

CompTIA.220-1102.vSep-2023.by.Junio.120q

Number: 220-1102

Passing Score: 800

Time Limit: 120

File Version: 9.9

Exam Code: 220-1102

Exam Name: CompTIA A+ Certification Exam: Core 2

Exam A

QUESTION 1

A user is setting up a computer for the first time and would like to create a secondary login with permissions that are different than the primary login. The secondary login will need to be protected from certain content such as games and websites. Which of the following Windows settings should the user utilize to create the secondary login?

- A. Privacy
- B. Accounts
- C. Personalization
- D. Shared resources

Correct Answer: B

Section:

Explanation:

To create a secondary login with different permissions in Windows 10, the user should utilize the Accounts setting. Here are the steps to create a new user account with different permissions:

Right-click the Windows Start menu button.

Select Control Panel.

Select User Accounts.

Select Manage another account.

Select Add a new user in PC settings.

Use the Accounts dialog box to configure a new account.1

QUESTION 2

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

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

Correct Answer: B

Section:

Explanation:

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

QUESTION 3

Which of the following is MOST likely contained in an EULA?

- A. Chain of custody
- B. Backup of software code
- C. Personally identifiable information
- D. Restrictions of use

Correct Answer: D

Section:

Explanation:

An EULA (End-User License Agreement) is a legally binding contract between a software supplier and a customer or end-user, generally made available to the customer via a retailer acting as an intermediary. A EULA specifies in detail the rights and restrictions which apply to the use of the software. Some of the main terms included in an EULA are the terms and scope of the license, any licensing fees, warranties and disclaimers, limitation of liability, revocation or termination of the license, and intellectual property information and restrictions on using the license (e.g. modification and copying)

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

QUESTION 4

A user installed a new application that automatically starts each time the user logs in to a Windows 10 system. The user does not want this to happen and has asked for this setting to be changed.

Which of the following tools would the technician MOST likely use to safely make this change?

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

Correct Answer: B

Section:

Explanation:

The technician would most likely use the Task Manager tool to safely make this change12 The Task Manager tool can be used to disable applications from starting automatically on Windows 10 The tool that a technician would most likely use to stop an application from automatically starting when a user logs in to a Windows 10 system is the Task Manager. The Task Manager can be used to view and manage processes, including those that are set to automatically start when a user logs in to the system.

QUESTION 5

A laptop user is visually impaired and requires a different cursor color. Which of the following OS utilities is used to change the color of the cursor?

- A. Keyboard
- B. Touch pad
- C. Ease of Access Center
- D. Display settings

Correct Answer: C

Section:

Explanation:

The OS utility used to change the color of the cursor in Windows is Ease of Access Center12 The user can change the cursor color by opening the Settings app, selecting Accessibility in the left sidebar, selecting Mouse pointer and touch under Vision, and choosing one of the cursor options.

The user can select Custom to pick a color and use the Size slider to make the cursor larger or smaller12 The Ease of Access Center in the Windows OS provides accessibility options for users with disabilities or impairments. One of these options allows the user to change the color and size of the cursor, making it more visible and easier to locate on the screen. The Keyboard and Touchpad settings do not offer the option to change cursor color, and Display Settings are used to adjust the resolution and other properties of the display. Therefore, C is the best answer. This information is covered in the Comptia A+ Core2 documents/guide under the Accessibility section.

QUESTION 6

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 7

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 8

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 9

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\(3-0\)](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 10

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 11

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 12

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 13

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 source

QUESTION 14

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

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

Correct Answer: B

Section:

Explanation:

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

QUESTION 15

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 16

Which of the following provide the BEST way to secure physical access to a data center 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 17

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 18

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

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

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

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

QUESTION 19

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 20

A user's smartphone data usage is well above average. The user suspects an installed application is transmitting data in the background. The user would like to be alerted when an application attempts to communicate with the internet.

Which of the following BEST addresses the user's concern?

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

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 21

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

QUESTION 22

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 23

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 24

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 25

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 26

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 27

A user reports a PC is running slowly. The technician suspects it has a badly fragmented hard drive.

Which of the following tools should the technician use?

- A. resmon.exe
- B. msconfig.extf

- C. dfrgui.exe
- D. msmf32.exe

Correct Answer: C

Section:

Explanation:

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

QUESTION 28

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

- A. Disk Cleanup
- B. Group Policy Editor
- C. Disk Management
- D. Resource Monitor

Correct Answer: D

Section:

Explanation:

QUESTION 29

A user is unable to log in to the domain with a desktop PC, but a laptop PC is working properly on the same network. A technician logs in to the desktop PC with a local account but is unable to browse to the secure intranet site to get troubleshooting tools. Which of the following is the MOST likely cause of the issue?

- A. Time drift
- B. Dual in-line memory module failure
- C. Application crash
- D. Filesystem errors

Correct Answer: A

Section:

Explanation:

The most likely cause of the issue is a “time drift”. Time drift occurs when the clock on a computer is not synchronized with the clock on the domain controller. This can cause authentication problems when a user tries to log in to the domain. The fact that the technician is unable to browse to the secure intranet site to get troubleshooting tools suggests that there may be a problem with the network connection or the firewall settings on the desktop PC12

QUESTION 30

Which of the following could be used to implement secure physical access to a data center?

- A. Geofence
- B. Alarm system
- C. Badge reader
- D. Motion sensor

Correct Answer: C

Section:

Explanation:

Badge readers are used to implement secure physical access to a data center. They are used to read the identification information on an employee's badge and grant access to the data center if the employee is authorized. This system requires individuals to have an access badge that contains their identification information or a unique code that can be scanned by a reader. After the badge is scanned, the system compares the information on the badge with the authorized personnel database to authenticate if the individual has the required clearance to enter that area. The other options listed, such as a geofence, alarm system, or motion sensor are security measures that may be used in conjunction with badge readers, but do not provide identification and authentication features.

QUESTION 31

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

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

Correct Answer: D

Section:

Explanation:

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

QUESTION 32

A user is experiencing frequent malware symptoms on a Windows workstation. The user has tried several times to roll back the state but the malware persists. Which of the following would MOST likely resolve the issue?

- A. Quarantining system files
- B. Reimaging the workstation
- C. Encrypting the hard drive
- D. Disabling TLS 1.0 support

Correct Answer: C

Section:

Explanation:

Since Windows systems support FAT32 and NTFS "out of the box" and Linux supports a whole range of them including FAT32 and NTFS, it is highly recommended to format the partition or disk you want to share in either FAT32 or NTFS, but since FAT32 has a file size limit of 4.2 GB, if you happen to work with huge files, then it is better you use NTFS.

QUESTION 33

A technician needs to format a USB drive to transfer 20GB of data from a Linux computer to a Windows computer. Which of the following filesystems will the technician MOST likely use?

- A. FAT32
- B. ext4
- C. NTFS
- D. exFAT

Correct Answer: D

Section:

Explanation:

QUESTION 34

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

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

Correct Answer: A

Section:

Explanation:

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

QUESTION 35

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

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

Correct Answer: A

Section:

Explanation:

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

QUESTION 36

An incident handler needs to preserve evidence for possible litigation. Which of the following will the incident handler MOST likely do to preserve the evidence?

- A. Encrypt the files
- B. Clone any impacted hard drives
- C. Contact the cyber insurance company
- D. Inform law enforcement

Correct Answer: B

Section:

Explanation:

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

QUESTION 37

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



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

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

Correct Answer: A

Section:

Explanation:

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

QUESTION 38

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

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

Correct Answer: D

Section:

Explanation:

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

QUESTION 39

A technician needs to exclude an application folder from being cataloged by a Windows 10 search. Which of the following utilities should be used?

- A. Privacy
- B. Indexing Options
- C. System
- D. Device Manager

Correct Answer: B

Section:

Explanation:

To exclude an application folder from being cataloged by a Windows 10 search, the technician should use the Indexing Options utility¹

QUESTION 40

A company needs to securely dispose of data stored on optical discs. Which of the following is the MOST effective method to accomplish this task?

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

Correct Answer: D

Section:

Explanation:

Shredding is the most effective method to securely dispose of data stored on optical discs¹² Reference: 4. How Can I Safely Destroy Sensitive Data CDs/DVDs? - How-To Geek. Retrieved from <https://www.howtogeek.com/174307/how-can-i-safely-destroy-sensitive-data-cdsdvs/> 5. Disposal — UK Data Service. Retrieved from <https://ukdataservice.ac.uk/learning-hub/research-data-management/store-your-data/disposal/>

QUESTION 41

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:

Multifactor authentication will be forced for Wi-Fi after deploying a client certificate to be used for Wi-Fi access for all devices in an organization

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

QUESTION 42

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

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

Correct Answer: A

Section:

Explanation:

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

QUESTION 43

An administrator has received approval for a change request for an upcoming server deployment.

Which of the following steps should be completed NEXT?

- A. Perform a risk analysis.
- B. Implement the deployment.
- C. Verify end user acceptance
- D. Document the lessons learned.

Correct Answer: A

Section:

Explanation:

Before making any changes to the system, it is important to assess the risks associated with the change and determine whether it is worth implementing. Risk analysis involves identifying potential risks, assessing their likelihood and impact, and determining what steps can be taken to mitigate them. It is important to perform this step before making any changes, as this allows the administrator to make an informed decision about whether or not the change should be implemented. Once the risks have been assessed and the administrator has decided to go ahead with the change, the next step is to implement the deployment.

QUESTION 44

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

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

Correct Answer: A

Section:

Explanation:

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

Furthermore, it also adheres to user privacy policies, as the technician is not exposing any confidential information to any external sources.

QUESTION 45

A manager reports that staff members often forget the passwords to their mobile devices and applications. Which of the following should the systems administrator do to reduce the number of help desk tickets submitted?

- A. Enable multifactor authentication.

- B. Increase the failed log-in threshold.
- C. Remove complex password requirements.
- D. Implement a single sign-on with biometrics.

Correct Answer: D

Section:

Explanation:

QUESTION 46

A Microsoft Windows PC needs to be set up for a user at a large corporation. The user will need access to the corporate domain to access email and shared drives. Which of the following versions of Windows would a technician MOST likely deploy for the user?

- A. Windows Enterprise Edition
- B. Windows Professional Edition
- C. Windows Server Standard Edition
- D. Windows Home Edition

Correct Answer: A

Section:

Explanation:

QUESTION 47

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

QUESTION 48

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 49

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 50

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 51

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

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

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 52

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 53

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 54

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 55

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 56

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 57

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 58

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 IP.
- 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 59

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 60

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 61

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 62

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:





















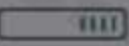
If a technician suspects high disk I/O, the technician should use the Resource Monitor (resmon.exe) to identify the process that is causing the high disk I/O1. Resource Monitor provides detailed information about the system's resource usage, including disk I/O1. The technician can use this information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

QUESTION 63

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:

Wall Outlet	Surge Protector	UPS	Drag & Drop
	Power Source: Wall Outlet ▼	Power Source: Surge Protector ▼	 Cable Modem
			 Computer
			 Monitor
			 Printer
			 Scanner
			 Wifi Router

Correct Answer:

- 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 65

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 66

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

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

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 67

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 68

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 69

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 70

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 71

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 72

A technician is troubleshooting a mobile device that was dropped. The technician finds that the screen (ails to rotate, even though the settings are correctly applied. Which of the following pieces of hardware should the technician replace to resolve the issue?

- A. LCD
- B. Battery
- C. Accelerometer
- D. Digitizer

Correct Answer: C

Section:

Explanation:

The piece of hardware that the technician should replace to resolve the issue of the screen failing to rotate on a mobile device that was dropped is the accelerometer. The accelerometer is a sensor that detects the orientation and movement of the mobile device by measuring the acceleration forces acting on it. The accelerometer allows the screen to rotate automatically according to the position and angle of the device. If the accelerometer is damaged or malfunctioning, the screen may not rotate properly or at all, even if the settings are correctly applied. LCD stands for Liquid Crystal Display and is a type of display that uses liquid crystals and backlight to produce images on the screen. LCD is not related to the screen rotation feature but to the quality and brightness of the display. Battery is a component that provides power to the mobile device by storing and releasing electrical energy. Battery is not related to the screen rotation feature but to the battery life and performance of the device. Digitizer is a component that converts touch inputs into digital signals that can be processed by the mobile device. Digitizer is not related to the screen rotation feature but to the touch sensitivity and accuracy of the display. Reference: CompTIA A+ Core 2 (220-1102) Certification Exam Objectives Version 4.0, Domain 1.5

QUESTION 73

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

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

Correct Answer: C

Section:

Explanation:

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

QUESTION 74

An implementation specialist is replacing a legacy system at a vendor site that has only one wireless network available. When the specialist connects to Wi-Fi, the specialist realizes the insecure network has open authentication. The technician needs to secure the vendor's sensitive data. Which of the following should the specialist do FIRST to protect the company's data?

- A. Manually configure an IP address, a subnet mask, and a default gateway.
- B. Connect to the vendor's network using a VPN.
- C. Change the network location to private.
- D. Configure MFA on the network.

Correct Answer: B

Section:

Explanation:

The first thing that the specialist should do to protect the company's data on an insecure network with open authentication is to connect to the vendor's network using a VPN. A VPN stands for Virtual Private Network and is a technology that creates a secure and encrypted connection over a public or untrusted network. A VPN can protect the company's data by preventing eavesdropping, interception or modification of the network traffic by unauthorized parties. A VPN can also provide access to the company's internal network and resources remotely. Manually configuring an IP address, a subnet mask and a default gateway may not be necessary or possible if the vendor's network uses DHCP to assign network configuration parameters automatically. Manually configuring an IP address, a subnet mask and a default gateway does not protect the company's data from network attacks or threats. Changing the network location to private may not be advisable or effective if the vendor's network is a public or untrusted network. Changing the network location to private does not protect the company's data from network attacks or threats. Configuring MFA on the network may not be feasible or sufficient if the vendor's network has open authentication and does not support or require MFA. Configuring MFA on the network does not protect the company's data from network attacks or threats. Reference: CompTIA A+ Core 2 (220-1102) Certification Exam Objectives Version 4.0, Domain 3.3

QUESTION 75

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

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

Correct Answer: D

Section:

Explanation:

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

QUESTION 76

A technician is finalizing a new workstation for a user. The user's PC will be connected to the internet but will not require the same private address each time. Which of the following protocols will the technician MOST likely utilize?

- A. DHCP
- B. SMTP
- C. DNS
- D. RDP

Correct Answer: A

Section:

Explanation:

DHCP stands for Dynamic Host Configuration Protocol and it is used to assign IP addresses and other network configuration parameters to devices on a network automatically. This is useful for devices that do not require the same private address each time they connect to the internet.

QUESTION 77

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

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

Correct Answer: C

Section:

Explanation:

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

QUESTION 78

A manager called the help desk to ask for assistance with creating a more secure environment for the finance department- which resides in a non-domain environment. Which of the following would be the BEST method to protect against unauthorized use?

- A. Implementing password expiration
- B. Restricting user permissions
- C. Using screen locks
- D. Disabling unnecessary services

Correct Answer: B

Section:

Explanation:

Restricting user permissions is a method of creating a more secure environment for the finance department in a non-domain environment. This means that users will only have access to the files and resources that they need to perform their tasks and will not be able to modify or delete other files or settings that could compromise security or functionality.

QUESTION 79

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

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

Correct Answer: B

Section:

Explanation:

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

QUESTION 80

A customer calls a service support center and begins yelling at a technician about a feature for a product that is not working to the customer's satisfaction. This feature is not supported by the service support center and requires a field technician to troubleshoot. The customer continues to demand service. Which of the following is the BEST course of action for the support center representative to take?

- A. Inform the customer that the issue is not within the scope of this department.
- B. Apologize to the customer and escalate the issue to a manager.
- C. Ask the customer to explain the issue and then try to fix it independently.
- D. Respond that the issue is something the customer should be able to fix.

Correct Answer: B

Section:

Explanation:

Apologizing to the customer and escalating the issue to a manager is the best course of action for the support center representative to take. This shows empathy and professionalism and allows the manager to handle the situation and provide the appropriate service or resolution for the customer.

QUESTION 81

All the desktop icons on a user's newly issued PC are very large. The user reports that the PC was working fine until a recent software patch was deployed. Which of the following would BEST resolve the issue?

- A. Rolling back video card drivers
- B. Restoring the PC to factory settings
- C. Repairing the Windows profile
- D. Reinstalling the Windows OS

Correct Answer: A

Section:

Explanation:

Rolling back video card drivers is the best way to resolve the issue of large desktop icons on a user's newly issued PC. This means restoring the previous version of the drivers that were working fine before the software patch was deployed. The software patch may have caused compatibility issues or corrupted the drivers, resulting in display problems

QUESTION 82

A technician is installing a program from an ISO file. Which of the following steps should the technician take?

- A. Mount the ISO and run the installation file.
- B. Copy the ISO and execute on the server.
- C. Copy the ISO file to a backup location and run the ISO file.
- D. Unzip the ISO and execute the setup.exe file.

Correct Answer: A

Section:

Explanation:

Mounting the ISO and running the installation file is the correct way to install a program from an ISO file. An ISO file is an image of a disc that contains all the files and folders of a program. Mounting the ISO means creating a virtual drive that can access the ISO file as if it were a physical disc. Running the installation file means executing the setup program that will install the program on the computer

QUESTION 83

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

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

Correct Answer: C

Section:

Explanation:

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

QUESTION 84

While staying at a hotel, a user attempts to connect to the hotel Wi-Fi but notices that multiple SSIDs have very similar names. Which of the following social-engineering attacks is being attempted?

- A. Evil twin
- B. Impersonation
- C. Insider threat
- D. Whaling

Correct Answer: A

Section:

Explanation:

An evil twin is a type of social-engineering attack that involves setting up a rogue wireless access point that mimics a legitimate one. The attacker can then intercept or modify the traffic of the users who connect to the fake SSID. The attacker may also use phishing or malware to steal credentials or personal information from the users

QUESTION 85

Which of the following is used to integrate Linux servers and desktops into Windows Active Directory environments?

- A. apt-get
- B. CIFS
- C. Samba
- D. greP

Correct Answer: C

Section:

Explanation:

Samba is a software suite that allows Linux servers and desktops to integrate with Windows Active Directory environments. Samba can act as a domain controller, a file server, a print server, or a client for Windows networks. Samba can also provide authentication and authorization services for Linux users and devices using Active Directory.

QUESTION 86

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

- A. System
- B. Indexing Options
- C. Device Manager

D. Programs and Features

Correct Answer: A

Section:

Explanation:

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

QUESTION 87

An organization implemented a method of wireless security that requires both a user and the user's computer to be in specific managed groups on the server in order to connect to Wi-Fi. Which of the following wireless security methods BEST describes what this organization implemented?

- A. TKIP
- B. RADIUS
- C. WPA2
- D. AES

Correct Answer: B

Section:

Explanation:

RADIUS stands for Remote Authentication Dial-In User Service and it is a protocol that provides centralized authentication, authorization, and accounting for network access. RADIUS can be used to implement a method of wireless security that requires both a user and the user's computer to be in specific managed groups on the server in order to connect to Wi-Fi. This is also known as 802.1X authentication or EAP-TLS authentication

QUESTION 88

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

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

Correct Answer: D

Section:

Explanation:

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

QUESTION 89

Which of the following macOS features provides the user with a high-level view of all open windows?

- A. Mission Control
- B. Finder
- C. Multiple Desktops
- D. Spotlight

Correct Answer: A

Section:

Explanation:

Mission Control is the macOS feature that provides the user with a high-level view of all open windows. Mission Control allows the user to see and switch between multiple desktops, full-screen apps, and windows in a single screen. Mission Control can be accessed by swiping up with three or four fingers on the trackpad, pressing F3 on the keyboard, or moving the cursor to a hot corner

QUESTION 90

Which of the following should be used to secure a device from known exploits?

- A. Encryption
- B. Remote wipe
- C. Operating system updates
- D. Cross-site scripting

Correct Answer: C

Section:

Explanation:

Operating system updates are used to secure a device from known exploits. Operating system updates are patches or fixes that are released by the vendor to address security vulnerabilities, bugs, or performance issues. Operating system updates can also provide new features or enhancements to the device. It is important to keep the operating system updated to prevent attackers from exploiting known flaws or weaknesses.

QUESTION 91

The audio on a user's mobile device is inconsistent when the user uses wireless headphones and moves around. Which of the following should a technician perform to troubleshoot the issue?

- A. Verify the Wi-Fi connection status.
- B. Enable the NFC setting on the device.
- C. Bring the device within Bluetooth range.
- D. Turn on device tethering.

Correct Answer: C

Section:

Explanation:

Bringing the device within Bluetooth range is the best way to troubleshoot the issue of inconsistent audio when using wireless headphones and moving around. Bluetooth is a wireless technology that allows devices to communicate over short distances, typically up to 10 meters or 33 feet. If the device is too far from the headphones, the Bluetooth signal may be weak or interrupted, resulting in poor audio quality or loss of connection.

QUESTION 92

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

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

Correct Answer: D

Section:

Explanation:

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

QUESTION 93

A data center is required to destroy SSDs that contain sensitive information. Which of the following is the BEST method to use for the physical destruction of SSDs?

- A. Wiping
- B. Low-level formatting
- C. Shredding
- D. Erasing

Correct Answer: C

Section:**Explanation:**

Shredding is the best method to use for the physical destruction of SSDs because it reduces them to small pieces that cannot be recovered or accessed. Wiping, low-level formatting, and erasing are not effective methods for destroying SSDs because they do not physically damage the flash memory chips that store data¹.

QUESTION 94

After a failed update, an application no longer launches and generates the following error message:

Application needs to be repaired. Which of the following Windows 10 utilities should a technician use to address this concern?

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

Correct Answer: D

Section:**Explanation:**

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

QUESTION 95

A technician receives a call from a user who is having issues with an application. To best understand the issue, the technician simultaneously views the user's screen with the user. Which of the following would BEST accomplish this task?

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

Correct Answer: C

Section:**Explanation:**

VNC (Virtual Network Computing) is a protocol that allows a technician to simultaneously view and control a user's screen remotely. VNC uses a server-client model, where the user's computer runs a VNC server

and the technician's computer runs a VNC client. VNC can work across different platforms and operating systems³. SSH (Secure Shell) is a protocol that allows a technician to access a user's command-line interface remotely, but not their graphical user interface. VPN (Virtual Private Network) is a technology that creates a secure and encrypted connection over a public network, but does not allow screen sharing. RDP (Remote Desktop Protocol) is a protocol that allows a technician to access a user's desktop remotely, but not simultaneously with the user.

QUESTION 96

A computer on a corporate network has a malware infection. Which of the following would be the BEST method for returning the computer to service?

- A. Scanning the system with a Linux live disc, flashing the BIOS, and then returning the computer to service
- B. Flashing the BIOS, reformatting the drive, and then reinstalling the OS
- C. Degaussing the hard drive, flashing the BIOS, and then reinstalling the OS
- D. Reinstalling the OS, flashing the BIOS, and then scanning with on-premises antivirus

Correct Answer: B

Section:

Explanation:

Flashing the BIOS, reformatting the drive, and then reinstalling the OS is the best method for returning a computer with a malware infection to service. Flashing the BIOS updates the firmware of the motherboard and can remove any malware that may have infected it. Reformatting the drive erases all data on it and can remove any malware that may have infected it. Reinstalling the OS restores the system files and settings to their original state and can remove any malware that may have modified them. Scanning the system with a Linux live disc may not detect or remove all malware infections. Degaussing the hard drive is an extreme method of destroying data that may damage the drive beyond repair. Reinstalling the OS before flashing the BIOS or scanning with antivirus may not remove malware infections that persist in the BIOS or other files.

QUESTION 97

A technician needs to access a Windows 10 desktop on the network in a SOHO using RDP. Although the connection is unsuccessful, the technician is able to ping the computer successfully. Which of the following is MOST likely preventing the connection?

- A. The Windows 10 desktop has Windows 10 Home installed.
- B. The Windows 10 desktop does not have DHCP configured.
- C. The Windows 10 desktop is connected via Wi-Fi.
- D. The Windows 10 desktop is hibernating.

Correct Answer: A

Section:

Explanation:

The Windows 10 desktop has Windows 10 Home installed, which does not support RDP (Remote Desktop Protocol) as a host. Only Windows 10 Pro, Enterprise, and Education editions can act as RDP hosts and allow remote access to their desktops¹. The Windows 10 desktop does not have DHCP configured, is connected via Wi-Fi, or is hibernating are not likely to prevent the RDP connection if the technician is able to ping the computer successfully.

QUESTION 98

Which of the following often uses an SMS or third-party application as a secondary method to access a system?

- A. MFA
- B. WPA2
- C. AES
- D. RADIUS

Correct Answer: A

Section:**Explanation:**

MFA (Multi-Factor Authentication) is a security measure that often uses an SMS or third-party application as a secondary method to access a system. MFA requires the user to provide two or more pieces of evidence to prove their identity, such as something they know (e.g., password), something they have (e.g., phone), or something they are (e.g., fingerprint)². WPA2 (Wi-Fi Protected Access 2) is a security protocol for wireless networks that does not use SMS or third-party applications. AES (Advanced Encryption Standard) is a symmetric encryption algorithm that does not use SMS or third-party applications. RADIUS (Remote Authentication Dial-In User Service) is a network protocol that provides centralized authentication and authorization for remote access clients, but does not use SMS or third-party applications.

QUESTION 99

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

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

Correct Answer: C

Section:**Explanation:**

A virtual private network (VPN) is a technology that creates a secure and encrypted connection over a public network, such as the internet. A VPN allows remote employees to access the corporate intranet as if they were physically connected to the local network³. Password-protected Wi-Fi is a security measure for wireless networks that does not provide access to the corporate intranet. Port forwarding is a technique that allows external devices to access services on a private network through a router, but does not provide access to the corporate intranet. A perimeter network is a network segment that lies between an internal network and an external network, such as the internet, and provides an additional layer of security, but does not provide access to the corporate intranet.

QUESTION 100

A systems administrator is creating a new document with a list of the websites that users are allowed to access. Which of the following types of documents is the administrator MOST likely creating?

- A. Access control list
- B. Acceptable use policy
- C. Incident report
- D. Standard operating procedure

Correct Answer: A

Section:**Explanation:**

An access control list (ACL) is a list of permissions associated with a system resource (object), such as a website. An ACL specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects¹. A systems administrator can create an ACL to define the list of websites that users are allowed to access.

Reference: 1: Access-control list - Wikipedia (https://en.wikipedia.org/wiki/Access-control_list)

QUESTION 101

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

- A. Remote wipe
- B. Firewall
- C. Device encryption
- D. Remote backup
- E. Antivirus

F. Global Positioning System

Correct Answer: A, C

Section:

Explanation:

Remote wipe is a feature that allows data to be deleted from a device or system remotely by an administrator or owner¹. It is used to protect data from being compromised if the device is lost, stolen, or changed hands¹. Device encryption is a feature that helps protect the data on a device by making it unreadable to unauthorized users². It requires a key or a password to access the data². Both features can help mitigate the risk of losing company trade secrets if a corporate phone is stolen.

Reference: 1: How to remote wipe Windows laptop (<https://www.thewindowsclub.com/remote-wipe-windows-10>) 2: Device encryption in Windows (<https://support.microsoft.com/en-us/windows/device-encryption-in-windows-ad5dcf4b-dbe0-2331-228f-7925c2a3012d>)

QUESTION 102

A user receives the following error while attempting to boot a computer.

BOOTMGR is missing

press Ctrl+Alt+Del to restart

Which of the following should a desktop engineer attempt FIRST to address this issue?

- A. Repair Windows.
- B. Partition the hard disk.
- C. Reimage the workstation.
- D. Roll back the updates.

Correct Answer: A

Section:

Explanation:

The error “BOOTMGR is missing” indicates that the boot sector is damaged or missing¹. The boot sector is a part of the hard disk that contains the code and information needed to start Windows¹. To fix this error, one of the possible methods is to run Startup Repair from Windows Recovery Environment (WinRE)¹. Startup Repair is a tool that can automatically diagnose and repair problems with the boot process².

Reference: 1: “Bootmgr is missing Press Ctrl+Alt+Del to restart” error when you start Windows (<https://support.microsoft.com/en-us/topic/-bootmgr-is-missing-press-ctrl-alt-del-to-restart-error-when-you-start-windows-8bc1b94b-d243-1027-5410-aeb04d5cd5e2>) 2: Startup Repair: frequently asked questions (<https://support.microsoft.com/en-us/windows/startup-repair-frequently-asked-questions-f5f412a0-19c4-8e0a-9f68-bb0f17f3daa0>)

QUESTION 103

A technician is in the process of installing a new hard drive on a server but is called away to another task. The drive has been unpackaged and left on a desk. Which of the following should the technician perform before leaving?

- A. Ask coworkers to make sure no one touches the hard drive.
- B. Leave the hard drive on the table; it will be okay while the other task is completed.
- C. Place the hard drive in an antistatic bag and secure the area containing the hard drive.
- D. Connect an electrostatic discharge strap to the drive.

Correct Answer: C

Section:

Explanation:

The technician should place the hard drive in an antistatic bag and secure the area containing the hard drive before leaving. This will protect the hard drive from electrostatic discharge (ESD), dust, moisture, and physical damage. Asking coworkers to make sure no one touches the hard drive is not a reliable or secure way to prevent damage. Leaving the hard drive on the table exposes it to ESD and other environmental hazards. Connecting an electrostatic discharge strap to the drive is not enough to protect it from dust, moisture, and physical damage.

QUESTION 104

A technician installed Windows 10 on a workstation. The workstation only has 3.5GB of usable RAM, even though the technician installed 8GB. Which of the following is the MOST likely reason this system is not utilizing all the available RAM?

- A. The system is missing updates.
- B. The systems utilizing a 32-bit OS.
- C. The system's memory is failing.
- D. The system requires BIOS updates.

Correct Answer: B

Section:

Explanation:

The most likely reason that the system is not utilizing all the available RAM is that it is running a 32-bit OS. A 32-bit OS can only address up to 4GB of RAM, and some of that is reserved for hardware and system use¹. Therefore, even if the technician installed 8GB of RAM, the system can only use around 3.5GB of usable RAM. To use the full 8GB of RAM, the technician would need to install a 64-bit OS, which can address much more memory². The system missing updates, the system's memory failing, or the system requiring BIOS updates are not likely to cause this issue.

Reference: 2: <https://support.microsoft.com/en-us/windows/windows-10-system-requirements-6d4e9a79-66bf-7950-467c-795cf0386715> 1: <https://www.makeuseof.com/tag/unlock-64gb-ram-32-bit-windows-pae-patch/>

QUESTION 105

An employee calls the help desk regarding an issue with a laptop PC. After a Windows update, the user can no longer use certain locally attached devices, and a reboot has not fixed the issue. Which of the following should the technician perform to fix the issue?

- A. Disable the Windows Update service.
- B. Check for updates.
- C. Restore hidden updates.
- D. Rollback updates.

Correct Answer: D

Section:

Explanation:

The technician should perform a rollback of the Windows update that caused the issue with the locally attached devices. A rollback is a process of uninstalling an update and restoring the previous version of the system. This can help to fix any compatibility or performance issues caused by the update¹. To rollback an update, the technician can use the Settings app, the Control Panel, or the System Restore feature. The technician should also check for any device driver updates that might be needed after rolling back the update. Disabling the Windows Update service is not a good practice, as it can prevent the system from receiving important security and feature updates. Checking for updates might not fix the issue, as the update that caused the issue might still be installed. Restoring hidden updates is not relevant, as it only applies to updates that have been hidden by the user to prevent them from being installed².

Reference: 1: <https://www.windowscentral.com/how-uninstall-and-reinstall-updates-windows-10> 2:

<https://support.microsoft.com/en-us/windows/show-or-hide-updates-in-windows-10-9c9f0a4f-9a6e-4c8e-8b44-afbc6b33f3cf>

QUESTION 106

A macOS user is installing a new application. Which of the following system directories is the software MOST likely to install by default?

- A. /etc/services
- B. /Applications
- C. /usr/bin
- D. C:\Program Files

Correct Answer: B

Section:**Explanation:**

The software is most likely to install by default in the /Applications directory, which is the standard location for macOS applications. This directory can be accessed from the Finder sidebar or by choosing Go > Applications from the menu bar. The /Applications directory contains all the applications that are available to all users on the system¹. Some applications might also offer the option to install in the ~/Applications directory, which is a personal applications folder for a single user². The /etc/services directory is a system configuration file that maps service names to port numbers and protocols³. The /usr/bin directory is a system directory that contains executable binaries for various commands and utilities⁴. The C:\Program Files directory is a Windows directory that does not exist on macOS.

QUESTION 107

A user needs assistance changing the desktop wallpaper on a Windows 10 computer. Which of the following methods will enable the user to change the wallpaper using a Windows 10 Settings tool?

- A. Open Settings, select Accounts, select Your info, click Browse, and then locate and open the image the user wants to use as the wallpaper.
- B. Open Settings, select Personalization, click Browse, and then locate and open the image the user wants to use as the wallpaper.
- C. Open Settings, select System, select Display, click Browse, and then locate and open the image the user wants to use as the wallpaper.
- D. Open Settings, select Apps, select Apps & features, click Browse, and then locate and open the image the user wants to use as the wallpaper.

Correct Answer: B**Section:****Explanation:**

The user can change the wallpaper using a Windows 10 Settings tool by following these steps¹²:

Open Settings by pressing the Windows key and typing Settings, or by clicking the gear icon in the Start menu.

Select Personalization from the left navigation menu.

On the right side of the window, click Background.

In the Background settings, click the drop-down menu and select Picture as the background type. Click Browse and then locate and open the image the user wants to use as the wallpaper. The other options are incorrect because they do not lead to the Background settings or they do not allow the user to browse for an image. Accounts, System, and Apps are not related to personalization settings. Your info, Display, and Apps & features are not related to wallpaper settings.

Reference: 1: <https://support.microsoft.com/en-us/windows/change-your-desktop-background-image-175618be-4cf1-c159-2785-ec2238b433a8> 2: <https://www.computerhope.com/issues/ch000592.htm>

QUESTION 108

Which of the following default system tools can be used in macOS to allow the technician to view the screen simultaneously with the user?

- A. Remote Assistance
- B. Remote Desktop Protocol
- C. Screen Sharing
- D. Virtual Network Computing

Correct Answer: C**Section:****Explanation:**

Screen Sharing is the default system tool that can be used in macOS to allow the technician to view the screen simultaneously with the user. Screen Sharing is a built-in app that lets users share their Mac screen with another Mac on the network. The user can enable screen sharing in the System Preferences > Sharing pane, and then allow other users to request or enter a password to access their screen¹. The technician can launch the Screen Sharing app from the Spotlight search or the Finder sidebar, and then enter the user's name, address, or Apple ID to connect to their screen². Remote Assistance is a Windows feature that allows users to invite someone to help them with a problem on their PC³. Remote Desktop Protocol (RDP) is a protocol that allows users to connect to a remote computer over a network⁴. Virtual Network Computing (VNC) is a technology that allows users to share their screen with other devices using a VNC viewer app¹. These are not default system tools in macOS, although they can be used with third-party software or settings.

Reference: 1: <https://support.apple.com/guide/mac-help/share-the-screen-of-another-macmh14066/mac> 2: <https://www.howtogeek.com/449239/how-to-share-your-macs-screen-withanother-mac/> 3: <https://support.microsoft.com/en-us/windows/solve-pc-problems-over-a-remoteconnection-b077e31a-16f4-2529-1a47-21f6a9040bf3> 4: <https://docs.microsoft.com/en-us/windowsserver/remote/remote-desktop->

QUESTION 109

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 110

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 111

A hard drive that previously contained PII 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 112

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 113

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 114

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 115

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 116

An administrator responded to an incident where an employee copied financial data to a portable hard drive and then left the company with the data. The administrator documented the movement of the evidence. Which of the following concepts did the administrator demonstrate?

- A. Preserving chain of custody
- B. Implementing data protection policies
- C. Informing law enforcement
- D. Creating a summary of the incident

Correct Answer: A

Section:**Explanation:**

Preserving chain of custody is a concept that refers to the documentation and tracking of who handled, accessed, modified, or transferred a piece of evidence, when, where, why, and how.

Preserving chain of custody can help establish the authenticity, integrity, and reliability of the evidence, as well as prevent tampering, alteration, or loss of the evidence. An administrator who documented the movement of the evidence demonstrated the concept of preserving chain of custody. Implementing data protection policies, informing law enforcement, and creating a summary of the incident are not concepts that describe the action of documenting the movement of the evidence.

QUESTION 117

Which of the following threats will the use of a privacy screen on a computer help prevent?

- A. Impersonation
- B. Shoulder surfing
- C. Whaling
- D. Tailgating

Correct Answer: B

Section:

Explanation:

Shoulder surfing is a threat that involves someone looking over another person's shoulder to observe their screen, keyboard, or other sensitive information. Shoulder surfing can be used to steal passwords, personal identification numbers (PINs), credit card numbers, or other confidential data.

The use of a privacy screen on a computer can help prevent shoulder surfing by limiting the viewing angle of the screen and making it harder for someone to see the screen from the side or behind.

Impersonation, whaling, and tailgating are not threats that can be prevented by using a privacy screen on a computer.

QUESTION 118

Users access files in the department share. When a user creates a new subfolder, only that user can access the folder and its files. Which of the following will MOST likely allow all users to access the new folders?

- A. Assigning share permissions
- B. Enabling inheritance
- C. Requiring multifactor authentication
- D. Removing archive attribute

Correct Answer: B

Section:

Explanation:

Enabling inheritance is a method that allows new subfolders to inherit the permissions and settings from their parent folder. If users can access files in the department share, but not in the new subfolders created by other users, it may indicate that inheritance is disabled and that each new subfolder has its own permissions and settings that restrict access to only the creator. Enabling inheritance can help resolve this issue by allowing all users to access the new subfolders with the same permissions and settings as the department share. Assigning share permissions, requiring multifactor authentication, and removing archive attribute are not methods that can most likely allow all users to access the new folders.

QUESTION 119

A user has a computer with Windows 10 Home installed and purchased a Windows 10 Pro license.

The user is not sure how to upgrade the OS. Which of the following should the technician do to apply this license?

- A. Copy the c:\Windows\windows.lie file over to the machine and restart.
- B. Redeem the included activation key card for a product key.
- C. Insert a Windows USB hardware dongle and initiate activation.
- D. Activate with the digital license included with the device hardware.

Correct Answer: B

Section:

Explanation:

Redeeming the included activation key card for a product key is the correct way to apply a Windows 10 Pro license to a computer that has Windows 10 Home installed. The activation key card is a physical or digital card that contains a 25-digit code that can be used to activate Windows 10 Pro online or by phone. Copying the windows.lie file, inserting a Windows USB hardware dongle and activating with the digital license are not valid methods of applying a Windows 10 Pro license.

Verified Reference: <https://www.comptia.org/blog/how-to-upgrade-windows-10-home-to-pro>

<https://www.comptia.org/certifications/a>

QUESTION 120

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

- A. Quarantine the host in the antivirus system.

- B. Run antivirus scan for malicious software.
- C. Investigate how malicious software was installed.
- D. Reimage the computer.

Correct Answer: B

Section:

Explanation:

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

<https://www.comptia.org/blog/how-to-remove-a-virus> <https://www.comptia.org/certifications/a>