

CompTIA

Exam Questions 220-1102

CompTIA A+ Certification Exam: Core 2



NEW QUESTION 1

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

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

Answer: D

Explanation:

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

NEW QUESTION 2

A developer receives the following error while trying to install virtualization software on a workstation:

VTx not supported by system

Which of the following upgrades will MOST likely fix the issue?

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

Answer: A

Explanation:

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

NEW QUESTION 3

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

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

Answer: B

Explanation:

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

NEW QUESTION 4

A technician is upgrading the backup system for documents at a high-volume law firm. The current backup system can retain no more than three versions of full backups before failing. The law firm is not concerned about restore times but asks the technician to retain more versions when possible. Which of the following backup methods should the technician MOST likely implement?

- A. Full
- B. Mirror
- C. Incremental
- D. Differential

Answer: C

Explanation:

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

NEW QUESTION 5

Which of the following data is MOST likely to be regulated?

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

Answer: B

Explanation:

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

NEW QUESTION 6

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 7

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

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

Answer: A

Explanation:

When a Blue Screen of Death (BSOD) appears on a Windows workstation, it indicates that there is a serious problem with the operating system. The stop code displayed on the BSOD can provide valuable information to help determine the cause of the issue. The stop code is a specific error code that is associated with the BSOD, and it can help identify the root cause of the problem.

In this scenario, the user has encountered a BSOD and has restarted the PC, only to see the BSOD reappear. This suggests that the problem is persistent and requires further investigation. By analyzing the stop code displayed on the BSOD, a technician can begin to identify the underlying issue and take appropriate actions to resolve it.

NEW QUESTION 8

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

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

Answer: C

Explanation:

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

NEW QUESTION 9

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

- A. eventvwr.msc
- B. perfmon.msc
- C. gpedit.msc
- D. devmgmt.msc

Answer: D

Explanation:

The technician should use devmgmt.msc tool to make adjustments for the touchpad issue after Windows installed updates on a laptop. Devmgmt.msc is a command that opens the Device Manager, which is a utility that allows users to view and manage the hardware devices and drivers installed on a computer. The

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

NEW QUESTION 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 11

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 it is running a 32-bit OS. A 32-bit OS can only address up to 4GB of RAM, and some of that is reserved for hardware and system use¹. Therefore, even if the technician installed 8GB of RAM, the system can only use around 3.5GB of usable RAM. To use the full 8GB of RAM, the technician would need to install a 64-bit OS, which can address much more memory². The system missing updates, the system's memory failing, or the system requiring BIOS updates are not likely to cause this issue.

References: ² <https://support.microsoft.com/en-us/windows/windows-10-system-requirements-6d4e9a79-66bf-7950-467c-795cf0386715> ¹ <https://www.makeuseof.com/tag/unlock-64gb-ram-32-bit-windows-pae-patch/>

NEW QUESTION 14

A systems administrator is configuring centralized desktop management for computers on a domain. The management team has decided that all users' workstations should have the same network drives, printers, and configurations. Which of the following should the administrator use to accomplish this task?

- A. Network and Sharing Center
- B. net use
- C. User Accounts
- D. regedit
- E. Group Policy

Answer: E

Explanation:

Group Policy is a feature of Windows that allows administrators to centrally manage and apply policies and settings to computers and users on a domain³. Group Policy can be used to configure network drives, printers, security settings, desktop preferences, and other configurations for all users' workstations³. Network and Sharing Center, net use, User Accounts, and regedit are not tools that can accomplish this task.

NEW QUESTION 15

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

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

Answer: D

Explanation:

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

NEW QUESTION 19

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

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

Answer: A

Explanation:

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

NEW QUESTION 23

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

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

Answer: A

Explanation:

Risk analysis is the process of identifying and evaluating the potential threats and impacts of a change on the system, network, or service. It is an essential step before approving a change request, as it helps to determine the level of risk, the mitigation strategies, and the contingency plans. Risk analysis also helps to prioritize the change requests based on their urgency and importance¹².

References: 1 The Change Request Process and Best Practices(<https://www.processmaker.com/blog/it-change-request-process-best-practices/>)2 Risk Assessment and Analysis Methods: Qualitative and Quantitative(<https://www.isaca.org/resources/isaca-journal/issues/2021/volume-2/risk-assessment-and-analysis-methods>).

NEW QUESTION 25

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

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

Answer: CD

Explanation:

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

NEW QUESTION 29

An Android user contacts the help desk because a company smartphone failed to complete a tethered OS update A technician determines there are no error

messages on the device Which of the following should the technician do NEXT?

- A. Verify all third-party applications are disabled
- B. Determine if the device has adequate storage available.
- C. Check if the battery is sufficiently charged
- D. Confirm a strong internet connection is available using Wi-Fi or cellular data

Answer: C

Explanation:

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

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

NEW QUESTION 33

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

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

Answer: C

Explanation:

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

NEW QUESTION 38

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

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

Answer: C

Explanation:

Open Settings, select System, select Display, and change the Scale and layout setting to a higher percentage123

Reference: 4. How to Increase the Text Size on Your Computer. Retrieved from

<https://www.laptopmag.com/articles/increase-text-size-computer> 5. How to Change the Size of Text in Windows 10. Retrieved from

<https://www.howtogeek.com/370055/how-to-change-the-size-of-text-in-windows-10/> 6. Change the size of text in Windows. Retrieved from

<https://support.microsoft.com/en-us/windows/change-the-size-of-text-in-windows-1d5830c3-eee3-8eaa-836b-abcc37d99b9a>

NEW QUESTION 43

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

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

Answer: D

Explanation:

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

NEW QUESTION 45

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

- A. Navigate to the Control Panel utility, select the Security and Maintenance submenu, select Change Security and Maintenance settings, select Windows Hello Fingerprint, and have the user place a fingerprint on the fingerprint reader repeatedly until Windows indicates setup is complete
- B. Navigate to the Windows 10 Settings menu, select the Accounts submenu, select Sign in options, select Windows Hello Fingerprint, and have the user place a fingerprint on the fingerprint reader repeatedly until Windows indicates setup is complete.

- C. Navigate to the Windows 10 Settings menu, select the Update & Security submenu select Windows Security, select Windows Hello Fingerprint and have the user place a fingerprint on the fingerprint reader repeatedly until Windows indicates setup is complete
- D. Navigate to the Control Panel utility, select the Administrative Tools submenu, select the user account in the list, select Windows Hello Fingerprint, and have the user place a fingerprint on the fingerprint reader repeatedly until Windows indicates setup is complete.

Answer: B

Explanation:

Navigate to the Windows 10 Settings menu, select the Accounts submenu, select Sign in options, select Windows Hello Fingerprint, and have the user place a fingerprint on the fingerprint reader repeatedly until Windows indicates setup is complete. Windows Hello Fingerprint can be set up by navigating to the Windows 10 Settings menu, selecting the Accounts submenu, selecting Sign in options, and then selecting Windows Hello Fingerprint. The user will then be asked to place a fingerprint on the fingerprint reader repeatedly until Windows indicates that setup is complete. Windows Hello Fingerprint allows the user to log into the laptop using just their fingerprint, providing an additional layer of security.

NEW QUESTION 47

A systems administrator is experiencing Issues connecting from a laptop to the corporate network using PKI. Which to the following tools can the systems administrator use to help remediate the issue?

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

Answer: A

Explanation:

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

NEW QUESTION 52

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

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

Answer: B

Explanation:

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

NEW QUESTION 57

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

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

Answer: C

Explanation:

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

NEW QUESTION 62

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

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

Answer: B

Explanation:

Verifying warranty status with the vendor is the most logical next step in the remediation process after determining that a motherboard has failed. A warranty is a

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

NEW QUESTION 65

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 67

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 72

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

- A. Shredding
- B. Degaussing
- C. Low-level formatting
- D. Recycling

Answer: A

Explanation:

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

NEW QUESTION 73

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

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

Answer: A

Explanation:

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

NEW QUESTION 76

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 79

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 83

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

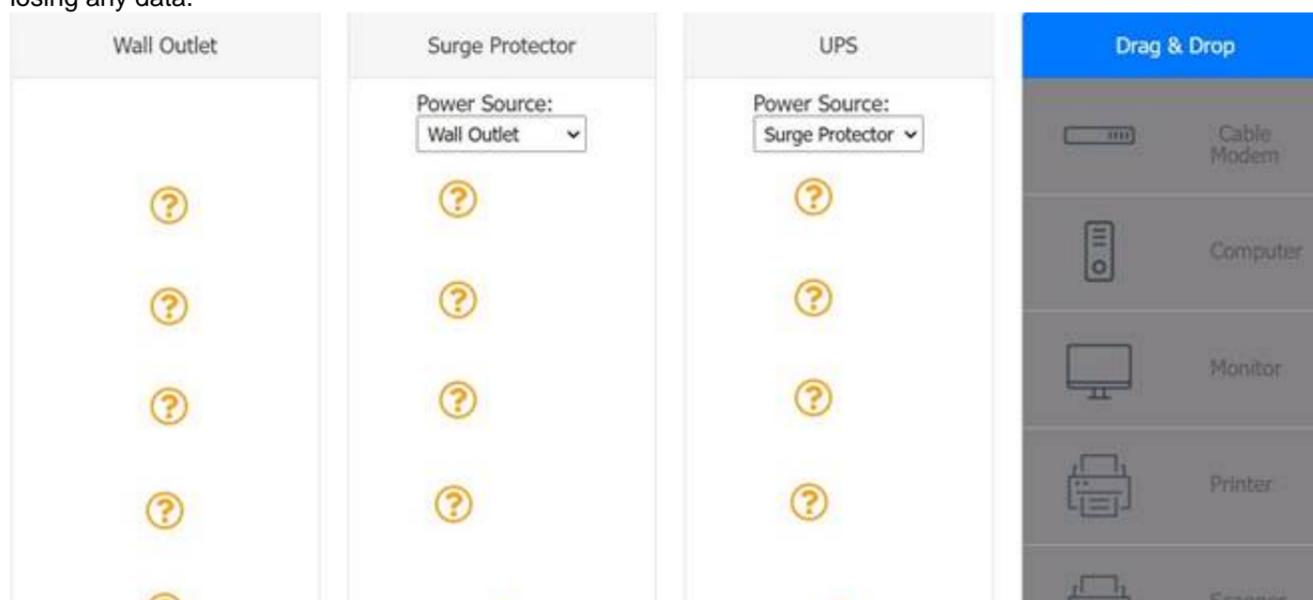
Explanation:

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 88

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.



The interface consists of three vertical columns representing power sources: 'Wall Outlet', 'Surge Protector', and 'UPS'. Each column has a 'Power Source:' dropdown menu at the top, currently set to 'Wall Outlet', 'Surge Protector', and 'Surge Protector' respectively. Below each dropdown are five yellow question mark icons. To the right is a 'Drag & Drop' panel with a blue header. It contains five items: 'Cable Modem' (with a modem icon), 'Computer' (with a computer tower icon), 'Monitor' (with a monitor icon), 'Printer' (with a printer icon), and 'Scanner' (with a scanner icon).

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 89

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. md
- D. rmdir

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 91

Which of the following operating systems is most commonly used in embedded systems?

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

Answer: D

Explanation:

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

NEW QUESTION 96

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? - Cisco
2: How to Harden Your Windows Server - ServerMania
3: Password Security: Complexity vs. Length - Norton
4: Password Hardening: 5 Ways to Protect Your Passwords - Infosec
5: What is Antivirus Software and How Does it Work? - Kaspersky
6: What is Anti-Malware? - Malwarebytes

NEW QUESTION 98

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

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

Answer: C

Explanation:

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

NEW QUESTION 100

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 105

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 109

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 110

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

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

Answer: D

Explanation:

Incremental backups are backups that only include the changes made since the last backup, whether it was a full or an incremental backup. Incremental backups minimize the capacity of storage used and are often used in conjunction with synthetic full backups, which are backups that combine a full backup and subsequent incremental backups into a single backup set.

Reference: CompTIA A+ Core 2 Exam Objectives, Section 3.3

NEW QUESTION 111

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

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

Answer: C

Explanation:

app files are application bundles that contain all the necessary files and resources for a Mac app. They can be easily deleted by dragging them to the Trash or using Launchpad¹². Other file types, such as .exe, .dmg, .rpm, and .pkg, are either not compatible with macOS or require additional steps to uninstall³⁴.

References: 1 Uninstall apps on your Mac - Apple Support(<https://support.apple.com/en-us/102610>)2 How to Uninstall Apps on a Mac (and Make Sure Leftover Files Are

...(<https://www.pcmag.com/how-to/uninstall-delete-apps-from-mac>)3 How to install and uninstall software on a Mac - Laptop

Mag(<https://www.laptopmag.com/articles/install-uninstall-mac-software>)4 How to completely uninstall an app on a Mac and delete all junk files(<https://www.xda-developers.com/how-to-uninstall-app-mac/>).

NEW QUESTION 113

The command `cat cor.ptia.txt` was issued on a Linux terminal. Which of the following results should be expected?

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

Answer: B

Explanation:

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

NEW QUESTION 117

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

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

Answer: B

Explanation:

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

<https://www.comptia.org/blog/what-is-full-disk-encryption> <https://www.comptia.org/certifications/a>

NEW QUESTION 119

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

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

Answer: C

Explanation:

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

NEW QUESTION 121

A technician is troubleshooting boot times for a user. The technician attempts to use MSConfig to see which programs are starting with the OS but receives a

message that it can no longer be used to view startup items. Which of the following programs can the technician use to view startup items?

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

Answer: D

Explanation:

When troubleshooting boot times for a user, a technician may want to check which programs are starting with the operating system to identify any that may be slowing down the boot process. MSConfig is a tool that can be used to view startup items on a Windows system, but it may not always be available or functional. In this scenario, the technician receives a message that MSConfig cannot be used to view startup items. As an alternative, the technician can use Task Manager (taskmgr), which can

also display the programs that run at startup. To access the list of startup items in Task Manager, the technician can follow these steps:

- ? Open Task Manager by pressing Ctrl+Shift+Esc.
- ? Click the "Startup" tab.
- ? The list of programs that run at startup will be displayed.

NEW QUESTION 126

All the desktop icons on a user's newly issued PC are very large. The user reports that the PC was working fine until a recent software patch was deployed. Which of the following would BEST resolve the issue?

- A. Rolling back video card drivers
- B. Restoring the PC to factory settings
- C. Repairing the Windows profile
- D. Reinstalling the Windows OS

Answer: A

Explanation:

Rolling back video card drivers is the best way to resolve the issue of large desktop icons on a user's newly issued PC. This means restoring the previous version of the drivers that were working fine before the software patch was deployed. The software patch may have caused compatibility issues or corrupted the drivers, resulting in display problems

NEW QUESTION 128

Which of the following is the best reason for sandbox testing in change management?

- A. To evaluate the change before deployment
- B. To obtain end-user acceptance
- C. To determine the affected systems
- D. To select a change owner

Answer: A

Explanation:

Sandbox testing is a method of testing changes in a simulated environment that mimics the real one, without affecting the actual production system. Sandbox testing is useful for change management because it allows the testers to evaluate the change before deployment, and ensure that it works as intended, does not cause any errors or conflicts, and meets the requirements and expectations of the stakeholders. Sandbox testing also helps to protect the investment in the existing system, as it reduces the risk of introducing bugs or breaking functionality that could harm the customer experience or the business operations. Sandbox testing also gives the testers more control over the customer experience, as they can experiment with different scenarios and configurations, and optimize the change for the best possible outcome.

References:

1: Change Management and Sandbox - Quickbase1 2: Embracing change: Build, test, and adapt in a sandbox environment - Zendesk3

NEW QUESTION 129

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 133

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

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

Answer: B

Explanation:

The correct answer is B. Power Options. The Power Options utility in the Control Panel allows you to configure various settings related to how your computer uses and saves power, such as the power plan, the sleep mode, the screen brightness, and the battery status. To access the Power Options utility, you can follow these steps:

? Go to Control Panel > Hardware and Sound > Power Options.

? Click on Change plan settings for the power plan you are using.

? Click on Change advanced power settings.

? Expand the USB settings category and then the USB selective suspend setting subcategory.

? Set the option to Disabled for both On battery and Plugged in.

? Click on OK and then on Save changes.

This will prevent the operating system from suspending the USB devices to save power. System, Devices and Printers, and Ease of Access are not the utilities that should be used to configure the setting. System is a utility that provides information about your computer's hardware and software, such as the processor,

memory, operating system, device manager, and system protection. Devices and Printers is a utility that allows you to view and manage the devices and printers connected to your computer, such as adding or removing devices, changing device settings, or troubleshooting problems. Ease of Access is a utility that allows you to customize your computer's accessibility options, such as the narrator, magnifier, high contrast, keyboard, mouse, and speech recognition. None of these utilities have any option to configure the USB selective suspend setting.

NEW QUESTION 137

A user enabled a mobile device's screen lock function with pattern unlock. The user is concerned someone could access the mobile device by repeatedly attempting random patterns to unlock the device. Which of the following features BEST addresses the user's concern?

- A. Remote wipe
- B. Anti-malware
- C. Device encryption
- D. Failed login restrictions

Answer: A

Explanation:

The feature that BEST addresses the user's concern is remote wipe. This is because remote wipe allows the user to erase all data on the mobile device if it is lost or stolen, which will prevent unauthorized access to the device.

NEW QUESTION 140

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

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

Answer: A

Explanation:

The technician'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 141

A technician is trying to encrypt a single folder on a PC. Which of the following should the technician use to accomplish this task?

- A. FAT32
- B. exFAT
- C. BitLocker
- D. EFS

Answer: D

Explanation:

EFS (Encrypting File System) is a feature that allows a user to encrypt a single folder or file on a Windows PC. It uses a public key encryption system to protect the data from unauthorized access. FAT32 and exFAT are file system formats that do not support encryption. BitLocker is a feature that encrypts the entire drive, not a single folder or file. Verified References: <https://www.comptia.org/blog/what-is-efs> <https://www.comptia.org/certifications/a>

NEW QUESTION 145

Users access files in the department share. When a user creates a new subfolder, only that user can access the folder and its files. Which of the following will MOST likely allow all users to access the new folders?

- A. Assigning share permissions
- B. Enabling inheritance
- C. Requiring multifactor authentication
- D. Removing archive attribute

Answer: B

Explanation:

Enabling inheritance is a method that allows new subfolders to inherit the permissions and settings from their parent folder. If users can access files in the department share, but not in the new subfolders created by other users, it may indicate that inheritance is disabled and that each new subfolder has its own permissions and settings that restrict access to only the creator. Enabling inheritance can help resolve this issue by allowing all users to access the new subfolders with the same permissions and settings as the department share. Assigning share permissions, requiring multifactor authentication, and removing archive attribute are not methods that can most likely allow all users to access the new folders.

NEW QUESTION 149

When a user calls in to report an issue, a technician submits a ticket on the user's behalf. Which of the following practices should the technician use to make sure the ticket is associated with the correct user?

- A. Have the user provide a callback phone number to be added to the ticket
- B. Assign the ticket to the department's power user

- C. Register the ticket with a unique user identifier
- D. Provide the user with a unique ticket number that can be referenced on subsequent calls.

Answer: D

Explanation:

The technician should provide the user with a unique ticket number that can be referenced on subsequent calls to make sure the ticket is associated with the correct user. This is because registering the ticket with a unique user identifier, having the user provide a callback phone number to be added to the ticket, or assigning the ticket to the department's power user will not ensure that the ticket is associated with the correct user2.

NEW QUESTION 154

A technician is installing a program from an ISO file. Which of the following steps should the technician take?

- A. Mount the ISO and run the installation file.
- B. Copy the ISO and execute on the server.
- C. Copy the ISO file to a backup location and run the ISO file.
- D. Unzip the ISO and execute the setup.exe file.

Answer: A

Explanation:

Mounting the ISO and running the installation file is the correct way to install a program from an ISO file. An ISO file is an image of a disc that contains all the files and folders of a program. Mounting the ISO means creating a virtual drive that can access the ISO file as if it were a physical disc. Running the installation file means executing the setup program that will install the program on the computer

NEW QUESTION 156

A user receives an error message from an online banking site that states the following:

Your connection is not private. Authority invalid.

Which of the following actions should the user take NEXT?

- A. Proceed to the site.
- B. Use a different browser.
- C. Report the error to the bank.
- D. Reinstall the browser.

Answer: C

Explanation:

The error message "Your connection is not private. Authority invalid." means that the web browser cannot verify the identity or security of the website's SSL certificate. This could indicate that the website has been compromised, has a configuration error, or has an expired or invalid certificate. The user should not proceed to the site or use a different browser, as this could expose their sensitive information to potential attackers. The user should also not reinstall the browser, as this is unlikely to fix the error and could cause data loss. The best action for the user to take is to report the error to the bank and wait for them to resolve it. References: : How to Fix "Your Connection Is Not Private" Errors (<https://www.howtogeek.com/874436/how-to-fix-your-connection-is-not-private-errors/>) : Fix connection errors (<https://support.google.com/chrome/answer/6098869?hl=en>)

NEW QUESTION 158

A technician is attempting to mitigate micro power outages, which occur frequently within the area of operation. The outages are usually short, with the longest occurrence lasting five minutes. Which of the following should the technician use to mitigate this issue?

- A. Surge suppressor
- B. Battery backup
- C. CMOS battery
- D. Generator backup

Answer: B

Explanation:

A battery backup, also known as an uninterruptible power supply (UPS), is a device that provides backup power during a power outage. When the power goes out, the battery backup provides a short amount of time (usually a few minutes up to an hour, depending on the capacity of the device) to save any work and safely shut down the equipment.

NEW QUESTION 163

A remote user contacts the help desk about an email that appears to be distorted. The technician is unsure what the user means and needs to view the email to assist with troubleshooting. Which of the following should the technician use to assist the user?

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

Answer: D

Explanation:

The best tool to use to assist the user with viewing the email is RMM, which stands for remote monitoring and management. This is a software that allows the technician to remotely access, monitor, and manage the user's computer and applications. The technician can use RMM to view the user's screen, control the mouse and keyboard, and troubleshoot the email issue. The other tools are not suitable for this task. VNC is a software that allows remote desktop sharing, but it

requires the user to install and configure it on their computer, which may not be feasible or convenient. SSH is a protocol that allows secure remote access to a command-line interface, but it is not useful for viewing graphical applications such as email. VPN is a technology that creates a secure and encrypted connection over a public network, but it does not provide remote access or control of the user's computer.

NEW QUESTION 166

During an enterprise rollout of a new application, a technician needs to validate compliance with an application's EULA while also reducing the number of licenses to manage. Which of the following licenses would best accomplish this goal?

- A. Personal use license
- B. Corporate use license
- C. Open-source license
- D. Non-expiring license

Answer: B

Explanation:

A corporate use license, also known as a volume license, is a type of software license that allows an organization to purchase and use multiple copies of a software product with a single license key. A corporate use license can help validate compliance with an application's EULA (end-user license agreement), which is a legal contract that defines the terms and conditions of using the software. A corporate use license can also reduce the number of licenses to manage, as it eliminates the need to activate and track individual licenses for each copy of the software. Personal use license, open-source license, and non-expiring license are not types of licenses that can best accomplish this goal.

NEW QUESTION 171

Which of the following would allow physical access to a restricted area while maintaining a record of events?

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Access control vestibule is the correct answer for this question. An access control vestibule is a physical security device that consists of two doors that form an enclosed space between them. The first door opens only after verifying the identity of the person entering, such as by using a card reader, biometric scanner, or keypad. The second door opens only after the first door closes, creating a buffer zone that prevents unauthorized access or tailgating. An access control vestibule also maintains a record of events, such as who entered or exited, when, and how. Hard token, key fob, and door lock are not sufficient to meet the requirements of this question. A hard token is a device that generates a one-time password or code for authentication purposes. A key fob is a small device that can be attached to a key ring and used to unlock doors or start vehicles remotely. A door lock is a mechanism that secures a door from opening without a key or a code. References: ? Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 25

NEW QUESTION 173

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 177

Which of the following is command options is used to display hidden files and directories?

- A. -a
- B. -s
- C. -lh
- D. -t

Answer: A

Explanation:

The -a option is used to display hidden files and directories in a command-line interface. Hidden files and directories are those that start with a dot (.) and are normally not shown by default. The -a option stands for "all" and shows all files and directories, including the hidden ones. The -a option can be used with commands such as ls, dir, or find to list or search for hidden files and directories. The -s, -lh, and -t options are not used to display hidden files and directories. The -s option stands for "size" and shows the size of files or directories in bytes. The -lh option stands for "long human-readable" and shows the size of files or directories in a more readable format, such as KB, MB, or GB. The -t option stands for "time" and sorts the files or directories by modification time. References: ? Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 17 ? CompTIA A+ Complete Study Guide: Core 1 Exam 220-1101 and Core 2 Exam ..., page 107

NEW QUESTION 179

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

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

Answer: A

Explanation:

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

- ? Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 15
- ? CompTIA A+ Core 1 (220-1101) and Core 2 (220-1102) Cert Guide, page 458

NEW QUESTION 180

A Windows user reported that a pop-up indicated a security issue. During inspection, an antivirus system identified malware from a recent download, but it was unable to remove the malware. Which of the following actions would be BEST to remove the malware while also preserving the user's files?

- A. Run the virus scanner in an administrative mode.
- B. Reinstall the operating system.
- C. Reboot the system in safe mode and rescan.
- D. Manually delete the infected files.

Answer: C

Explanation:

Rebooting the system in safe mode will limit the number of programs and processes running, allowing the antivirus system to more effectively identify and remove the malware. Rescanning the system will allow the antivirus system to identify and remove the malware while preserving the user's files.

NEW QUESTION 185

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

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

Answer: B

Explanation:

Power Options is a Control Panel utility that allows users to configure the power settings of their computer, such as when to turn off the display, when to put the computer to sleep, and how to manage the battery life. Power Options also allows users to configure the USB selective suspend setting, which is a feature that automatically suspends the power supply to USB devices that are not in use, in order to save energy. A user can disable this setting if they want to ensure that USB devices are not suspended by the operating system. System, Devices and Printers, and Ease of Access are not Control Panel utilities that can be used to configure the USB selective suspend setting.

NEW QUESTION 188

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

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

Answer: A

Explanation:

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

- ? Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 18
- ? CompTIA A+ Core 1 (220-1101) and Core 2 (220-1102) Cert Guide, page 459

NEW QUESTION 191

Which of the following would most likely be used in a small office environment?

- A. Print server
- B. Virtualization
- C. Domain access
- D. Workgroup

Answer: D

Explanation:

A workgroup is a network configuration that allows computers to communicate and share resources with each other without requiring a centralized server or domain controller. A workgroup is suitable for small office environments where there are only a few computers and users who need simple file and printer sharing. A workgroup does not have centralized management or security policies, which may be desirable for larger or more complex networks. Print server, virtualization, and domain access are not network configurations that are most likely used in a small office environment.

NEW QUESTION 192

A technician has been tasked with installing a workstation that will be used for point-of-sale transactions. The point-of-sale system will process credit cards and loyalty cards. Which of the following encryption technologies should be used to secure the workstation in case of theft?

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Disk encryption should be used to secure the workstation in case of theft. Disk encryption can help to protect data on the hard drive by encrypting it so that it cannot be accessed without the correct encryption key.

NEW QUESTION 197

While staying at a hotel, a user attempts to connect to the hotel Wi-Fi but notices that multiple SSIDs have very similar names. Which of the following social-engineering attacks is being attempted?

- A. Evil twin
- B. Impersonation
- C. Insider threat
- D. Whaling

Answer: A

Explanation:

An evil twin is a type of social-engineering attack that involves setting up a rogue wireless access point that mimics a legitimate one. The attacker can then intercept or modify the traffic of the users who connect to the fake SSID. The attacker may also use phishing or malware to steal credentials or personal information from the users

NEW QUESTION 202

Which of the following combinations meets the requirements for mobile device multifactor authentication?

- A. Password and PIN
- B. Password and swipe
- C. Fingerprint and password
- D. Swipe and PIN

Answer: C

Explanation:

Mobile device multifactor authentication (MFA) is a method of verifying a user's identity by requiring two or more factors, such as something the user knows (e.g., password, PIN, security question), something the user has (e.g., smartphone, OTP app, security key), or something the user is (e.g., fingerprint, face, iris)¹². The combination of fingerprint and password meets the requirements for mobile device MFA because it uses two different factors: something the user is (fingerprint) and something the user knows (password). The other combinations do not meet the requirements because they use only one factor: something the user knows (password or PIN) or something the user does (swipe). References¹: Set up the Microsoft Authenticator app as your verification method²: What is Multi-Factor Authentication (MFA)? | OneLogin

NEW QUESTION 204

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
Turn on fast startup
- D.

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 208

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. Ransormvare
- 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 temperatures¹²

NEW QUESTION 211

A small business owner wants to install newly purchased software on all networked PCs. The network is not configured as a domain, and the owner wants to use the easiest method possible. Which of the following is the MOST deficient way for the owner to install the application?

- A. Use a network share to share the installation files.
- B. Save software to an external hard drive to install.
- C. Create an imaging USB for each PC.
- D. Install the software from the vendor’s website

Answer: B

Explanation:

Saving software to an external hard drive and installing it on each individual PC is the most inefficient method for the small business owner. This method requires manual intervention on each PC, and there is a higher risk of error or inconsistencies between PCs. Additionally, if the software needs to be updated or reinstalled in the future, this process would need to be repeated on each PC.

NEW QUESTION 215

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

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

Answer: B

Explanation:

Recovery mode is a special boot option that allows the user to access advanced tools and features to troubleshoot and remove malware from the device. Recovery mode can also restore the system to a previous state or reset the device to factory settings. Running System Restore, scheduling a scan, or restarting the PC may not be effective in removing the malware, as it may still be active or hidden in the system files.

NEW QUESTION 219

A computer technician is investigating a computer that is not booting. The user reports that the computer was working prior to shutting it down last night. The technician notices a removable USB device is inserted, and the user explains the device is a prize the user received in the mail yesterday. Which of the following types of attacks does this describe?

- A. Phishing
- B. Dumpster diving
- C. Tailgating
- D. Evil twin

Answer: A

Explanation:

Phishing is the correct answer for this question. Phishing is a type of attack that uses fraudulent emails or other messages to trick users into revealing sensitive information or installing malicious software. Phishing emails often impersonate legitimate entities or individuals and offer incentives or threats to lure users into clicking on malicious links or attachments. In this scenario, the user received a removable USB device in the mail as a prize, which could be a phishing attempt to infect the user’s computer with malware or gain access to the user’s data. Dumpster diving, tailgating, and evil twin are not correct answers for this question. Dumpster diving is a type of attack that involves searching through trash bins or recycling containers to find discarded documents or devices that contain valuable information. Tailgating is a type of attack that involves following an authorized person into a restricted area without proper identification or authorization. Evil twin is a type of attack that involves setting up a rogue wireless access point that mimics a legitimate one to intercept or manipulate network traffic. References:

? Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 25
? [CompTIA Security+ SY0-601 Certification Study Guide], page 1004

NEW QUESTION 224

A technician needs to format a USB drive to transfer 20GB of data from a Linux computer to a Windows computer. Which of the following filesystems will the technician MOST likely use?

- A. FAT32
- B. ext4
- C. NTFS
- D. exFAT

Answer: D

Explanation:

exFAT is a file system that is supported by both Linux and Windows and can handle large files1.

NEW QUESTION 228

A user purchased a netbook that has a web-based, proprietary operating system. Which of the following operating systems is MOST likely installed on the netbook?

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

Answer: C

Explanation:

4. Chrome OS. Retrieved from https://en.wikipedia.org/wiki/Chrome_OS 5. What is Chrome OS? Retrieved from <https://www.google.com/chromebook/chrome-os/>
A netbook with a web-based, proprietary operating system is most likely running Chrome OS. Chrome OS is a web-based operating system developed by Google that is designed to work with web applications and cloud storage. It is optimized for netbooks and other low- power devices and is designed to be fast, secure, and easy to use.

NEW QUESTION 229

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 234

A technician has an external SSD. The technician needs to read and write to an external SSD on both Macs and Windows PCs. Which of the following filesystems is supported by both OS types?

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

Answer: D

Explanation:

The filesystem that is supported by both Macs and Windows PCs is D. exFAT. exFAT is a file system that is designed to be used on flash drives like USB sticks and SD cards. It is supported by both Macs and Windows PCs, and it can handle large files and volumes
<https://www.diskpart.com/articles/file-system-for-mac-and-windows-0310.html>

NEW QUESTION 235

A company discovered that numerous computers from multiple geographic locations are sending a very high number of connection requests which is causing the company's web server to become unavailable to the general public. Which of the following attacks is occurring?

- A. Zero day
- B. SQL injection
- C. Cross-site scripting
- D. Distributed denial of service

Answer: D

Explanation:

The company is experiencing a distributed denial of service (DDoS) attack. A DDoS attack is a type of cyber attack in which multiple compromised systems are used to target a single system, causing a denial of service for users of the targeted system.

NEW QUESTION 239

A company wants to remove information from past users' hard drives in order to reuse the hard drives. Which of the following is the MOST secure method?

- A. Reinstalling Windows
- B. Performing a quick format
- C. Using disk-wiping software
- D. Deleting all files from command-line interface

Answer: C

Explanation:

Using disk-wiping software is the most secure method for removing information from past users' hard drives in order to reuse the hard drives. Disk-wiping software can help to ensure that all data on the hard drive is completely erased and cannot be recovered.

NEW QUESTION 242

A technician needs to reimage a desktop in an area without network access. Which of the following should the technician use? (Select two).

- A. PXE
- B. USB
- C. Optical media
- D. Partition
- E. Boot record
- F. SMB

Answer: AC

Explanation:

A technician needs to reimage a desktop in an area without network access, which means that the technician cannot use network-based methods such as PXE or SMB to deploy the image. Therefore, the technician should use offline methods that involve removable media such as USB or optical media. USB and optical media are common ways to store and transfer system images, and they can be used to boot the desktop and initiate the reimaging process. The technician will need to create a bootable USB or optical media that contains the system image and the imaging software, and then insert it into the desktop and change the boot order in the BIOS or UEFI settings. The technician can then follow the instructions on the screen to reimage the desktop.

NEW QUESTION 246

A technician needs to document who had possession of evidence at every step of the process. Which of the following does this process describe?

- A. Rights management
- B. Audit trail
- C. Chain of custody
- D. Data integrity

Answer: C

Explanation:

The process of documenting who had possession of evidence at every step of the process is called chain of custody.

NEW QUESTION 247

A technician removed a virus from a user's device. The user returned the device a week later with the same virus on it. Which of the following should the technician do to prevent future infections?

- A. Disable System Restore.
- B. Educate the end user.
- C. Install the latest OS patches.
- D. Clean the environment reinstallation.

Answer: B

Explanation:

Educating the end user is the best way to prevent future infections by viruses or other malware. The technician should teach the user how to avoid risky behaviors, such as opening suspicious attachments, clicking on unknown links, downloading untrusted software, etc. Disabling System Restore, installing the latest OS patches and performing a clean installation are possible ways to remove existing infections, but they do not prevent future ones.

Verified References: <https://www.comptia.org/blog/how-to-prevent-malware> <https://www.comptia.org/certifications/a>

NEW QUESTION 250

During a network outage, a technician discovers a new network switch that was not listed in the support documentation. The switch was installed during a recent change window when a new office was added to the environment. Which of the following would most likely prevent this type of mismatch after next month's change window?

- A. Performing annual network topology reviews
- B. Requiring all network changes include updating the network diagrams
- C. Allowing network changes once per year
- D. Routinely backing up switch configuration files

Answer: B

Explanation:

This would ensure that the support documentation reflects the current state of the network and prevents any confusion or mismatch during a network outage. Updating the network diagrams is also one of the best practices for network documentation, as stated in the Official CompTIA A+ Core 2 Study Guide¹. The other options are not as effective or feasible as option B. Performing annual network topology reviews is too infrequent and may not capture recent changes. Allowing network changes once per year is too restrictive and may not meet the business needs. Routinely backing up switch configuration files is important, but it does not help with identifying new switches or devices on the network.

NEW QUESTION 254

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 256

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

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

Answer: B

Explanation:

The correct answer is B. Submit a change request form. A change request form is a document that describes the proposed change, the reason for the change, the expected benefits and impacts, the risks and mitigation strategies, the implementation plan, and the approval process. A change request form is an essential part of change management best practices, as it helps to ensure that the change is well-planned, communicated, and authorized before it is implemented¹². A change request form should be submitted immediately before network use is authorized, because it provides the necessary information and justification for the change to the relevant stakeholders, such as the network administrator, the IT manager, and the department manager. The change request form also allows the stakeholders to review and approve or reject the change, or request more information or modifications. The change request form also serves as a record of the change history and status¹².

NEW QUESTION 258

A customer is accessing a public kiosk in a company's lobby. Which of the following should be enforced to mitigate the risk of customer data being accidentally saved to the kiosk?

- A. Manually clearing browsing data
- B. Private-browsing mode
- C. Browser data synchronization
- D. Password manager

Answer: B

Explanation:

Private-browsing mode is the best option to mitigate the risk of customer data being accidentally saved to the kiosk. Private-browsing mode prevents the browser from storing cookies, history, passwords, and other data that could reveal the customer's identity or preferences. Manually clearing browsing data is not a reliable option, as it depends on the customer's awareness and willingness to do so. Browser data synchronization and password manager are features that could actually increase the risk of customer data being exposed, as they could sync or autofill sensitive information across devices or accounts. References:

? Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 12

? Certification Study Guides and Books | CompTIA IT Certifications, CompTIA A+ Core 1 220-1101 Certification Study Guide, page 234

NEW QUESTION 259

A technician is upgrading the backup system for documents at a high-volume law firm. The current backup system can retain no more than three versions of full backups before failing. The law firm is not concerned about restore times but asks the technician to retain more versions when possible. Which of the following backup methods should the technician MOST likely implement?

- A. Full
- B. Mirror
- C. Incremental
- D. Differential

Answer: C

Explanation:

The law firm wants to retain more versions of the backups when possible, so the best backup method for the technician to implement in this scenario would be incremental backup. Incremental backups only save the changes made since the last backup, which allows for more frequent backups and minimizes the amount of storage required. This would allow the law firm to retain more than three versions of backups without risking backup failure.

To retain more versions of backups, the technician should implement an incremental backup method.

An incremental backup method only backs up the data that has changed since the last backup, so it requires less storage space than a full backup.

NEW QUESTION 263

A workstation is displaying a message indicating that a user must exchange cryptocurrency for a decryption key. Which of the following is the best way for a technician to return the device to service safely?

- A. Run an AV scan.
- B. Reinstall the operating system.
- C. Install a software firewall.
- D. Perform a system restore.
- E. Comply with the on-screen instructions.

Answer: B

Explanation:

The best way for a technician to return the device to service safely is to reinstall the operating system. This is because the device is infected by ransomware, which is a form of malware that encrypts files and demands payment for decryption. Reinstalling the operating system will erase the ransomware and restore the device to its original state. However, this will also delete any data that was not backed up before the infection. Therefore, it is important to have regular backups of critical data and protect them from ransomware attacks.

The other options are not effective or safe for ransomware recovery. Running an AV scan may not detect or remove the ransomware, especially if it is a new or unknown variant. Installing a software firewall may prevent future attacks, but it will not help with the current infection. Performing a system restore may not work if the ransomware has corrupted or deleted the restore points. Complying with the on-screen instructions is not advisable, as it will encourage the attackers and there is no guarantee that they will provide the decryption key after receiving the payment.

To prevent and recover from ransomware attacks, it is recommended to follow some best practices, such as:

- ? Use strong passwords and multifactor authentication for all accounts and devices.
- ? Keep all software and firmware updated with the latest security patches.
- ? Avoid opening suspicious or unsolicited emails and attachments.
- ? Educate users and staff on how to recognize and report phishing and social engineering attempts.
- ? Use antivirus software and enable real-time protection.
- ? Enable network segmentation and firewall rules to limit the spread of ransomware.
- ? Implement a Zero Trust security model to verify all requests and devices before granting access.
- ? Create and test backups of critical data and store them offline or in a separate network.
- ? Recover safely by isolating the infected devices, identifying the ransomware variant, and restoring data from backups.
- ? Report any ransomware incidents to law enforcement agencies and seek help from experts.

NEW QUESTION 266

A user is unable to access a website, which is widely used across the organization, and receives the following error message:

The security certificate presented by this website has expired or is not yet valid.

The technician confirms the website works when accessing it from another computer but not from the user's computer. Which of the following should the technician perform NEXT to troubleshoot the issue?

- A. Reboot the computer.
- B. Reinstall the OS.
- C. Configure a static IP.
- D. Check the computer's date and time.

Answer: D

Explanation:

The error message indicates that the security certificate presented by the website has either expired or is not yet valid. This can happen if the computer's clock has the wrong date or time, as SSL/TLS certificates have a specific validity period. If the clock is off by too much, it may cause the certificate to fail to validate. Therefore, the technician should check the computer's date and time and ensure that they are correct.

NEW QUESTION 271

A Chief Executive Officer has learned that an exploit has been identified on the web server software, and a patch is not available yet. Which of the following attacks MOST likely occurred?

- A. Brute force
- B. Zero day
- C. Denial of service
- D. On-path

Answer: B

Explanation:

A zero-day attack is an attack that exploits a previously unknown vulnerability in a computer application, meaning that the attack occurs on "day zero" of awareness of the vulnerability.

? Configuring AAA Services. Retrieved from

https://www.cisco.com/c/en/us/td/docs/routers/crs/software/crs_r4-0/security/configuration/guide/sc40crsbook_chapter1.html

NEW QUESTION 273

A technician needs to interconnect two offices to the main branch while complying with good practices and security standards. Which of the following should the technician implement?

- A. MSRA

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

Answer: C

Explanation:

A technician needs to interconnect two offices to the main branch while complying with good practices and security standards. The technician should implement VPN

NEW QUESTION 276

Which of the following only has a web browser interface?

- A. Linux
- B. Microsoft Windows
- C. iOS
- D. Chromium

Answer: D

Explanation:

Chromium is an operating system that only has a web browser interface. Chromium is an open-source project that provides the source code and framework for Chrome OS, which is a Linux-based operating system developed by Google. Chromium and Chrome OS are designed to run web applications and cloud services through the Chrome web browser, which is the only user interface available on the system. Chromium and Chrome OS are mainly used on devices such as Chromebooks, Chromeboxes and Chromebits. Linux is an operating system that does not only have a web browser interface but also a graphical user interface and a command-line interface. Linux is an open-source and customizable operating system that can run various applications and services on different devices and platforms. Linux can also support different web browsers, such as Firefox, Opera and Chromium. Microsoft Windows is an operating system that does not only have a web browser interface but also a graphical user interface and a command-line interface. Microsoft Windows is a proprietary and popular operating system that can run various applications and services on different devices and platforms. Microsoft Windows can also support different web browsers, such as Edge, Internet Explorer and Chrome. iOS is an operating system that does not only have a web browser interface but also a graphical user interface and a voice-based interface. iOS is a proprietary and mobile operating system developed by Apple that can run various applications and services on devices such as iPhone, iPad and iPod Touch. iOS can also support different web browsers, such as Safari, Firefox and Chrome. References: CompTIA A+ Core 2 (220- 1002) Certification Exam Objectives Version 4.0, Domain 1.1

NEW QUESTION 280

A technician is familiar with most personnel at a customer's location and has clearance to work unsupervised. Which of the following describes how the technician should handle personal communication while on site?

- A. Respond to calls and text messages while on site but not when working directly with personnel.
- B. Respond to calls and text messages only from family.
- C. Respond to calls and text messages only when an emergency situation requires a response.
- D. Respond to calls and text messages discreetly while on site.

Answer: C

Explanation:

A technician should handle personal communication while on site in a professional and respectful manner. According to the CompTIA A+ Core 2 (220-1102) exam objectives, one of the best practices for communication skills is to “avoid distractions and interruptions” when working with customers¹. This means that the technician should not respond to calls and text messages that are not related to the work or the customer, unless there is an emergency situation that requires a response. Responding to personal communication while on site can be seen as rude, unprofessional, and disrespectful to the customer and their time. It can also affect the quality and efficiency of the technician’s work and cause errors or delays. Therefore, the technician should only respond to calls and text messages when an emergency situation requires a response, and inform the customer about the situation and apologize for the interruption. The other options are not appropriate for handling personal communication while on site.

Responding to calls and text messages while on site but not when working directly with personnel (A) is still distracting and unprofessional, as it can interfere with the technician’s focus and productivity. Responding to calls and text messages only from family (B) is not a valid criterion, as the technician may receive calls and text messages from other sources that are not related to the work or the customer. Responding to calls and text messages discreetly while on site (D) is not a good practice, as it can still be noticed by the customer or other personnel and create a negative impression.

References:

1: CompTIA A+ Certification Exam Core 2 Objectives - CompTIA

NEW QUESTION 282

A user requested that the file permissions on a Linux device be changed to only allow access to a certain group of users. Which of the following commands should be used to complete the user's request?

- A. cat
- B. chmod
- C. pwd
- D. cacls

Answer: B

Explanation:

The chmod command is used to change the permissions of files and directories in Linux. It can grant or revoke read, write, and execute permissions for the owner, the group, and others. To change the file permissions to only allow access to a certain group of users, the chmod command can use either the symbolic or the numeric mode. For example, to give read and write permissions to the group and no permissions to others, the command can be:

chmod g+rw,o-rwx filename or

chmod 660 filename

References: 1 Chmod Command in Linux (File Permissions) | Linuxize(<https://linuxize.com/post/chmod-command-in-linux/>)2 How To Change File or Directory Permissions in Linux | Tom’s Hardware(<https://www.tomshardware.com/how- to/change-file-directory-permissions-linux>).

NEW QUESTION 283

Which of the following is the MOST cost-effective version of Windows 10 that allows remote access through Remote Desktop?

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

Answer: D

Explanation:

The most cost-effective version of Windows 10 that allows remote access through Remote Desktop is Windows 10 Pro. Windows 10 Pro includes Remote Desktop, which allows users to connect to a remote computer and access its desktop, files, and applications. Windows 10 Home does not include Remote Desktop, while Windows 10 Pro for Workstations and Windows 10 Enterprise are more expensive versions of Windows 10 that include additional features for businesses

NEW QUESTION 285

A kiosk, which is running Microsoft Windows 10, relies exclusively on a numeric keypad to allow customers to enter their ticket numbers but no other information. If the kiosk is idle for four hours, the login screen locks. Which of the following sign-on options would allow any employee the ability to unlock the kiosk?

- A. Requiring employees to enter their usernames and passwords
- B. Setting up facial recognition for each employee
- C. Using a PIN and providing it to employees
- D. Requiring employees to use their fingerprints

Answer: C

Explanation:

The best sign-on option that would allow any employee the ability to unlock the kiosk that relies exclusively on a numeric keypad is to use a PIN and provide it to employees. A PIN is a Personal Identification Number that is a numeric code that can be used as part of authentication or access control. A PIN can be entered using only a numeric keypad and can be easily shared with employees who need to unlock the kiosk. Requiring employees to enter their usernames and passwords may not be feasible or convenient if the kiosk only has a numeric keypad and no other input devices. Setting up facial recognition for each employee may not be possible or secure if the kiosk does not have a camera or biometric sensor. Requiring employees to use their fingerprints may not be possible or secure if the kiosk does not have a fingerprint scanner or biometric sensor.

References: CompTIA A+ Core 2 (220-1102) Certification Exam Objectives Version 4.0, Domain 3.3

NEW QUESTION 286

A company needs to securely dispose of data stored on optical discs. Which of the following is the MOST effective method to accomplish this task?

- A. Degaussing
- B. Low-level formatting
- C. Recycling
- D. Shredding

Answer: D

Explanation:

Shredding is the most effective method to securely dispose of data stored on optical discs¹²

References: 4. How Can I Safely Destroy Sensitive Data CDs/DVDs? - How-To Geek. Retrieved from <https://www.howtogeek.com/174307/how-can-i-safely-destroy-sensitive-data-cdsdvs/> 5. Disposal — UK Data Service. Retrieved from <https://ukdataservice.ac.uk/learning-hub/research-data-management/store-your-data/disposal/>

NEW QUESTION 290

While browsing a website, a staff member received a message that the website could not be trusted. Shortly afterward, several other colleagues reported the same issue across numerous other websites. Remote users who were not connected to corporate resources did not have any issues. Which of the following is MOST likely the cause of this issue?

- A. A bad antivirus signature update was installed.
- B. A router was misconfigured and was blocking traffic.
- C. An upstream internet service provider was flapping.
- D. The time or date was not in sync with the website.

Answer: B

Explanation:

The most likely cause of this issue is that a router was misconfigured and was blocking traffic. This would explain why remote users who were not connected to corporate resources did not have any issues.

NEW QUESTION 291

A technician needs to transfer a large number of files over an unreliable connection. The technician should be able to resume the process if the connection is interrupted. Which of the following tools can be used?

- A. afc
- B. ehkdsk
- C. git clone
- D. zobocopy

Answer: A

Explanation:

The technician should use `afc` to transfer a large number of files over an unreliable connection and be able to resume the process if the connection is interrupted.

NEW QUESTION 293

Which of the following security methods supports the majority of current Wi-Fi-capable devices without sacrificing security?

- A. WPA3
- B. MAC filtering
- C. RADIUS
- D. TACACS+

Answer: A

Explanation:

WPA3 (Wi-Fi Protected Access 3) is a wireless security method that supports the majority of current Wi-Fi-capable devices without sacrificing security. It is backward compatible with WPA2 devices and offers enhanced encryption and authentication features. MAC filtering is another wireless security method, but it can be easily bypassed by spoofing MAC addresses. RADIUS (Remote Authentication Dial-In User Service) and TACACS+ (Terminal Access Controller Access-Control System Plus) are network authentication protocols, but they are not wireless security methods by themselves. Verified References: <https://www.comptia.org/blog/wireless-security-standards> <https://www.comptia.org/certifications/a>

NEW QUESTION 294

A customer calls the help desk asking for instructions on how to modify desktop wallpaper. Which of the following Windows 10 settings should the technician recommend?

- A. Personalization
- B. Apps
- C. Updates
- D. Display

Answer: A

Explanation:

Personalization is a Windows 10 setting that allows a user to modify the desktop wallpaper, as well as other aspects of the appearance and behavior of the desktop, such as colors, themes, sounds, etc. Apps is a Windows 10 setting that allows a user to manage the installed applications and their features. Updates is a Windows 10 setting that allows a user to check for and install the latest updates for the OS and other components. Display is a Windows 10 setting that allows a user to adjust the screen resolution, brightness, orientation, etc. Verified References: <https://www.comptia.org/blog/windows-10-settings> <https://www.comptia.org/certifications/a>

NEW QUESTION 298

A technician is reimaging a desktop PC. The technician connects the PC to the network and powers it on. The technician attempts to boot the computer via the NIC to image the computer, but this method does not work. Which of the following is the MOST likely reason the computer is unable to boot into the imaging system via the network?

- A. The computer's CMOS battery failed.
- B. The computer's NIC is faulty.
- C. The PXE boot option has not been enabled.
- D. The Ethernet cable the technician is using to connect the desktop to the network is faulty.

Answer: C

Explanation:

The most likely reason the computer is unable to boot into the imaging system via the network is that the PXE boot option has not been enabled. PXE (Preboot Execution Environment) is an environment that allows computers to boot up over the network, instead of from a local disk. In order for this to work, the PXE boot option must be enabled in the computer's BIOS settings. As stated in the CompTIA A+ Core 2 exam objectives, technicians should know how to enable PXE in BIOS to enable network booting on a computer.

NEW QUESTION 301

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

220-1102 Practice Exam Features:

- * 220-1102 Questions and Answers Updated Frequently
- * 220-1102 Practice Questions Verified by Expert Senior Certified Staff
- * 220-1102 Most Realistic Questions that Guarantee you a Pass on Your First Try
- * 220-1102 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The 220-1102 Practice Test Here](#)