the command prompt to address the issue without making any changes?

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

Answer: C

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

NEW QUESTION 60
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 65
A company acquired a local office, and a technician is attempting to join the machines at the office to the local domain. The technician notes that the domain join option appears to be missing. Which of the following editions of Windows is MOST likely installed on the machines?

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

Answer: D

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

NEW QUESTION 69
A company needs employees who work remotely to have secure access to the corporate intranet. Which of the following should the company implement?

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

Answer: C

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

NEW QUESTION 74
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 76
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 79
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 81
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 84
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 89
A new employee was hired recently. Which of the following documents will the new employee need to sign before being granted login access to the network?

A. Mastered
B. Not Mastered

Answer: A

Explanation:
A new employee will need to sign an AUP before being granted login access to the network. An AUP is an Acceptable Use Policy that defines the rules and guidelines for using network resources and services in an organization. An AUP typically covers topics such as security, privacy, ethics, compliance and liability issues related to network usage. An AUP helps protect the organization and its users from legal, regulatory and reputational risks associated with network activities. An MSDS is a Material Safety Data Sheet that provides information about hazardous substances and how to handle them safely. An MSDS is not related to network access or usage. A EULA is an End User License Agreement that specifies the terms and conditions for using a software product or service. A EULA is usually provided by software vendors or developers and does not apply to network access or usage in general. A UAC is a User Account Control that is a security feature that prompts users for permission or confirmation before performing certain actions that require elevated privileges or affect system settings. A UAC is not a document that needs to be signed by users but a mechanism that helps prevent unauthorized changes or malware infections on a system. References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 5.1

NEW QUESTION 94
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 95
A help desk technician determines a motherboard has failed. Which of the following is the most logical next step in the remediation process?

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

Answer: B

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

NEW QUESTION 96
A technician suspects a rootkit has been installed and needs to be removed. Which of the following would BEST resolve the issue?

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 99
Which of the following options should MOST likely be considered when preserving data from a hard drive for forensic analysis? (Select TWO).

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

Answer: B

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

NEW QUESTION 102
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 106
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 108
Upon downloading a new ISO, an administrator is presented with the following string: 59d15a16ce90cBcc97fa7c211b767aB
Which of the following BEST describes the purpose of this string?

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

Answer: C

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

NEW QUESTION 113
A user wants to set up speech recognition on a PC. In which of the following Windows Settings tools can the user enable this option?

A. Language
B. System
C. Personalization
D. Ease of Access

Answer: D

Explanation:
The user can enable speech recognition on a PC in the Ease of Access settings tool. To set up Speech Recognition on a Windows PC, the user should open Control Panel, click on Ease of Access, click on Speech Recognition, and click the Start Speech Recognition link. Language settings can be used to change the language of the speech recognition feature, but they will not enable the feature. System settings can be used to configure the hardware and software of the PC, but they will not enable the speech
recognition feature. Personalization settings can be used to customize the appearance and behavior of the PC, but they will not enable the speech recognition feature1
Open up ease of access, click on speech, then there is an on and off button for speech recognition.

NEW QUESTION 114
A user's computer unexpectedly shut down immediately after the user plugged in a USB headset. Once the user turned the computer back on, everything was functioning properly, including the headset. Which of the following Microsoft tools would most likely be used to determine the root cause?

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

Answer: A

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

NEW QUESTION 119
A user reports an issue when connecting a mobile device to Bluetooth. The user states the mobile device's Bluetooth is turned on. Which of the following steps should the technician take NEXT to resolve the issue?

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

Answer: C

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

NEW QUESTION 122
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 123
A user in a corporate office reports the inability to connect to any network drives. No other users have reported this issue. Which of the following is the MOST likely reason the user is having this issue?

A. Mastered
B. Not Mastered

Answer: A

NEW QUESTION 128
A technician, who is working at a local office, has found multiple copies of home edition software installed on computers. Which of the following does this MOST likely violate?

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

Answer: A

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

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

NEW QUESTION 129
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 134
A user's application is unresponsive. Which of the following Task Manager tabs will allow the user to address the situation?

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

Answer: D

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

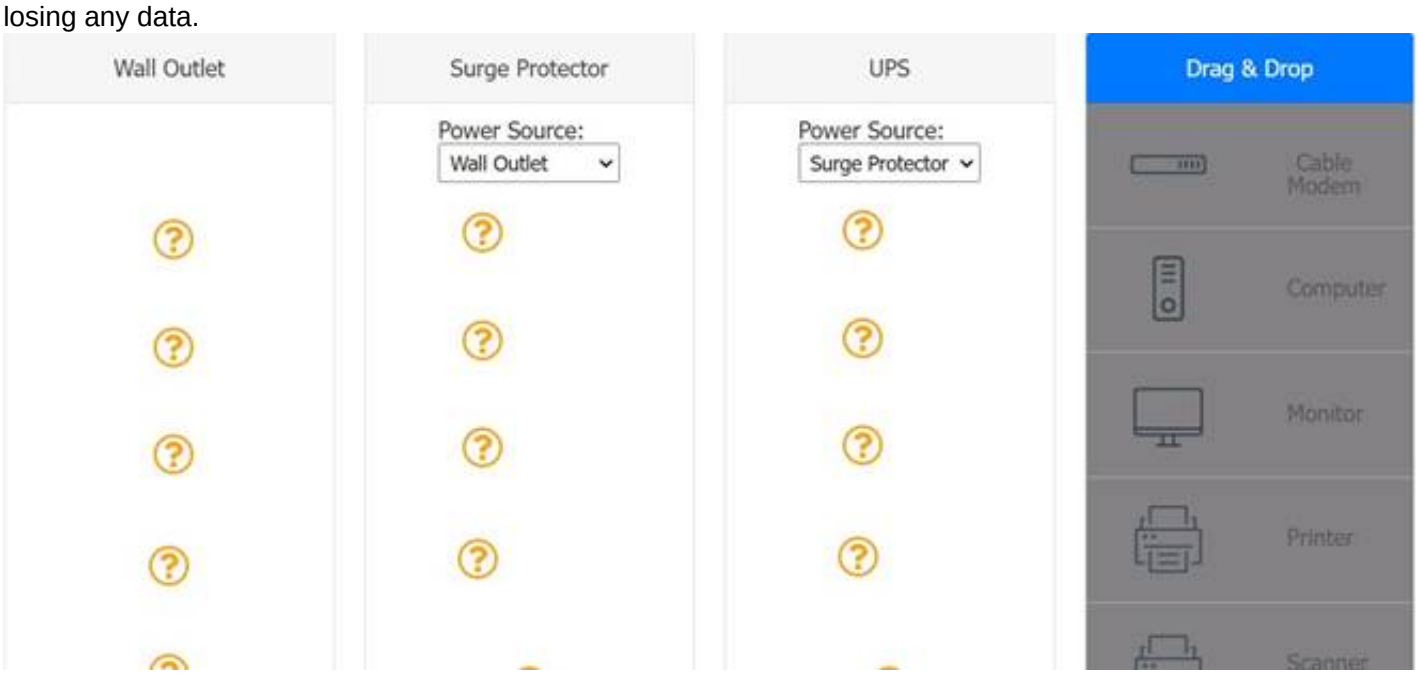
NEW QUESTION 139
A technician is unable to completely start up a system. The OS freezes when the desktop background appears, and the issue persists when the system is restarted. Which of the following should the technician do next to troubleshoot the issue?

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

Answer: B

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

NEW QUESTION 141
DRAG DROP
A customer recently experienced a power outage at a SOHO. The customer does not think the components are connected properly. A print job continued running for several minutes after the power failed, but the customer was not able to interact with the computer. Once the UPS stopped beeping, all functioning devices also turned off. In case of a future power failure, the customer wants to have the most time available to save cloud documents and shut down the computer without losing any data.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
UPS > Surge protector = Computer, wifi router, cable modem Surge protector = wallOutlet , printer and scanner

NEW QUESTION 144
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 147
A systems administrator is setting up a Windows computer for a new user Corporate policy requires a least privilege environment. The user will need to access advanced features and configuration settings for several applications. Which of the following BEST describes the account access level the user will need?

A. Power user account
B. Standard account
C. Guest account
D. Administrator account

Answer: B

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

NEW QUESTION 150
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 152
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 156
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 159
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 163
A systems administrator needs to reset a users password because the user forgot it. The systems administrator creates the new password and wants to further protect the user's account Which of the following should the systems administrator do?

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

Answer: A

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

NEW QUESTION 166
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 169
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 174
The network was breached over the weekend System logs indicate that a single user's account was successfully breached after 500 attempts with a dictionary attack. Which of the following would BEST mitigate this threat?

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

Answer: B

Explanation:
Account lockout would best mitigate the threat of a dictionary attack1

NEW QUESTION 175
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 178
A user wants to back up a Windows 10 device. Which of the following should the user select?

A. Devices and Printers
B. Email and Accounts
C. Update and Security
D. Apps and Features

Answer: C

Explanation:
Update and Security is the section in Windows 10 Settings that allows the user to back up their device. Backing up a device means creating a copy of the data and settings on the device and storing it in another location, such as an external drive or a cloud service. Backing up a device can help the user restore their data and settings in case of data loss, corruption, or theft. Devices and Printers, Email and Accounts, and Apps and Features are not sections in Windows 10 Settings that allow the user to back up their device.

NEW QUESTION 180
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 181
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 185
A user rotates a cell phone horizontally to read emails, but the display remains vertical, even though the settings indicate autorotate is on. VT1ich of the following will MOST likely resolve the issue?

A. Recalibrating the magnetometer
B. Recalibrating the compass
C. Recalibrating the digitizer
D. Recalibrating the accelerometer

Answer: D

Explanation:
When a user rotates a cell phone horizontally to read emails and the display remains vertical, even though the settings indicate autorotate is on, this is typically due to a problem with the phone's accelerometer. The accelerometer is the sensor that detects changes in the phone's orientation and adjusts the display accordingly. If the accelerometer is not calibrated correctly, the display may not rotate as expected.
Recalibrating the accelerometer is the most likely solution to this issue. The process for recalibrating the accelerometer can vary depending on the specific device and operating system, but it typically involves going to the device's settings and finding the option to calibrate or reset the sensor. Users may need to search their device's documentation or online resources to find specific instructions for their device.

NEW QUESTION 190
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 195
A systems administrator is tasked with configuring desktop systems to use a new proxy server that the organization has added to provide content filtering. Which of the following Windows utilities IS the BEST choice for accessing the necessary configuration to complete this goal?

A. Security and Maintenance
B. Network and Sharing Center
C. Windows Defender Firewall
D. Internet Options

Answer: D

Explanation:
The best choice for accessing the necessary configuration to configure the desktop systems to use a new proxy server is the Internet Options utility. This utility can be found in the Control Panel and allows you to configure the proxy settings for your network connection. As stated in the CompTIA A+ Core 2 exam objectives, technicians should be familiar with the Internet Options utility and how to configure proxy settings.

NEW QUESTION 199
Which of the following is a proprietary Cisco AAA protocol?

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

Answer: D

Explanation:
TACACS+ is a proprietary Cisco AAA protocol

NEW QUESTION 204
A company-owned mobile device is displaying a high number of ads, receiving data-usage limit notifications, and experiencing slow response. After checking the device, a technician notices the device has been jailbroken. Which of the following should the technician do next?

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

Answer: B

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

NEW QUESTION 205
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 208
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 209
A help desk technician runs the following script: Inventory.py. The technician receives the following error message:
How do you want to Open this file?
Which of the following is the MOST likely reason this script is unable to run?

A. Scripts are not permitted to run.
B. The script was not built for Windows.
C. The script requires administrator privileges,
D. The runtime environment is not installed.

Answer: D

Explanation:
The error message is indicating that the script is not associated with any program on the computer that can open and run it. This means that the script requires a runtime environment, such as Python, to be installed in order for it to execute properly. Without the appropriate runtime environment, the script will not be able to run.

NEW QUESTION 210
The Chief Executive Officer at a bark recently saw a news report about a high-profile cybercrime where a remote-access tool that the bank uses for support was also used in this crime. The report stated that attackers were able to brute force passwords to access systems. Which of the following would BEST limit the bark's risk? (Select TWO)

A. Enable multifactor authentication for each support account
B. Limit remote access to destinations inside the corporate network
C. Block all support accounts from logging in from foreign countries
D. Configure a replacement remote-access tool for support cases.
E. Purchase a password manager for remote-access tool users
F. Enforce account lockouts after five bad password attempts

Answer: AF

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

NEW QUESTION 215
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 219
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 223
Which of the following Linux commands would be used to install an application?

A. yum
B. grep
C. Is

D. sudo

Answer: D

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

NEW QUESTION 228
An administrator is designing and implementing a server backup system that minimizes the capacity of storage used. Which of the following is the BEST backup approach to use in conjunction with synthetic full backups?

A. Differential
B. Open file
C. Archive
D. Incremental

Answer: D

Explanation:
Incremental backups are backups that only include the changes made since the last backup, whether it was a full or an incremental backup. Incremental backups minimize the capacity of storage used and are often used in conjunction with synthetic full backups, which are backups that combine a full backup and subsequent incremental backups into a single backup set.
Reference: CompTIA A+ Core 2 Exam Objectives, Section 3.3

NEW QUESTION 232
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 235
A technician is installing new software on a macOS computer. Which of the following file types will the technician MOST likely use?

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

Answer: D

Explanation:
The file type that the technician will MOST likely use when installing new software on a macOS computer is .app. This is because .app is the file extension for applications on macOS1.

NEW QUESTION 236
A technician needs to perform after-hours service starting at 10:00 p.m. The technician is currently 20 minutes late. The customer will also be late. Which of the following should the technician do considering proper communication techniques and professionalism?

A. Do not notify the customer if arriving before the customer.
B. Dismiss the customer and proceed with the after-hours work.
C. Contact the customer if the technician is arriving late.
D. Disclose the experience via social media.

Answer: C

Explanation:
The best option for the technician to demonstrate proper communication techniques and professionalism is to contact the customer if the technician is arriving late. This shows respect for the customer's time and expectations, and allows the customer to adjust their schedule accordingly. It also helps to maintain a positive relationship and trust between the technician and the customer. The technician should apologize for the delay and provide a realistic estimate of their arrival time. The technician should also thank the customer for their patience and understanding.
The other options are not appropriate or professional. Do not notify the customer if arriving before the customer is not a good practice, as it may cause confusion or frustration for the customer. The customer may have made other plans or arrangements based on the technician's original schedule, and may not be available or prepared for the service. Dismiss the customer and proceed with the after-hours work is rude and disrespectful, as it ignores the customer's needs and preferences. The customer may have questions or concerns about the service, or may want to supervise or verify the work. The technician should always communicate with the customer before, during, and after the service.
Disclose the experience via social media is unethical and unprofessional, as it may violate the customer's privacy and the company's policies. The technician should not share any confidential or sensitive information about the customer or the service on social media, or make any negative or

inappropriate comments about the customer or the situation. References:
? CompTIA A+ Certification Exam Core 2 Objectives1
? CompTIA A+ Core 2 (220-1102) Certification Study Guide2
? 8 Ways You Can Improve Your Communication Skills3
? Professionalism in Communication | How To Do It And How It Pays4

NEW QUESTION 241
A user receives a notification indicating the data plan on the user's corporate phone has reached its limit. The user has also noted the performance of the phone is abnormally slow. A technician discovers a third-party GPS application was installed on the phone. Which of the following is the MOST likely cause?

A. The GPS application is installing software updates.
B. The GPS application contains malware.
C. The GPS application is updating its geospatial map data.
D. The GPS application is conflicting with the built-in GPS.

Answer: B

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

NEW QUESTION 244
Which of the following is a consequence of end-of-lite operating systems?
A. Operating systems void the hardware warranty.
B. Operating systems cease to function.
C. Operating systems no longer receive updates.
D. Operating systems are unable to migrate data to the new operating system.

Answer: C

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

NEW QUESTION 246
A PC is taking a long time to boot. Which of the following operations would be best to do to resolve the issue at a minimal expense? (Select two).

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

Answer: BE

Explanation:
The correct answers are B. Removing the applications from startup and E. Defragmenting the hard drive. These are the operations that would be best to do to resolve the issue of a slow boot at a minimal expense.
? Removing the applications from startup means disabling the programs that run automatically when the PC is turned on. This will reduce the load on the CPU and RAM and speed up the boot process1.
? Defragmenting the hard drive means rearranging the files on the disk so that they

are stored in contiguous blocks. This will improve the disk performance and reduce the time it takes to read and write data2.
1: CompTIA A+ Certification Exam: Core 2 Objectives, page 23, section 3.1. 2: CompTIA A+ Certification Exam: Core 2 Objectives, page 24, section 3.2.

NEW QUESTION 247
Maintaining the chain of custody is an important part of the incident response process. Which of the following reasons explains why this is important?

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

Answer: C

Explanation:
Maintaining the chain of custody is important to control evidence and maintain integrity. The chain of custody is a process that documents who handled, accessed, or modified a piece of evidence, when, where, how, and why. The chain of custody ensures that the evidence is preserved, protected, and authenticated throughout the incident response process. Maintaining the chain of custody can help prevent tampering, alteration, or loss of evidence, as well as establish its reliability and validity in legal proceedings. Maintaining an information security policy, properly identifying the issue, and gathering as much information as possible are not reasons why maintaining the chain of custody is important. Maintaining an information security policy is a general practice that defines the rules and guidelines for securing an organization's information assets and resources. Properly identifying the issue is a step in the incident response process that involves analyzing and classifying the incident based on its severity, impact, and scope. Gathering as much information as possible is a step in the incident response process that involves collecting and documenting relevant data and evidence from various sources, such as logs, alerts, or witnesses. References:
? Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 26

NEW QUESTION 249
A user notices a small USB drive is attached to the user's computer after a new vendor visited the office. The technician notices two files named grabber.exe and output.txt. Which of the following attacks is MOST likely occurring?

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

Answer: D

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

NEW QUESTION 250
Which of the following would MOST likely be used to change the security settings on a user's device in a domain environment?

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

Answer: C

Explanation:
Group Policy is the most likely tool to be used to change the security settings on a user's device in a domain environment. Group Policy is a feature of Windows that allows administrators to manage and configure settings for multiple devices and users in a centralized way. Group Policy can be used to enforce security policies such as password

complexity, account lockout, firewall rules, encryption settings, etc.

NEW QUESTION 255
The command cac cor.ptia. txt was issued on a Linux terminal. Which of the following results should be expected?

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

Answer: B

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

NEW QUESTION 260
A technician needs to remotely connect to a Linux desktop to assist a user with troubleshooting. The technician needs to make use of a tool natively designed for Linux. Which of the following tools will the technician MOST likely use?

A. VNC
B. MFA
C. MSRA
D. RDP

Answer: A

Explanation:
The tool that the technician will most likely use to remotely connect to a Linux desktop is VNC. VNC stands for Virtual Network Computing and is a protocol that allows remote access and control of a graphical desktop environment over a network. VNC is natively designed for Linux and can also support other operating systems, such as Windows and Mac OS. VNC can be used to assist users with troubleshooting by viewing and interacting with their desktops remotely. MFA stands for Multi-Factor Authentication and is a method of verifying identity using two or more factors, such as something you know, something you have or something you are. MFA is not a tool that can be used to remotely connect to a Linux desktop but a technique that can be used to enhance security

for systems or services. MSRA stands for Microsoft Remote Assistance and is a feature that allows remote access and control of a Windows desktop environment over a network. MSRA is not natively designed for Linux and may not be compatible or supported by Linux systems. RDP stands for Remote Desktop Protocol and is a protocol that allows remote access and control of a Windows desktop environment over a network. RDP is not natively designed for Linux and may not be compatible or supported by Linux systems. References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.6

NEW QUESTION 261
A user's corporate laptop with proprietary work Information was stolen from a coffee shop. The user togged in to the laptop with a simple password. and no other security mechanisms were in place. Which of the following would MOST likely prevent the stored data from being recovered?

A. Biometrics
B. Full disk encryption
C. Enforced strong system password
D. Two-factor authentication

Answer: B

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

NEW QUESTION 266
An application user received an email indicating the version of the application currently in use will no longer be sold. Users with this version of the application will no longer receive patches or updates either. Which of the following indicates a vendor no longer supports a product?

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

Answer: C

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

NEW QUESTION 269
Which of the following physical security controls can prevent laptops from being stolen?

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

Answer: D

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

NEW QUESTION 270
A technician is replacing the processor in a desktop computer prior to opening the computer, the technician wants to ensure the internal components are protected. Which of the following safety procedures would BEST protect the components in the PC? (Select TWO).

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

Answer: AC

Explanation:
The two safety procedures that would best protect the components in the PC are:
? Utilizing an ESD strap
? Placing the PSU in an antistatic bag

https://www.professormesser.com/free-a-plus-training/220-902/computer-safety- procedures-2/
https://www.skillsoft.com/course/comptia-a-core-2-safety-procedures-environmental-impacts-cbdf0f2c-61c0-4f4a-a659-dc98f1f00158

NEW QUESTION 271
A technician is troubleshooting boot times for a user. The technician attempts to use MSConfig to see which programs are starting with the OS but receives a message that it can no longer be used to view startup items. Which of the following programs can the technician use to view startup items?

A. msinfo32
B. perfmon
C. regedit
D. taskmgr

Answer: D

Explanation:
When troubleshooting boot times for a user, a technician may want to check which programs are starting with the operating system to identify any that may be slowing down the boot process. MSConfig is a tool that can be used to view startup items on a Windows system, but it may not always be available or functional. In this scenario, the technician receives a message that MSConfig cannot be used to view startup items. As an alternative, the technician can use Task Manager (taskmgr), which can also display the programs that run at startup. To access the list of startup items in Task Manager, the technician can follow these steps:
? Open Task Manager by pressing Ctrl+Shift+Esc.
? Click the "Startup" tab.
? The list of programs that run at startup will be displayed.

NEW QUESTION 275
Which of the following operating systems is considered closed source?

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

Answer: D

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

NEW QUESTION 278
A neighbor successfully connected to a user's Wi-Fi network. Which of the following should the user do after changing the network configuration to prevent the neighbor from being able to connect again?

A. Disable the SSID broadcast.
B. Disable encryption settings.

C. Disable DHCP reservations.
D. Disable logging.

Answer: A

Explanation:
? A. Disable the SSID broadcast1: The SSID broadcast is a feature that allows a Wi- Fi network to be visible to nearby devices. Disabling the SSID broadcast can make the network harder to find by unauthorized users, but it does not prevent them from accessing it if they know the network name and password.

NEW QUESTION 280
A user's permissions are limited to read on a shared network folder using NTFS security settings. Which of the following describes this type of security control?

A. SMS
B.

MFA
C. ACL
D. MDM

Answer: C

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

NEW QUESTION 285
A technician wants to enable BitLocker on a Windows 10 laptop and is unable to find the BitLocker Drive Encryption menu item in Control Panel. Which of the following explains why the technician unable to find this menu item?

A. The hardware does not meet BitLocker's minimum system requirements.
B. BitLocker was renamed for Windows 10.
C. BitLocker is not included on Windows 10 Home.
D. BitLocker was disabled in the registry of the laptop

Answer: C

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

NEW QUESTION 288
A user is unable to log in to the network. The network uses 802.1X with EAP-TLS to authenticate on the wired network. The user has been on an extended leave and has not logged in to the computer in several months. Which of the following is causing the login issue?

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

Application crash

E. Profile rebuild needed

Answer: A

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

NEW QUESTION 292
A technician is finalizing a new workstation for a user. The user's PC will be connected to the internet but will not require the same private address each time. Which of the following protocols will the technician MOST likely utilize?

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

Answer: A

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

NEW QUESTION 295
Which of the following file extensions should a technician use for a PowerShell script?

A.

.ps1

B. .py
C. .sh
D. .bat

E. .cmd

Answer: A

Explanation:
A PowerShell script is a plain text file that contains one or more PowerShell commands. Scripts have a .ps1 file extension and can be run on your computer or in a remote session. PowerShell scripts can be used to automate tasks and change settings on Windows devices. To create and run a PowerShell script, you need a text editor (such as Visual Studio Code or Notepad) and the PowerShell Integrated Scripting Environment (ISE) console. You also need to enable the correct execution policy to allow scripts to run on your system

NEW QUESTION 297
A macOS user reports seeing a spinning round cursor on a program that appears to be frozen. Which of the following methods does the technician use to force the program to close in macOS?

A. The technician presses the Ctrl+Alt+Del keys to open the Force Quit menu, selects the frozenapplication in the list, and clicks Force Quit.
B. The technician clicks on the frozen application and presses and holds the Esc key on the keyboard for 10 seconds Which causes the application to force quit.
C. The technician opens Finder, navigates to the Applications folder, locates the application that is frozen in the list, right-clicks on the application, and selects the Force Quit option.
D. The technician opens the Apple icon menu, selects Force Quit, selects the frozen application in thelist, and clicks Force Quit.

Answer: D

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

NEW QUESTION 299

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

A. Adjust the content filtering.
B. Unmap port forwarding.
C. Disable unused ports.

D. Reduce the encryption strength

Answer: A

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

NEW QUESTION 302
A user has been unable to receive emails or browse the internet from a smartphone while traveling. However, text messages and phone calls are working without issue. Which of the following should a support technician check FIRST?

A. User account status
B. Mobile OS version
C. Data plan coverage
D. Network traffic outages

Answer: C

Explanation:
The first thing that a support technician should check to resolve the issue of not being able to receive emails or browse the internet from a smartphone while traveling is the data plan coverage. The data plan coverage determines how much data and where the user can use on the smartphone's cellular network. The data plan coverage may vary depending on the user's location, carrier and subscription. The data plan coverage may not include or support certain areas or countries that the user is traveling to, or may charge extra fees or limit the speed or amount of data that the user can use. The data plan coverage does not affect text messages and phone calls, which use different network services and protocols. User account status is not likely to cause the issue of not being able to receive emails or browse the internet from a smartphone while traveling, unless the user account has been suspended or terminated by the carrier or the email provider. Mobile OS version is not likely to cause the issue of not being able to receive emails or browse the internet from a smartphone while traveling, unless the mobile OS has a major bug or compatibility problem with the network or the email app. Network traffic outages may cause the issue of not being able to receive emails or browse the internet from a smartphone while traveling, but they are less likely and less common than data plan coverage issues, and they should also affect text messages and phone calls. References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.5

NEW QUESTION 306
A user updates a mobile device's OS. A frequently used application becomes consistently unresponsive immediately after the device is launched. Which of the following troubleshooting steps should the user perform FIRST?

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

Answer: B

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

NEW QUESTION 307
A department manager submits a help desk ticket to request the migration of a printer's port utilization from USB to Ethernet so multiple users can access the printer. This will be a new network printer, thus a new IP address allocation is required. Which of the following should happen immediately before network use is authorized?

A. Document the date and time of the change.
B. Submit a change request form.
C. Determine the risk level of this change.
D. Request an unused IP address.

Answer: B

Explanation:
A change request form is a document that describes the proposed change, the reason for the change, the impact of the change, and the approval process for the change. A change request form is required for any planned changes to the network, such as adding a new network printer, to ensure that the change is authorized, documented, and communicated to all stakeholders. Submitting a change request form should happen immediately before network use is authorized, as stated in the Official CompTIA A+ Core 2 Study Guide. The other options are either too late (documenting the date and time of the change) or too early (determining the risk level of the change and requesting an unused IP address) in the change management process.

NEW QUESTION 311
A technician needs to ensure that USB devices are not suspended by the operating system Which of the following Control Panel utilities should the technician use to configure the setting?

A. System
B. Power Options

C. Devices and Printers
D. Ease of Access

Answer: B

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

NEW QUESTION 314
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

220-1102 Practice Exam Features:

* 220-1102 Questions and Answers Updated Frequently

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

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

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