

CompTIA.220-1102.v2023-05-24.q77

Exam Code:	220-1102
Exam Name:	CompTIA A+ Certification Exam: Core 2
Certification Provider:	CompTIA
Free Question Number:	77
Version:	v2023-05-24
# of views:	1174
# of Questions views:	770
https://www.freepdfdumps.com/CompTIA.220-1102.v2023-05-24.q77.html	

NEW QUESTION: 1

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

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

Answer: D (LEAVE A REPLY)

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

NEW QUESTION: 2

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

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

Answer: (SHOW ANSWER)

The feature that BEST addresses the user's concern is remote wipe. This is because remote wipe allows the user to erase all data on the mobile device if it is lost or stolen, which will prevent unauthorized access to the device1.

NEW QUESTION: 3

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: A,E (LEAVE A REPLY)

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: 4

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 (LEAVE A REPLY)

Account lockout would best mitigate the threat of a dictionary attack¹

NEW QUESTION: 5

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: (SHOW ANSWER)

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: 6

Upon downloading a new ISO, an administrator is presented with the following string:

59d15a16ce90cBcc97fa7c211b767aB

Which of the following BEST describes the purpose of this string?

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

Answer: C (LEAVE A REPLY)

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

NEW QUESTION: 7

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

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

Answer: A (LEAVE A REPLY)

[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: 8

A user corrects a laptop that is running Windows 10 to a docking station with external monitors when working at a desk. The user would like to close the laptop when it is docked, but the user reports it goes to sleep when it is closed. Which of the following is the BEST solution to prevent the laptop from going to sleep when it is closed and on the docking station?

- A. Within the Power Options of the Control Panel utility click the Change Plan Settings button for the enabled power plan and select Put the Computer to Sleep under the Plugged In category to Never
- B. Within the Power Options of the Control Panel utility, click the Change Plan Settings button for the enabled power plan and select Put the Computer to Sleep under the On Battery category to Never
- C. Within the Power Options of the Control Panel utility select the option Choose When to Turn Off the Display and select Turn Off the Display under the Plugged In category to Never
- D. Within the Power Options of the Control Panel utility, select the option Choose What Closing the Lid Does and select When I Close the Lid under the Plugged in category to Do Nothing

Answer: D (LEAVE A REPLY)

The laptop has an additional option under power and sleep settings that desktops do not have. Switching to do nothing prevents the screen from turning off when closed.

NEW QUESTION: 9

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: (SHOW ANSWER)

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: 10

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 (LEAVE A REPLY)

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

NEW QUESTION: 11

Which of the following is the STRONGEST wireless configuration?

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

Answer: B (LEAVE A REPLY)

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: 12

While assisting a customer with an issue, a support representative realizes the appointment is taking longer than expected and will cause the next customer meeting to be delayed by five minutes. Which of the following should the support representative do NEXT?

- A. Send a quick message regarding the delay to the next customer.
- B. Cut the current customer's time short and rush to the next customer.
- C. Apologize to the next customer when arriving late.
- D. Arrive late to the next meeting without acknowledging the time.

Answer: A (LEAVE A REPLY)

The support representative should send a quick message regarding the delay to the next customer. This will help the next customer understand the situation and adjust their schedule accordingly.

NEW QUESTION: 13

A user receives a notification indicating the antivirus protection on a company laptop is out of date. A technician is able to ping the user's laptop. The technician checks the antivirus parent servers and sees the latest signatures have been

installed. The technician then checks the user's laptop and finds the antivirus engine and definitions are current. Which of the following has MOST likely occurred?

- A. Ransomware
- B. Failed OS updates
- C. Adware
- D. Missing system files

Answer: B (LEAVE A REPLY)

The most likely reason for the antivirus protection on a company laptop being out of date is failed OS updates¹. Antivirus software relies on the operating system to function properly. If the operating system is not up-to-date, the antivirus software may not function properly and may not be able to receive the latest virus definitions and updates². Therefore, it is important to keep the operating system up-to-date to ensure the antivirus software is functioning properly².

NEW QUESTION: 14

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 off-site in cold storage
- D. Weekly, differential backups that are stored in a cloud-hosting provider

Answer: C (LEAVE A REPLY)

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: 15

A technician is unable to join a Windows 10 laptop to a domain. Which of the following is the MOST likely reason?

- A. The domain's processor compatibility is not met
- B. The laptop has Windows 10 Home installed
- C. The laptop does not have an onboard Ethernet adapter
- D. The Laptop does not have all current Windows updates installed

Answer: (SHOW ANSWER)

[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: 16

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 (LEAVE A REPLY)

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

Valid 220-1102 Dumps shared by Actual4test.com for Helping Passing 220-1102 Exam! Actual4test.com now offer the **newest 220-1102 exam dumps**, the Actual4test.com 220-1102 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com 220-1102 dumps with Test Engine here:

https://www.actual4test.com/220-1102_examcollection.html (845 Q&As Dumps, **30%OFF Special Discount:**

Freepdfdumps)

NEW QUESTION: 17

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 (LEAVE A REPLY)

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: 18

A technician downloaded software from the Internet that required the technician to scroll through a text box and at the end of the text box, click a button labeled Accept Which of the following agreements IS MOST likely in use?

A. DRM

B. NDA

C. EULA

D. MOU

Answer: C (LEAVE A REPLY)

The most likely agreement in use here is a EULA (End User License Agreement). This is a legally binding agreement between the user and the software developer, outlining the terms and conditions that the user must agree to in order to use the software. It is important that the user understands and agrees to the EULA before they can proceed with

downloading and installing the software. As stated in the CompTIA A+ Core 2 exam objectives, users should be aware of the EULA before downloading any software.

NEW QUESTION: 19

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 (LEAVE A REPLY)

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

NEW QUESTION: 20

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 (LEAVE A REPLY)

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: 21

A network administrator is deploying a client certificate to be used for Wi-Fi access for all devices in 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: (SHOW ANSWER)

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 Reference:

CompTIA Security+ (Plus) Practice Test Questions | CompTIA. Retrieved from <https://www.comptia.org/training/resources/comptia-security-practice-tests>

NEW QUESTION: 22

A technician is installing new network equipment in a SOHO and wants to ensure the equipment is secured against external threats on the Internet. Which of the following actions should the technician do FIRST?

- A. Lock all devices in a closet.
- B. Ensure all devices are from the same manufacturer.
- C. Change the default administrative password.
- D. Install the latest operating system and patches

Answer: C (LEAVE A REPLY)

The technician should change the default administrative password FIRST to ensure the network equipment is secured against external threats on the Internet. Changing the default administrative password is a basic security measure that can help prevent unauthorized access to the network equipment. Locking all devices in a closet is a physical security measure that can help prevent theft or damage to the devices, but it does not address external threats on the Internet. Ensuring all devices are from the same manufacturer is not a security measure and does not address external threats on the Internet. Installing the latest operating system and patches is important for maintaining the security of the network equipment, but it is not the first action the technician should take¹

NEW QUESTION: 23

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

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

Answer: C (LEAVE A REPLY)

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

NEW QUESTION: 24

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 (LEAVE A REPLY)

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: 25

A technician just completed a Windows 10 installation on a PC that has a total of 16GB of RAM. The technician notices the Windows OS has only 4GB of RAM available for use. Which of the following explains why the OS can only access 4GB of RAM?

- A. The UEFI settings need to be changed.
- B. The RAM has compatibility issues with Windows 10.
- C. Some of the RAM is defective.
- D. The newly installed OS is x86.

Answer: ([SHOW ANSWER](#))

The newly installed OS is x86. The x86 version of Windows 10 can only use up to 4GB of RAM. The x64 version of Windows 10 can use up to 2TB of RAM.

NEW QUESTION: 26

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.

Details

#8675310 **Open**
Priority Low
Category Technical / Bug Reports
Assigned To helpdesk@fictional.com
Assigned Date 7/13/2022

Subject Unable to access Z: on my
computer, but I can manually
enter the location in the window.

Attachments [File Explorer.jpg](#)

Issue

Resolution

Verify/Resolve

Close Ticket

TEST QUESTION

Welcome to your first day as a Fictional Company, LLC helpdesk employee. Please work the tickets in your helpdesk ticket queue.

	Date	Priority
Unable to boot. Screen I...	7/13/2022	High
Unable to access Z: on my co...	7/13/2022	Low

INSTRUCTIONS

Click on individual tickets 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.

At any time you would like to bring back the initial state of the simulation, please click the 'Reset All' button.

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
URL contains typo

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
Inform user of AUP violation

Verify/Resolve

chkdsk
dism
diskpart
sfc
dd
ctrl + alt + del
net use
net user
netstat
netsh
bootrec

Answer:

Welcome to your first day as a Fictional Company, LLC helpdesk employee. Please work the tickets in your helpdesk ticket queue.

	Date	Priority
ling to boot. Screen I...	7/13/2022	High
o access Z: on my co...	7/13/2022	Low

INSTRUCTIONS

Click on individual tickets 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.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

- 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
- URL contains typo

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
- Inform user of AUP violation

Resolution

chkdsk

Verify/Resolve

- dism
- diskpart
- sfc
- dd
- ctrl + alt + del
- net use
- net user
- netstat
- netsh
- bootrec

freepdfdumps.com

CompTIA

Details

#8675310 **Open**

Priority Low

Category Technical / Bug Reports

Assigned To helpdesk@fictional.com

Assigned Date 7/13/2022

CompTIA

Subject Unable to access Z: on my computer, but I can manually enter the location in the window.

Attachments [File Explorer.jpg](#)

Issue

Corrupt OS ▼

Resolution

Reinstall Operating System ▼

Verify/Resolve

chkdsk ▼

[Close Ticket](#)

NEW QUESTION: 27

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 (LEAVE A REPLY)

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: 28

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

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

Answer: C (LEAVE A REPLY)

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

NEW QUESTION: 29

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. SOL injection
- C. Cross-site scripting
- D. Distributed denial of service

Answer: D (LEAVE A REPLY)

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: 30

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 (LEAVE A REPLY)

A zero-day attack is an attack that exploits a previously unknown vulnerability in a computer application, meaning that the attack occurs on "day zero" of awareness of the vulnerability Configuring AAA Services. Retrieved from https://www.cisco.com/c/en/us/td/docs/routers/crs/software/crs_r4-0/security/configuration/guide/sc40crsbook_chapter1.html

NEW QUESTION: 31

A junior administrator is responsible for deploying software to a large group of computers in an organization. The administrator finds a script on a popular coding website to automate this distribution but does not understand the scripting language. Which of the following BEST describes the risks in running this script?

- A. The instructions from the software company are not being followed.
- B. Security controls will treat automated deployments as malware.

- C. The deployment script is performing unknown actions.
- D. Copying scripts off the internet is considered plagiarism.

Answer: C (LEAVE A REPLY)

The risks in running this script are that the deployment script is performing unknown actions. Running the script blindly could cause unintended actions, such as deploying malware or deleting important files, which could negatively impact the organization's network and data1.

Valid 220-1102 Dumps shared by Actual4test.com for Helping Passing 220-1102 Exam! Actual4test.com now offer the **newest 220-1102 exam dumps**, the Actual4test.com 220-1102 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com 220-1102 dumps with Test Engine here:
https://www.actual4test.com/220-1102_examcollection.html (845 Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)

NEW QUESTION: 32

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

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

Answer: A (LEAVE A REPLY)

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: 33

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: (SHOW ANSWER)

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: 34

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: (SHOW ANSWER)

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: 35

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 (LEAVE A REPLY)

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 capabilities.

NEW QUESTION: 36

Someone who is fraudulently claiming to be from a reputable bank calls a company employee. Which of the following describes this incident?

- A. Pretexting
- B. Spoofing
- C. Vishing
- D. Scareware

Answer: C (LEAVE A REPLY)

Vishing is a type of social engineering attack where a fraudulent caller impersonates a legitimate entity, such as a bank or financial institution, in order to gain access to sensitive information. The caller will typically use a variety of techniques, such as trying to scare the target or providing false information, in order to get the target to provide the information they are after. Vishing is often used to gain access to usernames, passwords, bank account information, and other sensitive data.

NEW QUESTION: 37

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 (LEAVE A REPLY)

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

NEW QUESTION: 38

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 (LEAVE A REPLY)

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: 39

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.



Answer:



NEW QUESTION: 40

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 (LEAVE A REPLY)

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: 41

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 simulation interface. On the left, there is a 'TEST QUESTION' window with instructions. The main area displays a list of tickets and a details view for a selected ticket.

TEST QUESTION

Welcome to your first day as a Fictional Company, LLC helpdesk employee. Please work the tickets in your helpdesk ticket queue.

INSTRUCTIONS

Click on individual tickets 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.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Ticket List:

	Date	Priority	
ing to boot. Screen i... 9	7/13/2022	High	
o access Z: on my co... 0	7/13/2022	Low	

Ticket 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: [bootmsg_not_loaded.png](#)

Issue: [Dropdown menu]

Resolution: [Dropdown menu]

Verify/Resolve: [Dropdown menu]

Details

Date	Priority
7/13/2022	High
7/13/2022	Low

#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

Resolution

- 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
- URL contains typo
- 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
- Inform user of AUP violation

Verify/Resolve

- chkdsk
- dism
- diskpart
- sfc
- dd
- ctrl + alt + del
- net use
- net user

```
netstat
netsh
bootrec
```

Answer:

Date	Priority	Details
ing to boot. Screen i...	7/13/2022	High
access Z: on my co...	7/13/2022	Low

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:

Resolution:

Verify/Resolve:

freepdfdumps.com

CompTIA

```
diskpart
sfc
dd
ctrl + alt + del
net use
net user
netstat
netsh
bootrec
```

NEW QUESTION: 42

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: ([SHOW ANSWER](#))

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

NEW QUESTION: 43

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: ([SHOW ANSWER](#))

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: 44

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. msmf32.exe

Answer: C (LEAVE A REPLY)

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

NEW QUESTION: 45

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. Service set identifier**
- D. Default passwords

Answer: C (LEAVE A REPLY)

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

NEW QUESTION: 46

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 (LEAVE A REPLY)

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.

Valid 220-1102 Dumps shared by Actual4test.com for Helping Passing 220-1102 Exam! Actual4test.com now offer the **newest 220-1102 exam dumps**, the Actual4test.com 220-1102 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com 220-1102 dumps with Test Engine here:

https://www.actual4test.com/220-1102_examcollection.html (845 Q&As Dumps, **30%OFF Special Discount:**

Freepdfdumps)

NEW QUESTION: 47

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: (SHOW ANSWER)

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

NEW QUESTION: 48

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 (LEAVE A REPLY)

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: 49

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 (LEAVE A REPLY)

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

NEW QUESTION: 50

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

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

Answer: (SHOW ANSWER)

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

NEW QUESTION: 51

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

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

Answer: D (LEAVE A REPLY)

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

NEW QUESTION: 52

A new spam gateway was recently deployed at a small business. However, users still occasionally receive spam. The management team is concerned that users will open the messages and potentially infect the network systems. Which of the following is the MOST effective method for dealing with this issue?

- A. Adjusting the spam gateway
- B. Updating firmware for the spam appliance
- C. Adjusting AV settings
- D. Providing user training

Answer: (SHOW ANSWER)

The most effective method for dealing with spam messages in a small business is to provide user training¹. Users should be trained to recognize spam messages and avoid opening them¹. They should also be trained to report spam messages to the IT department so that appropriate action can be taken¹. In addition, users should be trained to avoid clicking on links or downloading attachments from unknown sources¹. By providing user training, the management team can reduce the risk of users opening spam messages and potentially infecting the network systems¹.

NEW QUESTION: 53

A user connected a laptop to a wireless network and was tricked into providing login credentials for a website. Which of the following threats was used to carry out the attack?

- A. Zero day
- B. Vishing
- C. DDoS
- D. Evil twin

Answer: B (LEAVE A REPLY)

Vishing, also known as voice phishing, is a type of social engineering attack where the attacker tricks the victim into divulging sensitive information over the phone. In this case, the attacker tricked the user into providing login credentials for a website.

NEW QUESTION: 54

A technician connects an additional monitor to a PC using a USB port. The original HDMI monitor is mounted to the left of the new monitor. When moving the mouse to the right from the original monitor to the new monitor, the mouse stops at the end of the screen on the original monitor. Which of the following will allow the mouse to correctly move to the new monitor?

- A. Rearranging the monitor's position in display settings
- B. Swapping the cables for the monitors
- C. Using the Ctrl+Alt+> to correct the display orientation
- D. Updating the display drivers for the video card

Answer: B (LEAVE A REPLY)

The correct answer is B. Swapping the cables for the monitors. When the second monitor is connected with the HDMI port, it is necessary to swap the cables for the monitors so that the mouse can move from the original monitor to the new monitor. This is because the HDMI port is designed to only support one monitor, and the mouse will not be able to move from one to the other without the cables being swapped.

According to CompTIA A+ Core 2 documents, "When connecting multiple displays to a system, the cables used to connect the displays must be swapped between the displays. For example, if a monitor is connected to a system using a VGA cable, the VGA cable must be moved to the next display to allow the mouse to move between the two displays."

NEW QUESTION: 55

Which of the following is a proprietary Cisco AAA protocol?

- A. TKIP
- B. AES
- C. RADIUS
- D. TACACS+

Answer: D (LEAVE A REPLY)

TACACS+ is a proprietary Cisco AAA protocol

NEW QUESTION: 56

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

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

Answer: C (LEAVE A REPLY)

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

NEW QUESTION: 57

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

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

Answer: A (LEAVE A REPLY)

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: 58

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 (LEAVE A REPLY)

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: 59

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

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

Answer: C (LEAVE A REPLY)

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

NEW QUESTION: 60

A user created a file on a shared drive and wants to prevent its data from being accidentally deleted by others. Which of the following applications should the technician use to assist the user with hiding the file?

- A. Device Manager
- B. Indexing Options
- C. File Explorer

D. Administrative Tools

Answer: C (LEAVE A REPLY)

The technician should use the File Explorer application to assist the user with hiding the file 1. The user can right-click the file and select Properties. In the Properties dialog box, select the Hidden check box, and then click OK 1.

NEW QUESTION: 61

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: (SHOW ANSWER)

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.

Valid 220-1102 Dumps shared by Actual4test.com for Helping Passing 220-1102 Exam! Actual4test.com now offer the **newest 220-1102 exam dumps**, the Actual4test.com 220-1102 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com 220-1102 dumps with Test Engine here:
https://www.actual4test.com/220-1102_examcollection.html (845 Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)

NEW QUESTION: 62

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: (SHOW ANSWER)

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

NEW QUESTION: 63

A user's mobile phone has become sluggish A systems administrator discovered several malicious applications on the device and reset the phone. The administrator installed MDM software. Which of the following should the administrator do

to help secure the device against this threat in the future? (Select TWO).

- A. Prevent a device root
- B. Disable biometric authentication
- C. Require a PIN on the unlock screen
- D. Enable developer mode
- E. Block a third-party application installation
- F. Prevent GPS spoofing

Answer: C,E (LEAVE A REPLY)

To help secure the device against this threat in the future, the administrator should require a PIN on the unlock screen and block a third-party application installation. Requiring a PIN on the unlock screen can help to prevent unauthorized access to the device, while blocking third-party application installation can help to prevent malicious applications from being installed on the device.

NEW QUESTION: 64

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

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

Answer: B (LEAVE A REPLY)

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

NEW QUESTION: 65

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: (SHOW ANSWER)

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

NEW QUESTION: 66

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 (LEAVE A REPLY)

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: 67

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 (LEAVE A REPLY)

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 copying)¹

<https://www.termsfeed.com/blog/eula-vs-terms-conditions/>

NEW QUESTION: 68

Which of the following is a data security standard for protecting credit cards?

- A. PHI
- B. NIST
- C. PCI
- D. GDPR

Answer: C (LEAVE A REPLY)

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that ALL companies that accept, process, store or transmit credit card information maintain a secure environment.

NEW QUESTION: 69

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

- A. Uninstall and reinstall the application
- B. Reset the phone to factory settings
- C. Install an alternative application with similar functionality
- D. Clear the application cache.

Answer: (SHOW ANSWER)

The systems administrator should clear the application cache¹²

If clearing the application cache does not work, the systems administrator should uninstall and reinstall the application¹²

Resetting the phone to factory settings is not necessary at this point¹² Installing an alternative application with similar functionality is not necessary at this point¹²

NEW QUESTION: 70

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 (LEAVE A REPLY)

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: 71

Which of the following OS types provides a lightweight option for workstations that need an easy-to-use browser-based interface?

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

Answer: B (LEAVE A REPLY)

Chrome OS provides a lightweight option for workstations that need an easy-to-use browser-based interface¹

NEW QUESTION: 72

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 (LEAVE A REPLY)

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

NEW QUESTION: 73

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 (LEAVE A REPLY)

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: 74

A user reports a PC is running slowly. The technician suspects high disk I/O. Which of the following should the technician perform NEXT?

- A. resmon_exe
- B. dfrgui_exe
- C. msinf032exe
- D. msconfig_exe

Answer: (SHOW ANSWER)

If a technician suspects high disk I/O, the technician should use the Resource Monitor (resmon.exe) to identify the process that is causing the high disk I/O¹. Resource Monitor provides detailed information about the system's resource usage, including disk I/O¹. The technician can use this information to identify the process that is causing the high disk I/O and take appropriate action¹.

NEW QUESTION: 75

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: (SHOW ANSWER)

The user can use the following commands to give the technician the correct information: ipconfig /all and hostname 1. The ipconfig /all command displays the IP address, subnet mask, and default gateway for all adapters on the computer 1. The hostname command displays the name of the computer 1.

NEW QUESTION: 76

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 ransomware. 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: (SHOW ANSWER)

The technician should quarantine the system first.

Reference:

CompTIA A+ Certification Exam: Core 2 Objectives Version 4.0. Retrieved from [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))

Valid 220-1102 Dumps shared by Actual4test.com for Helping Passing 220-1102 Exam! Actual4test.com now offer the **newest 220-1102 exam dumps**, the Actual4test.com 220-1102 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com 220-1102 dumps with Test Engine here:

https://www.actual4test.com/220-1102_examcollection.html (845 Q&As Dumps, **30%OFF Special Discount:**

Freepdfdumps)

NEW QUESTION: 77

As part of a CYOD policy a systems administrator needs to configure each user's Windows device to require a password when resuming from a period of sleep or inactivity. Which of the following paths will lead the administrator to the correct settings?

- A. Use Settings to access Screensaver settings
- B. Use Settings to access Screen Timeout settings
- C. Use Settings to access General
- D. Use Settings to access Display.

Answer: A (LEAVE A REPLY)

The systems administrator should use Settings to access Screensaver settings to configure each user's Windows device to require a password when resuming from a period of sleep or inactivity1

Valid 220-1102 Dumps shared by Actual4test.com for Helping Passing 220-1102 Exam! Actual4test.com now offer the **newest 220-1102 exam dumps**, the Actual4test.com 220-1102 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com 220-1102 dumps with Test Engine here:

https://www.actual4test.com/220-1102_examcollection.html (**845** Q&As Dumps, **30%OFF** Special Discount:

Freepdfdumps)