

Exam Code: 220-1102
Exam Name: CompTIA A+ Certification Exam: Core 2



Exam A

QUESTION 1

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

- A. Scan the computer with the company-provided antivirus software
- B. Install a new hard drive and clone the user's drive to it
- C. Deploy an ad-blocking extension to the browser.
- D. Uninstall the company-provided antivirus software
- E. Click the link in the messages to pay for virus removal
- F. Perform a reset on the user's web browser

Correct Answer: C, F

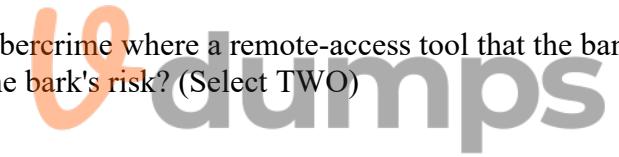
Section:

Explanation:

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

QUESTION 2

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

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

Correct Answer: A, F

Section:

Explanation:

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

QUESTION 3

A technician is asked to resize a partition on the internal storage drive of a computer running macOS.

Which of the following tools should the technician use to accomplish this task?

- A. Consoltf
- B. Disk Utility
- C. Time Machine
- D. FileVault

Correct Answer: B

Section:

Explanation:

The technician should use Disk Utility to resize a partition on the internal storage drive of a computer running macOS. Disk Utility is a built-in utility that allows users to manage disks, partitions, and volumes on a Mac. It can be used to resize, create, and delete partitions, as well as to format disks and volumes.

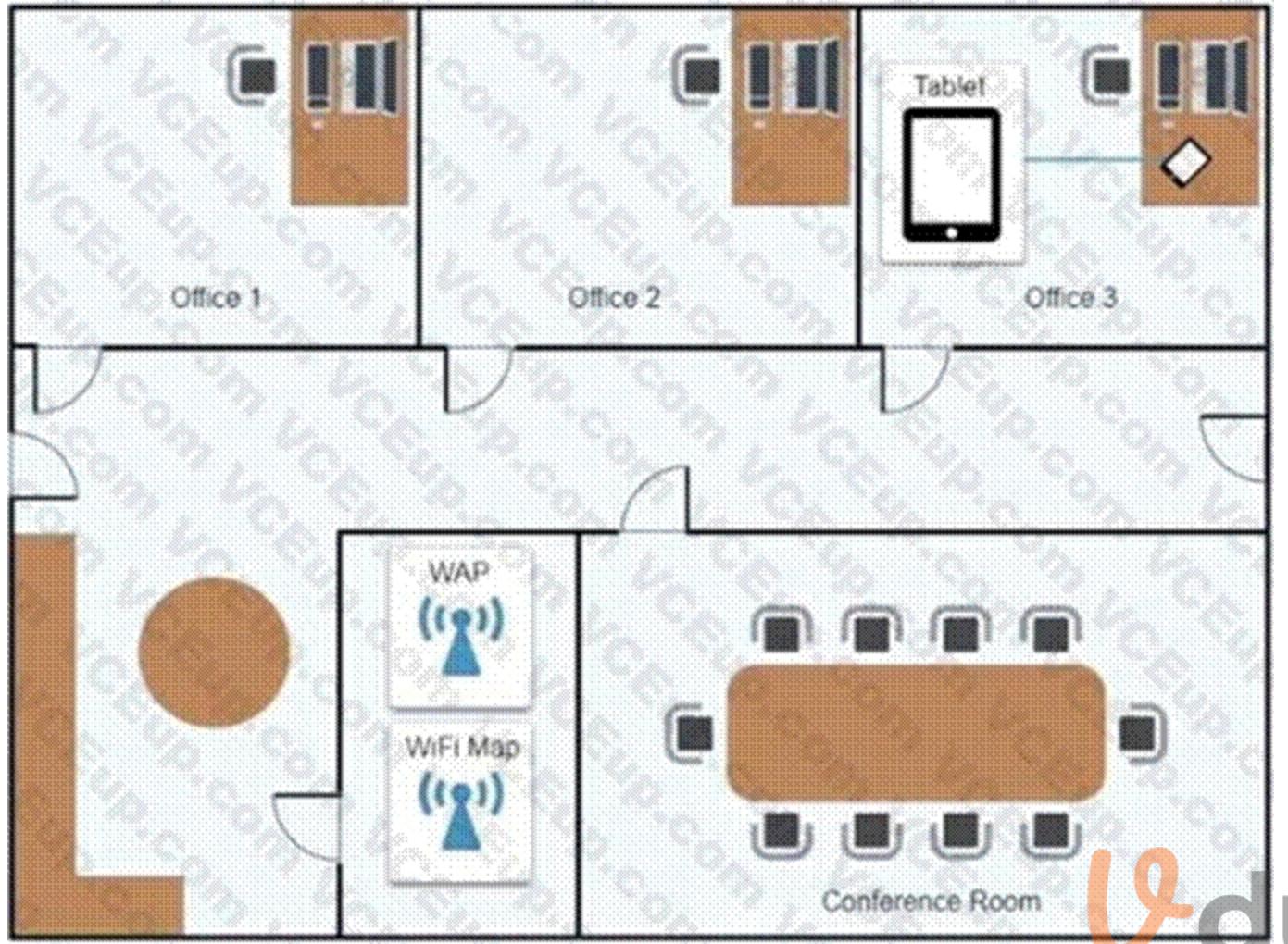
QUESTION 4

Ann, a CEO, has purchased a new consumer-class tablet for personal use, but she is unable to connect it to the company's wireless network. All the corporate laptops are connecting without issue. She has asked you to assist with getting the device online.

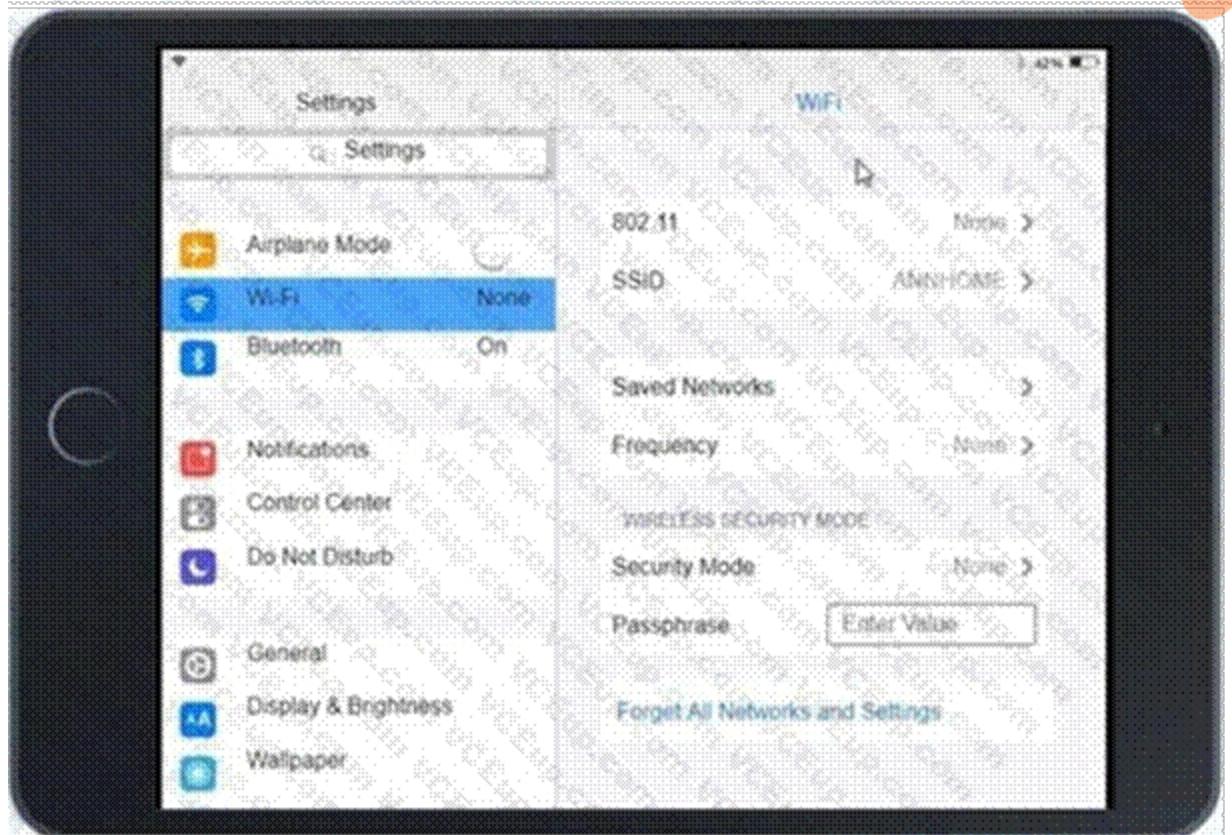
INSTRUCTIONS Review the network diagrams and device configurations to determine the cause of the problem and resolve any discovered issues.

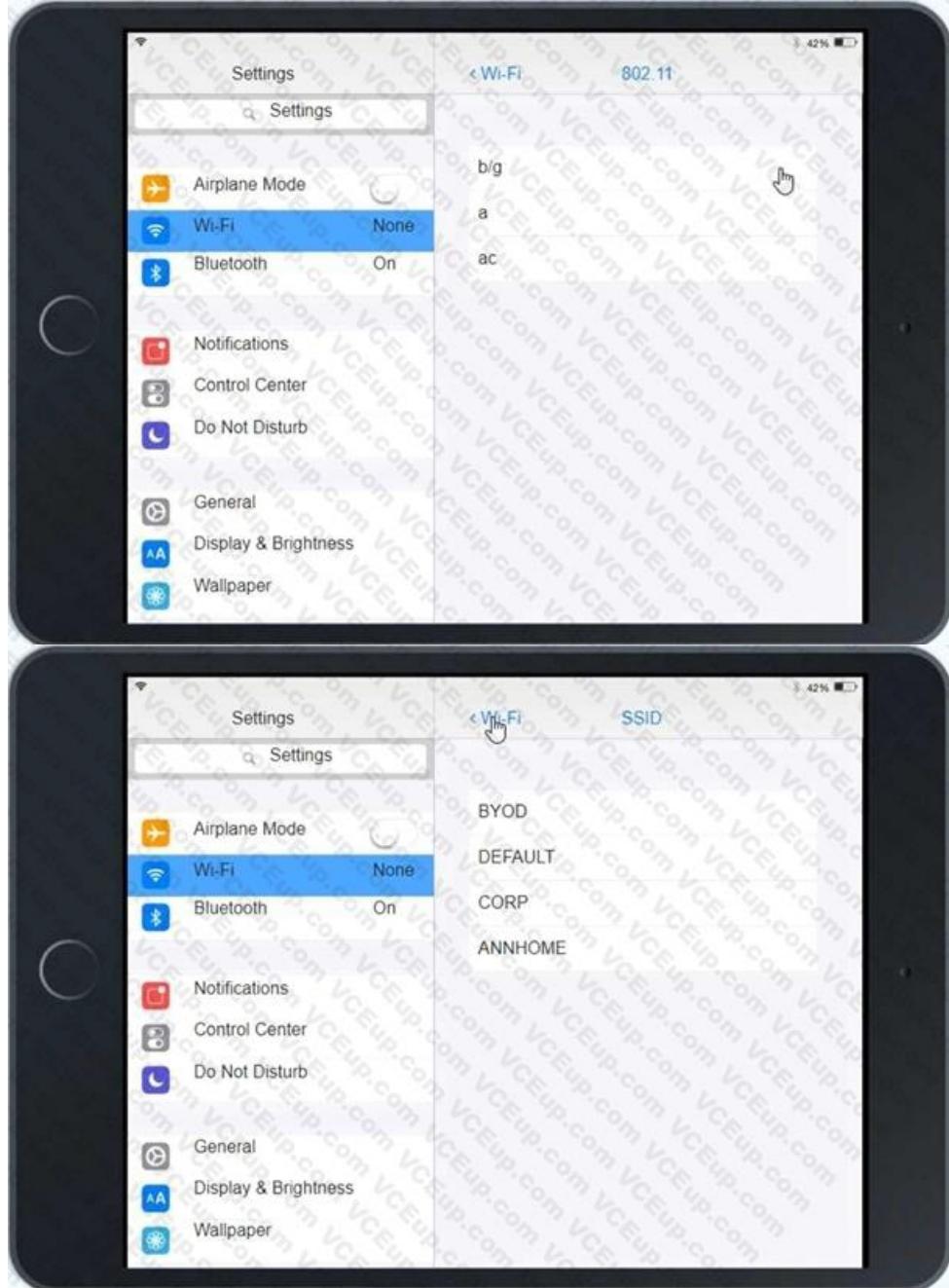
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



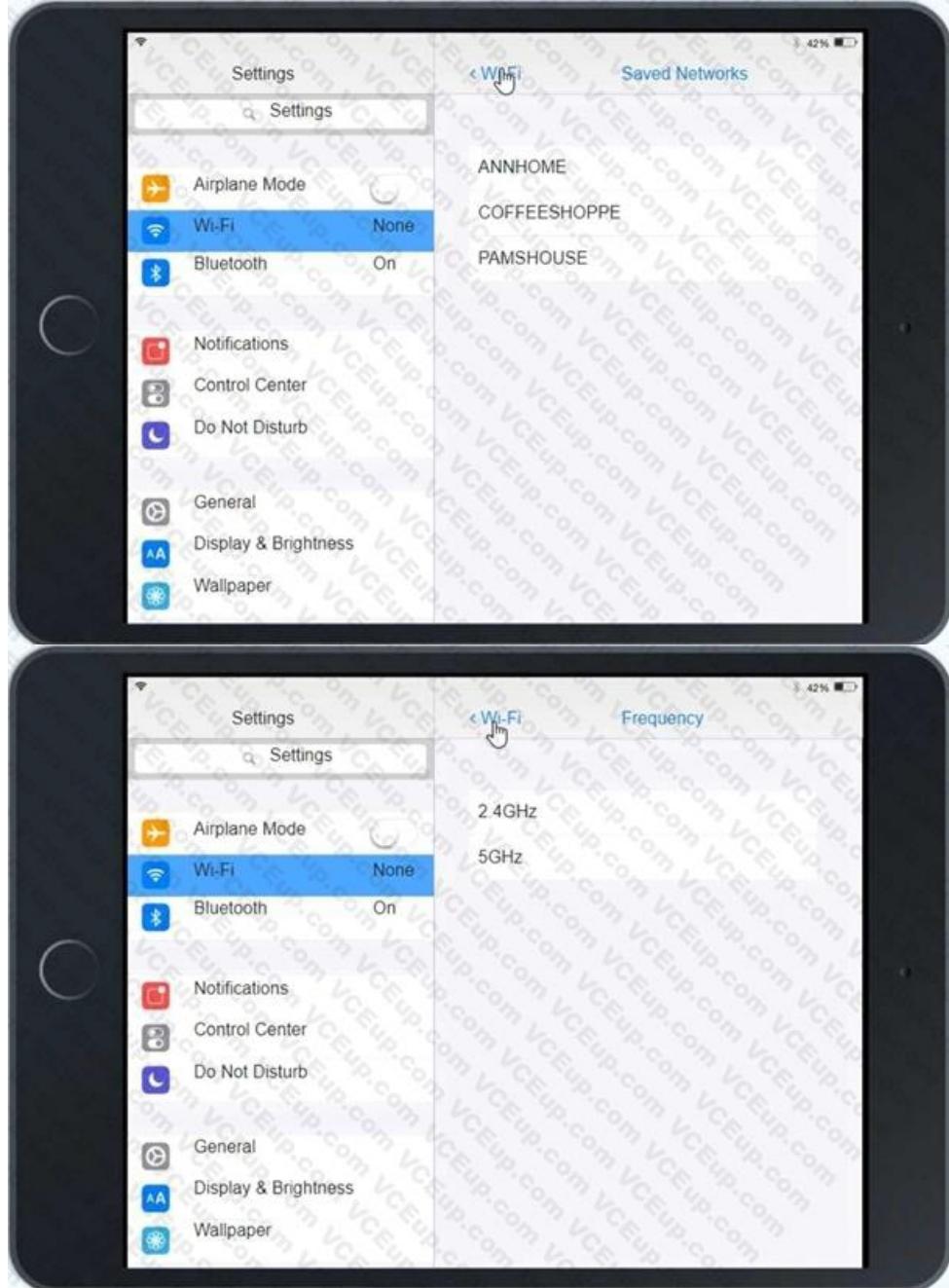


Vdumps





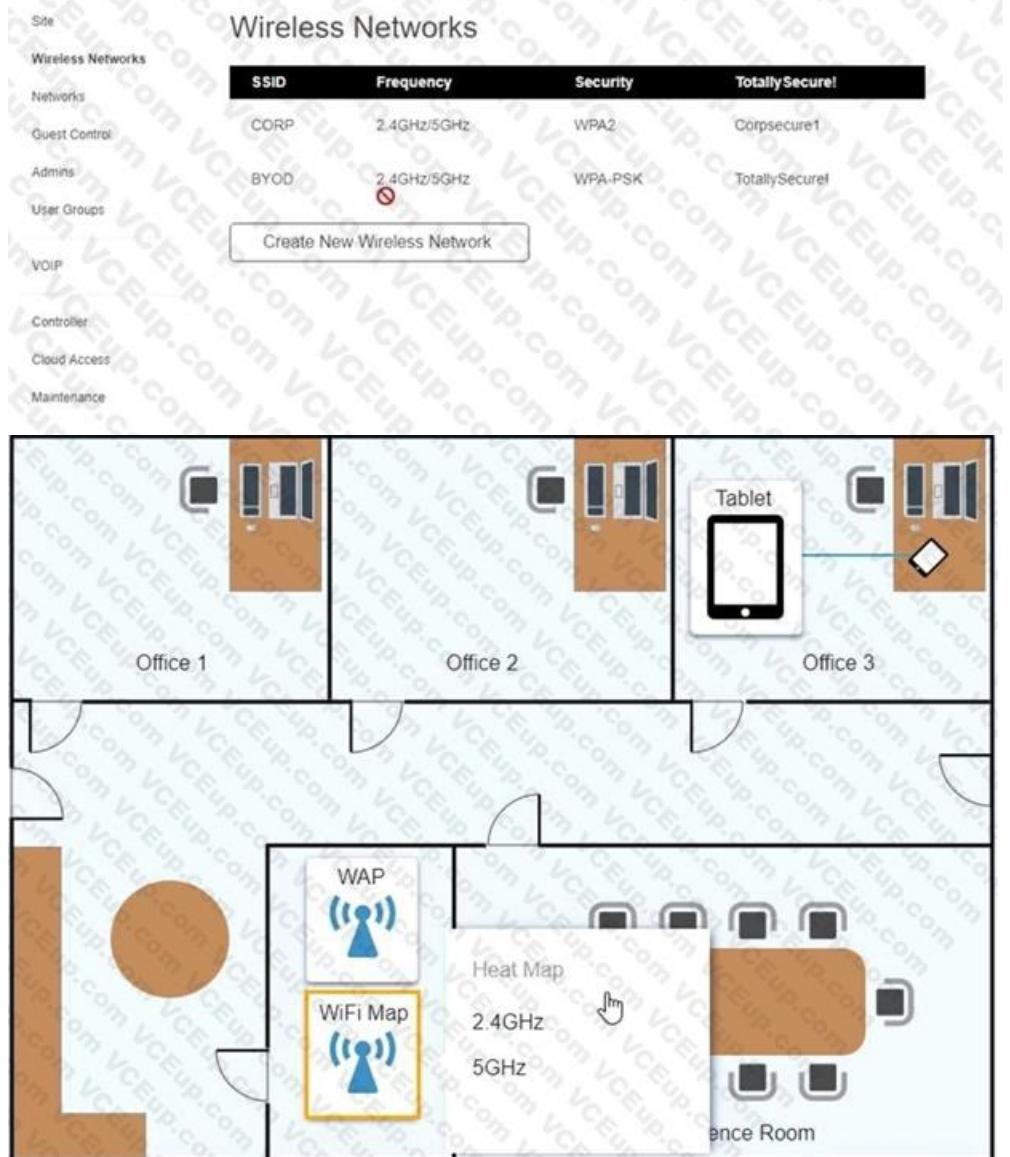
Vdumps



Vdumps



Settings



Vdumps

A. See the Explanation below

Correct Answer: A

Section:

Explanation:

Answer: A

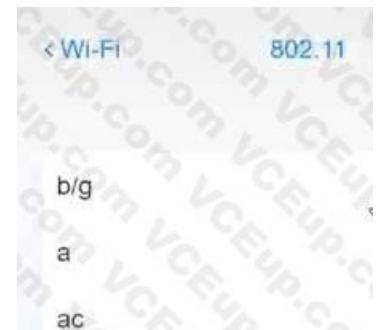
Explanation:

Explanation below:

Explanation:



Click on 802.11 and Select ac



Click on SSID and select CORP



Vdumps

Click on Frequency and select 5GHz



At Wireless Security Mode, Click on Security Mode



Select the WPA2



Explanation:

Ann needs to connect to the BYOD SSID, using 2.4GHZ. The selected security method chose should be WPA PSK, and the password should be set to TotallySecret.

Vdumps



Vdumps

QUESTION 5

HOTSPOT

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

Click on individual tickers to see the ticket details. View attachments to determine the problem.

Select the appropriate issue from the 'Issue' drop-down menu. Then, select the MOST efficient resolution from the 'Resolution' drop-down menu. Finally, select the proper command or verification to remediate or confirm your fix of the issue from the Verify Resolve drop-down menu.

TEST QUESTION

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

INSTRUCTIONS

Click on individual tickets to see the ticket details. View attachments to determine the problem.

Select the appropriate issue from the 'Issue' drop-down menu. Then, select the MOST efficient resolution from the 'Resolution' drop-down menu. Finally, select the proper command or verification to remediate or confirm your fix of the issue from the 'Verify/Resolve' drop-down menu.

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

Details

Date	Priority
PC is failing to boot. Screen is displaying error message, see attachment.	High
Cannot access Z: on my computer.	Low

No Ticket Selected
Please select a ticket from the list

Details

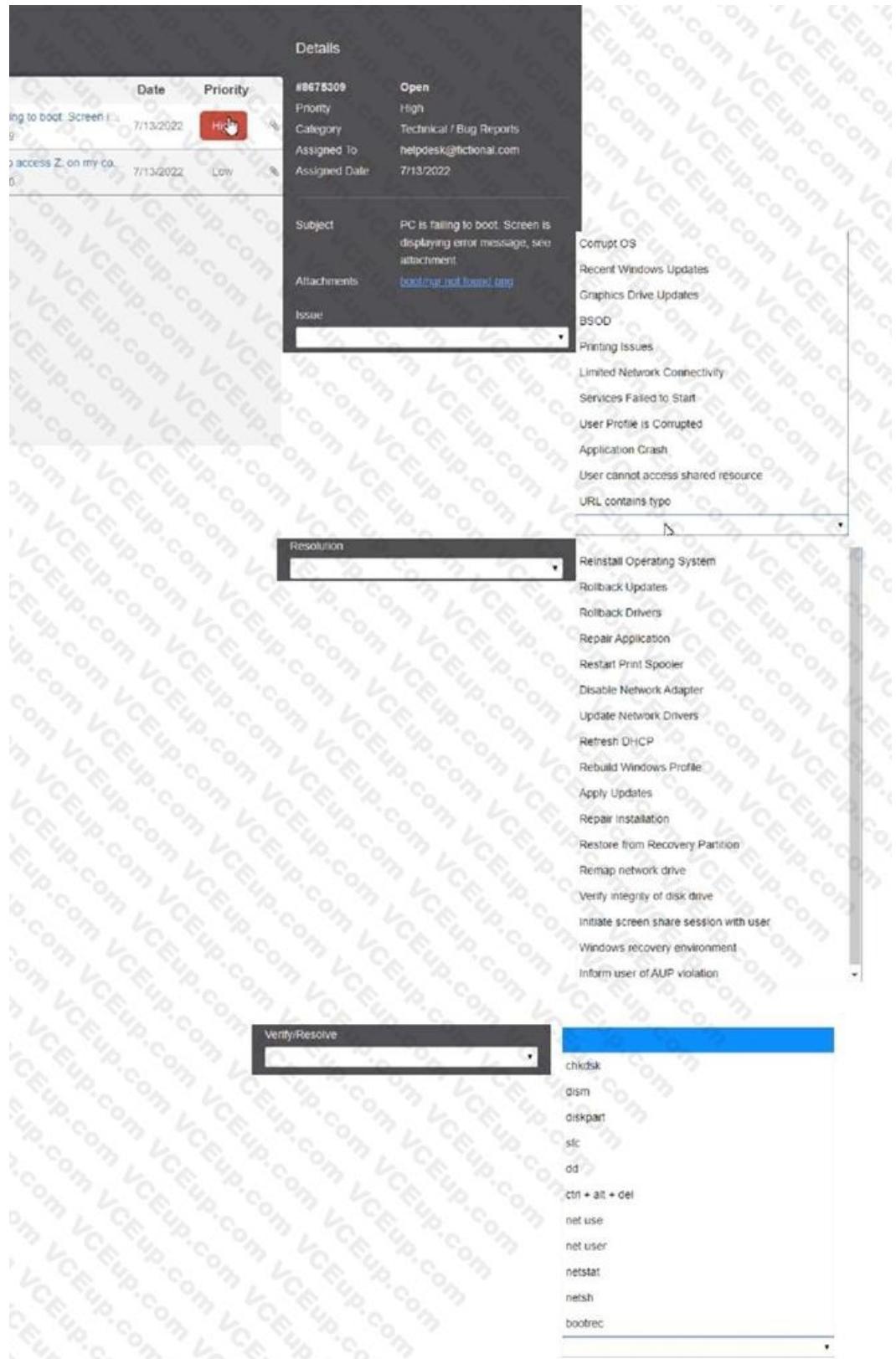
#	Status
8675309	Open

Priority: High
Category: Technical / Bug Reports
Assigned To: helpdesk@fictional.com
Assigned Date: 7/13/2022

Subject: PC is failing to boot. Screen is displaying error message, see attachment.
Attachments: [bootmgr not found.png](#)

Issue:
Resolution:
Verify/Resolve:

Vdumps



Hot Area:

Vdumps

Details

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

#8675309 Open
Priority High
Category Technical / Bug Reports
Assigned To helpdesk@fictional.com
Assigned Date 7/13/2022

Subject PC is failing to boot. Screen is displaying error message, see attachment.
Attachments bootmgr not found.png
Issue

Resolution

Reinstall Operating System
Rollback Updates
Rollback Drivers
Repair Application
Restart Print Spooler
Disable Network Adapter
Update Network Drivers
Refresh DHCP
Rebuild Windows Profile
Apply Updates
Repair Installation
Restore from Recovery Partition
Remap network drive
Verify integrity of disk drive
Initiate screen share session with user
Windows recovery environment
Inform user of AUP violation

Answer Area:



Details

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

#8675309 Open
Priority High
Category Technical / Bug Reports
Assigned To helpdesk@fictional.com
Assigned Date 7/13/2022

Subject PC is failing to boot. Screen is displaying error message, see attachment.
Attachments bootmgr not found.png
Issue

Resolution

Corrupt OS
Recent Windows Updates
Graphics Drive Updates
BSOD
Printing Issues
Limited Network Connectivity
Services Failed to Start
User Profile Is Corrupted
Application Crash
User cannot access shared resource
URL contains typo

Reinstall Operating System
Rollback Updates
Rollback Drivers
Repair Application
Restart Print Spooler
Disable Network Adapter
Update Network Drivers
Refresh DHCP
Rebuild Windows Profile
Apply Updates
Repair Installation
Restore from Recovery Partition
Remap network drive
Verify integrity of disk drive
Initiate screen share session with user
Windows recovery environment
Inform user of AUP violation

Section:**Explanation:**

Answer: A

Explanation:

Details

#8675309	Open
Priority	High
Category	Technical / Bug Reports
Assigned To	helpdesk@fictional.com
Assigned Date	7/13/2022

Subject PC is failing to boot. Screen is displaying error message, see attachment.

Attachments [bootmgr not found.png](#)

Issue

Corrupt OS
Resolution
Reinstall Operating System
Verify/Resolve
chkdsk

Close Ticket

**QUESTION 6**

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 7

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 8

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 9

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 10

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 11

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 12

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 13

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 14

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 15

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:

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

QUESTION 16

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

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

Correct Answer: C

Section:

Explanation:

Since there are no error messages on the device, the technician should check if the battery is sufficiently charged¹If the battery is low, the device may not have enough power to complete the update²In this scenario, the technician has already determined that there are no error messages on the device. The next best step would be to check if the battery is sufficiently charged. If the battery is low, it could be preventing the device from completing the update process.Verifying that third-party applications are disabled, determining if the device has adequate storage available, and confirming a strong internet connection are all important steps in troubleshooting issues with mobile devices.

However, since the problem in this scenario is related to a failed OS update, it is important to first check the battery level before proceeding with further troubleshooting steps.

QUESTION 17

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

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

Correct Answer: C

Section:

Explanation:

Open Settings, select System, select Display, and change the Scale and layout setting to a higher percentage¹² Reference: 4. How to Increase the Text Size on Your Computer. Retrieved from <https://www.laptopmag.com/articles/increase-text-size-computer>

5. How to Change the Size of Text in Windows 10. Retrieved from <https://www.howtogeek.com/370055/how-to-change-the-size-of-text-in-windows-10/> 6. Change the size of text in Windows. Retrieved from

<https://support.microsoft.com/en-us/windows/change-the-size-of-text-in-windows-1d5830c3-eee3-8eaa-836b-abcc37d99b9a>

QUESTION 18

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

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

Correct Answer: C

Section:

Explanation:

The technician should change the default administrative password FIRST to ensure the network equipment is secured against external threats on the Internet. Changing the default administrative password is a basic security measure that can help prevent unauthorized access to the network equipment. Locking all devices in a closet is a physical security measure that can help prevent theft or damage to the devices, but it does not address external threats on the Internet.

Ensuring all devices are from the same manufacturer is not a security measure and does not address external threats on the Internet. Installing the latest operating system and patches is important for maintaining the security of the network equipment, but it is not the first action the technician should take¹

QUESTION 19

Which of the following Linux commands would be used to install an application?

- A. yum
- B. grep
- C. ls
- D. sudo

Correct Answer: D

Section:

Explanation:

The Linux command used to install an application is sudo. The sudo command allows users to run programs with the security privileges of another user, such as the root user. This is necessary to install applications because it requires administrative privileges.

QUESTION 20

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

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

Correct Answer: C

Section:

Explanation:

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

QUESTION 21

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:

To change the desktop wallpaper on a Windows 10 computer using a Windows 10 Settings tool, the user should open Settings, select Personalization, click Browse, and then locate and open the image the user wants to use as the wallpaper.
<https://www.lifewire.com/change-desktop-background-windows-11-5190733>

QUESTION 22

A technician is working with a company to determine the best way to transfer sensitive personal information between offices when conducting business. The company currently uses USB drives and is resistant to change. The company's compliance officer states that all media at rest must be encrypted. Which of the following would be the BEST way to secure the current workflow?

- A. Deploy a secondary hard drive with encryption on the appropriate workstation
- B. Configure a hardened SFTP portal for file transfers between file servers
- C. Require files to be individually password protected with unique passwords
- D. Enable BitLocker To Go with a password that meets corporate requirements

Correct Answer: D

Section:

Explanation:

The BEST way to secure the current workflow of transferring sensitive personal information between offices when conducting business is to enable BitLocker To Go with a password that meets corporate requirements. This is because BitLocker To Go is a full-disk encryption feature that encrypts all data on a USB drive, which is what the company currently uses, and requires a password to access the data.

QUESTION 23

A technician is configuring a new Windows laptop Corporate policy requires that mobile devices make use of full disk encryption at all times Which of the following encryption solutions should the technician choose?

- A. Encrypting File System
- B. FileVault
- C. BitLocker
- D. Encrypted LVM

Correct Answer: A

Section:

Explanation:

The encryption solution that the technician should choose when configuring a new Windows laptop and corporate policy requires that mobile devices make use of full disk encryption at all times is BitLocker. This is because BitLocker is a full-disk encryption feature that encrypts all data on a hard drive and is included with Window

QUESTION 24

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

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

Correct Answer: B

Section:

Explanation:

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

QUESTION 25

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

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

Correct Answer: A

Section:

Explanation:

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

QUESTION 26

When a user calls in to report an issue, a technician submits a ticket on the user's behalf. Which of the following practices should the technician use to make sure the ticket is associated with the correct user?

- A. Have the user provide a callback phone number to be added to the ticket
- B. Assign the ticket to the department's power user
- C. Register the ticket with a unique user identifier



- D. Provide the user with a unique ticket number that can be referenced on subsequent calls.

Correct Answer: D

Section:

Explanation:

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

QUESTION 27

Which of the following is the MOST cost-effective version of Windows 10 that allows remote access through Remote Desktop?

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

Correct Answer: D

Section:

Explanation:

The most cost-effective version of Windows 10 that allows remote access through Remote Desktop is Windows 10 Pro. Windows 10 Pro includes Remote Desktop, which allows users to connect to a remote computer and access its desktop, files, and applications. Windows 10 Home does not include Remote Desktop, while Windows 10 Pro for Workstations and Windows 10 Enterprise are more expensive versions of Windows 10 that include additional features for businesses

QUESTION 28

Once weekly a user needs Linux to run a specific open-source application that is not available for the currently installed Windows platform. The user has limited bandwidth throughout the day. Which of the following solutions would be the MOST efficient, allowing for parallel execution of the Linux application and Windows applications?

- A. Install and run Linux and the required application in a PaaS cloud environment
- B. Install and run Linux and the required application as a virtual machine installed under the Windows OS
- C. Use a swappable drive bay for the boot drive and install each OS with applications on its own drive Swap the drives as needed
- D. Set up a dual boot system by selecting the option to install Linux alongside Windows

Correct Answer: B

Section:

Explanation:

The user should install and run Linux and the required application as a virtual machine installed under the Windows OS. This solution would allow for parallel execution of the Linux application and Windows applications². The MOST efficient solution that allows for parallel execution of the Linux application and Windows applications is to install and run Linux and the required application as a virtual machine installed under the Windows OS. This is because it allows you to run both Linux and Windows together without the need to keep the Linux portion confined to a VM window³.

QUESTION 29

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

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

Correct Answer: C

Section:**Explanation:**

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

QUESTION 30

A technician is installing new software on a macOS computer. Which of the following file types will the technician MOST likely use?

- A. .deb
- B. .vbs
- C. .exe
- D. .app

Correct Answer: D**Section:****Explanation:**

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

QUESTION 31

Which of the following is the MOST important environmental concern inside a data center?

- A. Battery disposal
- B. Electrostatic discharge mats
- C. Toner disposal
- D. Humidity levels

**Correct Answer: D****Section:****Explanation:**

One of the most important environmental concerns inside a data center is the level of humidity. High levels of humidity can cause condensation, which can result in corrosion of components and other equipment. Low levels of humidity can cause static electricity to build up, potentially leading to electrostatic discharge (ESD) and damage to components. Therefore, it is crucial to maintain a relative humidity range of 40-60% in a data center to protect the equipment and ensure proper operation.

QUESTION 32

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

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

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

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

QUESTION 33

A change advisory board just approved a change request. Which of the following is the MOST likely next step in the change process?

- A. End user acceptance
- B. Perform risk analysis
- C. Communicate to stakeholders
- D. Sandbox testing

Correct Answer: A

Section:

Explanation:

QUESTION 34

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

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

Correct Answer: B

Section:

Explanation:

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

QUESTION 35

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

QUESTION 36

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

- A. All updated software must be tested with alt system types and accessories
- B. Extra technician hours must be budgeted during installation of updates
- C. Network utilization will be significantly increased due to the size of CAD files

- D. Large update and installation files will overload the local hard drives.

Correct Answer: C

Section:

Explanation:

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

QUESTION 37

A wireless network is set up, but it is experiencing some interference from other nearby SSIDs.

Which of the following can BEST resolve the interference?

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

Correct Answer: A

Section:

Explanation:

Changing channels can best resolve interference from other nearby SSIDs. Wireless networks operate on different channels, and changing the channel can help to avoid interference from other nearby networks.

QUESTION 38

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

- A. Application updates
- B. Anti-malware software
- C. OS reinstallation
- D. File restore



Correct Answer: C

Section:

Explanation:

If a rootkit has caused a deep infection, then the only way to remove the rootkit is to reinstall the operating system. This is because rootkits are designed to be difficult to detect and remove, and they can hide in the operating system's kernel, making it difficult to remove them without reinstalling the operating system <https://www.minitool.com/backup-tips/how-to-get-rid-of-rootkit-windows-10.html>

QUESTION 39

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

- A. Install alternate open-source software in place of the applications with issues
- B. Run both CPU and memory tests to ensure that all hardware functionality is normal
- C. Check for any installed patches and roll them back one at a time until the issue is resolved
- D. Reformat the hard drive, and then reinstall the newest Windows 10 release and all applications.

Correct Answer: C

Section:

Explanation:

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

QUESTION 40

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

- A. Data-in-transit encryption
- B. File encryption
- C. USB drive encryption
- D. Disk encryption

Correct Answer: D

Section:

Explanation:

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

QUESTION 41

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

- A. Full
- B. Non-parity
- C. Differential
- D. Incremental



Correct Answer: A

Section:

Explanation:

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

QUESTION 42

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

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

Correct Answer: C

Section:

Explanation:

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

QUESTION 43

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

- A. Pretexting

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

Correct Answer: C

Section:

Explanation:

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

QUESTION 44

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

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

Correct Answer: B

Section:

Explanation:

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



QUESTION 45

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

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

Correct Answer: B

Section:

Explanation:

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

QUESTION 46

A technician has been tasked with using the fastest and most secure method of logging in to laptops.

Which of the following log-in options meets these requirements?

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

Correct Answer: A

Section:

Explanation:

This is because a PIN is a fast and secure method of logging in to laptops, and it is more secure than a password because it is not susceptible to keyloggers.

QUESTION 47

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

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

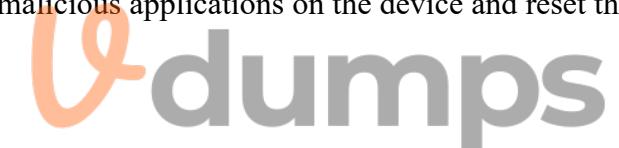
Correct Answer: A, B

Section:**Explanation:**

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

QUESTION 48

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



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

Correct Answer: C, E

Section:**Explanation:**

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

QUESTION 49

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

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

Correct Answer: C

Section:**Explanation:**

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

QUESTION 50

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

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

Correct Answer: A**Section:****Explanation:**

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

QUESTION 51

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

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

Correct Answer: A**Section:****Explanation:**

The smartphone's line was not provisioned with a data plan. The user is unable to use any internet-related functions on the smartphone when it is not connected to Wi-Fi because the smartphone's line was not provisioned with a data plan. The user can send and receive text messages and phone calls when the smartphone is not connected to Wi-Fi because these functions do not require an internet connection.

QUESTION 52

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

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

- A. Turn on autorotation
- B. Activate airplane mode.
- C. Close unnecessary applications
- D. Perform a factory reset
- E. Update the device's operating system
- F. Reinstall the applications that have crashed.



Correct Answer: A, C

Section:

Explanation:

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

QUESTION 53

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

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

Correct Answer: D

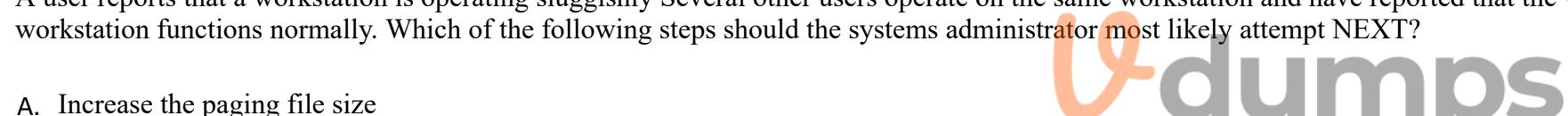
Section:

Explanation:

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

QUESTION 54

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



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

Correct Answer: C

Section:

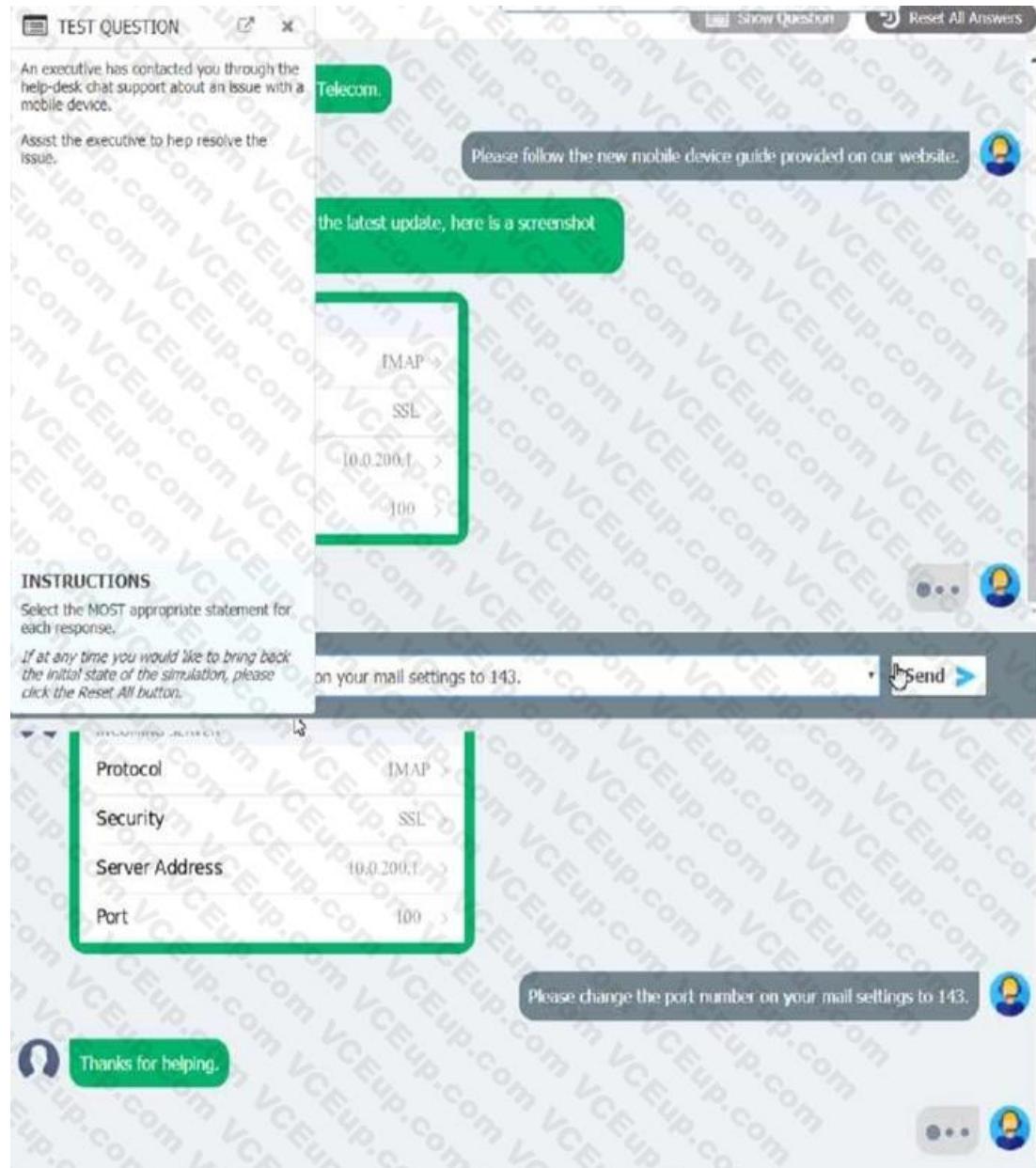
Explanation:

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

QUESTION 55

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

Assist the executive to help resolve the issue.



Which of the following should be done NEXT?

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

Correct Answer: A

Section:

Explanation:

QUESTION 56

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

- A. The hardware does not meet BitLocker's minimum system requirements.

Vdumps

- B. BitLocker was renamed for Windows 10.
- C. BitLocker is not included on Windows 10 Home.
- D. BitLocker was disabled in the registry of the laptop

Correct Answer: C

Section:

Explanation:

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

QUESTION 57

A user receives a notification indicating the antivirus protection on a company laptop is out of date. A technician is able to ping the user's laptop. The technician checks the antivirus parent servers and sees the latest signatures have been installed. The technician then checks the user's laptop and finds the antivirus engine and definitions are current. Which of the following has MOST likely occurred?

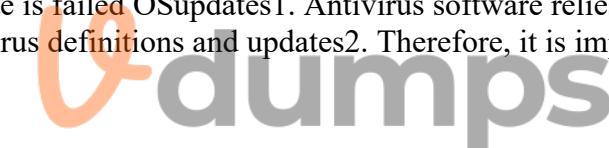
- A. Ransomware
- B. Failed OS updates
- C. Adware
- D. Missing system files

Correct Answer: B

Section:

Explanation:

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



QUESTION 58

Which of the following is a proprietary Cisco AAA protocol?

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

Correct Answer: D

Section:

Explanation:

TACACS+ is a proprietary Cisco AAA protocol

QUESTION 59

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

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

Correct Answer: C

Section:**Explanation:**

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

QUESTION 60

A Chief Executive Officer has learned that an exploit has been identified on the web server software, and a patch is not available yet. Which of the following attacks MOST likely occurred?

- A. Brute force
- B. Zero day
- C. Denial of service
- D. On-path

Correct Answer: B

Section:**Explanation:**

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

QUESTION 61

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:**

exFAT is a file system that is supported by both Linux and Windows and can handle large files1.

QUESTION 62

A user purchased a netbook that has a web-based, proprietary operating system. Which of the following operating systems is MOST likely installed on the netbook?

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

Correct Answer: C

Section:**Explanation:**

4. Chrome OS. Retrieved from https://en.wikipedia.org/wiki/Chrome_OS 5. What is Chrome OS?Retrieved from <https://www.google.com/chromebook/chrome-os/> A netbook with a web-based, proprietary operating system is most likely running Chrome OS.Chrome OS is a web-based operating system developed by Google that is designed to work with web applications and cloud storage. It is optimized for netbooks and other low-power devices and is designed to be fast, secure, and easy to use.

QUESTION 63

An Android user reports that when attempting to open the company's proprietary mobile application it immediately doses. The user states that the issue persists, even after rebooting the phone. The application contains critical

information that cannot be lost. Which of the following steps should a systems administrator attempt FIRST?

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

Correct Answer: D

Section:

Explanation:

The systems administrator should clear the application cache¹² If clearing the application cache does not work, the systems administrator should uninstall and reinstall the application¹² Resetting the phone to factory settings is not necessary at this point¹² Installing an alternative application with similar functionality is not necessary at this point¹²

QUESTION 64

A technician needs to document who had possession of evidence at every step of the process. Which of the following does this process describe?

- A. Rights management
- B. Audit trail
- C. Chain of custody
- D. Data integrity

Correct Answer: C

Section:

Explanation:

The process of documenting who had possession of evidence at every step of the process is called chain of custody



QUESTION 65

A user calls the help desk to report potential malware on a computer. The anomalous activity began after the user clicked a link to a free gift card in a recent email. The technician asks the user to describe any unusual activity, such as slow performance, excessive pop-ups, and browser redirections. Which of the following should the technician do NEXT?

- A. Advise the user to run a complete system scan using the OS anti-malware application
- B. Guide the user to reboot the machine into safe mode and verify whether the anomalous activities are still present
- C. Have the user check for recently installed applications and outline those installed since the link in the email was clicked
- D. Instruct the user to disconnect the Ethernet connection to the corporate network.

Correct Answer: D

Section:

Explanation:

First thing you want to do is quarantine/disconnect the affected system from the network so whatever malicious software doesn't spread

QUESTION 66

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-cdsdvds/> 5. Disposal — UK Data Service. Retrieved from <https://ukdataservice.ac.uk/learning-hub/research-data-management/store-your-data/disposal/>

QUESTION 67

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 68

A bank would like to enhance building security in order to prevent vehicles from driving into the building while also maintaining easy access for customers. Which of the following BEST addresses this need?



- A. Guards
- B. Bollards
- C. Motion sensors
- D. Access control vestibule

Correct Answer: B

Section:

Explanation:

Bollards are the best solution to enhance building security in order to prevent vehicles from driving into the building while also maintaining easy access for customers⁴ Reference: 2. Bollards. Retrieved from <https://en.wikipedia.org/wiki/Bollard>

QUESTION 69

A technician is working to resolve a Wi-Fi network issue at a doctor's office that is located next to an apartment complex. The technician discovers that employees and patients are not the only people on the network. Which of the following should the technician do to BEST minimize this issue?

- A. Disable unused ports.
- B. Remove the guest network
- C. Add a password to the guest network
- D. Change the network channel.

Correct Answer: D

Section:

Explanation:

Changing the network channel is the best solution to minimize the issue of employees and patients not being the only people on the Wi-Fi network5Reference: 3. Sample CompTIA Security+ exam questions and answers.
Retrieved from
<https://www.techtarget.com/searchsecurity/quiz/Sample-CompTIA-Security-exam-questions-and-answers>

QUESTION 70

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

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

Correct Answer: D

Section:**Explanation:**

The newly installed OS is x86. The x86 version of Windows 10 can only use up to 4GB of RAM. The x64 version of Windows 10 can use up to 2TB of RAM1.

QUESTION 71

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

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



Correct Answer: C

Section:**Explanation:**

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

QUESTION 72

Which of the following should be used to control security settings on an Android phone in a domain environment?

- A. MDM
- B. MFA
- C. ACL
- D. SMS

Correct Answer: A

Section:**Explanation:**

The best answer to control security settings on an Android phone in a domain environment is to use “Mobile Device Management (MDM)”. MDM is a type of software that is used to manage and secure mobile devices such as smartphones and tablets. MDM can be used to enforce security policies, configure settings, and remotely wipe data from devices. In a domain environment, MDM can be used to manage Android phones and enforce security policies such as password requirements, encryption, and remote wipe capabilities12

QUESTION 73

A user is being directed by the help desk to look up a Windows PC's network name so the help desk can use a remote administration tool to assist the user. Which of the following commands would allow the user to give the technician the correct information? (Select TWO).

- A. ipconfig /all
- B. hostname
- C. netstat /?
- D. nslookup localhost
- E. arp —a
- F. ping :: 1

Correct Answer: A, B

Section:

Explanation:

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

QUESTION 74

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

- A. Device Manager
- B. Indexing Options
- C. File Explorer
- D. Administrative Tools



Correct Answer: C

Section:

Explanation:

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

QUESTION 75

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

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

Correct Answer: D

Section:

Explanation:

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

QUESTION 76

Before leaving work, a user wants to see the traffic conditions for the commute home. Which of the following tools can the user employ to schedule the browser to automatically launch a traffic website at 4:45 p.m.?

- A. taskschd.msc
- B. perfmon.msc
- C. lusrmgr.msc
- D. Eventvwr.msc

Correct Answer: A

Section:

Explanation:

The user can use the Task Scheduler (taskschd.msc) to schedule the browser to automatically launch a traffic website at 4:45 p.m. The Task Scheduler is a tool in Windows that allows users to schedule tasks to run automatically at specified times or in response to certain events.

QUESTION 77

A technician is installing a new business application on a user's desktop computer. The machine is running Windows 10 Enterprise 32-bit operating system. Which of the following files should the technician execute in order to complete the installation?

- A. Installer_x64.exe
- B. Installer_Files.zip
- C. Installer_32.msi
- D. Installer_x86.exe
- E. Installer_Win10Enterprise.dmg

Correct Answer: D

Section:

Explanation:

The 32-bit operating system can only run 32-bit applications, so the technician should execute the 32-bit installer. The "x86" in the file name refers to the 32-bit architecture. <https://www.digitaltrends.com/computing/32-bit-vs-64-bit-operating-systems/>

QUESTION 78

A user is having issues with document-processing software on a Windows workstation. Other users that log in to the same device do not have the same issue.

Which of the following should a technician do to remediate the issue?

- A. Roll back the updates.
- B. Increase the page file.
- C. Update the drivers.
- D. Rebuild the profile.

Correct Answer: D

Section:

Explanation:

The issue is specific to the user's profile, so the technician should rebuild the profile. Rebuilding the profile will create a new profile and transfer the user's data to the new profile.

QUESTION 79

Which of the following is an example of MFA?

- A. Fingerprint scan and retina scan
- B. Password and PIN
- C. Username and password



- D. Smart card and password

Correct Answer: D

Section:

Explanation:

Smart card and password is an example of two-factor authentication (2FA), not multi-factor authentication (MFA). MFA requires two or more authentication factors. Smart card and password is an example of two-factor authentication (2FA)

QUESTION 80

Which of the following command-line tools will delete a directory?

- A. md
- B. del
- C. dir
- D. rd
- E. cd

Correct Answer: D

Section:

Explanation:

To delete an empty directory, enter rd Directory or rmdir Directory . If the directory is not empty, you can remove files and subdirectories from it using the /s switch. You can also use the /q switch to suppress confirmation messages (quiet mode).

QUESTION 81

A police officer often leaves a workstation for several minutes at a time. Which of the following is the BEST way the officer can secure the workstation quickly when walking away?

- A. Use a key combination to lock the computer when leaving.
- B. Ensure no unauthorized personnel are in the area.
- C. Configure a screensaver to lock the computer automatically after approximately 30 minutes of inactivity.
- D. Turn off the monitor to prevent unauthorized visibility of information.

Correct Answer: A

Section:

Explanation:

The BEST way to secure the workstation quickly when walking away is to use a key combination to lock the computer when leaving

QUESTION 82

A call center handles inquiries into billing issues for multiple medical facilities. A security analyst notices that call center agents often walk away from their workstations, leaving patient data visible for anyone to see. Which of the following should a network administrator do to BEST prevent data theft within the call center?

- A. Encrypt the workstation hard drives.
- B. Lock the workstations after five minutes of inactivity.
- C. Install privacy screens.
- D. Log off the users when their workstations are not in use.

Correct Answer: B

Section:

Explanation:

The BEST solution for preventing data theft within the call center in this scenario would be to lock the workstations after a period of inactivity. This would prevent unauthorized individuals from accessing patient data if call center agents were to step away from their workstations without logging out.

QUESTION 83

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

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

Correct Answer: D**Section:****Explanation:**

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

QUESTION 84

A help desk team lead contacts a systems administrator because the technicians are unable to log in to a Linux server that is used to access tools. When the administrator tries to use remote desktop to log in to the server, the administrator sees the GUI is crashing. Which of the following methods can the administrator use to troubleshoot the server effectively?

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

**Correct Answer: B****Section:****Explanation:****QUESTION 85**

A user turns on a new laptop and attempts to log in to specialized software, but receives a message stating that the address is already in use. The user logs on to the old desktop and receives the same message. A technician checks the account and sees a comment that the user requires a specifically allocated address before connecting to the software. Which of the following should the technician do to MOST likely resolve the issue?

- A. Bridge the LAN connection between the laptop and the desktop.
- B. Set the laptop configuration to DHCP to prevent conflicts.
- C. Remove the static IP configuration from the desktop.
- D. Replace the network card in the laptop, as it may be defective.

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

The new laptop was set up with the static IP it needs to connect to the software. The old desktop is still configured with that IP, hence the conflict.

QUESTION 86

A technician is upgrading the backup system for documents at a high-volume law firm. The current backup system can retain no more than three versions of full backups before failing. The law firm is not concerned about

restore times but asks the technician to retain more versions when possible.
Which of the following backup methods should the technician MOST likely implement?

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

Correct Answer: C

Section:

QUESTION 87

A company discovered that numerous computers from multiple geographic locations are sending a very high number of connection requests which is causing the company's web server to become unavailable to the general public. Which of the following attacks is occurring?

- A. Zero day
- B. SQL injection
- C. Cross-site scripting
- D. Distributed denial of service

Correct Answer: D

Section:

Explanation:

The company is experiencing a distributed denial of service (DDoS) attack. A DDoS attack is a type of cyber attack in which multiple compromised systems are used to target a single system, causing a denial of service for users of the targeted system.



QUESTION 88

While browsing a website, a staff member received a message that the website could not be trusted.

Shortly afterward, several other colleagues reported the same issue across numerous other websites. Remote users who were not connected to corporate resources did not have any issues.

Which of the following is MOST likely the cause of this issue?

- A. A bad antivirus signature update was installed.
- B. A router was misconfigured and was blocking traffic.
- C. An upstream internet service provider was flapping.
- D. The time or date was not in sync with the website.

Correct Answer: D

Section:

Explanation:

QUESTION 89

Security software was accidentally uninstalled from all servers in the environment. After requesting the same version of the software be reinstalled, the security analyst learns that a change request will need to be filled out. Which of the following is the BEST reason to follow the change management process in this scenario?

- A. Owners can be notified a change is being made and can monitor it for performance impact. Most Voted
- B. A risk assessment can be performed to determine if the software is needed.
- C. End users can be aware of the scope of the change.

- D. A rollback plan can be implemented in case the software breaks an application.

Correct Answer: A

Section:

Explanation:

change management process can help ensure that owners are notified of changes being made and can monitor them for performance impact (A). This can help prevent unexpected issues from arising.

QUESTION 90

Which of the following should be done NEXT?

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

Correct Answer: D

Section:

Explanation:

educating the user on the solution that was performed is a good next step after resolving an issue. This can help prevent similar issues from happening again and empower users to solve problems on their own.

QUESTION 91

A user calls the help desk and reports a workstation is infected with malicious software. Which of the following tools should the help desk technician use to remove the malicious software? (Select TWO).

- A. File Explorer
- B. User Account Control
- C. Windows Backup and Restore
- D. Windows Firewall
- E. Windows Defender
- F. Network Packet Analyzer



Correct Answer: A, E

Section:

Explanation:

The correct answers are E. Windows Defender and A. File Explorer. Windows Defender is a built-in antivirus program that can detect and remove malicious software from a workstation. File Explorer can be used to locate and delete files associated with the malicious software.

QUESTION 92

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

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

Correct Answer: D

Section:

Explanation:

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

QUESTION 93

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

Which of the following backup methods should the technician MOST likely implement?

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

Correct Answer: C

Section:

Explanation:

The law firm wants to retain more versions of the backups when possible, so the best backup method for the technician to implement in this scenario would be Incremental backup. Incremental backups only save the changes made since the last backup, which allows for more frequent backups and minimizes the amount of storage required. This would allow the law firm to retain more than three versions of backups without risking backup failure. To retain more versions of backups, the technician should implement an Incremental backup method.¹²An incremental backup method only backs up the data that has changed since the last backup, so it requires less storage space than a full backup

QUESTION 94

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

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



Correct Answer: B

Section:

Explanation:

QUESTION 95

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

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

Correct Answer: B

Section:

Explanation:

The GPS application contains malware. The third-party GPS application is likely the cause of the slow performance of the phone. The application may contain malware that is using up system resources and slowing down the phone. The user should uninstall the application and run a malware scan on the phone¹³

QUESTION 96

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

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

Correct Answer: D

Section:

Explanation:

A full backup involves creating a copy of all data on the workstation, including system files and usercreated data, and storing it on a set of tapes. This ensures that all data is backed up, and ensures that the data can be restored in the event of a system failure or data loss.

QUESTION 97

A technician is troubleshooting a lack of outgoing audio on a third-party Windows 10 VoIP application. The PC uses a USB microphone connected to a powered hub. The technician verifies the microphone works on the PC using Voice Recorder. Which of the following should the technician do to solve the issue?

- A. Remove the microphone from the USB hub and plug it directly into a USB port on the PC.
- B. Enable the microphone under Windows Privacy settings to allow desktop applications to access it.
- C. Delete the microphone from Device Manager and scan for new hardware.
- D. Replace the USB microphone with one that uses a traditional 3.5mm plug.

Correct Answer: B

Section:

Explanation:

In Windows 10, there are privacy settings that control access to certain devices, such as microphones, cameras, and other input devices. If the microphone is not enabled under these privacy settings, the VoIP application may not have access to it, causing a lack of outgoing audio.

The technician can go to the Windows 10 Settings menu, select the Privacy submenu, and under App permissions, select Microphone. The technician should then turn on the toggle switch for the VoIP application to allow it to access the microphone.

Removing the microphone from the USB hub and plugging it directly into a USB port on the PC may or may not solve the issue, as the issue could be related to the privacy settings. Deleting the microphone from Device Manager and scanning for new hardware may also not solve the issue, as the issue could be related to the privacy settings. Replacing the USB microphone with one that uses a traditional 3.5 mm plug is not recommended, as it would require purchasing a new microphone and may not solve the issue.

QUESTION 98

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 99

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 100

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 101

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\(3-0\).pdf](https://partners.comptia.org/docs/default-source/resources/comptia-a-220-1102-exam-objectives(3-0).pdf) 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 102

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 103

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 104

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 105

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 106

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 107

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 software.

QUESTION 108

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 109

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 110

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 111

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 112

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 network.

QUESTION 113

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 114

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 115

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 issue.

QUESTION 116

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 117

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 118

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 119

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 120

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. msinfo32exe
- 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 121

DRAG DROP

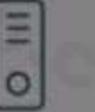
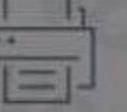
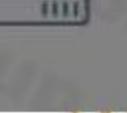
A customer recently experienced a power outage at a SOHO. The customer does not think the components are connected properly. A print job continued running for several minutes after the power failed, but the customer was not able to interact with the computer. Once the UPS stopped beeping, all functioning 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
	<p>Power Source:</p> <p>Wall Outlet</p>	<p>Power Source:</p> <p>Surge Protector</p>	<p>Cable Modem</p> <p>Computer</p> <p>Monitor</p> <p>Printer</p> <p>Scanner</p> <p>Wifi Router</p>

Vdumps

Correct Answer:

Wall Outlet	Surge Protector	UPS	Drag & Drop
 Monitor	 Printer	 Computer	
 Scanner		 Wifi Router	
 Cable Modem		 Cable Modem	
 ?	 ?	 ?	
 ?	 ?	 ?	
 ?		 ?	
 ?			

Vdumps

Section:

Explanation:

QUESTION 122

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

- A. Dock
- B. Spotlight
- C. Mission Control

D. Launchpad

Correct Answer: C

Section:

Explanation:

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

QUESTION 123

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 124

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 125

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 126

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

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

Correct Answer: D

Section:

Explanation:

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



QUESTION 127

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

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

Correct Answer: B

Section:

Explanation:

Local Users and Groups is a Microsoft Management Console (MMC) snap-in that allows you to manage user accounts or groups on your computer¹. If you cannot find it in the MMC console, you can add it manually by following these steps²:

Press Windows key + R to open the Run dialog box, or open the Command Prompt. Type mmc and hit Enter. This will open a blank MMC console.

Click File and then Add/Remove Snap-in.

In the Add or Remove Snap-ins window, select Local Users and Groups from the Available snap-ins list, and click Add.

In the Select Computer window, choose Local computer or Another computer, depending on which computer you want to manage, and click Finish.

Click OK to close the Add or Remove Snap-ins window. You should now see Local Users and Groups in the MMC console.

QUESTION 128

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

- A. ipconfig

- B. ifconfig
- C. arpa
- D. ping

Correct Answer: B

Section:

Explanation:

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

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

sudo ifconfig en1 192.168.0.150

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

QUESTION 129

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

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



Correct Answer: C

Section:

Explanation:

NFC stands for Near Field Communication, and it is a wireless technology that allows your phone to act as a contactless payment device, among other things². Payment applications that allow payments to be made with a mobile device usually rely on NFC to communicate with the payment terminal¹. Therefore, if NFC is disabled on the phone, the payment will not work. To enable NFC on an Android phone, you need to follow these steps³:

On your Android device, open the Settings app.

Select Connected devices.

Tap on Connection preferences.

You should see the NFC option. Toggle it on.

The other options are not directly related to using a payment application with a mobile device. Airplane mode is a setting that disables all wireless communication on the phone, including NFC⁴, but it also affects calls, texts, and internet access. Bluetooth is a wireless technology that allows you to connect your phone with other devices such as headphones or speakers, but it is not used for contactless payments. Wi-Fi is a wireless technology that allows you to access the internet or a local network, but it is also not used for contactless payments. Location services are a feature that allows your phone to determine your geographic location using GPS or other methods, but they are not required for contactless payments.

QUESTION 130

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

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

Correct Answer: A

Section:**Explanation:**

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

QUESTION 131

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

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

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

Sometimes, an OS update can cause compatibility issues with some applications that are not optimized for the new version of the OS. To fix this, the user should check if there are any updates available for the application that can resolve the issue. The user can check for application updates by following these steps:

On an Android device, open the Google Play Store app and tap on the menu icon in the top left corner. Then tap on My apps & games and look for any updates available for the application. If there is an update, tap on Update to install it.

On an iOS device, open the App Store app and tap on the Updates tab at the bottom. Then look for any updates available for the application. If there is an update, tap on Update to install it.

QUESTION 132

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

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

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

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

QUESTION 133

A technician is troubleshooting application crashes on a Windows workstation. Each time the workstation user tries to open a website in a browser, the following message is displayed:
crypt32.dll is missing not found

Which of the following should the technician attempt FIRST?



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

Correct Answer: D

Section:

Explanation:

If this file is missing or corrupted, it can cause application crashes or errors when trying to open websites in a browser. To fix this, the technician can perform a system file check, which is a utility that scans and repairs corrupted or missing system files¹. To perform a system file check, the technician can follow these steps:

Open the Command Prompt as an administrator. To do this, type cmd in the search box on the taskbar, right-click on Command Prompt, and select Run as administrator. In the Command Prompt window, type sfc /scannow and hit Enter. This will start the scanning and repairing process, which may take some time.

Wait for the process to complete. If any problems are found and fixed, you will see a message saying Windows Resource Protection found corrupt files and successfully repaired them. If no problems are found, you will see a message saying Windows Resource Protection did not find any integrity violations.

Restart your computer and check if the issue is resolved.

QUESTION 134

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

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



Correct Answer: B

Section:

Explanation:

MSRA stands for Microsoft Remote Assistance, and it is a feature that allows a technician to remotely view and control another user's Windows PC with their permission. MSRA is built-in to Windows and does not require any additional software installation. To use MSRA, the technician and the user need to follow these steps:

On the user's PC, type msra in the search box on the taskbar and select Invite someone to connect to your PC and help you, or offer to help someone else.

Select Save this invitation as a file and choose a location to save the file. This file contains a password that the technician will need to connect to the user's PC.

Send the file and the password to the technician via email or another secure method. On the technician's PC, type msra in the search box on the taskbar and select Help someone who has invited you.

Select Use an invitation file and browse to the location where the file from the user is saved. Enter the password when prompted.

The user will see a message asking if they want to allow the technician to connect to their PC. The user should select Yes.

The technician will see the user's desktop and can request control of their PC by clicking Request control on the top bar. The user should allow this request by clicking Yes. The technician can now view and control the user's PC and assist them with installing software.

QUESTION 135

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

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

Correct Answer: C

Section:

Explanation:

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

QUESTION 136

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

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

Correct Answer: D**Section:****Explanation:**

Operating system updates can sometimes cause compatibility issues with some applications, such as Outlook, that may prevent them from opening or working properly. This can happen if the update changes some system files or settings that Outlook relies on, or if the update conflicts with some Outlook add-ins or extensions. To fix this, the technician can try some of these troubleshooting steps:

Start Outlook in safe mode and disable add-ins. Safe mode is a way of starting Outlook without any add-ins or extensions that may interfere with its functionality. To start Outlook in safe mode, press and hold the Ctrl key while clicking on the Outlook icon. You should see a message asking if you want to start Outlook in safe mode. Click Yes. If Outlook works fine in safe mode, it means one of the add-ins is causing the problem. To disable add-ins, go to File > Options > Add-ins. In the Manage drop-down list, select COM Add-ins and click Go. Uncheck any add-ins that you don't need and click OK. Restart Outlook normally and check if the issue is resolved.

Create a new Outlook profile. A profile is a set of settings and information that Outlook uses to manage your email accounts and data. Sometimes, a profile can get corrupted or damaged and cause Outlook to malfunction. To create a new profile, go to Control Panel > Mail > Show Profiles. Click Add and follow the instructions to set up a new profile with your email account. Make sure to select the option to use the new profile as the default one. Restart Outlook and check if the issue is resolved.

Repair your Outlook data files. Data files are files that store your email messages, contacts, calendar events, and other items on your computer. Sometimes, data files can get corrupted or damaged and cause Outlook to malfunction. To repair your data files, you can use a tool called scanpst.exe, which is located in the same folder where Outlook is installed (usually C:\Program Files\Microsoft Office\root\Office16). To use scanpst.exe, close Outlook and locate the tool in the folder. Double-click on it and browse to the location of your data file (usually

C:\Users\username\AppData\Local\Microsoft\Outlook). Select the file and click Start to begin the scanning and repairing process. When it's done, restart Outlook and check if the issue is resolved. Run the /resetnavpane command. The navigation pane is the panel on the left side of Outlook that shows your folders and accounts. Sometimes, the navigation pane can get corrupted or damaged and cause Outlook to malfunction. To reset the navigation pane, press Windows key + R to open the Run dialog box, or open the Command Prompt. Type outlook.exe /resetnavpane and hit Enter. This will clear and regenerate the navigation pane settings for Outlook. Restart Outlook and check if the issue is resolved.

QUESTION 137

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). 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 server. 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 reactivated. 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 138

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 Viewer
- 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 139

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 system. Device Manager, Administrator Tools, and Programs and Features are not Windows 10 utilities that can fix a failed update.

QUESTION 140

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 systems. 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 141

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. Reformating 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 142

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 desktops. 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 143

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). 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 144

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

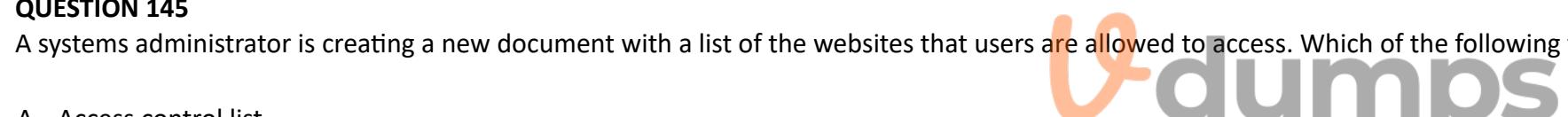
- A. Password-protected Wi-Fi
- B. Port forwarding
- C. Virtual private network
- D. Perimeter network

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 network. 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 145

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 objects. 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 146

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 147

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 148

A user requires local administrative access to a workstation. Which of the following Control Panel utilities allows the technician to grant access to the user?

- A. System
- B. Network and Sharing Center
- C. User Accounts
- D. Security and Maintenance

Correct Answer: C

Section:

Explanation:

User Accounts is a Control Panel utility that allows the technician to manage user accounts and groups on a workstation¹. The technician can use User Accounts to grant local administrative access to a user by adding the user to the Administrators group¹. The Administrators group has full control over the workstation and can perform tasks such as installing software, changing system settings, and accessing all files.

Reference: 1: User Accounts (Control Panel) (<https://docs.microsoft.com/en-us/windows/win32/shell/user-accounts>) : Local Users and Groups (<https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/local-users-and-groups>)

QUESTION 149

A user receives an error message from an online banking site that states the following:

Your connection is not private. Authority invalid.

Which of the following actions should the user take NEXT?

- A. Proceed to the site.
- B. Use a different browser.
- C. Report the error to the bank.
- D. Reinstall the browser.

Correct Answer: C

Section:

Explanation:

The error message “Your connection is not private. Authority invalid.” means that the web browser cannot verify the identity or security of the website’s SSL certificate. This could indicate that the website has been compromised, has a configuration error, or has an expired or invalid certificate. The user should not proceed to the site or use a different browser, as this could expose their sensitive information to potential attackers. The user should also not reinstall the browser, as this is unlikely to fix the error and could cause data loss. The best action for the user to take is to report the error to the bank and wait for them to resolve it.

Reference: : How to Fix “Your Connection Is Not Private” Errors (<https://www.howtogeek.com/874436/how-to-fix-your-connection-is-not-private-errors/>) : Fix connection errors (<https://support.google.com/chrome/answer/6098869?hl=en>)

QUESTION 150

A user notices a small USB drive is attached to the user's computer after a new vendor visited the office. The technician notices two files named grabber.exe and output.txt. Which of the following attacks is MOST likely occurring?

- A. Trojan
- B. Rootkit
- C. Cryptominer
- D. Keylogger

Correct Answer: D

Section:

Explanation:

A keylogger is a type of malware that records the keystrokes of a user and sends them to a remote attacker¹. The attacker can use the captured information to steal passwords, credit card numbers, or other sensitive data. A keylogger can be installed on a computer by attaching a small USB drive that contains a malicious executable file, such as grabber.exe². The output.txt file may contain the recorded keystrokes. The user should remove the USB drive and scan the computer for malware.

Reference: 2: What is grabber.exe? (<https://www.freewrapper.com/library/file/grabber.exe-55857/>) 1:

What is a keylogger? (<https://www.kaspersky.com/resource-center/definitions/keylogger>)



QUESTION 151

A SOHO client is having trouble navigating to a corporate website. Which of the following should a technician do to allow access?

- A. Adjust the content filtering.
- B. Unmap port forwarding.
- C. Disable unused ports.
- D. Reduce the encryption strength

Correct Answer: A

Section:

Explanation:

Content filtering is a process that manages or screens access to specific emails or webpages based on their content categories¹. Content filtering can be used by organizations to control content access through their firewalls and enforce corporate policies around information system management². A SOHO client may have content filtering enabled on their network and may need to adjust it to allow access to a corporate website that is blocked by default. The client can use a software program, a hardware device, or a subscription service to configure the content filtering settings and whitelist the desired website².

Reference: 1: Web content filtering (<https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/web-content-filtering?view=o365-worldwide>) 2: What is Content Filtering? Definition and Types of Content Filters (<https://www.fortinet.com/resources/cyberglossary/content-filtering>)

QUESTION 152

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

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

Correct Answer: D

Section:

Explanation:

Keychain is a feature of macOS that securely stores passwords, account numbers, and other confidential information for your Mac, apps, servers, and websites¹. You can use the Keychain Access app on your Mac to view and manage your keychains and the items stored in them¹. Keychain can also sync your passwords and other secure information across your devices using iCloud Keychain¹. Keychain can be used as a password manager in macOS to help you keep track of and protect your passwords.

Reference: 1: Manage passwords using keychains on Mac (<https://support.apple.com/guide/mac-help/use-keychains-to-store-passwords-mchlf375f392/mac>)

QUESTION 153

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

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



Correct Answer: C

Section:

Explanation:

Robocopy is a command-line utility that can be used to mirror the source data for the backup. It can copy files and folders with various options, such as copying only changed files, preserving attributes and permissions, and retrying failed copies. Robocopy is more powerful and flexible than copy or xcopy, which are simpler commands that can only copy files and folders without mirroring or other advanced features. Copy-Item is a PowerShell cmdlet that can also copy files and folders, but it is not a native Windows utility and it requires PowerShell to run¹.

Reference: 1: <https://windowsreport.com/mirror-backup-software/>

QUESTION 154

A change advisory board authorized a setting change so a technician is permitted to implement the change. The technician successfully implemented the change. Which of the following should be done NEXT?

- A. Document the date and time of change.
- B. Document the purpose of the change.
- C. Document the risk level.
- D. Document findings of the sandbox test.

Correct Answer: A

Section:

Explanation:

After implementing a change authorized by the change advisory board (CAB), the technician should document the date and time of change as part of the post-implementation review. This helps to track the change history, verify the success of the change, and identify any issues or incidents caused by the change¹. Documenting the purpose of the change, the risk level, and the findings of the sandbox test are all part of the pre-implementation activities that should be done before submitting the change request to the CAB².

Reference: 2: <https://www.manageengine.com/products/service-desk/itil-change-management/cab-change-advisory-board.html> 1: <https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/success/quick->

QUESTION 155

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 156

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 system is 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 157

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 158

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 159

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 steps^{1,2}:

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 160

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-services/clients/remote-desktop-protocol>

QUESTION 161

A company implemented a BYOD policy and would like to reduce data disclosure caused by malware that may infect these devices. Which of the following should the company deploy to address these concerns?

- A. UAC
- B. MDM
- C. LDAP
- D. SSO

Correct Answer: B

Section:

Explanation:

MDM stands for mobile device management, which is a type of software solution that allows remote management and security of mobile devices. MDM can help a company reduce data disclosure caused by malware that may infect these devices by enforcing security policies, such as encryption,

password protection, antivirus software, and remote wipe. MDM can also monitor and control the access of personal devices to corporate data and networks. UAC stands for user account control, which is a feature of Windows that prompts users for permission or an administrator password before making changes that affect the system. UAC may not be effective in preventing malware infection or data disclosure on personal devices. LDAP stands for lightweight directory access protocol, which is a protocol for accessing and managing information stored in a directory service, such as user names and passwords. LDAP does not directly address the issue of malware infection or data disclosure on personal devices. SSO stands for single sign-on, which is a feature that allows users to access multiple applications or services with one set of credentials. SSO may not prevent

malware infection or data disclosure on personal devices, and may even increase the risk if the credentials are compromised.

<https://www.nist.gov/news-events/news/2021/03/mobile-device-security-bring-your-own-devicebyod-draft-sp-1800-22>

QUESTION 162

A user's company phone was stolen. Which of the following should a technician do next?

- A. Perform a low-level format.
- B. Remotely wipe the device.
- C. Degauss the device.
- D. Provide the GPS location of the device.

Correct Answer: B

Section:

Explanation:

Remotely wiping the device is the best option to prevent unauthorized access to the company data stored on the phone. A low-level format, degaussing, or providing the GPS location of the device are not feasible or effective actions to take in this scenario.

QUESTION 163

Which of the following protocols supports fast roaming between networks?

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

Correct Answer: B

Section:

Explanation:

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

The Official CompTIA A+ Core 2 Study Guide², page 263.

WiFi Fast Roaming, Simplified³

QUESTION 164

A technician wants to mitigate unauthorized data access if a computer is lost or stolen. Which of the following features should the technician enable?

- A. Network share
- B. Group Policy
- C. BitLocker
- D. Static IP

Correct Answer: C

Section:

Explanation:

BitLocker is a Windows security feature that provides encryption for entire volumes, addressing the threats of data theft or exposure from lost, stolen, or inappropriately decommissioned devices¹. BitLocker helps mitigate unauthorized data access by enhancing file and system protections, rendering data inaccessible when BitLocker-protected devices are decommissioned or recycled¹. Network share, Group Policy, and Static IP are not features that can prevent unauthorized data access if a computer is lost or stolen.

BitLocker overview - Windows Security | Microsoft Learn¹

The Official CompTIA A+ Core 2 Study Guide², page 315.

QUESTION 165

Applications on a computer are not updating, which is preventing the user from opening certain files. Which of the following MMC snap-ins should the technician launch next to continue troubleshooting the issue?

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

Correct Answer: C

Section:

Explanation:



devmgmt.msc is the MMC snap-in that opens the Device Manager, a tool that allows the technician to view and manage the hardware devices and their drivers on the computer¹. If the applications are not updating properly, it could be due to outdated, corrupted, or incompatible drivers that prevent the hardware from functioning normally.²The technician can use the Device Manager to update, uninstall, rollback, or disable the drivers, as well as scan for hardware changes, troubleshoot problems, and view device properties.

gpedit.msc is the MMC snap-in that opens the Group Policy Editor, a tool that allows the technician to configure the local or domain group policy settings for the computer or a group of computers³. Group policy settings can affect the security, performance, and functionality of the system, but they are not directly related to the application updates or the hardware drivers.

perfmon.msc is the MMC snap-in that opens the Performance Monitor, a tool that allows the technician to monitor and analyze the performance of the system and its components, such as processor, memory, disk, network, etc⁴.Performance Monitor can display real-time data or collect log data for later analysis, as well as generate reports and alerts based on the performance counters⁵. Performance Monitor can help the technician identify and diagnose performance issues, but it does not provide a way to manage the hardware drivers.

The Official CompTIA A+ Core 2 Study Guide⁶, page 223, 225, 227, 228.

QUESTION 166

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

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

Correct Answer: A

Section:

Explanation:

The Network & Internet settings in Windows 10 allow the user to input the SSID and password of a Wi-Fi network, as well as manage other network-related options, such as airplane mode, mobile hotspot, VPN, proxy, etc¹.To access the Network & Internet settings, the user can select the Start button, then select Settings > Network & Internet².Alternatively, the user can right-click the Wi-Fi icon on the taskbar and click 'Open Network & Internet Settings'³.

The System settings in Windows 10 allow the user to configure the display, sound, notifications, power, storage, and other system-related options¹.The Personalization settings in Windows 10 allow the user to customize the background, colors, lock screen, themes, fonts, and other appearance-related options¹.The Accounts settings in Windows 10 allow the user to manage the user accounts, sign-in options, sync settings, and other account-related options¹. None of these settings can be used to input the SSID and password of a Wi-Fi network.

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

QUESTION 167

Which of the following does MFA provide?

- A. Security enhancement
- B. Encryption
- C. Digital signature
- D. Public key infrastructure

Correct Answer: A

Section:

Explanation:

MFA stands for multi-factor authentication, which is an electronic authentication method that requires the user to provide two or more verification factors to gain access to a resource such as an application, online account, or a VPN¹. MFA provides security enhancement by making it harder for attackers to compromise the user's identity or credentials, as they would need to obtain more than just the username and password.MFA can also prevent unauthorized access to sensitive data or resources, as well as reduce the risk of identity theft or fraud².

QUESTION 168

In an organization with a standardized set of installed software, a developer submits a request to have new software installed. The company does not currently have a license for this software, but the developer already downloaded the installation file and is requesting that the technician install it. The developer states that the management team approved the business use of this software. Which of the following is the best action for the technician to take?

- A. Contact the software vendor to obtain the license for the user, and assist the user with installation once the license is purchased.
- B. Run a scan on the downloaded installation file to confirm that it is free of malicious software, install the software, and document the software installation process.
- C. Indicate to the developer that formal approval is needed; then, the IT team should investigate the software and the impact it will have on the organization before installing the software.
- D. Install the software and run a full system scan with antivirus software to confirm that the operating system is free of malicious software.

Correct Answer: C

Section:

Explanation:

Installing new software on an organization's system or device can have various implications, such as compatibility, security, performance, licensing, and compliance issues. Therefore, it is important to follow the best practices for software installation, such as doing research on the software, checking the system requirements, scanning the installation file for malware, and obtaining the proper license. The technician should not install the software without formal approval from the management team, as this could violate the organization's policies or regulations. The technician should also not install the software without investigating the software and its impact on the organization, as this could introduce potential risks or problems to the system or device. The technician should indicate to the developer that formal approval is needed, and then work with the IT team to evaluate the software and its suitability for the organization before installing it.

QUESTION 169

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

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

Correct Answer: B

Section:

Explanation:

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

QUESTION 170

A technician needs to reimagine a desktop in an area without network access. Which of the following should the technician use? (Select two).

- A. USB
- B. PXE
- C. Optical media
- D. Partition
- E. Boot record
- F. SMB

Correct Answer: A, C

Section:

Explanation:

A technician needs to reimagine a desktop in an area without network access, which means that the technician cannot use network-based methods such as PXE or SMB to deploy the image. Therefore, the technician should use offline methods that involve removable media such as USB or optical media. USB and optical media are common ways to store and transfer system images, and they can be used to boot the desktop and initiate the reimaging process. The technician will need to create a bootable USB or optical media that contains the system image and the imaging software, and then insert it into the desktop and change the boot order in the BIOS or UEFI settings. The technician can then follow the instructions on the screen to reimagine the desktop.

QUESTION 171

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

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

Correct Answer: C

Section:

Explanation:

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

QUESTION 172

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

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

Correct Answer: B

Section:

Explanation:

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

QUESTION 173

A management team at a small office wants to block access to inappropriate websites and create a log of these access attempts. Which of the following is a way to meet these requirements?

- A. Content filter
- B. Screened subnet
- C. Port forwarding
- D. Access control list

Correct Answer: A

Section:

Explanation:

A content filter is a device or software that blocks or allows access to web pages based on predefined criteria, such as keywords, categories, or ratings. A content filter can also create a log of the blocked or allowed web requests, which can help the management team monitor and audit the web usage of their employees. A content filter is different from the other options because:

A screened subnet is a network segment that is protected by two firewalls, one facing the internet and one facing the internal network. A screened subnet can isolate servers or hosts that need to be accessed from both sides, such as a web server or a bastion host. A screened subnet does not filter web content based on predefined criteria, but rather on network addresses, ports, and protocols.

Port forwarding is a technique that allows a router to forward packets from one port to another port, usually on a different device. Port forwarding can enable remote access to services or applications that are hosted on a private network, such as a web server or a game server. Port forwarding does not filter web content based on predefined criteria, but rather on destination ports and addresses.

An access control list (ACL) is a set of rules that defines which packets are allowed or denied on a network device, such as a router or a firewall. An ACL can filter packets based on source and destination addresses, ports,



protocols, and other criteria. An ACL can also create a log of the matched or unmatched packets, which can help the management team troubleshoot and secure their network. An ACL does not filter web content based on predefined criteria, but rather on packet headers and fields.

QUESTION 174

Which of the following is the best way to limit the loss of confidential data if an employee's company smartphone is lost or stolen?

- A. Installing a VPN
- B. Implementing location tracking
- C. Configuring remote wipe
- D. Enabling backups

Correct Answer: C

Section:

Explanation:

Configuring remote wipe allows the device owner or administrator to erase all the data on the device remotely, in case it is lost or stolen. This prevents unauthorized access to confidential data and reduces the risk of data breaches. Installing a VPN, implementing location tracking, and enabling backups are useful features, but they do not directly limit the loss of data if the device is compromised. Reference: CompTIA A+ Certification Exam Core 2 Objectives, Domain 2.0: Security, Objective 2.5: Given a scenario, use methods to secure mobile devices.

QUESTION 175

Which of the following are mobile operating systems used on smartphones? (Select two).

- A. macOS
- B. Windows
- C. Chrome OS
- D. Linux
- E. iOS
- F. Android



Correct Answer: E, F

Section:

Explanation:

iOS and Android are the two most popular and widely used mobile operating systems for smartphones. They are both based on Unix-like kernels and provide a variety of features and applications for users and developers. iOS is developed by Apple and runs exclusively on Apple devices, such as iPhones and iPads. Android is developed by Google and runs on a range of devices from different manufacturers, such as Samsung, Huawei, and Motorola. The other options are not mobile operating systems for smartphones, but rather for other types of devices or platforms. macOS is a desktop operating system for Apple computers, such as MacBooks and iMacs. Windows is a desktop operating system for Microsoft computers, such as Surface and Dell. Chrome OS is a web-based operating system for Google devices, such as Chromebooks and Chromecast. Linux is a family of open-source operating systems for various devices and platforms, such as Ubuntu, Fedora, and Raspberry Pi.

QUESTION 176

Which of the following languages is used for scripting the creation of Active Directory accounts?

- A. Bash
- B. SQL
- C. PHP
- D. PowerShell

Correct Answer: D

Section:

Explanation:

PowerShell is a scripting language that can interact with Active Directory and other Windows components. It has a built-in cmdlet called New-ADUser that can create user accounts in Active Directory. PowerShell can also use the Active Directory module to access other AD-related functions and attributes. Other languages, such as Bash, SQL, and PHP, are not designed for creating Active Directory accounts and would require additional tools or libraries to do so.

