# CompTIA

## Exam Questions 220-1102

CompTIA A+ Certification Exam: Core 2

**NEW QUESTION 1**
After a failed update, an application no longer launches and generates the following error message: Application needs to be repaired. Which of the following Windows 10 utilities should a technician use to address this concern?

A. Device Manager
B. Administrator Tools
C. Programs and Features
D. Recovery

**Answer:** D

**Explanation:**
Recovery is a Windows 10 utility that can be used to address the concern of a failed update that prevents an application from launching. Recovery allows the user to reset the PC, go back to a previous version of Windows, or use advanced startup options to troubleshoot and repair the system2. Device Manager, Administrator Tools, and Programs and Features are not Windows 10 utilities that can fix a failed update.

**NEW QUESTION 2**
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 3**
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 4**
When trying to access a secure internal network, the user receives an error messaging stating, "There is a problem with this website's security certificate." The user reboots the desktop and tries to access the website again, but the issue persists. Which of the following should the user do to prevent this error from reoccurring?

A. Reimage the system and install SSL.
B. Install Trusted Root Certificate.
C. Select View Certificates and then Install Certificate.
D. Continue to access the website.

**Answer:** C

**Explanation:**
The error message indicates that the website’s security certificate is not trusted by the user’s device, which may prevent the user from accessing the secure internal network. To resolve this issue, the user can view the certificate details and install it on the device, which will add it to the trusted root certificate store. Reimaging the system and installing SSL, installing Trusted Root Certificate, or continuing to access the website are not recommended solutions, as they may compromise the security of the device or the network.

**NEW QUESTION 5**
A developer receives the following error while trying to install virtualization software on a workstation:
VTx not supported by system
Which of the following upgrades will MOST likely fix the issue?

A. Processor
B. Hard drive

C Memory
D: Video card

**Answer:** A

**Explanation:**
The processor is the component that determines if the system supports virtualization technology (VTx), which is required for running virtualization software. The hard drive, memory and video card are not directly related to VTx support, although they may affect the performance of the virtual machines. Verified References: https://www.comptia.org/blog/what-is-virtualization https://www.comptia.org/certifications/a

**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**
A technician is upgrading the backup system for documents at a high-volume law firm. The current backup system can retain no more than three versions of full backups before failing. The law firm is not concerned about restore times but asks the technician to retain more versions when possible. Which of the following backup methods should the technician MOST likely implement?

A. Full
B. Mirror
C. Incremental
D. Differential

**Answer:** C

**Explanation:**
Incremental backup is a backup method that only backs up the files that have changed since the last backup, whether it was a full or an incremental backup. Incremental backup can save storage space and bandwidth, as it does not copy the same files over and over again. Incremental backup can also retain more versions of backups, as it only stores the changes made to the files. However, incremental backup can have longer restore times, as it requires restoring the last full backup and all the subsequent incremental backups in order to recover the data. The law firm is not concerned about restore times but asks the technician to retain more versions when possible, so incremental backup would be a suitable choice for them.

**NEW QUESTION 8**
A user reports a computer is running slow. Which of the following tools will help a technician identity the issued

A. Mastered
B. Not Mastered

**Answer:** A

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

**NEW QUESTION 9**
A customer installed a new web browser from an unsolicited USB drive that the customer received in the mail. The browser is not working as expected, and internet searches are redirected to another site. Which of the following should the user do next after uninstalling the browser?

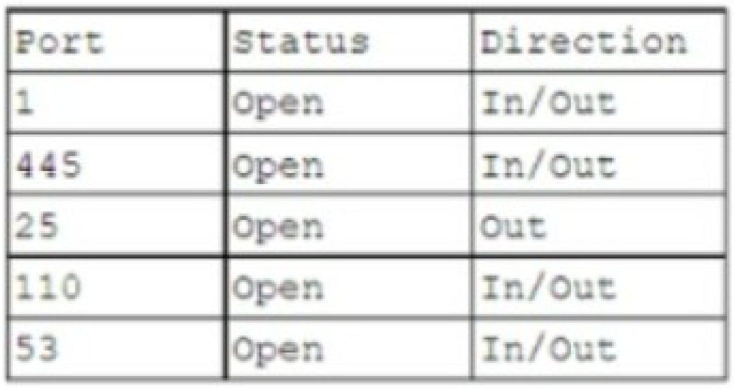
A. Delete the browser cookies and history.
B. Reset all browser settings.
C. Change the browser default search engine.
D. Install a trusted browser.

**Answer:** D

**Explanation:**
The customer's web browser is likely infected by a browser hijacker, which is a type of malware that changes the browser's settings and redirects the user to malicious websites. A browser hijacker can also steal the user's personal data, display unwanted ads, and install more malware on the device. To remove a browser hijacker, the user should first uninstall the browser from the Control Panel, then scan the device with an antivirus or anti-malware program, and finally install a trusted browser from a legitimate source. Deleting the browser cookies and history, resetting the browser settings, or changing the browser default search engine may not be enough to get rid of the browser hijacker, as it may have embedded itself into the system or other browser components.

**NEW QUESTION 10**

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 10**
A technician installs specialized software on a workstation. The technician then attempts to run the software. The workstation displays a message indicating the software is not authorized to run. Which of the following should the technician do to most likely resolve the issue?

A. Install the software in safe mode.
B. Attach the external hardware token.
C. Install OS updates.
D. Restart the workstation after installation.

**Answer:** B

**Explanation:**
A hardware token is a physical device that provides an additional layer of security for software authorization. Some specialized software may require a hardware token to be attached to the workstation in order to run. A hardware token may contain a cryptographic key, a password, or a one-time code that verifies the user's identity or permission. Installing the software in safe mode, installing OS updates, and restarting the workstation after installation are not likely to resolve the issue of software authorization.

**NEW QUESTION 12**
A user is unable to access files on a work PC after opening a text document. The text document was labeled "URGENT PLEASE READ.txt - In active folder, .txt file titled urgent please read". Which of the following should a support technician do FIRST?

A. Quarantine the host in the antivirus system.
B. Run antivirus scan tor malicious software.
C. Investigate how malicious software was Installed.
D. Reimage the computer.

**Answer:** B

**Explanation:**
Running an antivirus scan for malicious software is the first step that a support technician should do when a user reports a virus on a PC. The antivirus scan can detect and remove the virus, as well as prevent further damage or infection. Quarantining the host, investigating how the malware was installed and reimaging the computer are possible steps that can be done after running the antivirus scan, depending on the situation and the results of the scan. Verified References: https://www.comptia.org/blog/how-to- remove-a-virus https://www.comptia.org/certifications/a

**NEW QUESTION 14**
A remote user is experiencing issues connecting to a corporate email account on a laptop. The user clicks the internet connection icon and does not recognize the connected Wi-Fi. The help desk technician, who is troubleshooting the issue, assumes this is a rogue access point. Which of the following is the first action the technician should take?

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

**Answer:** C

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

**NEW QUESTION 18**
A user reports a PC is running slowly. The technician suspects it has a badly fragmented hard drive. Which of the following tools should the technician use?

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

**Answer:** C

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

**NEW QUESTION 21**
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. ext3
B. FAT32
C. exFAT
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 24**
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 27**
Which of the following filesystem formats would be the BEST choice to ensure read and write compatibility of USB flash drives across several generations of Microsoft operating systems?

A. APFS
B. ext4
C. CDFS
D. FAT32

**Answer:** D

**Explanation:**
The best filesystem format to ensure read and write compatibility of USB flash drives across several generations of Microsoft operating systems is FAT32. FAT32 stands for File Allocation Table 32-bit and is a filesystem format that organizes and manages files and folders on storage devices using 32-bit clusters. FAT32 is compatible with most Microsoft operating systems since Windows 95 OSR2, as well as other operating systems such as Linux and Mac OS X. FAT32 can support storage devices up to 2TB in size and files up to 4GB in size. APFS stands for Apple File System and is a filesystem format that organizes and manages files and folders on storage devices using encryption, snapshots and cloning features. APFS is compatible with Mac OS X 10.13 High Sierra and later versions but not with Microsoft operating systems natively. Ext4 stands for Fourth Extended File System and is a filesystem format that organizes and manages files and folders on storage devices using journaling, extents and delayed allocation features. Ext4 is compatible with Linux operating systems but not with Microsoft operating systems natively.

**NEW QUESTION 29**
A user is having phone issues after installing a new application that claims to optimize performance. The user downloaded the application directly from the vendor's website and is now experiencing high network utilization and is receiving repeated security warnings. Which of the following should the technician perform FIRST to mitigate the issue?

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

**Answer:** B

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

**NEW QUESTION 33**
A technician installed a new application on a workstation. For the program to function
properly, it needs to be listed in the Path Environment Variable. Which of the following Control Panel utilities should the technician use?

A. System
B. Indexing Options
C. Device Manager
D. Programs and Features

**Answer:** A

**Explanation:**
System is the Control Panel utility that should be used to change the Path Environment Variable. The Path Environment Variable is a system variable that specifies the directories where executable files are located. To edit the Path Environment Variable, the technician should go to System > Advanced system settings > Environment Variables and then select Path from the list of system variables and click Edit.

**NEW QUESTION 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 39**
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 43**

A user connected a smartphone to a coffee shop's public Wi-Fi and noticed the smartphone started sending unusual SMS messages and registering strange network activity A technician thinks a virus or other malware has infected the device. Which of the following should the technician suggest the user do to best address these security and privacy concerns? (Select two).

A. Disable Wi-Fi autoconnect.
B. Stay offline when in public places.
C. Uninstall all recently installed applications.
D. Schedule an antivirus scan.
E. Reboot the device
F. Update the OS

**Answer:** CD

**Explanation:**
The best way to address the security and privacy concerns caused by a malware infection on a smartphone is to uninstall all recently installed applications and schedule an antivirus scan. Uninstalling the applications that may have introduced the malware can help remove the source of infection and prevent further damage. Scheduling an antivirus scan can help detect and remove any remaining traces of malware and restore the device’s functionality. References: CompTIA A+ Core 2 (220-1102) Certification Study Guide, Chapter 5: Mobile Devices, Section 5.3: Mobile Device Security1

**NEW QUESTION 48**

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 52**

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

A. Disk Cleanup
B. Resource Monitor
Disk Defragment
C
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 57**

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 60**

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 63**
A technician is creating a tunnel that hides IP addresses and secures all network traffic. Which of the following protocols is capable of enduring enhanced security?

A. DNS
B. IPS
C. VPN
D. SSH

**Answer:** C

**Explanation:**
A VPN (virtual private network) is a protocol that creates a secure tunnel between two devices over the internet, hiding their IP addresses and encrypting their traffic. DNS (domain name system) is a protocol that translates domain names to IP addresses. IPS (intrusion prevention system) is a device that monitors and blocks malicious network traffic. SSH (secure shell) is a protocol that allows remote access and command execution on another device. Verified References: https://www.comptia.org/blog/what-is-a-vpn
https://www.comptia.org/certifications/a

**NEW QUESTION 68**
A technician suspects the boot disk of a user's computer contains bad sectors. Which of the following should the technician verify in the command prompt to address the issue without making any changes?

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

**Answer:** C

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

**NEW QUESTION 73**
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 78**
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 (220-1002) Certification Exam Objectives Version 4.0, Domain 3.3

**NEW QUESTION 80**
A systems administrator is experiencing Issues connecting from a laptop to the corporate network using PKI. Which to the following tools can the systems administrator use to help remediate the issue?

A. certmgr.msc
B. msconfig.exe
C. lusrmgr.msc
D. perfmon.msc

**Answer:** A

**Explanation:**
certmgr.msc is a tool that can be used to troubleshoot issues with PKI (public key infrastructure) on a Windows machine. It allows a system administrator to view, manage and import certificates, as well as check their validity, expiration and revocation status. msconfig.exe, lusrmgr.msc and perfmon.msc are other tools that can be used for different purposes on a Windows machine, but they are not related to PKI. Verified References: https://www.comptia.org/blog/what-is-certmgr-msc https://www.comptia.org/certifications/a

**NEW QUESTION 82**
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 87**
A user's mobile phone has become sluggish A systems administrator discovered several malicious applications on the device and reset the phone. The administrator installed MDM software. Which of the following should the administrator do to help secure the device against this threat in the future? (Select TWO).

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

**Answer:** CE

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

**NEW QUESTION 88**
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 93**
While trying to repair a Windows 10 OS, a technician receives a prompt asking for a key. The technician tries the administrator password, but it is rejected. Which of the following does the technician need in order to continue the OS repair?

A. SSL key
B. Preshared key
C. WPA2 key
D. Recovery key

**Answer:** D

**Explanation:**
A recovery key is a code that can be used to unlock a BitLocker-encrypted drive when the normal authentication methods (such as password or PIN) are not available or have been forgotten. BitLocker is a feature of Windows that encrypts the entire drive to protect data from unauthorized access. If a technician is trying to repair a Windows 10 OS that has BitLocker enabled, they will need the recovery key to access the drive and continue the OS repair. SSL key, preshared key, and WPA2 key are not keys that are related to BitLocker or OS repair.

**NEW QUESTION 97**
Which of the following filesystems replaced FAT as the preferred filesystem for Microsoft Windows OS?

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

**Answer:** C

**Explanation:**
NTFS stands for New Technology File System and it is the preferred filesystem for Microsoft Windows OS since Windows NT 3.1 in 19931. NTFS replaced FAT (File Allocation Table) as the default filesystem for Windows because it offers many advantages over FAT, such as:
? Support for larger volumes and files (up to 16 exabytes)2
? Support for file compression, encryption, and permissions2
? Support for journaling, which records changes to the filesystem and helps recover from errors2
? Support for hard links, symbolic links, and mount points2
? Support for long filenames and Unicode characters2
FAT32 is an improved version of FAT that supports larger volumes and files (up to 32 GB and 4 GB respectively) and is compatible with older versions of Windows and other operating systems3. However, FAT32 still has many limitations and drawbacks compared
to NTFS, such as:
? No support for file compression, encryption, and permissions3
? No support for journaling, which makes it vulnerable to corruption and data loss3
? No support for hard links, symbolic links, and mount points3
? No support for long filenames and Unicode characters3
APFS (Apple File System) is the default filesystem for macOS, iOS, iPadOS, watchOS, and tvOS since 20174. APFS replaced HFS+ (Hierarchical File System Plus) as the preferred filesystem for Apple devices because it offers many advantages over HFS+, such as:
? Support for larger volumes and files (up to 8 zettabytes)4
? Support for file cloning, snapshots, and encryption4
? Support for space sharing, which allows multiple volumes to share the same storage pool4
? Support for fast directory sizing, which improves performance and efficiency4 ext4 (Fourth Extended Filesystem) is the default filesystem for most Linux distributions since 20085. ext4 replaced ext3 as the preferred filesystem for Linux because it offers many advantages over ext3, such as:
? Support for larger volumes and files (up to 1 exabyte and 16 terabytes respectively)5
? Support for extents, which reduce fragmentation and improve performance5
? Support for journal checksumming, which improves reliability and reduces recovery time5
? Support for delayed allocation, which improves efficiency and reduces metadata overhead5
References:
1: NTFS - Wikipedia 2: [NTFS vs FAT32 vs exFAT: What's the Difference?] 3: [FAT32 - Wikipedia] 4: [Apple File System - Wikipedia] 5: [ext4 - Wikipedia] : NTFS vs FAT32 vs exFAT: What's the Difference? : FAT32 - Wikipedia : Apple File System - Wikipedia : ext4 - Wikipedia

**NEW QUESTION 99**
A user calls the help desk to report that none of the files on a PC will open. The user also indicates a program on the desktop is requesting payment in exchange for file access A technician verifies the user's PC is infected with ransorrrware. Which of the following should the technician do FIRST?

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

**Answer:** C

**Explanation:**
The technician should quarantine the system first1 Reference:
CompTIA A+ Certification Exam: Core 2 Objectives Version 4.0. Retrieved from https://partners.comptia.org/docs/default-source/resources/comptia-a-220-1102-exam- objectives-(3-0)

**NEW QUESTION 101**
An IT security team is implementing a new Group Policy that will return a computer to the login after three minutes. Which of the following BEST describes the

change in policy?

A. Login times
B. Screen lock
C. User permission
D. Login lockout attempts

**Answer:** B

**Explanation:**
Screen lock is a feature that returns a computer to the login screen after a period of inactivity, requiring the user to enter their credentials to resume their session. Screen lock can be configured using Group Policy settings, such as Screen saver timeout and Interactive logon: Machine inactivity limit. Screen lock can help prevent unauthorized access to a computer when the user is away from their desk. Login times are not a feature that returns a computer to the login screen, but a measure of how long it takes for a user to log in to a system. User permission is not a feature that returns a computer to the login screen, but a set of rights and privileges that determine what a user can do on a system. Login lockout attempts are not a feature that returns a computer to the login screen, but a security policy that locks out a user account after a number of failed login attempts. https://woshub.com/windows-lock-screen-after-idle-via-gpo/

**NEW QUESTION 105**
A company is experiencing a DDoS 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. Ransomware
F. Spyware

**Answer:** AD

**Explanation:**
Zombies and botnets are terms that describe the types of infections that can cause internal workstations to participate in a DDoS (distributed denial-of-service) attack. A DDoS attack is a malicious attempt to disrupt the normal functioning of a website or a network by overwhelming it with a large amount of traffic from multiple sources. Zombies are infected computers that are remotely controlled by hackers without the owners' knowledge or consent. Botnets are networks of zombies that are coordinated by hackers to launch DDoS attacks or other malicious activities. Keylogger, adware, ransomware, and spyware are not types of infections that can cause internal workstations to participate in a DDoS attack.

**NEW QUESTION 110**
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

**NEW QUESTION 113**
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 116**
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 121**
A help desk technician determines a motherboard has failed. Which of the following is the most logical next step in the remediation process?

A. Escalating the issue to Tier 2
B. Verifying warranty status with the vendor
C. Replacing the motherboard
D. Purchasing another PC

**Answer:** B

**Explanation:**
Verifying warranty status with the vendor is the most logical next step in the remediation process after determining that a motherboard has failed. A warranty is a guarantee from the vendor that covers the repair or replacement of defective or faulty products within a specified period of time. Verifying warranty status with the vendor can help the technician determine if the motherboard is eligible for warranty service and what steps to take to obtain it. Escalating the issue to Tier 2, replacing the motherboard, and purchasing another PC are not the most logical next steps in the remediation process.

**NEW QUESTION 126**
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 128**
Which of the following options should MOST likely be considered when preserving data from a hard drive for forensic analysis? (Select TWO).

A. Licensing agreements
B. Chain of custody
C. Incident management documentation
D. Data integrity
E. Material safety data sheet
F. Retention requirements

**Answer:** B

**Explanation:**
Chain of custody and data integrity are two options that should most likely be considered when preserving data from a hard drive for forensic analysis. Chain of custody refers to the documentation and tracking of who has access to the data and how it is handled, stored, and transferred. Data integrity refers to the assurance that the data has not been altered, corrupted, or tampered with during the preservation process

**NEW QUESTION 132**
The findings from a security audit indicate the risk of data loss from lost or stolen laptops is high. The company wants to reduce this risk with minimal impact to users who want to use their laptops when not on the network. Which of the following would BEST reduce this risk for Windows laptop users?

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

**Answer:** D

**Explanation:**
BitLocker is a disk encryption tool that can be used to encrypt the hard drive of a Windows laptop. This will protect the data stored on the drive in the event that the

laptop is lost or stolen, and will help to reduce the risk of data loss. Additionally, BitLocker can be configured to require a PIN or other authentication in order to unlock the drive, providing an additional layer of security.

**NEW QUESTION 133**
A user's corporate phone was stolen, and the device contains company trade secrets. Which of the following technologies should be implemented to mitigate this risk? (Select TWO).

A. Remote wipe
B. Firewall
C. Device encryption
D. Remote backup
E. Antivirus
F. Global Positioning System

**Answer:** AC

**Explanation:**
Remote wipe is a feature that allows data to be deleted from a device or system remotely by an administrator or owner1. It is used to protect data from being compromised if the device is lost, stolen, or changed hands1. Device encryption is a feature that helps protect the data on a device by making it unreadable to unauthorized users2. It requires a key or a password to access the data2. Both features can help mitigate the risk of losing company trade secrets if a corporate phone is stolen.
References: 1: How to remote wipe Windows laptop (https://www.thewindowsclub.com/remote-wipe-windows-10) 2: Device encryption in Windows (https://support.microsoft.com/en-us/windows/device-encryption-in-windows-ad5dcf4b-dbe0-2331-228f-7925c2a3012d)

**NEW QUESTION 138**
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 141**
A technician is troubleshooting a customer's PC and receives a phone call. The technician does not take the call and sets the phone to silent. Which of the following BEST describes the technician's actions?

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

**Answer:** A

**Explanation:**
The technician has taken the appropriate action by not taking the call and setting the phone to silent in order to avoid any distractions and remain focused on the task at hand. This is a good example of how to maintain focus and productivity when working on a customer's PC, and will help to ensure that the job is completed in a timely and efficient manner.

**NEW QUESTION 144**
A user wants to set up speech recognition on a PC. In which of the following Windows Settings tools can the user enable this option?

A. Language
B. System
C. Personalization
D. Ease of Access

**Answer:** D

**Explanation:**
The user can enable speech recognition on a PC in the Ease of Access settings tool. To set up Speech Recognition on a Windows PC, the user should open Control Panel, click on Ease of Access, click on Speech Recognition, and click the Start Speech Recognition link. Language settings can be used to change the language of the speech recognition feature, but they will not enable the feature. System settings can be used to configure the hardware and software of the PC, but they will not enable the speech
recognition feature. Personalization settings can be used to customize the appearance and behavior of the PC, but they will not enable the speech recognition feature1
Open up ease of access, click on speech, then there is an on and off button for speech recognition.

**NEW QUESTION 147**
A company is experiencing a ODDS attack. Several internal workstations are the source of the traffic Which of the following types of infections are the workstations

most likely experiencing? (Select two)

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

**Answer:** AD

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

**NEW QUESTION 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 156**
A user contacts a technician about an issue with a laptop. The user states applications open without being launched and the browser redirects when trying to go to certain websites. Which of the following is MOST likely the cause of the user's issue?

A. Keylogger
B. Cryptominers
C. Virus
D. Malware

**Answer:** D

**Explanation:**
The most likely cause of the user’s issue of applications opening without being launched and browser redirects when trying to go to certain websites is malware. Malware is a general term that refers to any software or code that is malicious or harmful to a computer or system. Malware can perform various unwanted or unauthorized actions on a computer or system, such as opening applications, redirecting browsers, displaying ads, stealing data, encrypting files or damaging hardware. Malware can infect a computer or system through various means, such as email attachments, web downloads, removable media or network connections. Keylogger is a type of malware that records and transmits the keystrokes made by a user on a keyboard. Keylogger can be used to steal personal or sensitive information, such as passwords, credit card numbers or chat messages. Keylogger does not typically open applications or redirect browsers but only captures user inputs. Cryptominers are a type of malware that use the computing resources of a computer or system to mine cryptocurrency, such as Bitcoin or Ethereum. Cryptominers can degrade the performance and increase the power consumption of a computer or system. Cryptominers do not typically open applications or redirect browsers but only consume CPU or GPU cycles. Virus is a type of malware that infects and replicates itself on other files or programs on a computer or system.

**NEW QUESTION 160**
A technician, who is working at a local office, has found multiple copies of home edition software installed on computers. Which of the following does this MOST likely violate?

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

**Answer:** A

**Explanation:**
The installation of home edition software on computers at a local office most likely violates the EULA. EULA stands for End User License Agreement and is a legal contract that specifies the terms and conditions for using a software product or service. EULA typically covers topics such as license scope, duration and limitations, rights and obligations of the parties, warranties and disclaimers, liability and indemnity clauses, and termination procedures. EULA may also restrict the use of home edition software to personal or non- commercial purposes only, and prohibit the use of home edition software in business or professional settings. Violating EULA may result in legal actions or penalties from the software vendor or developer. PII stands for Personally Identifiable Information and is any

information that can be used to identify or locate an individual, such as name, address, phone number, email address, social security number or credit card number. PII is not related to software installation or licensing but to data protection and privacy. DRM stands for Digital Rights Management and is a technology that controls or restricts the access and use of digital content, such as music, movies, books or games. DRM is not related to software installation or licensing but to content distribution and piracy prevention. Open- source agreement is a type of license that allows users to access, modify and distribute the source code of a software product or service freely and openly. Open-source agreement does not restrict the use of software to home edition only but encourages collaboration and innovation among developers and users. References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 5.1

**NEW QUESTION 165**
A user reports that the hard drive activity light on a Windows 10 desktop computer has been steadily lit for more than an hour, and performance is severely degraded. Which of the following tabs in Task Manager would contain the information a technician would use to identify the cause of this issue?

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

**Answer:** B

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

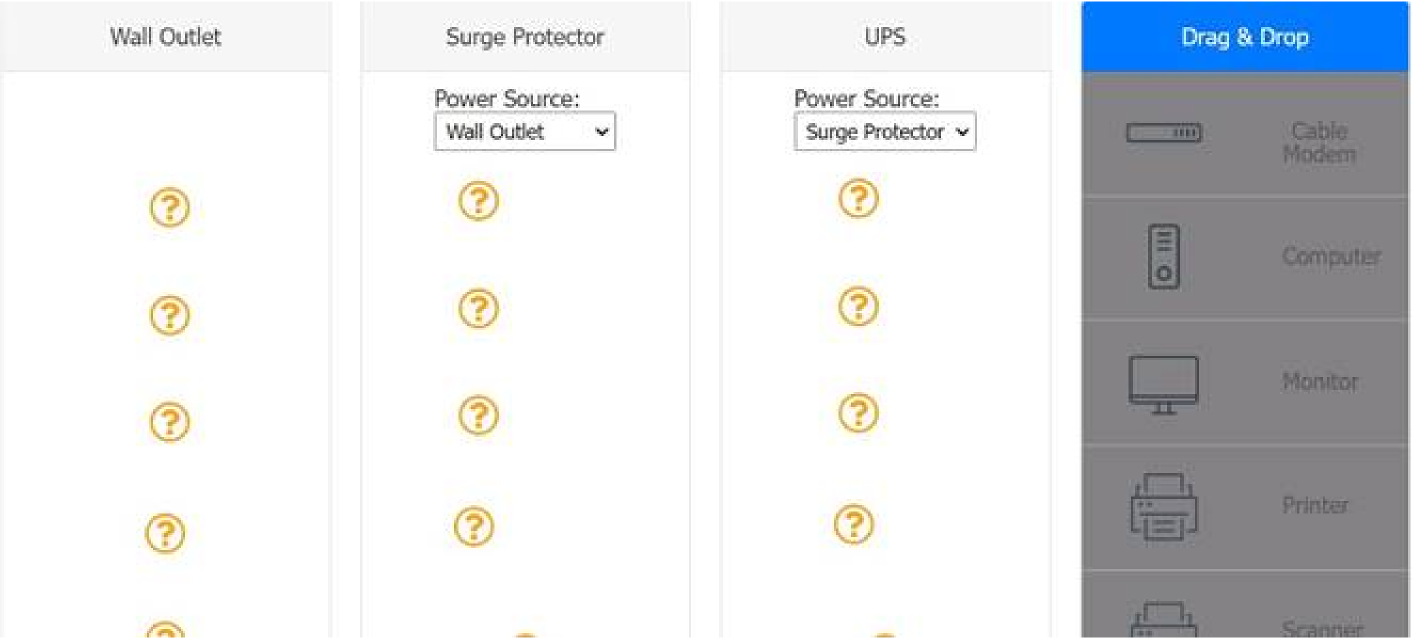
**NEW QUESTION 168**
A technician is unable to completely start up a system. The OS freezes when the desktop background appears, and the issue persists when the system is restarted. Which of the following should the technician do next to troubleshoot the issue?

A. Disable applicable BIOS options.
B. Load the system in safe mode.
C. Start up using a flash drive OS and run System Repair.
D. Enable Secure Boot and reinstall the system.

**Answer:** B

**Explanation:**
Loading the system in safe mode is a common troubleshooting step that allows the technician to isolate the problem by disabling unnecessary drivers and services. This can help determine if the issue is caused by a faulty device, a corrupted system file, or a malware infection.

**NEW QUESTION 173**
DRAG DROP
A customer recently experienced a power outage at a SOHO. The customer does not think the components are connected properly. A print job continued running for several minutes after the power failed, but the customer was not able to interact with the computer. Once the UPS stopped beeping, all functioning devices also turned off. In case of a future power failure, the customer wants to have the most time available to save cloud documents and shut down the computer without losing any data.


Surge Protector: Power Source: Wall Outlet
UPS: Power Source: Surge Protector

A. Mastered
B. Not Mastered

**Answer:** A

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

**NEW QUESTION 178**
A Windows workstation that was recently updated with approved system patches shut down instead of restarting. Upon reboot, the technician notices an alert stating the workstation has malware in the root OS folder. The technician promptly performs a System Restore and reboots the workstation, but the malware is still detected. Which of the following BEST describes why the system still has malware?

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

**Answer:** D

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

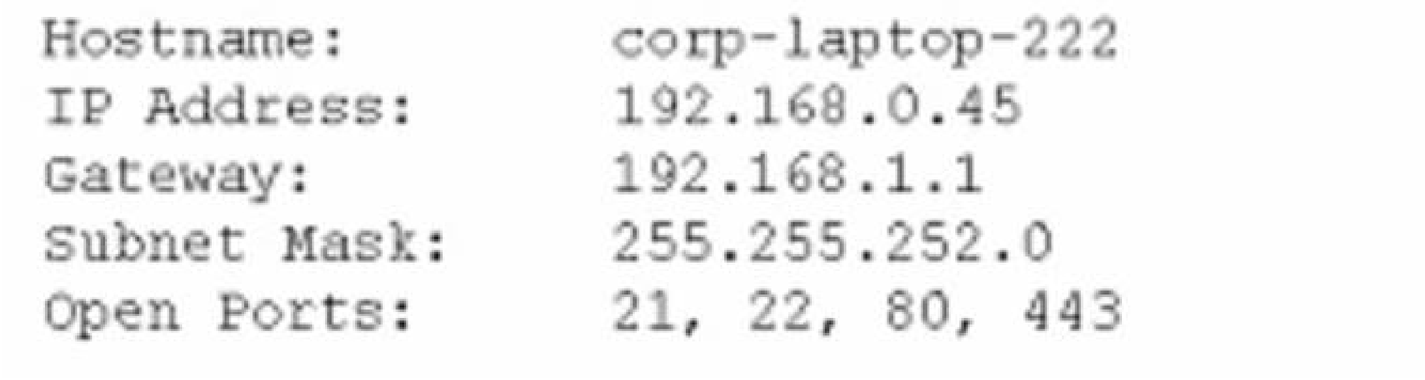
**NEW QUESTION 182**
A technician is unable to access the internet or named network resources. The technician receives a valid IP address from the DHCP server and can ping the default gateway. Which of the following should the technician check next to resolve the issue?

A. Verify the DNS server settings.
B. Turn off the Windows firewall.
C. Confirm the subnet mask is correct.
D. Configure a static IP address.

**Answer:** A

**Explanation:**
The correct answer is A. Verify the DNS server settings. This is because the DNS server is responsible for resolving domain names to IP addresses, which is necessary for accessing the internet or named network resources. If the DNS server settings are incorrect or the DNS server is down, the technician will not be able to access these resources even if they have a valid IP address and can ping the default gateway1.
1: CompTIA A+ Certification Exam: Core 2 Objectives, page 16, section 1.10.

**NEW QUESTION 184**
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 188**
The screen on a user's mobile device is not autorotating even after the feature has been enabled and the device has been restarted. Which of the following should the technician do next to troubleshoot the issue?

A. Calibrate the phone sensors.
B. Enable the touch screen.

C. Reinstall the operating system.
D. Replace the screen.

**Answer:** A

**Explanation:**
Calibrating the phone sensors is a step that can troubleshoot the issue of screen not autorotating on a mobile device. Screen autorotation is a feature that automatically adjusts the screen orientation based on the device's position and movement. Screen autorotation relies on sensors such as accelerometer and gyroscope to detect the device's tilt and rotation. Calibrating the phone sensors can help fix any errors or inaccuracies in the sensor readings that may prevent screen autorotation from working properly. Enabling the touch screen, reinstalling the operating system, and replacing the screen are not steps that should be done next to troubleshoot this issue.

**NEW QUESTION 190**
A user's smartphone data usage is well above average. The user suspects an installed application is transmitting data in the background. The user would like to be alerted when an application attempts to communicate with the internet. Which of the following BEST addresses the user's concern?

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

**Answer:** D

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

**NEW QUESTION 193**
A company is recycling old hard drives and wants to quickly reprovision the drives for reuse. Which of the following data destruction methods should the company use?

A. Degaussing
B. Standard formatting
C. Low-level wiping
D. Deleting

**Answer:** C

**Explanation:**
Low-level wiping is the best data destruction method for recycling old hard drives for reuse. Low-level wiping is a process that overwrites every bit of data on a drive with zeros or random patterns, making it impossible to recover any data from the drive. Low-level wiping also restores the hard drive to its factory state, removing any bad sectors or errors that may have accumulated over time. Low-level wiping can be done using specialized software tools or hardware devices that connect to the drive. Degaussing, standard formatting, and deleting are not suitable data destruction methods for recycling old hard drives for reuse. Degaussing is a process that exposes a hard drive to a strong magnetic field, destroying both the data and the drive itself. Degaussing renders the drive unusable for reuse. Standard formatting is a process that erases the data on a hard drive by removing the file system structure, but it does not overwrite the data itself. Standard formatting leaves some data recoverable using forensic tools or software utilities. Deleting is a process that removes the data from a hard drive by marking it as free space, but it does not erase or overwrite the data itself. Deleting leaves most data recoverable using undelete tools or software utilities.
References:
? Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 15
? CompTIA A+ Complete Study Guide: Core 1 Exam 220-1101 and Core 2 Exam …, page 105

**NEW QUESTION 196**
Which of the following must be maintained throughout the forensic evidence life cycle when dealing with a piece of evidence?

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

**Answer:** B

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

**NEW QUESTION 197**
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 200**
A user wants to back up a Windows 10 device. Which of the following should the user select?

A. Devices and Printers
B. Email and Accounts
C. Update and Security
D. Apps and Features

**Answer:** C

**Explanation:**
Update and Security is the section in Windows 10 Settings that allows the user to back up their device. Backing up a device means creating a copy of the data and settings on the device and storing it in another location, such as an external drive or a cloud service. Backing up a device can help the user restore their data and settings in case of data loss, corruption, or theft. Devices and Printers, Email and Accounts, and Apps and Features are not sections in Windows 10 Settings that allow the user to back up their device.

**NEW QUESTION 202**
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 204**
A technician is setting up a newly built computer. Which of the following is the fastest way for the technician to install Windows 10?

A. Factory reset
B. System Restore
C. In-place upgrade
D. Unattended installation

**Answer:** D

**Explanation:**
Windows 10

The correct answer is D. Unattended installation. An unattended installation is a way of installing Windows 10 without requiring any user input or interaction. It uses a configuration file called answer file that contains the settings and preferences for the installation, such as the product key, language, partition, and network settings. An unattended installation can be performed by using a bootable USB flash drive or DVD that contains the Windows 10 installation files and the answer file1. This is the fastest way for the technician to install Windows 10 on a newly built computer, as it automates the whole process and saves time. A factory reset is a way of restoring a computer to its original state by deleting all the data and applications and reinstalling the operating system. A factory reset can be performed by using the recovery partition or media that came with the computer, or by using the Reset this PC option in Windows 10 settings2. A factory reset is not a way of installing Windows 10 on a newly built computer, as it requires an existing operating system to be present.
A system restore is a way of undoing changes to a computer's system files and settings by using a restore point that was created earlier. A system restore can be performed by using the System Restore option in Windows 10 settings or by using the Advanced Startup Options menu3. A system restore is not a way of installing Windows 10 on a newly built computer, as it requires an existing operating system and restore points to be present.
An in-place upgrade is a way of upgrading an existing operating system to a newer version without losing any data or applications. An in-place upgrade can be performed by using the Windows 10 Media Creation Tool or by running the Setup.exe file from the Windows 10 installation media. An in-place upgrade is not a way of installing Windows 10 on a newly built computer, as it requires an existing operating system to be present.

**NEW QUESTION 208**
An Android user reports that when attempting to open the company's proprietary mobile application it immediately doses. The user states that the issue persists, even after rebooting the phone. The application contains critical information that cannot be lost. Which of the following steps should a systems administrator attempt FIRST?

A. Mastered
B. Not Mastered

**Answer:** A

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

**NEW QUESTION 209**
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 213**
A systems administrator is tasked with configuring desktop systems to use a new proxy server that the organization has added to provide content filtering. Which of the following Windows utilities IS the BEST choice for accessing the necessary configuration to complete this goal?

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

**Answer:** D

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

**NEW QUESTION 215**
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 216**
A company-owned mobile device is displaying a high number of ads, receiving data-usage limit notifications, and experiencing slow response. After checking the device, a technician notices the device has been jailbroken. Which of the following should the technician do next?

A. Run an antivirus and enable encryption.
Restore the defaults and reimage the corporate OS.
B.
C. Back up the files and do a system restore.
D. Undo the jailbreak and enable an antivirus.

**Answer:** B

**Explanation:**
Jailbreaking a device exposes it to various security risks, such as malware, data theft, network attacks, and service disruption1234. Running an antivirus and enabling encryption may not be enough to remove the threats and restore the device's functionality. Undoing the jailbreak may not be possible or effective, depending on the method used. Backing up the files and doing a system restore may preserve the jailbreak and the associated problems. The best option is to erase the device and reinstall the original operating system that is compatible with the corporate policies and standards. This will ensure that the device is clean, secure, and compliant25.

References: 1 What is Jailbreaking & Is it safe? - Kaspersky(https://www.kaspersky.com/resource-center/definitions/what-is- jailbreaking). 2 Jailbreak Detection: Why is jailbreaking a potential security risk? - Cybersecurity ASEE(https://cybersecurity.asee.co/blog/what-is-jailbreaking/). 3 Jailbreaking Information for iOS Devices | University IT(https://uit.stanford.edu/service/mydevices/jailbreak)4 What does it mean to jailbreak your phone—and is it legal? - Microsoft(https://www.microsoft.com/en-us/microsoft-365-life- hacks/privacy-and-safety/what-is-jailbreaking-a-phone). 5 Resetting a corporate laptop back to a personal laptop… Enterprise vs Pro - Windows 10(https://community.spiceworks.com/topic/2196812-resetting-a-corporate-laptop-back-to-a-personal-laptop-enterprise-vs-pro).

**NEW QUESTION 218**

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 220**

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

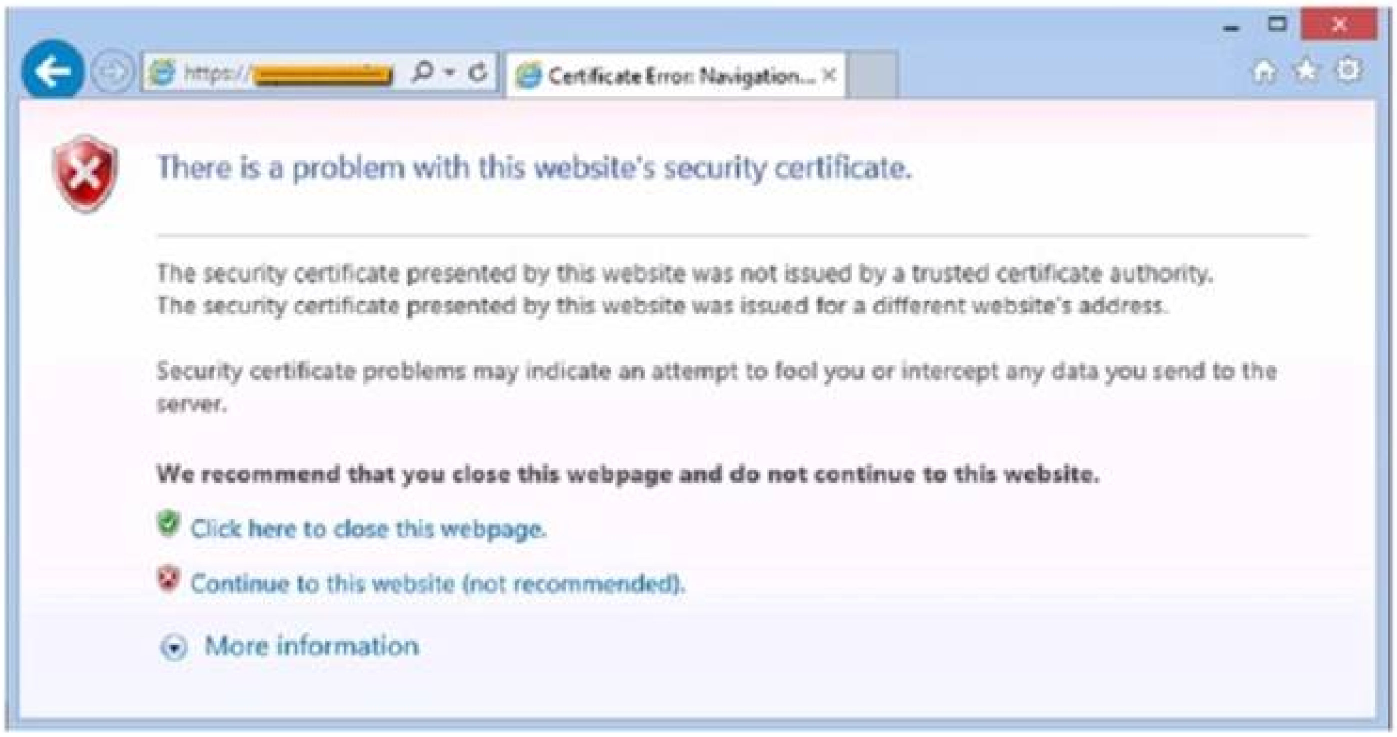
**Explanation:**

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 run1.

References: 1: https://windowsreport.com/mirror-backup-software/

**NEW QUESTION 223**

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



There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

**We recommend that you close this webpage and do not continue to this website.**

Click here to close this webpage.

Continue to this website (not recommended).

More information

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 CFCs 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 224**
Which of the following protocols supports fast roaming between networks?

A. WEP
B. WPA
C. WPA2
D. LEAP
E. PEAP

**Answer:** B

**Explanation:**
WPA2 is the only protocol among the options that supports fast roaming between networks. Fast roaming, also known as IEEE 802.11r or Fast BSS Transition (FT), enables a client device to roam quickly in environments implementing WPA2 Enterprise security, by ensuring that the client device does not need to re-authenticate to the RADIUS server every time it roams from one access point to another1. WEP, WPA, LEAP, and PEAP do not support fast roaming and require the client device to perform the full authentication process every time it roams, which can cause delays and interruptions in the network service.
References:
? The Official CompTIA A+ Core 2 Study Guide2, page 263.
? WiFi Fast Roaming, Simplified3

**NEW QUESTION 226**
A user wants to acquire antivirus software for a SOHO PC. A technician recommends a licensed software product, but the user does not want to pay for a license. Which of the following license types should the technician recommend?

A. Corporate
B. Open-source
C. Personal
D. Enterprise

**Answer:** B

**Explanation:**
Open-source software is software that has its source code available for anyone to inspect, modify, and distribute. Open-source software is usually free of charge and does not require a license to use. Some examples of open-source antivirus software are ClamAV, Comodo, and Immunet12. The other license types are either not free or not suitable for a SOHO PC. Corporate and enterprise licenses are designed for large-scale organizations and networks, and they usually require a subscription fee. Personal licenses are for individual users and may have limited features or support.
References: 1 What is Open Source Software? - Definition from Techopedia(https://www.tomsguide.com/us/best-antivirus,review-2588.html). 2 7 Best Lifetime License Antivirus Tools [2023 Guide] - Windows Report(https://windowsreport.com/antivirus-with-unlimited-validity/).

**NEW QUESTION 231**
A help desk technician runs the following script: Inventory.py. The technician receives the following error message:
How do you want to Open this file?
Which of the following is the MOST likely reason this script is unable to run?

A. Scripts are not permitted to run.
B. The script was not built for Windows.
C. The script requires administrator privileges,
D. The runtime environment is not installed.

**Answer:** D

**Explanation:**
The error message is indicating that the script is not associated with any program on the computer that can open and run it. This means that the script requires a runtime environment, such as Python, to be installed in order for it to execute properly. Without the appropriate runtime environment, the script will not be able to run.

**NEW QUESTION 236**
A technician is editing the hosts file on a few PCs in order to block certain domains. Which of the following would the technician need to execute after editing the hosts file?

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

**Answer:** D

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

**NEW QUESTION 237**
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 241**
A technician needs to perform after-hours service starting at 10:00 p.m. The technician is currently 20 minutes late. The customer will also be late. Which of the following should the technician do considering proper communication techniques and professionalism?

A. Do not notify the customer if arriving before the customer.
B. Dismiss the customer and proceed with the after-hours work.
C. Contact the customer if the technician is arriving late.
D. Disclose the experience via social media.

**Answer:** C

**Explanation:**
The best option for the technician to demonstrate proper communication techniques and professionalism is to contact the customer if the technician is arriving late. This shows respect for the customer's time and expectations, and allows the customer to adjust their schedule accordingly. It also helps to maintain a positive relationship and trust between the technician and the customer. The technician should apologize for the delay and provide a realistic estimate of their arrival time. The technician should also thank the customer for their patience and understanding.
The other options are not appropriate or professional. Do not notify the customer if arriving before the customer is not a good practice, as it may cause confusion or frustration for the customer. The customer may have made other plans or arrangements based on the technician's original schedule, and may not be available or prepared for the service. Dismiss the customer and proceed with the after-hours work is rude and disrespectful, as it ignores the customer's needs and preferences. The customer may have questions or concerns about the service, or may want to supervise or verify the work. The technician should always communicate with the customer before, during, and after the service.
Disclose the experience via social media is unethical and unprofessional, as it may violate the customer's privacy and the company's policies. The technician should not share any confidential or sensitive information about the customer or the service on social media, or make any negative or inappropriate comments about the customer or the situation. References:
? CompTIA A+ Certification Exam Core 2 Objectives1
? CompTIA A+ Core 2 (220-1102) Certification Study Guide2
? 8 Ways You Can Improve Your Communication Skills3
? Professionalism in Communication | How To Do It And How It Pays4

**NEW QUESTION 243**
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.
The GPS application is updating its geospatial map data.
C
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 phone1

**NEW QUESTION 244**
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:** BE

**Explanation:**
The correct answers are B. Removing the applications from startup and E. Defragmenting the hard drive. These are the operations that would be best to do to resolve the issue of a slow boot at a minimal expense.
? Removing the applications from startup means disabling the programs that run
automatically when the PC is turned on. This will reduce the load on the CPU and RAM and speed up the boot process1.
? Defragmenting the hard drive means rearranging the files on the disk so that they
are stored in contiguous blocks. This will improve the disk performance and reduce the time it takes to read and write data2.
1: CompTIA A+ Certification Exam: Core 2 Objectives, page 23, section 3.1. 2: CompTIA A+ Certification Exam: Core 2 Objectives, page 24, section 3.2.

**NEW QUESTION 249**
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 250**
A technician needs to transfer a file to a user's workstation. Which of the following would BEST accomplish this task utilizing the workstation's built-in protocols?

A.

VPN
B. SMB
C. RMM
D. MSRA

**Answer:** B

**Explanation:**
SMB stands for Server Message Block, which is a network file sharing protocol that allows applications on a computer to read and write to files and to request services from server programs in a computer network. SMB is a built-in protocol in Windows operating systems and can be used to transfer files between computers over a network. The technician can use SMB to access a file share on the user’s workstation and copy the file to or from it. VPN stands for virtual private network, which is a technology that creates a secure and encrypted connection over a public network. VPN is not a built-in protocol in Windows operating systems and does not directly transfer files between computers. RMM stands for remote monitoring and management, which is a type of software solution that allows remote management and monitoring of devices and networks. RMM is not a built-in protocol in Windows operating systems and does not directly transfer files between computers. MSRA stands for Microsoft Remote Assistance, which is a feature that allows a user to invite another user to view or control their computer remotely. MSRA is not a protocol, but an application that uses Remote Desktop Protocol (RDP) to establish a connection. MSRA does not directly transfer files between computers. https://www.pcmag.com/picks/the-best-desktop-workstations

**NEW QUESTION 251**
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 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.6

**NEW QUESTION 256**
A user's corporate laptop with proprietary work Information was stolen from a coffee shop. The user togged 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 258**
A network technician is deploying a new machine in a small branch office that does not have a DHCP server. The new machine automatically receives the IP address of 169.254.0.2 and is unable to communicate with the rest of the network. Which of the following would restore communication?

A. Static entry
B. ARP table
C.

APIPA address
D. NTP specification

**Answer:** A

**Explanation:**
A static entry is the best option to restore communication for the new machine in a small branch office that does not have a DHCP server. A static entry means manually configuring the IP address, subnet mask, default gateway, and DNS server for the network adapter of the machine. A static entry ensures that the machine has a valid and unique IP address that matches the network configuration and can communicate with the rest of the network.
The new machine automatically receives the IP address of 169.254.0.2 because it uses APIPA (Automatic Private IP Addressing), which is a feature that enables computers to self-assign an IP address when a DHCP server is not available. However, APIPA only works for local communication within the same subnet, and does not provide a default gateway or a DNS server. Therefore, the new machine is unable to communicate with the rest of the network, which may be on a different subnet or require a gateway or a DNS server to access.
The other options are not related to restoring communication for the new machine. ARP table is a cache that stores the mapping between IP addresses and MAC

addresses for the devices on the network. NTP specification is a protocol that synchronizes the clocks of the devices on the network.
References:
? CompTIA A+ Certification Exam Core 2 Objectives1
? CompTIA A+ Core 2 (220-1102) Certification Study Guide2
? What is APIPA (Automatic Private IP Addressing)? - Study-CCNA3
? How to Configure a Static IP Address in Windows and OS X4

**NEW QUESTION 262**
A company would like to implement multifactor authentication for all employees at a minimal cost. Which of the following best meets the company's requirements?

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

**Answer:** B

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

**NEW QUESTION 263**
A technician is setting up a SOHO wireless router. The router is about ten years old. The customer would like the most secure wireless network possible. Which of the following should the technician configure?

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

**Answer:** B

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

**NEW QUESTION 266**
A user is setting up a new Windows 10 laptop. Which of the following Windows settings should be used to input the SSID and password?

A.

Network & Internet
B. System
C. Personalization
D. Accounts

**Answer:** A

**Explanation:**
The Network & Internet settings in Windows 10 allow the user to input the SSID and password of a Wi-Fi network, as well as manage other network-related options, such as airplane mode, mobile hotspot, VPN, proxy, etc1. To access the Network & Internet settings, the user can select the Start button, then select Settings > Network & Internet2. Alternatively, the user can right-click the Wi-Fi icon on the taskbar and click "Open Network & Internet Settings"3.
The System settings in Windows 10 allow the user to configure the display, sound, notifications, power, storage, and other system-related options1. The Personalization settings in Windows 10 allow the user to customize the background, colors, lock screen, themes, fonts, and other appearance-related options1. The Accounts settings in Windows 10 allow the user to manage the user accounts, sign-in options, sync settings, and other account-related options1. None of these settings can be used to input the SSID and password of a Wi-Fi network.

References:
? The Official CompTIA A+ Core 2 Study Guide1, page 221, 222, 223, 224.

**NEW QUESTION 271**
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 276**
A technician wants to enable BitLocker on a Windows 10 laptop and is unable to find the BitLocker Drive Encryption menu item in Control Panel. Which of the following explains why the technician unable to find this menu item?

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

**Answer:** C

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

**NEW QUESTION 280**
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 282**
Which of the following file extensions should a technician use for a PowerShell script?

A.

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

**Answer:** A

**Explanation:**
A PowerShell script is a plain text file that contains one or more PowerShell commands. Scripts have a .ps1 file extension and can be run on your computer or in a remote session. PowerShell scripts can be used to automate tasks and change settings on Windows devices. To create and run a PowerShell script, you need a text editor (such as Visual Studio Code or Notepad) and the PowerShell Integrated Scripting Environment (ISE) console. You also need to enable the correct execution policy to allow scripts to run on your system

**NEW QUESTION 287**
A technician is setting up a newly built computer. Which of the following is the fastest way for the technician to install Windows 10?

A. Factory reset
B. System Restore

C. In-place upgrade
D. Unattended installation

**Answer:** D

**Explanation:**
An unattended installation is a method of installing Windows 10 that does not require any user input or interaction during the installation process. An unattended installation can be performed by using an answer file, which is a file that contains all the configuration settings and preferences for the installation, such as the product key, the language, the partition size, and the user accounts. An unattended installation can be the fastest way to install Windows 10, as it automates and streamlines the installation process. Factory reset, System Restore, and in-place upgrade are not methods of installing Windows 10.

**NEW QUESTION 291**
A technician is setting up a backup method on a workstation that only requires two sets of tapes to restore. Which of the following would BEST accomplish this task?

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

**Answer:** D

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

**NEW QUESTION 294**
A customer calls desktop support and begins yelling at a technician. The customer claims to have submitted a support ticket two hours ago and complains that the issue still has not been resolved. Which of the following describes how the technician should respond?

A. Place the customer on hold until the customer calms down.
B. Disconnect the call to avoid a confrontation.
C. Wait until the customer is done speaking and offer assistance.
D. Escalate the issue to a supervisor.

**Answer:** C

**Explanation:**
The best way to deal with an angry customer who is yelling at a technician is to wait until the customer is done speaking and offer assistance. This shows respect, empathy, and professionalism, and allows the technician to understand the customer’s problem and find a solution. According to the CompTIA A+ Core 2 (220-1102) Certification Study Guide1, some of the steps to handle angry customers are:
? Stay calm and do not take it personally.
? Listen actively and acknowledge the customer’s feelings.
? Apologize sincerely and offer to help.
? Restate the customer’s issue and ask for clarification if needed.
? Explain the possible causes and solutions for the problem.
? Provide clear and realistic expectations for the resolution.

? Follow up with the customer until the issue is resolved.

The other options are not appropriate ways to deal with angry customers, as they may worsen the situation or damage the customer relationship. Placing the customer on hold may make them feel ignored or dismissed. Disconnecting the call may make them feel disrespected or abandoned. Escalating the issue to a supervisor may make them feel frustrated or powerless, unless the technician cannot resolve the issue or the customer requests to speak to a supervisor.

References:

? CompTIA A+ Certification Exam Core 2 Objectives2
? CompTIA A+ Core 2 (220-1102) Certification Study Guide1
? How To Deal with Angry Customers (With Examples and Tips)3
? 17 ways to deal with angry customers: Templates and examples4
? Six Ways to Handle Angry Customers5

**NEW QUESTION 297**

Which of the following would cause a corporate-owned iOS device to have an Activation Lock issue?

A. A forgotten keychain password
B. An employee's Apple ID used on the device
C. An operating system that has been jailbroken
D. An expired screen unlock code

**Answer:** B

**Explanation:**

Activation Lock is a feature that prevents anyone from erasing or activating an iOS device without the owner's Apple ID and password. If a corporate-owned iOS device is linked to an employee's Apple ID, it will have an Activation Lock issue when the employee leaves the company or forgets their Apple ID credentials.

Reference: CompTIA A+ Core 2 Exam Objectives, Section 4.1

**NEW QUESTION 302**

An engineer is configuring a new server that requires a bare-metal installation. Which of the following installation methods should the engineer use if installation media is not available on site?

A. Image deployment
B. Recovery partition installation
C. Remote network installation
D. Repair installation

**Answer:** C

**Explanation:**

Remote network installation is the best option for configuring a new server that requires a bare-metal installation without installation media on site. A remote network installation is a method of installing an operating system or an application over a network connection, such as LAN, WAN, or Internet. A remote network installation can use various protocols, such as PXE, HTTP, FTP, or SMB, to access the installation files from a server or a cloud service. A remote network installation can also use various tools, such as Windows Deployment Services, Microsoft Deployment Toolkit, or Red Hat Kickstart, to automate and customize the installation process. A remote network installation can save time and resources by eliminating the need for physical media and allowing centralized management of multiple installations. Image deployment, recovery partition installation, and repair installation are not correct answers for this question. Image deployment is a method of installing an operating system or an application by copying a preconfigured image file to a target device. Image deployment requires an existing image file and a compatible device. Recovery partition installation is a method of restoring an operating system or an application from a hidden partition on the hard disk that contains the original factory settings. Recovery partition installation requires an existing recovery partition and a functional hard disk. Repair installation is a method of fixing an operating system or an application that is corrupted or damaged by replacing or repairing the system files without affecting the user data or settings. Repair installation requires an existing operating system or application and a working device. References:

? Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 16
? CompTIA A+ Complete Study Guide: Core 1 Exam 220-1101 and Core 2 Exam …, page 106

**NEW QUESTION 306**

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

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

**Answer:** B

**Explanation:**
Checking for application updates is the first troubleshooting step that the user should perform, because the application may not be compatible with the new OS version and may need an update to fix the issue. Deleting the application’s cache, rolling back the OS update, or uninstalling and reinstalling the application are possible solutions, but they are more time-consuming and disruptive than checking for updates. References: : https://www.comptia.org/training/resources/exam-objectives/comptia-a-core-2-exam- objectives : https://www.lifewire.com/how-to-update-apps-on-android-4173855

**NEW QUESTION 308**
During a recent flight an executive unexpectedly received several dog and cat pictures while trying to watch a movie via in-flight Wi-Fi on an iPhone. The executive has no records of any contacts sending pictures like these and has not seen these pictures before. To BEST resolve this issue, the executive should:

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

**Answer:** A

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

**NEW QUESTION 313**
A technician needs to ensure that USB devices are not suspended by the operating system Which of the following Control Panel utilities should the technician use to configure the setting?

A. System
B. Power Options
C. Devices and Printers
D. Ease of Access

**Answer:** B

**Explanation:**
The correct answer is B. Power Options. The Power Options utility in the Control Panel allows you to configure various settings related to how your computer uses and saves power, such as the power plan, the sleep mode, the screen brightness, and the battery status. To access the Power Options utility, you can follow these steps:
? Go to Control Panel > Hardware and Sound > Power Options.
? Click on Change plan settings for the power plan you are using.
? Click on Change advanced power settings.
? Expand the USB settings category and then the USB selective suspend setting subcategory.
? Set the option to Disabled for both On battery and Plugged in.
? Click on OK and then on Save changes.
This will prevent the operating system from suspending the USB devices to save power . System, Devices and Printers, and Ease of Access are not the utilities that should be used to configure the setting. System is a utility that provides information about your computer’s hardware and software, such as the processor, memory, operating system, device manager, and system protection. Devices and Printers is a utility that allows you to view and manage the devices and printers connected to your computer, such as adding or removing devices, changing device settings, or troubleshooting problems. Ease of Access is a utility that allows you to customize your computer’s accessibility options, such as the narrator, magnifier, high contrast, keyboard, mouse, and speech recognition. None of these utilities have any option to configure the USB selective suspend setting.

**NEW QUESTION 317**
......

# Thank You for Trying Our Product

## We offer two products:

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

2nd - Questons and Answers in PDF Format

## 220-1102 Practice Exam Features:

* 220-1102 Questions and Answers Updated Frequently

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

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

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

100% Actual & Verified — Instant Download, Please Click
Order The 220-1102 Practice Test Here