

Exam Questions 220-1102

CompTIA A+ Certification Exam: Core 2

<https://www.2passeasy.com/dumps/220-1102/>



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

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

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

Answer: C

Explanation:

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

NEW QUESTION 4

A wireless network is set up, but it is experiencing some interference from other nearby SSIDs. Which of the following can BEST resolve the interference?

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

Answer: A

Explanation:

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

NEW QUESTION 5

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

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

Answer: B

Explanation:

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

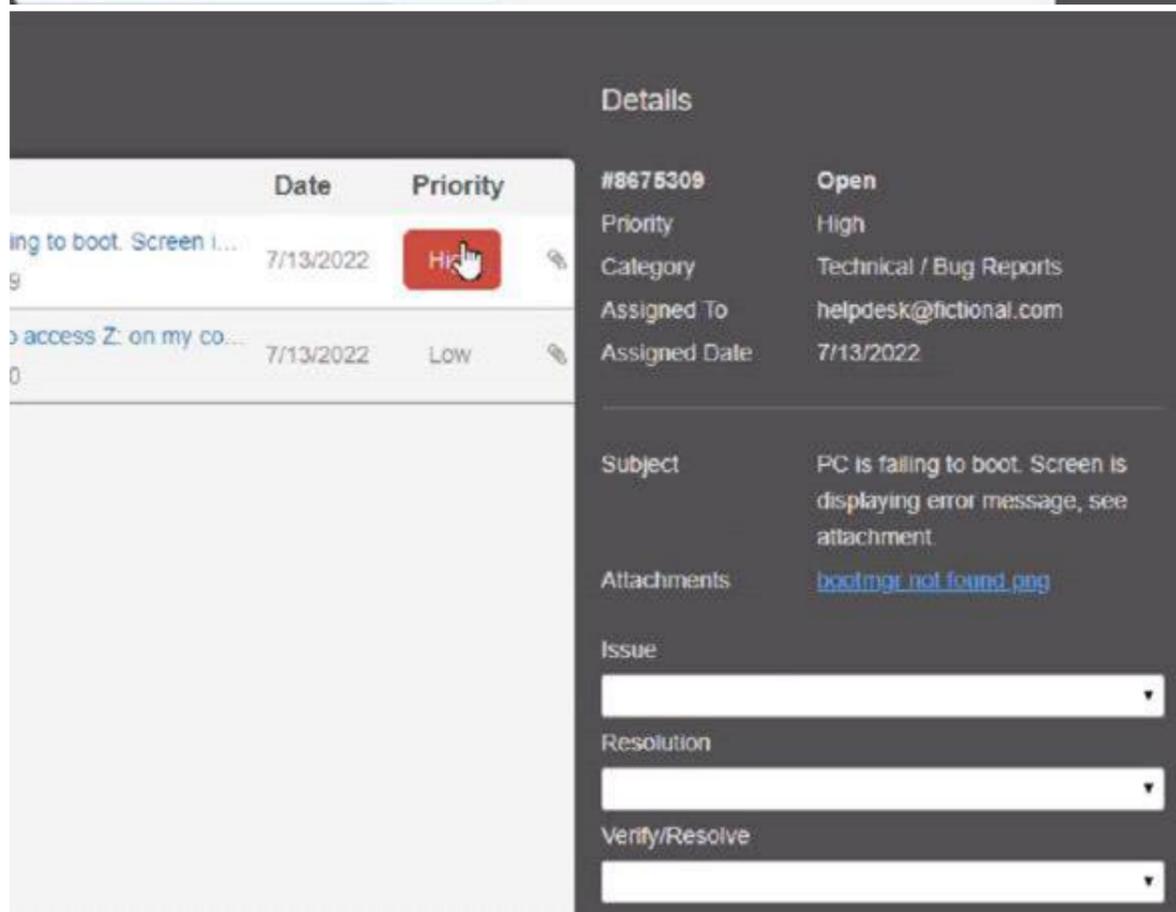
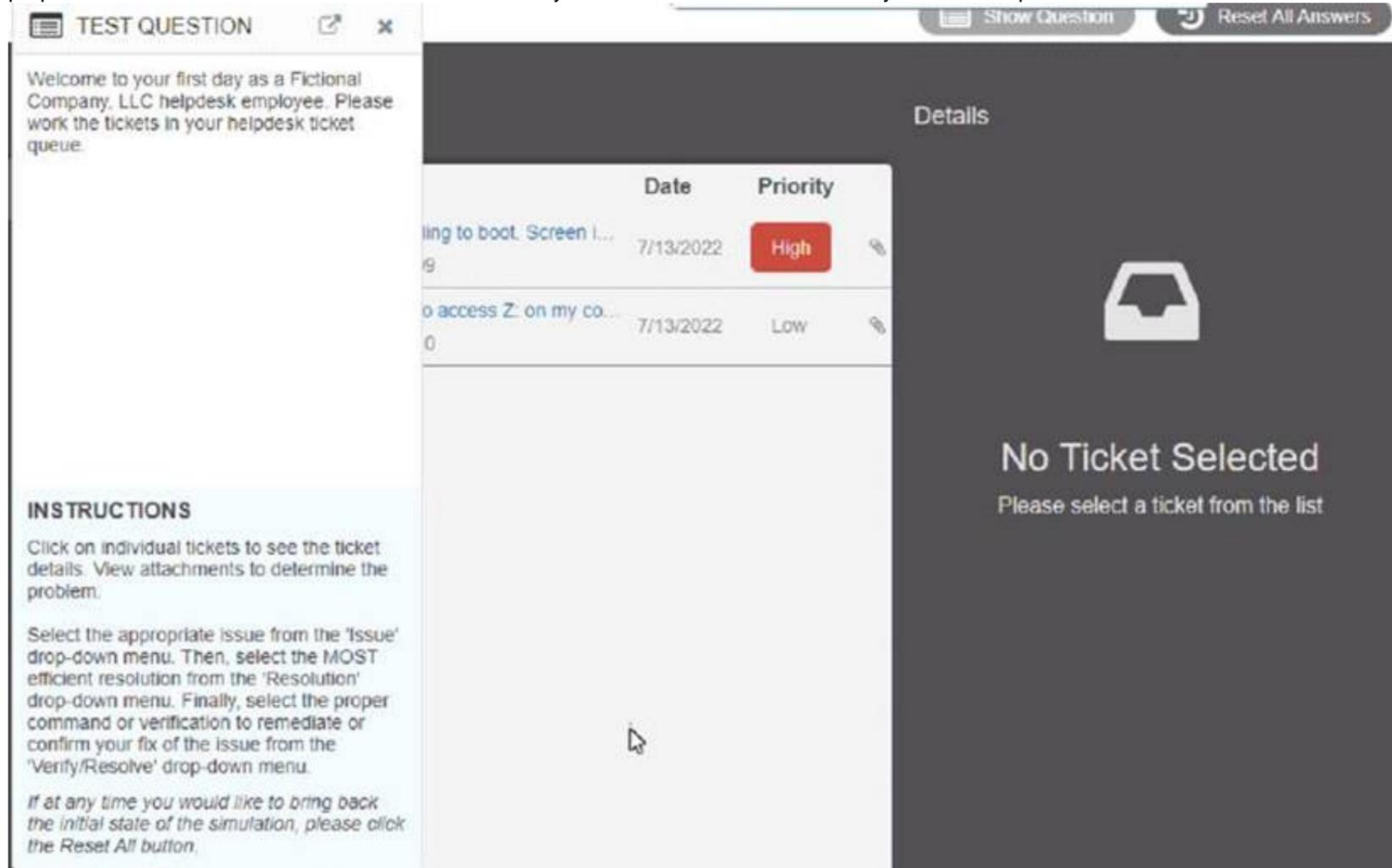
The MOST efficient solution that allows for parallel execution of the Linux application and Windows applications is to install and run Linux and the required application as a virtual machine installed under the Windows OS. This is because it allows you to run both Linux and Windows together without the need to keep the Linux portion confined to a VM window3.

NEW QUESTION 6

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.



The screenshot shows a helpdesk interface. On the left, a table lists tickets with columns for 'Date' and 'Priority'. The first ticket is 'ing to boot. Screen i...' with a 'High' priority. The second is 'access Z: on my co...' with a 'Low' priority. A 'Details' panel for ticket #8675309 is open, showing 'Open' status, 'High' priority, 'Technical / Bug Reports' category, and 'helpdesk@fictional.com' assigned to. The subject is 'PC is failing to boot. Screen is displaying error message, see attachment.' and the attachment is 'bootmgr not found.png'. Below the details, there are two dropdown menus. The first is labeled 'Issue' and is open, showing a list of Windows error messages including 'Corrupt OS', 'Recent Windows Updates', 'Graphics Drive Updates', 'BSOD', 'Printing Issues', 'Limited Network Connectivity', 'Services Failed to Start', 'User Profile is Corrupted', 'Application Crash', 'User cannot access shared resource', and 'URL contains typo'. The second dropdown is labeled 'Resolution' and is also open, showing a list of troubleshooting steps such as 'Reinstall Operating System', 'Rollback Updates', 'Rollback Drivers', 'Repair Application', 'Restart Print Spooler', 'Disable Network Adapter', 'Update Network Drivers', 'Refresh DHCP', 'Rebuild Windows Profile', 'Apply Updates', 'Repair Installation', 'Restore from Recovery Partition', 'Remap network drive', 'Verify integrity of disk drive', 'Initiate screen share session with user', 'Windows recovery environment', and 'Inform user of AUP violation'. Below these, another dropdown labeled 'Verify/Resolve' is open, showing a list of commands: 'chkdsk', 'dism', 'diskpart', 'sfc', 'dd', 'ctrl + alt + del', 'net use', 'net user', 'netstat', 'netsh', and 'bootrec'.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text, application Description automatically generated

Details

#8675309	Open
Priority	High
Category	Technical / Bug Reports
Assigned To	helpdesk@fictional.com
Assigned Date	7/13/2022

Subject: PC is failing to boot. Screen is displaying error message, see attachment

Attachments: [bootmgr not found.png](#)

Issue

Corrupt OS

Resolution

Reinstall Operating System

Verify/Resolve

chkdsk

Close Ticket

NEW QUESTION 7

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 user.

NEW QUESTION 8

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 9

A department has the following technical requirements for a new application:

```
Quad Core processor
250GB of hard drive space
6GB of RAM
Touch screens
```

The company plans to upgrade from a 32-bit Windows OS to a 64-bit OS. Which of the following will the company be able to fully take advantage of after the upgrade?

- A. CPU
- B. Hard drive
- C. RAM
- D. Touch screen

Answer: C

Explanation:

<https://www.makeuseof.com/tag/difference-32-bit-64-bit-windows/>

After upgrading from a 32-bit Windows OS to a 64-bit OS, the company will be able to fully take advantage of the RAM of the computer. This is because a 64-bit operating system is able to use larger amounts of RAM compared to a 32-bit operating system, which may benefit the system's overall performance if it has more than 4GB of RAM installed

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 10

Which of the following is the STRONGEST wireless configuration?

- A. WPS
- B. WPA3
- C. WEP
- D. WMN

Answer: B

Explanation:

The strongest wireless configuration is B. WPA3. WPA3 is the most up-to-date wireless encryption protocol and is the most secure choice. It replaces PSK with SAE, a more secure way to do the initial key exchange. At the same time, the session key size of WPA3 increases to 128-bit in WPA3-Personal mode and 192-bit in WPA3-Enterprise, which makes the password harder to crack than the previous Wi-Fi security standards
<https://www.makeuseof.com/tag/wep-wpa-wpa2-wpa3-explained/>

NEW QUESTION 14

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

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

Answer: D

Explanation:

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

NEW QUESTION 19

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 20

A new service desk is having a difficult time managing the volume of requests. Which of the following is the BEST solution for the department?

- A. Implementing a support portal
- B. Creating a ticketing system
- C. Commissioning an automated callback system
- D. Submitting tickets through email

Answer: A

Explanation:

A support portal is an online system that allows customers to access customer service tools, submit requests and view status updates, as well as access information such as how-to guides, FAQs, and other self-service resources. This would be the best solution for the service desk, as it would allow them to easily manage the volume of requests by allowing customers to submit their own requests and view the status of their requests. Additionally, the portal would provide customers with self-service resources that can help them resolve their own issues, reducing the amount of tickets that need to be handled by the service desk.

NEW QUESTION 24

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

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

Answer: B

Explanation:

If customers are unable to access the company-hosted public website after installing a new SOHO router, the company should check for firmware updates¹. Firmware updates can fix bugs and compatibility issues that may be preventing customers from accessing the website¹. The company should also ensure that the router is properly configured to allow traffic to the website¹. If the router is blocking traffic to the website, the company should configure the router to allow traffic to the website¹.

NEW QUESTION 25

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

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

Answer: B

Explanation:

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

➤ [Configuring AAA Services](https://www.cisco.com/c/en/us/td/docs/routers/crs/software/crs_r4-0/security/configuration/guide/sc40crsb). Retrieved from https://www.cisco.com/c/en/us/td/docs/routers/crs/software/crs_r4-0/security/configuration/guide/sc40crsb

NEW QUESTION 26

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

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

Answer: C

Explanation:

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

NEW QUESTION 31

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

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

Answer: D

Explanation:

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

NEW QUESTION 33

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 37

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 39

A user installed a new application that automatically starts each time the user logs in to a Windows 10 system. The user does not want this to happen and has asked for this setting to be changed. Which of the following tools would the technician MOST likely use to safely make this change?

- A. Registry Editor
- B. Task Manager
- C. Event Viewer
- D. Local Users and Groups

Answer: B

Explanation:

The technician would most likely use the Task Manager tool to safely make this change. The Task Manager tool can be used to disable applications from starting automatically on Windows 10. The tool that a technician would most likely use to stop an application from automatically starting when a user logs in to a Windows 10 system is the Task Manager. The Task Manager can be used to view and manage processes, including those that are set to automatically start when a user logs in to the system.

NEW QUESTION 44

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

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 48

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

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

Answer: D

Explanation:

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

NEW QUESTION 51

In which of the following scenarios would remote wipe capabilities MOST likely be used? (Select TWO).

- A. A new IT policy requires users to set up a lock screen PIN.
- B. A user is overseas and wants to use a compatible international SIM Card.
- C. A user left the phone at home and wants to prevent children from gaining access to the phone.
- D. A user traded in the company phone for a cell carrier upgrade by mistake.
- E. A user cannot locate the phone after attending a play at a theater.
- F. A user forgot the phone in a taxi, and the driver called the company to return the device.

Answer: EF

Explanation:

Remote wipe capabilities are used to erase all data on a mobile device remotely. This can be useful in situations where a device is lost or stolen, or when sensitive data needs to be removed from a device. Remote wipe capabilities are most likely to be used in the following scenarios:

- E. A user cannot locate the phone after attending a play at a theater.
 - F. A user forgot the phone in a taxi, and the driver called the company to return the device
- In scenario E, remote wipe capabilities would be used to prevent unauthorized access to the device and to protect sensitive data. In scenario F, remote wipe capabilities would be used to erase all data on the device before it is returned to the user.

NEW QUESTION 54

A user is being directed by the help desk to look up a Windows PC's network name so the help desk can use a remote administration tool to assist the user. Which of the following commands would allow the user to give the technician the correct information? (Select TWO).

- A. ipconfig /all
- B. hostname
- C. netstat /?
- D. nslookup localhost
- E. arp -a
- F. ping :: 1

Answer: AB

Explanation:

The user can use the following commands to give the technician the correct information: ipconfig /all and hostname

The ipconfig /all command displays the IP address, subnet mask, and default gateway all adapters on the computer. The hostname command displays the name of the computer.

NEW QUESTION 58

Sensitive data was leaked from a user's smartphone. A technician discovered an unapproved application was installed, and the user has full access to the device's command shell. Which of the following is the NEXT step the technician should take to find the cause of the leaked data?

- A. Restore the device to factory settings.
- B. Uninstall the unapproved application.
- C. Disable the ability to install applications from unknown sources.
- D. Ensure the device is connected to the corporate WiFi network.

Answer: B

Explanation:

The technician should disable the user's access to the device's command shell. This will prevent the user from accessing sensitive data and will help to prevent further data leaks. The technician should then investigate the unapproved application to determine if it is the cause of the data leak. If the application is found to be the cause of the leak, the technician should uninstall the application and restore the device to factory settings. If the application is not the cause of the leak, the technician should investigate further to determine the cause of the leak. Disabling the ability to install applications from unknown sources can help to prevent future data leaks, but it is not the next step the technician should take in this scenario. Ensuring the device is connected to the corporate WiFi network is not relevant to this scenario.

NEW QUESTION 60

A technician has verified that a user's computer has a virus, and the antivirus software is out of date. Which of the following steps should the technician take NEXT?

- A. Quarantine the computer.
- B. Use a previous restore point.

- C. Educate the end user about viruses
- D. Download the latest virus definitions

Answer: D

Explanation:

This will ensure that the antivirus software is up-to-date, and can detect any new viruses that may have been released since the last virus definition update. The CompTIA A+ Core 2 220-1002 exam covers this topic in the following domains: 1.3 Explain the importance of security awareness and 2.2 Given a scenario, use secure data management and disaster recovery principles.

NEW QUESTION 63

A company has just refreshed several desktop PCs. The hard drives contain PII. Which of the following is the BEST method to dispose of the drives?

- A. Drilling
- B. Degaussing
- C. Low-level formatting
- D. Erasing/wiping

Answer: D

Explanation:

Erasing/wiping the hard drives is the best method to dispose of the drives containing PII

NEW QUESTION 67

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 environment.

NEW QUESTION 70

A technician is asked to resize a partition on the internal storage drive of a computer running macOS. Which of the following tools should the technician use to accomplish this task?

- A. Console
- B. Disk Utility
- C. Time Machine
- D. FileVault

Answer: B

Explanation:

The technician should use Disk Utility to resize a partition on the internal storage drive of a computer running macOS. Disk Utility is a built-in utility that allows users to manage disks, partitions, and volumes on a Mac. It can be used to resize, create, and delete partitions, as well as to format disks and volumes.

NEW QUESTION 73

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 cleanmgr 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 74

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

NEW QUESTION 75

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

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

Answer: A

Explanation:

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

NEW QUESTION 80

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

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

Answer: C

Explanation:

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

NEW QUESTION 85

Which of the following is a consequence of end-of-life 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 87

A company is issuing smartphones to employees and needs to ensure data is secure if the devices are lost or stolen. Which of the following provides the BEST solution?

- A. Anti-malware
- B. Remote wipe
- C. Locator applications
- D. Screen lock

Answer: B

Explanation:

This is because remote wipe allows the data on the smartphone to be erased remotely, which helps to ensure that sensitive data does not fall into the wrong hands.

NEW QUESTION 88

A user calls the help desk to report potential malware on a computer. The anomalous activity began after the user clicked a link to a free gift card in a recent email. The technician asks the user to describe any unusual activity, such as slow performance, excessive pop-ups, and browser redirections. Which of the following

should the technician do NEXT?

- A. Advise the user to run a complete system scan using the OS anti-malware application
- B. Guide the user to reboot the machine into safe mode and verify whether the anomalous activities are still present
- C. Have the user check for recently installed applications and outline those installed since the link in the email was clicked
- D. Instruct the user to disconnect the Ethernet connection to the corporate network.

Answer: D

Explanation:

First thing you want to do is quarantine/disconnect the affected system from the network so whatever malicious software doesn't spread.

NEW QUESTION 92

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 (2FA)2

NEW QUESTION 94

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 99

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 percentage12 3

NEW QUESTION 103

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

- A. 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 107

A user reports a computer is running slow. Which of the following tools will help a technician identify the issued

- A. Disk Cleanup
- B. Group Policy Editor
- C. Disk Management

D. Resource Monitor

Answer: D

Explanation:

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

NEW QUESTION 112

A suite of security applications was installed a few days ago on a user's home computer. The user reports that the computer has been running slowly since the installation. The user notices the hard drive activity light is constantly solid. Which of the following should be checked FIRST?

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

Answer: C

Explanation:

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

NEW QUESTION 116

A technician is installing a new business application on a user's desktop computer. The machine is running Windows 10 Enterprise 32-bit operating system. Which of the following files should the technician execute in order to complete the installation?

- A. Installer_x64.exe
- B. Installer_Files.zip
- C. Installer_32.msi
- D. Installer_x86.exe
- E. Installer_Win10Enterprise.dmg

Answer: D

Explanation:

The 32-bit operating system can only run 32-bit applications, so the technician should execute the 32-bit installer. The "x86" in the file name refers to the 32-bit architecture.

<https://www.digitaltrends.com/computing/32-bit-vs-64-bit-operating-systems/>

NEW QUESTION 120

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

The image shows a drag-and-drop interface for connecting devices to power sources. It consists of three main columns: 'Wall Outlet', 'Surge Protector', and 'UPS'. Each column has a 'Power Source' dropdown menu at the top. Below the dropdowns are vertical lists of question marks representing devices. To the right is a 'Drag & Drop' panel with a blue header and a list of device icons: Cable Modem, Computer, Monitor, Printer, and Scanner.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 125

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 130

A technician is configuring a new Windows laptop Corporate policy requires that mobile devices make use of full disk encryption at all times Which of the following encryption solutions should the technician choose?

- A. Encrypting File System
- B. FileVault
- C. BitLocker
- D. Encrypted LVM

Answer: A

Explanation:

The encryption solution that the technician should choose when configuring a new Windows laptop and corporate policy requires that mobile devices make use of full disk encryption at all times is BitLocker. This is because BitLocker is a full-disk encryption feature that encrypts all data on a hard drive and is included with Windows

NEW QUESTION 132

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 133

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 138

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

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

Answer: AE

Explanation:

The correct answers are E. Windows Defender and A. File Explorer. Windows Defender is a built-in antivirus program that can detect and remove malicious software from a workstation. File Explorer can be used to locate and delete files associated with the malicious software¹

NEW QUESTION 143

A Microsoft Windows PC needs to be set up for a user at a target 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 146

Which of the following must be maintained throughout the forensic evidence life cycle when dealing with a piece of evidence?

- A. Acceptable use
- B. Chain of custody
- C. Security policy
- D. Information management

Answer: B

Explanation:

The aspect of forensic evidence life cycle that must be maintained when dealing with a piece of evidence is chain of custody. This is because chain of custody is the documentation of the movement of evidence from the time it is collected to the time it is presented in court, and it is important to maintain the integrity of the evidence

NEW QUESTION 149

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

- A. yum
- B. grep
- C. ls
- D. sudo

Answer: D

Explanation:

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

NEW QUESTION 151

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

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

Answer: B

Explanation:

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

NEW QUESTION 155

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

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

Answer: B

Explanation:

Processes tab in Task Manager would contain the information a technician would use to identify the cause of this issue. The Processes tab in Task Manager displays all the processes running on the computer, including the CPU and memory usage of each process. The technician can use this tab to identify the process that is causing the hard drive activity light to remain lit and the performance degradation¹

NEW QUESTION 158

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

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

Answer: B

Explanation:

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

Shutting down the infected computer and swapping it with another computer is not necessary at this point¹² The technician should not immediately assume that the message is legitimate or perform any actions without knowing what the interface is and what triggered it to pop up. It is important to investigate the issue further, including checking the legitimacy of the antivirus program and the message it is displaying.

NEW QUESTION 163

A systems administrator needs to reset a user's password because the user forgot it. The systems administrator creates the new password and wants to further protect the user's account. Which of the following should the systems administrator do?

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

Answer: A

Explanation:

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

NEW QUESTION 164

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

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

Answer: B

Explanation:

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

NEW QUESTION 168

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 170

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 173

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 edition1s. 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 175

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 177

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 178

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 182

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

- A. afc
- B. ehkdsd

- C. git clone
- D. zobocopy

Answer: A

Explanation:

The technician should use afc to transfer a large number of files over an unreliable connection and be able to resume the process if the connection is interrupted1

NEW QUESTION 185

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 186

A technician is setting up a SOHO wireless router. The router is about ten years old. The customer would like the most secure wireless network possible. Which of the following should the technician configure?

- A. WPA2 with TKIP
- B. WPA2 with AES
- C. WPA3withAES-256
- D. WPA3 with AES-128

Answer: B

Explanation:

This is because WPA2 with AES is the most secure wireless network configuration that is available on a ten-year-old SOHO wireless router.

NEW QUESTION 190

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 195

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 200

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

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

Answer: B

Explanation:

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

NEW QUESTION 204

A user is unable to use any internet-related functions on a smartphone when it is not connected to Wi-Fi. When the smartphone is connected to Wi-Fi, the user can browse the internet and send and receive email. The user is also able to send and receive text messages and phone calls when the smartphone is not connected to Wi-Fi. Which of the following is the MOST likely reason the user is unable to use the internet on the smartphone when it is not connected to Wi-Fi?

- A. The smartphone's line was not provisioned with a data plan
- B. The smartphone's SIM card has failed
- C. The smartphone's Bluetooth radio is disabled.
- D. The smartphone has too many applications open

Answer: A

Explanation:

The smartphone's line was not provisioned with a data plan. The user is unable to use any internet-related functions on the smartphone when it is not connected to Wi-Fi because the smartphone's line was not provisioned with a data plan. The user can send and receive text messages and phone calls when the smartphone is not connected to Wi-Fi because these functions do not require an internet connection.

NEW QUESTION 209

A technician found that an employee is mining cryptocurrency on a work desktop. The company has decided that this action violates its guidelines. Which of the following should be updated to reflect this new requirement?

- A. MDM
- B. EULA
- C. IRP
- D. AUP

Answer: D

Explanation:

AUP (Acceptable Use Policy) should be updated to reflect this new requirement. The AUP is a document that outlines the acceptable use of technology within an organization. It is a set of rules that employees must follow when using company resources. The AUP should be updated to include a policy on cryptocurrency mining on work desktops.

NEW QUESTION 212

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 220-1102 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 220-1102 Product From:

<https://www.2passeasy.com/dumps/220-1102/>

Money Back Guarantee

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