

220-1102 Dumps

CompTIA A+ Certification Exam: Core 2

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



NEW QUESTION 1

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

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

Answer: C

Explanation:

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

References⁵: Malware: what it is, how it works, and how to stop it - Norton⁶: How to Prevent Malware: 15 Best Practices for Malware Prevention⁷: 10 Security Tips for How to Prevent Malware Infections - Netwrix

NEW QUESTION 2

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

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

Answer: D

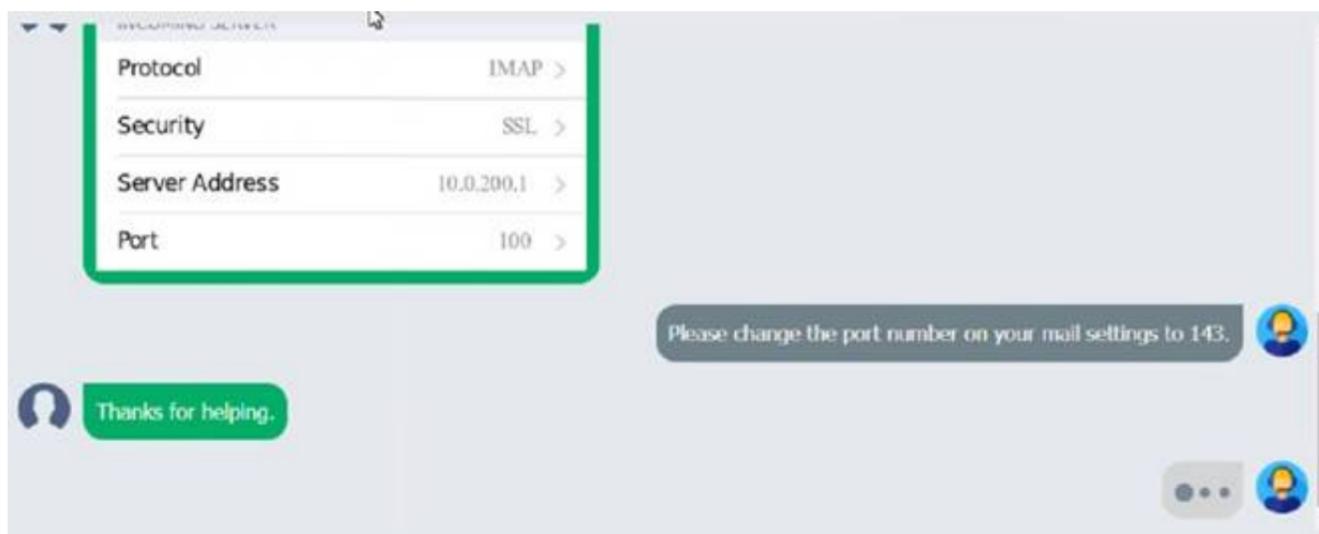
Explanation:

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

NEW QUESTION 3

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

The screenshot shows a help-desk chat interface. On the left, a 'TEST QUESTION' window displays the question text and instructions. The main chat window shows a conversation with 'Telecom'. The chat history includes a message from the user: 'Please follow the new mobile device guide provided on our website.' and a response from Telecom: 'the latest update, here is a screenshot'. The screenshot shows a list of mail settings: IMAP >, SSL >, 10.0.200.1 >, and 100 >. At the bottom of the chat window, there is a text input field with the text 'on your mail settings to 143.' and a 'Send' button.



Which of the following should be done NEXT?

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

Answer: A

NEW QUESTION 4

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 5

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. Video card
- D. Memory

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 6

A user reports a computer is running slow. Which of the following tools will help a technician identify 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 customer installed a new web browser from an unsolicited USB drive that the customer received in the mail. The browser is not working as expected, and internet searches are redirected to another site. Which of the following should the user do next after uninstalling the browser?

- A. Delete the browser cookies and history.
- B. Reset all browser settings.
- C. Change the browser default search engine.

D. Install a trusted browser.

Answer: D

Explanation:

The customer's web browser is likely infected by a browser hijacker, which is a type of malware that changes the browser's settings and redirects the user to malicious websites. A browser hijacker can also steal the user's personal data, display unwanted ads, and install more malware on the device. To remove a browser hijacker, the user should first uninstall the browser from the Control Panel, then scan the device with an antivirus or anti-malware program, and finally install a trusted browser from a legitimate source. Deleting the browser cookies and history, resetting the browser settings, or changing the browser default search engine may not be enough to get rid of the browser hijacker, as it may have embedded itself into the system or other browser components.

NEW QUESTION 8

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

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

Answer: C

Explanation:

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

NEW QUESTION 9

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 Viewer
- 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 10

Which of the following is used to identify potential issues with a proposed change prior to implementation?

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

Answer: D

Explanation:

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

NEW QUESTION 10

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

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

Answer: D

Explanation:

A keylogger is a type of malware that records the keystrokes of a user and sends them to a remote attacker. A keylogger can be used to steal passwords, credit card numbers, personal information, and other sensitive data. A keylogger can be delivered through a USB drive that contains a malicious executable file, such as

grabber.exe, and an output file that stores the captured keystrokes, such as output.txt. The other options are not likely to use this method of attack. References: : <https://www.comptia.org/training/resources/exam-objectives/comptia-a-core-2-exam-objectives> : <https://www.kaspersky.com/resource-center/definitions/keylogger>

NEW QUESTION 12

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

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

Answer: B

Explanation:

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

NEW QUESTION 16

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

- A. resmon.exe
- B. msconfig.exe
- C. dfrgui.exe
- D. msinfo32.exe

Answer: C

Explanation:

The technician should use dfrgui.exe to defragment the hard drive.

NEW QUESTION 18

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 Security

NEW QUESTION 22

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

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

Answer: C

Explanation:

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

NEW QUESTION 27

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

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

Answer: D

Explanation:

Open-ended questions are questions that require more than a yes or no answer and encourage the customer to provide more details and information. Using open-ended questions can help the support technician to understand the problem better, identify the root cause, and find a suitable solution.

Some examples of open-ended questions are:

- ? What exactly is not working on your machine?
- ? When did you notice the problem?
- ? How often does the problem occur?
- ? What were you doing when the problem happened?
- ? What have you tried to fix the problem?

Offering to wipe and reset the device for the customer is not a good option, as it may result in data loss and inconvenience for the customer. It should be used as a last resort only if other troubleshooting steps fail. Advising that the help desk will investigate and follow up at a later date is not a good option, as it may leave the customer unsatisfied and frustrated. It should be used only if the problem requires further research or escalation and cannot be resolved on the first call. Putting the customer on hold and escalating the call to a manager is not a good option, as it may waste time and resources. It should be used only if the problem is beyond the support technician's scope or authority and requires managerial intervention.

NEW QUESTION 32

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 charged. If the battery is low, the device may not have enough power to complete the update.

In this scenario, the technician has already determined that there are no error messages on the device. The next best step would be to check if the battery is sufficiently charged. If the battery is low, it could be preventing the device from completing the update process. Verifying that third-party applications are disabled, determining if the device has adequate storage available, and confirming a strong internet connection are all important steps in troubleshooting issues with mobile devices. However, since the problem in this scenario is related to a failed OS update, it is important to first check the battery level before proceeding with further troubleshooting steps.

NEW QUESTION 36

A 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 37

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

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

Answer: E

Explanation:

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

NEW QUESTION 39

A systems administrator is experiencing issues connecting from a laptop to the corporate network using PKI. Which of 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 41

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

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

Answer: B

Explanation:

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

NEW QUESTION 42

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

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

Answer: D

Explanation:

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

NEW QUESTION 43

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

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

Answer: A

Explanation:

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

NEW QUESTION 47

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

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

Answer: D

Explanation:

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

NEW QUESTION 50

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 (220-1102) Certification Exam Objectives Version 4.0, Domain 5.1

NEW QUESTION 51

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 System
- B. Troubleshooting System
- D. Device Manager
- E. Administrative Tools

Answer: D

NEW QUESTION 53

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

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

Answer: D

Explanation:

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

NEW QUESTION 54

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

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

Answer: D

Explanation:

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

NEW QUESTION 58

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 62

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 67

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 69

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. PII
- 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 (220-1102) Certification Exam Objectives Version 4.0, Domain 5.1

NEW QUESTION 72

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-\(3-0\)](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 73

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

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

Answer: B

Explanation:

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

NEW QUESTION 75

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 78

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 80

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 83

A technician is hardening a company file server and needs to prevent unauthorized LAN devices from accessing stored files. Which of the following should the technician use?

- A. Software firewall
- B. Password complexity
- C. Antivirus application
- D. Anti-malware scans

Answer: A

Explanation:

A software firewall is a program that monitors and controls the incoming and outgoing network traffic on a computer or a server. A software firewall can help prevent unauthorized LAN devices from accessing stored files on a company file server by applying rules and policies that filter the network packets based on their source, destination, protocol, port, or content. A software firewall can also block or allow specific applications or services from communicating with the network, and alert the administrator of any suspicious or malicious activity¹².

A software firewall is a better option than the other choices because:

? Password complexity (B) is a good practice to protect the file server from

unauthorized access, but it is not sufficient by itself. Password complexity refers to the use of strong passwords that are hard to guess or crack by attackers, and that are changed frequently and securely. Password complexity can prevent brute force attacks or credential theft, but it cannot stop network attacks that exploit vulnerabilities in the file server software or hardware, or that bypass the authentication process³⁴.

? Antivirus application © and anti-malware scans (D) are important tools to protect

the file server from viruses and malware that can infect, damage, or encrypt the stored files. However, they are not effective in preventing unauthorized LAN devices from accessing the files in the first place. Antivirus and anti-malware tools can only detect and remove known threats, and they may not be able to stop zero- day attacks or advanced persistent threats that can evade or disable them. Moreover, antivirus and anti-malware tools cannot control the network traffic or the file server permissions, and they may not be compatible with all file server platforms or configurations⁵⁶.

References:

1: What is a Firewall and How Does it Work? - Cisco¹ 2: How to Harden Your Windows Server - ServerMania² 3: Password Security: Complexity vs. Length - Norton⁷ 4: Password Hardening: 5 Ways to Protect Your Passwords - Infosec⁵ 5: What is Antivirus Software and How Does it Work? - Kaspersky⁶ 6: What is Anti-Malware? - Malwarebytes

NEW QUESTION 85

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

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

Answer: B

Explanation:

Ease of Access is a utility in the Control Panel that allows users to adjust various accessibility settings on Windows, such as the on-screen keyboard, magnifier, narrator, high contrast, etc. The on-screen keyboard can be turned on by going to Ease of Access > Keyboard and toggling the switch to On¹². Alternatively, the on-screen keyboard can be opened by pressing Windows + Ctrl + O keys or by typing osk.exe in the Run dialog box³.

References: 1 Use the On-Screen Keyboard (OSK) to type(<https://support.microsoft.com/en-us/windows/use-the-on-screen-keyboard-osk-to-type-ecbb5e08-5b4e-d8c8-f794-81dbf896267a>)² How to Enable or Disable the On-Screen Keyboard in Windows 10 - Lifewire(<https://www.lifewire.com/enable-or-disable-on-screen-keyboard-in-windows-10-5180667>)³ On-Screen Keyboard Settings, Tips and Tricks in Windows 11/10(<https://www.thewindowsclub.com/windows-onscreen-keyboard>).

NEW QUESTION 87

Which of the following defines the extent of a change?

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

Answer: A

Explanation:

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

References: CompTIA A+ Core 2 (220-1102) Certification Exam Objectives Version 4.0, Domain 5.2

NEW QUESTION 90

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. Automatic screen lock
- C. Account lockout
- D. Antivirus

Answer: B

Explanation:

Account lockout would best mitigate the threat of a dictionary attack1

NEW QUESTION 95

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

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

Answer: D

Explanation:

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

NEW QUESTION 97

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 102

A user rotates a cell phone horizontally to read emails, but the display remains vertical, even though the settings indicate autorotate is on. Which 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 105

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

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

Answer: B

Explanation:

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

NEW QUESTION 106

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 111

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

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

Answer: C

Explanation:

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

NEW QUESTION 114

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 119

Remote employees need access to information that is hosted on local servers at the company. The IT department needs to find a solution that gives employees secure access to the company's resources as if the employees were on premises. Which of the following remote connection services should the IT team implement?

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

Answer: C

Explanation:

A VPN (Virtual Private Network) is a service that allows remote employees to access the company's network resources securely over the internet as if they were on premises. A VPN encrypts the data traffic between the employee's device and the VPN server, and assigns the employee a virtual IP address that belongs to

the company's network. This way, the employee can access the local servers, files, printers, and other resources without exposing them to the public internet. A VPN also protects the employee's privacy and identity by masking their real IP address and location.

NEW QUESTION 124

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 127

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

If airplane mode is enabled

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

Answer: C

Explanation:

NFC stands for Near Field Communication, and it is a wireless technology that allows your phone to act as a contactless payment device, among other things². Payment applications that allow payments to be made with a mobile device usually rely on NFC to communicate with the payment terminal¹. Therefore, if NFC is disabled on the phone, the payment will not work. To enable NFC on an Android phone, you need to follow these steps³:

? On your Android device, open the Settings app.

? Select Connected devices.

? Tap on Connection preferences.

? You should see the NFC option. Toggle it on.

The other options are not directly related to using a payment application with a mobile device. Airplane mode is a setting that disables all wireless communication on the phone, including NFC⁴, but it also affects calls, texts, and internet access. Bluetooth is a wireless technology that allows you to connect your phone with other devices such as headphones or speakers, but it is not used for contactless payments. Wi-Fi is a wireless technology that allows you to access the internet or a local network, but it is also not used for contactless payments. Location services are a feature that allows your phone to determine your geographic location using GPS or other methods, but they are not required for contactless payments.

NEW QUESTION 129

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

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

Answer: A

Explanation:

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

NEW QUESTION 131

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

- A. yum
- B. grep
- C. ls
- 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 132

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 (220-1102) Certification Exam Objectives Version 4.0, Domain 1.6

NEW QUESTION 137

A network technician is deploying a new machine in a small branch office that does not have a DHCP server. The new machine automatically receives the IP address of 169.254.0.2 and is unable to communicate with the rest of the network. Which of the following would restore communication?

- A. Static entry
- B. ARP table
- C.

APIPA address

- D. NTP specification

Answer: A

Explanation:

A static entry is the best option to restore communication for the new machine in a small branch office that does not have a DHCP server. A static entry means manually configuring the IP address, subnet mask, default gateway, and DNS server for the network adapter of the machine. A static entry ensures that the machine has a valid and unique IP address that matches the network configuration and can communicate with the rest of the network.

The new machine automatically receives the IP address of 169.254.0.2 because it uses APIPA (Automatic Private IP Addressing), which is a feature that enables computers to self-assign an IP address when a DHCP server is not available. However, APIPA only works for local communication within the same subnet, and does not provide a default gateway or a DNS server. Therefore, the new machine is unable to communicate with the rest of the network, which may be on a different subnet or require a gateway or a DNS server to access.

The other options are not related to restoring communication for the new machine. ARP table is a cache that stores the mapping between IP addresses and MAC addresses for the devices on the network. NTP specification is a protocol that synchronizes the clocks of the devices on the network.

References:

? CompTIA A+ Certification Exam Core 2 Objectives1

- ? CompTIA A+ Core 2 (220-1102) Certification Study Guide2
- ? What is APIPA (Automatic Private IP Addressing)? - Study-CCNA3
- ? How to Configure a Static IP Address in Windows and OS X4

NEW QUESTION 142

A company would like to implement multifactor authentication for all employees at a minimal cost. Which of the following best meets the company's requirements?

- A. Biometrics
- B. Soft token
- C. Access control lists
- D. Smart card

Answer: B

Explanation:

A soft token, also known as a software token or an OTP (one-time password) app, is a type of multifactor authentication that generates a temporary code or password on a user's device, such as a smartphone or a tablet. The user must enter this code or password along with their username and password to access their account or service. A soft token can help improve security by adding an extra layer of verification and preventing unauthorized access even if the user's credentials are compromised. A soft token can also be implemented at a minimal cost, as it does not require any additional hardware or infrastructure. Biometrics, access control lists, and smart card are not types of multifactor authentication that can be implemented at a minimal cost.

NEW QUESTION 144

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 146

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.skillssoft.com/course/comptia-a-core-2-safety-procedures-environmental-impacts-cbdf0f2c-61c0-4f4a-a659-dc98f1f00158>

NEW QUESTION 151

A technician has identified malicious traffic originating from a user's computer. Which of the following is the best way to identify the source of the attack?

- A. Investigate the firewall logs.
- B. Isolate the machine from the network.
- C. Inspect the Windows Event Viewer.
- D. Take a physical inventory of the device.

Answer: B

Explanation:

Isolating the machine from the network is the best way to identify the source of the attack, because it prevents the malicious traffic from spreading to other devices or reaching the attacker. Isolating the machine can also help preserve the evidence of the attack, such as the malware files, the network connections, the registry entries, or the system logs. By isolating the machine, a technician can safely analyze the machine and determine the source of the attack, such as a phishing email, a compromised website, a removable media, or a network vulnerability.

NEW QUESTION 155

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 159

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

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

Answer: A

Explanation:

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

NEW QUESTION 161

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 164

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 169

A user is setting up a computer for the first time and would like to create a secondary login with permissions that are different than the primary login. The secondary login will need to be protected from certain content such as games and websites. Which of the following Windows settings should the user utilize to create the secondary login?

- A. Privacy
- B. Accounts
- C. Personalization
- D. Shared resources

Answer: B

Explanation:

To create a secondary login with different permissions in Windows 10, the user should utilize the Accounts setting. Here are the steps to create a new user account with different permissions:

- ? Right-click the Windows Start menu button.
- ? Select Control Panel.
- ? Select User Accounts.
- ? Select Manage another account.
- ? Select Add a new user in PC settings.
- ? Use the Accounts dialog box to configure a new account.1

NEW QUESTION 171

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

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

Answer: D

Explanation:

The technician should escalate the ticket to ensure that the CEO's device is returned as soon as possible1

NEW QUESTION 172

A user receives the following error while attempting to boot a computer.

BOOTMGR is missing

press Ctrl+Alt+Del to restart

Which of the following should a desktop engineer attempt FIRST to address this issue?

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

Answer: A

Explanation:

The error "BOOTMGR is missing" indicates that the boot sector is damaged or missing1

. The boot sector is a part of the hard disk that contains the code and information needed to

start Windows1. To fix this error, one of the possible methods is to run Startup Repair from Windows Recovery Environment (WinRE)1.

Startup Repair is a tool that can automatically diagnose and repair problems with the boot process2.

References: 1: "Bootmgr is missing Press Ctrl+Alt+Del to restart" error when you start Windows (<https://support.microsoft.com/en-us/topic/-bootmgr-is-missing-press-ctrl-alt-del-to-restart-error-when-you-start-windows-8bc1b94b-d243-1027-5410-aeb04d5cd5e2>) 2: Startup Repair: frequently asked questions (<https://support.microsoft.com/en-us/windows/startup-repair-frequently-asked-questions-f5f412a0-19c4-8e0a-9f68-bb0f17f3daa0>)

NEW QUESTION 175

A technician is setting up a backup method on a workstation that only requires two sets of

tapes to restore. Which of the following would BEST accomplish this task?

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

Answer: D

Explanation:

To accomplish this task, the technician should use a Full backup method

A full backup only requires two sets of tapes to restore because it backs up all the data from the workstation. With a differential backup, the backups need to be taken multiple times over a period of time, so more tapes would be needed to restore the data

NEW QUESTION 177

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

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

Answer: C

Explanation:

The best way to deal with an angry customer who is yelling at a technician is to wait until the customer is done speaking and offer assistance. This shows respect, empathy, and professionalism, and allows the technician to understand the customer's problem and find a solution. According to the CompTIA A+ Core 2 (220-1102) Certification Study Guide¹, some of the steps to handle angry customers are:

- ? Stay calm and do not take it personally.
- ? Listen actively and acknowledge the customer's feelings.
- ? Apologize sincerely and offer to help.
- ? Restate the customer's issue and ask for clarification if needed.
- ? Explain the possible causes and solutions for the problem.
- ? Provide clear and realistic expectations for the resolution.

? Follow up with the customer until the issue is resolved.

The other options are not appropriate ways to deal with angry customers, as they may worsen the situation or damage the customer relationship. Placing the customer on hold may make them feel ignored or dismissed. Disconnecting the call may make them feel disrespected or abandoned. Escalating the issue to a supervisor may make them feel frustrated or powerless, unless the technician cannot resolve the issue or the customer requests to speak to a supervisor.

References:

- ? CompTIA A+ Certification Exam Core 2 Objectives²
- ? CompTIA A+ Core 2 (220-1102) Certification Study Guide¹
- ? How To Deal with Angry Customers (With Examples and Tips)³
- ? 17 ways to deal with angry customers: Templates and examples⁴
- ? Six Ways to Handle Angry Customers⁵

NEW QUESTION 182

Which of the following would cause a corporate-owned iOS device to have an Activation Lock issue?

- A. A forgotten keychain password
- B. An employee's Apple ID used on the device
- C. An operating system that has been jailbroken
- D. An expired screen unlock code

Answer: B

Explanation:

Activation Lock is a feature that prevents anyone from erasing or activating an iOS device without the owner's Apple ID and password. If a corporate-owned iOS device is linked to an employee's Apple ID, it will have an Activation Lock issue when the employee leaves the company or forgets their Apple ID credentials.

Reference: CompTIA A+ Core 2 Exam Objectives, Section 4.1

NEW QUESTION 183

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 187

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

- A. Verify the Wi-Fi connection status.
- B. Enable the NFC setting on the device.
- C. Bring the device within Bluetooth range.
- D. Turn on device tethering.

Answer: C

Explanation:

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

NEW QUESTION 188

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

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

Answer: A

Explanation:

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

NEW QUESTION 189

A technician has been tasked with troubleshooting audiovisual issues in a conference room. The meeting presenters are unable to play a video with sound. The following error is received:

The Audio Driver is not running.

Which of the following will MOST likely resolve the issue?

- A. compmgmt.msc
- B. regedit.exe
- C. explorer.exe
- D. taskmgmt.exe
- E. gpmmc.msc
- F. services.msc

Answer: F

Explanation:

services.msc is a tool that can be used to resolve the issue of "The Audio Driver is not running" on a Windows machine. It allows a technician to view, start, stop and configure the services that run on the system, such as the Windows Audio service. compmgmt.msc, regedit.exe, explorer.exe, taskmgmt.exe and gpmmc.msc are other tools that can be used for different purposes on a Windows machine, but they are not related to audio drivers or services. Verified References: <https://www.comptia.org/blog/what-is-services-msc> <https://www.comptia.org/certifications/a>

NEW QUESTION 191

Which of the following should be done NEXT?

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

Answer: D

Explanation:

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

NEW QUESTION 193

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

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

Answer: C

Explanation:

Badge readers are used to implement secure physical access to a data center. They are used to read the identification information on an employee's badge and grant access to the data center if the employee is authorized.

This system requires individuals to have an access badge that contains their identification information or a unique code that can be scanned by a reader. After the badge is scanned, the system compares the information on the badge with the authorized personnel database to authenticate if the individual has the required clearance to enter that area. The other options listed, such as a geofence, alarm system, or motion sensor are security measures that may be used in conjunction with badge readers, but do not provide identification and authentication features.

NEW QUESTION 198

Which of the following would typically require the most computing resources from the host computer?

- A. Chrome OS
- B. Windows
- C. Android
- D. macOS
- E. Linux

Answer: B

Explanation:

Windows is the operating system that typically requires the most computing resources from the host computer, compared to the other options. Computing resources include hardware components such as CPU, RAM, disk space, graphics card, and network adapter. The minimum system requirements for an operating system indicate the minimum amount of computing resources needed to install and run the operating system on a computer. The higher the minimum system requirements, the more computing resources the operating system consumes.

According to the web search results, the minimum system requirements for Windows 10 and Windows 11 are as follows:

- ? CPU: 1 GHz or faster with two or more cores (Windows 10); 1 GHz or faster with two or more cores on a compatible 64-bit processor (Windows 11)
- ? RAM: 1 GB for 32-bit or 2 GB for 64-bit (Windows 10); 4 GB (Windows 11)
- ? Disk space: 16 GB for 32-bit or 32 GB for 64-bit (Windows 10); 64 GB (Windows 11)
- ? Graphics card: DirectX 9 or later with WDDM 1.0 driver (Windows 10); DirectX 12 compatible with WDDM 2.0 driver (Windows 11)
- ? Network adapter: Ethernet or Wi-Fi (Windows 10); Ethernet or Wi-Fi that supports 5 GHz (Windows 11)

The minimum system requirements for macOS Ventura are as follows:

- ? CPU: Intel Core i3 or higher, or Apple M1 chip
- ? RAM: 4 GB
- ? Disk space: 35.5 GB
- ? Graphics card: Metal-capable
- ? Network adapter: Ethernet or Wi-Fi

The minimum system requirements for Chrome OS are as follows:

- ? CPU: Intel Celeron or higher
- ? RAM: 2 GB

- ? Disk space: 16 GB
- ? Graphics card: Integrated
- ? Network adapter: Ethernet or Wi-Fi

The minimum system requirements for Android are as follows:

- ? CPU: 1 GHz or higher

- ? RAM: 512 MB
- ? Disk space: 8 GB
- ? Graphics card: OpenGL ES 2.0
- ? Network adapter: Ethernet or Wi-Fi

The minimum system requirements for Linux vary depending on the distribution, but a common example is Ubuntu, which has the following minimum system requirements:

- ? CPU: 2 GHz dual core processor or better
- ? RAM: 4 GB
- ? Disk space: 25 GB
- ? Graphics card: 1024 x 768 screen resolution
- ? Network adapter: Ethernet or Wi-Fi

Based on the comparison of the minimum system requirements, Windows has the highest requirements for CPU, RAM, disk space, and graphics card, while Chrome OS and Android have the lowest requirements. macOS and Linux have moderate requirements, depending on the hardware and software configuration. Therefore, Windows is the operating system that typically requires the most computing resources from the host computer.

References:

- ? Windows, macOS, Chrome OS, or Linux: Which Operating System Is Right for You?1
- ? Comparison of operating systems3
- ? Windows 10 vs 11 Minimum System Requirements: Why Need a New One?2
- ? macOS Monterey - Technical Specifications
- ? Chrome OS - Wikipedia
- ? Android - Wikipedia
- ? Installation/SystemRequirements - Community Help Wiki

NEW QUESTION 202

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

the technician's actions?

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

Answer: A

Explanation:

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

NEW QUESTION 205

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

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

Answer: A

Explanation:

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

NEW QUESTION 206

A macOS user is installing a new application. Which of the following system directories is the software MOST likely to install by default?

- A. /etc/services
- B. /Applications
- C. /usr/bin
- D. C:\Program Files

Answer: B

Explanation:

The software is most likely to install by default in the /Applications directory, which is the standard location for macOS applications. This directory can be accessed from the Finder sidebar or by choosing Go > Applications from the menu bar. The /Applications directory contains all the applications that are available to all users on the system1. Some applications might also offer the option to install in the ~/Applications directory, which is a personal applications folder for a single user2. The /etc/services directory is a system configuration file that maps service names to port numbers and protocols3. The /usr/bin directory is a system directory that contains executable binaries for various commands and utilities4. The C:\Program Files directory is a Windows directory that does not exist on macOS.

NEW QUESTION 208

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

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

Answer: B

Explanation:

The user should install and run Linux and the required application as a virtual machine installed under the Windows OS. This solution would allow for parallel execution of the Linux application and Windows applications.

The MOST efficient solution that allows for parallel execution of the Linux application and Windows applications is to install and run Linux and the required application as a virtual machine installed under the Windows OS. This is because it allows you to run both Linux and Windows together without the need to keep the Linux portion confined to a VM window.

NEW QUESTION 210

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

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

Answer: D

Explanation:

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

NEW QUESTION 214

A branch office suspects a machine contains ransomware. Which of the following mitigation steps should a technician take first?

- A. Disable System Restore.
- B. Remediate the system.
- C. Educate the system user.
- D. Quarantine the system.

Answer: D

Explanation:

The first mitigation step that a technician should take when a machine is suspected to contain ransomware is to quarantine the system. This means isolating the infected machine from the network and other devices, to prevent the ransomware from spreading and encrypting more data. The technician can quarantine the system by disconnecting the network cable, turning off the wireless adapter, or using firewall rules to block the traffic from and to the machine.

This step is more important than the other options because:

? Disabling System Restore (A) is not a priority, as it will not stop the ransomware from running or spreading. System Restore is a feature that allows users to restore their system to a previous state, but it may not work if the ransomware has encrypted or deleted the restore points. Moreover, disabling System Restore may prevent the user from recovering some data or settings in the future.

? Remediating the system (B) is the ultimate goal, but it cannot be done before quarantining the system. Remediating the system means removing the ransomware, restoring the data, and fixing the vulnerabilities that allowed the attack. However, this process requires careful analysis, planning, and execution, and it may not be possible if the ransomware is still active and communicating with the attackers. Therefore, the technician should first isolate the system and then proceed with the remediation steps.

? Educating the system user (C) is a preventive measure, but it is not a mitigation step. Educating the system user means raising awareness and providing training on how to avoid ransomware attacks, such as by recognizing phishing emails, avoiding suspicious links or attachments, and updating and patching the system regularly. However, this step will not help if the system is already infected, and it may not be effective if the user is not willing or able to follow the best practices. Therefore, the technician should focus on resolving the current incident and then educate the user as part of the recovery plan.

References:

1: How to Mitigate Ransomware Attacks in 10 Steps - Heimdal Security
2: 3 steps to prevent and recover from ransomware | Microsoft Security Blog
3: How to use System Restore on Windows 10 | Windows Central
4: Ransomware Mitigation | Prevention and Mitigation Strategies - Delinea

NEW QUESTION 218

Which of the following command-line tools will delete a directory?

- A. md
- B. del
- C. dir
- D. rd
- E. cd

Answer: D

Explanation:

To delete an empty directory, enter `rd Directory` or `rmdir Directory`. If the directory is not empty, you can remove files and subdirectories from it using the `/s` switch. You can also use the `/q` switch to suppress confirmation messages (quiet mode).

NEW QUESTION 223

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

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

Answer: A

Explanation:

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

NEW QUESTION 226

After a company installed a new SOHO router customers were unable to access the company-hosted public website. Which of the following will MOST likely allow customers to access the website?

- A. Port forwarding
- B. Firmware updates
- C. IP filtering
- D. Content filtering

Answer: B

Explanation:

If customers are unable to access the company-hosted public website after installing a new SOHO router, the company should check for firmware updates. Firmware updates can fix bugs and compatibility issues that may be preventing customers from accessing the website. The company should also ensure that the router is properly configured to allow traffic to the website. If the router is blocking traffic to the website, the company should configure the router to allow traffic to the website.

NEW QUESTION 228

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

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

Answer: B

Explanation:

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

? Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 14

? CompTIA A+ Complete Study Guide: Core 1 Exam 220-1101 and Core 2 Exam ..., page 105

NEW QUESTION 233

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

Full

- A**: Non-parity
- C. Differential
- D. Incremental

Answer: A

Explanation:

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

NEW QUESTION 236

A suite of security applications was installed a few days ago on a user's home computer.

The user reports that the computer has been running slowly since the installation. The user notices the hard drive activity light is constantly solid. Which of the following should be checked FIRST?

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

Answer: C

Explanation:

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

NEW QUESTION 237

A new employee is having difficulties using a laptop with a docking station. The laptop is connected to the docking station, and the laptop is closed. The external monitor works for a few seconds, but then the laptop goes to sleep. Which of the following options should the technician configure in order to fix the issue?

- A. Hibernate
- B. Sleep/suspend
- C. Choose what closing the lid does
- D. Turn on fast startup

Answer: C

Explanation:

The correct answer is C. Choose what closing the lid does. This option allows you to configure how the laptop behaves when you close the lid, such as whether it goes to sleep, hibernates, shuts down, or does nothing. To access this option, you can follow these steps :

- ? Go to Settings > System > Power & sleep.
- ? Click on Additional power settings on the right side.
- ? Click on Choose what closing the lid does on the left side.
- ? Under When I close the lid, select Do nothing for both On battery and Plugged in.
- ? Click on Save changes.

This will prevent the laptop from going to sleep when you close the lid while it is connected to the docking station and the external monitor.

Hibernate, sleep/suspend, and turn on fast startup are not the options that should be configured to fix the issue. Hibernate and sleep/suspend are both power-saving modes that allow you to resume your work without losing any data. However, they also turn off the display and other components of the laptop, which means you will not be able to use the external monitor when the laptop is closed. Turn on fast startup is a feature that reduces the boot time of Windows by saving some system information to a file when you shut down. It does not affect how the laptop behaves when you close the lid .

NEW QUESTION 241

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

- A. Spyware
- B. Cryptominer
- C. Ransomware
- D. Boot sector virus

Answer: B

Explanation:

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

NEW QUESTION 243

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

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

Answer: A

Explanation:

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

NEW QUESTION 248

A user reports that antivirus software indicates a computer is infected with viruses. The user thinks this happened while browsing the internet. The technician does not recognize the interface with which the antivirus message is presented. Which of the following is the NEXT step the technician should take?

- A. Shut down the infected computer and swap it with another computer
- B. Investigate what the interface is and what triggered it to pop up
- C. Proceed with initiating a full scan and removal of the viruses using the presented interface
- D. Call the phone number displayed in the interface of the antivirus removal tool

Answer: B

Explanation:

The technician should not proceed with initiating a full scan and removal of the viruses using the presented interface or call the phone number displayed in the interface of the antivirus removal tool¹²

Shutting down the infected computer and swapping it with another computer is not necessary at this point¹²

The technician should not immediately assume that the message is legitimate or perform any actions without knowing what the interface is and what triggered it to pop up. It is important to investigate the issue further, including checking the legitimacy of the antivirus program and the message it is displaying.

NEW QUESTION 251

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

- A. Roll back the updates.
- B. Increase the page file.
- C. Update the drivers.
- D. Rebuild the profile.

Answer: D

Explanation:

The issue is specific to the user's profile, so the technician should rebuild the profile. Rebuilding the profile will create a new profile and transfer the user's data to the new profile¹

NEW QUESTION 252

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

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

Answer: B

Explanation:

The most likely reason that the system is not utilizing all the available RAM is that the system is utilizing a 32-bit OS. A 32-bit OS is an operating system that uses 32 bits to address memory locations and perform calculations. A 32-bit OS can only support up to 4GB of RAM, and some of that RAM may be reserved for hardware devices or system functions, leaving less than 4GB of usable RAM for applications and processes. A 32-bit OS cannot recognize or utilize more than 4GB of RAM, even if more RAM is installed on the system. To utilize all the available RAM, the system needs to use a 64-bit OS, which can support much more RAM than a 32-bit OS. The system missing updates may cause some performance or compatibility issues, but it does not affect the amount of usable RAM on the system. The system's memory failing may cause some errors or crashes, but it does not affect the amount of usable RAM on the system. The system requiring BIOS updates may cause some configuration or compatibility issues, but it does not affect the amount of usable RAM on the system. References: CompTIA A+ Core 2 (220-1102) Certification

Exam Objectives Version 4.0, Domain 1.1

NEW QUESTION 257

A user's company phone was stolen. Which of the following should a technician do next?

- A. Perform a low-level format.
- B. Remotely wipe the device.
- C. Degauss the device.
- D. Provide the GPS location of the device.

Answer: B

Explanation:

Remotely wiping the device is the best option to prevent unauthorized access to the company data stored on the phone. A low-level format, degaussing, or providing the GPS location of the device are not feasible or effective actions to take in this scenario.

References: The Official CompTIA A+ Core 2 Study Guide¹, page 315.

NEW QUESTION 261

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

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

Answer: A

Explanation:

This is because a PIN is a fast and secure method of logging in to laptops, and it is more secure than a password because it is not susceptible to keyloggers.

NEW QUESTION 266

A user receives a call from someone claiming to be a technical support agent. The caller asks the user to log in to the computer. Which of the following security measures should the user take to ensure security and privacy?

- A. Only accept calls from known people.
- B. Disregard any suspicious emails.
- C. Update the antivirus software.
- D. Enable two-factor authentication.
- E. Install a malware scanner.

Answer: A

Explanation:

This is a scenario of a potential tech support scam, where a fraudster pretends to be a technical support agent and tries to trick the user into giving them access to the computer, personal information, or money. The user should not trust any unsolicited calls from unknown people claiming to be from tech support, as they might be trying to install malware, steal data, or charge for fake services. The user should only accept calls from known people, such as their IT department, their service provider, or their software vendor, and verify their identity before logging in to the computer. The user should also report any suspicious calls to the appropriate authorities or organizations.

References:

- ? How to protect against tech support scams1
- ? Avoid and report Microsoft technical support scams2
- ? How to Protect Against Technical Support Scams3
- ? How To Recognize and Avoid Tech Support Scams4

NEW QUESTION 270

A wireless network is set up, but it is experiencing some interference from other nearby

SSIDs. Which of the following can BEST resolve the interference?

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

Answer: A

Explanation:

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

NEW QUESTION 274

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

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

Answer: D

Explanation:

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

NEW QUESTION 278

A corporate smartphone was stored for five months after setup. During this time, the company did not have any system updates. When the phone is turned on, an application runs, but it crashes intermittently. Which of the following should a technician do next?

- A. Restart the phone.
- B. Reimage the OS.
- C. Reinstall the application.
- D. Clear the cache.

Answer: C

Explanation:

Reinstalling the application is the best option to fix the intermittent crashing of the application on the corporate smartphone. Reinstalling the application will ensure that the latest version of the app is installed, which may have bug fixes and compatibility updates that can resolve the crashing issue. Reinstalling the app will also clear any corrupted or outdated data or cache that may cause the app to malfunction.

The other options are not as effective or appropriate as reinstalling the app. Restarting the phone may temporarily fix the issue, but it will not address the root cause of the app crashing, which may be related to the app itself or its data. Reimaging the OS is a drastic and unnecessary measure that will erase all the data

and settings on the phone and restore it to its factory state. This will also remove all the other apps and files that may be important for the corporate use of the phone. Clearing the cache may help to free up some space and improve the performance of the app, but it will not update the app or fix any bugs that may cause the app to crash.

References:

- ? Top 5 Reasons Behind Your App Crash and Solutions To Fix Them¹
- ? How to Stop Apps From Crashing on Android²
- ? Why are my Android phone apps crashing or closing & how to fix the issue³

NEW QUESTION 280

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

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

Answer: B

Explanation:

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

NEW QUESTION 282

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

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

Answer: D

Explanation:

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

NEW QUESTION 285

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

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

Answer: C

Explanation:

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

NEW QUESTION 290

A user needs assistance installing software on a Windows PC but will not be in the office. Which of the following solutions would a technician MOST likely use to assist the user without having to install additional software?

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

Answer: B

Explanation:

MSRA stands for Microsoft Remote Assistance, and it is a feature that allows a technician to remotely view and control another user's Windows PC with their permission. MSRA is built-in to Windows and does not require any additional software installation. To use MSRA, the technician and the user need to follow these steps:

- ? On the user's PC, type msra in the search box on the taskbar and select Invite someone to connect to your PC and help you, or offer to help someone else.
- ? Select Save this invitation as a file and choose a location to save the file. This file contains a password that the technician will need to connect to the user's PC.
- ? Send the file and the password to the technician via email or another secure method.
- ? On the technician's PC, type msra in the search box on the taskbar and select Help someone who has invited you.
- ? Select Use an invitation file and browse to the location where the file from the user is saved. Enter the password when prompted.
- ? The user will see a message asking if they want to allow the technician to connect to their PC. The user should select Yes.
- ? The technician will see the user's desktop and can request control of their PC by clicking Request control on the top bar. The user should allow this request by clicking Yes.
- ? The technician can now view and control the user's PC and assist them with installing software.

NEW QUESTION 294

A technician was assigned a help desk ticket and resolved the issue. Which of the following should the technician update to assist other technicians in resolving similar issues?

- A. End user training
- B. Progress notes
- C. Knowledge base
- D. Acceptable use policy document

Answer: C

Explanation:

A knowledge base is a centralized repository of information that can be used by technicians to find solutions to common problems, best practices, troubleshooting guides, and other useful resources¹². Updating the knowledge base with the details of the issue and the resolution can help other technicians who encounter similar issues in the future. It can also reduce the number of tickets and improve customer satisfaction³. References¹: The Official CompTIA A+ Core 2 Student Guide (Exam 220-1102), page 10-11 ²: CompTIA A+ Certification Exam Core 2 Objectives, page 13 ³: CompTIA A+ Core 2 (220-1102) Certification Study Guide, page 10-12

NEW QUESTION 299

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

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

Answer: C

Explanation:

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

NEW QUESTION 304

A company is retiring old workstations and needs a certificate of destruction for all hard drives. Which of the following would be BEST to perform on the hard drives to ensure the data is unrecoverable? (Select TWO).

- A. Standard formatting
- B. Drilling
- C. Erasing
- D. Recycling
- E. Incinerating
- F. Low-level formatting

Answer: BE

Explanation:

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

NEW QUESTION 305

A technician discovers user input has been captured by a malicious actor. Which of the following malware types is MOST likely being used?

- A. Cryptominers
- B. Rootkit
- C. Spear phishing
- D. Keylogger

Answer: D

Explanation:

A keylogger is a type of malware that captures user input, such as keystrokes, mouse clicks, and clipboard data, and sends it to a malicious actor. Keyloggers can be used to steal passwords, credit card numbers, personal information, and other sensitive data.
Reference: CompTIA A+ Core 2 Exam Objectives, Section 5.1

NEW QUESTION 308

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

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

Answer: C

Explanation:

The administrator can use Virtual Network Computing (VNC) to troubleshoot the server effectively. VNC is a graphical desktop sharing system that allows the administrator to remotely control the desktop of a Linux server.

NEW QUESTION 309

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

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

Answer: A

Explanation:

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

NEW QUESTION 314

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

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

Answer: C

Explanation:

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

NEW QUESTION 315

A user calls the help desk and reports a workstation is infected with malicious software. Which of the following tools should the help desk technician use to remove the malicious software? (Select TWO).

- A. File Explorer
- B. User Account Control
- C. Windows Backup and Restore
- D. Windows Firewall
- E. Windows Defender
- F. Network Packet Analyzer

Answer: AE

Explanation:

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

NEW QUESTION 317

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

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

* One year free update

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

* Trusted by Millions

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

* Shop Securely

All transactions are protected by VeriSign!

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

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