Number: 220-1102
Passing Score: 800
Time Limit: 120
File Version: 12.0

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

Exam A

QUESTION 1
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 application12Resetting 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 2
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 3
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 4

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

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

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

QUESTION 5
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 6
A desktop engineer is deploying a master image. Which of the following should the desktop engineer consider when building the master image? (Select TWO).

A. Device drivers
B. Keyboard backlight settings
C. Installed application license keys
D. Display orientation
E. Target device power supply
F. Disabling express charging

Correct Answer: A, C

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

QUESTION 7
A technician is setting up a conference room computer with a script that boots the application on login. Which of the following would the technician use to accomplish this task? (Select TWO).

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

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

QUESTION 8
A neighbor successfully connected to a user's Wi-Fi network. Which of the following should the user do after changing the network configuration to prevent the neighbor from being able to connect again?

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

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

QUESTION 9
A technician is troubleshooting a PC that has been performing poorly. Looking at the Task Manager, the technician sees that CPU and memory resources seem fine, but disk throughput is at 100%.
Which of the following types of malware is the system MOST likely infected with?

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

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

QUESTION 10
A homeowner recently moved and requires a new router for the new ISP to function correctly. The internet service has been installed and has been confirmed as functional. Which of the following is the FIRST step the homeowner should take after installation of all relevant cabling and hardware?

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

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

QUESTION 11
A user rotates a cell phone horizontally to read emails, but the display remains vertical, even though the settings indicate autorotate is on. VT1ich of the following will MOST likely resolve the issue?

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

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

QUESTION 12
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 13
A network administrator is deploying a client certificate lo be used for Wi-Fi access for all devices m 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 14
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 customers4Reference: 2. Bollards. Retrieved from https://en.wikipedia.org/wiki/
Bollard

QUESTION 15
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 16
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 46B 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. Thex64 version of Windows 10 can use up to 2TB of RAM1.

QUESTION 17
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 18
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 19
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 20
A user is unable to use any internet-related functions on a smartphone when it is not connected to Wi-Fi When the smartphone is connected to Wi-Fi the user can browse the internet and send and receive email. The user is also able to send and receive text messages and phone calls when the smartphone is not connected to Wi-Fi. Which of the following is the MOST likely reason the user is unable to use the internet on the smartphone when it is not connected to Wi-Fi?

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

Correct Answer: A
Section:
Explanation:
The smartphone’s line was not provisioned with a data plan. The user is unable to use any internet- related functions on the smartphone when it is not connected to Wi-Fi because the smartphone’sline was not provisioned with a data plan. The user can send and receive text messages and phone calls when the smartphone is not connected to Wi-Fi because these functions do not require an internet connection1

QUESTION 21
A technician is investigating an employee's smartphone that has the following symptoms
• The device is hot even when it is not in use.
•Applications crash, especially when others are launched
• Certain applications, such as GPS, are in portrait mode when they should be in landscape mode Which of the following can the technician do to MOST likely resolve these issues with minimal impact? (Select TWO).

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

Correct Answer: A, C
Section:
Explanation:
The technician can close unnecessary applications and turn on autorotation to resolve these issues with minimal impact. Autorotation can help the device to switch between portrait and landscapemodes automatically. Closing

unnecessary applications can help to free up the device's memory and reduce the device's temperature1Reference:CompTIA A+ Certification Exam: Core 2 (220-1102) Exam Objectives Version 4.0. Retrieved from https://partners.comptia.org/docs/default-source/resources/comptia-a-220-1102-exam-objectives- (3-0)

QUESTION 22
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 23
A department has the following technical requirements for a new application:

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

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

A. CPU
B. Hard drive
C. RAM
D. Touch screen

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

QUESTION 24
Which of the following Wi-Fi protocols is the MOST secure?

A. WPA3
B. WPA-AES
C. WEP
D. WPA-TKIP

Correct Answer: A
Section:

Explanation:

QUESTION 25
A user attempts to open some files, but a message appears stating that the files are encrypted. The user was able to access these files before without receiving this message and no changes have been made within the company. Which of the following has infected the computer?

A. Cryptominer
B. Phishing
C. Ransomware
D. Keylogger

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

QUESTION 26
A help desk technician is troubleshooting a workstation in a SOHO environment that is running above normal system baselines. The technician discovers an unknown executable with a random string name running on the system. The technician terminates the process, and the system returns to normal operation. The technician thinks the issue was an infected file, but the antivirus is not detecting a threat. The technician is concerned other machines may be infected with this unknown virus. Which of the following is the MOST effective way to check other machines on the network for this unknown threat?

A. Run a startup script that removes files by name.
B. Provide a sample to the antivirus vendor.
C. Manually check each machine.
D. Monitor outbound network traffic.

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

QUESTION 27
A user reports that a PC seems to be running more slowly than usual. A technician checks system resources, but disk, CPU, and memory usage seem to be fine. The technician sees that GPU temperature is extremely high. Which of the following types of malware is MOST likely to blame?

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

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

of malware that infects the boot sector of a hard drive, but they do not typically cause high GPU temperatures12

QUESTION 28
Upon downloading a new ISO, an administrator is presented with the following string:
59d15a16ce90cBcc97fa7c211b767aB Which of the following BEST describes the purpose of this string?

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

Correct Answer: C
Section:
Explanation:
Hash verification is a process that verifies the integrity of a file by comparing the hash value of the downloaded file to the hash value provided by the source1

QUESTION 29
Which of the following OS types provides a lightweight option for workstations thai need an easy-touse browser-based interface?

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

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

QUESTION 30
Following the latest Windows update PDF files are opening in Microsoft Edge instead of Adobe Reader. Which of the following utilities should be used to ensure all PDF files open in Adobe Reader?

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

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

QUESTION 31
Which of the following provide the BEST way to secure physical access to a data cento server room?
(Select TWO).

A. Biometric lock
B. Badge reader

C. USB token
D. Video surveillance
E. Locking rack
F. Access control vestibule

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

QUESTION 32
During a recent flight an executive unexpectedly received several dog and cat pictures while trying to watch a movie via in-flight Wi-Fi on an iPhone. The executive has no records of any contacts sending pictures like these and has not seen these pictures before. To BEST resolve this issue, the executive should:

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

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

QUESTION 33
A user reports that antivirus software indicates a computer is infected with viruses. The user thinks this happened white browsing the internet. The technician does not recognize the interface with which the antivirus message is presented.
Which of the following is the NEXT step the technician should take?

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

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

QUESTION 34
The command cac cor.pti a. txt was issued on a Linux terminal. Which of the following results should be expected?

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

Correct Answer: B
Section:
Explanation:
The command cac cor.ptia. txt was issued on a Linux terminal. This command would display the contents of the text comptia.txt.

QUESTION 35
A user's smarlphone data usage is well above average. The user suspects an installed application is transmitting data in the background The user would like to be alerted when an application attempts to communicate with the internet.
Which of the following BEST addresses the user's concern?

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

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

QUESTION 36
A technician is unable to join a Windows 10 laptop to a domain Which of the following is the MOST likely reason?

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

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

QUESTION 37
A technician is troubleshooting an issue involving programs on a Windows 10 machine that are loading on startup but causing excessive boot times. Which of the following should the technician do to selectively prevent programs from loading?

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

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

QUESTION 38
A desktop specialist needs to prepare a laptop running Windows 10 for a newly hired employee.
Which of the following methods should the technician use to refresh the laptop?

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

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

QUESTION 39
A technician found that an employee is mining cryptocurrency on a work desktop. The company has decided that this action violates its guidelines. Which of the following should be updated to reflect this new requirement?

A. MDM
B. EULA
C. IRP
D. AUP

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

QUESTION 40
A user calls the help desk to report that none of the files on a PC will open. The user also indicates a program on the desktop is requesting payment in exchange for file access A technician verifies the user's PC is infected with ransorrrware.
Which of the following should the technician do FIRST?

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

Correct Answer: C
Section:

Explanation:
The technician should quarantine the system first1Reference:CompTIA A+ Certification Exam: Core 2 Objectives Version 4.0. Retrieved from https://partners.comptia.org/docs/default-source/resources/comptia-a-220-1102-exam-objectives- (3-0)

QUESTION 41
A user has requested help setting up the fingerprint reader on a Windows 10 laptop. The laptop is equipped with a fingerprint reader and is joined to a domain Group Policy enables Windows Hello on all computers in the environment. Which of the following options describes how to set up Windows Hello Fingerprint for the user?

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

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

QUESTION 42
A user reports a PC is running slowly. The technician suspects it has a badly fragmented hard drive.
Which of the following tools should the technician use?

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

Correct Answer: C
Section:
Explanation:
The technician should use dfrgui.exe to defragment the hard drive1

QUESTION 43
A user reports a computer is running stow. Which of the following tools will help a technician identify the issue?

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

Correct Answer: D
Section:

Explanation:

QUESTION 44
A user is unable to log in to the domain with a desktop PC, but a laptop PC is working properly on the same network. A technician logs in lo the desktop PC with a local account but is unable to browse to the secure intranet site to get
troubleshooting tools. Which of the following is the MOST likely cause of the issue?

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

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

QUESTION 45
Which of the following could be used to implement secure physical access to a data center?

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

Correct Answer: C
Section:
Explanation:
Badge readers are used to implement secure physical access to a data center. They are used to readthe identification information on an employee’s badge and grant access to the data center if the employee is authorized2.This system requires individuals to have an access badge that contains their identification information or a unique code that can be scanned by a reader. After the badge is scanned, the system compares the information on the badge with the authorized personnel database to authenticate if the individual has the required clearance to enter that area. The other options listed, such as a geofence, alarm system, or motion sensor are security measures that may be used in conjunction with badge readers, but do not provide identification and authentication features.

QUESTION 46
A user wants to set up speech recognition on a PC In which of the following Windows Settings tools can the user enable this option?

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

Correct Answer: D
Section:
Explanation:
The user can enable speech recognition on a PC in the Ease of Access settings tool. To set up Speech Recognition on a Windows PC, the user should open Control Panel, click on Ease of Access, click on Speech Recognition, and click the Start Speech Recognition link. Language settings can be used to change the language of the speech recognition feature, but they will not enable the feature. System settings can be used to configure the hardware

and software of the PC, but they will not enable thespeech recognition feature. Personalization settings can be used to customize the appearance and behavior of the PC, but they will not enable the speech recognition feature1Open up ease of access, click on speech, then there is an on and off button for speech recognition.

QUESTION 47
A user is experiencing frequent malware symptoms on a Windows workstation. The user has tried several times to roll back the state but the malware persists. Which of the following would MOST likely resolve the issue?

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

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

QUESTION 48
A technician needs lo formal a USB drive to transfer 20GB of data from a Linux computer to a Windows computer. Which of the following filesystems will the technician MOST likely use?

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

Correct Answer: D
Section:
Explanation:

QUESTION 49
A technician is setting up a desktop computer in a small office. The user will need to access files on a drive shared from another desktop on the network. Which of the following configurations should the technician employ to achieve this goal?

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

Correct Answer: A
Section:
Explanation:
The technician should configure the network as private to allow the user to access files on a drive shared from another desktop on the network1

QUESTION 50
A technician needs to transfer a large number of files over an unreliable connection. The technician should be able to resume the process if the connection is interrupted. Which of the following tools can be used?

A. afc

B. ehkdsk
C. git clone
D. zobocopy

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

QUESTION 51
An incident handler needs to preserve evidence for possible litigation. Which of the following will the incident handler MOST likely do to preserve the evidence?

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

Correct Answer: B
Section:
Explanation:
The incident handler should clone any impacted hard drives to preserve evidence for possible litigation1

QUESTION 52
After clicking on a link in an email a Chief Financial Officer (CFO) received the following error:

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

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

D. Instruct the CFO to exit the browser

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

QUESTION 53
A technician has spent hours trying to resolve a computer issue for the company's Chief Executive Officer (CEO). The CEO needs the device returned as soon as possible. Which of the following steps should the technician take NEXT?

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

Correct Answer: D
Section:
Explanation:
The technician should escalate the ticket to ensure that the CEO's device is returned as soon as possible1

QUESTION 54
A technician needs to exclude an application folder from being cataloged by a Windows 10 search.
Which of the following utilities should be used?

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

Correct Answer: B
Section:
Explanation:
To exclude an application folder from being cataloged by a Windows 10 search, the technician should use the Indexing Options utility1

QUESTION 55
The network was breached over the weekend System logs indicate that a single user's account was successfully breached after 500 attempts with a dictionary attack. Which of the following would BEST mitigate this threat?

A. Encryption at rest
B. Account lockout
C. Automatic screen lock
D. Antivirus

Correct Answer: B
Section:
Explanation:
Account lockout would best mitigate the threat of a dictionary attack

QUESTION 56
As part of a CYOD policy a systems administrator needs to configure each user's Windows device to require a password when resuming from a period of sleep or inactivity. Which of the following paths will lead the administrator to the correct settings?

A. Use Settings to access Screensaver settings
B. Use Settings to access Screen Timeout settings
C. Use Settings to access General
D. Use Settings to access Display.

Correct Answer: A
Section:
Explanation:
The systems administrator should use Settings to access Screensaver settings to configure each user's Windows device to require a password when resuming from a period of sleep or inactivity

QUESTION 57
A user is configuring a new SOHO Wi-Fi router for the first time. Which of the following settings should the user change FIRST?

A. Encryption
B. Wi-Fi channel
C. Default passwords
D. Service set identifier

Correct Answer: C
Section:
Explanation:
the user should change the default passwords first when configuring a new SOHO Wi-Fi router1

QUESTION 58
An organization is centralizing support functions and requires the ability to support a remote user's desktop. Which of the following technologies will allow a technician to see the issue along with the user?

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

Correct Answer: B
Section:
Explanation:
VNC will allow a technician to see the issue along with the user when an organization is centralizing support functions and requires the ability to support a remote user's desktop1

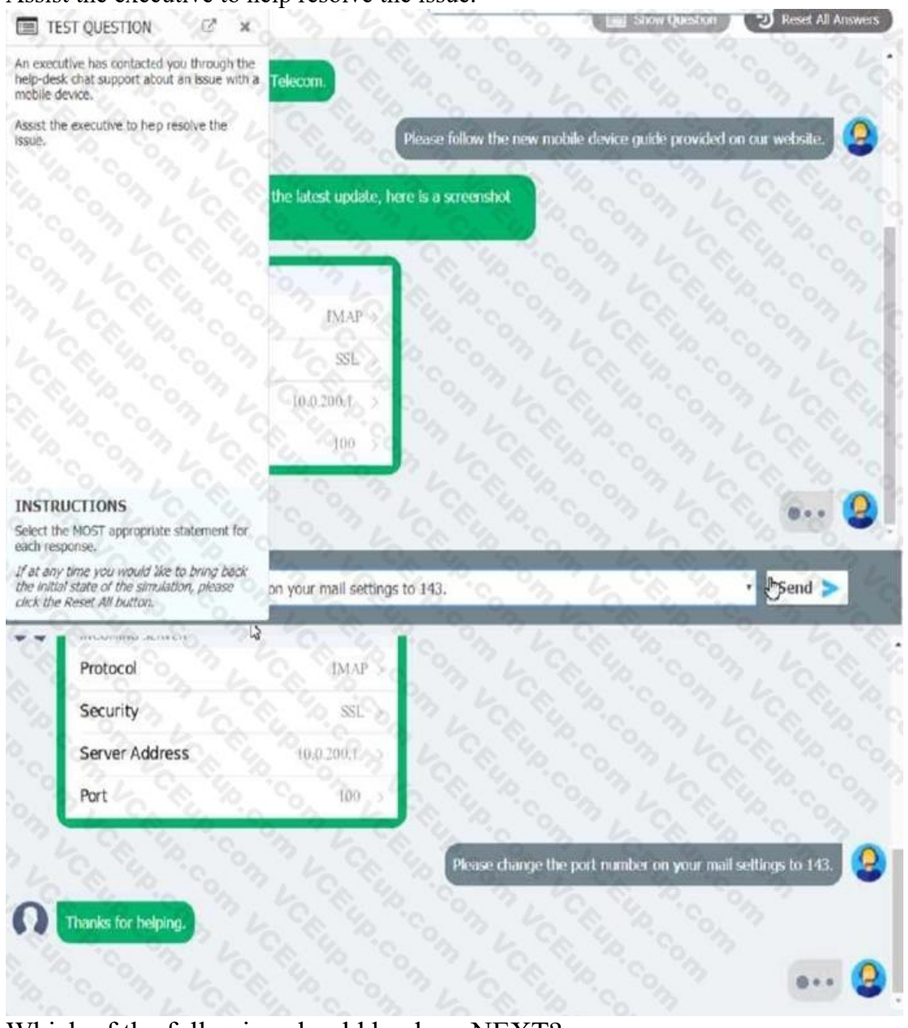
QUESTION 59
A user reports that a workstation is operating sluggishly Several other users operate on the same workstation and have reported that the workstation is operating normally. The systems administrator has validated that the workstation functions normally. Which of the following steps should 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 60
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.

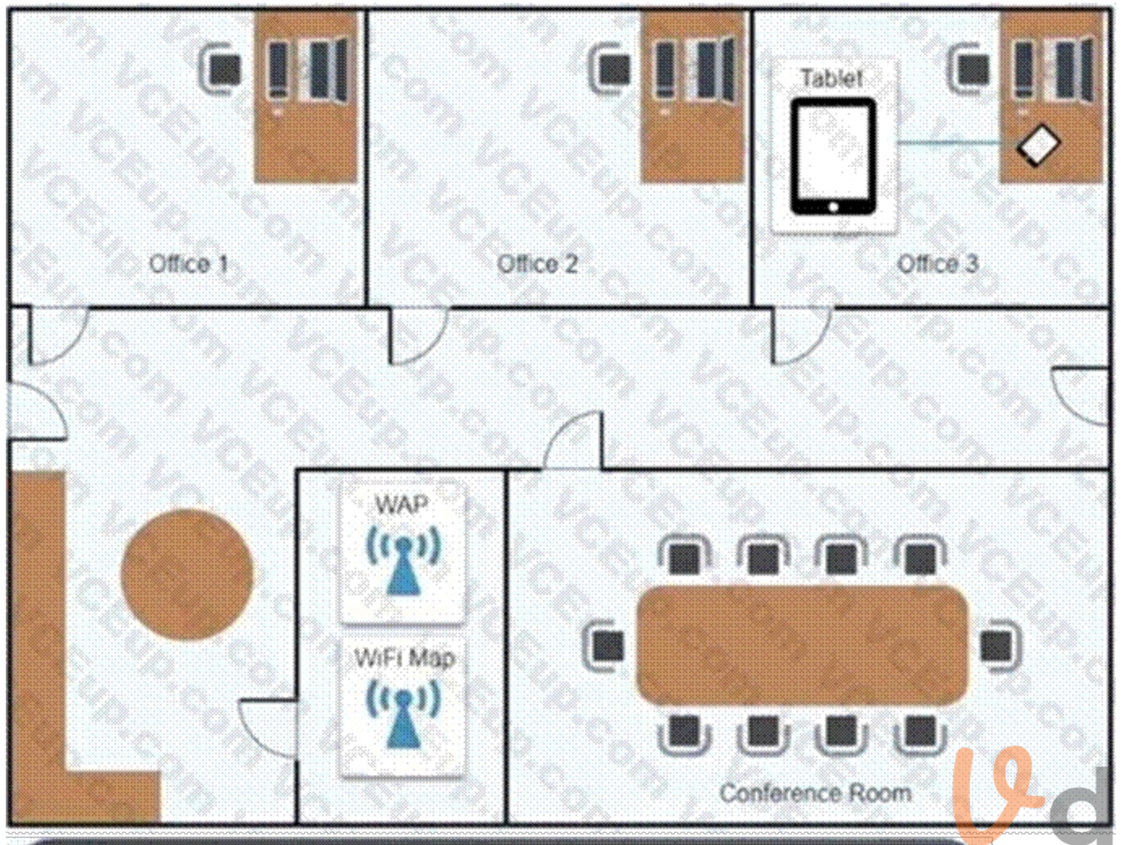


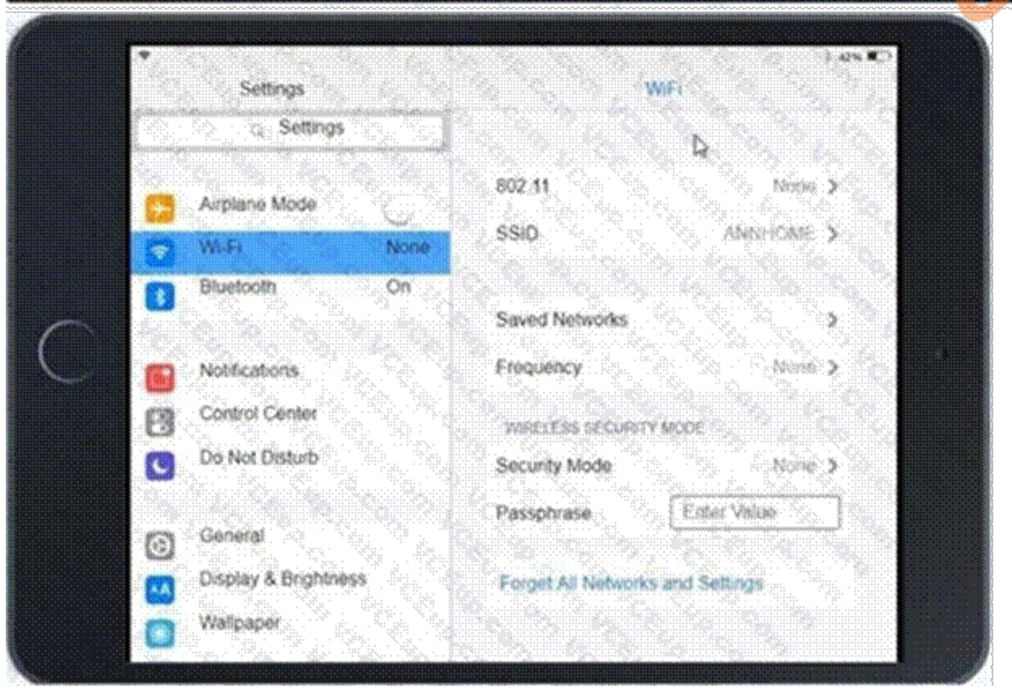
Which of the following should be done NEXT?

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.

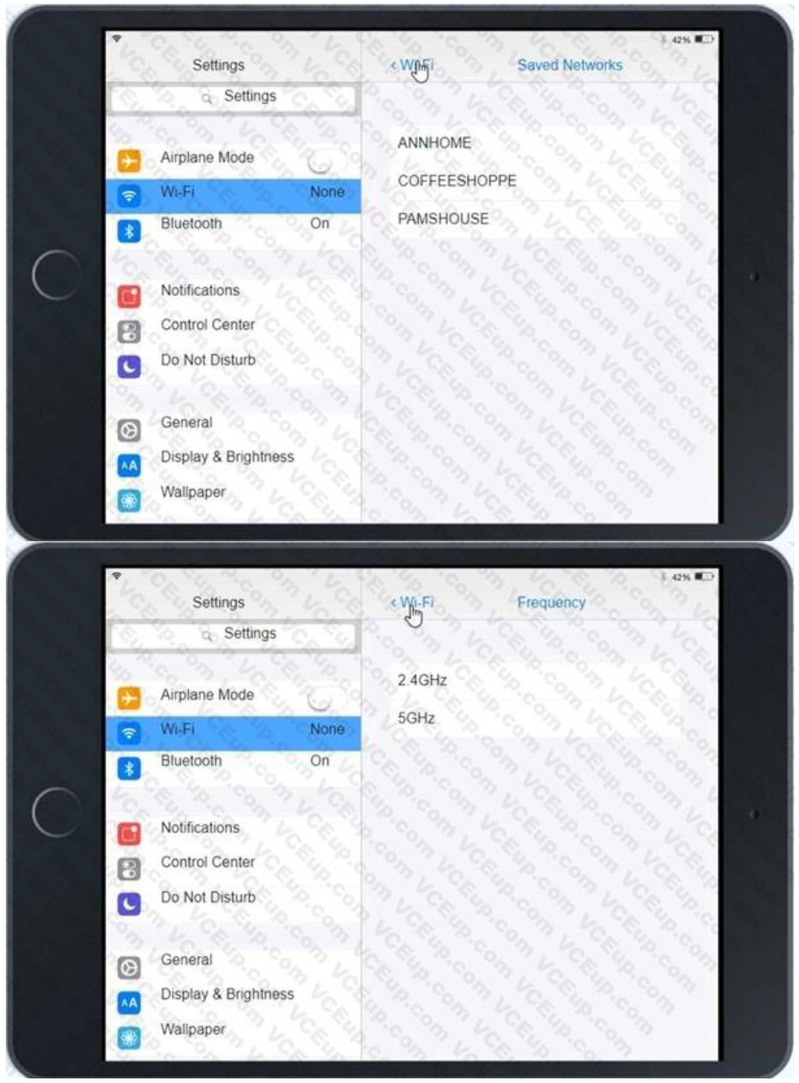
Correct Answer: A
Section:
Explanation:

QUESTION 61
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.

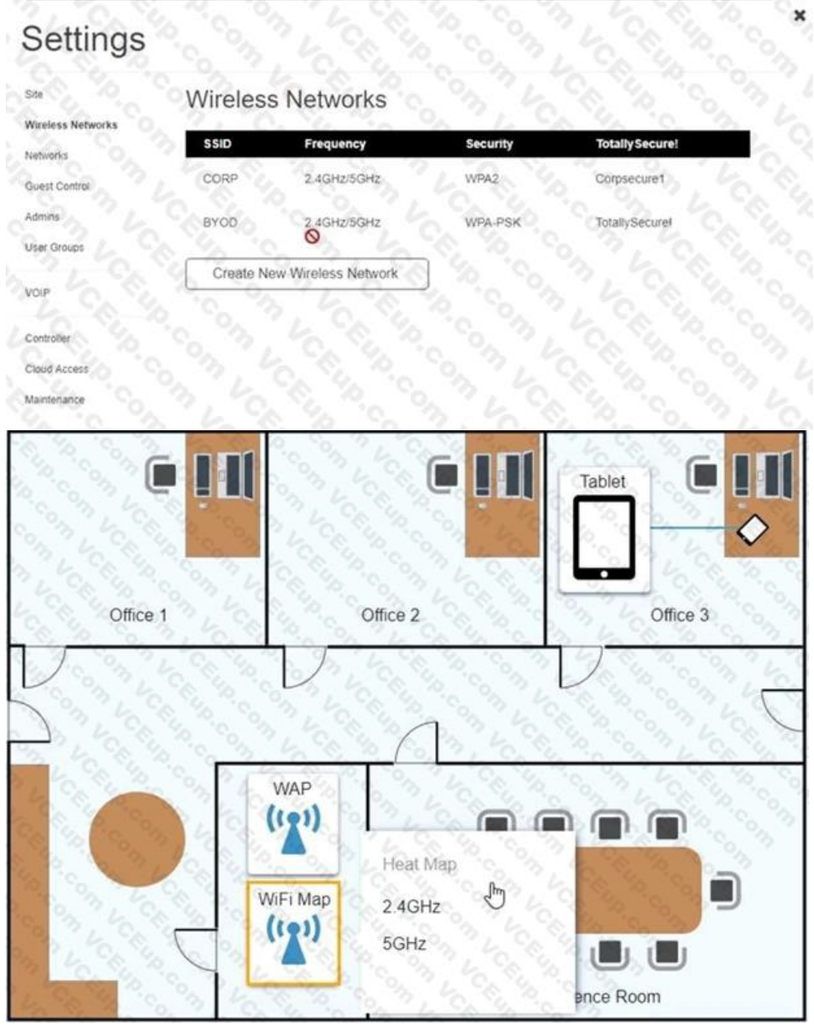

Tablet
Office 1
Office 2
Office 3
WAP
WiFi Map
Conference Room


Settings
Settings
Airplane Mode
Wi-Fi None
Bluetooth On
Notifications
Control Center
Do Not Disturb
General
Display & Brightness
Wallpaper
WiFi
802.11 None
SSID
Saved Networks
Frequency None
WIRELESS SECURITY MODE
Security Mode None
Passphrase Enter Value
Forget All Networks and Settings


Settings
Settings
Airplane Mode
Wi-Fi None
Bluetooth On
Notifications
Control Center
Do Not Disturb
General
Display & Brightness
Wallpaper
< Wi-Fi 802.11
b/g
a
ac
Settings
Settings
Airplane Mode
Wi-Fi None
Bluetooth On
Notifications
Control Center
Do Not Disturb
General
Display & Brightness
Wallpaper
< Wi-Fi SSID
BYOD
DEFAULT
CORP
ANNHOME


Settings
Settings
Airplane Mode
Wi-Fi None
Bluetooth On
Notifications
Control Center
Do Not Disturb
General
Display & Brightness
Wallpaper
< Wi-Fi
Saved Networks
ANNHOME
COFFEESHOPPE
PAMSHOUSE
Settings
Settings
Airplane Mode
Wi-Fi None
Bluetooth On
Notifications
Control Center
Do Not Disturb
General
Display & Brightness
Wallpaper
< Wi-Fi
Frequency
2.4GHz
5GHz


Settings
Settings
Airplane Mode
Wi-Fi None
Bluetooth On
Notifications
Control Center
Do Not Disturb
General
Display & Brightness
Wallpaper
Wi-Fi
Security Mode
OPEN
WEP
WPA
WPA2


Settings
Site
Wireless Networks
Networks
Guest Control
Admins
User Groups
VOIP
Controller
Cloud Access
Maintenance
Wireless Networks
SSID
Frequency
Security
Totally Secure!
CORP
2.4GHz/5GHz
WPA2
Corpsecure1
BYOD
2.4GHz/5GHz
WPA-PSK
TotallySecure!
Create New Wireless Network
Office 1
Office 2
Office 3
Tablet
WAP
WiFi Map
Heat Map
2.4GHz
5GHz
ence Room

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

Click on Frequency and select 5GHz

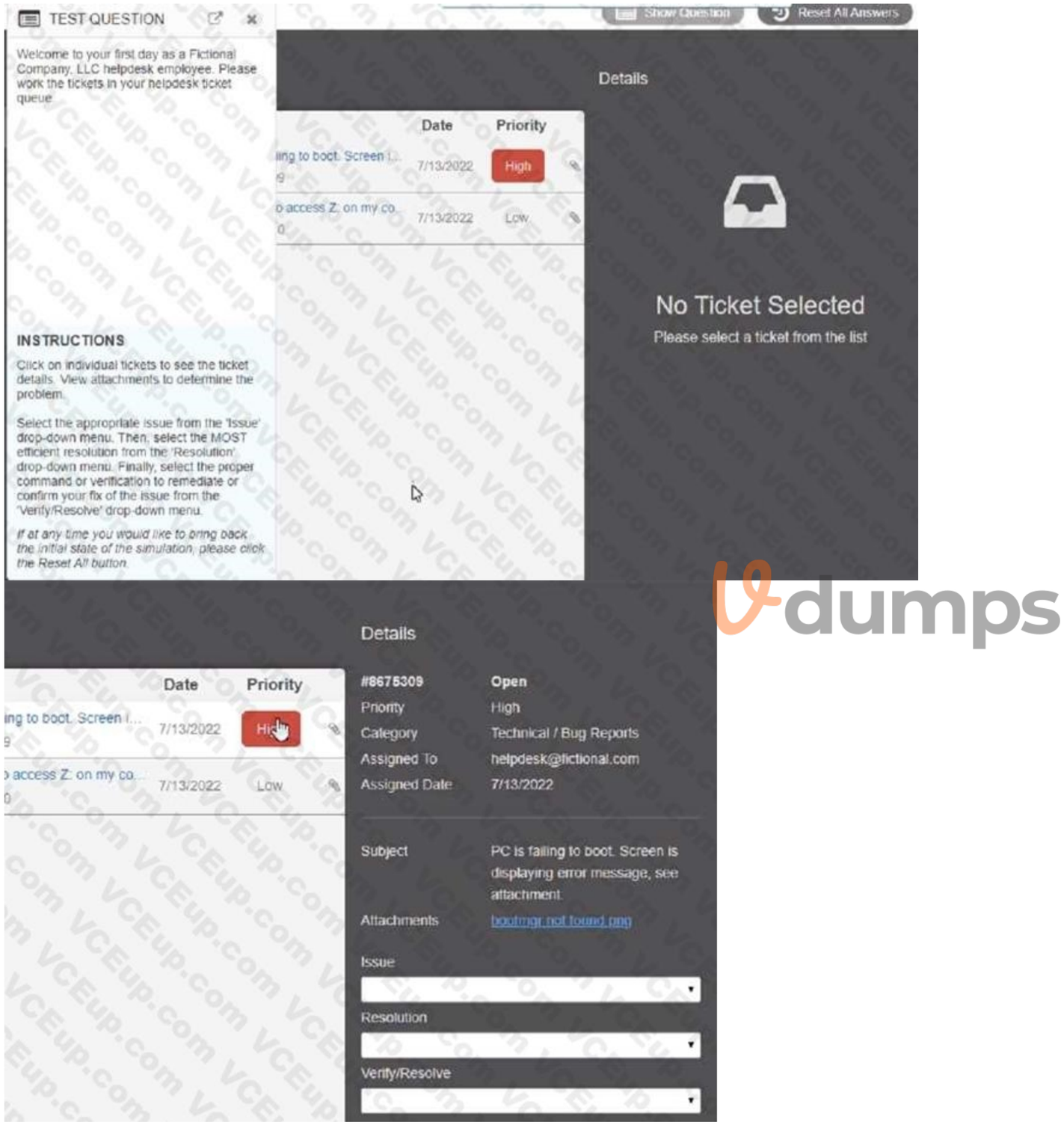
At Wireless Security Mode, Click on Security Mode

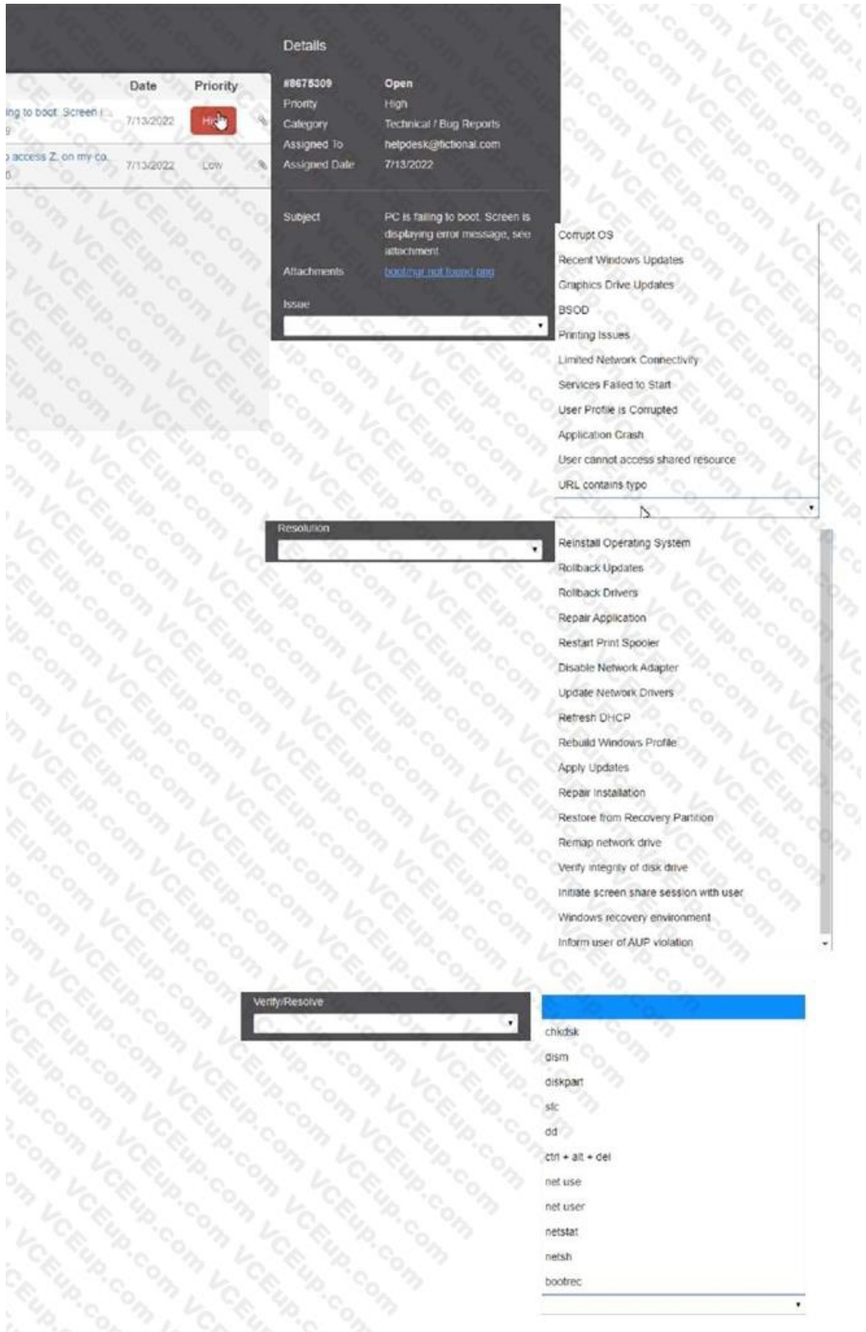
Select the WPA2

Explanation:

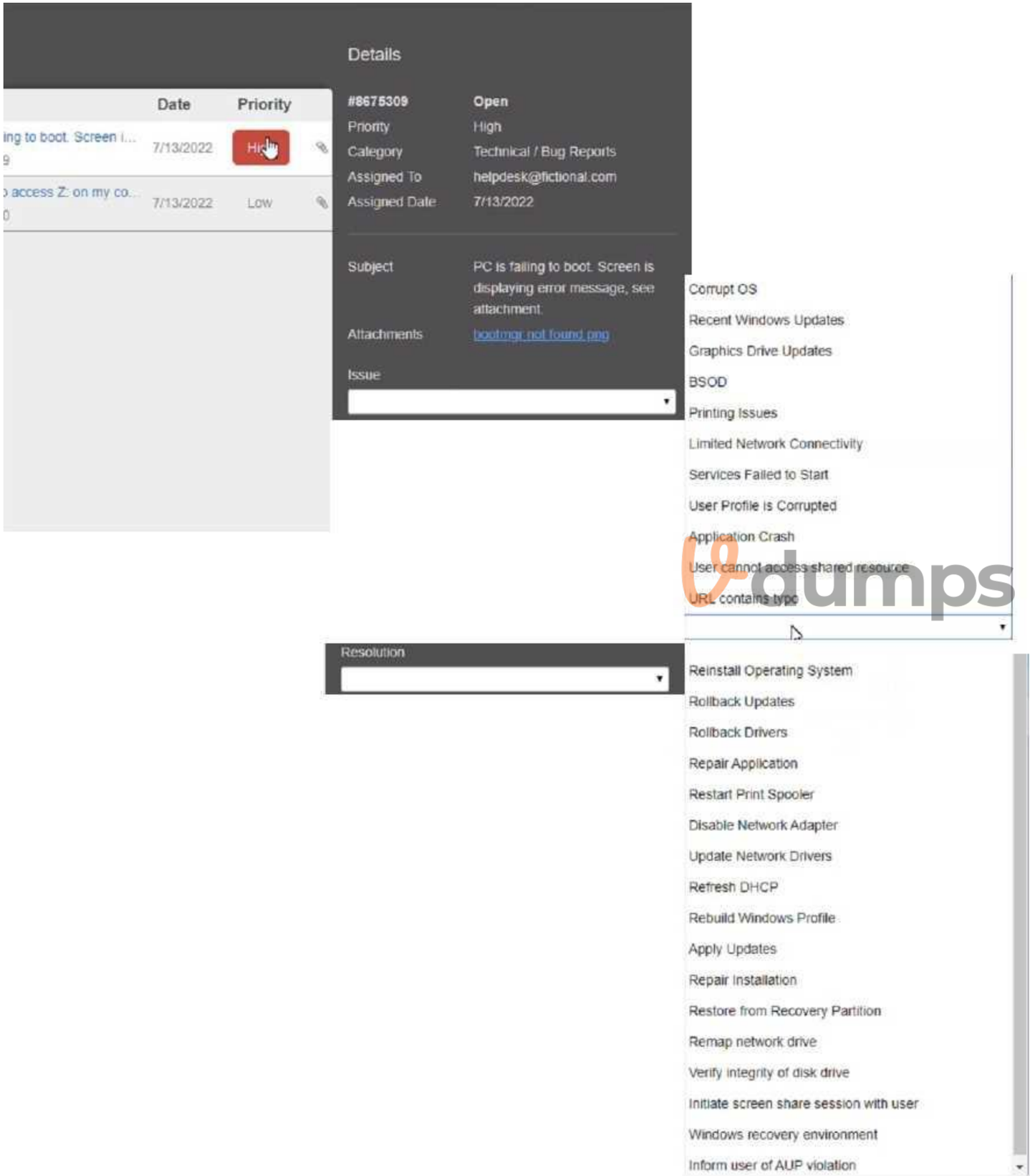
Ann needs to connect to the BYOD SSID, using 2.4GHZ. The selected security method chose should be WPA PSK, and the password should be set to TtotallySecret.

QUESTION 62
HOTSPOT
Welcome to your first day as a Fictional Company. LLC helpdesk employee. Please work the tickets in your helpdesk ticket queue.
Click on individual tickers to see the ticket details. View attachments to determine the problem.
Select the appropriate issue from the 'issue' drop-down menu. Then, select the MOST efficient resolution from the 'Resolution' drop-down menu. Finally, select the proper command or verification to remediate or confirm your fix of the issue from the Verify Resolve drop-down menu.

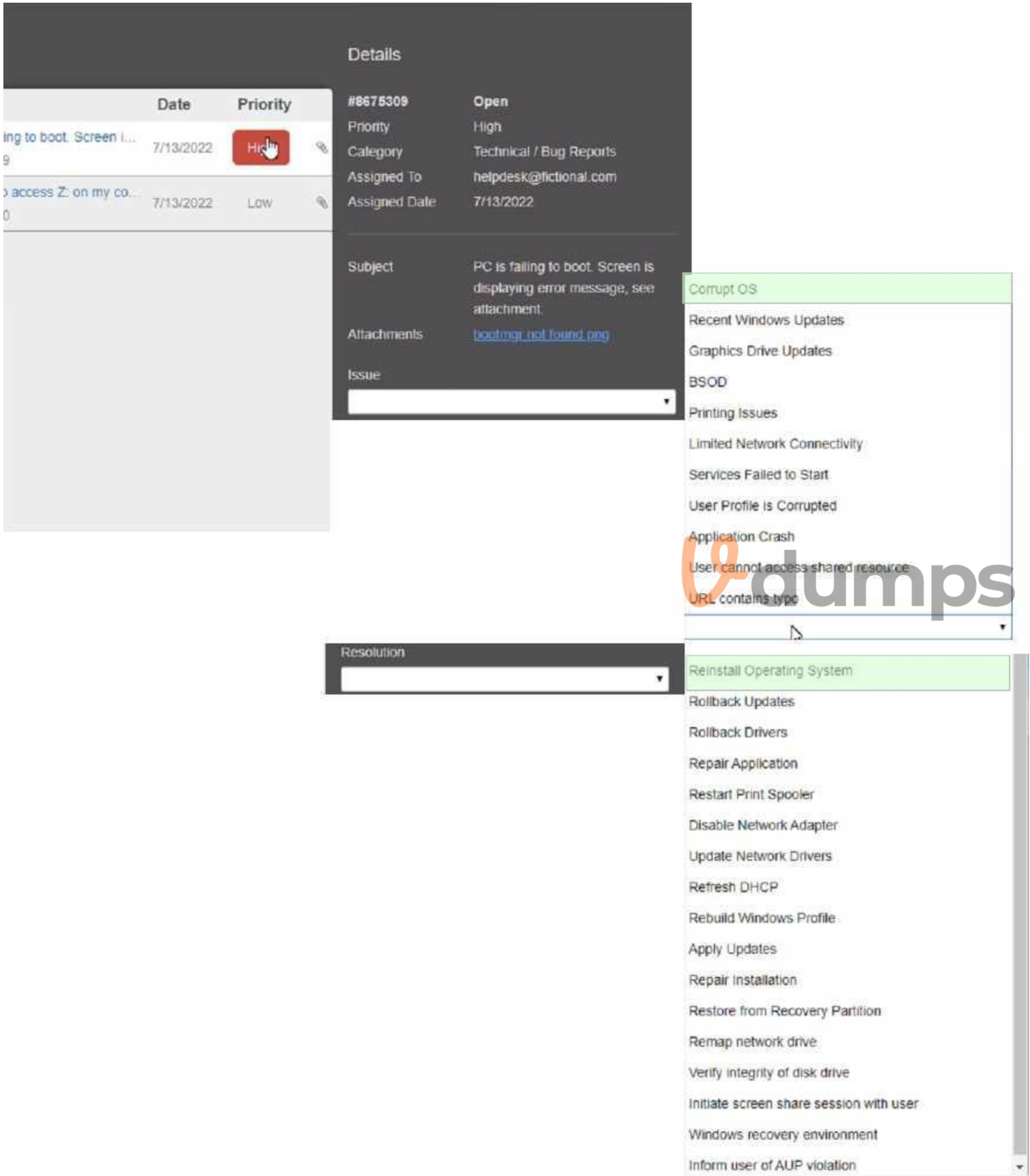

TEST QUESTION
Welcome to your first day as a Fictional Company, LLC helpdesk employee. Please work the tickets in your helpdesk ticket queue.
INSTRUCTIONS
Click on individual tickets to see the ticket details. View attachments to determine the problem.
Select the appropriate issue from the 'Issue' drop-down menu. Then, select the MOST efficient resolution from the 'Resolution' drop-down menu. Finally, select the proper command or verification to remediate or confirm your fix of the issue from the 'Verify/Resolve' drop-down menu.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.
Show Question
Reset All Answers
Details
Date
Priority
ing to boot. Screen i...
7/13/2022
High
o access Z: on my co...
7/13/2022
Low
No Ticket Selected
Please select a ticket from the list
Details
#8675309
Open
Priority
High
Category
Technical / Bug Reports
Assigned To
helpdesk@fictional.com
Assigned Date
7/13/2022
Subject
PC is failing to boot. Screen is displaying error message, see attachment.
Attachments
bootmgr not found.png
Issue
Resolution
Verify/Resolve


Details
Date
Priority
#8675309
Open
Priority
High
Category
Technical / Bug Reports
Assigned To
helpdesk@fictional.com
Assigned Date
7/13/2022
7/13/2022
Low
Subject
PC is failing to boot. Screen is displaying error message, see attachment
Attachments
bootmgr not found.png
Issue
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
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
Verify/Resolve
chkdsk
dism
diskpart
sfc
dd
ctrl + alt + del
net use
net user
netstat
netsh
bootrec

Hot Area:



Answer Area:



Section:
Explanation:
Answer: A
Explanation:

QUESTION 63
A user reports a computer is running slow. Which of the following tools will help a technician identity the issued

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 64
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 65
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 percentage123 Reference: 4. How to Increase the Text Size on Your Computer. Retrieved from https://www.laptopmag.com/articles/
increase-text-size-computer 5. How to Change the Size of Text in Windows 10. Retrieved from https://www.howtogeek.com/370055/how-to-change-the-size-of- text-in-windows-10/ 6. Change the size of text in Windows. Retrieved from
https://support.microsoft.com/en-us/windows/change-the-size-of-text-in-windows-1d5830c3-eee3- 8eaa-836b-abcc37d99b9a

QUESTION 66
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 externalthreats 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 67
Which of the following Linux commands would be used to install an application?

A. yum
B. grep
C. Is
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 toinstall applications because it requires administrative privileges1

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

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

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 69
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 imagethe user wants to use as the wallpaper1 https://www.lifewire.com/change-desktop-background-windows-11-5190733

QUESTION 70
A technician wants to enable BitLocker on a Windows 10 laptop and is unable to find the BitLocker Drive Encryption menu item in Control Panel. Which of the following explains why the technician unable to find this menu item?

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

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 71
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 OSupdates1. Antivirus software relies on the operating system to function properly. If the operatingsystem 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 72
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 73
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 74
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 75
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 76
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 77

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 78
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 beused to manage Android phones and enforce security policies such as password requirements, encryption, and remote wipe capabilities12

QUESTION 79
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 80
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. Theuser can right-click the file and select Properties. In the Properties dialog box, select the Hiddencheck box, and then click OK 1.

QUESTION 81
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 82
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 83
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 84
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 theprofile will create a new profile and transfer the user’s data to the new profile1

QUESTION 85
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 isan example of two-factor authentication (2FA)

QUESTION 86
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 87
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 leaving1

QUESTION 88
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 89
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 method1 A full backup only requires two sets of tapes to restore because it backs up all the data from theworkstation. 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 90
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 91
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 92
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 93
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. SOL 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 94
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 95
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 96
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 97

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 Explorercan be used to locate and delete files associated with the malicious software

QUESTION 98
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 99
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 method12An 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 100
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 101
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 resourcesand slowing down the phone. The user should uninstall the application and run a malware scan on the phone1

QUESTION 102
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 103
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 104
A technician is setting up a new laptop for an employee who travels, Which of the following is the BEST security practice for this scenario?

A. PIN-based login
B. Quarterly password changes
C. Hard drive encryption
D. A physical laptop lock

Correct Answer: C
Section:
Explanation:
Encrypting the laptop's hard drive will ensure that any sensitive data stored on the laptop is secure, even if the laptop is lost or stolen. Encryption ensures that the data cannot be accessed by anyone without the correct encryption key. This is an important security measure for any laptop used by an employee who travels, as it helps to protect the data stored on the laptop from unauthorized access.

QUESTION 105
A user in a corporate office reports the inability to connect to any network drives. No other users have reported this issue. Which of the following is the MOST likely reason the user is having this issue?

A. The user is not connected to the VPN.
B. The file server is offline.
C. A low battery is preventing the connection.
D. The log-in script failed.

Correct Answer: D
Section:

QUESTION 106
A user received the following error upon visiting a banking website:
The security presented by website was issued a different website' s address .
A technician should instruct the user to:

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

Correct Answer: A
Section:
Explanation:

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

QUESTION 107
A user is attempting to browse the internet using Internet Explorer. When trying to load a familiar web page, the user is unexpectedly redirected to an unfamiliar website. Which of the following would MOST likely solve the issue? (Choose Correct Answer and provide from Comptia A+ Core2 Study guide or manual from Comptia.org)

A. Updating the operating system
B. Changing proxy settings
C. Reinstalling the browser
D. Enabling port forwarding

Correct Answer: C
Section:
Explanation:
Reinstalling the browser would most likely solve the issue. This would remove any malicious software or add-ons that may be causing the issue and restore the browser to its default settings.

QUESTION 108
Which of the following is a consequence of end-of-lite operating systems?

A. Operating systems void the hardware warranty.
B. Operating systems cease to function.
C. Operating systems no longer receive updates.
D. Operating systems are unable to migrate data to the new operating system.

Correct Answer: C
Section:
Explanation:
End-of-life operating systems are those which have reached the end of their life cycle and are no longer supported by the software developer. This means that the operating system will no longer receive updates, security patches, or other new features. This can leave users vulnerable to security threats, as the system will no longer be protected against the latest threats. Additionally, this can make it difficult to migrate data to a newer operating system, as the old system is no longer supported.

QUESTION 109
Which of the following data is MOST likely to be regulated?

A. Name in a Phone book
B. Name on a medical diagnosis
C. Name on a job application
D. Name on a employer's website

Correct Answer: B
Section:

QUESTION 110
Which of the following file extensions are commonly used to install applications on a macOS machine? (Select THREE).

A. .mac
B. .Pkg
C. .deb
D. .dmg
E. .msi
F. .appx
G. .app
H. .apk

Correct Answer: B, D, G
Section:

QUESTION 111
A help desk technician runs the following script: Inventory.py. The technician receives the following error message:
How do you want to Open this file?
Which of the following is the MOST likely reason this script is unable to run?

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

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

QUESTION 112
A technician downloaded software from the Internet that required the technician to scroll through a text box and at the end of the text box, click a button labeled Accept Which of the following agreements IS MOST likely in use?

A. DRM
B. NDA
C. EULA
D. MOU

Correct Answer: C
Section:
Explanation:
The most likely agreement in use here is a EULA (End User License Agreement). This is a legally binding agreement between the user and the software developer, outlining the terms and conditions that the user must agree to in order to use the software. It is important that the user understands and agrees to the EULA before they can proceed with downloading and installing the software. As stated in the CompTIA A+ Core 2 exam objectives, users should be aware of the EULA before downloading any software.

QUESTION 113
A technician is reimaging a desktop PC. The technician connects the PC to the network and powers it on. The technician attempts to boot the computer via the NIC to image the computer, but this method does not work. Which of the following is the MOST likely reason the computer is unable to boot into the imaging system via the network?

A. The computer's CMOS battery failed.
B. The computer's NIC is faulty.
C. The PXE boot option has not been enabled
D. The Ethernet cable the technician is using to connect the desktop to the network is faulty.

Correct Answer: C
Section:
Explanation:
The most likely reason the computer is unable to boot into the imaging system via the network is that the PXE boot option has not been enabled. PXE (Preboot Execution Environment) is an environment that allows computers to boot up over the network, instead of from a local disk. In order for this to work, the PXE boot option must be enabled in the computer's BIOS settings. As stated in the CompTIA A+ Core 2 exam objectives, technicians should know how to enable PXE in BIOS to enable network booting on a computer.

QUESTION 114
A systems administrator is tasked with configuring desktop systems to use a new proxy server that the organization has added to provide content filtering. Which of the following Windows utilities IS the BEST choice for accessing the necessary configuration to complete this goal?

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

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

QUESTION 115
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 116
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 117
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 118
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 119
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 120
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 121
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 122
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 123
A technician is troubleshooting application crashes on a Windows workstation. Each time the workstation user tries to open a website in a browser, the following message is displayed:
crypt32.d11 is missing not found
Which of the following should the technician attempt FIRST?

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

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

QUESTION 124
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 125
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 126
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 resolved4.
Create a new Outlook profile. A profile is a set of settings and information that Outlook uses to manage your email accounts and data. Sometimes, a profile can get corrupted or damaged and cause Outlook to malfunction. To create a new profile, go to Control Panel > 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 resolved5.
Repair your Outlook data files. Data files are files that store your email messages, contacts, calendar events, and other items on your computer. Sometimes, data files can get corrupted or damaged and cause Outlook to malfunction. To repair your data files, you can use a tool called scanpst.exe, which is located in the same folder where Outlook is installed (usually C:\Program Files\Microsoft Office\root\Office16). To use scanpst.exe, close Outlook and locate the tool in the folder. Double-click on it and browse to the location of your data file (usually C:\Users\username\AppData\Local\Microsoft\Outlook). Select the file and click Start to begin the scanning and repairing process. When it's done, restart Outlook and check if the issue is resolved. Run the /resetnavpane command. The navigation pane is the panel on the left side of Outlook that shows your folders and accounts. Sometimes, the navigation pane can get corrupted or damaged and cause Outlook to malfunction. To reset the navigation pane, press Windows key + R to open the Run dialog box, or open the Command Prompt. Type outlook.exe /resetnavpane and hit Enter. This will clear and regenerate the navigation pane settings for Outlook. Restart Outlook and check if the issue is resolved.

QUESTION 127
Which of the following editions of Windows 10 requires reactivation every 180 days?

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

Correct Answer: A
Section:
Explanation:
Windows 10 Enterprise is an edition of Windows 10 that is designed for large organizations that need advanced security and management features. Windows 10 Enterprise can be activated using different methods, such as Multiple Activation Key (MAK), Active Directory-based Activation (ADBA), or Key Management Service (KMS)1. KMS is a method of activation that uses a local server to activate multiple devices on a network. KMS activations are valid for 180 days and need to be renewed periodically by connecting to the KMS server2. If a device does not renew its activation within 180 days, it will enter a grace period of 30 days, after which it will display a warning message and lose some functionality until it is reactivated3. The other editions of Windows 10 do not require reactivation every 180 days. Windows 10 Pro for Workstation is an edition of Windows 10 that is designed for high-performance devices that need advanced features such as ReFS file system, persistent memory, and faster file sharing. Windows 10 Pro for Workstation can be activated using a digital license or a product key. Windows 10 Home is an edition of Windows 10 that is designed for personal or home use. Windows 10 Home can be activated using a digital license or a product key. Windows 10 Pro is an edition of Windows 10 that is designed for business or professional use. Windows 10 Pro can be activated using a digital license or a product key. None of these editions require reactivation every 180 days unless there are significant hardware changes or other issues that affect the activation status.

QUESTION 128
Which of the following is the proper way for a technician to dispose of used printer consumables?

A. Proceed with the custom manufacturer's procedure.
B. Proceed with the disposal of consumables in standard trash receptacles.
C. Empty any residual ink or toner from consumables before disposing of them in a standard recycling bin.
D. Proceed with the disposal of consumables in standard recycling bins.

Correct Answer: A
Section:
Explanation:

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

QUESTION 129
A large company is selecting a new Windows operating system and needs to ensure it has built-in encryption and endpoint protection. Which of the following Windows versions will MOST likely be selected?

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

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

QUESTION 130
A user tries to access commonly used web pages but is redirected to unexpected websites. Clearing the web browser cache does not resolve the issue. Which of the following should a technician investigate NEXT to resolve the issue?

A. Enable firewall ACLs.
B. Examine the localhost file entries.
C. Verify the routing tables.
D. Update the antivirus definitions.

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

QUESTION 131
A network technician installed a SOHO router for a home office user. The user has read reports about home routers being targeted by malicious actors and then used in DDoS attacks. Which of the following can the technician MOST likely do to defend against this threat?

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

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

QUESTION 132
A technician is preparing to remediate a Trojan virus that was found on a workstation. Which of the following steps should the technician complete BEFORE removing the virus?

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

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

QUESTION 133
A new employee was hired recently. Which of the following documents will the new employee need to sign before being granted login access to the network?

A. MSDS
B. EULA
C. UAC
D. AUP

Correct Answer: D
Section:
Explanation:
A new employee will need to sign an AUP before being granted login access to the network. An AUP is an Acceptable Use Policy that defines the rules and guidelines for using network resources and services in an organization. An AUP typically covers topics such as security, privacy, ethics, compliance and liability issues related to network usage. An AUP helps protect the organization and its users from legal, regulatory and reputational risks associated with network activities. An MSDS is a Material Safety Data Sheet that provides information about hazardous substances and how to handle them safely. An MSDS is not related to network access or usage. A EULA is an End User License Agreement that specifies the terms and conditions for using a software product or service. A EULA is usually provided by software vendors or developers and does not apply to network access or usage in general. A UAC is a User Account Control that is a security feature that prompts users for permission or confirmation before performing certain actions that require elevated privileges or affect system settings. A UAC is not a document that needs to be signed by users but a mechanism that helps prevent unauthorized changes or malware infections on a system. Reference: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 5.1

QUESTION 134
A user lost a company tablet that was used for customer intake at a doctor's office. Which of the following actions would BEST protect against unauthorized access of the data?

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

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

QUESTION 135
Which of the following is used to explain issues that may occur during a change implementation?

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

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

QUESTION 136
Which of the following would MOST likely be deployed to enhance physical security for a building? (Select TWO).

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

Correct Answer: B, E
Section:
Explanation:
Badge reader and motion sensor are devices that can be deployed to enhance physical security for a building. A badge reader is a device that scans and verifies an identification card or tag that grants access to authorized

personnel only. A badge reader can help prevent unauthorized entry or intrusion into a building or a restricted area. A motion sensor is a device that detects movement and triggers an alarm or an action when motion is detected. A motion sensor can help deter or alert potential intruders or trespassers in a building or an area. Multifactor authentication is a method of verifying identity using two or more factors, such as something you know, something you have or something you are. Multifactor authentication is not a device that can be deployed to enhance physical security for a building but a technique that can be used to enhance logical security for systems or services. Personal identification number is a numeric code that can be used as part of authentication or access control. Personal identification number is not a device that can be deployed to enhance physical security for a building but an example of something you know factor in multifactor authentication. Firewall is a device or software that filters network traffic based on rules and policies. Firewall is not a device that can be deployed to enhance physical security for a building but a device that can be used to enhance network security for systems or services. Soft token is an application or software that generates one-time passwords or codes for authentication purposes. Soft token is not a device that can be deployed to enhance physical security for a building but an example of something you have factor in multifactor authentication. Reference: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 3.3

QUESTION 137
A technician is troubleshooting an issue with a computer that contains sensitive information. The technician determines the computer needs to be taken off site for repair. Which of the following should the technician do NEXT?

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

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

QUESTION 138
A technician needs to remotely connect to a Linux desktop to assist a user with troubleshooting. The technician needs to make use of a tool natively designed for Linux. Which of the following tools will the technician MOST likely use?

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

Correct Answer: A
Section:
Explanation:
The tool that the technician will most likely use to remotely connect to a Linux desktop is VNC. VNC stands for Virtual Network Computing and is a protocol that allows remote access and control of a graphical desktop environment over a network. VNC is natively designed for Linux and can also support other operating systems, such as Windows and Mac OS. VNC can be used to assist users with troubleshooting by viewing and interacting with their desktops remotely. MFA stands for Multi- Factor Authentication and is a method of verifying identity using two or more factors, such as something you know, something you have or something you are. MFA is not a tool that can be used to remotely connect to a Linux desktop but a technique that can be used to enhance security for systems or services. MSRA stands for Microsoft Remote Assistance and is a feature that allows remote access and control of a Windows desktop environment over a network. MSRA is not natively designed for Linux and may not be compatible or supported by Linux systems. RDP stands for Remote Desktop Protocol and is a protocol that allows remote access and control of a Windows desktop environment over a network. RDP is not natively designed for Linux and may not be compatible or supported by Linux systems. Reference: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.6

QUESTION 139

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

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

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

QUESTION 140
A user is trying to use a third-party USB adapter but is experiencing connection issues. Which of the following tools should the technician use to resolve this issue?

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

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

QUESTION 141
A technician, who is working at a local office, has found multiple copies of home edition software installed on computers. Which of the following does this MOST likely violate?

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

Correct Answer: A
Section:
Explanation:

The installation of home edition software on computers at a local office most likely violates the EULA. EULA stands for End User License Agreement and is a legal contract that specifies the terms and conditions for using a software product or service. EULA typically covers topics such as license scope, duration and limitations, rights and obligations of the parties, warranties and disclaimers, liability and indemnity clauses, and termination procedures. EULA may also restrict the use of home edition software to personal or non-commercial purposes only, and prohibit the use of home edition software in business or professional settings. Violating EULA may result in legal actions or penalties from the software vendor or developer. PII stands for Personally Identifiable Information and is any information that can be used to identify or locate an individual, such as name, address, phone number, email address, social security number or credit card number. PII is not related to software installation or licensing but to data protection and privacy. DRM stands for Digital Rights Management and is a technology that controls or restricts the access and use of digital content, such as music, movies, books or games. DRM is not related to software installation or licensing but to content distribution and piracy prevention. Open-source agreement is a type of license that allows users to access, modify and distribute the source code of a software product or service freely and openly. Open-source agreement does not restrict the use of software to home edition only but encourages collaboration and innovation among developers and users. Reference: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 5.1

QUESTION 142
A user reports that the pages flash on the screen two or three times before finally staying open when attempting to access banking web pages. Which of the following troubleshooting steps should the technician perform NEXT to resolve the issue?

A. Examine the antivirus logs.
B. Verify the address bar URL.
C. Test the internet connection speed.
D. Check the web service status.

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

QUESTION 143
A Windows user recently replaced a computer The user can access the public internet on the computer; however, an internal site at https7/companyintranet.com:8888 is no longer loading. Which of the following should a technician adjust to resolve the issue?

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

Correct Answer: D
Section:
Explanation:
The technician should adjust the firewall settings to resolve the issue of not being able to access an internal site at https://companyintranet.com:8888. The firewall settings control how the firewall filters and allows network traffic based on rules and policies. The firewall settings may be blocking or preventing the access to the internal site by mistake or by default, especially if the site uses a non- standard port number such as 8888. The technician should check and modify the firewall settings to allow the access to the internal site or its port number. Default gateway settings determine how a computer connects to other networks or the internet. Default gateway settings are not likely to cause the issue of not being able to access an internal site if the user can access the public internet. DHCP settings determine how a computer obtains its IP address and other network configuration parameters automatically from a DHCP server. DHCP settings are not likely to cause the issue of not being able to access an internal site if the user can access other network resources. IP address settings determine how a computer identifies itself and communicates with other devices on a network. IP address settings are not likely to cause the issue of not being able to access an internal site if the user can access other network resources. Antivirus settings control how the antivirus software scans and protects the computer from malware and threats. Antivirus settings are less likely to cause the issue of not being able to access an internal site than firewall settings, unless the antivirus software has its own firewall feature that may interfere with the network traffic. Reference:
CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.6

QUESTION 144
A technician is securing a new Windows 10 workstation and wants to enable a Screensaver lock. Which of the following options in the Windows settings should the technician use?

A. Ease of Access
B. Privacy
C. Personalization
D. Update and Security

Correct Answer: C
Section:
Explanation:
The technician should use the Personalization option in the Windows settings to enable a Screensaver lock. The Personalization option allows users to customize the appearance and behavior of their desktop, such as themes, colors, backgrounds, lock screen and screensaver. The technician can enable a Screensaver lock by choosing a screensaver from the drop-down menu, setting a wait time in minutes and checking the box that says “On resume, display logon screen”. This will lock the computer and require a password or PIN to log back in after the screensaver is activated. Ease of Access is an option in the Windows settings that allows users to adjust accessibility features and settings, such as narrator, magnifier, high contrast and keyboard shortcuts. Ease of Access is not related to enabling a Screensaver lock. Privacy is an option in the Windows settings that allows users to manage privacy and security settings, such as location, camera, microphone and app permissions. Privacy is not related to enabling a Screensaver lock. Update and Security is an option in the Windows settings that allows users to check and install updates, troubleshoot problems, backup files and restore system. Update and Security is not related to enabling a Screensaver lock. Reference:
CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.7

QUESTION 145
A user calls the help desk to report that mapped drives are no longer accessible. The technician verifies that clicking on any of the drives on the user's machine results in an error message. Other users in the office are not having any issues. As a first step, the technician would like to remove and attempt to reconnect the drives. Which of the following command-line tools should the technician use?

A. net use
B. set
C. mkdir
D. rename

Correct Answer: A
Section:
Explanation:
The technician should use net use command-line tool to remove and reconnect mapped drives. Net use is a command that allows users to manage network connections and resources, such as shared folders or printers. Net use can be used to map or unmap network drives by specifying their drive letters and network paths. For example, net use Z: \server\share maps drive Z: to \server\share folder, and net use Z: /delete unmaps drive Z:. Set is a command that displays or modifies environment variables for the current user or process. Set is not related to managing mapped drives. Mkdir is a command that creates a new directory or folder in the current or specified location. Mkdir is not related to managing mapped drives. Rename is a command that renames a file or folder in the current or specified location. Rename is not related to managing mapped drives. Reference:
CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.6

QUESTION 146
A user has been unable to receive emails or browse the internet from a smartphone while traveling. However, text messages and phone calls are working without issue. Which of the following should a support technician check FIRST?

A. User account status
B. Mobile OS version
C. Data plan coverage
D. Network traffic outages

Correct Answer: C
Section:
Explanation:
The first thing that a support technician should check to resolve the issue of not being able to receive emails or browse the internet from a smartphone while traveling is the data plan coverage. The data plan coverage

determines how much data and where the user can use on the smartphone's cellular network. The data plan coverage may vary depending on the user's location, carrier and subscription. The data plan coverage may not include or support certain areas or countries that the user is traveling to, or may charge extra fees or limit the speed or amount of data that the user can use. The data plan coverage does not affect text messages and phone calls, which use different network services and protocols. User account status is not likely to cause the issue of not being able to receive emails or browse the internet from a smartphone while traveling, unless the user account has been suspended or terminated by the carrier or the email provider. Mobile OS version is not likely to cause the issue of not being able to receive emails or browse the internet from a smartphone while traveling, unless the mobile OS has a major bug or compatibility problem with the network or the email app. Network traffic outages may cause the issue of not being able to receive emails or browse the internet from a smartphone while traveling, but they are less likely and less common than data plan coverage issues, and they should also affect text messages and phone calls.
Reference: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.5

QUESTION 147
Which of the following script types is used with the Python language by default?

A. .ps1
B. .vbs
C. .bat
D. .py

Correct Answer: D
Section:
Explanation:
The script type that is used with the Python language by default is .py. .py is a file extension that indicates a Python script file that contains Python code that can be executed by a Python interpreter or compiler. Python is a high-level, general-purpose and interpreted programming language that can be used for various applications, such as web development, data analysis, machine learning and automation. .ps1 is a file extension that indicates a PowerShell script file that contains PowerShell code that can be executed by a PowerShell interpreter or compiler. PowerShell is a task-based, command-line and scripting language that can be used for system administration and automation on Windows systems. .vbs is a file extension that indicates a VBScript file that contains VBScript code that can be executed by a VBScript interpreter or compiler. VBScript is an Active Scripting language that can be used for web development and automation on Windows systems. .bat is a file extension that indicates a batch file that contains a series of commands that can be executed by a command- line interpreter or shell on Windows systems. Batch files can be used for system administration and automation on Windows systems. Reference: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 4.3

QUESTION 148
A user added a second monitor and wants to extend the display to it. In which of the following Windows settings will the user MOST likely be able to make this change?

A. System
B. Devices
C. Personalization
D. Accessibility

Correct Answer: A
Section:
Explanation:
The user can most likely make the change of extending the display to a second monitor in the System option in the Windows settings. The System option allows users to manage system settings and features, such as display, sound, notifications, power and storage. The user can extend the display to a second monitor by selecting Display from the System option and then choosing Extend these displays from the Multiple displays drop-down menu. This will allow the user to use both monitors as one large desktop area. Devices is an option in the Windows settings that allows users to add and manage devices connected to the computer, such as printers, scanners, mice and keyboards. Devices is not related to extending the display to a second monitor but to configuring device settings and preferences. Personalization is an option in the Windows settings that allows users to customize the appearance and behavior of their desktop, such as themes, colors, backgrounds, lock screen and screensaver.

QUESTION 149
Which of the following only has a web browser interface?

A. Linux
B. Microsoft Windows

C. iOS
D. Chromium

Correct Answer: D
Section:
Explanation:
Chromium is an operating system that only has a web browser interface. Chromium is an open- source project that provides the source code and framework for Chrome OS, which is a Linux-based operating system developed by Google. Chromium and Chrome OS are designed to run web applications and cloud services through the Chrome web browser, which is the only user interface available on the system. Chromium and Chrome OS are mainly used on devices such as Chromebooks, Chromeboxes and Chromebits. Linux is an operating system that does not only have a web browser interface but also a graphical user interface and a command-line interface. Linux is an open-source and customizable operating system that can run various applications and services on different devices and platforms. Linux can also support different web browsers, such as Firefox, Opera and Chromium. Microsoft Windows is an operating system that does not only have a web browser interface but also a graphical user interface and a command-line interface. Microsoft Windows is a proprietary and popular operating system that can run various applications and services on different devices and platforms. Microsoft Windows can also support different web browsers, such as Edge, Internet Explorer and Chrome. iOS is an operating system that does not only have a web browser interface but also a graphical user interface and a voice-based interface. iOS is a proprietary and mobile operating system developed by Apple that can run various applications and services on devices such as iPhone, iPad and iPod Touch. iOS can also support different web browsers, such as Safari, Firefox and Chrome. Reference: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.1

QUESTION 150
A kiosk, which is running Microsoft Windows 10, relies exclusively on a numeric keypad to allow customers to enter their ticket numbers but no other information. If the kiosk is idle for four hours, the login screen locks. Which of the following sign-on options would allow any employee the ability to unlock the kiosk?

A. Requiring employees to enter their usernames and passwords
B. Setting up facial recognition for each employee
C. Using a PIN and providing it to employees
D. Requiring employees to use their fingerprints

Correct Answer: C
Section:
Explanation:
The best sign-on option that would allow any employee the ability to unlock the kiosk that relies exclusively on a numeric keypad is to use a PIN and provide it to employees. A PIN is a Personal Identification Number that is a numeric code that can be used as part of authentication or access control. A PIN can be entered using only a numeric keypad and can be easily shared with employees who need to unlock the kiosk. Requiring employees to enter their usernames and passwords may not be feasible or convenient if the kiosk only has a numeric keypad and no other input devices. Setting up facial recognition for each employee may not be possible or secure if the kiosk does not have a camera or biometric sensor. Requiring employees to use their fingerprints may not be possible or secure if the kiosk does not have a fingerprint scanner or biometric sensor. Reference: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 3.3

QUESTION 151
A user calls the help desk to report that Windows installed updates on a laptop and rebooted overnight. When the laptop started up again, the touchpad was no longer working. The technician thinks the software that controls the touchpad might be the issue. Which of the following tools should the technician use to make adjustments?

A. eventvwr.msc
B. perfmon.msc
C. gpedic.msc
D. devmgmt.msc

Correct Answer: D
Section:
Explanation:
The technician should use devmgmt.msc tool to make adjustments for the touchpad issue after Windows installed updates on a laptop. Devmgmt.msc is a command that opens the Device Manager, which is a utility that allows users to view and manage the hardware devices and drivers installed on a computer. The technician can use the Device Manager to check the status, properties and compatibility of the touchpad device and its driver, and perform actions such as updating, uninstalling or reinstalling the driver, enabling or disabling the device, or scanning for hardware changes. Eventvwr.msc is a command that opens the Event Viewer, which is a utility that

allows users to view and monitor the system logs and events. The Event Viewer may provide some information or clues about the touchpad issue, but it does not allow users to manage or troubleshoot the device or its driver directly. Perfmon.msc is a command that opens the Performance Monitor, which is a utility that allows users to measure and analyze the performance of the system

QUESTION 152
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 the system is utilizing a 32-bit OS. A 32-bit OS is an operating system that uses 32 bits to address memory locations and perform calculations. A 32-bit OS can only support up to 4GB of RAM, and some of that RAM may be reserved for hardware devices or system functions, leaving less than 4GB of usable RAM for applications and processes. A 32-bit OS cannot recognize or utilize more than 4GB of RAM, even if more RAM is installed on the system. To utilize all the available RAM, the system needs to use a 64- bit OS, which can support much more RAM than a 32-bit OS. The system missing updates may cause some performance or compatibility issues, but it does not affect the amount of usable RAM on the system. The system's memory failing may cause some errors or crashes, but it does not affect the amount of usable RAM on the system. The system requiring BIOS updates may cause some configuration or compatibility issues, but it does not affect the amount of usable RAM on the system.
Reference: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.1

QUESTION 153
A Windows workstation that was recently updated with approved system patches shut down instead of restarting. Upon reboot, the technician notices an alert stating the workstation has malware in the root OS folder. The technician promptly performs a System Restore and reboots the workstation, but the malware is still detected. Which of the following BEST describes why the system still has malware?

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

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

QUESTION 154
Which of the following is the default GUI and file manager in macOS?

A. Disk Utility
B. Finder
C. Dock
D. FileVault

Correct Answer: B
Section:
Explanation:
Finder is the default GUI and file manager in macOS. Finder is an application that allows users to access and manage files and folders on their Mac computers. Finder also provides features such as Quick Look, Spotlight, AirDrop and iCloud Drive. Finder uses a graphical user interface that consists of icons, menus, toolbars and windows to display and interact with files and folders. Disk Utility is a utility that allows users to view and manage disk drives and partitions on their Mac computers. Disk Utility is not a GUI or a file manager but a disk management tool. Dock is a feature that allows users to access and launch applications on their Mac computers. Dock is not a GUI or a file manager but an application launcher. FileVault is a feature that allows users to encrypt and protect their data on their Mac computers. FileVault is not a GUI or a file manager but an encryption tool.
Reference: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.1

QUESTION 155
A technician needs to add an individual as a local administrator on a Windows home PC. Which of the following utilities would the technician MOST likely use?

A. Settings > Personalization
B. Control Panel > Credential Manager
C. Settings > Accounts > Family and Other Users
D. Control Panel > Network and Sharing Center

Correct Answer: C
Section:
Explanation:
The technician would most likely use Settings > Accounts > Family and Other Users to add an individual as a local administrator on a Windows home PC. Settings > Accounts > Family and Other Users allows users to add and manage other user accounts on their Windows PC. The technician can add an individual as a local administrator by selecting Add someone else to this PC under Other users and following the steps to create a new user account with administrator privileges. Settings > Personalization allows users to customize the appearance and behavior of their desktop, such as themes, colors, backgrounds, lock screen and screensaver. Settings > Personalization is not related to adding an individual as a local administrator on a Windows home PC but to configuring desktop settings and preferences. Control Panel > Credential Manager allows users to view and manage their web credentials and Windows credentials stored on their Windows PC. Control Panel > Credential Manager is not related to adding

QUESTION 156
Which of the following features allows a technician to configure policies in a Windows 10 Professional desktop?

A. gpedit
B. gpmc
C. gpresult
D. gpupdate

Correct Answer: A
Section:
Explanation:
The feature that allows a technician to configure policies in a Windows 10 Professional desktop is gpedit. Gpedit is a command that opens the Local Group Policy Editor, which is a utility that allows users to view and modify local group policies on their Windows PC. Local group policies are a set of rules and settings that control the behavior and configuration of the system and its users. Local group policies can be used to configure policies such as security, network, software installation and user rights. Gpmc is a command that opens the Group Policy Management Console, which is a utility that allows users to view and modify domain-based group policies on a Windows Server. Domain-based group policies are a set of rules and settings that control the behavior and configuration of the computers and users in a domain. Domain-based group policies are not available on a Windows 10 Professional desktop. Gpresult is a command that displays the result of applying group policies on a Windows PC. Gpresult can be used to troubleshoot or verify group policy settings but not to configure them. Gpupdate is a command that updates or refreshes the group policy settings on a Windows PC. Gpupdate can be used to apply new or changed group policy settings but not to configure them. Reference: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.6

QUESTION 157
Which of the following defines the extent of a change?

A. Scope
B. Purpose
C. Analysis
D. Impact

Correct Answer: A
Section:
Explanation:
The term that defines the extent of a change is scope. Scope is a measure of the size, scale and boundaries of a project or an activity. Scope defines what is included and excluded in the project or activity, such as goals, requirements, deliverables, tasks and resources. Scope helps determine the feasibility, duration and cost of the project or activity. Scope also helps manage the expectations and needs of the stakeholders involved in the project or activity. Purpose is the reason or objective for doing a project or an activity. Purpose defines why the project or activity is important or necessary, such as solving a problem, meeting a need or achieving a goal. Purpose helps provide direction, motivation and justification for the project or activity. Analysis is the process of examining, evaluating and interpreting data or information related to a project or an activity. Analysis helps identify, understand and prioritize issues, risks, opportunities and solutions for the project or activity. Impact is the effect or outcome of a project or an activity on something or someone else. Impact defines how the project or activity affects or influences other factors, such as performance, quality, satisfaction or value. Impact helps measure the success and effectiveness of the project or activity.
Reference: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 5.2

QUESTION 158
Which of the following filesystem formats would be the BEST choice to ensure read and write compatibility of USB flash drives across several generations of Microsoft operating systems?

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

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

QUESTION 159
A technician is troubleshooting a mobile device that was dropped. The technician finds that the screen (ails to rotate, even though the settings are correctly applied. Which of the following pieces of hardware should the technician replace to resolve the issue?

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

Correct Answer: C
Section:
Explanation:
The piece of hardware that the technician should replace to resolve the issue of the screen failing to rotate on a mobile device that was dropped is the accelerometer. The accelerometer is a sensor that detects the orientation and movement of the mobile device by measuring the acceleration forces acting on it. The accelerometer allows the screen to rotate automatically according to the position and angle of the device. If the accelerometer is

damaged or malfunctioning, the screen may not rotate properly or at all, even if the settings are correctly applied. LCD stands for Liquid Crystal Display and is a type of display that uses liquid crystals and backlight to produce images on the screen. LCD is not related to the screen rotation feature but to the quality and brightness of the display. Battery is a component that provides power to the mobile device by storing and releasing electrical energy. Battery is not related to the screen rotation feature but to the battery life and performance of the device. Digitizer is a component that converts touch inputs into digital signals that can be processed by the mobile device. Digitizer is not related to the screen rotation feature but to the touch sensitivity and accuracy of the display. Reference: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.5

QUESTION 160
A technician downloads a validated security tool and notes the vendor hash of a58e87a2. When the download is complete, the technician again validates the hash, but the value returns as 2a876a7d3. Which of the following is the MOST likely cause of the issue?

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

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

QUESTION 161
An implementation specialist is replacing a legacy system at a vendor site that has only one wireless network available. When the specialist connects to Wi-Fi. the specialist realizes the insecure network has open authentication. The technician needs to secure the vendor's sensitive dat a. Which of the following should the specialist do FIRST to protect the company's data?

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

Correct Answer: B
Section:
Explanation:
The first thing that the specialist should do to protect the company's data on an insecure network with open authentication is to connect to the vendor's network using a VPN. A VPN stands for Virtual Private Network and is a technology that creates a secure and encrypted connection over a public or untrusted network. A VPN can protect the company's data by preventing eavesdropping, interception or modification of the network traffic by unauthorized parties. A VPN can also provide access to the company's internal network and resources remotely. Manually configuring an IP address, a subnet mask and a default gateway may not be necessary or possible if the vendor's network uses DHCP to assign network configuration parameters automatically. Manually configuring an IP address, a subnet mask and a default gateway does not protect the company's data from network attacks or threats. Changing the network location to private may not be advisable or effective if the vendor's network is a public or untrusted network. Changing the network location to private does not protect the company's data from network attacks or threats. Configuring MFA on the network may not be feasible or sufficient if the vendor's network has open authentication and does not support or require MFA. Configuring MFA on the network does not protect the company's data from network attacks or threats. Reference: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 3.3

QUESTION 162
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 163
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 164
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 165
After a failed update, an application no longer launches and generates the following error message:
Application needs to be repaired. Which of the following Windows 10 utilities should a technician use to address this concern?

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

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

QUESTION 166
A technician receives a call (rom a user who is having issues with an application. To best understand the issue, the technician simultaneously views the user's screen with the user. Which of the following would BEST accomplish this task?

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

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

QUESTION 167
A computer on a corporate network has a malware infection. Which of the following would be the BEST method for returning the computer to service?

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

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

QUESTION 168
A technician needs to access a Windows 10 desktop on the network in a SOHO using RDP. Although the connection is unsuccessful, the technician is able to ping the computer successfully. Which of the following is MOST likely preventing the connection?

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

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

QUESTION 169
Which of the following often uses an SMS or third-party application as a secondary method to access a system?

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

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

QUESTION 170
A company needs employees who work remotely to have secure access to the corporate intranet. Which of the following should the company implement?

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

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

QUESTION 171
A Windows computer is experiencing slow performance when the user tries to open programs and files. The user recently installed a new software program from an external website.
Various websites are being redirected to an unauthorized site, and Task Manager shows the CPU usage is consistently at 100%. Which of the following should the technician do first?

A. Uninstall the new program.
B. Check the HOSTS file.
C. Restore from a previous backup.
D. Clear the web browser cache.

Correct Answer: A
Section:
Explanation:
The symptoms that the user's Windows computer is experiencing suggest that the new software program that the user installed from an external website may be malicious or incompatible with the system. The program may be consuming a lot of CPU resources, slowing down the performance of other programs and files. The program may also be altering the browser settings or the HOSTS file, causing the web redirection to an unauthorized site. The first step that the technician should do is to uninstall the new program from the Control Panel or the Settings app, and then restart the computer. This may resolve the issue and restore the normal functionality of the computer.If the problem persists, the technician may need to perform additional steps, such as scanning for malware, checking the HOSTS file, clearing the web browser cache, or restoring from a previous backup

QUESTION 172
Which of the following should be documented to ensure that the change management plan is followed?

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

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

QUESTION 173
Which of the following combinations meets the requirements for mobile device multifactor authentication?

A. Password and PIN
B. Password and swipe
C. Fingerprint and password
D. Swipe and PIN

Correct Answer: C
Section:
Explanation:
Mobile device multifactor authentication (MFA) is a method of verifying a user's identity by requiring two or more factors, such as something the user knows (e.g., password, PIN, security question), something the user has (e.g., smartphone, OTP app, security key), or something the user is (e.g., fingerprint, face, iris)12. The combination of fingerprint and password meets the requirements for mobile device MFA because it uses two different factors: something the user is (fingerprint) and something the user knows (password). The other combinations do not meet the requirements because they use only one factor: something the user knows (password or PIN) or something the user does (swipe).
Reference 1: Set up the Microsoft Authenticator app as your verification method 2: What is Multi-Factor Authentication (MFA)? | OneLogin

QUESTION 174
Which of the following Windows 10 editions is the most appropriate for a single user who wants to encrypt a hard drive with BitLocker?

A. Professional
B. Home
C. Enterprise
D. Embedded

Correct Answer: A
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 is available on supported devices running Windows 10 or 11 Pro, Enterprise, or Education2.Windows 10 Home does not support BitLocker3, and Windows 10 Embedded is designed for specialized devices and does not offer BitLocker as a feature4. Therefore, the most appropriate Windows 10 edition for a single user who wants to encrypt a hard drive with BitLocker is Professional.
Reference 1: BitLocker overview - Windows Security | Microsoft Learn 2: Device encryption in Windows - Microsoft Support 3: Can You Turn on BitLocker on Windows 10 Home? 4: How to enable device encryption on Windows 10 Home

QUESTION 175
An employee has repeatedly contacted a technician about malware infecting a work computer. The technician has removed the malware several times, but the user's PC keeps getting infected. Which of the following should the technician do to reduce the risk of future infections?

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

Correct Answer: C
Section:
Explanation:
Malware is software that infects computer systems to damage, disable or exploit the computer or network for various malicious purposes5.Malware is typically distributed via email attachments, fake internet ads, infected applications or websites, and often relies on user interaction to execute6.Therefore, one of the most effective ways to prevent malware infections is to educate the end user about the common signs and sources of malware, and how to avoid them7. Configuring the firewall, restoring the system from backups, and updating the antivirus program are also important security measures, but they do not address the root cause of the user's repeated infections, which is likely due to a lack of awareness or caution.
Reference 5: Malware: what it is, how it works, and how to stop it - Norton 6: How to Prevent Malware: 15 Best Practices for Malware Prevention 7: 10 Security Tips for How to Prevent Malware Infections - Netwrix

QUESTION 176
A remote user's smartphone is performing very slowly. The user notices that the performance improves slightly after rebooting but then reverts back to performing slowly. The user also notices that the phone does not get any faster after connecting to the company's corporate guest network. A technician sees that the phone has a large number of applications installed on it. Which of the following is the most likely cause of the issue?

A. The user is in a poor signal area.
B. The user has too many processes running.
C. The smartphone has malware on it.
D. The smartphone has been jailbroken.

Correct Answer: B
Section:
Explanation:
One of the common reasons for a slow smartphone performance is having too many apps installed and running in the background. These apps consume the device's memory (RAM) and CPU resources, which can affect the speed and responsiveness of the phone. Rebooting the phone can temporarily clear the RAM and stop some background processes, but they may resume after a while. Connecting to a different network does not affect the performance of the phone, unless the network is congested or has a poor signal.The user can improve the phone's performance by uninstalling unused apps, clearing app caches, and restricting background activities12.Malware can also slow down a phone, but it is not the most likely cause in this scenario, as the user does not report any other symptoms of infection, such as pop-ups, battery drain, or data usage spikes3. Jailbreaking a phone can also affect its performance, but it is not a cause, rather a consequence, of the user's actions.Jailbreaking is the process of removing the manufacturer's restrictions on a phone, which allows the user to install unauthorized apps, customize the system, and access root privileges4.However, jailbreaking also exposes the phone to security risks, voids the warranty, and may cause instability or compatibility issues5.
Reference 1: Speed up a slow Android device - Android Help - Google Help 2: Why your phone slows down over time and what you can do to stop it | TechRadar 3: How to tell if your phone has a virus | Norton 4: What is Jailbreaking?- Definition from Techopedia 5: What is Jailbreaking an iPhone? - Lifewire

QUESTION 177
A technician is creating a location on a Windows workstation for a customer to store meeting minutes. Which of the following commands should the technician use?

A. c: \minutes
B. dir
C. rmdir
D. md

Correct Answer: D
Section:
Explanation:
The commandmdstands formake directoryand is used to create a new directory or folder in the current location. In this case, the technician can usemd minutesto create a folder named minutes in the C: drive. The other commands are not relevant for this task.c: \minutesis not a command but a path to a folder.diris used to display a list of files and folders in the current directory.rmdiris used to remove or delete an existing directory or folder.