

CompTIA

Exam Questions 220-1102

CompTIA A+ Certification Exam: Core 2



NEW QUESTION 1

An employee has repeatedly contacted a technician about malware infecting a work computer. The technician has removed the malware several times, but the user's PC keeps getting infected. Which of the following should the technician do to reduce the risk of future infections?

- A. Configure the firewall.
- B. Restore the system from backups.
- C. Educate the end user
- D. Update the antivirus program.

Answer: C

Explanation:

Malware is software that infects computer systems to damage, disable or exploit the computer or network for various malicious purposes⁵. Malware is typically distributed via email attachments, fake internet ads, infected applications or websites, and often relies on user interaction to execute⁶. Therefore, one of the most effective ways to prevent malware infections is to educate the end user about the common signs and sources of malware, and how to avoid them⁷. Configuring the firewall, restoring the system from backups, and updating the antivirus program are also important security measures, but they do not address the root cause of the user's repeated infections, which is likely due to a lack of awareness or caution.

References⁵: Malware: what it is, how it works, and how to stop it - Norton⁶: How to Prevent Malware: 15 Best Practices for Malware Prevention⁷: 10 Security Tips for How to Prevent Malware Infections - Netwrix

NEW QUESTION 2

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

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

Answer: C

Explanation:

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

NEW QUESTION 3

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

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

Answer: D

Explanation:

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

NEW QUESTION 4

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

TEST QUESTION

An executive has contacted you through the help-desk chat support about an issue with a mobile device.

Assist the executive to help resolve the issue.

INSTRUCTIONS

Select the MOST appropriate statement for each response.

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

Telecom.

Please follow the new mobile device guide provided on our website.

the latest update, here is a screenshot

IMAP >

SSL >

10.0.200.1 >

100 >

on your mail settings to 143.

Send

ProtocolIMAP >

SecuritySSL >

Server Address10.0.200.1 >

Port100 >

Please change the port number on your mail settings to 143.

Thanks for helping.

Which of the following should be done NEXT?

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

Answer: A

NEW QUESTION 5

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

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

Answer: EG

Explanation:

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

NEW QUESTION 6

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

- A. Examine the antivirus logs.
- B. Verify the address bar URL.

- C. Test the internet connection speed.
- D. Check the web service status.

Answer: B

Explanation:

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

NEW QUESTION 7

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

Explanation:

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

NEW QUESTION 8

A hotel's Wi-Fi was used to steal information on a corporate laptop. A technician notes the following security log:
SRC: 192.168.1.1/secrets.zip Protocol SMB >> DST: 192.168.1.50/capture
The technician analyses the following Windows firewall information:

Port	Status	Direction
1	Open	In/Out
445	Open	In/Out
25	Open	Out
110	Open	In/Out
53	Open	In/Out

Which of the following protocols most likely allowed the data theft to occur?

- A. 1
- B. 53
- C. 110
- D. 445

Answer: D

Explanation:

The protocol that most likely allowed the data theft to occur is SMB over TCP port 445. SMB is a network file sharing protocol that enables access to files, printers, and other resources on a network. Port 445 is used by SMB to communicate directly over TCP without the need for NetBIOS, which is an older and less secure protocol. The security log shows that the source IP address 192.168.1.1 sent a file named secrets.zip using SMB protocol to the destination IP address 192.168.1.50, which captured the file. The Windows firewall information shows that port 445 is enabled for inbound and outbound traffic, which means that it is not blocked by the firewall. Therefore, port 445 is the most likely port that was exploited by the attacker to steal the data from the corporate laptop.

References:

- ? SMB port number: Ports 445, 139, 138, and 137 explained1
- ? What is an SMB Port + Ports 445 and 139 Explained2
- ? CompTIA A+ Certification Exam Core 2 Objectives3

NEW QUESTION 9

A technician at a customer site is troubleshooting a laptop. A software update needs to be downloaded but the company's proxy is blocking traffic to the update site. Which of the following should the technician perform?

- A. Change the DNS address to 1.1.1.1
- B. Update Group Policy
- C. Add the site to the client's exceptions list
- D. Verify the software license is current.

Answer: C

Explanation:

The technician should add the update site to the client's exceptions list to bypass the proxy. This can be done through the client's web browser settings, where the proxy settings can be configured. By adding the update site to the exceptions list, the client will be able to access the site and download the software update.

NEW QUESTION 10

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

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

Answer: D

Explanation:

The technician should adjust the firewall settings to resolve the issue of not being able to access an internal site at <https://companyintranet.com:8888>. The firewall settings control how the firewall filters and allows network traffic based on rules and policies. The firewall settings may be blocking or preventing the access to the internal site by mistake or by default, especially if the site uses a non-standard port number such as 8888. The technician should check and modify the firewall settings to allow the access to the internal site or its port number. Default gateway settings determine how a computer connects to other networks or the internet. Default gateway settings are not likely to cause the issue of not being able to access an internal site if the user can access the public internet. DHCP settings determine how a computer obtains its IP address and other network configuration parameters automatically from a DHCP server. DHCP settings are not likely to cause the issue of not being able to access an internal site if the user can access other network resources. IP address settings determine how a computer identifies itself and communicates with other devices on a network. IP address settings are not likely to cause the issue of not being able to access an internal site if the user can access other network resources. Antivirus settings control how the antivirus software scans and protects the computer from malware and threats. Antivirus settings are less likely to cause the issue of not being able to access an internal site than firewall settings, unless the antivirus software has its own firewall feature that may interfere with the network traffic. References: CompTIA A+ Core 2 (220-1102) Certification Exam Objectives Version 4.0, Domain 1.6

NEW QUESTION 10

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

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

Answer: A

Explanation:

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

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

NEW QUESTION 14

A technician is troubleshooting a Windows 10 PC that is unable to start the GUI. A new SSD and a new copy of Windows were recently installed on the PC. Which of the following is the most appropriate command to use to fix the issue?

- A. msconfig
- B. chkdsk
- C. sfc
- D. diskpart
- E. mstsc

Answer: C

Explanation:

The sfc command is a tool for scanning and repairing system files that are corrupted or missing on Windows operating systems¹². System files are essential files that are required for the proper functioning of the operating system, such as the GUI, drivers, services, and applications. If system files are damaged or deleted, the operating system may fail to start or run properly, causing errors, crashes, or blue screens.

The sfc command can be used to fix the issue of the PC that is unable to start the GUI, assuming that the problem is caused by corrupted or missing system files. The sfc command can be run from the command prompt, which can be accessed by booting the PC from the installation media, choosing the repair option, and selecting the command prompt option³. The sfc command can be used with different switches, such as /scannow, /verifyonly, /scanfile, or /offbootdir, depending on the situation and the desired action⁴. The

most common switch is /scannow, which scans all the system files and repairs any problems that are found⁵. The syntax of the sfc command with the /scannow switch is: sfc /scannow

The sfc command will then scan and repair the system files, and display the results on the screen. If the sfc command is able to fix the system files, the PC should be able to start the GUI normally after rebooting. If the sfc command is unable to fix the system files, the PC may need further troubleshooting or a clean installation of Windows.

References¹: CompTIA A+ Certification Exam Core 2 Objectives, page 10 ²: CompTIA A+ Core 2 (220-1102) Complete Video Course, Lesson 26 Documentation ³: How to use SFC Scannow to repair Windows system files ⁴: SFC Command (System File Checker) ⁵: How to Repair Windows 10 using Command Prompt

NEW QUESTION 16

A large university wants to equip all classrooms with high-definition IP videoconferencing equipment. Which of the following would most likely be impacted in this situation?

- A. SAN
- B. LAN
- C. GPU
- D. PAN

Answer: B

Explanation:

LAN is the most likely option to be impacted in this situation. LAN stands for Local Area Network, and it is a network that connects devices within a limited area, such as a building or a campus. Installing high-definition IP videoconferencing equipment in all classrooms would require a high bandwidth and reliable LAN infrastructure to support the video and audio transmission. The LAN would also need to be configured with proper security, quality of service, and multicast protocols to ensure the optimal performance of the videoconferencing system. SAN, GPU, and PAN are not directly related to this scenario. SAN stands for Storage Area Network, and it is a network that provides access to consolidated storage devices. GPU stands for Graphics Processing Unit, and it is a hardware component that handles graphics rendering and computation. PAN stands for Personal Area Network, and it is a network that connects devices within a short range, such as Bluetooth or infrared. References:

? Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 20

? CompTIA A+ Complete Study Guide: Core 1 Exam 220-1101 and Core 2 Exam ..., page 104

NEW QUESTION 17

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

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

Answer: D

Explanation:

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

NEW QUESTION 22

A technician is preparing to remediate a Trojan virus that was found on a workstation. Which of the following steps should the technician complete BEFORE removing the virus?

- A. Disable System Restore.
- B. Schedule a malware scan.
- C. Educate the end user.
- D. Run Windows Update.

Answer: A

Explanation:

Before removing a Trojan virus from a workstation, a technician should disable System Restore. System Restore is a feature that allows users to restore their system to a previous state in case of problems or errors. However, System Restore can also restore infected files or registry entries that were removed by antivirus software or manual actions. By disabling System Restore, a technician can ensure that the Trojan virus is completely removed and does not reappear after a system restore operation. Scheduling a malware scan may help detect and remove some malware but may not be effective against all types of Trojan viruses. Educating the end user may help prevent future infections but does not address the current issue of removing the Trojan virus. Running Windows Update may help

patch some security vulnerabilities but does not guarantee that the Trojan virus will be removed. References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.3

NEW QUESTION 25

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

- A. resmon.exe
- B. msconfig.extf
- C. dfrgui.exe
- D. msmf32.exe

Answer: C

Explanation:

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

NEW QUESTION 29

A Linux technician needs a filesystem type that meets the following requirements:

- . All changes are tracked.
- . The possibility of file corruption is reduced.
- . Data recovery is easy.

Which of the following filesystem types best meets these requirements?

- ☒ A. FAT32
- ☐ B: FAT32
- ☐ C. exFAT
- ☐ D. ext3

D. NTFS

Answer: A

Explanation:

The ext3 file system is a Linux native file system that meets the requirements of the question. It has the following features:

? All changes are tracked. The ext3 file system uses a journaling mechanism that

records all changes to the file system metadata in a special log called the journal before applying them to the actual file system. This ensures that the file system can be restored to a consistent state in case of a power failure or system crash¹².

? The possibility of file corruption is reduced. The journaling feature of ext3 also

reduces the possibility of file corruption, as it avoids the need for a full file system check after an unclean shutdown. The file system can be quickly replayed from the journal and any inconsistencies can be fixed¹².

? Data recovery is easy. The ext3 file system supports undeletion of files using tools

such as ext3grep or extundelete, which can scan the file system for deleted inodes and attempt to recover the data blocks associated with them³⁴.

References:

1: Introduction to Linux File System [Structure and Types] - MiniTool¹ 2: 7 Ways to Determine the File System Type in Linux (Ext2, Ext3 or Ext4) - Tecmint³ 3:

How to Recover Deleted Files in Linux with ext3grep 4: How to Recover Deleted Files from ext3 Partitions

NEW QUESTION 31

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

A. Network and Sharing Center

B. net use

C. User Accounts

D. regedit

E. Group Policy

Answer: E

Explanation:

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

NEW QUESTION 35

After a security event, a technician removes malware from an affected laptop and disconnects the laptop from the network. Which of the following should the technician do to prevent the operating system from automatically returning to an infected state?

A. Enable System Restore.

B. Disable System Restore.

C. Enable antivirus.

D. Disable antivirus.

E. Educate the user.

Answer: B

Explanation:

System Restore is a feature that allows the user to revert the system to a previous state. However, this can also restore the malware that was removed by the technician. Disabling System Restore can prevent the operating system from automatically returning to an infected state. Enabling antivirus, educating the user, and enabling System Restore are good preventive measures, but they do not address the question. Disabling antivirus can make the system more vulnerable to malware attacks

NEW QUESTION 37

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: D

Explanation:

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 41

A technician needs to track evidence for a forensic investigation on a Windows computer. Which of the following describes this process?

A. Valid license

B. Data retention requirements

C. Material safety data sheet

D. Chain of custody

Answer: D

Explanation:

Chain of custody is a legal term that refers to the chronological documentation or paper trail that records the sequence of custody, control, transfer, analysis, and disposition of materials, including physical or electronic evidence¹. It is important in forensic investigations to establish that the evidence is in fact related to the case, and that it has not been tampered with or contaminated. A technician needs to track evidence for a forensic investigation on a Windows computer by following the proper procedures for collecting, handling, storing, and analyzing the evidence, and documenting every step of the process on a chain of custody form²³

NEW QUESTION 43

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

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

Answer: A

Explanation:

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

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

NEW QUESTION 47

A small-office customer needs three PCs to be configured in a network with no server. Which of the following network types is the customer's BEST choice for this environment?

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

A workgroup network is a peer-to-peer network where each PC can share files and resources with other PCs without a central server. A public network is a network that is accessible to anyone on the internet. A wide area network is a network that spans a large geographic area, such as a country or a continent. A domain network is a network where a server controls the access and security of the PCs. Verified References: <https://www.comptia.org/blog/network-types>
<https://www.comptia.org/certifications/a>

NEW QUESTION 50

A customer called the help desk to report that a machine that was recently updated is no longer working. The support technician checks the latest logs to see what updates were deployed, but nothing was deployed in more than three weeks. Which of the following should the support technician do to BEST resolve the situation?

- A. Offer to wipe and reset the device for the customer.
- B. Advise that the help desk will investigate and follow up at a later date.
- C. Put the customer on hold and escalate the call to a manager.
- D. Use open-ended questions to further diagnose the issue.

Answer: D

Explanation:

Open-ended questions are questions that require more than a yes or no answer and encourage the customer to provide more details and information. Using open-ended questions can help the support technician to understand the problem better, identify the root cause, and find a suitable solution.

Some examples of open-ended questions are:

- ? What exactly is not working on your machine?
- ? When did you notice the problem?
- ? How often does the problem occur?
- ? What were you doing when the problem happened?
- ? What have you tried to fix the problem?

Offering to wipe and reset the device for the customer is not a good option, as it may result in data loss and inconvenience for the customer. It should be used as a last resort only if other troubleshooting steps fail. Advising that the help desk will investigate and follow up at a later date is not a good option, as it may leave the customer unsatisfied and frustrated. It should be used only if the problem requires further research or escalation and cannot be resolved on the first call. Putting the customer on hold and escalating the call to a manager is not a good option, as it may waste time and resources. It should be used only if the problem is beyond the support technician's scope or authority and requires managerial intervention.

NEW QUESTION 52

A technician is investigating options to secure a small office's wireless network. One requirement is to allow automatic log-ins to the network using certificates instead of passwords. Which of the following should the wireless solution have in order to support this feature?

- A. RADIUS
- B. AES

- C. EAP-EKE
- D. MFA

Answer: A

Explanation:

RADIUS is the correct answer for this question. RADIUS stands for Remote Authentication Dial-In User Service, and it is a protocol that provides centralized authentication, authorization, and accounting for wireless networks. RADIUS can support certificate-based authentication, which allows users to log in to the network automatically without entering passwords. RADIUS also provides other benefits, such as enforcing security policies, logging user activities, and managing network access. AES, EAP-EKE, and MFA are not wireless solutions, but rather encryption algorithms, authentication methods, and security factors, respectively.

References:

- ? Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 23
- ? CompTIA A+ Core 1 (220-1101) and Core 2 (220-1102) Cert Guide, page 459

NEW QUESTION 56

A system drive is nearly full, and a technician needs to free up some space. Which of the following tools should the technician use?

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

Answer: A

Explanation:

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

NEW QUESTION 61

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

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

Answer: B

Explanation:

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

NEW QUESTION 62

Antivirus software indicates that a workstation is infected with ransomware that cannot be quarantined. Which of the following should be performed first to prevent further damage to the host and other systems?

- A. Turn off the machine.
- B. Run a full antivirus scan.
- C. Remove the LAN card.
- D. Install a different endpoint solution.

Answer: A

Explanation:

Turning off the machine is the first and most urgent step to prevent further damage to the host and other systems. Ransomware can encrypt files, steal data, and spread to other devices on the network if the infected machine remains online. Turning off the machine will stop the ransomware process and isolate the machine from the network. The other options are either ineffective or risky. Running a full antivirus scan may not detect or remove the ransomware, especially if it is a new or unknown variant. Removing the LAN card may disconnect the machine from the network, but it will not stop the ransomware from encrypting or deleting files on the local drive. Installing a different endpoint solution may not be possible or helpful if the ransomware has already compromised the system or blocked the installation.

References: 1 3 steps to prevent and recover from ransomware(<https://www.microsoft.com/en-us/security/blog/2021/09/07/3-steps-to-prevent-and-recover-from-ransomware/>)2 #StopRansomware Guide | CISA(<https://www.cisa.gov/stopransomware/ransomware-guide>).

NEW QUESTION 63

An Android user contacts the help desk because a company smartphone failed to complete a tethered OS update. A technician determines there are no error messages on the device. Which of the following should the technician do NEXT?

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

Answer: C

Explanation:

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

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

NEW QUESTION 67

Which of the following is used as a password manager in the macOS?

- A. Terminal
- B. FileVault
- C. Privacy
- D. Keychain

Answer: D

Explanation:

Keychain is a feature of macOS that securely stores passwords, account numbers, and other confidential information for your Mac, apps, servers, and websites1. You can use the Keychain Access app on your Mac to view and manage your keychains and the items stored in them1. Keychain can also sync your passwords across your devices using iCloud Keychain1. Keychain can be used as a password manager in macOS to and other secure information. Help you keep track of and protect your passwords. References: 1: Manage passwords using keychains on Mac (<https://support.apple.com/guide/mac-help/use-keychains-to-store-passwords-mchlf375f392/mac>)

NEW QUESTION 71

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

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

Answer: C

Explanation:

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

NEW QUESTION 72

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

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

Answer: C

Explanation:

Open Settings, select System, select Display, and change the Scale and layout setting to a higher percentage123
Reference: 4. How to Increase the Text Size on Your Computer. Retrieved from <https://www.laptopmag.com/articles/increase-text-size-computer> 5. How to Change the Size of Text in Windows 10. Retrieved from <https://www.howtogeek.com/370055/how-to-change-the-size-of-text-in-windows-10/> 6. Change the size of text in Windows. Retrieved from <https://support.microsoft.com/en-us/windows/change-the-size-of-text-in-windows-1d5830c3-eee3-8eaa-836b-abcc37d99b9a>

NEW QUESTION 76

A technician is modifying the default home page of all the workstations in a company. Which of the following will help to implement this change?

- A. Group Policy
- B. Browser extension
- C. System Configuration
- D. Task Scheduler

Answer: A

Explanation:

Group Policy is a feature of Windows that allows administrators to centrally manage and configure the settings of computers and users in a domain network. Group Policy can be used to modify the default home page of all the workstations in a company by creating and applying a policy that specifies the desired URL for the home page. This way, the change will be automatically applied to all the workstations that are joined to the domain and receive the policy.

NEW QUESTION 81

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 83

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 85

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

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

Answer: D

Explanation:

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

NEW QUESTION 89

Which of the following would MOST likely be deployed to enhance physical security for a building? (Select TWO).

- A. Multifactor authentication
- B. Badge reader
- C. Personal identification number
- D. Firewall
- E. Motion sensor
- F. Soft token

Answer: BE

Explanation:

Badge reader and motion sensor are devices that can be deployed to enhance physical security for a building. A badge reader is a device that scans and verifies an identification card or tag that grants access to authorized personnel only. A badge reader can help prevent unauthorized entry or intrusion into a building or a restricted area. A motion sensor is a device that detects movement and triggers an alarm or an action when motion is detected. A motion sensor can help deter or alert potential intruders or trespassers in a building or an area. Multifactor authentication is a method of verifying identity using two or more factors, such as something you know, something you have or something you are. Multifactor authentication is not a device that can be deployed to enhance physical security for a building but a technique that can be used to enhance logical security for systems or services. Personal identification number is a numeric code that can be used as part of authentication or access control. Personal identification number is not a device that can be deployed to enhance physical security for a building but an example of something you know factor in multifactor authentication. Firewall is a device or software that filters network traffic based on rules and policies. Firewall is not a device that can be deployed to enhance physical security for a building but a device that can be used to enhance network security for systems or services. Soft token is an application or software that generates one-time passwords or codes for authentication purposes. Soft token is not a device that can be deployed to enhance physical security for a building but an example of something you have factor in multifactor authentication. References: CompTIA A+ Core 2 (220-1102) Certification Exam Objectives Version 4.0, Domain 3.3

NEW QUESTION 94

A salesperson's computer is unable to print any orders on a local printer that is connected to the computer Which of the following tools should the salesperson use to restart the print spooler?

- A. Control Panel
- B. Processes
- C. Startup
- D. Services

Answer: D

Explanation:

The correct answer is D. Services. The print spooler is a service that manages the print queue and sends print jobs to the printer. To restart the print spooler, the salesperson can use the Services app, which allows them to stop and start the service. Alternatively, they can also use the Task Manager or the Command Prompt to restart the print spooler.

References and Explanation

? The Services app is a tool that displays all the services that are running on the

computer. It can be accessed by typing services.msc in the Run window or by searching for Services in the Start menu. The Services app allows users to start, stop, restart, or configure any service, including the print spooler¹²³.

? The Task Manager is a tool that shows information about the processes,

applications, and services that are running on the computer. It can be accessed by pressing Ctrl + Shift + Esc or by right-clicking on the taskbar and selecting Task Manager. The Task Manager allows users to start, stop, or restart any service by going to the Services tab and right-clicking on the service name¹².

? The Command Prompt is a tool that allows users to execute commands and

perform tasks using text input. It can be accessed by typing cmd in the Run window or by searching for Command Prompt in the Start menu. The Command Prompt allows users to start, stop, or restart any service by using the net command with the service name. For example, to restart the print spooler, users can type net stop spooler and then net start spooler¹.

? The Control Panel is a tool that provides access to various settings and options for

the computer. It can be accessed by typing control panel in the Run window or by searching for Control Panel in the Start menu. The Control Panel does not allow users to restart the print spooler directly, but it can be used to access other tools such as Devices and Printers, Troubleshooting, or Administrative Tools².

? The Processes tab is a part of the Task Manager that shows information about the

processes that are running on the computer. It can be accessed by opening the Task Manager and selecting the Processes tab. The Processes tab does not allow users to restart the print spooler directly, but it can be used to end any process that is related to printing or causing problems with the print spooler².

? The Startup tab is a part of the Task Manager that shows information about the

programs that run automatically when the computer starts. It can be accessed by opening the Task Manager and selecting the Startup tab. The Startup tab does not allow users to restart the print spooler directly, but it can be used to disable or enable any program that affects printing or interferes with the print spooler².

NEW QUESTION 98

A company needs employees who work remotely to have secure access to the corporate intranet. Which of the following should the company implement?

- A. Password-protected Wi-Fi
- B. Port forwarding
- C. Virtual private network
- D. Perimeter network

Answer: C

Explanation:

A virtual private network (VPN) is a technology that creates a secure and encrypted connection over a public network, such as the internet. A VPN allows remote employees to access the corporate intranet as if they were physically connected to the local network³.

Password-protected Wi-Fi is a security measure for wireless networks that does not provide access to the corporate intranet. Port forwarding is a technique that allows external devices to access services on a private network through a router, but does not provide access to the corporate intranet. A perimeter network is a network segment that lies between an internal network and an external network, such as the internet, and provides an additional layer of security, but does not provide access to the corporate intranet.

NEW QUESTION 99

Windows updates need to be performed on a department's servers. Which of the following methods should be used to connect to the server?

- A. FIP
- B. MSRA
- C. RDP
- D. VPN

Answer: C

Explanation:

RDP (Remote Desktop Protocol) is a protocol that allows a user to connect to and control a remote computer over a network. RDP can be used to perform Windows updates on a department's servers without physically accessing them.

Reference: CompTIA A+ Core 2 Exam Objectives, Section 5.6

NEW QUESTION 103

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Malware is malicious software that can cause damage or harm to a computer system or network⁴. A technician has verified a computer is infected with malware by observing unusual behavior, such as slow performance, pop-ups, or unwanted ads. The technician isolates the system and updates the anti-malware software to prevent further infection or spread of the malware. The next step is to run repeated remediation scans until the malware is removed. A remediation scan is a

scan that detects and removes malware from the system. Running one scan may not be enough to remove all traces of malware, as some malware may hide or regenerate itself.

NEW QUESTION 104
SIMULATION

A user reports that after a recent software deployment to upgrade applications, the user can no longer use the Testing program. However, other employees can successfully use the Testing program.

INSTRUCTIONS

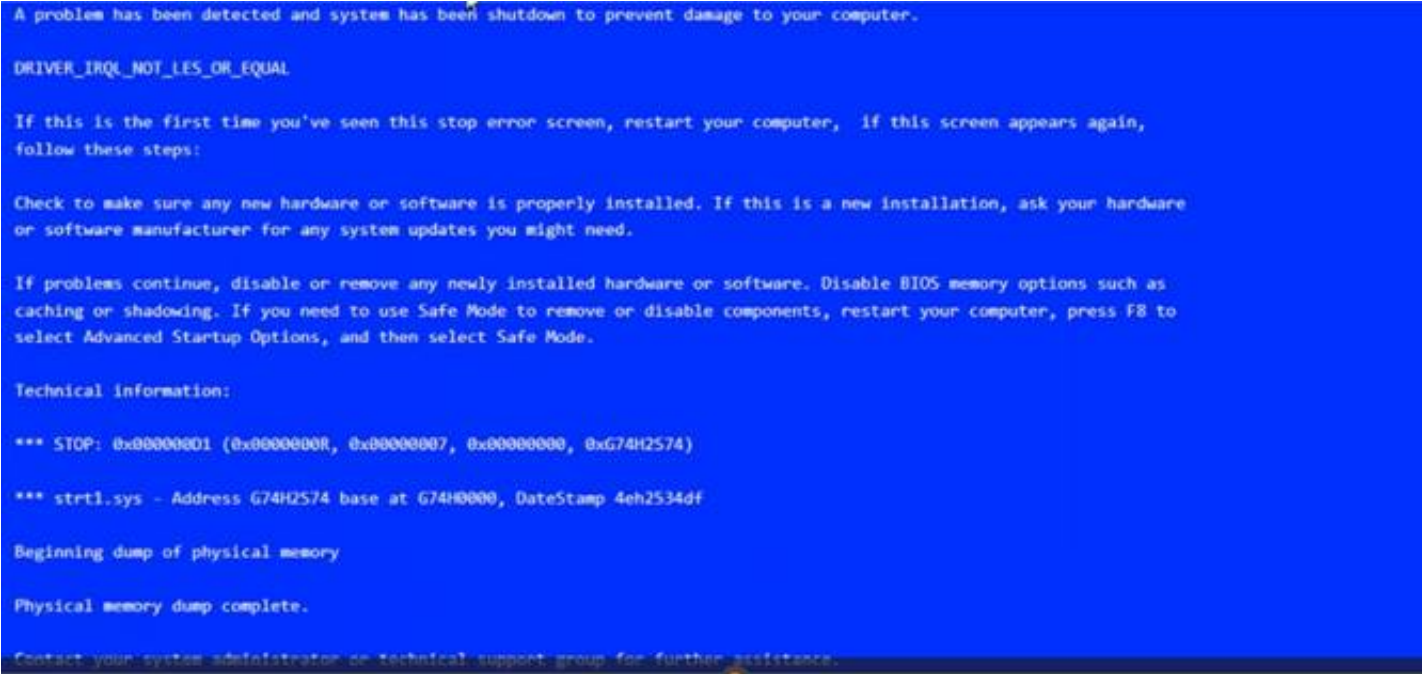
Review the information in each tab to verify the results of the deployment and resolve any issues discovered by selecting the:

? Index number of the Event Viewer issue

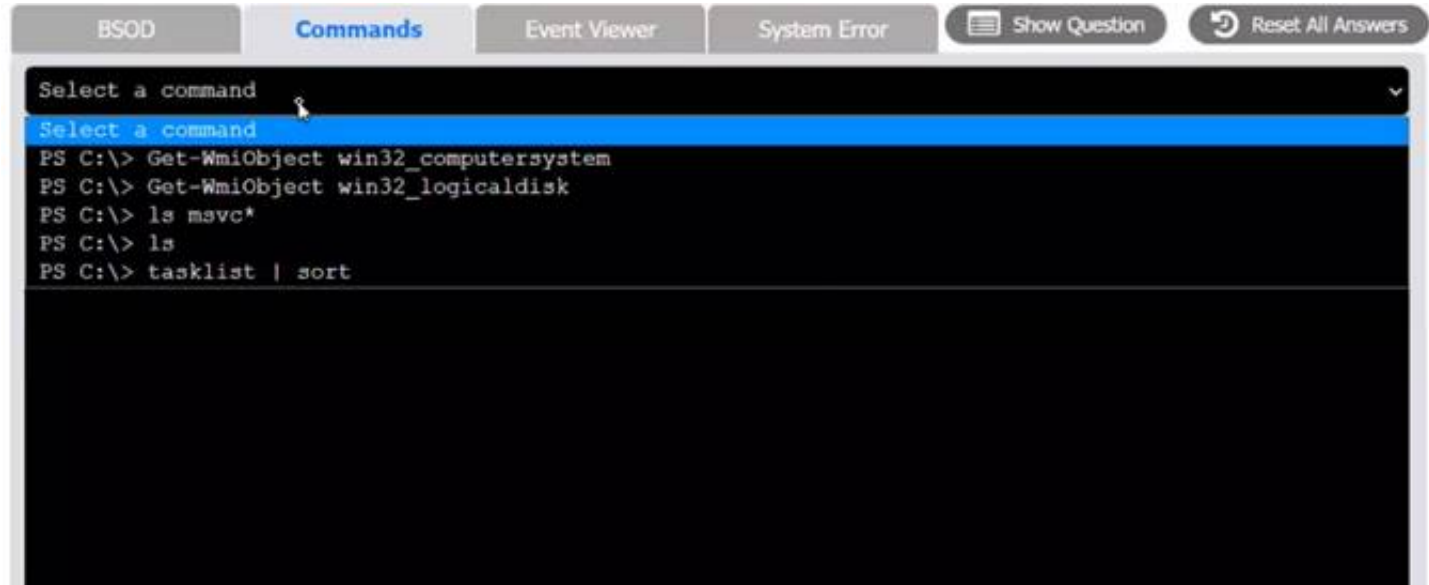
? First command to resolve the issue

? Second command to resolve the issue

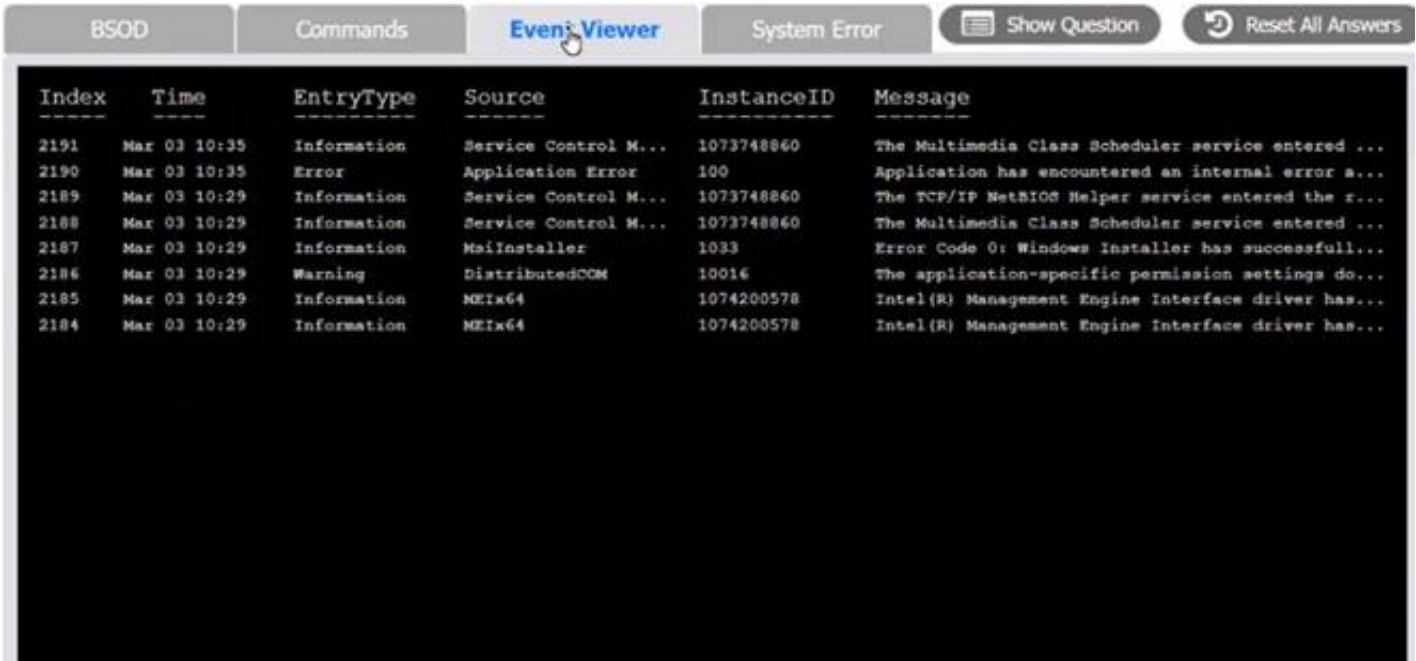
BSOD



Commands:



Event Viewer:



System Error:

BSOD


Commands

Event Viewer

System Error

Show Question

Reset All Answers



The program can't start because MSVCP100.dll is missing from your computer. Try reinstalling the program to fix this problem.

OK

Event Viewer Issue

Select Event Viewer Issue

2184
2185
2186
2187
2188
2189
2190
2191

Select Event Viewer Issue

Event Viewer Issue

1st CLI Resolution

Select Resolution

```
reg /s "msvc100.reg"
Get-WmiObject win32_computersystem
setx path "C:\Windows\System32"
Get-EventLog -LogName System -Newest 8
regsvr32 msvc100.dll
robocopy "\\User-PC02\C$\Windows\System32" "C:\Program Files (x86)\Testing" "msvc100.dll"
Get-WmiObject win32_logicaldisk
shutdown -s -f -t 0
gpupdate /force
copy "C:\Program Files\Testing\msvc100.dll" "\\User-PC02\C$\Windows\System32" /v /y
ls msvc*
tasklist | sort
```

Select Resolution

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

Event Viewer Issue

2187

1st CLI Resolution

copy "C:\Program Files\Testing\msvc100.dll" "\\User-PC02\C\$\Windows\System32" /v /y

The user is experiencing a system error that prevents them from using the Testing program. The error message indicates that the file MSVCP100.dll is missing from the computer. This file is part of the Microsoft Visual C++ 2010 Redistributable Package, which is required by some applications to run properly. The error may have occurred due to a corrupted or incomplete software deployment.

To resolve this issue, the user needs to restore the missing file and register it in the system. One possible way to do this is to copy the file from another computer that has the

Testing program installed and working, and then use the regsvr32 command to register it. The steps are as follows:

- ? On another computer (User-PC02) that has the Testing program installed and working, locate the file MSVCP100.dll in the folder C:\Program Files\Testing.
- ? Share the folder C:\Windows\System32 on User-PC02 by right-clicking on it, selecting Properties, then Sharing, then Advanced Sharing, then checking Share this folder, then clicking OK.
- ? On the user's computer (User-PC01), open a command prompt as an administrator by clicking Start, typing cmd, right-clicking on Command Prompt, and selecting Run as administrator.
- ? In the command prompt, type the following command to copy the file MSVCP100.dll from User-PC02 to User-PC01: copy "C:\Program Files\Testing\msvc100.dll" "\\User-PC02\C\$\Windows\System32"
- ? After the file is copied, type the following command to register it in the system: regsvr32 msvc100.dll
- ? Restart the user's computer and try to run the Testing program again. Therefore, based on the instructions given by the user, the correct answers are: Select Event Viewer Issue: 2187
 Select First Command: copy "C:\Program Files\Testing\msvc100.dll" "\\User- PC02\C\$\Windows\System32"
 Select Second Command: regsvr32 msvc100.dll

NEW QUESTION 107

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

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

Answer: B

Explanation:

A synthetic backup is a backup type that provides a backup for all data on the system while providing the lowest impact to the network. It combines a full backup

with one or more incremental backups to create a single backup set, without requiring access to the original data source. Off-site is a backup location, not a backup type. Full and differential are backup types, but they have a higher impact on the network than synthetic. Verified References:
<https://www.comptia.org/blog/what-is-a-synthetic-backup> <https://www.comptia.org/certifications/a>

NEW QUESTION 112

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

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

Answer: B

Explanation:

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

NEW QUESTION 114

A technician is troubleshooting application crashes on a Windows workstation. Each time the workstation user tries to open a website in a browser, the following message is displayed:

crypt32.dll is missing not found

Which of the following should the technician attempt FIRST?

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

Answer: D

Explanation:

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

NEW QUESTION 115

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

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

Answer: C

Explanation:

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

NEW QUESTION 116

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

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

Answer: C

Explanation:

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

NEW QUESTION 120

A team of support agents will be using their workstations to store credit card data. Which of the following should the IT department enable on the workstations in order to remain compliant with common regulatory controls? (Select TWO).

- A. Encryption
- B. Antivirus
- C. AutoRun
- D. Guest accounts
- E. Default passwords
- F. Backups

Answer: AF

Explanation:

Encryption is a way of protecting cardholder data by transforming it into an unreadable format that can only be decrypted with a secret key¹. Backups are a way of ensuring that cardholder data is not lost or corrupted in case of a disaster or system failure². Both encryption and backups are part of the PCI DSS requirements that apply to any entity that stores, processes, or transmits cardholder data¹. The other options are not directly related to credit card data security or compliance.

NEW QUESTION 122

Which of the following should be documented to ensure that the change management plan is followed?

- A. Scope of the change
- B. Purpose of the change
- C. Change rollback plan
- D. Change risk analysis

Answer: A

Explanation:

The scope of the change is one of the elements that should be documented to ensure that the change management plan is followed. The scope of the change defines the boundaries and limitations of the change, such as what is included and excluded, what are the deliverables and outcomes, what are the assumptions and constraints, and what are the dependencies and risks. The scope of the change helps to clarify the expectations and objectives of the change, as well as to prevent scope creep or deviation from the original plan. The scope of the change also helps to measure the progress and success of the change, as well as to communicate the change to the stakeholders and the team

NEW QUESTION 126

A user reported that a laptop's screen turns off very quickly after silting for a few moments and is also very dim when not plugged in to an outlet Everything else seems to be functioning normally. Which of the following Windows settings should be configured?

- A. Power Plans
- B. Hibernate
- C. Sleep/Suspend
- D. Screensaver

Answer: A

Explanation:

Power Plans are Windows settings that allow a user to configure how a laptop's screen behaves when plugged in or running on battery power. They can adjust the screen brightness and the time before the screen turns off due to inactivity. Hibernate, Sleep/Suspend and Screensaver are other Windows settings that affect how a laptop's screen behaves, but they do not allow changing the screen brightness or turning off time. Verified References: <https://www.comptia.org/blog/windows-power-plans> <https://www.comptia.org/certifications/a>

NEW QUESTION 129

A new employee was hired recently. Which of the following documents will the new employee need to sign before being granted login access to the network?

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

A new employee will need to sign an AUP before being granted login access to the network. An AUP is an Acceptable Use Policy that defines the rules and guidelines for using network resources and services in an organization. An AUP typically covers topics such as security, privacy, ethics, compliance and liability issues related to network usage. An AUP helps protect the organization and its users from legal, regulatory and reputational risks associated with network activities. An MSDS is a Material Safety Data Sheet that provides information about hazardous substances and how to handle them safely. An MSDS is not related to network access or usage. A EULA is an End User License Agreement that specifies the terms and conditions for using a software product or service. A EULA is usually provided by software vendors or developers and does not apply to network access or usage in general. A UAC is a User Account Control that is a security feature that prompts users for permission or confirmation before performing certain actions that require elevated privileges or affect system settings. A UAC is not

a document that needs to be signed by users but a mechanism that helps prevent unauthorized changes or malware infections on a system. References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 5.1

NEW QUESTION 132

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 133

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:

The first step in removing a virus from a computer is to update the antivirus software with the latest virus definitions. Virus definitions are files that contain information about the characteristics and behavior of known viruses and malware. They help the antivirus software to identify and remove the malicious threats from the computer. Without the latest virus definitions, the antivirus software may not be able to detect or remove the virus that infected the user's computer. Therefore, the technician should download the latest virus definitions from the antivirus vendor's website or use the update feature in the antivirus program before scanning the computer for viruses.

References:

- ? How to remove malware or viruses from my Windows 10 PC, section 21
- ? How to Remove a Virus From a Computer in 2023, section 32
- ? The Official CompTIA A+ Core 2 Study Guide (220-1102), page 2193

NEW QUESTION 135

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

- A. Mastered
- B. Not Mastered

Answer: A

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 138

A user visits a game vendor's website to view the latest patch notes, but this information is not available on the page. Which of the following should the user perform before reloading the page?

- A. Synchronize the browser data.
- B. Enable private browsing mode.
- C. Mark the site as trusted.
- D. Clear the cached file.

Answer: D

Explanation:

Clearing the cached file is an action that can help resolve the issue of not seeing the latest patch notes on a game vendor's website. A cached file is a copy of a web page or file that is stored locally on the user's browser or device for faster loading and offline access. However, sometimes a cached file may become outdated or corrupted and prevent the user from seeing the most recent or accurate version of a web page or file. Clearing the cached file can force the browser to download and display the latest version from the server instead of using the old copy from the cache. Synchronizing the browser data, enabling private browsing mode, and marking the site as trusted are not actions that can help resolve this issue.

NEW QUESTION 139

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

Explanation:

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.

NEW QUESTION 144

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

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

Answer: C

Explanation:

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

NEW QUESTION 147

A user reports an issue when connecting a mobile device to Bluetooth. The user states the mobile device's Bluetooth is turned on. Which of the following steps should the technician take NEXT to resolve the issue?

- A. Restart the mobile device.
- B. Turn on airplane mode.
- C. Check that the accessory is ready to pair.
- D. Clear all devices from the phone's Bluetooth settings.

Answer: C

Explanation:

The first step in troubleshooting a Bluetooth connection issue is to check that the accessory is ready to pair with the mobile device. Some accessories may have a button or a switch that needs to be pressed or turned on to initiate pairing mode. If the accessory is not ready to pair, the mobile device will not be able to detect it.
Reference: CompTIA A+ Core 2 Exam Objectives, Section 2.4

NEW QUESTION 149

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

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

Answer: AD

Explanation:

The correct answers are A and D. Zombies and botnets are types of infections that allow malicious actors to remotely control infected computers and use them to launch distributed denial-of-service (DDoS) attacks against a target. A DDoS attack is a type of cyberattack that aims to overwhelm a server or a network with a large volume of traffic from multiple sources, causing it to slow down or crash.

A keylogger is a type of malware that records the keystrokes of a user and sends them to a remote server, often for the purpose of stealing passwords, credit card numbers, or other sensitive information.

Adware is a type of software that displays unwanted advertisements on a user's computer, often in the form of pop-ups, banners, or redirects. Adware can also collect user data and compromise the security and performance of the system.

Ransomware is a type of malware that encrypts the files or locks the screen of a user's computer and demands a ransom for their restoration. Ransomware can also threaten to delete or expose the user's data if the ransom is not paid.

Spyware is a type of software that covertly monitors and collects information about a user's online activities, such as browsing history, search queries, or personal data. Spyware can also alter the settings or functionality of the user's system without their consent.

NEW QUESTION 151

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. Mastered
- B. Not Mastered

Answer: A

Explanation:

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 154

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

- A. Mastered
- B. Not Mastered

Answer: A

NEW QUESTION 155

A user received the following error upon visiting a banking website:

The security presented by website was issued a different website' s address . A technician should instruct the user to:

- A. clear the browser cache and contact the bank.
- B. close out of the site and contact the bank.
- C. continue to the site and contact the bank.
- D. update the browser and contact the bank.

Answer: A

Explanation:

The technician should instruct the user to clear the browser cache and contact the bank (option A). This error indicates that the website the user is visiting is not the correct website and is likely due to a cached version of the website being stored in the user's browser. Clearing the browser cache should remove any stored versions of the website and allow the user to access the correct website. The user should also contact the bank to confirm that they are visiting the correct website and to report the error.

NEW QUESTION 156

HOTSPOT

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.

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.

Show Question

Reset All Answers

Details

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



No Ticket Selected

Please select a ticket from the list

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

A. Mastered
B. Not Mastered

Explanation:

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 160

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. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

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 163

A technician is hardening a company file server and needs to prevent unauthorized LAN devices from accessing stored files. Which of the following should the technician use?

- A. Software firewall
- B. Password complexity
- C. Antivirus application
- D. Anti-malware scans

Answer: A

Explanation:

A software firewall is a program that monitors and controls the incoming and outgoing network traffic on a computer or a server. A software firewall can help prevent unauthorized LAN devices from accessing stored files on a company file server by applying rules and policies that filter the network packets based on their source, destination, protocol, port, or content. A software firewall can also block or allow specific applications or services from communicating with the network, and alert the administrator of any

suspicious or malicious activity¹².

A software firewall is a better option than the other choices because:

? Password complexity (B) is a good practice to protect the file server from

unauthorized access, but it is not sufficient by itself. Password complexity refers to the use of strong passwords that are hard to guess or crack by attackers, and that are changed frequently and securely. Password complexity can prevent brute force attacks or credential theft, but it cannot stop network attacks that exploit vulnerabilities in the file server software or hardware, or that bypass the authentication process³⁴.

? Antivirus application © and anti-malware scans (D) are important tools to protect

the file server from viruses and malware that can infect, damage, or encrypt the stored files. However, they are not effective in preventing unauthorized LAN devices from accessing the files in the first place. Antivirus and anti-malware tools can only detect and remove known threats, and they may not be able to stop zero- day attacks or advanced persistent threats that can evade or disable

them. Moreover, antivirus and anti-malware tools cannot control the network traffic or the file server permissions, and they may not be compatible with all file server platforms or configurations⁵⁶.

References:

1: What is a Firewall and How Does it Work? - Cisco1 2: How to Harden Your Windows Server - ServerMania2 3: Password Security: Complexity vs. Length - Norton7 4: Password Hardening: 5 Ways to Protect Your Passwords - Infosec 5: What is Antivirus Software and How Does it Work? - Kaspersky 6: What is Anti-Malware? - Malwarebytes

NEW QUESTION 164

A technician is trying to connect to a user's laptop in order to securely install updates. Given the following information about the laptop:

```
Hostname:      corp-laptop-222
IP Address:    192.168.0.45
Gateway:       192.168.1.1
Subnet Mask:   255.255.252.0
Open Ports:    21, 22, 80, 443
```

Which of the following should the technician do to connect via RDP?

- A. Confirm the user can ping the default gateway.
- B. Change the IP address on the user's laptop.
- C. Change the subnet mask on the user's laptop.
- D. Open port 3389 on the Windows firewall.

Answer: D

Explanation:

In order to connect to a user's laptop via RDP, the technician should open port 3389 on the Windows firewall. This is because RDP uses port 3389 for communication¹². The other options are not necessary or relevant for establishing an RDP connection.

? Confirming the user can ping the default gateway is not required for RDP, as it

only tests the network connectivity between the user's laptop and the router. RDP works over the internet, so the technician should be able to ping the user's laptop directly using its IP address³.

? Changing the IP address on the user's laptop is not needed for RDP, as long as

the IP address is valid and not conflicting with another device on the network. The user's laptop has a valid IP address of 192.168.0.45, which belongs to the same subnet as the gateway (192.168.0.1) and the subnet mask (255.255.255.0)⁴.

? Changing the subnet mask on the user's laptop is not required for RDP, as long as

the subnet mask matches the network configuration. The user's laptop has a correct subnet mask of 255.255.255.0, which defines a network with 254 possible hosts⁴.

References:

1: [What is RDP and How Does It Work? - CompTIA] 2: CompTIA A+ Certification Exam Core 2 Objectives - CompTIA 3: [Ping (networking utility) - Wikipedia] 4: [IP address - Wikipedia] : What is RDP and How Does It Work? - CompTIA : CompTIA A+ Certification Exam Core 2 Objectives - CompTIA : Ping (networking utility) - Wikipedia) : IP address - Wikipedia

NEW QUESTION 166

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

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

Answer: B

Explanation:

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

NEW QUESTION 168

Which of the following filesystem types does macOS use?

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

D. APFS

Answer: D

Explanation:

APFS stands for Apple File System and it is the default filesystem type for macOS since High Sierra (10.13) version1. APFS is optimized for flash storage and supports features such as encryption, snapshots, cloning, and space sharing1.

NEW QUESTION 171

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

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

Answer: C

Explanation:

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

NEW QUESTION 176

A technician is concerned about a large increase in the number of whaling attacks happening in the industry. The technician wants to limit the company's risk to avoid any issues. Which of the following items should the technician implement?

- A. Screened subnet
- B. Firewall
- C. Anti-phishing training
- D. Antivirus

Answer: C

Explanation:

Anti-phishing training is a method of educating users on how to identify and avoid phishing attacks, which are attempts to trick users into revealing sensitive information or performing malicious actions by impersonating legitimate entities or persons. Whaling attacks are a specific type of phishing attack that target high-level executives or influential individuals within an organization. Anti-phishing training can help users recognize the signs of whaling attacks and prevent them from falling victim to them. Screened subnet, firewall, and antivirus are not items that can directly address the issue of whaling attacks.

NEW QUESTION 181

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 2 220-1102 exam covers this topic in the domain 1.4 Given a scenario, use appropriate data destruction and disposal methods.

NEW QUESTION 182

A developer's Type 2 hypervisor is performing inadequately when compiling new source code. Which of the following components should the developer upgrade to improve the hypervisor's performance?

- A. Amount of system RAM
- B. NIC performance
- C. Storage IOPS
- D. Dedicated GPU

Answer: A

Explanation:

The correct answer is A. Amount of system RAM. A Type 2 hypervisor is a virtualization software that runs on top of a host operating system, which means it shares the system resources with the host OS and other applications. Therefore, increasing the amount of system RAM can improve the performance of the hypervisor and the virtual machines running on it. RAM is used to store data and instructions that are frequently accessed by the CPU, and having more RAM can reduce the need for swapping data to and from the storage device, which is slower than RAM.

NIC performance, storage IOPS, and dedicated GPU are not as relevant for improving the hypervisor's performance in this scenario. NIC performance refers to the speed and quality of the network interface card, which is used to connect the computer to a network. Storage IOPS refers to the number of input/output operations per second that can be performed by the storage device, which is a measure of its speed and efficiency. Dedicated GPU refers to a separate graphics processing unit that can handle complex graphics tasks, such as gaming or video editing. These components may affect other aspects of the computer's performance, but they are not directly related to the hypervisor's ability to compile new source code.

NEW QUESTION 185

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. Automatic screen lock
- C. Account lockout
- D. Antivirus

Answer: B

Explanation:

Account lockout would best mitigate the threat of a dictionary attack1

NEW QUESTION 188

A technician is setting up a desktop computer in a small office. The user will need to access files on a drive shared from another desktop on the network. Which of the following configurations should the technician employ to achieve this goal?

- A. Configure the network as private
- B. Enable a proxy server
- C. Grant the network administrator role to the user
- D. Create a shortcut to public documents

Answer: A

Explanation:

The technician should configure the network as private to allow the user to access files on a drive shared from another desktop on the network1

NEW QUESTION 191

Which of the following helps ensure that a piece of evidence extracted from a PC is admissible in a court of law?

- A. Data integrity form
- B. Valid operating system license
- C. Documentation of an incident
- D. Chain of custody

Answer: D

Explanation:

Chain of custody is a process that helps ensure that a piece of evidence extracted from a PC is admissible in a court of law. Chain of custody refers to the documentation and tracking of who handled, accessed, modified, or transferred the evidence, when, where, why, and how. Chain of custody can help establish the authenticity, integrity, and reliability of the evidence, as well as prevent tampering, alteration, or loss of the evidence. Data integrity form, valid operating system license, and documentation of an incident are not processes that can ensure that a piece of evidence extracted from a PC is admissible in a court of law.

NEW QUESTION 192

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. Mastered
- B. Not Mastered

Answer: A

Explanation:

The systems administrator should clear the application cache1e2

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 195

Which of the following is a package management utility for PCs that are running the Linux operating system?

- A. chmod
- B. yum
- C. man
- D. grep

Answer: B

Explanation:

yum (Yellowdog Updater Modified) is a package management utility for PCs that are running the Linux operating system. It can be used to install, update and remove software packages from repositories. chmod (change mode) is a command that changes the permissions of files and directories in Linux. man (manual) is a command that displays the documentation of other commands in Linux. grep (global regular expression print) is a command that searches for patterns in text files in Linux. Verified References: <https://www.comptia.org/blog/linux-package-management> <https://www.comptia.org/certifications/a>

NEW QUESTION 197

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 alt 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

Explanation:

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 201

Which of the following is a proprietary Cisco AAA protocol?

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

Answer: D

Explanation:

TACACS+ is a proprietary Cisco AAA protocol

NEW QUESTION 204

Remote employees need access to information that is hosted on local servers at the company. The IT department needs to find a solution that gives employees secure access to the company's resources as if the employees were on premises. Which of the following remote connection services should the IT team implement?

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

Answer: C

Explanation:

A VPN (Virtual Private Network) is a service that allows remote employees to access the company's network resources securely over the internet as if they were on premises. A VPN encrypts the data traffic between the employee's device and the VPN server, and assigns the employee a virtual IP address that belongs to the company's network. This way, the employee can access the local servers, files, printers, and other resources without exposing them to the public internet. A VPN also protects the employee's privacy and identity by masking their real IP address and location.

NEW QUESTION 207

A technician has just used an anti-malware removal tool to resolve a user's malware issue on a corporate laptop. Which of the following BEST describes what the technician should do before returning the laptop to the user?

- A. Educate the user on malware removal.
- B. Educate the user on how to reinstall the laptop OS.
- C. Educate the user on how to access recovery mode.
- D. Educate the user on common threats and how to avoid them.

Answer: D

Explanation:

educating the user on common threats and how to avoid them (D) would be a good step before returning the laptop to the user. This can help prevent similar issues from happening again.

NEW QUESTION 212

A user reports that a workstation is operating sluggishly Several other users operate on the same workstation and have reported that the workstation is operating normally. The systems administrator has validated that the workstation functions normally. Which of the following steps should the systems administrator most likely attempt NEXT?

- A. Increase the paging file size
- B. Run the chkdsk command
- C. Rebuild the user's profile
- D. Add more system memory.
- E. Defragment the hard drive.

Answer: C

Explanation:

Since the systems administrator has validated that the workstation functions normally and other users operate on the same workstation without any issues, the next step should be to rebuild the user's profile. This will ensure that any corrupted files or settings are removed and the user's profile is restored to its default state.

NEW QUESTION 214

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. Mastered
- B. Not Mastered

Answer: A

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 215

A systems administrator is creating periodic backups of a folder on a Microsoft Windows machine. The source data is very dynamic, and files are either added or deleted regularly. Which of the following utilities can be used to 'mirror the source data for the backup?

- A. copy
- B. xcopy
- C. robocopy
- D. Copy-Item

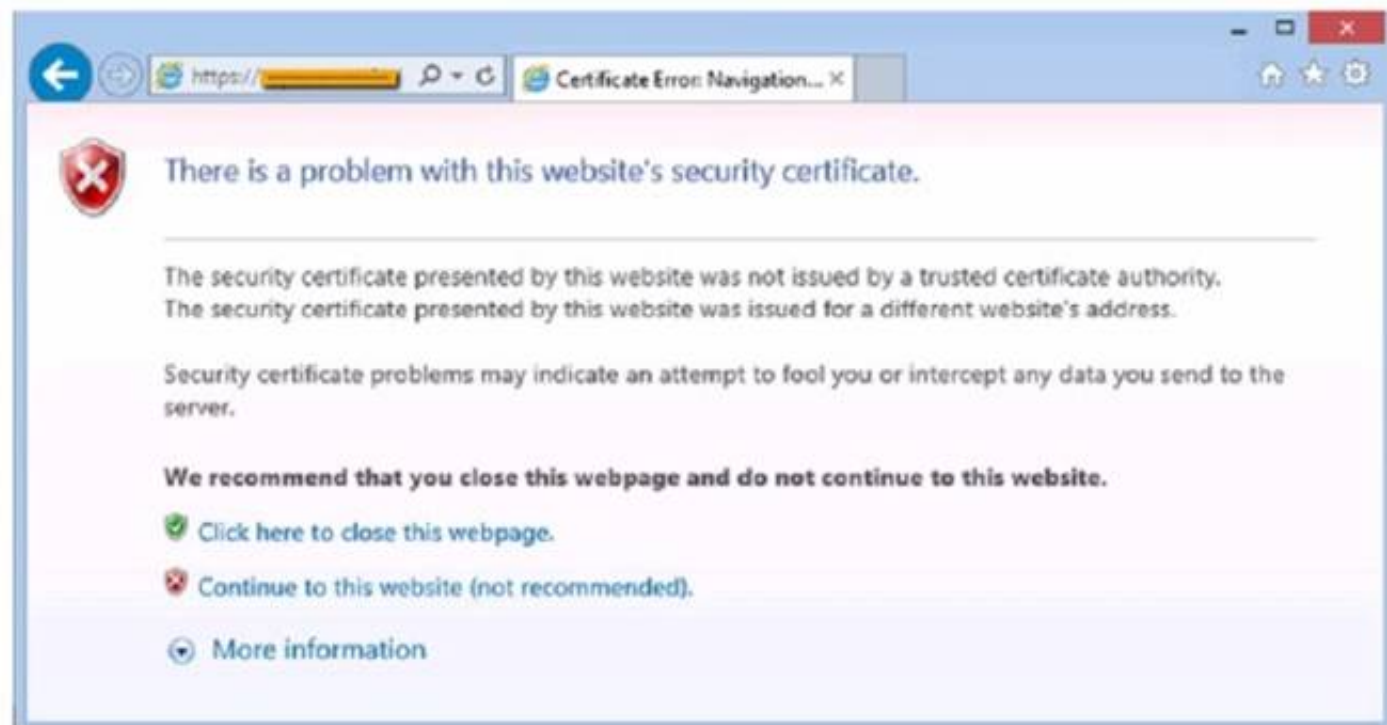
Answer: C

Explanation:

Robocopy is a command-line utility that can be used to mirror the source data for the backup. It can copy files and folders with various options, such as copying only changed files, preserving attributes and permissions, and retrying failed copies. Robocopy is more powerful and flexible than copy or xcopy, which are simpler commands that can only copy files and folders without mirroring or other advanced features. Copy-Item is a PowerShell cmdlet that can also copy files and folders, but it is not a native Windows utility and it requires PowerShell to run.
 References: 1: <https://windowsreport.com/mirror-backup-software/>

NEW QUESTION 219

After clicking on a link in an email a Chief Financial Officer (CFO) received the following error:



The CFO then reported the incident to a technician. The link is purportedly to the organization's bank. Which of the following should the technician perform FIRST?

- A. Update the browser's CRLs
- B. File a trouble ticket with the bank.
- C. Contact the ISP to report the CFO's concern
- D. Instruct the CFO to exit the browser

Answer: A

Explanation:

The technician should update the browser's CRLs first. The error message indicates that the certificate revocation list (CRL) is not up to date. Updating the CRLs will ensure that the browser can verify the authenticity of the bank's website.

NEW QUESTION 220

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

- A. PIN code
- B. OS updates

- C. Antivirus software
- D. BYOD policy

Answer: A

Explanation:

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

NEW QUESTION 223

The Chief Executive Officer at a bank recently saw a news report about a high-profile cybercrime where a remote-access tool that the bank uses for support was also used in this crime. The report stated that attackers were able to brute force passwords to access systems. Which of the following would BEST limit the bank's risk? (Select TWO)

- A. Enable multifactor authentication for each support account
- B. Limit remote access to destinations inside the corporate network
- C. Block all support accounts from logging in from foreign countries
- D. Configure a replacement remote-access tool for support cases.
- E. Purchase a password manager for remote-access tool users
- F. Enforce account lockouts after five bad password attempts

Answer: AF

Explanation:

The best ways to limit the bank's risk are to enable multifactor authentication for each support account and enforce account lockouts after five bad password attempts. Multifactor authentication adds an extra layer of security to the login process, making it more difficult for attackers to gain access to systems. Account lockouts after five bad password attempts can help to prevent brute force attacks by locking out accounts after a certain number of failed login attempts.

NEW QUESTION 224

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

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

Answer: C

Explanation:

Quarantining the infected system is the most appropriate way to remediate the issue of an infection that the antivirus software cannot remove. Quarantining means isolating the system from the network and other devices to prevent the infection from spreading or causing further damage. Quarantining also allows the technician to perform further analysis and removal of the infection without risking the security of other systems or data.

Some of the steps involved in quarantining an infected system are:

- ? Disconnect the system from the internet and any local network connections, such as Wi-Fi, Ethernet, Bluetooth, or USB.
- ? Disable any file-sharing or remote access services on the system, such as Windows File Sharing, Remote Desktop, or TeamViewer.
- ? Use a separate device to download and update the antivirus software and any other tools that may be needed to remove the infection, such as malware scanners, rootkit removers, or bootable rescue disks.
- ? Transfer the updated antivirus software and tools to the infected system using a removable media, such as a CD, DVD, or USB flash drive. Scan the removable media for any infections before and after using it on the infected system.
- ? Run the antivirus software and tools on the infected system and follow the instructions to delete or quarantine the infection. If the infection is persistent or complex, it may require booting the system from a rescue disk or using a Linux live disc to access and clean the system files.
- ? After the infection is removed, restore the system to a previous clean state using System Restore, backup, or recovery partition. Scan the system again to ensure that it is clean and secure. Reconnect the system to the network and update the system and the antivirus software.

References:

- ? How to Identify and Repair Malware or Virus Infected Computers, section 31
- ? Uninstalling Antivirus Software, the Clean Way: 40 Removal Tools & Instructions, section 22
- ? How to manually remove an infected file from a Windows computer³
- ? The Official CompTIA A+ Core 2 Study Guide (220-1102), page 2194

NEW QUESTION 227

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 230

An administrator is designing and implementing a server backup system that minimizes the capacity of storage used. Which of the following is the BEST backup

approach to use in conjunction with synthetic full backups?

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

Answer: D

Explanation:

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

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

NEW QUESTION 233

A user is trying to use proprietary software, but it crashes intermittently. The user notices that the desktop is displaying a "low memory" warning message. Upon restarting the desktop, the issue persists. Which of the following should a technician do next to troubleshoot the issue?

- A. Reimage the computer.
- B. Replace the system RAM.
- C. Reinstall and update the failing software.
- D. Decrease the page file size.

Answer: C

Explanation:

The most likely cause of the intermittent crashes is that the proprietary software is incompatible, outdated, or corrupted. Reinstalling and updating the software can fix these issues and ensure the software runs smoothly. Reimaging the computer or replacing the system RAM are too drastic and unnecessary steps. Decreasing the page file size can worsen the low memory problem and affect the performance of other applications.

NEW QUESTION 235

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

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

Answer: B

Explanation:

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

NEW QUESTION 239

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

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

Answer: B

Explanation:

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

? Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 13

? CompTIA A+ Complete Study Guide: Core 1 Exam 220-1101 and Core 2 Exam ..., page 103

NEW QUESTION 242

Maintaining the chain of custody is an important part of the incident response process. Which of the following reasons explains why this is important?

- A. To maintain an information security policy
- B. To properly identify the issue
- C. To control evidence and maintain integrity
- D. To gather as much information as possible

Answer: C

Explanation:

Maintaining the chain of custody is important to control evidence and maintain integrity. The chain of custody is a process that documents who handled, accessed, or modified a piece of evidence, when, where, how, and why. The chain of custody ensures that the evidence is preserved, protected, and authenticated throughout the incident response process. Maintaining the chain of custody can help prevent tampering, alteration, or loss of evidence, as well as establish its reliability and validity in legal proceedings. Maintaining an information security policy, properly identifying the issue, and gathering as much information as possible are not reasons why maintaining the chain of custody is important. Maintaining an information security policy is a general practice that defines the rules and guidelines for securing an organization's information assets and resources. Properly identifying the issue is a step in the incident response process that

involves analyzing and classifying the incident based on its severity, impact, and scope. Gathering as much information as possible is a step in the incident response process that involves collecting and documenting relevant data and evidence from various sources, such as logs, alerts, or witnesses. References:

? Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 26

NEW QUESTION 247

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

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

Answer: A

Explanation:

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

NEW QUESTION 250

Which of the following would MOST likely be used to change the security settings on a user's device in a domain environment?

- A. Security groups
- B. Access control list
- C. Group Policy
- D. Login script

Answer: C

Explanation:

Group Policy is the most likely tool to be used to change the security settings on a user's device in a domain environment. Group Policy is a feature of Windows that allows administrators to manage and configure settings for multiple devices and users in a centralized way. Group Policy can be used to enforce security policies such as password

complexity, account lockout, firewall rules, encryption settings, etc.

NEW QUESTION 253

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

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

Answer: B

Explanation:

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

NEW QUESTION 257

A technician needs to remotely connect to a Linux desktop to assist a user with troubleshooting. The technician needs to make use of a tool natively designed for Linux. Which of the following tools will the technician MOST likely use?

- A. VNC
- B. MFA
- C. MSRA
- D. RDP

Answer: A

Explanation:

The tool that the technician will most likely use to remotely connect to a Linux desktop is VNC. VNC stands for Virtual Network Computing and is a protocol that allows remote access and control of a graphical desktop environment over a network. VNC is natively designed for Linux and can also support other operating systems, such as Windows and Mac OS. VNC can be used to assist users with troubleshooting by viewing and interacting with their desktops remotely. MFA stands for Multi-Factor Authentication and is a method of verifying identity using two or more factors, such as something you know, something you have or something you are. MFA is not a tool that can be used to remotely connect to a Linux desktop but a technique that can be used to enhance security

for systems or services. MSRA stands for Microsoft Remote Assistance and is a feature that allows remote access and control of a Windows desktop environment over a network. MSRA is not natively designed for Linux and may not be compatible or supported by Linux systems. RDP stands for Remote Desktop Protocol and is a protocol that allows remote access and control of a Windows desktop environment over a network. RDP is not natively designed for Linux and may not be compatible or supported by Linux systems. References: CompTIA A+ Core 2 (220-1102) Certification Exam Objectives Version 4.0, Domain 1.6

NEW QUESTION 260

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

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

Answer: B

Explanation:

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

NEW QUESTION 264

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

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

Answer: C

Explanation:

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

NEW QUESTION 266

Which of the following physical security controls can prevent laptops from being stolen?

- A. Encryption
- B. LoJack
- C. Multifactor authentication
- D. Equipment lock
- E. Bollards

Answer: D

Explanation:

An equipment lock is a physical security device that attaches a laptop to a fixed object, such as a desk or a table, with a cable and a lock. This can prevent the laptop from being stolen by unauthorized persons. Encryption, LoJack, multifactor authentication and bollards are other security measures, but they do not physically prevent theft. Verified References: <https://www.comptia.org/blog/physical-security> <https://www.comptia.org/certifications/a>

NEW QUESTION 270

A technician has identified malicious traffic originating from a user's computer. Which of the following is the best way to identify the source of the attack?

- A. Investigate the firewall logs.
- B. Isolate the machine from the network.
- C. Inspect the Windows Event Viewer.
- D. Take a physical inventory of the device.

Answer: B

Explanation:

Isolating the machine from the network is the best way to identify the source of the attack, because it prevents the malicious traffic from spreading to other devices or reaching the attacker. Isolating the machine can also help preserve the evidence of the attack, such as the malware files, the network connections, the registry entries, or the system logs. By isolating the machine, a technician can safely analyze the machine and determine the source of the attack, such as a phishing email, a compromised website, a removable media, or a network vulnerability.

NEW QUESTION 272

A technician is troubleshooting boot times for a user. The technician attempts to use MSConfig to see which programs are starting with the OS but receives a message that it can no longer be used to view startup items. Which of the following programs can the technician use to view startup items?

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

Answer: D

Explanation:

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

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

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

NEW QUESTION 275

Which of the following operating systems is considered closed source?

- A. Ubuntu
- B. Android
- C. CentOS
- D. OSX

Answer: D

Explanation:

OSX (now macOS) is an operating system that is considered closed source, meaning that its source code is not publicly available or modifiable by anyone except its

developers. It is owned and maintained by Apple Inc. Ubuntu, Android and CentOS are operating systems that are considered open source, meaning that their source code is publicly available and modifiable by anyone who wants to contribute or customize them. Verified References:
<https://www.comptia.org/blog/open-source-vs-closed-source-software> <https://www.comptia.org/certifications/a>

NEW QUESTION 279

A large company is selecting a new Windows operating system and needs to ensure it has built-in encryption and endpoint protection. Which of the following Windows versions will MOST likely be selected?

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

Answer: D

Explanation:

When selecting a new Windows operating system for a large company that needs built-in encryption and endpoint protection, the Enterprise edition is the most likely choice. This edition provides advanced security features such as Windows Defender Advanced Threat Protection (ATP), AppLocker, and BitLocker Drive Encryption. These features can help to protect the company's data and endpoints against malware attacks, unauthorized access, and data theft. The Home and Pro editions of Windows do not include some of the advanced security features provided by the Enterprise edition, such as Windows Defender ATP and AppLocker. The Pro for Workstations edition is designed for high-performance and high-end hardware configurations, but it does not provide additional security features beyond those provided by the Pro edition.

NEW QUESTION 281

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

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

Answer: BD

Explanation:

Removing the applications from startup can improve the boot time of a PC by reducing the number of programs that load automatically when the PC starts. Some applications may add themselves to the startup list without the user's knowledge or

consent, which can slow down the PC's performance. Running the Disk Cleanup utility can also improve the boot time of a PC by deleting unnecessary or temporary files that take up disk space and affect the PC's speed. Disk Cleanup can also remove old system files that may cause conflicts or errors during booting. Installing additional RAM, installing a faster SSD, defragmenting the hard drive, and ending the processes in the Task Manager are not operations that would be best to do to resolve the issue of slow boot time at a minimal expense, as they may require purchasing new hardware or software, or may have negative impacts on other aspects of the PC's performance.

NEW QUESTION 285

A user is unable to log in to the network. The network uses 802.1X with EAP-TLS to authenticate on the wired network. The user has been on an extended leave and has not logged in to the computer in several months. Which of the following is causing the login issue?

- A. Expired certificate
- B. OS update failure
- C. Service not started
- D.

Application crash

E. Profile rebuild needed

Answer: A

Explanation:

EAP-TLS is a method of authentication that uses certificates to establish a secure tunnel between the client and the server³. The certificates have a validity period and must be renewed before they expire¹. If the user has been on an extended leave and has not logged in to the computer in several months, it is possible that the certificate on the client or the server has expired and needs to be renewed². The other options are not directly related to EAP-TLS authentication or 802.1X network access.

NEW QUESTION 286

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

220-1102 Practice Exam Features:

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

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