CompTIA

Exam Questions 220-1102

CompTIA A+ Certification Exam: Core 2

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

  All examinations will be up to date.

* 24/7 Quality Support

  We will provide service round the clock.

* 100% Pass Rate

  Our guarantee that you will pass the exam.

* Unique Gurantee

  If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
A macOS user reports seeing a spinning round cursor on a program that appears to be frozen. Which of the following methods does the technician use to force the program to close in macOS?

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

Answer: D

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

NEW QUESTION 2
A company installed a new backup and recovery system. Which of the following types of backups should be completed FIRST?

A. Full
B. Non-parity
C. Differential
D. Incremental

Answer: A

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

NEW QUESTION 3
Which of the following file extensions are commonly used to install applications on a macOS machine? (Select THREE).

A. .mac
B. .Pkg
C. .deb
D. .dmg
E. .msi
F. .appx
G. .app
H. .apk

Answer: BDG

Explanation:
https://support.microsoft.com/en-us/windows/common-file-name-extensions-in-windows-da4a4430-8e76-89c5
.pkg and .dmg are files used to distribute and install applications on macOS. .pkg files are installer packages that may contain multiple files and executable code, while .dmg files are disk images that can contain a single bundled application or multiple applications. .app files are typically the main executable files for macOS applications. The other options listed are file extensions for applications or installers on other platforms (such as .deb for Debian-based Linux systems, .msi for Windows, and .apk for Android). This information is covered in the Comptia A+ Core2 documents/guide under the Mac OS section.

NEW QUESTION 4
A technician is troubleshooting a lack of outgoing audio on a third-party Windows 10 VoIP application, The PC uses a USB microphone connected to a powered hub. The technician verifies the microphone works on the PC using Voice Recorder. Which of the following should the technician do to solve the issue?

A. Remove the microphone from the USB hub and plug it directly into a USB port on the PC.
B. Enable the microphone under Windows Privacy settings to allow desktop applications to access it.
C. Delete the microphone from Device Manager and scan for new hardware,
D. Replace the USB microphone with one that uses a traditional 3.5mm plug.

Answer: B

Explanation:
In Windows 10, there are privacy settings that control access to certain devices, such as microphones, cameras, and other input devices. If the microphone is not enabled under these privacy settings, the VoIP application may not have access to it, causing a lack of outgoing audio.
The technician can go to the Windows 10 Settings menu, select the Privacy submenu, and under App permissions, select Microphone. The technician should then turn on the toggle switch for the VoIP application to allow it to access the microphone.
Removing the microphone from the USB hub and plugging it directly into a USB port on the PC may or may not solve the issue, as the issue could be related to the privacy settings. Deleting the microphone from Device Manager and scanning for new hardware may also not solve the issue, as the issue could be related to the privacy settings. Replacing the USB microphone with one that uses a traditional 3.5mm plug is not recommended, as it would require purchasing a new microphone and may not solve the issue.

NEW QUESTION 5
A user is experiencing frequent malware symptoms on a Windows workstation. The user has tried several times to roll back the state but the malware persists. Which of the following would MOST likely resolve the issue?

A. Quarantining system files
B. Reimaging the workstation
C. Encrypting the hard drive
D. Disabling TLS 1.0 support

Answer: C

Explanation:
Encrypting the hard drive would most likely resolve the issue1

NEW QUESTION 6
A user is having issues with document-processing software on a Windows workstation. Other users that log in to the same device do not have the same issue. Which of the following should a technician do to remediate the issue?

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

Answer: D

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

NEW QUESTION 7
A call center technician receives a call from a user asking how to update Windows Which of the following describes what the technician should do?

A. Have the user consider using an iPad if the user is unable to complete updates
B. Have the user text the user's password to the technician.
C. Ask the user to click in the Search field, type Check for Updates, and then press the Enter key
D. Advise the user to wait for an upcoming, automatic patch

Answer: C

Explanation:
The technician should guide the user to update Windows through the built-in "Check for Updates" feature. This can be done by having the user click in the Search field, type "Check for Updates", and then press the Enter key. This will bring up the Windows Update function, which will search for any available updates and give the user the option to install them.

NEW QUESTION 8
A network administrator is deploying a client certificate lo be used for Wi-Fi access for all devices m an organization The certificate will be used in conjunction with the user's existing username and password Which of the following BEST describes the security benefits realized after this deployment?

A. Multifactor authentication will be forced for Wi-Fi
B. All Wi-Fi traffic will be encrypted in transit
C. Eavesdropping attempts will be prevented
D. Rogue access points will not connect

Answer: A

Explanation:
Multifactor authentication will be forced for Wi-Fi after deploying a client certificate to be used for Wi-Fi access for all devices in an organization3
References:
CompTIA Security+ (Plus) Practice Test Questions | CompTIA. Retrieved from https://www.comptia.org/training/resources/comptia-security-practice-tests

NEW QUESTION 9
A technician is reimaging a desktop PC. The technician connects the PC to the network and powers it on. The technician attempts to boot the computer via the NIC to image the computer, but this method does not work. Which of the following is the MOST likely reason the computer is unable to boot into the imaging system via the network?

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

Answer: C

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

NEW QUESTION 10
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 10
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 15
An analyst needs GUI access to server software running on a macOS server. Which of the following options provides the BEST way for the analyst to access the macOS server from the Windows workstation?

A. RDP through RD Gateway
B. Apple Remote Desktop
C. SSH access with SSH keys
D. VNC with username and password

Answer: B

Explanation:
Apple Remote Desktop is a remote access solution that allows a user to access and control another macOS computer from their Windows workstation. It provides a graphical user interface so that the analyst can easily access the server software running on the macOS server. Apple Remote Desktop also supports file transfers, so the analyst can easily transfer files between the two computers. Additionally, Apple Remote Desktop supports encryption, so data is secure during transmission.

NEW QUESTION 18
A technician receives a ticket indicating the user cannot resolve external web pages However, specific IP addresses are working. Which of the following does the technician MOST likely need to change on the workstation to resolve the issue?

A. Default gateway
B. Host address
C. Name server
D. Subnet mask

Answer: A

Explanation:
The technician most likely needs to change the default gateway on the workstation to resolve the issue. The default gateway is the IP address of the router that connects the workstation to the internet, and it is responsible for routing traffic between the workstation and the internet. If the default gateway is incorrect, the workstation will not be able to access external web pages.

NEW QUESTION 19
A technician has been tasked with using the fastest and most secure method of logging in to laptops. Which of the following log-in options meets these requirements?

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

Answer: A

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

NEW QUESTION 24
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-61c0-4f

NEW QUESTION 28
A user contacted the help desk to report pop-ups on a company workstation indicating the computer has been infected with 137 viruses and payment is needed to remove them. The user thought the company-provided antivirus software would prevent this issue. The help desk ticket states that the user only receives these messages when first opening the web browser. Which of the following steps would MOST likely resolve the issue? (Select TWO)

A. Scan the computer with the company-provided antivirus software
B. Install a new hard drive and clone the user's drive to it
C. Deploy an ad-blocking extension to the browser.
D. Uninstall the company-provided antivirus software
E. Click the link in the messages to pay for virus removal
F. Perform a reset on the user's web browser

Answer: CF

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

NEW QUESTION 33
While browsing a website, a staff member received a message that the website could not be trusted. Shortly afterward, several other colleagues reported the same issue across numerous other websites. Remote users who were not connected to corporate resources did not have any issues. Which of the following is MOST likely the cause of this issue?

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

Answer: B

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

NEW QUESTION 34
The web browsing speed on a customer's mobile phone slows down every few weeks and then returns to normal after three or four days. Restarting the device does not usually restore performance. Which of the following should a technician check FIRST to troubleshoot this issue?

A. Data usage limits
B. Wi-Fi connection speed
C. Status of airplane mode
D. System uptime

Answer: B

Explanation:
The technician should check the Wi-Fi connection speed first to troubleshoot this issue. Slow web browsing speed on a mobile phone can be caused by a slow Wi-Fi connection. The technician should check the Wi-Fi connection speed to ensure that it is fast enough to support web browsing. If the Wi-Fi connection speed is slow, the technician should troubleshoot the Wi-Fi network to identify and resolve the issue.

NEW QUESTION 36
A call center handles inquiries into billing issues for multiple medical facilities. A security analyst notices that call center agents often walk away from their workstations, leaving patient data visible for anyone to see. Which of the following should a network administrator do to BEST prevent data theft within the call center?

A. Encrypt the workstation hard drives.
B. Lock the workstations after five minutes of inactivity.
C. Install privacy screens.

D. Log off the users when their workstations are not in use.

Answer: B

Explanation:
The BEST solution for preventing data theft within the call center in this scenario would be to lock the workstations after a period of inactivity. This would prevent unauthorized individuals from accessing patient data if call center agents were to step away from their workstations without logging out.

NEW QUESTION 37
The command cac cor.ptia. txt was issued on a Linux terminal. Which of the following results should be expected?

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

Answer: B

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

NEW QUESTION 42
A user is attempting to make a purchase at a store using a phone. The user places the phone on the payment pad, but the device does not recognize the phone. The user attempts to restart the phone but still has the same results. Which of the following should the user do to resolve the issue?

A. Turn off airplane mode while at the register.
B. Verify that NFC is enabled.
C. Connect to the store's Wi-Fi network.
D. Enable Bluetooth on the phone.

Answer: B

Explanation:
The user should verify that NFC is enabled on their phone. NFC is a technology that allows two devices to communicate with each other when they are in close proximity2.
NFC (Near Field Communication) technology allows a phone to wirelessly communicate with a payment terminal or other compatible device. In order to use NFC to make a payment or transfer information, the feature must be enabled on the phone. Therefore, the user should verify that NFC is enabled on their phone before attempting to make a payment with it. The other options, such as turning off airplane mode, connecting to Wi-Fi, or enabling Bluetooth, do not pertain to the NFC feature and are unlikely to resolve the issue. This information is covered in the Comptia A+ Core2 documents/guide under the Mobile Devices section.

NEW QUESTION 45
A technician has been asked to set up a new wireless router with the best possible security. Which of the following should the technician implement?

A. WPS
B. TKIP
C. WPA3
D. WEP

Answer: C

Explanation:
WPA3 (Wi-Fi Protected Access version 3) is the latest version of Wi-Fi security and offers the highest level of protection available. It is designed to protect against brute force password attempts and protect against eavesdropping and man-in-the-middle attacks. WPA3 also supports the use of stronger encryption algorithms, such as the Advanced Encryption Standard (AES), which provides additional protection for wireless networks. WPA3 should be implemented in order to ensure the best possible security for the new wireless router.

NEW QUESTION 46
Which of the following Wi-Fi protocols is the MOST secure?

A. WPA3
B. WPA-AES
C. WEP
D. WPA-TKIP

Answer: A

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

NEW QUESTION 49
A technician has an external SSD. The technician needs to read and write to an external SSD on both Macs and Windows PCs. Which of the following filesystems is supported by both OS types?

A. NTFS

B. APFS
C. ext4
D. exFAT

Answer: D

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

NEW QUESTION 53
A technician is troubleshooting an issue involving programs on a Windows 10 machine that are loading on startup but causing excessive boot times. Which of the following should the technician do to selectively prevent programs from loading?

A. Right-click the Windows button, then select Run entering shell startup and clicking OK, and then move items one by one to the Recycle Bin
B. Remark out entries listed HKEY_LOCAL_MACHINE>SOFTWARE>Microsoft>Windows>CurrentVersion>Run
C. Manually disable all startup tasks currently listed as enabled and reboot checking for issue resolution at startup
D. Open the Startup tab and methodically disable items currently listed as enabled and reboot, checking for issue resolution at each startup.

Answer: D

Explanation:
This is the most effective way to selectively prevent programs from loading on a Windows 10 machine. The Startup tab can be accessed by opening Task Manager and then selecting the Startup tab. From there, the technician can methodically disable items that are currently listed as enabled, reboot the machine, and check for issue resolution at each startup. If the issue persists, the technician can then move on to disabling the next item on the list.

NEW QUESTION 57
A systems administrator is setting up a Windows computer for a new user Corporate policy requires a least privilege environment. The user will need to access advanced features and configuration settings for several applications. Which of the following BEST describes the account access level the user will need?

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

Answer: B

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

NEW QUESTION 60
A technician suspects the boot disk of a user's computer contains bad sectors. Which of the following should the technician verify in the command prompt to address the issue without making any changes?

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

Answer: C

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

NEW QUESTION 62
A user's system is infected with malware. A technician updates the anti-malware software and runs a scan that removes the malware. After the user reboots the system, it once again becomes infected with malware. Which of the following will MOST likely help to permanently remove the malware?

A. Enabling System Restore
B. Educating the user
C. Booting into safe mode
D. Scheduling a scan

Answer: B

Explanation:
Although updating the anti-malware software and running scans are important steps in removing malware, they may not be sufficient to permanently remove the malware if the user keeps engaging in behaviors that leave the system vulnerable, such as downloading unknown files or visiting malicious websites. Therefore, educating the user on safe computing practices is the best way to prevent future infections and permanently remove the malware.
Enabling System Restore, Booting into safe mode, and scheduling a scan are not the most efficient ways to permanently remove the malware. Enabling System Restore and Booting into safe mode may help in some cases, but they may not be sufficient to permanently remove the malware. Scheduling a scan is also important for detecting and removing malware, but it may not be sufficient to prevent future infections.
https://partners.comptia.org/docs/default-source/resources/comptia-a-220-1102-exam-objectives-(3-0)

NEW QUESTION 66
A technician is configuring a SOHO device Company policy dictates that static IP addresses cannot be used. The company wants the server to maintain the same IP address at all times. Which of the following should the technician use?

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

Answer: A

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

NEW QUESTION 67
A user reports a PC is running slowly. The technician suspects it has a badly fragmented hard drive. Which of the following tools should the technician use?

A. resmon exe
B. msconfig.extf
C. dfrgui exe
D. msmfo32.exe

Answer: C

Explanation:
The technician should use dfrgui.exe to defragment the hard drive1

NEW QUESTION 71
The network was breached over the weekend System logs indicate that a single user's account was successfully breached after 500 attempts with a dictionary attack. Which of the following would BEST mitigate this threat?

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

Answer: B

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

NEW QUESTION 72
Which of the following is a consequence of end-of-lite operating systems?

A. Operating systems void the hardware warranty.
B. Operating systems cease to function.
C. Operating systems no longer receive updates.
D. Operating systems are unable to migrate data to the new operating system.

Answer: C

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

NEW QUESTION 77
An administrator has received approval for a change request for an upcoming server deployment. Which of the following steps should be completed NEXT?

A. Perform a risk analysis.
B. Implement the deployment.
C. Verify end user acceptance
D. Document the lessons learned.

Answer: A

Explanation:
Before making any changes to the system, it is important to assess the risks associated with the change and determine whether it is worth implementing. Risk analysis involves identifying potential risks, assessing their likelihood and impact, and determining what steps can be taken to mitigate them. It is important to perform this step before making any changes, as this allows the administrator to make an informed decision about whether or not the change should be implemented. Once the risks have been assessed and the administrator has decided to go ahead with the change, the next step is to implement the deployment.

NEW QUESTION 82
A desktop support technician is tasked with migrating several PCs from Windows 7 Pro to Windows 10 Pro, The technician must ensure files and user preferences

are retained, must perform the operation locally, and should migrate one station at a time. Which of the following methods would be MOST efficient?

A. Golden image
B. Remote network install
C. In-place upgrade
D. Clean install

Answer: C

Explanation:
An in-place upgrade is the most efficient method for migrating from Windows 7 Pro to Windows 10 Pro, as it will retain all user files and preferences, can be done locally, and can be done one station at a time. An
in-place upgrade involves installing the new version of Windows over the existing version, and can be done quickly and easily.

NEW QUESTION 87
A user is unable to log in to the domain with a desktop PC, but a laptop PC is working properly on the same network. A technician logs in lo the desktop PC with a local account but is unable to browse to the secure intranet site to get troubleshooting tools. Which of the following is the MOST likely cause of the issue?

A. Time drift
B. Dual in-line memory module failure
C. Application crash
D. Filesystem errors

Answer: A

Explanation:
The most likely cause of the issue is a “time drift”. Time drift occurs when the clock on a computer is not synchronized with the clock on the domain controller. This can cause authentication problems when a user tries to log in to the domain. The fact that the technician is unable to browse to the secure intranet site to get troubleshooting tools suggests that there may be a problem with the network connection or the firewall settings on the desktop PC12

NEW QUESTION 92
An organization's Chief Financial Officer (CFO) is concerned about losing access to very sensitive, legacy unmaintained PII on a workstation if a ransomware outbreak occurs. The CFO has a regulatory requirement to retain this data for many years. Which of the following backup methods would BEST meet the requirements?

A. A daily, incremental backup that is saved to the corporate file server
B. An additional, secondary hard drive in a mirrored RAID configuration
C. A full backup of the data that is stored of site in cold storage
D. Weekly, differential backups that are stored in a cloud-hosting provider

Answer: C

Explanation:
According to CompTIA A+ Core 2 objectives, a full backup stored off-site provides the greatest protection against data loss in the event of a ransomware attack or other data disaster. By storing the backup in a separate physical location, it is less likely to be affected by the same event that could cause data loss on the original system. Cold storage is a term used for data archiving, which typically refers to a long-term storage solution that is used for retaining data that is infrequently accessed, but still needs to be kept for regulatory or compliance reasons.

NEW QUESTION 93
A user is attempting to browse the internet using Internet Explorer. When trying to load a familiar web page, the user is unexpectedly redirected to an unfamiliar website. Which of the following would MOST likely solve the issue?

A. Updating the operating system
B. Changing proxy settings
C. Reinstalling the browser
D. Enabling port forwarding

Answer: C

Explanation:
Reinstalling the browser would most likely solve the issue. This would remove any malicious software or add-ons that may be causing the issue and restore the browser to its default settings.

NEW QUESTION 96
A user receives a notification indicating the data plan on the user's corporate phone has reached its limit. The user has also noted the performance of the phone is abnormally slow. A technician discovers a third-party GPS application was installed on the phone. Which of the following is the MOST likely cause?

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

Answer: B

Explanation:
The GPS application contains malware. The third-party GPS application is likely the cause of the slow performance of the phone. The application may contain malware that is using up system resources and slowing down the phone. The user should uninstall the application and run a malware scan on the phon1e

NEW QUESTION 99
A technician has been tasked with installing a workstation that will be used tor point-of-sale transactions. The point-of-sale system will process credit cards and loyalty cards. Which of the following encryption technologies should be used to secure the workstation in case of theft?

A. Data-in-transit encryption
B. File encryption
C. USB drive encryption
D. Disk encryption

Answer: D

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

NEW QUESTION 100
Which of the following should be used to control security settings on an Android phone in a domain environment?

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

Answer: A

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

NEW QUESTION 103
A user reports a workstation has been performing strangely after a suspicious email was opened on it earlier in the week. Which of the following should the technician perform FIRST?

A. Escalate the ticket to Tier 2.
B. Run a virus scan.
C. Utilize a Windows restore point.
D. Reimage the computer.

Answer: B

Explanation:
https://partners.comptia.org/docs/default-source/resources/comptia-a-220-1102-exam-objectives-(3-0)
When a user reports that their workstation is behaving strangely after opening a suspicious email, the first step a technician should take is to run a virus scan on the computer. This is because opening a suspicious email is a common way for viruses and malware to infect a computer. Running a virus scan can help identify and remove any infections that may be causing the computer to behave strangely.

NEW QUESTION 104
Which of the following is the MOST basic version of Windows that includes BitLocker?

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

Answer: D

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

NEW QUESTION 105
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 107

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

A. Scan and remove the malware
B. Schedule automated malware scans
C. Quarantine the system
D. Disable System Restore

Answer: C

Explanation:
The technician should quarantine the system first1

NEW QUESTION 112
A company needs to securely dispose of data stored on optical discs. Which of the following is the MOST effective method to accomplish this task?

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

Answer: D

Explanation:
Shredding is the most effective method to securely dispose of data stored on optical discs12 References: 4. How Can I Safely Destroy Sensitive Data CDs/DVDs? - How-To Geek. Retrieved from https://www.howtogeek.com/174307/how-can-i-safely-destroy-sensitive-data-cdsdvds/ 5. Disposal — UK Data Service. Retrieved from https://ukdataservice.ac.uk/learning-hub/research-data-management/store-your-data/disposal/

NEW QUESTION 117
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 122
An incident handler needs to preserve evidence for possible litigation. Which of the following will the incident handler MOST likely do to preserve the evidence?

A. Encrypt the files
B. Clone any impacted hard drives
C. Contact the cyber insurance company
D. Inform law enforcement

Answer: B

Explanation:
The incident handler should clone any impacted hard drives to preserve evidence for possible litigation1

NEW QUESTION 124
A technician needs lo formal a USB drive to transfer 20GB of data from a Linux computer to a Windows computer. Which of the following filesystems will the technician MOST likely use?

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

Answer: C

Explanation:
Since Windows systems support FAT32 and NTFS "out of the box" and Linux supports a whole range of them including FAT32 and NTFS, it is highly

recommended to format the partition or disk you want to share in either FAT32 or NTFS, but since FAT32 has a file size limit of 4.2 GB, if you happen to work with huge files, then it is better you use NTFS

NEW QUESTION 128
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

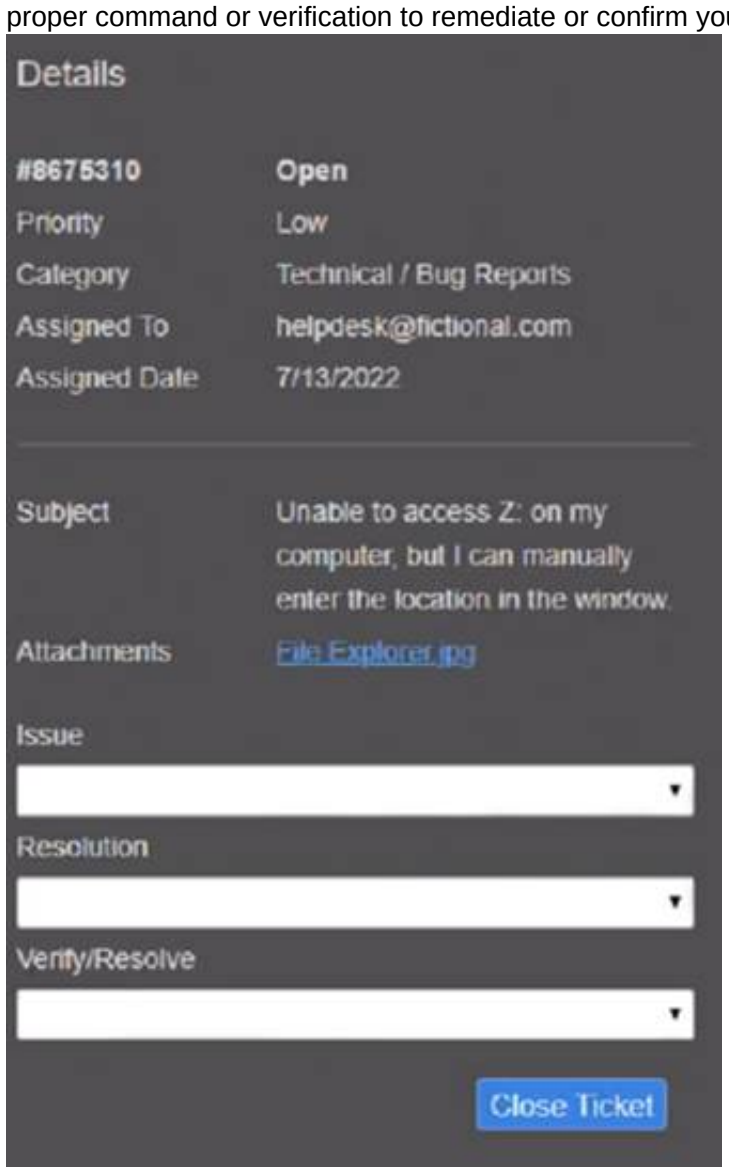
NEW QUESTION 129
A Microsoft Windows PC needs to be set up for a user at a targe corporation. The user will need access to the corporate domain to access email and shared drives. Which of the following versions of Windows would a technician MOST likely deploy for the user?

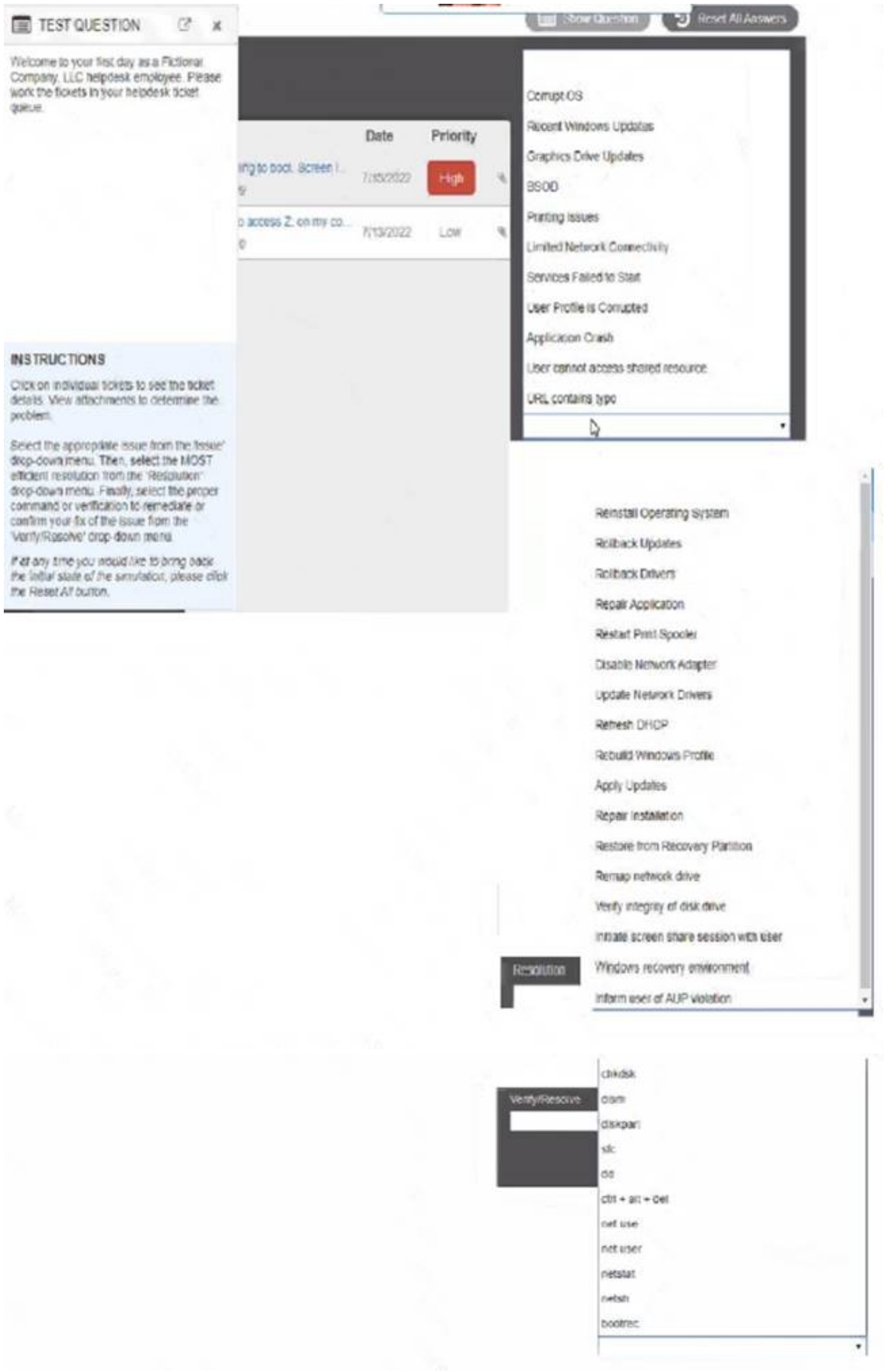
A. Windows Enterprise Edition
B. Windows Professional Edition
C. Windows Server Standard Edition
D. Windows Home Edition

Answer: B

Explanation:
The Windows Professional Edition is the most likely version that a technician would deploy for a user at a target corporation. This version of Windows is designed for business use and provides the necessary features and capabilities that a user would need to access the corporate domain, such as email and shared drives.

NEW QUESTION 132
Welcome to your first day as a Fictional Company. LLC helpdesk employee. Please work the tickets in your helpdesk ticket queue.
Click on individual tickers to see the ticket details. View attachments to determine the problem.
Select the appropriate issue from the 'issue' drop-down menu. Then, select the MOST efficient resolution from the 'Resolution' drop-down menu. Finally, select the proper command or verification to remediate or confirm your fix of the issue from the Verify Resolve drop-down menu.

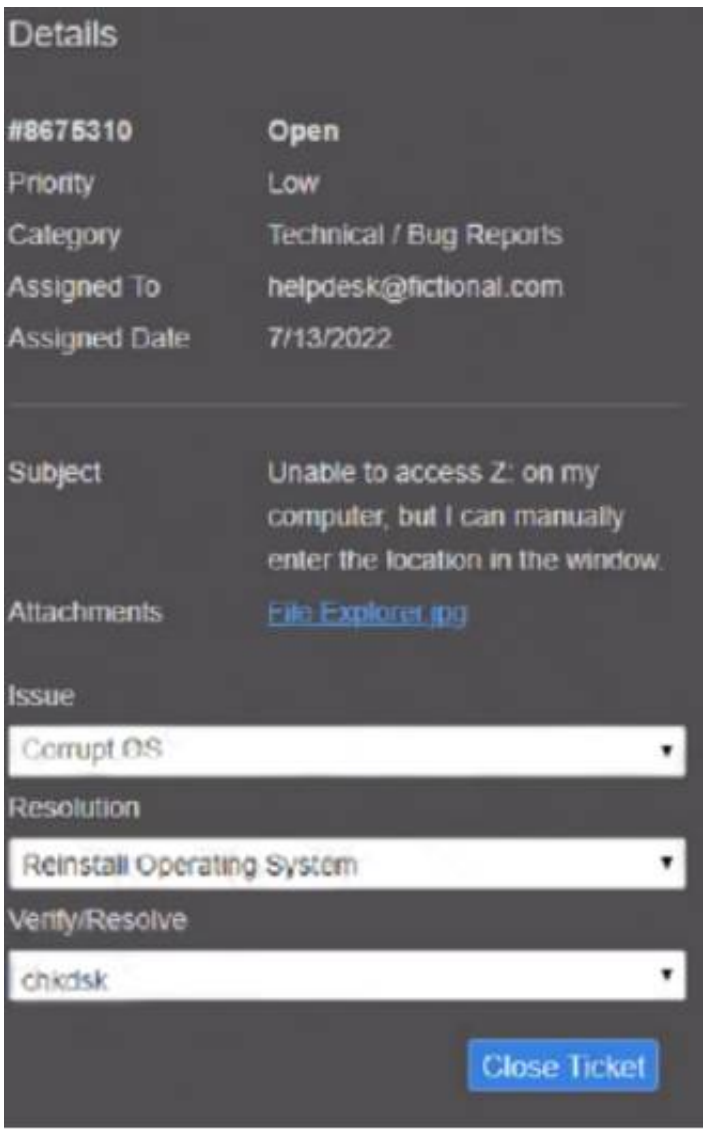




A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, text, application Description automatically generated



NEW QUESTION 134
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 135
A user reports that a PC seems to be running more slowly than usual. A technician checks system resources, but disk, CPU, and memory usage seem to be fine. The technician sees that GPU temperature is extremely high. Which of the following types of malware is MOST likely to blame?

A. Spyware
B. Cryptominer
C. Ransormvare
D. Boot sector virus

Answer: B

Explanation:
The type of malware that is most likely to blame for a PC running more slowly than usual and having an extremely high GPU temperature is a “cryptominer”. Cryptominers are a type of malware that use the resources of a computer to mine cryptocurrency. This can cause the computer to run more slowly than usual and can cause the GPU temperature to rise. Spyware is a type of malware that is used to spy on a user’s activities, but it does not typically cause high GPU temperatures. Ransomware is a type of malware that encrypts a user’s files and demands payment to unlock them, but it does not typically cause high GPU temperatures. Boot sector viruses are a type of malware that infects the boot sector of a hard drive, but they do not typically cause high GPU temperatures12

NEW QUESTION 139
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 Cente1r2
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 1sm2 aller
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 142
Which of the following provide the BEST way to secure physical access to a data cento server room? (Select TWO).

A. Biometric lock
B. Badge reader
C. USB token
D. Video surveillance
E. Locking rack
F. Access control vestibule

Answer: AB

Explanation:
A biometric lock requires an authorized user to provide a unique biometric identifier, such as a fingerprint, in order to gain access to the server room. A badge reader requires an authorized user to swipe an access card in order to gain access. Both of these methods ensure that only authorized personnel are able to access the server room. Additionally, video surveillance and access control vestibules can be used to further secure the server room. Finally, a locking rack can be used to physically secure the servers, so that they cannot be accessed without the appropriate key.

NEW QUESTION 144
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 147
A technician suspects a rootkit has been installed and needs to be removed. Which of the following would BEST resolve the issue?

A. Application updates
B. Anti-malware software
C. OS reinstallation
D. File restore

Answer: C

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

NEW QUESTION 152
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 156
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 157
A customer reported that a home PC with Windows 10 installed in the default configuration is having issues loading applications after a reboot occurred in the middle of the night. Which of the following is the FIRST step in troubleshooting?

A. Install alternate open-source software in place of the applications with issues
B. Run both CPU and memory tests to ensure that all hardware functionality is normal
C. Check for any installed patches and roll them back one at a time until the issue is resolved
D. Reformat the hard drive, and then reinstall the newest Windows 10 release and all applications.

Answer: C

Explanation:
The first step in troubleshooting is to check for any installed patches and roll them back one at a time until the issue is resolved. This can help to identify any patches that may be causing the issue and allow them to be removed.

NEW QUESTION 158
Which of the following change management documents includes how to uninstall a patch?

A. Purpose of change
B. Rollback plan
C. Scope of change
D. Risk analysis

Answer: B

Explanation:
The change management document that includes how to uninstall a patch is called the “rollback plan”. The rollback plan is a document that outlines the steps that should be taken to undo a change that has been made to a system. In the case of a patch, the rollback plan would include instructions on how to uninstall the patch if it causes problems or conflicts with other software12

NEW QUESTION 162
A Windows user reported that a pop-up indicated a security issue. During inspection, an antivirus system identified malware from a recent download, but it was unable to remove the malware. Which of the following actions would be BEST to remove the malware while also preserving the user's files?

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

Answer: C

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

NEW QUESTION 166
A manager reports that staff members often forget the passwords to their mobile devices and applications. Which of the following should the systems administrator do to reduce the number of help desk tickets submitted?

A. Enable multifactor authentication.
B. Increase the failed log-in threshold.
C. Remove complex password requirements.
D. Implement a single sign-on with biometrics.

Answer: A

Explanation:
Multifactor authentication (MFA) is a security measure that requires users to provide multiple pieces of evidence when logging in to an account or system. This can include a combination of something the user knows (e.g. a password or PIN), something the user has (e.g. a security token or smartphone) and something the user is (e.g. biometrics such as a fingerprint or face scan). By enabling MFA, the systems administrator can ensure that users are required to provide multiple pieces of evidence when logging in, making it more difficult for unauthorized users to gain access to the system. This can help reduce the number of help desk tickets submitted due to forgotten passwords.

NEW QUESTION 170
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 172
A technician is setting up a new laptop. The company's security policy states that users cannot install virtual machines. Which of the following should the technician implement to prevent users from enabling virtual technology on their laptops?

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

Answer: B

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

NEW QUESTION 174
Which of the following is MOST likely contained in an EULA?

A. Chain of custody
B. Backup of software code
C. Personally identifiable information
D. Restrictions of use

Answer: D

Explanation:
An EULA (End-User License Agreement) is a legally binding contract between a software supplier and a customer or end-user, generally made available to the customer via a retailer acting as an intermediary. A EULA specifies in detail the rights and restrictions which apply to the use of the software. Some of the main terms included in an EULA are the terms and scope of the license, any licensing fees, warranties and disclaimers, limitation of liability, revocation or termination of the license, and intellectual property information and restrictions on using the license (e.g. modification and copying1)
https://www.termsfeed.com/blog/eula-vs-terms-conditions/

NEW QUESTION 177
A technician is investigating an employee's smartphone that has the following symptoms
• The device is hot even when it is not in use.
•Applications crash, especially when others are launched
• Certain applications, such as GPS, are in portrait mode when they should be in landscape mode
Which of the following can the technician do to MOST likely resolve these issues with minimal impact? (Select TWO).

A. Turn on autorotation
B. Activate airplane mode.
C. Close unnecessary applications
D. Perform a factory reset
E. Update the device's operating system
F. Reinstall the applications that have crashed.

Answer: AC

Explanation:
The technician can close unnecessary applications and turn on autorotation to resolve these issues with minimal impact. Autorotation can help the device to switch between portrait and landscape modes automatically. Closing unnecessary applications can help to free up the device’s memory and reduce the device’s temperature1

NEW QUESTION 178
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
.a pp. This is because .app is the file extension for applications on macO1S.

NEW QUESTION 181
A help desk technician is troubleshooting a workstation in a SOHO environment that is running above normal system baselines. The technician discovers an unknown executable with a random string name running on the system. The technician terminates the process, and the system returns to normal operation. The technician thinks the issue was an infected file, but the antivirus is not detecting a threat. The technician is concerned other machines may be infected with this unknown virus. Which of the following is the MOST effective way to check other machines on the network for this unknown threat?

A. Run a startup script that removes files by name.
B. Provide a sample to the antivirus vendor.
C. Manually check each machine.
D. Monitor outbound network traffic.

Answer: C

Explanation:
The most effective way to check other machines on the network for this unknown threat is to manually check each machine. This can help to identify any other machines that may be infected with the unknown virus and allow them to be cleaned.

NEW QUESTION 184
.....

Relate Links

100% Pass Your 220-1102 Exam with Exambible Prep Materials

https://www.exambible.com/220-1102-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/