CompTIA

Exam Questions 220-1102

CompTIA A+ Certification Exam: Core 2

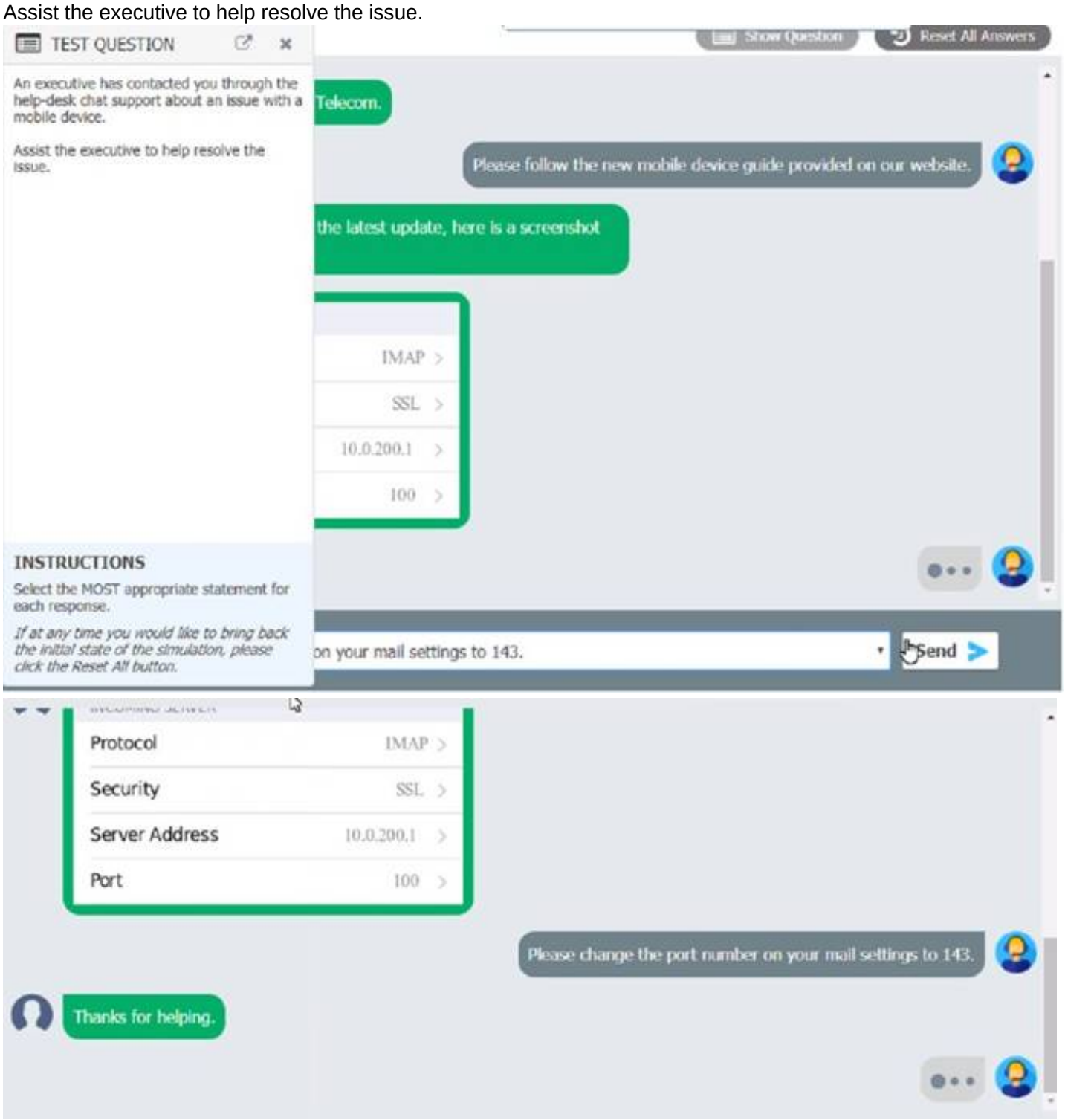
NEW QUESTION 1
A user is no longer able to start the OS on a computer and receives an error message indicating there is no OS found. A technician reviews the audit logs and notes that the user's system posted a S.M.A.R.T. error just days before this issue. Which of the following is the MOST likely cause of this issue?

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

Answer: C

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

NEW QUESTION 2
An executive has contacted you through the help-desk chat support about an issue with a mobile device.
Assist the executive to help resolve the issue.



Which of the following should be done NEXT?

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

Answer: A

NEW QUESTION 3
A company recently experienced a security incident in which a USB drive containing malicious software was able to covertly install malware on a workstation.
Which of the following actions should be taken to prevent this incident from happening again? (Select two).

A. Install a host-based IDS.
B. Restrict log-in times.
C. Enable a BIOS password.
D. Update the password complexity.
E. Disable AutoRun.

F. Update the antivirus definitions.
G. Restrict user permissions.

Answer: EG

Explanation:
AutoRun is a feature of Windows that automatically executes a program or file when a removable media such as a USB drive is inserted into the computer. Disabling AutoRun can prevent a USB drive containing malicious software from covertly installing malware on a workstation, as it would require the user to manually open the drive and run the file. Restricting user permissions can also prevent a USB drive containing malicious software from covertly installing malware on a workstation, as it would limit the user's ability to execute or install unauthorized programs or files. Installing a host-based IDS, restricting log-in times, enabling a BIOS password, updating the password complexity, and updating the antivirus definitions are not actions that can directly prevent this incident from happening again.

NEW QUESTION 4
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 5
A Windows user recently replaced a computer The user can access the public internet on the computer; however, an internal site at https7/companyintranet.com:8888 is no longer loading. Which of the following should a technician adjust to resolve the issue?

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

Answer: D

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

NEW QUESTION 6
A user calls the help desk to report that Windows installed updates on a laptop and rebooted overnight. When the laptop started up again, the touchpad was no longer working. The technician thinks the software that controls the touchpad might be the issue. Which of the following tools should the technician use to make adjustments?

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

Answer: D

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

NEW QUESTION 7
A remote user is experiencing issues connecting to a corporate email account on a laptop. The user clicks the internet connection icon and does not recognize the connected Wi-Fi. The help desk technician, who is troubleshooting the issue, assumes this is a rogue access point. Which of the following is the first action the technician should take?

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

Answer: C

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

NEW QUESTION 8
A user is having phone issues after installing a new application that claims to optimize performance. The user downloaded the application directly from the vendor's website and is now experiencing high network utilization and is receiving repeated security warnings. Which of the following should the technician perform FIRST to mitigate the issue?

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

Answer: B

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

NEW QUESTION 9
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 10
A technician is securing a new Windows 10 workstation and wants to enable a Screensaver lock. Which of the following options in the Windows settings should the technician use?

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

Answer: C

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

NEW QUESTION 10
A system drive is nearly full, and a technician needs lo tree up some space. Which of the following tools should the technician use?

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

Answer: A

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

NEW QUESTION 14
A user requires a drive to be mapped through a Windows command line. Which of the following command-line tools can be utilized to map the drive?

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

Answer: B

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

NEW QUESTION 17
A user attempts to open some files, but a message appears stating that the files are encrypted. The user was able to access these files before without receiving this message and no changes have been made within the company. Which of the following has infected the computer?

A. Cryptominer
B. Phishing
C. Ransomware
D. Keylogger

Answer: C

Explanation:
Ransomware is malicious software that encrypts files on a computer, making them inaccessible until a ransom is paid. In this case, the user was able to access the files before without issue, and no changes have been made within the company, so it is likely that the computer was infected with ransomware.

NEW QUESTION 22
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 26
Which of the following features allows a technician to configure policies in a Windows 10 Professional desktop?

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

Answer: A

Explanation:
The feature that allows a technician to configure policies in a Windows 10 Professional desktop is gpedit. Gpedit is a command that opens the Local Group Policy Editor, which is a utility that allows users to view and modify local group policies on their Windows PC. Local group policies are a set of rules and settings that control the behavior and configuration of the system and its users. Local group policies can be used to configure policies such as security, network, software installation and user rights. Gpmc is a command that opens the Group Policy Management Console, which is a utility that allows users to view and modify domain-based group policies on a Windows Server. Domain- based group policies are a set of rules and settings that control the behavior and configuration of the computers and users in a domain. Domain-based group policies are not available on a Windows 10 Professional desktop. Gpresult is a command that displays the

result of applying group policies on a Windows PC. Gpresult can be used to troubleshoot or verify group policy settings but not to configure them. Gpupdate is a command that updates or refreshes the group policy settings on a Windows PC. Gpupdate can be used to apply new or changed group policy settings but not to configure them.

References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.6

NEW QUESTION 29
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 30
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 34
A technician has verified a computer is infected with malware. The technician isolates the system and updates the anti-malware software. Which of the following should the technician do next?

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 38
A company is looking lot a solution that provides a backup for all data on the system while providing the lowest impact to the network. Which of the following backup types will the company MOST likely select?

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

Answer: B

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

NEW QUESTION 43
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 47
A technician is troubleshooting application crashes on a Windows workstation. Each time the workstation user tries to open a website in a browser, the following message is displayed:
crypt32.d11 is missing not found
Which of the following should the technician attempt FIRST?

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

Answer: D

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

NEW QUESTION 52
Which of the following is also known as something you know, something you have, and something you are?

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

Answer: B

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

NEW QUESTION 55
A technician downloads a validated security tool and notes the vendor hash of a58e87a2. When the download is complete, the technician again validates the hash, but the value returns as 2a876a7d3. Which of the following is the MOST likely cause of the issue?

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

Answer: C

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

valid or trusted digital certificate that proves its identity and secures its communication. Invalid certificate does not affect the hash value of a downloaded file but only how the browser verifies the website or server's credibility. Browser cache is a temporary storage that stores copies of web pages, images and other content that users have visited on their browser.

NEW QUESTION 58
A hard drive that previously contained PI I needs to be repurposed for a public access workstation. Which of the following data destruction methods should a technician use to ensure data is completely removed from the hard drive?

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

Answer: A

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

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

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

Answer: C

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

NEW QUESTION 61
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 62
A company is experiencing a ODDS attack. Several internal workstations are the source of the traffic Which of the following types of infections are the workstations most likely experiencing? (Select two)

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

Answer: AD

Explanation:
The correct answers are A and D. Zombies and botnets are types of infections that allow malicious actors to remotely control infected computers and use them to launch distributed denial-of-service (DDoS) attacks against a target. A DDoS attack is a type of cyberattack that aims to overwhelm a server or a network with a large volume of traffic from multiple sources, causing it to slow down or crash.
A keylogger is a type of malware that records the keystrokes of a user and sends them to a remote server, often for the purpose of stealing passwords, credit card numbers, or other sensitive information.
Adware is a type of software that displays unwanted advertisements on a user's computer, often in the form of pop-ups, banners, or redirects. Adware can also collect user data and compromise the security and performance of the system.
Ransomware is a type of malware that encrypts the files or locks the screen of a user's computer and demands a ransom for their restoration. Ransomware can also threaten to delete or expose the user's data if the ransom is not paid.
Spyware is a type of software that covertly monitors and collects information about a user's online activities, such as browsing history, search queries, or personal data. Spyware can also alter the settings or functionality of the user's system without their consent.

NEW QUESTION 67
A user in a corporate office reports the inability to connect to any network drives. No other users have reported this issue. Which of the following is the MOST likely reason the user is having this issue?

A. Mastered
B. Not Mastered

Answer: A

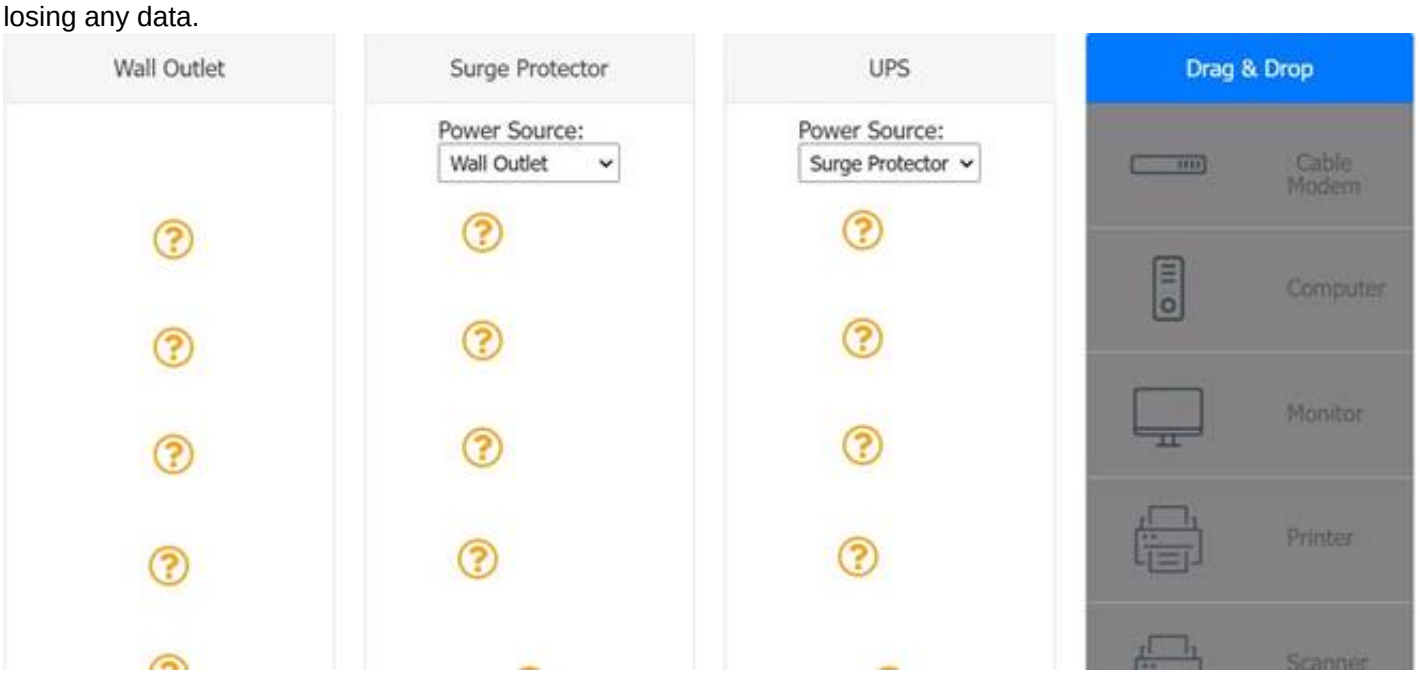
NEW QUESTION 68
A technician, who is working at a local office, has found multiple copies of home edition software installed on computers. Which of the following does this MOST likely violate?

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

Answer: A

Explanation:
The installation of home edition software on computers at a local office most likely violates the EULA. EULA stands for End User License Agreement and is a legal contract that specifies the terms and conditions for using a software product or service. EULA typically covers topics such as license scope, duration and limitations, rights and obligations of the parties, warranties and disclaimers, liability and indemnity clauses, and termination procedures. EULA may also restrict the use of home edition software to personal or non- commercial purposes only, and prohibit the use of home edition software in business or professional settings. Violating EULA may result in legal actions or penalties from the software vendor or developer. PII stands for Personally Identifiable Information and is any information that can be used to identify or locate an individual, such as name, address, phone number, email address, social security number or credit card number. PII is not related to software installation or licensing but to data protection and privacy. DRM stands for Digital Rights Management and is a technology that controls or restricts the access and
use of digital content, such as music, movies, books or games. DRM is not related to software installation or licensing but to content distribution and piracy prevention. Open- source agreement is a type of license that allows users to access, modify and distribute the source code of a software product or service freely and openly. Open-source agreement does not restrict the use of software to home edition only but encourages collaboration and innovation among developers and users. References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 5.1

NEW QUESTION 69
DRAG DROP
A customer recently experienced a power outage at a SOHO. The customer does not think the components are connected properly. A print job continued running for several minutes after the power failed, but the customer was not able to interact with the computer. Once the UPS stopped beeping, all functioning devices also turned off. In case of a future power failure, the customer wants to have the most time available to save cloud documents and shut down the computer without losing any data.



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 70
A Windows workstation that was recently updated with approved system patches shut down instead of restarting. Upon reboot, the technician notices an alert stating the workstation has malware in the root OS folder. The technician promptly performs a System Restore and reboots the workstation, but the malware is still detected. Which of the following BEST describes why the system still has malware?

A. A system patch disabled the antivirus protection and host firewall.
B. The system updates did not include the latest anti-malware definitions.
C. The system restore process was compromised by the malware.
D. The malware was installed before the system restore point was created.

Answer: D

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

NEW QUESTION 74
A technician is creating a location on a Windows workstation for a customer to store meeting minutes. Which of the following commands should the technician use?

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

Answer: D

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

NEW QUESTION 76
Which of the following wireless security features can be enabled lo allow a user to use login credentials to attach lo available corporate SSIDs?

A. TACACS+
B. Kerberos
C. Preshared key
D. WPA2/AES

Answer: D

Explanation:
WPA2/AES (Wi-Fi Protected Access 2/Advanced Encryption Standard) is a wireless security standard that supports enterprise mode, which allows a user to use login credentials (username and password) to authenticate to available corporate SSIDs (service set identifiers). TACACS+ (Terminal Access Controller Access-Control System Plus) and Kerberos are network authentication protocols, but they are not wireless security features. Preshared key is another wireless security feature, but it does not use login credentials. Verified References: https://www.comptia.org/blog/wireless-security-standards https://www.comptia.org/certifications/a

NEW QUESTION 81
A user's smartphone data usage is well above average. The user suspects an installed application is transmitting data in the background. The user would like to be alerted when an application attempts to communicate with the internet. Which of the following BEST addresses the user's concern?

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

Answer: D

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

NEW QUESTION 83
A technician is installing RAM in a new workstation and needs to protect against electrostatic discharge. Which of the following will best resolve this concern?

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

Answer: C

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

NEW QUESTION 84
A user rotates a cell phone horizontally to read emails, but the display remains vertical, even though the settings indicate autorotate is on. VT1ich of the following will MOST likely resolve the issue?

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

Answer: D

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

NEW QUESTION 88
An Android user reports that when attempting to open the company's proprietary mobile application it immediately doses. The user states that the issue persists, even after rebooting the phone. The application contains critical information that cannot be lost. Which of the following steps should a systems administrator attempt FIRST?

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 90
Which of the following protects a mobile device against unwanted access when it is left unattended?

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

Answer: A

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

NEW QUESTION 91
A user's antivirus software reports an infection that it is unable to remove. Which of the following is the most appropriate way to remediate the issue?

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

Answer: C

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

? Uninstalling Antivirus Software, the Clean Way: 40 Removal Tools & Instructions, section 22
? How to manually remove an infected file from a Windows computer3
? The Official CompTIA A+ Core 2 Study Guide (220-1102), page 2194

NEW QUESTION 92
A technician is editing the hosts file on a few PCs in order to block certain domains. Which of the following would the technician need to execute after editing the hosts file?

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

Answer: D

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

NEW QUESTION 93
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 94
A technician is installing new software on a macOS computer. Which of the following file types will the technician MOST likely use?

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

Answer: D

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

NEW QUESTION 99
Which of the following macOS utilities uses AES-128 to encrypt the startup disk?

A. fdisk
B. Diskpart
C. Disk Utility
D. FileVault

Answer: D

Explanation:
FileVault is a macOS utility that uses AES-128 (Advanced Encryption Standard) to encrypt the startup disk of a Mac computer. It protects the data from unauthorized access if the computer is lost or stolen. fdisk and Diskpart are disk partitioning utilities for Linux and Windows, respectively. Disk Utility is another macOS utility that can perform disk management tasks, such as formatting, resizing, repairing, etc. Verified References: https://www.comptia.org/blog/what-is-filevault https://www.comptia.org/certifications/a

NEW QUESTION 100
A technician needs administrator access on a Windows workstation to facilitate system changes without elevating permissions. Which of the following would best accomplish this task?

A. Group Policy Editor
B. Local Users and Groups
C. Device Manager
D. System Configuration

Answer: B

Explanation:

Local Users and Groups is the best option to accomplish this task. Local Users and Groups is a tool that allows managing the local user accounts and groups on a Windows workstation. The technician can use this tool to create a new user account with administrator privileges or add an existing user account to the Administrators group. This way, the technician can log in with the administrator account and make system changes without elevating permissions. Group Policy Editor, Device Manager, and System Configuration are not correct answers for this question. Group Policy Editor is a tool that allows configuring policies and settings for users and computers in a domain environment. Device Manager is a tool that allows managing the hardware devices and drivers on a Windows workstation. System Configuration is a tool that allows modifying the startup options and services on a Windows workstation. None of these tools can directly grant administrator access to a user account. References:
? Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 13
? CompTIA A+ Complete Study Guide: Core 1 Exam 220-1101 and Core 2 Exam …, page 103

NEW QUESTION 103
Which of the following best describes when to use the YUM command in Linux?

A. To add functionality
B. To change folder permissions
C. To show documentation
D. To list file contents

Answer: A

Explanation:
YUM stands for Yellowdog Updater Modified and it is a command-line tool that allows users to install, update, remove, and manage software packages in Linux. YUM can be used to add functionality to a Linux system by installing new software packages or updating existing ones. To change folder permissions, show documentation, or list file contents, other commands such as chmod, man, or ls can be used in Linux.

NEW QUESTION 105
A user notices a small USB drive is attached to the user's computer after a new vendor visited the office. The technician notices two files named grabber.exe and output.txt. Which of the following attacks is MOST likely occurring?

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

Answer: D

Explanation:

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

NEW QUESTION 108
A company would like to implement multifactor authentication for all employees at a minimal cost. Which of the following best meets the company's requirements?

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

Answer: B

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

NEW QUESTION 113
A desktop specialist needs to prepare a laptop running Windows 10 for a newly hired employee. Which of the following methods should the technician use to refresh the laptop?

A. Internet-based upgrade
B. Repair installation
C. Clean install
D. USB repair
E.

In place upgrade

Answer: C

Explanation:
The desktop specialist should use a clean install to refresh the laptop. A clean install will remove all data and applications from the laptop and install a fresh copy of Windows 10, ensuring that the laptop is ready for the newly hired employee.

NEW QUESTION 114
A technician is replacing the processor in a desktop computer prior to opening the computer, the technician wants to ensure the internal components are protected. Which of the following safety procedures would BEST protect the components in the PC? (Select TWO).

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

Answer: AC

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

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

NEW QUESTION 119
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 124
A technician wants to enable BitLocker on a Windows 10 laptop and is unable to find the BitLocker Drive Encryption menu item in Control Panel. Which of the following explains why the technician unable to find this menu item?

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

Answer: C

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

NEW QUESTION 127
Which of the following file extensions should a technician use for a PowerShell script?

A.

.ps1
B. .py
C. .sh
D. .bat
E. .cmd

Answer: A

Explanation:
A PowerShell script is a plain text file that contains one or more PowerShell commands. Scripts have a .ps1 file extension and can be run on your computer or in a

remote session. PowerShell scripts can be used to automate tasks and change settings on Windows devices. To create and run a PowerShell script, you need a text editor (such as Visual Studio Code or Notepad) and the PowerShell Integrated Scripting Environment (ISE) console. You also need to enable the correct execution policy to allow scripts to run on your system

NEW QUESTION 132
A user is setting up a computer for the first time and would like to create a secondary login with permissions that are different than the primary login. The secondary login will need to be protected from certain content such as games and websites. Which of the following Windows settings should the user utilize to create the secondary login?

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

Answer: B

Explanation:
To create a secondary login with different permissions in Windows 10, the user should utilize the Accounts setting. Here are the steps to create a new user account with different permissions:
? Right-click the Windows Start menu button.
? Select Control Panel.
? Select User Accounts.
? Select Manage another account.
? Select Add a new user in PC settings.
? Use the Accounts dialog box to configure a new account.1

NEW QUESTION 134
A technician is setting up a backup method on a workstation that only requires two sets of tapes to restore. Which of the following would BEST accomplish this task?

A. Differential backup

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

Answer: D

Explanation:
To accomplish this task, the technician should use a Full backup meth1od
A full backup only requires two sets of tapes to restore because it backs up all the data from the workstation. With a differential backup, the backups need to be taken multiple times over a period of time, so more tapes would be needed to restore the data1

NEW QUESTION 138

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

A. Adjust the content filtering.
B. Unmap port forwarding.
C. Disable unused ports.
D. Reduce the encryption strength

Answer: A

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

NEW QUESTION 142

During a recent flight an executive unexpectedly received several dog and cat pictures while trying to watch a movie via in-flight Wi-Fi on an iPhone. The executive has no records of any contacts sending pictures like these and has not seen these pictures before. To BEST resolve this issue, the executive should:

A. set AirDrop so that transfers are only accepted from known contacts
B. completely disable all wireless systems during the flight
C. discontinue using iMessage and only use secure communication applications
D. only allow messages and calls from saved contacts

Answer: A

Explanation:
To best resolve this issue, the executive should set AirDrop so that transfers are only accepted from known contacts (option A). AirDrop is a feature on iOS devices that allows users to share files, photos, and other data between Apple devices. By setting AirDrop so that it only accepts transfers from known contacts, the executive can ensure that unwanted files and photos are not sent to their device. Additionally, the executive should ensure that the AirDrop setting is only enabled when it is necessary, as this will protect their device from any unwanted files and photos.

NEW QUESTION 144
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 147
A change advisory board authorized a setting change so a technician is permitted to Implement the change. The technician successfully implemented the change. Which of the following should be done next?

A. Document the date and time of change
B. Document the purpose of the change.
C. Document the risk level.
D. Document the findings of the sandbox test,

Answer: A

Explanation:
The correct answer is A. Document the date and time of change. After implementing a change, the technician should document the date and time of change in the change log or record. This helps to track the change history, monitor the change performance, and identify any issues or incidents related to the change.
Documenting the date and time of change is also a good practice for auditing and compliance purposes. Documenting the purpose of the change (B) and the risk level © are steps that should be done before implementing the change, not after. These are important information that help to justify, prioritize, and plan the change. The purpose of the change should explain why the change is needed and what benefits it will bring to the organization. The risk level should assess the potential impact and probability of the change causing any problems or disruptions to the business.
Documenting the findings of the sandbox test (D) is also a step that should be done before implementing the change, not after. A sandbox test is a way of testing the change in an isolated environment that mimics the production environment. This helps to verify that the change works as expected and does not cause any errors or conflicts with other systems or processes. The findings of the sandbox test should be documented and reviewed by the change advisory board (CAB) before approving the change for implementation. References:
? What is a Change Advisory Board? (Overview, Roles, and Responsibilities)
? Best Practices in Change Management
? 10 Top change management best practices

NEW QUESTION 149
A user attempts to install additional software and receives a UAC prompt. Which of the following is the BEST way to resolve this issue?

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

Answer: A

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

NEW QUESTION 152
A technician sees a file that is requesting payment to a cryptocurrency address. Which of the following should the technician do first?

A. Quarantine the computer.
B. Disable System Restore.
C. Update the antivirus software definitions.
D. Boot to safe mode.

Answer: A

Explanation:
Quarantining the computer means isolating it from the network and other devices to prevent the spread of malware or ransomware. Ransomware is a type of malware that encrypts the files on a computer and demands payment (usually in cryptocurrency) to restore them. If a technician sees a file that is requesting payment to a cryptocurrency address, it is likely that the computer has been infected by ransomware. Quarantining the computer should be the first step to contain the infection and prevent further damage. Disabling System Restore, updating the antivirus software definitions, and booting to safe mode are not steps that should be done before quarantining the computer.

NEW QUESTION 155
A technician has been tasked with troubleshooting audiovisual issues in a conference room. The meeting presenters are unable to play a video with sound. The following error is received:

The Audio Driver is not running.

Which of the following will MOST likely resolve the issue?

A. compmgmt.msc
B. regedit.exe
C. explorer.exe
D. taskmgt.exe
E. gpmc.msc
F. services.msc

Answer: F

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

NEW QUESTION 156
Which of the following is the most likely to use NTFS as the native filesystem?

A. macOS
B. Linux
C. Windows
D. Android

Answer: C

Explanation:
NTFS stands for New Technology File System, which is a proprietary file system developed by Microsoft4. NTFS is the default file system for the Windows NT family of operating systems, which includes Windows 10, Windows Server 2019, and other versions5. NTFS provides features such as security, encryption, compression, journaling, and large volume support45. NTFS is not the native file system for other operating systems, such as macOS, Linux, or Android, although some of them can read or write to NTFS volumes with third-party drivers or tools

NEW QUESTION 158
A technician requires graphical remote access to various Windows, Linux, and macOS desktops on the company LAN. The security administrator asks the technician to utilize a single software solution that does not require an external internet connection. Which of the following remote access tools is the technician most likely to install?

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

Answer: A

Explanation:
VNC (Virtual Network Computing) is a remote access tool that allows the technician to access and control various Windows, Linux, and macOS desktops on the company LAN using a graphical user interface. VNC does not require an external internet connection, as it works over a local network or a VPN. VNC uses a client-server model, where the server runs on the remote desktop and the client connects to it from another device. VNC can transmit the keyboard and mouse events from the client to the server, and the screen updates from the server to the client, enabling the technician to interact with the remote desktop as if it were local12.
VNC is a better option than the other choices because:
? RMM (Remote Monitoring and Management) (B) is not a single software solution, but a category of software solutions that enable IT professionals to remotely monitor, manage, and troubleshoot multiple devices and networks. RMM software may include remote access tools, but also other features such as patch management, backup and recovery, security, reporting, and automation. RMM software may require an external internet connection, as it often relies on cloud-based services or web-based consoles34.
? RDP (Remote Desktop Protocol) © is a remote access tool that allows the technician to access and control Windows desktops on the company LAN using a graphical user interface. However, RDP is not compatible with Linux or macOS desktops, unless they have third-party software installed that can emulate or translate the RDP protocol. RDP also has some security and performance issues, such as encryption vulnerabilities, bandwidth consumption, and latency problems56.
? SSH (Secure Shell) (D) is a remote access tool that allows the technician to access and control various Windows, Linux, and macOS desktops on the company LAN using a command-line interface. SSH does not require an external internet connection, as it works over a local network or a VPN. SSH uses encryption and authentication to secure the communication between the client and the server. However, SSH does not provide a graphical user interface, which may limit the functionality and usability of the remote desktop7 .
References:
1: What is VNC? - Definition from Techopedia1 2: How VNC Works - RealVNC2 3: What is Remote Monitoring and Management (RMM)? - Definition from Techopedia3 4: What is RMM Software? - NinjaRMM4 5: What is Remote Desktop Protocol (RDP)? - Definition from Techopedia5 6: Remote Desktop Protocol: What it is and how to secure it - CSO Online6 7: What is Secure Shell (SSH)? - Definition from Techopedia7 : How to Use SSH to Access a Remote Server in Linux or Windows - Hostinger Tutorials

NEW QUESTION 160
A change advisory board just approved a change request. Which of the following is the MOST likely next step in the change process?

A. End user acceptance
B. Perform risk analysis
C. Communicate to stakeholders
D. Sandbox testing

Answer: D

Explanation:
The risk analysis should be performed before it's taken to the board. The step after the board approves the change is End User Agreenment Reference: https://www.youtube.com/watch?v=Ru77iZxuElA&list=PLG49S3nxzAnna96gzhJrzkii4hH_mgW4b&index=59

NEW QUESTION 163
Which of the following is an example of MFA?

A. Fingerprint scan and retina scan
B. Password and PIN
C. Username and password
D. Smart card and password

Answer: D

Explanation:
Smart card and password is an example of two-factor authentication (2FA), not multi-factor authentication (MFA). MFA requires two or more authentication factors. Smart card and password is an example of two-factor authentication (2FA2)

NEW QUESTION 166
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 170
An employee calls the help desk regarding an issue with a laptop PC. After a Windows update, the user can no longer use certain locally attached devices, and a reboot has not fixed the issue. Which of the following should the
technician perform to fix the issue?

A. Disable the Windows Update service.
B. Check for updates.
C. Restore hidden updates.
D. Rollback updates.

Answer: D

Explanation:
The technician should perform a rollback of the Windows update that caused the issue with the locally attached devices. A rollback is a process of uninstalling an update and restoring the previous version of the system. This can help to fix any compatibility or performance issues caused by the update1. To rollback an update, the technician can use the Settings app, the Control Panel, or the System Restore feature. The technician should also check for any device driver updates that might be needed after rolling back the update. Disabling the Windows Update service is not a good practice, as it can prevent the system from receiving important security and feature updates. Checking for updates might not fix the
issue, as the update that caused the issue might still be installed. Restoring hidden updates is not relevant, as it only applies to updates that have been hidden by the user to prevent them from being installed2.
References: 1: https://www.windowscentral.com/how-uninstall-and-reinstall-updates-windows-10 2: https://support.microsoft.com/en-us/windows/show-or-hide-updates-in-windows-10-9c9f0a4f-9a6e-4c8e-8b44-afbc6b33f3cf

NEW QUESTION 174
Once weekly a user needs Linux to run a specific open-source application that is not available for the currently installed Windows platform. The user has limited bandwidth throughout the day. Which of the following solutions would be the MOST efficient, allowing for parallel execution of the Linux application and Windows applications?

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

Answer: B

Explanation:
The user should install and run Linux and the required application as a virtual machine installed under the Windows OS. This solution would allow for parallel execution of the Linux application and Windows applications2.
The MOST efficient solution that allows for parallel execution of the Linux application and Windows applications is to install and run Linux and the required application as a virtual machine installed under the Windows OS. This is because it allows you to run both Linux and Windows together without the need to keep

the Linux portion confined to a VM window 3.

NEW QUESTION 175
A change advisory board did not approve a requested change due to the lack of alternative actions if implementation failed. Which of the following should be updated before requesting approval again?

A. Scope of change
B. Risk level
C. Rollback plan
D. End user acceptance

Answer: C

Explanation:
The rollback plan should be updated before requesting approval again. A rollback plan is a plan for undoing a change if it causes problems, and it is an important part of any change management process. If the change advisory board did not approve the requested change due to the lack of alternative actions if implementation failed, then updating the rollback plan would be the best way to address this concern.

NEW QUESTION 176
Which of the following is the MOST important environmental concern inside a data center?

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

Answer: D

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

NEW QUESTION 181
A company implemented a BYOD policy and would like to reduce data disclosure caused by malware that may infect these devices. Which of the following should the company deploy to address these concerns?

A. UAC
B. MDM
C. LDAP
D. SSO

Answer: B

Explanation:
MDM stands for mobile device management, which is a type of software solution that allows remote management and security of mobile devices. MDM can help a company reduce data disclosure caused by malware that may infect these devices by enforcing security policies, such as encryption, password protection, antivirus software, and remote wipe. MDM can also monitor and control the access of personal devices to corporate data and networks. UAC stands for user account control, which is a feature of Windows that prompts users for permission or an administrator password before making changes that affect the system. UAC may not be effective in preventing malware infection or data disclosure on personal devices. LDAP stands for lightweight directory access protocol, which is a protocol for accessing and managing information stored in a directory service, such as user names and passwords. LDAP does not directly address the issue of malware infection or data disclosure on personal devices. SSO stands for single sign-on, which is a feature that allows users to access multiple applications or services with one set of credentials. SSO may not prevent malware infection or data disclosure on personal devices, and may even increase the risk if the credentials are compromised.
https://www.nist.gov/news-events/news/2021/03/mobile-device-security-bring-your-own-device-byod-draft-sp-1800-22

NEW QUESTION 183
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 185

A technician received a call from a user who clicked on a web advertisement Now. every time the user moves the mouse, a pop-up display across the monitor. Which of the following procedures should the technician perform?

A. Boot into safe mode.
B. Perform a malware scan.
C. Restart the machine.
D. Reinstall the browser

Answer: AB

Explanation:
Booting into safe mode and performing a malware scan are the steps that a technician should perform when troubleshooting an issue with pop-up advertising messages on a PC. Safe mode is a diagnostic mode that starts the PC with minimal drivers and services, which can prevent the pop-up malware from running. Malware scan is a tool that can detect and remove the pop-up malware, as well as prevent further infection or damage. Investigating how the malware was installed, reinstalling the browser and restarting the machine are possible steps that can be done after booting into safe mode and performing a malware scan, depending on the situation and the results of the scan. Verified References: https://www.comptia.org/blog/how-to-boot-into-safe-mode https://www.comptia.org/certifications/a

NEW QUESTION 188
A police officer often leaves a workstation for several minutes at a time. Which of the following is the BEST way the officer can secure the workstation quickly when walking away?

A. Use a key combination to lock the computer when leaving.
B. Ensure no unauthorized personnel are in the area.
C. Configure a screensaver to lock the computer automatically after approximately 30 minutes of inactivity.
D. Turn off the monitor to prevent unauthorized visibility of information.

Answer: A

Explanation:
The BEST way to secure the workstation quickly when walking away is to use a key combination to lock the computer when leaving1

NEW QUESTION 193
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 194
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 197
Which of the following involves sending arbitrary characters in a web page request?

A. SMS
B. SSL
C. XSS
D. VPN

Answer: C

Explanation:

XSS stands for cross-site scripting, which is a web security vulnerability that allows an attacker to inject malicious code into a web page that is viewed by other users1. XSS involves sending arbitrary characters in a web page request, such as a query string, a form field, a cookie, or a header, that contain a malicious script. The web server does not validate or encode the input, and returns it as part of the web page response. The browser then executes the script, which can perform various actions on behalf of the attacker, such as stealing cookies, session tokens, or other sensitive information, redirecting the user to a malicious site, or displaying fake content

NEW QUESTION 199
A user reports seeing random, seemingly non-malicious advertisement notifications in the Windows 10 Action Center. The notifications indicate the advertisements are coming from a web browser. Which of the following is the best solution for a technician to implement?

A. Disable the browser from sending notifications to the Action Center.
B. Run a full antivirus scan on the computer.
C. Disable all Action Center notifications.
D. Move specific site notifications from Allowed to Block.

Answer: A

Explanation:
The best solution for a technician to implement is to disable the browser from sending notifications to the Action Center. This will prevent the random advertisement notifications from appearing in the Windows 10 Action Center, which can be annoying and distracting for the user. The technician can follow these steps to disable the browser notifications1:
? Open the browser that is sending the notifications, such as Microsoft Edge, Google Chrome, or Mozilla Firefox.
? Go to the browser settings or options menu, and look for the privacy and security section.
? Find the option to manage site permissions or notifications, and click on it.
? You will see a list of sites that are allowed or blocked from sending notifications to the browser and the Action Center. You can either block all sites from sending notifications, or select specific sites that you want to block or allow.
? Save the changes and close the browser settings. This solution is better than the other options because:
? Running a full antivirus scan on the computer (B) is not necessary, as the advertisement notifications are not malicious or harmful, and they are not caused by a virus or malware infection. Running a scan will not stop the notifications from appearing, and it will consume system resources and time.
? Disabling all Action Center notifications © is not advisable, as the Action Center is a useful feature that shows notifications and alerts from various apps and system events, such as email, calendar, security, updates, etc. Disabling all notifications will make the user miss important information and reminders, and reduce the functionality of the Action Center.
? Moving specific site notifications from Allowed to Block (D) is not the best solution, as it will only stop the notifications from some sites, but not from others. The user may still receive advertisement notifications from other sites that are not blocked, or from new sites that are added to the Allowed list. This solution will also require the user to manually manage the list of sites, which can be tedious and time- consuming.
References:
1: How to Disable Annoying Browser Notifications - PCMag

NEW QUESTION 202
A user reports a computer is running slow. Which of the following tools will help a technician identify the issue?

A. Disk Cleanup
B. Group Policy Editor
C. Disk Management
D. Resource Monitor

Answer: D

Explanation:
Resource Monitor is a Windows utility that can be used to monitor and analyze the system resources and processes running on a computer. It can be used to identify and troubleshoot any issues that might be causing the computer to run slowly, such as CPU usage, memory usage, disk I/O, and network usage.

NEW QUESTION 203
A technician receives a help desk ticket from a user who is unable to update a phone. The technician investigates the issue and notices the following error message: Insufficient storage space
While analyzing the phone, the technician does not discover any third-party' applications or photos. Which of the following is the best way to resolve the issue?

A. Exchange the device for a newer one.
B. Upgrade the onboard storage
C. Allocate more space by removing factory applications
D. Move factory applications to external memory.

Answer: D

Explanation:
The best way to resolve the issue is to move factory applications to external memory. This will free up some space on the phone’s internal storage, which is required for updating the phone. To do this, you can follow these steps1:
? Insert a microSD card into your phone if you don’t have one already.
? Go to Settings > Apps and tap on the app you want to move.
? Tap on Storage and then on Change.
? Select the SD card option and tap on Move.
You may need to repeat this process for multiple apps until you have enough space to update your phone. Alternatively, you can also clear the cache and data of some apps, or uninstall the apps that you don’t use frequently. You can find more information on how to fix insufficient storage error on your phone in these articles234. I hope this helps.

NEW QUESTION 207

A user's Windows computer seems to work well at the beginning of the day. However, its performance degrades throughout the day, and the system freezes when several applications are open. Which of the following should a technician do to resolve the issue? (Select two).

A. Install the latest GPU drivers.
B. Reinstall the OS.
C. Increase the RAM.
D. Increase the hard drive space.
E. Uninstall unnecessary software.
F. Disable scheduled tasks.

Answer: CE

Explanation:
The most likely causes of the user's Windows computer performance degradation and freezing are insufficient RAM and excessive software running in the background. Therefore, the technician should do the following to resolve the issue:
? Increase the RAM. RAM is the memory that the computer uses to store and run applications and processes. If the RAM is not enough to handle the workload, the computer will use the hard drive as a virtual memory, which is much slower and can cause performance issues. Increasing the RAM will allow the computer to run more applications and processes smoothly and avoid freezing. The technician should check the system requirements of the applications that the user needs to run, and install additional RAM modules that are compatible with the motherboard and the existing RAM. The technician should also make sure that the system is managing the page file size automatically, or adjust it manually to optimize the virtual memory usage12.
? Uninstall unnecessary software. Software that the user does not need or use can take up valuable disk space and system resources, and can interfere with the performance of other applications. Some software may also run in the background or start automatically when the computer boots up, which can slow down the system and cause freezing. The technician should help the user to identify and uninstall unnecessary software from the control panel or the settings app, and disable unnecessary startup programs from the task manager or the system configuration tool. The technician should also check for and remove viruses and malware that may affect the system performance134.
References:
1: Tips to improve PC performance in Windows - Microsoft Support1 2: How to Upgrade or Install RAM on Your Windows PC - Lifewire5 3: How to Uninstall Programs on Windows 10
- PCMag6 4: How to Fix a Windows Computer that Hangs or Freezes - wikiHow

NEW QUESTION 212
A user needs assistance changing the desktop wallpaper on a Windows 10 computer. Which of the following methods will enable the user to change the wallpaper using a Windows 10 Settings tool?

A. Open Settings, select Accounts, select Your info, click Browse, and then locate and open the image the user wants to use as the wallpaper.
B. Open Settings, select Personalization, click Browse, and then locate and open the image the user wants to use as the wallpaper.
C. Open Settings, select System, select Display, click Browse, and then locate and open the image the user wants to use as the wallpaper.
D. Open Settings, select Apps, select Apps & features, click Browse, and then locate and open the image the user wants to use as the wallpaper.

Answer: B

Explanation:
The user can change the wallpaper using a Windows 10 Settings tool by following these steps12:
? Open Settings by pressing the Windows key and typing Settings, or by clicking the gear icon in the Start menu.
? Select Personalization from the left navigation menu.
? On the right side of the window, click Background.
? In the Background settings, click the drop-down menu and select Picture as the background type.
? Click Browse and then locate and open the image the user wants to use as the wallpaper.
The other options are incorrect because they do not lead to the Background settings or they do not allow the user to browse for an image. Accounts, System, and Apps are not related to personalization settings. Your info, Display, and Apps & features are not related to wallpaper settings.
References: 1: https://support.microsoft.com/en-us/windows/change-your-desktop-background-image-175618be-4cf1-c159-2785-ec2238b433a8 2: https://www.computerhope.com/issues/ch000592.htm

NEW QUESTION 214
A technician is troubleshooting an issue that requires a user profile to be rebuilt. The technician is unable to locate Local Users and Groups in the Mtv1C console. Which of the following is the NEXT step the technician should take to resolve the issue?

A. Run the antivirus scan.
B. Add the required snap-in.
C. Restore the system backup
D. use the administrator console.

Answer: B

Explanation:
Local Users and Groups is a Microsoft Management Console (MMC) snap-in that allows you to manage user accounts or groups on your computer1. If you cannot find it in the MMC console, you can add it manually by following these steps2:
? Press Windows key + R to open the Run dialog box, or open the Command
Prompt.
? Type mmc and hit Enter. This will open a blank MMC console.
? Click File and then Add/Remove Snap-in.
? In the Add or Remove Snap-ins window, select Local Users and Groups from the Available snap-ins list, and click Add.
? In the Select Computer window, choose Local computer or Another computer, depending on which computer you want to manage, and click Finish.
? Click OK to close the Add or Remove Snap-ins window. You should now see Local Users and Groups in the MMC console.

NEW QUESTION 216
Which of the following common security vulnerabilities can be mitigated by using input validation?

A. Brute-force attack
B. Cross-site scripting

C. SQL injection
D. Cross-site request forgery

Answer: BC

Explanation:
Cross-site scripting (XSS) and SQL injection are common security vulnerabilities that can be mitigated by using input validation. Input validation is a technique that checks the user input for any malicious or unexpected characters or commands before processing it. XSS is an attack that injects malicious scripts into web pages to steal cookies, session tokens or other sensitive information from users or web servers. SQL injection is an attack that injects malicious SQL statements into web applications to manipulate databases, execute commands or access unauthorized data. Verified References: https://www.comptia.org/blog/what-is-input-validation https://www.comptia.org/certifications/a

NEW QUESTION 221
A laptop user is visually impaired and requires a different cursor color. Which of the following OS utilities is used to change the color of the cursor?

A. Keyboard
B. Touch pad
C. Ease of Access Center
D. Display settings

Answer: C

Explanation:
The OS utility used to change the color of the cursor in Windows is Ease of Access Center 12
The user can change the cursor color by opening the Settings app,
selecting Accessibility in the left sidebar, selecting Mouse pointer and touch under Vision, and choosing one of the cursor options. The user can select Custom to pick a color and
use the Size slider to make the cursor larger or sma1lle2r
The Ease of Access Center in the Windows OS provides accessibility options for users with disabilities or impairments. One of these options allows the user to change the color and size of the cursor, making it more visible and easier to locate on the screen. The Keyboard and Touchpad settings do not offer the option to change cursor color, and Display Settings are used to adjust the resolution and other properties of the display. Therefore, C is the best answer. This information is covered in the Comptia A+ Core2 documents/guide under the Accessibility section.

NEW QUESTION 225
Following a recent power outage, several computers have been receiving errors when booting. The technician suspects file corruption has occurred. Which of the following steps should the technician try FIRST to correct the issue?

A. Rebuild the Windows profiles.
B. Restore the computers from backup.
C. Reimage the computers.
D. Run the System File Checker.

Answer: D

Explanation:
The technician should run the System File Checker (SFC) first to correct file corruption errors on computers after a power outage. SFC is a command-line utility that scans for and repairs corrupted system files. It can be run from the command prompt or from the Windows Recovery Environment. Rebuilding the Windows profiles, restoring the computers from backup, and reimaging the computers are more drastic measures that should be taken only if SFC fails to correct the issue1

NEW QUESTION 227
An administrator responded to an incident where an employee copied financial data to a portable hard drive and then left the company with the data. The administrator documented the movement of the evidence. Which of the following concepts did the administrator demonstrate?

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

Answer: A

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

NEW QUESTION 232
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 lor 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 233
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 238
Which of the following script types is used with the Python language by default?

A. .ps1
B. .vbs
C. .bat
D. .py

Answer: D

Explanation:
The script type that is used with the Python language by default is .py. .py is a file extension that indicates a Python script file that contains Python code that can be executed by a Python interpreter or compiler. Python is a high-level, general-purpose and interpreted programming language that can be used for various applications, such as web development, data analysis, machine learning and automation. .ps1 is a file extension that indicates a PowerShell script file that contains PowerShell code that can be executed by a PowerShell interpreter or compiler. PowerShell is a task-based, command-line and scripting language that can be used for system administration and automation on Windows systems. .vbs is a file extension that indicates a VBScript file that contains VBScript code that can be executed by a VBScript interpreter or compiler. VBScript is an Active Scripting language that can be used for web development and automation on Windows systems. .bat is a file extension that indicates a batch file that contains a series of commands that can be executed by a command-line interpreter or shell on Windows systems. Batch files can be used for system administration and automation on Windows systems. References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 4.3

NEW QUESTION 243
A technician installed Windows 10 on a workstation. The workstation only has 3.5GB of usable RAM, even though the technician installed 8GB. Which of the following is the MOST likely reason this system is not utilizing all the available RAM?

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

Answer: B

Explanation:
The most likely reason that the system is not utilizing all the available RAM is that the system is utilizing a 32-bit OS. A 32-bit OS is an operating system that uses 32 bits to address memory locations and perform calculations. A 32-bit OS can only support up to 4GB of RAM, and some of that RAM may be reserved for hardware devices or system functions, leaving less than 4GB of usable RAM for applications and processes. A 32-bit OS cannot recognize or utilize more than 4GB of RAM, even if more RAM is installed on the system. To utilize all the available RAM, the system needs to use a 64-bit OS, which can support much more RAM than a 32-bit OS. The system missing updates may cause some performance or compatibility issues, but it does not affect the amount of usable RAM on the system. The system's memory failing may cause some errors or crashes, but it does not affect the amount of usable RAM on the system. The system requiring BIOS updates may cause some configuration or compatibility issues, but it does not affect the amount of usable RAM on the system. References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.1

NEW QUESTION 245
A technician is working on a Windows 10 PC that has unwanted applications starting on boot. Which of the following tools should the technician use to disable applications on startup?

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Task Manager is the best tool to use to disable applications on startup in Windows 10. Task Manager is a built-in utility that shows the current processes, performance, and users on a system. It also has a Startup tab that lists the applications that run on boot and their impact on the system. The technician can use

Task Manager to disable or enable any application on startup by right-clicking on it and selecting the appropriate option. System Configuration, Performance Monitor, and Group Policy Editor are other tools that can be used to manage system settings, but they are not as simple or convenient as Task Manager for this task. References:
? Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 13
? CompTIA A+ Complete Study Guide: Core 1 Exam 220-1101 and Core 2 Exam …, page 103

NEW QUESTION 248
A user's company phone was stolen. Which of the following should a technician do next?

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

Answer: B

Explanation:
Remotely wiping the device is the best option to prevent unauthorized access to the company data stored on the phone. A low-level format, degaussing, or providing the GPS location of the device are not feasible or effective actions to take in this scenario.
References: The Official CompTIA A+ Core 2 Study Guide1, page 315.

NEW QUESTION 250
A user updates a mobile device's OS. A frequently used application becomes consistently unresponsive immediately after the device is launched. Which of the following troubleshooting steps should the user perform FIRST?

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

Answer: B

Explanation:
Sometimes, an OS update can cause compatibility issues with some applications that are not optimized for the new version of the OS. To fix this, the user should check if there are any updates available for the application that can resolve the issue. The user can check for application updates by following these steps:
? On an Android device, open the Google Play Store app and tap on the menu icon in the top left corner. Then tap on My apps & games and look for any updates available for the application. If there is an update, tap on Update to install it.
? On an iOS device, open the App Store app and tap on the Updates tab at the bottom. Then look for any updates available for the application. If there is an update, tap on Update to install it.

NEW QUESTION 251
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 254
A user has a license for an application that is in use on a personal home laptop. The user approaches a systems administrator about using the same license on multiple computers on the corporate network. Which of the following BEST describes what the systems administrator should tell the user?

A. Use the application only on the home laptop because it contains the initial license.
B. Use the application at home and contact the vendor regarding a corporate license.
C. Use the application on any computer since the user has a license.
D. Use the application only on corporate computers.

Answer: B

Explanation:
Use the application at home and contact the vendor regarding a corporate license. The user should use the application only on the home laptop because it contains the initial license. The user should contact the vendor regarding a corporate license if they want to use the application on multiple computers on the corporate network1

NEW QUESTION 258
A PC is taking a long time to boot Which of the following operations would be best to do to resolve the issue at a minimal expense? (Select two).

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

Answer: BD

Explanation:
The best operations to do to resolve the issue of a long boot time at a minimal expense are B. Removing the applications from startup and D. Running the Disk Cleanup utility. These are two simple and effective ways to speed up your PC's boot time without spending any money on hardware upgrades.
Removing the applications from startup means preventing unnecessary programs from launching automatically when you turn on your computer. This can reduce the load on your system resources and make the boot process faster. You can do this in Windows 10 by pressing Ctrl + Alt + Esc to open the Task Manager, and going to the Startup tab. There, you can see a list of programs that start with your computer, and their impact on the startup performance. You can disable any program that you don't need by right-clicking on it and choosing Disable12.
Running the Disk Cleanup utility means deleting temporary files, system files, and other unnecessary data that may be taking up space and slowing down your computer. This can free up some disk space and improve the performance of your system. You can do this in Windows 10 by typing disk cleanup in the search box and selecting the Disk Cleanup app. There, you can choose which files you want to delete, such as Recycle Bin, Temporary Internet Files, Thumbnails, etc. You can also click on Clean up system files to delete more files, such as Windows Update Cleanup, Previous Windows installation(s), etc34.

NEW QUESTION 261
A technician is setting up a backup method on a workstation that only requires two sets of tapes to restore. Which of the following would BEST accomplish this task?

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

Answer: D

Explanation:
A full backup involves creating a copy of all data on the workstation, including system files and user-created data, and storing it on a set of tapes. This ensures that all data is backed up, and ensures that the data can be restored in the event of a system failure or data loss.

NEW QUESTION 262
Which of The following refers to the steps to be taken if an Issue occurs during a change Implementation?

A. Testing
B. Rollback
C. Risk
D. Acceptance

Answer: B

Explanation:
Rollback refers to the steps to be taken if an issue occurs during a change implementation. It means restoring the system to its previous state before the change was applied, using backup data or configuration files. It can minimize the impact and downtime caused by a failed change. Testing refers to the steps to be taken before a change implementation, to verify that the change works as expected and does not cause any errors or conflicts. Risk refers to the potential negative consequences of a change implementation, such as data loss, security breach, performance degradation, etc.
Acceptance refers to the steps to be taken after a change implementation, to confirm that the change meets the requirements and expectations of the stakeholders. Verified References: https://www.comptia.org/blog/change-management-process https://www.comptia.org/certifications/a

NEW QUESTION 263
Which of the following is used to integrate Linux servers and desktops into Windows Active Directory environments?

A. apt-get
B. CIFS
C. Samba
D. greP

Answer: C

Explanation:
Samba is a software suite that allows Linux servers and desktops to integrate with Windows Active Directory environments. Samba can act as a domain controller, a file server, a print server, or a client for Windows networks. Samba can also provide authentication and authorization services for Linux users and devices using Active Directory.

NEW QUESTION 264
A technician cannot uninstall a system driver because the driver is currently in use. Which of the following tools should the technician use to help uninstall the driver?

A. msinfo32.exe
B. dxdiag.exe
C. msconfig.exe
D. regedit.exe

Answer: C

Explanation:
The msconfig.exe tool, also known as the System Configuration utility, is a tool that allows users to modify various system settings, such as startup options, services, boot options, and more. One of the features of msconfig.exe is the ability to disable or enable device drivers that are loaded during the system startup. By using msconfig.exe, a technician can prevent a driver from being loaded and used by the system, which will allow them to uninstall it without any errors. To use msconfig.exe to disable a driver, the technician can follow these steps:
? Open the Run dialog box by pressing the Windows key + R.
? Type msconfig.exe and press Enter.
? Click on the Boot tab and then click on Advanced options.
? Check the box next to No GUI boot and click OK. This will prevent the graphical user interface from loading during the boot process, which will also prevent some drivers from loading.
? Click on the Services tab and check the box next to Hide all Microsoft services.
This will show only the third-party services and drivers that are running on the system.
? Find the service or driver that corresponds to the device that the technician wants
to uninstall and uncheck the box next to it. This will disable the service or driver from starting during the system startup.
? Click Apply and OK and then restart the computer.
? After the computer restarts, the technician can use the Device Manager or the Control Panel to uninstall the driver that was previously in use.
References:
? How to Completely Remove/Uninstall a Driver in Windows, section 31
? The Official CompTIA A+ Core 2 Study Guide (220-1102), page 2212

NEW QUESTION 267
A malicious file was executed automatically when a flash drive was plugged in. Which of the following features would prevent this type of incident?

A. Disabling UAC
B. Restricting local administrators
C. Enabling UPnP
D. Turning off AutoPlay

Answer: D

Explanation:
AutoPlay is a feature that automatically runs programs or files when a removable media device, such as a flash drive, is plugged in. This can be exploited by malware authors who place malicious files on flash drives that execute automatically when inserted into a computer. Turning off AutoPlay can prevent this type of incident by requiring the user to manually open or run files from removable media devices. Disabling UAC (user account control), restricting local administrators and enabling UPnP (universal plug and play) are not effective ways to prevent this type of incident. Verified References: https://www.comptia.org/blog/autoplay-security-risk https://www.comptia.org/certifications/a

NEW QUESTION 269
A user is configuring a new SOHO Wi-Fi router for the first time. Which of the following settings should the user change FIRST?

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

Answer: C

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

NEW QUESTION 273
A technician needs to recommend the best backup method that will mitigate ransomware attacks. Only a few files are regularly modified, however, storage space is a concern. Which of the following backup methods would BEST address these concerns?

A. Full
B. Differential
C. Off-site
D. Grandfather-father-son

Answer: B

Explanation:
The differential backup method would best address these concerns. Differential backups only back up files that have changed since the last full backup, which means that only a few files would be backed up each time. This would help to mitigate the risk of ransomware attacks, as only a few files would be affected if an attack occurred. Additionally, differential backups require less storage space than full backups.

NEW QUESTION 274
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

220-1102 Practice Exam Features:

* 220-1102 Questions and Answers Updated Frequently

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

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

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