CompTIA.220-1102 .vNov-2023.143q

Number: 220-1102
Passing Score: 800
Time Limit: 120
File Version: 22.0

Exam Code: 220-1102

Exam Name: CompTIA A+ Certification Exam: Core 2

Exam A

QUESTION 1

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

A. Install alternate open-source software in place of the applications with issues

B. Run both CPU and memory tests to ensure that all hardware functionality is normal

C. Check for any installed patches and roll them back one at a time until the issue is resolved

D. Reformat the hard drive, and then reinstall the newest Windows 10 release and all applications.

Correct Answer: C

Section:

Explanation:

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

QUESTION 2

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

A. Data-in-transit encryption

B. File encryption

C. USB drive encryption

D. Disk encryption

Correct Answer: D

Section:

Explanation:

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

QUESTION 3

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

A. Full

B. Non-parity

C. Differential

D. Incremental

Correct Answer: A

Section:

Explanation:

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

QUESTION 4

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

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

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

QUESTION 5
Someone who is fraudulently claiming to be from a reputable bank calls a company employee. Which of the following describes this incident?

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

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

QUESTION 6
A company is Issuing smartphones to employees and needs to ensure data is secure if the devices are lost or stolen. Which of the following provides the BEST solution?

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

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

QUESTION 7
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. WPA2withAES
C. WPA3withAES-256
D. WPA3 with AES-128

Correct Answer: B
Section:
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.

QUESTION 8
A technician has been tasked with using the fastest and most secure method of logging in to laptops.
Which of the following log-in options meets these requirements?

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

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

QUESTION 9
A technician is replacing the processor in a desktop computer prior to opening the computer, the technician wants to ensure the internal components are protected. Which of the following safety procedures would BEST protect the components in the PC? (Select TWO).

A. Utilizing an ESD strap
B. Disconnecting the computer from the power source
C. Placing the PSU in an antistatic bag
D. Ensuring proper ventilation
E. Removing dust from the ventilation fans
F. Ensuring equipment is grounded

Correct Answer: A, B
Section:
Explanation:
The two safety procedures that would best protect the components in the PC are: Utilizing an ESD strap Placing the PSU in an antistatic bag https://www.professormesser.com/free-a-plus-training/220-902/computer-safety-procedures-2/
https://www.skillsoft.com/course/comptia-a-core-2-safety-procedures-environmental-impacts- cbdf0f2c-61c0-4f4a-a659-dc98f1f00158

QUESTION 10
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

Correct Answer: C, E
Section:
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.

QUESTION 11
A company wants to remove information from past users' hard drives in order to reuse the hard drives Witch of the following is the MOST secure method

A. Reinstalling Windows
B. Performing a quick format
C. Using disk-wiping software
D. Deleting all files from command-line interface

Correct Answer: C
Section:
Explanation:
Using disk-wiping software is the most secure method for removing information from past users' hard drives in order to reuse the hard drives. Disk-wiping software can help to ensure that all data on the hard drive is completely erased and cannot be recovered.

QUESTION 12
A technician is configuring a SOHO device Company policy dictates that static IP addresses cannot be used. The company wants the server to maintain the same IP address at all times. Which of the following should the technician use?

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

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

QUESTION 13
A user is unable to use any internet-related functions on a smartphone when it is not connected to Wi-Fi When the smartphone is connected to Wi-Fi the user can browse the internet and send and receive email. The user is also able to send and receive text messages and phone calls when the smartphone is not connected to Wi-Fi. Which of the following is the MOST likely reason the user is unable to use the internet on the smartphone when it is not connected to Wi-Fi?

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

Correct Answer: A
Section:
Explanation:
The smartphone's line was not provisioned with a data plan. The user is unable to use any internet- related functions on the smartphone when it is not connected to Wi-Fi because the smartphone'sline was not provisioned with

a data plan. The user can send and receive text messages and phone calls when the smartphone is not connected to Wi-Fi because these functions do not require an internet connection1

QUESTION 14

A technician is investigating an employee's smartphone that has the following symptoms

- The device is hot even when it is not in use.
- Applications crash, especially when others are launched
- Certain applications, such as GPS, are in portrait mode when they should be in landscape mode Which of the following can the technician do to MOST likely resolve these issues with minimal impact? (Select TWO).

A. Turn on autorotation

B. Activate airplane mode.

C. Close unnecessary applications

D. Perform a factory reset

E. Update the device's operating system

F. Reinstall the applications that have crashed.

Correct Answer: A, C

Section:

Explanation:

The technician can close unnecessary applications and turn on autorotation to resolve these issues with minimal impact. Autorotation can help the device to switch between portrait and landscapemodes automatically. Closing unnecessary applications can help to free up the device’s memory and reduce the device’s temperature1Reference:CompTIA A+ Certification Exam: Core 2 (220-1102) Exam Objectives Version 4.0. Retrieved from https://partners.comptia.org/docs/default-source/resources/comptia-a-220-1102-exam-objectives- (3-0)

QUESTION 15

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

A. Within the Power Options of the Control Panel utility click the Change Plan Settings button for the enabled power plan and select Put the Computer to Sleep under the Plugged In category to Never

B. Within the Power Options of the Control Panel utility, click the Change Plan Settings button for the enabled power plan and select Put the Computer to Sleep under the On Battery category to Never

C. Within the Power Options of the Control Panel utility select the option Choose When to Turn Off the Display and select Turn Off the Display under the Plugged In category to Never

D. Within the Power Options of the Control Panel utility, select the option Choose What Closing the Lid Does and select When I Close the Lid under the Plugged in category to Do Nothing

Correct Answer: D

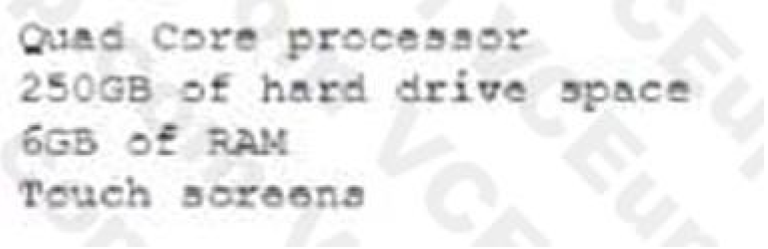
Section:

Explanation:

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

QUESTION 16

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



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

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

A. CPU

B. Hard drive

C. RAM

D. Touch screen

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

QUESTION 17
Which of the following Wi-Fi protocols is the MOST secure?

A. WPA3

B. WPA-AES

C. WEP

D. WPA-TKIP

Correct Answer: A
Section:
Explanation:

QUESTION 18
A user attempts to open some files, but a message appears stating that the files are encrypted. The user was able to access these files before without receiving this message and no changes have been made within the company. Which of the following has infected the computer?

A. Cryptominer

B. Phishing

C. Ransomware

D. Keylogger

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

QUESTION 19
A help desk technician is troubleshooting a workstation in a SOHO environment that is running above normal system baselines. The technician discovers an unknown executable with a random string name running on the system. The technician terminates the process, and the system returns to normal operation. The technician thinks the issue was an infected file, but the antivirus is not detecting a threat. The technician is concerned other machines may be infected with this unknown virus. Which of the following is the MOST effective way to check other machines on the network for this unknown threat?

A. Run a startup script that removes files by name.

B. Provide a sample to the antivirus vendor.

C. Manually check each machine.

D. Monitor outbound network traffic.

Correct Answer: C

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

QUESTION 20
A user reports that a PC seems to be running more slowly than usual. A technician checks system resources, but disk, CPU, and memory usage seem to be fine. The technician sees that GPU temperature is extremely high. Which of the following types of malware is MOST likely to blame?

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

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

QUESTION 21
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

Correct Answer: C
Section:
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

QUESTION 22
Which of the following OS types provides a lightweight option for workstations thai need an easy-touse browser-based interface?

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

Correct Answer: B
Section:
Explanation:
Chrome OS provides a lightweight option for workstations that need an easy-to-use browser-based interface1

QUESTION 23

Following the latest Windows update PDF files are opening in Microsoft Edge instead of Adobe Reader. Which of the following utilities should be used to ensure all PDF files open in Adobe Reader?

A. Network and Sharing Center
B. Programs and Features
C. Default Apps
D. Add or Remove Programs

Correct Answer: C
Section:
Explanation:
Default Apps should be used to ensure all PDF files open in Adobe Reader

QUESTION 24

Which of the following provide the BEST way to secure physical access to a data cento server room?
(Select TWO).

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

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

QUESTION 25

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

Correct Answer: A
Section:
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.

QUESTION 26

A user reports that antivirus software indicates a computer is infected with viruses. The user thinks this happened white browsing the internet. The technician does not recognize the interface with which the antivirus message is presented.

Which of the following is the NEXT step the technician should take?

A. Shut down the infected computer and swap it with another computer

B. Investigate what the interface is and what triggered it to pop up

C. Proceed with initiating a full scan and removal of the viruses using the presented interface

D. Call the phone number displayed in the interface of the antivirus removal tool

Correct Answer: B

Section:

Explanation:

The technician should not proceed with initiating a full scan and removal of the viruses using the presented interface or call the phone number displayed in the interface of the antivirus removal tool12Shutting down the infected computer and swapping it with another computer is not necessary at this point12The technician should not immediately assume that the message is legitimate or perform any actions without knowing what the interface is and what triggered it to pop up. It is important to investigate the issue further, including checking the legitimacy of the antivirus program and the message it is displaying.

QUESTION 27

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

A. The contents of the text comptia.txt will be replaced with a new blank document

B. The contents of the text comptia. txt would be displayed.

C. The contents of the text comptia.txt would be categorized in alphabetical order.

D. The contents of the text comptia. txt would be copied to another comptia. txt file

Correct Answer: B

Section:

Explanation:

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

QUESTION 28

A user's smarlphone 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

Correct Answer: D

Section:

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.

QUESTION 29

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

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

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

QUESTION 30
A technician is troubleshooting an issue involving programs on a Windows 10 machine that are loading on startup but causing excessive boot times. Which of the following should the technician do to selectively prevent programs from loading?

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

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

QUESTION 31
A desktop specialist needs to prepare a laptop running Windows 10 for a newly hired employee.
Which of the following methods should the technician use to refresh the laptop?

A. Internet-based upgrade
B. Repair installation
C. Clean install
D. USB repair
E. In place upgrade

Correct Answer: C
Section:
Explanation:
The desktop specialist should use a clean install to refresh the laptop. A clean install will remove all data and applications from the laptop and install a fresh copy of Windows 10, ensuring that the laptop is ready for the newly hired employee.

QUESTION 32
A technician found that an employee is mining cryptocurrency on a work desktop. The company has decided that this action violates its guidelines. Which of the following should be updated to reflect this new requirement?

A. MDM
B. EULA
C. IRP

D. AUP

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

QUESTION 33
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

Correct Answer: C
Section:
Explanation:
The technician should quarantine the system first1Reference: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)

QUESTION 34
A user has requested help setting up the fingerprint reader on a Windows 10 laptop. The laptop is equipped with a fingerprint reader and is joined to a domain Group Policy enables Windows Hello on all computers in the environment. Which of the following options describes how to set up Windows Hello Fingerprint for the user?

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

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

QUESTION 35
A user is attempting to make a purchase at a store using a phone. The user places the phone on the payment pad, but the device does not recognize the phone. The user attempts to restart the phone but still has the same results. Which of the following should the user do to resolve the issue?

A. Turn off airplane mode while at the register.

B. Verify that NFC is enabled.

C. Connect to the store's Wi-Fi network.

D. Enable Bluetooth on the phone.

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

QUESTION 36
A junior administrator is responsible for deploying software to a large group of computers in an organization. The administrator finds a script on a popular coding website to automate this distribution but does not understand the scripting language. Which of the following BEST describes the risks in running this script?

A. The instructions from the software company are not being followed.

B. Security controls will treat automated deployments as malware.

C. The deployment script is performing unknown actions.

D. Copying scripts off the internet is considered plagiarism.

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

QUESTION 37
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

Correct Answer: A
Section:
Explanation:
A risk analysis must be completed before a change request for an upcoming server deployment can be approved Risk analysis is an important step in the change management process because it helps identify and mitigate potential risks before changes are implemented. Once the risks have been analyzed and the appropriate measures have been taken to minimize them, the change can be approved and implemented.

QUESTION 38
A user reports a workstation has been performing strangely after a suspicious email was opened on it earlier in the week. Which of the following should the technician perform FIRST?

A. Escalate the ticket to Tier 2.

B. Run a virus scan.

C. Utilize a Windows restore point.

D. Reimage the computer.

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

QUESTION 39
Each time a user tries to go to the selected web search provider, a different website opens. Which of the following should the technician check FIRST?

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

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

QUESTION 40
Which of the following is the STRONGEST wireless configuration?

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

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

QUESTION 41
A technician has an external SSD. The technician needs to read and write to an external SSD on both Macs and Windows PCs. Which of the following filesystems is supported by both OS types?

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

Correct Answer: D
Section:
Explanation:
The filesystem that is supported by both Macs and Windows PCs is D. exFAT. exFAT is a file system that is designed to be used on flash drives like USB sticks and SD cards. It is supported by both Macs and Windows PCs,

and it can handle large files and volumes
https://www.diskpart.com/articles/file-system-for-mac-and-windows-0310.html

QUESTION 42
A user's system is infected with malware. A technician updates the anti-malware software and runs a scan that removes the malware. After the user reboots the system, it once again becomes infected with malware. Which of the following will MOST likely help to permanently remove the malware?

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

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

QUESTION 43
A user connected a laptop to a wireless network and was tricked into providing login credentials for a website. Which of the following threats was used to carry out the attack?

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

Correct Answer: D
Section:
Explanation:

QUESTION 44
Which of the following change management documents includes how to uninstall a patch?

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

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

QUESTION 45
A network administrator is deploying a client certificate to be used for Wi-Fi access for all devices in an organization. The certificate will be used in conjunction with the user's existing username and password. Which of the following BEST describes the security benefits realized after this deployment?

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

Correct Answer: A
Section:
Explanation:

QUESTION 46
In which of the following scenarios would remote wipe capabilities MOST likely be used? (Select TWO).

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

Correct Answer: E, F
Section:
Explanation:
Remote wipe capabilities are used to erase all data on a mobile device remotely. This can be useful in situations where a device is lost or stolen, or when sensitive data needs to be removed from a device. Remote wipe capabilities are most likely to be used in the following scenarios:
1. A user cannot locate the phone after attending a play at a theater. F. A user forgot the phone in a taxi, and the driver called the company to return the device1 In scenario E, remote wipe capabilities would be used to prevent unauthorized access to the device and to protect sensitive data. In scenario F, remote wipe capabilities would be used to erase all data on the device before it is returned to the user.

QUESTION 47
Sensitive data was leaked from a user's smartphone. A technician discovered an unapproved application was installed, and the user has full access to the device's command shell. Which of the following is the NEXT step the technician should take to find the cause of the leaked data?

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

Correct Answer: B
Section:
Explanation:
The technician should disable the user's access to the device's command shell. This will prevent the user from accessing sensitive data and will help to prevent further data leaks. The technician should then investigate the unapproved application to determine if it is the cause of the data leak. If the application is found to be the cause of the leak, the technician should uninstall the application and restore the device to factory settings. If the application is not the cause of the leak, the technician should investigate further to determine the cause of the leak. Disabling the ability to install applications from unknown sources can help to prevent future data leaks, but it is not the next step the technician should take in this scenario. Ensuring the device is connected to the corporate WiFi network is not relevant to this scenario1

QUESTION 48
A technician is attempting to mitigate micro power outages, which occur frequently within the area of operation. The outages are usually short, with the longest occurrence lasting five minutes. Which of the following should the technician use to mitigate this issue?

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

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

QUESTION 49
A user has a license for an application that is in use on a personal home laptop. The user approaches a systems administrator about using the same license on multiple computers on the corporate network. Which of the following BEST describes what the systems administrator should tell the user?

A. Use the application only on the home laptop because it contains the initial license.
B. Use the application at home and contact the vendor regarding a corporate license.
C. Use the application on any computer since the user has a license.
D. Use the application only on corporate computers.

Correct Answer: B
Section:
Explanation:
Use the application at home and contact the vendor regarding a corporate license. The user should use the application only on the home laptop because it contains the initial license. The user should contact the vendor regarding a corporate license if they want to use the application on multiple computers on the corporate network1

QUESTION 50
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

Correct Answer: B
Section:
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.

QUESTION 51
The web browsing speed on a customer's mobile phone slows down every few weeks and then returns to normal after three or four days. Restarting the device does not usually restore performance. Which of the following should a technician check FIRST to troubleshoot this issue?

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

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

QUESTION 52
Following a recent power outage, several computers have been receiving errors when booting. The technician suspects file corruption has occurred. Which of the following steps should the technician try FIRST to correct the issue?

A. Rebuild the Windows profiles.
B. Restore the computers from backup.
C. Reimage the computers.
D. Run the System File Checker.

Correct Answer: D
Section:
Explanation:
The technician should run the System File Checker (SFC) first to correct file corruption errors on computers after a power outage. SFC is a command-line utility that scans for and repairs corrupted system files. It can be run from the command prompt or from the Windows Recovery Environment. Rebuilding the Windows profiles, restoring the computers from backup, and reimaging the computers are more drastic measures that should be taken only if SFC fails to correct the issue1

QUESTION 53
A user is unable to access a website, which is widely used across the organization, and receives the following error message:
The security certificate presented by this website has expired or is not yet valid.
The technician confirms the website works when accessing it from another computer but not from the user's computer. Which of the following should the technician perform NEXT to troubleshoot the issue?

A. Reboot the computer.
B. Reinstall the OS.
C. Configure a static 12
D. Check the computer's date and time.

Correct Answer: D
Section:
Explanation:
The error message indicates that the security certificate presented by the website has either expired or is not yet valid. This can happen if the computer's clock has the wrong date or time, as SSL/TLS certificates have a specific validity period. If the clock is off by too much, it may cause the certificate to fail to validate. Therefore, the technician should check the computer's date and time and ensure that they are correct.

QUESTION 54
A company has just refreshed several desktop PCs. The hard drives contain PII. Which of the following is the BEST method to dispose of the drives?

A. Drilling

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

Correct Answer: D
Section:
Explanation:
Erasing/wiping the hard drives is the best method to dispose of the drives containing PII

QUESTION 55
After a company installed a new SOHO router customers were unable to access the company-hosted public website. Which of the following will MOST likely allow customers to access the website?

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

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

QUESTION 56
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

Correct Answer: D
Section:
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.

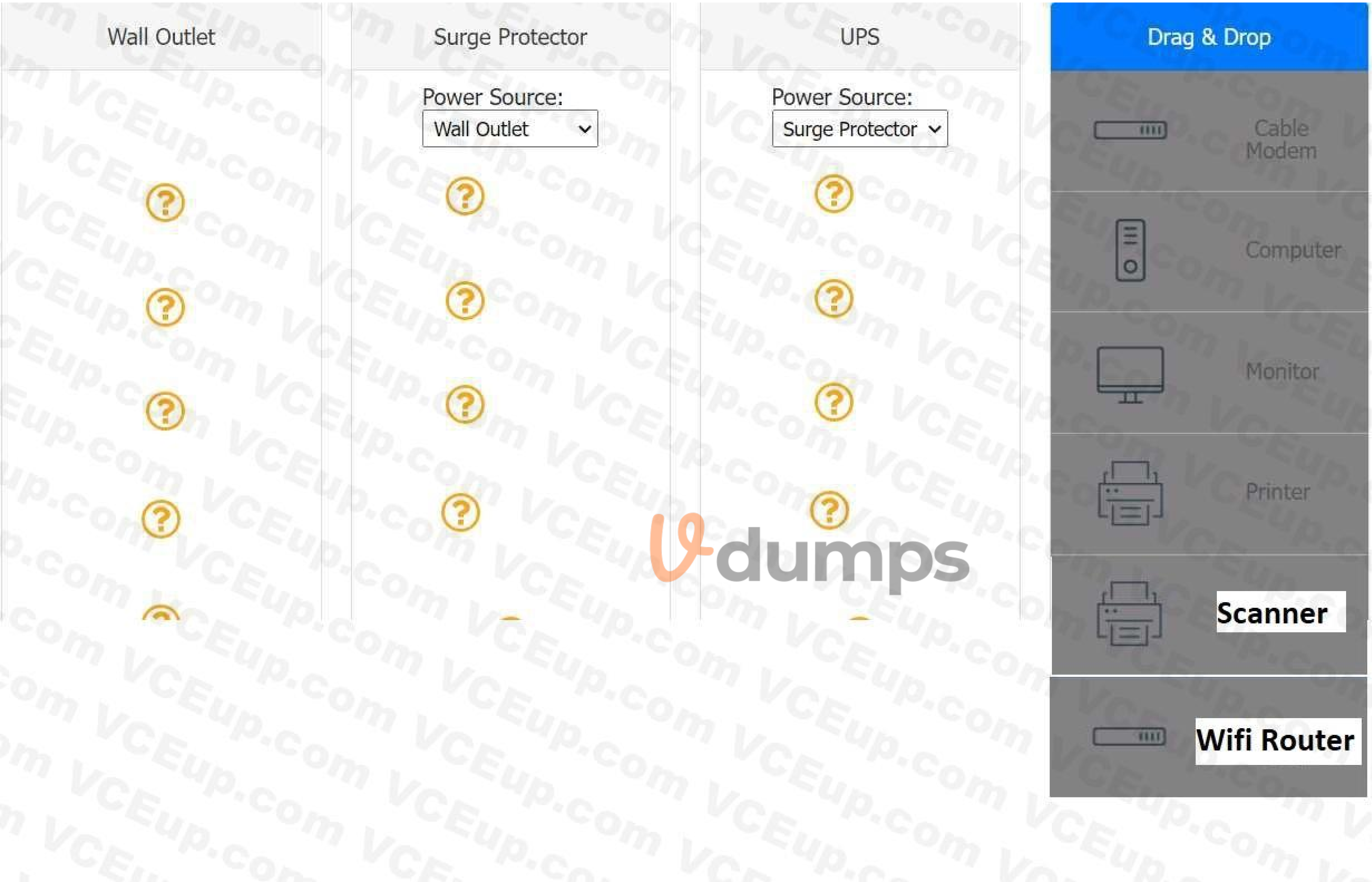
QUESTION 57
A user reports a PC is running slowly. The technician suspects high disk I/O. Which of the following should the technician perform NEXT?

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

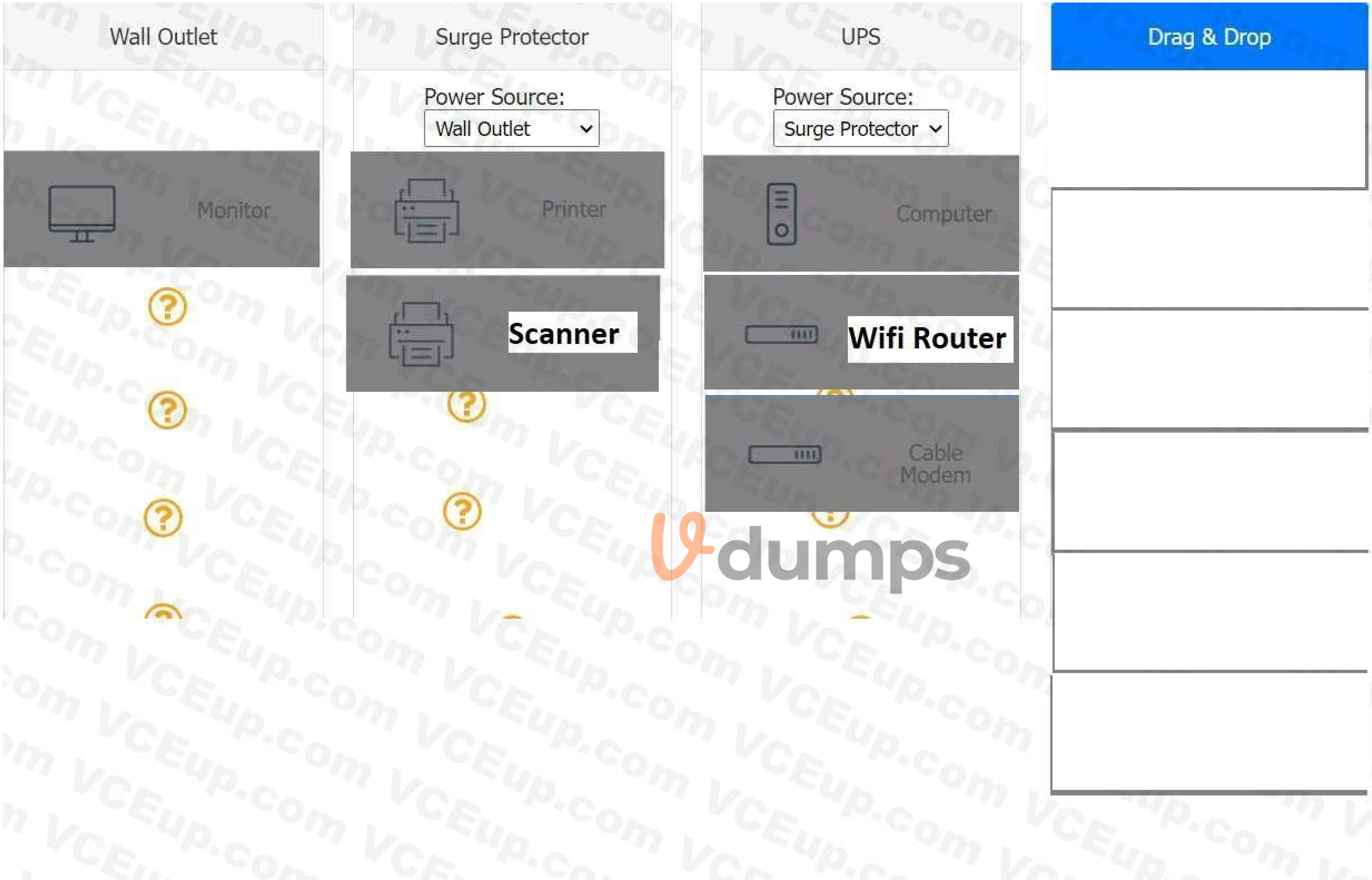
Correct Answer: A
Section:
Explanation:
If a technician suspects high disk I/O, the technician should use the Resource Monitor (resmon.exe) to identify the process that is causing the high disk I/O1. Resource Monitor provides detailed information about the system's resource usage, including disk I/O1.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

QUESTION 58
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.

Select and Place:



Correct Answer:



Section:
Explanation:

QUESTION 59
A macOS user needs to create another virtual desktop space. Which of the following applications will allow the user to accomplish this task?

A. Dock
B. Spotlight
C. Mission Control

D. Launchpad

Correct Answer: C
Section:
Explanation:
application that will allow a macOS user to create another virtual desktop space is Mission Control Mission Control lets you create additional desktops, called spaces, to organize the windows of your apps. You can create a space by entering Mission Control and clicking the Add button in the Spaces bar1. You can also assign apps to specific spaces and move between them easily1.

QUESTION 60
A technician is troubleshooting a computer with a suspected short in the power supply. Which of the following is the FIRST step the technician should take?

A. Put on an ESD strap
B. Disconnect the power before servicing the PC.
C. Place the PC on a grounded workbench.
D. Place components on an ESD mat.

Correct Answer: B
Section:
Explanation:
The first step a technician should take when troubleshooting a computer with a suspected short in the power supply is B. Disconnect the power before servicing the PC. This is to prevent any electrical shock or damage to the components. A power supply can be dangerous even when unplugged, as capacitors can maintain a line voltage charge for a long time1. Therefore, it is important to disconnect the power cord and press the power button to discharge any residual power before opening the case2. The other steps are also important for safety and proper diagnosis, but they should be done after disconnecting the power.

QUESTION 61
A team of support agents will be using their workstations to store credit card dat a. Which of the following should the IT department enable on the workstations in order to remain compliant with common regulatory controls? (Select TWO).

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

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

QUESTION 62
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

Correct Answer: A
Section:
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.

QUESTION 63
A company is deploying mobile phones on a one-to-one basis, but the IT manager is concerned that users will root/jailbreak their phones. Which of the following technologies can be implemented to prevent this issue?

A. Signed system images
B. Antivirus
C. SSO
D. MDM

Correct Answer: D
Section:
Explanation:
MDM stands for Mobile Device Management, and it is a way of remotely managing and securing mobile devices that are used for work purposes1. MDM can enforce policies and restrictions on the devices, such as preventing users from installing unauthorized apps, modifying system settings, or accessing root privileges2. MDM can also monitor device status, wipe data, lock devices, or locate lost or stolen devices1.

QUESTION 64
A technician is troubleshooting an issue that requires a user profile to be rebuilt. The technician is unable to locate Local Users and Groups in the Mtv1C console. Which of the following is the NEXT step the technician should take to resolve the issue?

A. Run the antivirus scan.
B. Add the required snap-in.
C. Restore the system backup
D. use the administrator console.

Correct Answer: B
Section:
Explanation:
Local Users and Groups is a Microsoft Management Console (MMC) snap-in that allows you to manage user accounts or groups on your computer1. If you cannot find it in the MMC console, you can add it manually by following these steps2:
Press Windows key + R to open the Run dialog box, or open the Command Prompt. Type mmc and hit Enter. This will open a blank MMC console.
Click File and then Add/Remove Snap-in.
In the Add or Remove Snap-ins window, select Local Users and Groups from the Available snap-ins list, and click Add.
In the Select Computer window, choose Local computer or Another computer, depending on which computer you want to manage, and click Finish.
Click OK to close the Add or Remove Snap-ins window. You should now see Local Users and Groups in the MMC console.

QUESTION 65
A technician needs to manually set an IP address on a computer that is running macOS. Which of the following commands should the technician use?

A. ipconfig

B. ifconfig
C. arpa
D. ping

Correct Answer: B
Section:
Explanation:
ifconfig is a command-line utility that allows you to configure network interfaces on macOS and other Unix-like systems1. To set an IP address using ifconfig, you need to know the name of the network interface you want to configure (such as en0 or en1), and the IP address you want to assign (such as 192.168.0.150). You also need to use sudo to run the command with administrative privileges2. The syntax of the command is:

```
sudo ifconfig interface address
```

For example, to set the IP address of en1 to 192.168.0.150, you would type:

```
sudo ifconfig en1 192.168.0.150
```

You may also need to specify other parameters such as subnet mask, gateway, or DNS servers, depending on your network configuration3. The other commands are not directly related to setting an IP address on macOS. ipconfig is a similar command for Windows systems4, arpa is a domain name used for reverse DNS lookup, and ping is a command for testing network connectivity.

QUESTION 66
A mobile phone user has downloaded a new payment application that allows payments to be made with a mobile device. The user attempts to use the device at a payment terminal but is unable to do so successfully. The user contacts a help desk technician to report the issue. Which of the following should the technician confirm NEXT as part of the troubleshooting process?

A. If airplane mode is enabled
B. If Bluetooth is disabled
C. If NFC is enabled
D. If WiFi is enabled
E. If location services are disabled

Correct Answer: C
Section:
Explanation:
NFC stands for Near Field Communication, and it is a wireless technology that allows your phone to act as a contactless payment device, among other things2. Payment applications that allow payments to be made with a mobile device usually rely on NFC to communicate with the payment terminal1. Therefore, if NFC is disabled on the phone, the payment will not work. To enable NFC on an Android phone, you need to follow these steps3:
On your Android device, open the Settings app.
Select Connected devices.
Tap on Connection preferences.
You should see the NFC option. Toggle it on.
The other options are not directly related to using a payment application with a mobile device. Airplane mode is a setting that disables all wireless communication on the phone, including NFC4, but it also affects calls, texts, and internet access. Bluetooth is a wireless technology that allows you to connect your phone with other devices such as headphones or speakers, but it is not used for contactless payments. Wi-Fi is a wireless technology that allows you to access the internet or a local network, but it is also not used for contactless payments. Location services are a feature that allows your phone to determine your geographic location using GPS or other methods, but they are not required for contactless payments.

QUESTION 67
Antivirus software indicates that a workstation is infected with ransomware that cannot be quarantined. Which of the following should be performed FIRST to prevent further damage to the host and other systems?

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

Correct Answer: A

Section:
Explanation:
Ransomware is a type of malware that encrypts the files on a system and demands a ransom for their decryption1. Ransomware can also spread to other systems on the network or exfiltrate sensitive data to the attackers2. Therefore, it is important to isolate the infected machine as soon as possible to contain the infection and prevent further damage3. Powering off the machine is a quick and effective way of disconnecting it from the network and stopping any malicious processes running on it12. The other options are not directly related to preventing ransomware damage or may not be effective. Running a full antivirus scan may not be able to detect or remove the ransomware, especially if it is a new or unknown variant1. Removing the LAN card may disconnect the machine from the network, but it may not stop any malicious processes running on it or any data encryption or exfiltration that has already occurred2. Installing a different endpoint solution may not be possible or helpful if the system is already infected and locked by ransomware1.

QUESTION 68
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.

Correct Answer: B
Section:
Explanation:
Sometimes, an OS update can cause compatibility issues with some applications that are not optimized for the new version of the OS. To fix this, the user should check if there are any updates available for the application that can resolve the issue. The user can check for application updates by following these steps:
On an Android device, open the Google Play Store app and tap on the menu icon in the top left corner. Then tap on My apps & games and look for any updates available for the application. If there is an update, tap on Update to install it.
On an iOS device, open the App Store app and tap on the Updates tab at the bottom. Then look for any updates available for the application. If there is an update, tap on Update to install it.

QUESTION 69
A technician needs to provide recommendations about how to upgrade backup solutions for a site in an area that has frequent hurricanes and an unstable power grid. Which of the following should the technician recommend implementing?

A. High availability
B. Regionally diverse backups
C. On-site backups
D. Incremental backups

Correct Answer: B
Section:
Explanation:
Regionally diverse backups are backups that are stored in different geographic locations, preferably far away from the primary site1. This way, if a disaster such as a hurricane or a power outage affects one location, the backups in another location will still be available and accessible2. Regionally diverse backups can help ensure business continuity and data recovery in case of a disaster3. The other options are not the best backup solutions for a site in an area that has frequent hurricanes and an unstable power grid. High availability is a feature that allows a system to remain operational and accessible even if one or more components fail, but it does not protect against data loss or corruption4. On-site backups are backups that are stored in the same location as the primary site, which means they are vulnerable to the same disasters that can affect the primary site. Incremental backups are backups that only store the changes made since the last backup, which means they require less storage space and bandwidth, but they also depend on previous backups to restore data and may not be sufficient for disaster recovery.

QUESTION 70
A technician is troubleshooting application crashes on a Windows workstation. Each time the workstation user tries to open a website in a browser, the following message is displayed:
crypt32.d11 is missing not found
Which of the following should the technician attempt FIRST?

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

Correct Answer: D
Section:
Explanation:
If this file is missing or corrupted, it can cause application crashes or errors when trying to open websites in a browser. To fix this, the technician can perform a system file check, which is a utility that scans and repairs corrupted or missing system files1. To perform a system file check, the technician can follow these steps:
Open the Command Prompt as an administrator. To do this, type cmd in the search box on the taskbar, right-click on Command Prompt, and select Run as administrator. In the Command Prompt window, type sfc /scannow and hit Enter. This will start the scanning and repairing process, which may take some time.
Wait for the process to complete. If any problems are found and fixed, you will see a message saying Windows Resource Protection found corrupt files and successfully repaired them. If no problems are found, you will see a message saying Windows Resource Protection did not find any integrity violations.
Restart your computer and check if the issue is resolved.

QUESTION 71
A user needs assistance installing software on a Windows PC but will not be in the office. Which of the following solutions would a technician MOST likely use to assist the user without having to install additional software?

A. VPN
B. MSRA
C. SSH
D. RDP

Correct Answer: B
Section:
Explanation:
MSRA stands for Microsoft Remote Assistance, and it is a feature that allows a technician to remotely view and control another user’s Windows PC with their permission. MSRA is built-in to Windows and does not require any additional software installation. To use MSRA, the technician and the user need to follow these steps:
On the user’s PC, type msra in the search box on the taskbar and select Invite someone to connect to your PC and help you, or offer to help someone else.
Select Save this invitation as a file and choose a location to save the file. This file contains a password that the technician will need to connect to the user’s PC.
Send the file and the password to the technician via email or another secure method. On the technician’s PC, type msra in the search box on the taskbar and select Help someone who has invited you.
Select Use an invitation file and browse to the location where the file from the user is saved. Enter the password when prompted.
The user will see a message asking if they want to allow the technician to connect to their PC. The user should select Yes.
The technician will see the user’s desktop and can request control of their PC by clicking Request control on the top bar. The user should allow this request by clicking Yes. The technician can now view and control the user’s PC and assist them with installing software.

QUESTION 72
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

Correct Answer: C
Section:

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.

QUESTION 73
A technician receives a call from a user who is unable to open Outlook. The user states that Outlook worked fine yesterday, but the computer may have restarted sometime overnight. Which of the following is the MOST likely reason Outlook has stopped functioning?

A. Spam filter installation
B. Invalid registry settings
C. Malware infection
D. Operating system update

Correct Answer: D
Section:
Explanation:
Operating system updates can sometimes cause compatibility issues with some applications, such as Outlook, that may prevent them from opening or working properly. This can happen if the update changes some system files or settings that Outlook relies on, or if the update conflicts with some Outlook add-ins or extensions. To fix this, the technician can try some of these troubleshooting steps:
Start Outlook in safe mode and disable add-ins. Safe mode is a way of starting Outlook without any add-ins or extensions that may interfere with its functionality. To start Outlook in safe mode, press and hold the Ctrl key while clicking on the Outlook icon. You should see a message asking if you want to start Outlook in safe mode. Click Yes. If Outlook works fine in safe mode, it means one of the add- ins is causing the problem. To disable add-ins, go to File &gt; Options &gt; Add-ins. In the Manage drop- down list, select COM Add-ins and click Go. Uncheck any add-ins that you don't need and click OK. Restart Outlook normally and check if the issue is resolved4.
Create a new Outlook profile. A profile is a set of settings and information that Outlook uses to manage your email accounts and data. Sometimes, a profile can get corrupted or damaged and cause Outlook to malfunction. To create a new profile, go to Control Panel &gt; Mail &gt; Show Profiles. Click Add and follow the instructions to set up a new profile with your email account. Make sure to select the option to use the new profile as the default one. Restart Outlook and check if the issue is resolved5.
Repair your Outlook data files. Data files are files that store your email messages, contacts, calendar events, and other items on your computer. Sometimes, data files can get corrupted or damaged and cause Outlook to malfunction. To repair your data files, you can use a tool called scanpst.exe, which is located in the same folder where Outlook is installed (usually C:\Program Files\Microsoft Office\root\Office16). To use scanpst.exe, close Outlook and locate the tool in the folder. Double-click on it and browse to the location of your data file (usually
C:\Users\username\AppData\Local\Microsoft\Outlook). Select the file and click Start to begin the scanning and repairing process. When it's done, restart Outlook and check if the issue is resolved. Run the /resetnavpane command. The navigation pane is the panel on the left side of Outlook that shows your folders and accounts. Sometimes, the navigation pane can get corrupted or damaged and cause Outlook to malfunction. To reset the navigation pane, press Windows key + R to open the Run dialog box, or open the Command Prompt. Type outlook.exe /resetnavpane and hit Enter. This will clear and regenerate the navigation pane settings for Outlook. Restart Outlook and check if the issue is resolved.

QUESTION 74
Which of the following editions of Windows 10 requires reactivation every 180 days?

A. Enterprise
B. Pro for Workstation
C. Home
D. Pro

Correct Answer: A
Section:
Explanation:
Windows 10 Enterprise is an edition of Windows 10 that is designed for large organizations that need advanced security and management features. Windows 10 Enterprise can be activated using different methods, such as Multiple Activation Key (MAK), Active Directory-based Activation (ADBA), or Key Management Service (KMS)1. KMS is a method of activation that uses a local server to activate multiple devices on a network. KMS activations are valid for 180 days and need to be renewed periodically by connecting to the KMS server2. If a device does not renew its activation within 180 days, it will enter a grace period of 30 days, after which it will display a warning message and lose some functionality until it is reactivated3. The other editions of Windows 10 do not require reactivation every 180 days. Windows 10 Pro for Workstation is an edition of Windows 10 that is designed

for high-performance devices that need advanced features such as ReFS file system, persistent memory, and faster file sharing. Windows 10 Pro for Workstation can be activated using a digital license or a product key. Windows 10 Home is an edition of Windows 10 that is designed for personal or home use. Windows 10 Home can be activated using a digital license or a product key. Windows 10 Pro is an edition of Windows 10 that is designed for business or professional use. Windows 10 Pro can be activated using a digital license or a product key. None of these editions require reactivation every 180 days unless there are significant hardware changes or other issues that affect the activation status.

QUESTION 75

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

A. Stop code

B. Event Mewer

C. Services

D. System Configuration

Correct Answer: A
Section:
Explanation:

When a Blue Screen of Death (BSOD) appears on a Windows workstation, it indicates that there is a serious problem with the operating system. The stop code displayed on the BSOD can provide valuable information to help determine the cause of the issue. The stop code is a specific error code that is associated with the BSOD, and it can help identify the root cause of the problem. In this scenario, the user has encountered a BSOD and has restarted the PC, only to see the BSOD reappear. This suggests that the problem is persistent and requires further investigation. By analyzing the stop code displayed on the BSOD, a technician can begin to identify the underlying issue and take appropriate actions to resolve it.

QUESTION 76

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

A. msinfo32

B. perfmon

C. regedit

D. taskmgr

Correct Answer: D
Section:
Explanation:

When troubleshooting boot times for a user, a technician may want to check which programs are starting with the operating system to identify any that may be slowing down the boot process. MSConfig is a tool that can be used to view startup items on a Windows system, but it may not always be available or functional.

In this scenario, the technician receives a message that MSConfig cannot be used to view startup items. As an alternative, the technician can use Task Manager (taskmgr), which can also display the programs that run at startup. To access the list of startup items in Task Manager, the technician can follow these steps:

Open Task Manager by pressing Ctrl+Shift+Esc.

Click the "Startup" tab.

The list of programs that run at startup will be displayed.

QUESTION 77

A desktop engineer is deploying a master image. Which of the following should the desktop engineer consider when building the master image? (Select TWO).

A. Device drivers

B. Keyboard backlight settings

C. Installed application license keys

D. Display orientation
E. Target device power supply
F. Disabling express charging

Correct Answer: A, C
Section:
Explanation:
A. Device drivers23: Device drivers are software components that enable the operating system to communicate with hardware devices. Different devices may require different drivers, so the desktop engineer should include the appropriate drivers in the master image or configure the deployment process to install them automatically.
C. Installed application license keys2: Installed application license keys are codes that activate or authenticate software applications. Some applications may require license keys to be entered during installation or after deployment. The desktop engineer should include the license keys in the master image or configure the deployment process to apply them automatically.

QUESTION 78
A technician is setting up a conference room computer with a script that boots the application on login. Which of the following would the technician use to accomplish this task? (Select TWO).

A. File Explorer
B. Startup Folder
C. System Information
D. Programs and Features
E. Task Scheduler
F. Device Manager

Correct Answer: B, E
Section:
Explanation:
B. Startup Folder1: The Startup folder is a special folder that contains shortcuts to programs or scripts that will run automatically when a user logs on. The technician can create a shortcut to the script and place it in the Startup folder for the conference room computer or for all users.
E. Task Scheduler23: The Task Scheduler is a tool that allows you to create tasks that run at specified times or events. The technician can create a task that runs the script at logon for the conference room computer or for all users.

QUESTION 79
A neighbor successfully connected to a user's Wi-Fi network. Which of the following should the user do after changing the network configuration to prevent the neighbor from being able to connect again?

A. Disable the SSID broadcast.
B. Disable encryption settings.
C. Disable DHCP reservations.
D. Disable logging.

Correct Answer: A
Section:
Explanation:
A. Disable the SSID broadcast1: The SSID broadcast is a feature that allows a Wi-Fi network to be visible to nearby devices. Disabling the SSID broadcast can make the network harder to find by unauthorized users, but it does not prevent them from accessing it if they know the network name and password.

QUESTION 80
A technician is troubleshooting a PC that has been performing poorly. Looking at the Task Manager, the technician sees that CPU and memory resources seem fine, but disk throughput is at 100%.
Which of the following types of malware is the system MOST likely infected with?

A. Keylogger
B. Rootkit
C. Ransomware
D. Trojan

Correct Answer: C
Section:
Explanation:
Ransomware is a type of malware that encrypts the files on the victim’s computer and demands a ransom for their decryption. Ransomware can cause high disk throughput by encrypting large amounts of data in a short time.

QUESTION 81
A homeowner recently moved and requires a new router for the new ISP to function correctly. The internet service has been installed and has been confirmed as functional. Which of the following is the FIRST step the homeowner should take after installation of all relevant cabling and hardware?

A. Convert the PC from a DHCP assignment to a static IP address.
B. Run a speed test to ensure the advertised speeds are met.
C. Test all network sharing and printing functionality the customer uses.
D. Change the default passwords on new network devices.

Correct Answer: D
Section:
Explanation:
When a homeowner moves and sets up a new router for the new ISP it is important to take appropriate security measures to protect their network from potential security threats. The FIRST step that the homeowner should take after installation of all relevant cabling and hardware is to change the default passwords on new network devices.
Most modern routers come with default usernames and passwords that are widely known to potential attackers. If these defaults are not changed, it could make it easier for external attackers to gain unauthorized access to the network. Changing the passwords on new network devices is a simple but effective way to improve the security posture of the network.

QUESTION 82
A user rotates a cell phone horizontally to read emails, but the display remains vertical, even though the settings indicate autorotate is on. VT1ich of the following will MOST likely resolve the issue?

A. Recalibrating the magnetometer
B. Recalibrating the compass
C. Recalibrating the digitizer
D. Recalibrating the accelerometer

Correct Answer: D
Section:
Explanation:
When a user rotates a cell phone horizontally to read emails and the display remains vertical, even though the settings indicate autorotate is on, this is typically due to a problem with the phone's accelerometer. The accelerometer is the sensor that detects changes in the phone's orientation and adjusts the display accordingly. If the accelerometer is not calibrated correctly, the display may not rotate as expected.
Recalibrating the accelerometer is the most likely solution to this issue. The process for recalibrating the accelerometer can vary depending on the specific device and operating system, but it typically involves going to the device's settings and finding the option to calibrate or reset the sensor. Users may need to search their device's documentation or online resources to find specific instructions for their device.

QUESTION 83
Which of the following is the proper way for a technician to dispose of used printer consumables?

A. Proceed with the custom manufacturer's procedure.
B. Proceed with the disposal of consumables in standard trash receptacles.

C. Empty any residual ink or toner from consumables before disposing of them in a standard recycling bin.

D. Proceed with the disposal of consumables in standard recycling bins.

Correct Answer: A
Section:
Explanation:
When it comes to disposing of used printer consumables , it is important to follow the manufacturer's instructions or guidelines for proper disposal, as different types of consumables may require different disposal procedures. Some manufacturers provide specific instructions for proper disposal, such as sending the used consumables back to the manufacturer or using special recycling programs.
Therefore, the proper way for a technician to dispose of used printer consumables is to proceed with the custom manufacturer's procedure , if provided. This option ensures that the disposal is handled in an environmentally friendly and safe manner.

QUESTION 84
A large company is selecting a new Windows operating system and needs to ensure it has built-in encryption and endpoint protection. Which of the following Windows versions will MOST likely be selected?

A. Home

B. Pro

C. Pro for Workstations

D. Enterprise

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

QUESTION 85
A user tries to access commonly used web pages but is redirected to unexpected websites. Clearing the web browser cache does not resolve the issue. Which of the following should a technician investigate NEXT to resolve the issue?

A. Enable firewall ACLs.

B. Examine the localhost file entries.

C. Verify the routing tables.

D. Update the antivirus definitions.

Correct Answer: B
Section:
Explanation:
A possible cause of the user being redirected to unexpected websites is that the localhost file entries have been modified by malware or hackers to point to malicious or unwanted websites. The localhost file is a text file that maps hostnames to IP addresses and can override DNS settings. By examining the localhost file entries, a technician can identify and remove any suspicious or unauthorized entries that may cause the redirection issue.
Enabling firewall ACLs may not resolve the issue if the firewall rules do not block the malicious or unwanted websites. Verifying the routing tables may not resolve the issue if the routing configuration is correct and does not affect the web traffic. Updating the antivirus definitions may help prevent future infections but may not remove the existing malware or changes to the localhost file. Reference: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.3

QUESTION 86
A network technician installed a SOHO router for a home office user. The user has read reports about home routers being targeted by malicious actors and then used in DDoS attacks. Which of the following can the technician MOST likely do to defend against this threat?

A. Add network content filtering.
B. Disable the SSID broadcast.
C. Configure port forwarding.
D. Change the default credentials.

Correct Answer: D
Section:
Explanation:
One of the most effective ways to defend against malicious actors targeting home routers for DDoS attacks is to change the default credentials of the router. The default credentials are often well- known or easily guessed by attackers, who can then access and compromise the router settings and firmware. By changing the default credentials to strong and unique ones, a technician can prevent unauthorized access and configuration changes to the router. Adding network content filtering may help block some malicious or unwanted websites but may not prevent attackers from exploiting router vulnerabilities or backdoors. Disabling the SSID broadcast may help reduce the visibility of the wireless network but may not prevent attackers from scanning or detecting it. Configuring port forwarding may help direct incoming traffic to specific devices or services but may not prevent attackers from sending malicious packets or requests to the router. Reference: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 3.3

QUESTION 87
A technician is preparing to remediate a Trojan virus that was found on a workstation. Which of the following steps should the technician complete BEFORE removing the virus?

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

Correct Answer: A
Section:
Explanation:
Before removing a Trojan virus from a workstation, a technician should disable System Restore. System Restore is a feature that allows users to restore their system to a previous state in case of problems or errors. However, System Restore can also restore infected files or registry entries that were removed by antivirus software or manual actions. By disabling System Restore, a technician can ensure that the Trojan virus is completely removed and does not reappear after a system restore operation. Scheduling a malware scan may help detect and remove some malware but may not be effective against all types of Trojan viruses. Educating the end user may help prevent future infections but does not address the current issue of removing the Trojan virus. Running Windows Update may help patch some security vulnerabilities but does not guarantee that the Trojan virus will be removed. Reference: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.3

QUESTION 88
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. MSDS
B. EULA
C. UAC
D. AUP

Correct Answer: D
Section:
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. Reference: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 5.1

QUESTION 89
A user lost a company tablet that was used for customer intake at a doctor's office. Which of the following actions would BEST protect against unauthorized access of the data?

A. Changing the office's Wi-Fi SSID and password
B. Performing a remote wipe on the device
C. Changing the user's password
D. Enabling remote drive encryption

Correct Answer: B
Section:
Explanation:
The best action to protect against unauthorized access of the data on the lost company tablet is to perform a remote wipe on the device. A remote wipe is a feature that allows an administrator or a user to erase all the data and settings on a device remotely, usually through a web portal or an email command. A remote wipe can help prevent the data from being accessed or compromised by anyone who finds or steals the device. Changing the office's Wi-Fi SSID and password may prevent the device from connecting to the office network but may not prevent the data from being accessed locally or through other networks. Changing the user's password may prevent the device from logging in to the user's account but may not prevent the data from being accessed by other means or accounts. Enabling remote drive encryption may protect the data from being read by unauthorized parties but may not be possible if the device is already lost or turned off. Reference: CompTIA A+ Core 2 (220- 1002) Certification Exam Objectives Version 4.0, Domain 3.1

QUESTION 90
Which of the following is used to explain issues that may occur during a change implementation?

A. Scope change
B. End-user acceptance
C. Risk analysis
D. Rollback plan

Correct Answer: C
Section:
Explanation:
Risk analysis is used to explain issues that may occur during a change implementation. Risk analysis is a process of identifying, assessing and prioritizing potential risks that may affect a project or an activity. Risk analysis can help determine the likelihood and impact of various issues that may arise during a change implementation, such as technical errors, compatibility problems, security breaches, performance degradation or user dissatisfaction. Risk analysis can also help plan and prepare for mitigating or avoiding these issues. Scope change is a modification of the original goals, requirements or deliverables of a project or an activity. Scope change is not used to explain issues that may occur during a change implementation but to reflect changes in expectations or needs of the stakeholders. End-user acceptance is a measure of how well the users are satisfied with and adopt a new system or service. End-user acceptance is not used to explain issues that may occur during a change implementation but to evaluate the success and effectiveness of the change. Rollback plan is a contingency plan that describes how to restore a system or service to its previous state in case of a failed or problematic change implementation. Rollback plan is not used to explain issues that may occur during a change implementation but to recover from them. Reference:
CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 5.2

QUESTION 91
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

Correct Answer: B, E
Section:
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. Reference: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 3.3

QUESTION 92
A technician is troubleshooting an issue with a computer that contains sensitive information. The technician determines the computer needs to be taken off site for repair. Which of the following should the technician do NEXT?

A. Remove the HDD and then send the computer for repair.
B. Check corporate polices for guidance.
C. Delete the sensitive information before the computer leaves the building.
D. Get authorization from the manager.

Correct Answer: D
Section:
Explanation:
The next step that the technician should do before taking the computer off site for repair is to get authorization from the manager. Getting authorization from the manager is important because it ensures that the technician has permission and approval to remove the computer from the premises and perform the repair work off site. Getting authorization from the manager can also help document and communicate the reason and duration of the repair and avoid any misunderstanding or conflict with the user or the organization. Removing the HDD and then sending the computer for repair may not be feasible or necessary if the issue is not related to the HDD or if the HDD contains essential data or software for the repair. Checking corporate policies for guidance may be a good step but it does not replace getting authorization from the manager who is responsible for the computer and its data. Deleting the sensitive information before the computer leaves the building may not be possible or advisable if the issue prevents access to the data or if the data is needed for troubleshooting or recovery purposes. Reference: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 5.1

QUESTION 93
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

Correct Answer: A
Section:
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. Reference: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.6

QUESTION 94
A user receives a call from someone who claims to be from the user's bank and requests information to ensure the user's account is safe. Which of the following social-engineering attacks is the user experiencing?

A. Phishing
B. Smishing
C. Whaling
D. Vishing

Correct Answer: D
Section:
Explanation:
The user is experiencing a vishing attack. Vishing stands for voice phishing and is a type of social- engineering attack that uses phone calls or voice messages to trick users into revealing personal or financial information. Vishing attackers often pretend to be from legitimate organizations, such as banks, government agencies or service providers, and use various tactics, such as urgency, fear or reward, to persuade users to comply with their requests. Phishing is a type of social-engineering attack that uses fraudulent emails or websites to trick users into revealing personal or financial information. Phishing does not involve phone calls or voice messages. Smishing is a type of social- engineering attack that uses text messages or SMS to trick users into revealing personal or financial information. Smishing does not involve phone calls or voice messages. Whaling is a type of social-engineering attack that targets high-profile individuals, such as executives, celebrities or politicians, to trick them into revealing personal or financial information. Whaling does not necessarily involve phone calls or voice messages. Reference: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 3.1

QUESTION 95
A user is trying to use a third-party USB adapter but is experiencing connection issues. Which of the following tools should the technician use to resolve this issue?

A. taskschd.msc
B. eventvwr.msc
C. de vmgmt. msc
D. diskmgmt.msc

Correct Answer: C
Section:
Explanation:
The tool that the technician should use to resolve the connection issues with the third-party USB adapter is devmgmt.msc. Devmgmt.msc is a command that opens the Device Manager, which is a utility that allows users to view and manage the hardware devices and drivers installed on a computer. The technician can use the Device Manager to check the status, properties and compatibility of the USB adapter and its driver, and perform actions such as updating, uninstalling or reinstalling the driver, enabling or disabling the device, or scanning for hardware changes. Taskschd.msc is a command that opens the Task Scheduler, which is a utility that allows users to create and manage tasks that run automatically at specified times or events. The Task Scheduler is not relevant or useful for resolving connection issues with the USB adapter. Eventvwr.msc is a command that opens the Event Viewer, which is a utility that allows users to view and monitor the system logs and events. The Event Viewer may provide some information or clues about the connection issues with the USB adapter, but it does not allow users to manage or troubleshoot the device or its driver directly. Diskmgmt.msc is a command that opens the Disk Management, which is a utility that allows users to view and manage the disk drives and partitions on a computer. The Disk Management is not relevant or useful for resolving connection issues with the USB adapter.
Reference: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.6

QUESTION 96
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

Correct Answer: A
Section:
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. Reference: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 5.1

QUESTION 97
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.

Correct Answer: B
Section:
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.

QUESTION 98
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

Correct Answer: A, D
Section:
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 dat a. Spyware can also alter the settings or functionality of the user's system without their consent.

QUESTION 99
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

Correct Answer: A
Section:
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.

QUESTION 100
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

Correct Answer: D
Section:
Explanation:

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 medi a. 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.

QUESTION 101
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

Correct Answer: D
Section:
Explanation:

Explore The correct answer is D. Internet Options. The Internet Options utility in Windows allows you to configure various settings related to your internet connection, including the proxy server settings. To access the Internet Options utility, you can either open the Control Panel and click on Internet Options, or open any web browser and click on the Tools menu and then on Internet Options. In the Internet Options window, go to the Connections tab and click on the LAN settings button. Here, you can enable or disable the use of a proxy server, as well as enter the address and port number of the proxy server you want to use12.
Security and Maintenance is a utility in Windows that allows you to view and manage the security and maintenance status of your computer, such as firewall, antivirus, backup, troubleshooting, and recovery settings. It does not have any option to configure proxy server settings.
Network and Sharing Center is a utility in Windows that allows you to view and manage your network connections, such as Wi-Fi, Ethernet, VPN, or dial-up. It also allows you to change network settings, such as network discovery, file and printer sharing, homegroup, and adapter settings. It does not have any option to configure proxy server settings.
Windows Defender Firewall is a utility in Windows that allows you to enable or disable the firewall protection for your computer, as well as configure firewall rules for inbound and outbound traffic. It does not have any option to configure proxy server settings.

QUESTION 102
A technician receives a help desk ticket from a user who is unable to update a phone. The technician investigates the issue and notices the following error message: Insufficient storage space While analyzing the phone, the technician does not discover any third-party' applications or photos.
Which of the following is the best way to resolve the issue?

A. Exchange the device for a newer one.
B. Upgrade the onboard storage
C. Allocate more space by removing factory applications
D. Move factory applications to external memory.

Correct Answer: D
Section:
Explanation:
The best way to resolve the issue is to move factory applications to external memory. This will free up some space on the phone's internal storage, which is required for updating the phone. To do this, you can follow these steps1:
Insert a microSD card into your phone if you don't have one already.
Go to Settings > Apps and tap on the app you want to move.
Tap on Storage and then on Change.
Select the SD card option and tap on Move.
You may need to repeat this process for multiple apps until you have enough space to update your phone. Alternatively, you can also clear the cache and data of some apps, or uninstall the apps that you don't use frequently.
You can find more information on how to fix insufficient storage error on your phone in these articles234. I hope this helps.

QUESTION 103
A company recently experienced a security incident in which a USB drive containing malicious software was able to covertly install malware on a workstation_ Which of the following actions should be taken to prevent this Incident from happening again? (Select two).

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

Correct Answer: E, F
Section:
Explanation:
The correct answers are E and F. Disabling AutoRun and updating the antivirus definitions are two actions that should be taken to prevent the incident from happening again.
AutoRun is a feature of Windows that automatically executes a predetermined action when a removable media such as a USB drive is inserted in a computer. For example, AutoRun can launch or install a new program on the media, or open the file in File Explorer. However, this feature can also be exploited by malicious software that can run without the user's consent or knowledge. Therefore, disabling AutoRun can help prevent accidental installation of viruses and other malware from USB drives123.
Updating the antivirus definitions is another important action that can help prevent malware infections from USB drives. Antivirus definitions are files that contain information about the latest known threats and how to detect and remove them. By updating the antivirus definitions regularly, you can ensure that your antivirus software can recognize and block any malicious software that may be on the USB drive before it can harm your computer45.
A host-based IDS is a system that monitors and analyzes the activity on a single computer or device for any signs of intrusion or malicious behavior. A host-based IDS can help detect and prevent malware infections from USB drives, but it is not a sufficient action by itself. A host-based IDS needs to be complemented by other security measures, such as disabling AutoRun and updating the antivirus definitions6.
Restricting login times, enabling a BIOS password, and updating the password complexity are all actions that can help improve the security of a computer or device, but they are not directly related to preventing malware infections from USB drives. These actions can help prevent unauthorized access to the computer or device, but they do not affect how the computer or device interacts with the USB drive or its contents.
Restricting user permissions is an action that can help limit the damage that malware can cause on a computer or device, but it does not prevent the malware from being installed in the first place.
Restricting user permissions means limiting what actions a user can perform on the computer or device, such as installing or deleting programs, modifying system settings, or accessing certain files or folders. By restricting user permissions, you can reduce the impact of malware infections by preventing them from affecting other users or system components7.

QUESTION 104
A new employee is having difficulties using a laptop with a docking station The laptop is connected to the docking station, and the laptop is closed. The external monitor works for a few seconds, but then the laptop goes to sleep. Which of the following options should the technician configure in order to fix the Issue?

A. Hibernate
B. Sleep/suspend

C. Choose what closing the lid does
D. Turn on fast startup

Correct Answer: C
Section:
Explanation:
The correct answer is C. Choose what closing the lid does. This option allows you to configure how the laptop behaves when you close the lid, such as whether it goes to sleep, hibernates, shuts down, or does nothing. To access this option, you can follow these steps :
Go to Settings > System > Power & sleep.
Click on Additional power settings on the right side.
Click on Choose what closing the lid does on the left side.
Under When I close the lid, select Do nothing for both On battery and Plugged in.
Click on Save changes.
This will prevent the laptop from going to sleep when you close the lid while it is connected to the docking station and the external monitor.
Hibernate, sleep/suspend, and turn on fast startup are not the options that should be configured to fix the issue. Hibernate and sleep/suspend are both power-saving modes that allow you to resume your work without losing any dat a. However, they also turn off the display and other components of the laptop, which means you will not be able to use the external monitor when the laptop is closed. Turn on fast startup is a feature that reduces the boot time of Windows by saving some system information to a file when you shut down. It does not affect how the laptop behaves when you close the lid .

QUESTION 105
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

Correct Answer: B
Section:
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.

QUESTION 106
Which of the following filesystem types does macOS use?

A. ext4
B. exFAT

C. NTFS
D. APFS

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

QUESTION 107
A user is unable to access several documents saved on a work PC. A technician discovers the files were corrupted and must change several system settings within Registry Editor to correct the issue.
Which of the following should the technician do before modifying the registry keys?

A. Update the anti-malware software.
B. Create a restore point.
C. Run the PC in sate mode.
D. Roll back the system updates.

Correct Answer: B
Section:
Explanation:
A restore point is a snapshot of the system settings and configuration at a specific point in time2. Creating a restore point before modifying the registry keys allows the technician to revert the system back to a previous state if something goes wrong or causes instability2. Updating the antimalware software, running the PC in safe mode, and rolling back the system updates are not necessary steps before modifying the registry keys.

QUESTION 108
A systems administrator is configuring centralized desktop management for computers on a domain. The management team has decided that all users' workstations should have the same network drives, printers, and configurations. Which of the following should the administrator use to accomplish this task?

A. Network and Sharing Center
B. net use
C. User Accounts
D. regedit
E. Group Policy

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

QUESTION 109
A user connected an external hard drive but is unable to see it as a destination to save files. Which of the following tools will allow the drive to be formatted?

A. Disk Management
B. Device Manager
C. Disk Cleanup
D. Disk Defragmenter

Correct Answer: A
Section:
Explanation:
Disk Management is a tool that allows users to create, format, delete, shrink, extend, and manage partitions on hard drives. If the external hard drive is not formatted or has an incompatible filesystem type, Disk Management can be used to format it with a supported filesystem type such as NTFS, FAT32, or exFAT. Device Manager, Disk Cleanup, and Disk Defragmenter are not tools that can format a hard drive.

QUESTION 110
A technician is concerned about a large increase in the number of whaling attacks happening in the industry. The technician wants to limit the company's risk to avoid any issues. Which of the following items should the technician implement?

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

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

QUESTION 111
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

Correct Answer: D
Section:
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.

QUESTION 112
A technician sees a file that is requesting payment to a cryptocurrency address. Which of the following should the technician do first?

A. Quarantine the computer.
B. Disable System Restore.
C. Update the antivirus software definitions.
D. Boot to safe mode.

Correct Answer: A
Section:

Explanation:
Quarantining the computer means isolating it from the network and other devices to prevent the spread of malware or ransomware. Ransomware is a type of malware that encrypts the files on a computer and demands payment (usually in cryptocurrency) to restore them. If a technician sees a file that is requesting payment to a cryptocurrency address, it is likely that the computer has been infected by ransomware. Quarantining the computer should be the first step to contain the infection and prevent further damage. Disabling System Restore, updating the antivirus software definitions, and booting to safe mode are not steps that should be done before quarantining the computer.

QUESTION 113
A user contacts the help desk to request assistance with a program feature. The user is in a different building but on the same network as the help desk technician. Which of the following should the technician use to assist the user?

A. AAA
B. SSH
C. RDP
D. VPN

Correct Answer: C
Section:
Explanation:
RDP stands for Remote Desktop Protocol and it is a protocol that allows a user to remotely access and control another computer over a network. A technician can use RDP to assist a user who is in a different building but on the same network by connecting to the user's computer and viewing their screen, keyboard, and mouse. AAA, SSH, and VPN are not protocols that can be used to assist a user with a program feature.

QUESTION 114
A technician is installing RAM in a new workstation and needs to protect against electrostatic discharge. Which of the following will best resolve this concern?

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

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

QUESTION 115
The battery life on an employee's new phone seems to be drastically less than expected, and the screen stays on for a very long time after the employee sets the phone down. Which of the following should the technician check first to troubleshoot this issue? (Select two).

A. Screen resolution
B. Screen zoom
C. Screen timeout
D. Screen brightness
E. Screen damage
F. Screen motion smoothness

Correct Answer: C, D
Section:
Explanation:
Screen timeout is the setting that determines how long the screen stays on after the user stops interacting with the phone. Screen brightness is the setting that determines how much light the screen emits. Both of these settings affect the battery life of the phone, as keeping the screen on longer and brighter consumes more power than turning it off sooner and dimmer. A technician should check these settings first to troubleshoot the issue of low battery life and adjust them accordingly. Screen resolution, screen zoom, screen damage, and screen motion smoothness are not settings that directly affect the battery life or the screen staying on for a long time.

QUESTION 116
A hard drive that previously contained PI I needs to be repurposed for a public access workstation.
Which of the following data destruction methods should a technician use to ensure data is completely removed from the hard drive?

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

Correct Answer: A
Section:
Explanation:
Shredding is a data destruction method that physically destroys the hard drive by cutting it into small pieces using a machine. Shredding ensures that data is completely removed from the hard drive and cannot be recovered by any means. Shredding is suitable for hard drives that contain PII (personally identifiable information), which is any information that can be used to identify, contact, or locate an individual. Degaussing, low-level formatting, and recycling are not data destruction methods that can guarantee complete data removal from a hard drive.

QUESTION 117
Which of the following best describes when to use the YUM command in Linux?

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

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

QUESTION 118
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.

Correct Answer: B
Section:

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 onetime 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.

QUESTION 119
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

Correct Answer: B
Section:
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.

QUESTION 120
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

Correct Answer: B
Section:
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.

QUESTION 121
A company's assets are scanned annually. Which of the following will most likely help the company gain a holistic view of asset cost?

A. Creating a database
B. Assigning users to assets
C. Inventorying asset tags
D. Updating the procurement account owners

Correct Answer: A
Section:
Explanation:

Creating a database is the most likely option to help the company gain a holistic view of asset cost. A database can store and organize information about the assets, such as purchase date, depreciation value, maintenance cost, warranty status, and replacement cost. Assigning users to assets, inventorying asset tags, and updating the procurement account owners are important steps for asset management, but they do not directly provide a holistic view of asset cost. Reference:
Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 18
CompTIA A+ Complete Study Guide: Core 1 Exam 220-1101 and Core 2 Exam ..., page 101

QUESTION 122
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.

Correct Answer: C
Section:
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. Reference:
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

QUESTION 123
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

Correct Answer: A
Section:
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. Reference:
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

QUESTION 124
A technician is working on a Windows 10 PC that has unwanted applications starting on boot. Which of the following tools should the technician use to disable applications on startup?

A. System Configuration

B. Task Manager
C. Performance Monitor
D. Group Policy Editor

Correct Answer: B
Section:
Explanation:
Task Manager is the best tool to use to disable applications on startup in Windows 10. Task Manager is a built-in utility that shows the current processes, performance, and users on a system. It also has a Startup tab that lists the applications that run on boot and their impact on the system. The technician can use Task Manager to disable or enable any application on startup by right-clicking on it and selecting the appropriate option. System Configuration, Performance Monitor, and Group Policy Editor are other tools that can be used to manage system settings, but they are not as simple or convenient as Task Manager for this task. Reference:
Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 13
CompTIA A+ Complete Study Guide: Core 1 Exam 220-1101 and Core 2 Exam ..., page 103

QUESTION 125
Which of the following is an advantage of using WPA2 instead of WPA3?

A. Connection security
B. Encryption key length
C. Device compatibility
D. Offline decryption resistance

Correct Answer: C
Section:
Explanation:
Device compatibility is an advantage of using WPA2 instead of WPA3. WPA2 is the previous version of the Wi-Fi Protected Access protocol, which provides security and encryption for wireless networks. WPA3 is the latest version, which offers improved security features, such as stronger encryption, enhanced protection against brute-force attacks, and easier configuration. However, WPA3 is not backward compatible with older devices that only support WPA2 or earlier protocols.
Therefore, using WPA3 may limit the range of devices that can connect to the wireless network. Connection security, encryption key length, and offline decryption resistance are advantages of using WPA3 instead of WPA2. Reference:
Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 24
CompTIA A+ Certification All-in-One Exam Guide (Exams 220-1101 & ..., page 1000

QUESTION 126
A large university wants to equip all classrooms with high-definition IP videoconferencing equipment. Which of the following would most likely be impacted in this situation?

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

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

Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 20
CompTIA A+ Complete Study Guide: Core 1 Exam 220-1101 and Core 2 Exam ..., page 104

QUESTION 127
A systems administrator is troubleshooting network performance issues in a large corporate office.
The end users report that traffic to certain internal environments is not stable and often drops. Which of the following command-line tools can provide the most detailed information for investigating the issue further?

A. ipconfig
B. arp
C. nslookup
D. pathping

Correct Answer: D
Section:
Explanation:
Pathping is the best command-line tool to provide the most detailed information for investigating the network performance issue further. Pathping is a utility that combines the functions of ping and tracert, which are two other command-line tools that test network connectivity and latency.
Pathping sends packets to each router on the path to a destination and then computes results based on the packets returned from each hop. Pathping can show the route taken by the packets, the number of hops, the latency of each hop, and the packet loss percentage. This information can help the systems administrator identify where the network problem occurs and how severe it is. Ipconfig, arp, and nslookup are not as useful as pathping for this task. Ipconfig shows the configuration of the network interface card, such as IP address, subnet mask, and default gateway. Arp shows the mapping of IP addresses to MAC addresses in the local network. Nslookup queries DNS servers for
domain name resolution. Reference: Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 21
CompTIA A+ Core 1 (220-1101) and Core 2 (220-1102) Cert Guide, page 457

QUESTION 128
Which of the following would allow physical access to a restricted area while maintaining a record of events?

A. Hard token
B. Access control vestibule
C. Key fob
D. Door Lock

Correct Answer: B
Section:
Explanation:
Access control vestibule is the correct answer for this question. An access control vestibule is a physical security device that consists of two doors that form an enclosed space between them. The first door opens only after verifying the identity of the person entering, such as by using a card reader, biometric scanner, or keypad. The second door opens only after the first door closes, creating a buffer zone that prevents unauthorized access or tailgating. An access control vestibule also maintains a record of events, such as who entered or exited, when, and how. Hard token, key fob, and door lock are not sufficient to meet the requirements of this question. A hard token is a device
that generates a one-time password or code for authentication purposes. A key fob is a small device that can be attached to a key ring and used to unlock doors or start vehicles remotely. A door lock is a mechanism that secures a door from opening without a key or a code. Reference:
Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 25

QUESTION 129
A technician is partitioning a hard disk. The five primary partitions should contain 4TB of free space.
Which of the following partition styles should the technician use to partition the device?

A. EFS

B. GPT
C. MBR
D. FAT32

Correct Answer: B
Section:

QUESTION 130
A user is setting up backups on a workstation. The user wants to ensure that the restore process is as simple as possible. Which of the following backup types should the user select?

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

Correct Answer: A
Section:
Explanation:
Full backup is the best option to ensure that the restore process is as simple as possible. A full backup is a backup type that copies all the data from the source to the destination, regardless of whether the data has changed or not. A full backup provides the most complete and consistent backup of the data, and it allows the user to restore the data from a single backup set without relying on any previous or subsequent backups. Incremental, differential, and synthetic backups are not as simple as full backups for restoring data. An incremental backup is a backup type that copies only the data that has changed since the last backup, whether it was full or incremental. An incremental backup
requires less time and space than a full backup, but it also requires multiple backup sets to restore the data completely. A differential backup is a backup type that copies only the data that has changed since the last full backup. A differential backup requires more time and space than an incremental backup, but it also requires fewer backup sets to restore the data than an incremental backup. A synthetic backup is a backup type that combines a full backup with one or more incremental or differential backups to create a consolidated backup set. A synthetic backup requires less time and bandwidth than a full backup, but it also requires more processing power and storage space than an
incremental or differential backup. Reference:
Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 15
CompTIA A+ Core 1 (220-1101) and Core 2 (220-1102) Cert Guide, page 458

QUESTION 131
Which of the following is used to ensure users have the appropriate level of access to perform their job functions?

A. Access control list
B. Multifactor authentication
C. Least privilege
D. Mobile device management

Correct Answer: C
Section:
Explanation:
Least privilege is the principle that is used to ensure users have the appropriate level of access to perform their job functions. Least privilege means granting users only the minimum amount of access rights and permissions they need to perform their tasks, and nothing more. Least privilege reduces the risk of unauthorized access, data leakage, malware infection, or accidental damage by limiting what users can do on the system or network. Access control list, multifactor authentication, and mobile device management are not principles, but rather mechanisms or methods that can implement least privilege. Access control list is a list that specifies the users or groups that are allowed or denied access to a resource, such as a file, folder, or printer. Multifactor authentication is a method that requires users to provide two or more pieces of evidence to prove their identity, such as a password, a token, or a biometric factor. Mobile device management is a tool that allows managing and securing mobile devices, such as smartphones or tablets, that are used by employees to access corporate data or applications. Reference:
Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 25

[CompTIA Security+ SY0-601 Certification Study Guide], page 1003

QUESTION 132
Which of the following is command options is used to display hidden files and directories?

A. -a
B. -s
C. -lh
D. -t

Correct Answer: A
Section:
Explanation:
The -a option is used to display hidden files and directories in a command-line interface. Hidden files and directories are those that start with a dot (.) and are normally not shown by default. The -a option stands for “all” and shows all files and directories, including the hidden ones. The -a option can be used with commands such as ls, dir, or find to list or search for hidden files and directories.
The -s, -lh, and -t options are not used to display hidden files and directories. The -s option stands for “size” and shows the size of files or directories in bytes. The -lh option stands for “long humanreadable” and shows the size of files or directories in a more readable format, such as KB, MB, or GB.
The -t option stands for “time” and sorts the files or directories by modification time. Reference:
Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 17
CompTIA A+ Complete Study Guide: Core 1 Exam 220-1101 and Core 2 Exam ..., page 107

QUESTION 133
Which of the following file types would be used in the Windows Startup folder to automate copying a personal storage table (.pst file) to a network drive at log-in?

A. .bat
B. .dll
C. .ps1
D. .txt

Correct Answer: A
Section:
Explanation:
The .bat file type would be used in the Windows Startup folder to automate copying a personal storage table (.pst) file to a network drive at log-in. A .bat file is a batch file that contains a series of commands that can be executed by the command interpreter. A .bat file can be used to perform various tasks, such as copying, moving, deleting, or renaming files or directories. A .bat file can be placed in the Windows Startup folder to run automatically when a user logs in to the system. A .bat file can use the copy command to copy a .pst file from a local drive to a network drive. A .pst file is a personal storage table file that contains email messages, contacts, calendars, and other data from
Microsoft Outlook. A .pst file can be backed up to a network drive for security or recovery purposes.
The .dll, .ps1, and .txt file types are not used in the Windows Startup folder to automate copying a .pst file to a network drive at log-in. A .dll file is a dynamic link library file that contains code or data that can be shared by multiple programs. A .dll file cannot be executed directly by the user or the system. A .ps1 file is a PowerShell script file that contains commands or expressions that can be executed by the PowerShell interpreter. A .ps1 file can also perform various tasks, such as copying files or directories, but it requires PowerShell to be installed and configured on the system. A .txt file is a plain text file that contains unformatted text that can be read by any text editor or word processor. A .txt file cannot contain commands or expressions that can be executed by the system. Reference:
Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 18
CompTIA A+ Core 1 (220-1101) and Core 2 (220-1102) Cert Guide, page 459

QUESTION 134
A systems administrator received a request to limit the amount of cellular data a user's Windows 10 tablet can utilize when traveling. Which of the following can the administrator do to best solve the user's issue?

A. Turn on airplane mode.

B. Set the connection to be metered.
C. Configure the device to use a static IP address.
D. Enable the Windows Defender Firewall.

Correct Answer: B
Section:
Explanation:
Setting the connection to be metered is the best solution for limiting the amount of cellular data a user's Windows 10 tablet can utilize when traveling. A metered connection is a network connection that has a data limit or charges fees based on the amount of data used. Windows 10 allows users to set any network connection as metered, which reduces the amount of data that Windows and some apps use in the background. For example, setting a connection as metered will prevent Windows from downloading updates automatically, stop some apps from syncing data online, and disable some live tiles on the Start menu. Setting a connection as metered can help users save cellular data
and avoid extra charges when traveling. Turning on airplane mode, configuring the device to use a static IP address, and enabling the Windows Defender Firewall are not effective solutions for limiting the amount of cellular data a user's Windows 10 tablet can utilize when traveling. Turning on airplane mode will disable all wireless connections on the device, including Wi-Fi, Bluetooth, and cellular data. This will prevent the user from accessing any online services or applications on the tablet. Configuring the device to use a static IP address will assign a fixed IP address to the device instead of obtaining one dynamically from a DHCP server. This will not affect the amount of cellular data the device uses, and it may cause IP conflicts or connectivity issues on some networks. Enabling the Windows Defender Firewall will block or allow incoming and outgoing network traffic based on predefined or custom rules. This will not reduce the amount of cellular data the device uses, and it may interfere with some apps or services that require network access. Reference:
Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 19
CompTIA A+ Complete Study Guide: Core 1 Exam 220-1101 and Core 2 Exam ..., page 108

QUESTION 135
A technician successfully removed malicious software from an infected computer after running updates and scheduled scans to mitigate future risks. Which of the following should the technician do next?

A. Educate the end user on best practices for security.
B. Quarantine the host in the antivirus system.
C. Investigate how the system was infected with malware.
D. Create a system restore point.

Correct Answer: A
Section:
Explanation:
Educating the end user on best practices for security is the next step that the technician should take after successfully removing malicious software from an infected computer. Educating the end user on best practices for security is an important part of preventing future infections and mitigating risks. The technician should explain to the end user how to avoid common sources of malware, such as phishing emails, malicious websites, or removable media. The technician should also advise the end user to use strong passwords, update software regularly, enable antivirus and firewall protection, and backup data frequently. Educating the end user on best practices for security can help the end
user become more aware and responsible for their own security and reduce the likelihood of recurrence of malware infections. Quarantining the host in the antivirus system, investigating how the system was infected with malware, and creating a system restore point are not the next steps that the technician should take after successfully removing malicious software from an infected computer. Quarantining the host in the antivirus system is a step that the technician should take before removing malicious software from an infected computer. Quarantining the host in the antivirus system means isolating the infected computer from the network or other devices to prevent the spread of malware. Investigating how the system was infected with malware is a step that the technician should take during or after removing malicious software from an infected computer. Investigating how the system was infected with malware means identifying the source, type, and impact of malware on the system and documenting the findings and actions taken.
Creating a system restore point is a step that the technician should take before removing malicious software from an infected computer. Creating a system restore point means saving a snapshot of the system's configuration and settings at a certain point in time, which can be used to restore the system in case of failure or corruption. Reference:
Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 15
CompTIA A+ Core 1 (220-1101) and Core 2 (220-1102) Cert Guide, page 458

QUESTION 136
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

Correct Answer: C
Section:
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. Reference:
Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 26

QUESTION 137
A computer technician is investigating a computer that is not booting. The user reports that the computer was working prior to shutting it down last night. The technician notices a removable USB device is inserted, and the user explains the device is a prize the user received in the mail yesterday. Which of the following types of attacks does this describe?

A. Phishing
B. Dumpster diving
C. Tailgating
D. Evil twin

Correct Answer: A
Section:
Explanation:
Phishing is the correct answer for this question. Phishing is a type of attack that uses fraudulent emails or other messages to trick users into revealing sensitive information or installing malicious software. Phishing emails often impersonate legitimate entities or individuals and offer incentives or threats to lure users into clicking on malicious links or attachments. In this scenario, the user received a removable USB device in the mail as a prize, which could be a phishing attempt to infect the user's computer with malware or gain access to the user's data. Dumpster diving, tailgating, and evil twin are not correct answers for this question. Dumpster diving is a type of attack that involves
searching through trash bins or recycling containers to find discarded documents or devices that contain valuable information. Tailgating is a type of attack that involves following an authorized person into a restricted area without proper identification or authorization. Evil twin is a type of attack that involves setting up a rogue wireless access point that mimics a legitimate one to intercept or manipulate network traffic. Reference:
Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 25
[CompTIA Security+ SY0-601 Certification Study Guide], page 1004

QUESTION 138
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

Correct Answer: C
Section:
Explanation:

Remote network installation is the best option for configuring a new server that requires a baremetal 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. Reference:
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

QUESTION 139
A technician needs administrator access on a Windows workstation to facilitate system changes without elevating permissions. Which of the following would best accomplish this task?

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

Correct Answer: B
Section:
Explanation:
Local Users and Groups is the best option to accomplish this task. Local Users and Groups is a tool that allows managing the local user accounts and groups on a Windows workstation. The technician can use this tool to create a new user account with administrator privileges or add an existing user account to the Administrators group. This way, the technician can log in with the administrator account and make system changes without elevating permissions. Group Policy Editor, Device Manager, and System Configuration are not correct answers for this question. Group Policy Editor is a tool that allows configuring policies and settings for users and computers in a domain environment.
Device Manager is a tool that allows managing the hardware devices and drivers on a Windows workstation. System Configuration is a tool that allows modifying the startup options and services on a Windows workstation. None of these tools can directly grant administrator access to a user account. Reference:
Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 13
CompTIA A+ Complete Study Guide: Core 1 Exam 220-1101 and Core 2 Exam ..., page 103

QUESTION 140
A technician receives an invalid certificate error when visiting a website. Other workstations on the same local network are unable to replicate this issue. Which of the following is most likely causing the issue?

A. Date and time
B. User access control
C. UEFI boot mode
D. Log-on times

Correct Answer: A
Section:
Explanation:
Date and time is the most likely cause of the issue. The date and time settings on a workstation affect the validity of the certificates used by websites to establish secure connections. If the date and time are incorrect, the workstation may not recognize the certificate as valid and display an invalid certificate error. Other workstations on the same local network may not have this issue if their date and time are correct. User access control, UEFI boot mode, and log-on times are not likely causes of the issue. User access control is a feature that prevents unauthorized changes to the system by prompting for confirmation or credentials. UEFI boot mode is a firmware interface that controls the
boot process of the workstation. Log-on times are settings that restrict when a user can log in to the workstation. None of these factors affect the validity of the certificates used by websites. Reference:

Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 14
CompTIA A+ Core 1 (220-1101) and Core 2 (220-1102) Cert Guide, page 456

QUESTION 141
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

Correct Answer: C
Section:
Explanation:
Low-level wiping is the best data destruction method for recycling old hard drives for reuse. Lowlevel wiping is a process that overwrites every bit of data on a hard drive with zeros or random patterns, making it impossible to recover any data from the drive. Low-level wiping also restores the 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. Reference:
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

QUESTION 142
Antivirus software indicates that a workstation is infected with ransomware that cannot be quarantined. Which of the following should be performed first to prevent further damage to the host and other systems?

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

Correct Answer: A
Section:
Explanation:
Turning off the machine is the first and most urgent step to prevent further damage to the host and other systems. Ransomware can encrypt files, steal data, and spread to other devices on the network if the infected machine remains online.Turning off the machine will stop the ransomware process and isolate the machine from the network12. The other options are either ineffective or risky. Running a full antivirus scan may not detect or remove the ransomware, especially if it is a new or unknown variant. Removing the LAN card may disconnect the machine from the network, but it will not stop the ransomware from encrypting or deleting files on the local drive. Installing a different endpoint solution may not be possible or helpful if the ransomware has already compromised the system or blocked the installation.

QUESTION 143
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

Correct Answer: B
Section:
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.