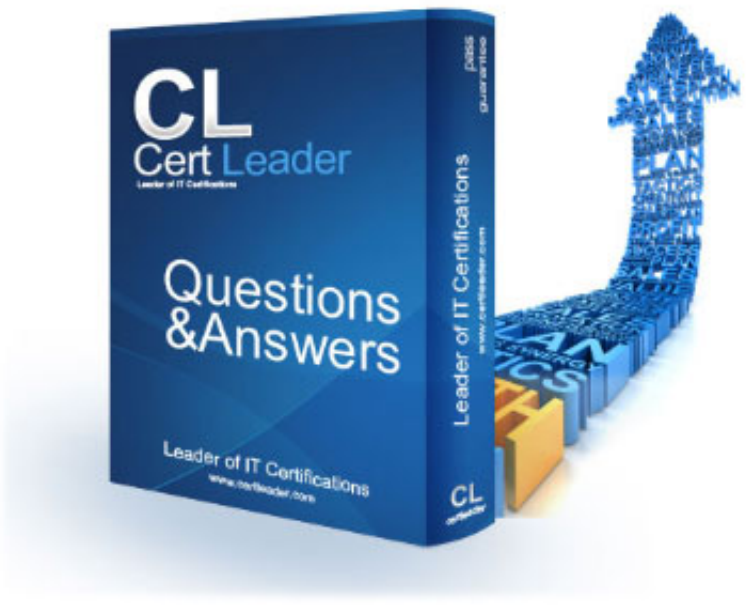
220-1102 Dumps

CompTIA A+ Certification Exam: Core 2

https://www.certleader.com/220-1102-dumps.html



NEW QUESTION 1
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

Answer: C

Explanation:
Badge readers are used to implement secure physical access to a data center. They are used to read the identification information on an employee's badge and grant access to the data center if the employee is 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.

NEW QUESTION 2
A macOS user reports seeing a spinning round cursor on a program that appears to be frozen. Which of the following methods does the technician use to force the program to close in macOS?

A. The technician presses the Ctrl+Alt+Del keys to open the Force Quit menu, selects the frozen application in the list, and clicks Force Quit.
B. The technician clicks on the frozen application and presses and holds the Esc key on the keyboard for 10 seconds Which causes the application to force quit.
C. The technician opens Finder, navigates to the Applications folder, locates the application that is frozen in the list, right-clicks on the application, and selects the Force Quit option.
D. The technician opens the Apple icon menu, selects Force Quit, selects the frozen application in the list, and clicks Force Quit.

Answer: D

Explanation:
The technician opens the Apple icon menu, selects Force Quit, selects the frozen application in the list, and clicks Force Quit. This is the most common method of force quitting a program in macOS. This can be done by clicking on the Apple icon in the top left of the screen, selecting Force Quit, selecting the frozen application in the list, and then clicking Force Quit. This will force the application to quit and the spinning round cursor will disappear.

NEW QUESTION 3
A company installed a new backup and recovery system. Which of the following types of backups should be completed FIRST?

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

Answer: A

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

NEW QUESTION 4
A wireless network is set up, but it is experiencing some interference from other nearby SSIDs. Which of the following can BEST resolve the interference?

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

Answer: A

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

NEW QUESTION 5
Upon downloading a new ISO, an administrator is presented with the following string: 59d15a16ce90cBcc97fa7c211b767aB
Which of the following BEST describes the purpose of this string?

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

Answer: C

Explanation:

Hash verification is a process that verifies the integrity of a file by comparing the hash value of the downloaded file to the hash value provided by the source1

NEW QUESTION 6
A call center technician receives a call from a user asking how to update Windows Which of the following describes what the technician should do?

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

Answer: C

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

NEW QUESTION 7
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.

Answer: C

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.

NEW QUESTION 8
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.

Answer: D

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.

NEW QUESTION 9
Which of the following OS types provides a lightweight option for workstations thai need an easy-to-use browser-based interface?

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

Answer: B

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

NEW QUESTION 10
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

Answer: C

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.

NEW QUESTION 10
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

Answer: D

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.

NEW QUESTION 13
A new service desk is having a difficult time managing the volume of requests. Which of the following is the BEST solution for the department?

A. Implementing a support portal
B. Creating a ticketing system
C. Commissioning an automated callback system
D. Submitting tickets through email

Answer: A

Explanation:
A support portal is an online system that allows customers to access customer service tools, submit requests and view status updates, as well as access information such as how-to guides, FAQs, and other self-service resources. This would be the best solution for the service desk, as it would allow them to easily manage the volume of requests by allowing customers to submit their own requests and view the status of their requests. Additionally, the portal would provide customers with self-service resources that can help them resolve their own issues, reducing the amount of tickets that need to be handled by the service desk.

NEW QUESTION 18
A technician has been tasked with using the fastest and most secure method of logging in to laptops. Which of the following log-in options meets these requirements?

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

Answer: A

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

NEW QUESTION 19
A technician is replacing the processor in a desktop computer prior to opening the computer, the technician wants to ensure the internal components are protected. Which of the following safety procedures would BEST protect the components in the PC? (Select TWO).

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

Answer: AC

Explanation:
The two safety procedures that would best protect the components in the PC are:
- Utilizing an ESD strap
- Placing the PSU in an antistatic bag

https://www.professormesser.com/free-a-plus-training/220-902/computer-safety-procedures-2/ https://www.skillsoft.com/course/comptia-a-core-2-safety-procedures-environmental-impacts-cbdf0f2c-61c0-4f

NEW QUESTION 24
A user contacted the help desk to report pop-ups on a company workstation indicating the computer has been infected with 137 viruses and payment is needed to remove them. The user thought the company-provided antivirus software would prevent this issue. The help desk ticket states that the user only receives these messages when first opening the web browser. Which of the following steps would MOST likely resolve the issue? (Select TWO)

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

F. Perform a reset on the user's web browser

Answer: CF

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

NEW QUESTION 27
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

Answer: B

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 vulnerability

Configuring AAA Services. Retrieved from https://www.cisco.com/c/en/us/td/docs/routers/crs/software/crs_r4-0/security/configuration/guide/sc40crsb

NEW QUESTION 29
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.

Answer: B

Explanation:
The most likely cause of this issue is that a router was misconfigured and was blocking traffic. This would explain why remote users who were not connected to corporate resources did not have any issues.

NEW QUESTION 34
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

Answer: C

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.

NEW QUESTION 39
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

Answer: C

Explanation:
The administrator can use Virtual Network Computing (VNC) to troubleshoot the server effectively. VNC is a graphical desktop sharing system that allows the administrator to remotely control the desktop of a Linux
server.

NEW QUESTION 43
The web browsing speed on a customer's mobile phone slows down every few weeks and then returns to normal after three or four days. Restarting the device does not usually restore performance. Which of the following should a technician check FIRST to troubleshoot this issue?

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

Answer: B

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

NEW QUESTION 48
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.

Answer: B

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.

NEW QUESTION 51
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

Answer: B

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

NEW QUESTION 56
An administrator has submitted a change request for an upcoming server deployment. Which of the following must be completed before the change can be approved?

A. Risk analysis
B. Sandbox testing
C. End user acceptance
D. Lessons learned

Answer: A

Explanation:
A risk analysis must be completed before a change request for an upcoming server deployment can be approved 1
Risk analysis is an important step in the change management process because it helps identify and mitigate potential risks before changes are implemented. Once the risks have been analyzed and the appropriate measures have been taken to minimize them, the change can be approved and implemented.

NEW QUESTION 61
A technician has been asked to set up a new wireless router with the best possible security. Which of the following should the technician implement?

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

Answer: C

Explanation:
WPA3 (Wi-Fi Protected Access version 3) is the latest version of Wi-Fi security and offers the highest level of protection available. It is designed to protect against brute force password attempts and protect against eavesdropping and man-in-the-middle attacks. WPA3 also supports the use of stronger encryption algorithms, such as the Advanced Encryption Standard (AES), which provides additional protection for wireless networks. WPA3 should be implemented in order to ensure the best possible security for the new wireless router.

NEW QUESTION 65
Which of the following Wi-Fi protocols is the MOST secure?

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

Answer: A

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

NEW QUESTION 68
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.

Answer: D

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.

NEW QUESTION 71
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

Answer: AB

Explanation:
The user can use the following commands to give the technician the correct information: ipconfig
/all and hostna1m.e
The ipconfig /all command displays the IP address, subnet mask, and default gateway
all adapters on the computer 1. The hostname command displays the name of the comp1u. ter

NEW QUESTION 74
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

Answer: C

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

NEW QUESTION 76
A user reports a PC is running slowly. The technician suspects high disk I/O. Which of the following should the technician perform NEXT?

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

Answer: A

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

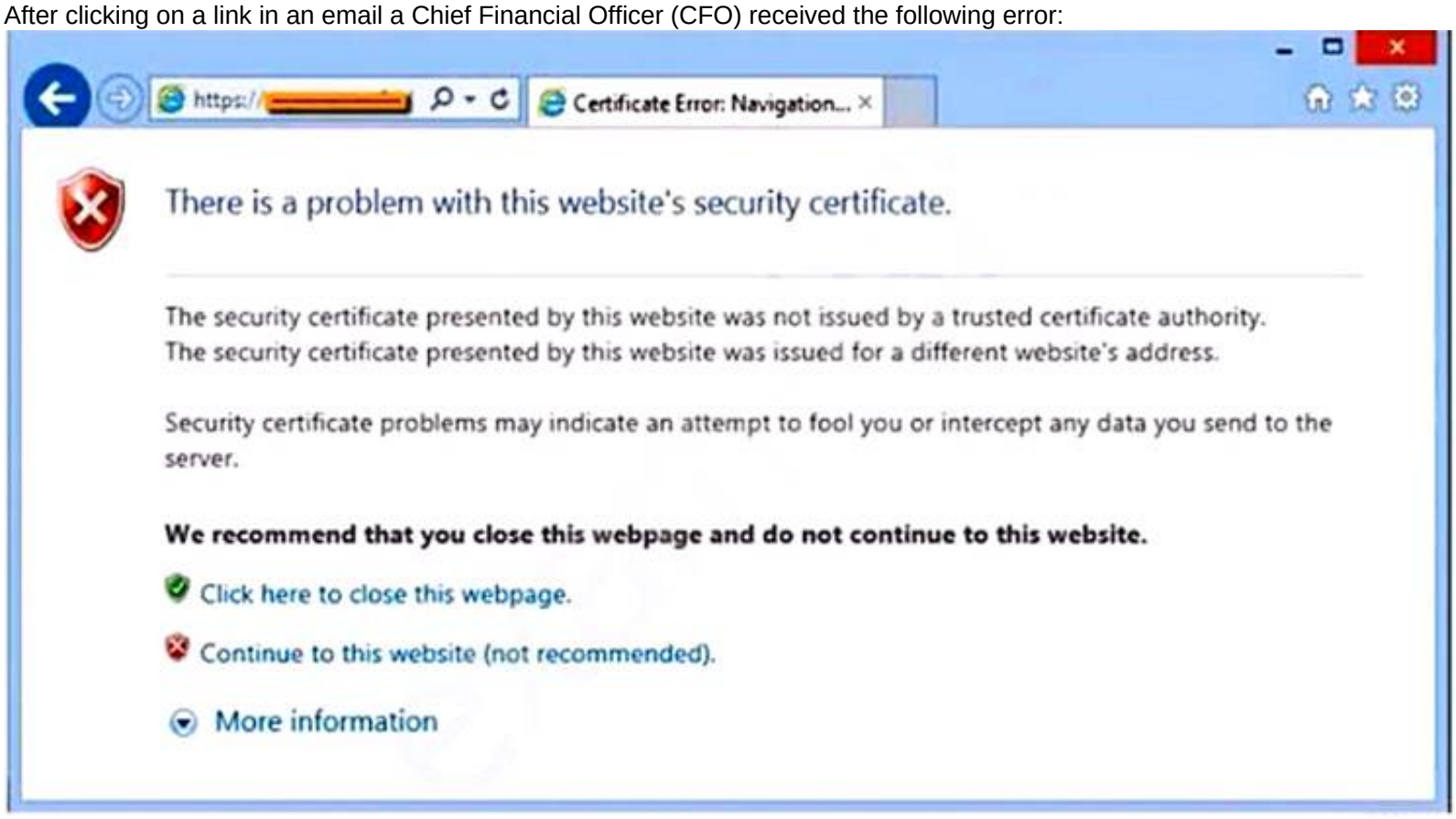
NEW QUESTION 78
Sensitive data was leaked from a user's smartphone. A technician discovered an unapproved application was installed, and the user has full access to the device's command shell. Which of the following is the NEXT step the technician should take to find the cause of the leaked data?

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

Answer: B

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

NEW QUESTION 80
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

Answer: A

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

NEW QUESTION 83
Which of the following is a proprietary Cisco AAA protocol?

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

Answer: D

Explanation:
TACACS+ is a proprietary Cisco AAA protocol

NEW QUESTION 84
The findings from a security audit indicate the risk of data loss from lost or stolen laptops is high. The company wants to reduce this risk with minimal impact to users who want to use their laptops when not on the network. Which of the following would BEST reduce this risk for Windows laptop users?

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

Answer: D

Explanation:

BitLocker is a disk encryption tool that can be used to encrypt the hard drive of a Windows laptop. This will protect the data stored on the drive in the event that the laptop is lost or stolen, and will help to reduce the risk of data loss. Additionally, BitLocker can be configured to require a PIN or other authentication in order to unlock the drive, providing an additional layer of security.

NEW QUESTION 88
A technician received a call stating that all files in a user's documents folder appear to be Changed, and each of the files now has a look file extension Which pf the following actions is the FIRST step the technician should take?

A. Runa live disk clone.
B. Run a full antivirus scan.
C. Use a batch file to rename the files
D. Disconnect the machine from the network

Answer: D

Explanation:
The CompTIA A+ Core 2 220-1002 exam covers this topic in the following domains: 1.2 Given a scenario, use appropriate resources to support users and 1.3 Explain the importance of security awareness.

NEW QUESTION 90
A systems administrator is setting up a Windows computer for a new user Corporate policy requires a least privilege environment. The user will need to access advanced features and configuration settings for several applications. Which of the following BEST describes the account access level the user will need?

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

Answer: B

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

NEW QUESTION 94
A technician is asked to resize a partition on the internal storage drive of a computer running macOS. Which of the followings tools should the technician use to accomplish this task?

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

Answer: B

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

NEW QUESTION 98
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

Answer: C

Explanation:
Default Apps should be used to ensure all PDF files open in Adobe Reader1

NEW QUESTION 100
A technician is troubleshooting a customer's PC and receives a phone call. The technician does not take the call and sets the phone to silent. Which of the following BEST describes the technician's actions?

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

Answer: A

Explanation:

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

NEW QUESTION 105
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

Answer: A

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.

NEW QUESTION 109
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

Answer: B

Explanation:
Account lockout would best mitigate the threat of a dictionary attack1

NEW QUESTION 110
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.

Answer: C

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.

NEW QUESTION 112
A company is Issuing smartphones to employees and needs to ensure data is secure if the devices are lost or stolen. Which of the following provides the BEST solution?

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

Answer: B

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

NEW QUESTION 114
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?

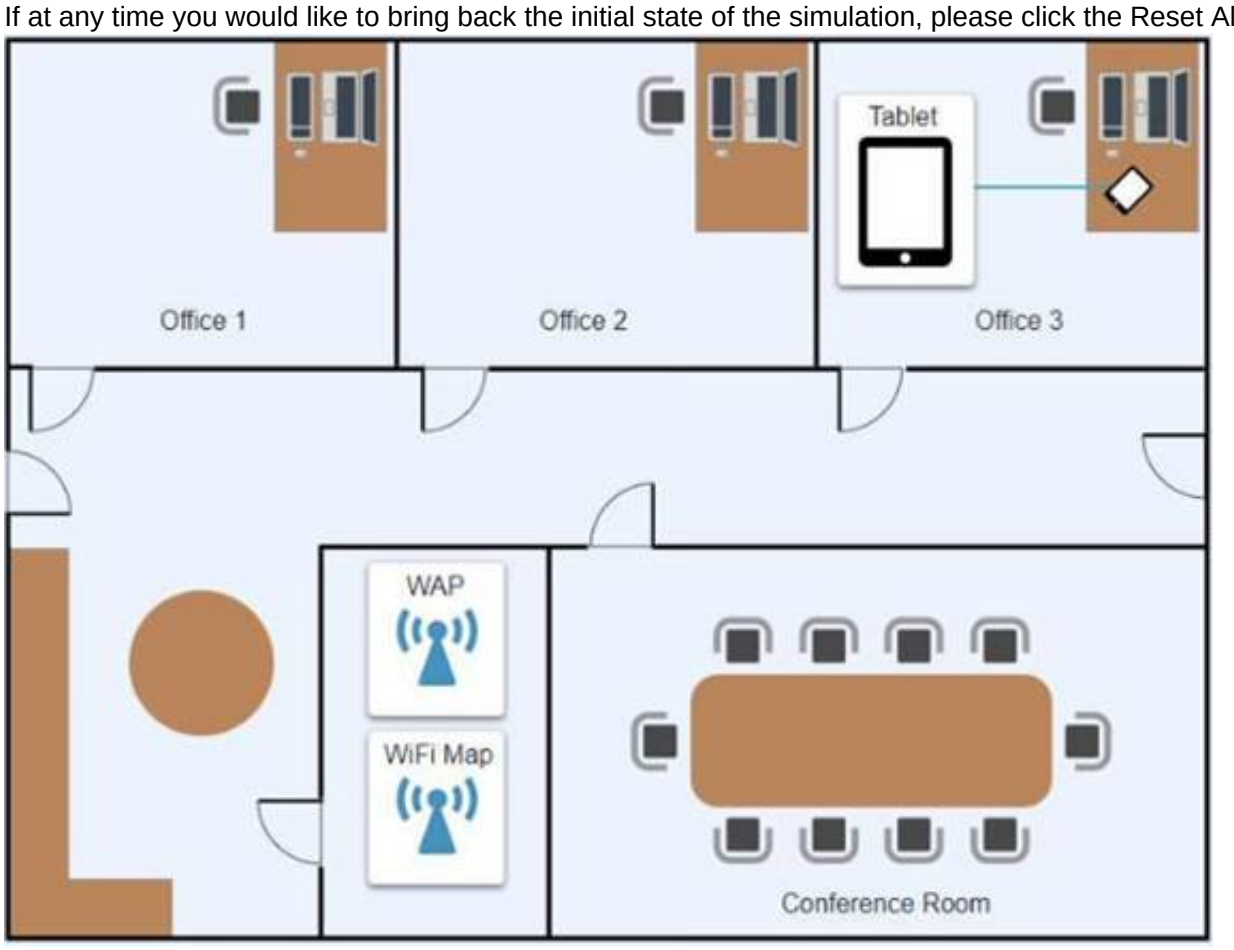
A. Use a key combination to lock the computer when leaving.
B. Ensure no unauthorized personnel are in the area.
C. Configure a screensaver to lock the computer automatically after approximately 30 minutes of inactivity.
D. Turn off the monitor to prevent unauthorized visibility of information.

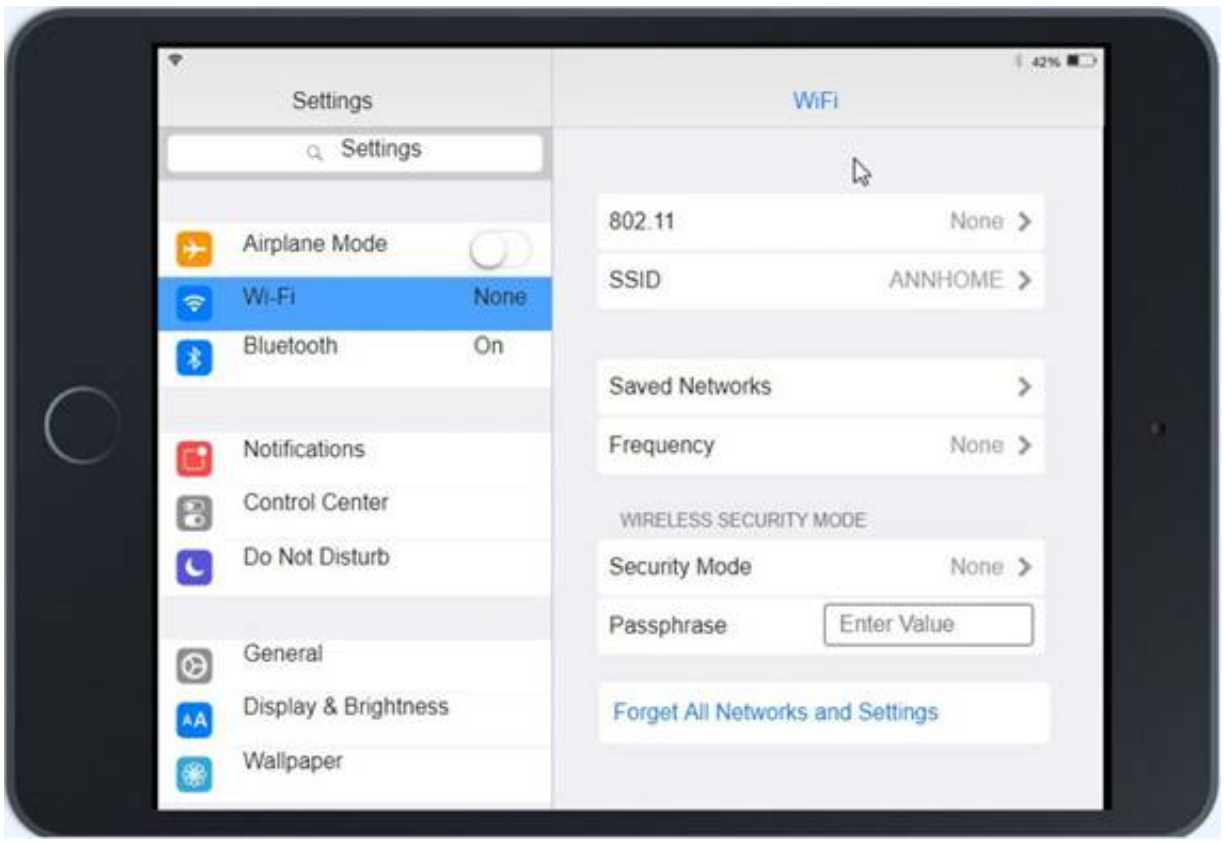
Answer: A

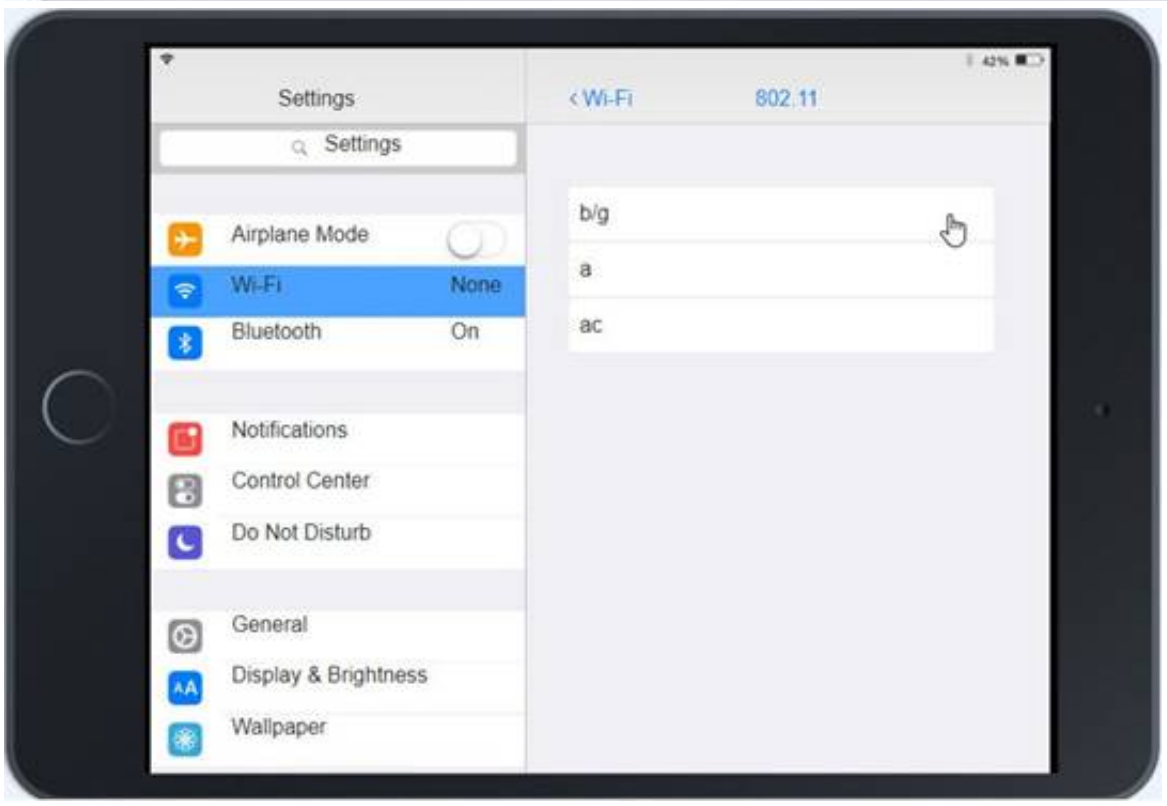
Explanation:

The BEST way to secure the workstation quickly when walking away is to use a key combination to lock the computer when leaving1

NEW QUESTION 115
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.

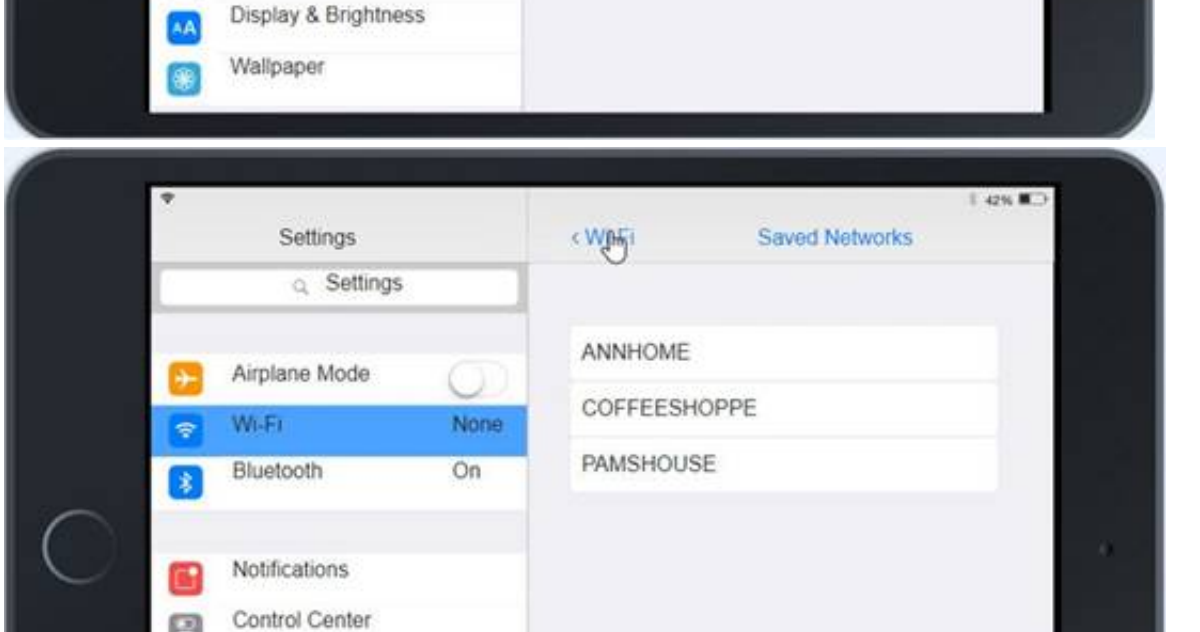


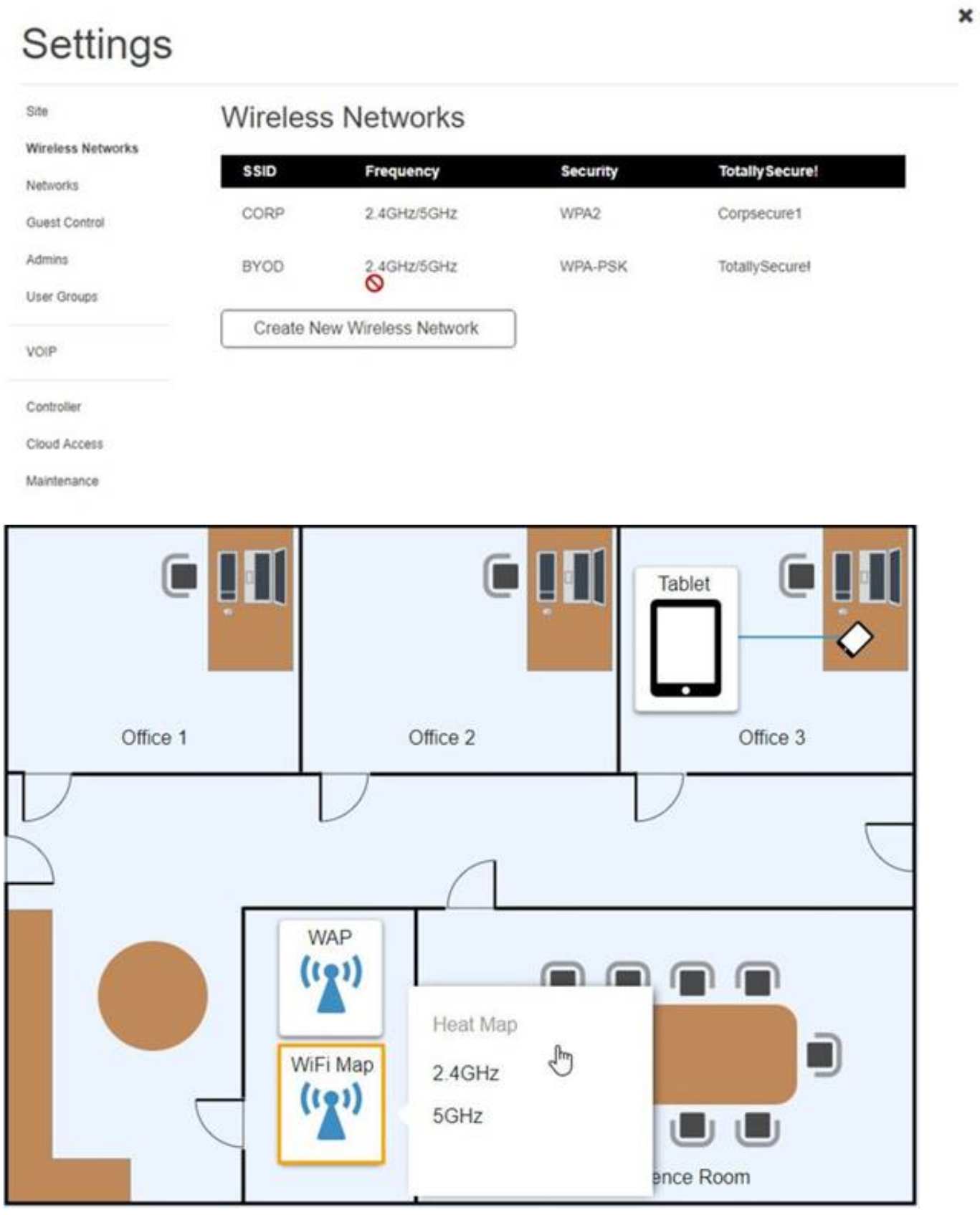





Settings
Settings
Airplane Mode
Wi-Fi None
Bluetooth On
Notifications
Control Center
Do Not Disturb
General
Display & Brightness
Wallpaper
Wi-Fi
SSID
BYOD
DEFAULT
CORP
ANNHOME

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

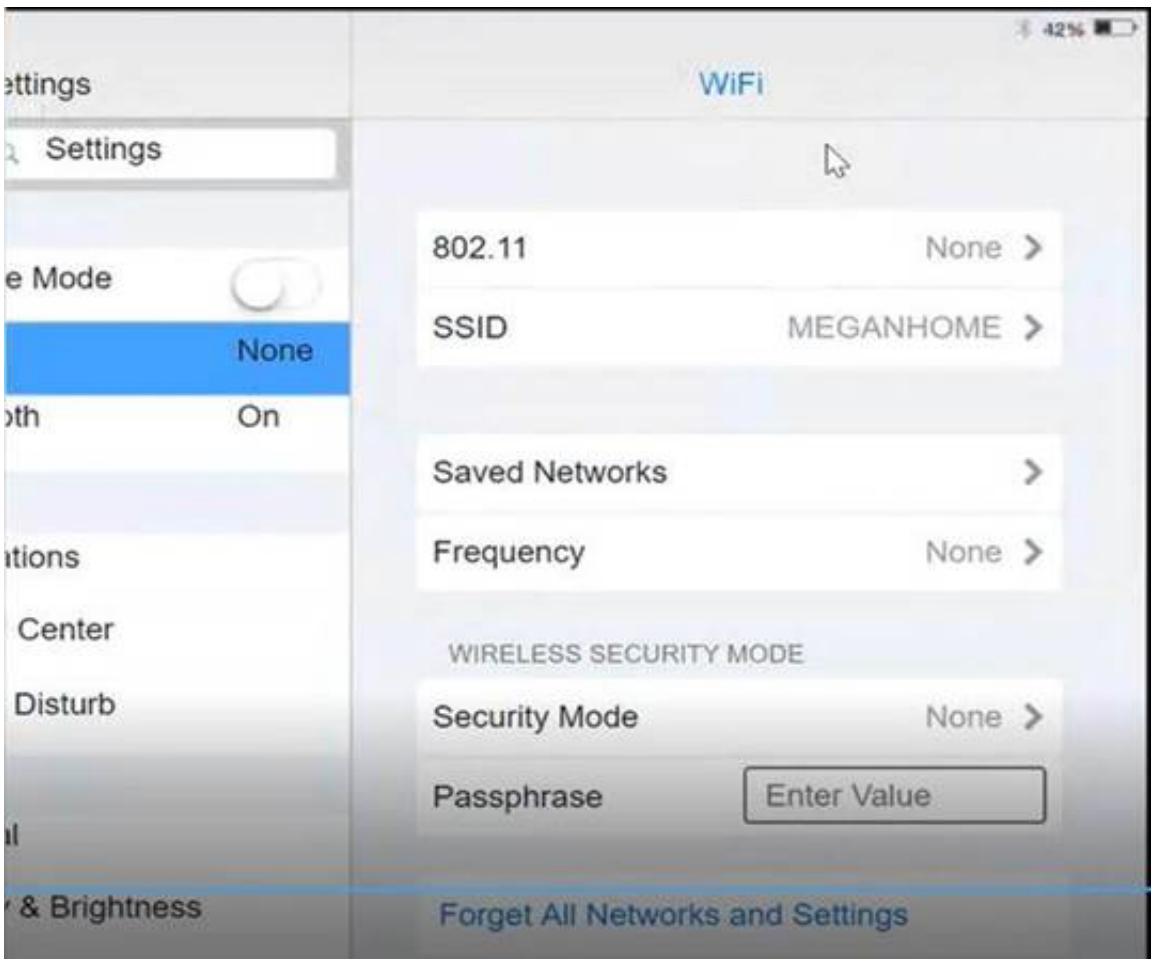

Settings
Settings
Airplane Mode
Wi-Fi None
Bluetooth On
Notifications
Control Center
Do Not Disturb
General
Display & Brightness
Wallpaper
Wi-Fi
Frequency
2.4GHz
5GHz



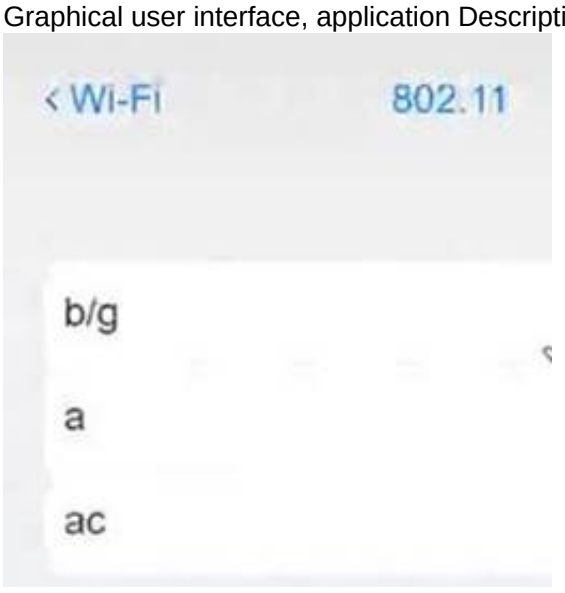
A. Mastered
B. Not Mastered

Answer: A

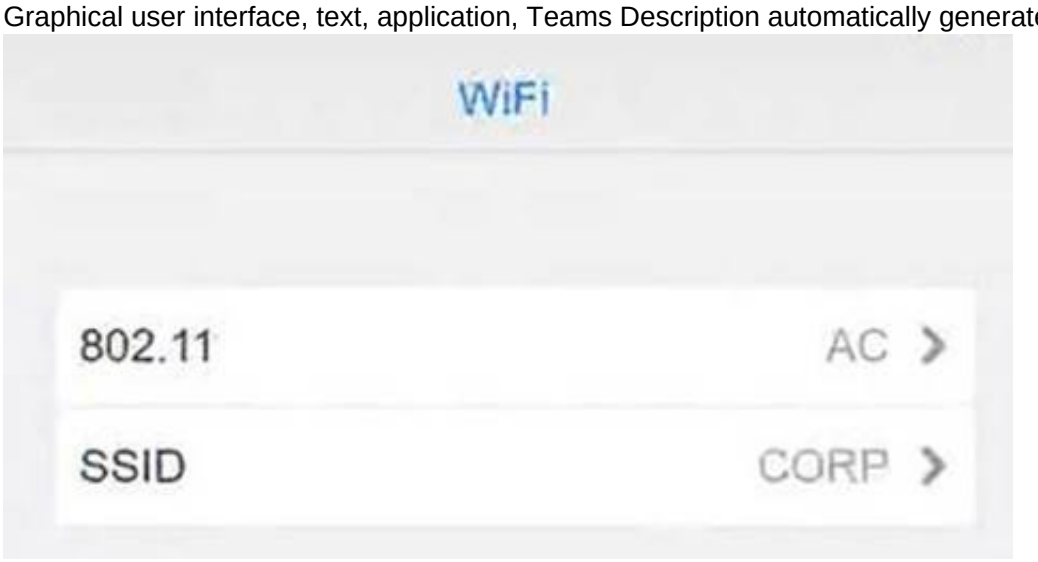
Explanation:
Graphical user interface, application Description automatically generated



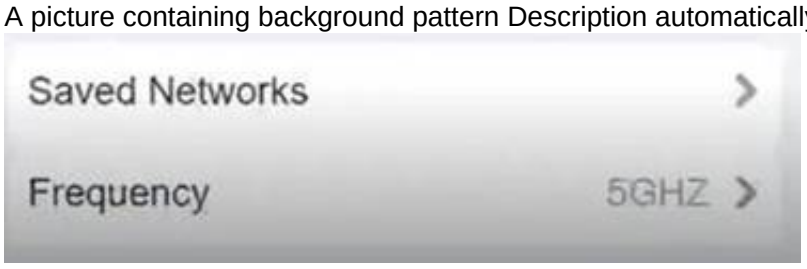
Click on 802.11 and Select ac
Graphical user interface, application Description automatically generated



Click on SSID and select CORP
Graphical user interface, text, application, Teams Description automatically generated

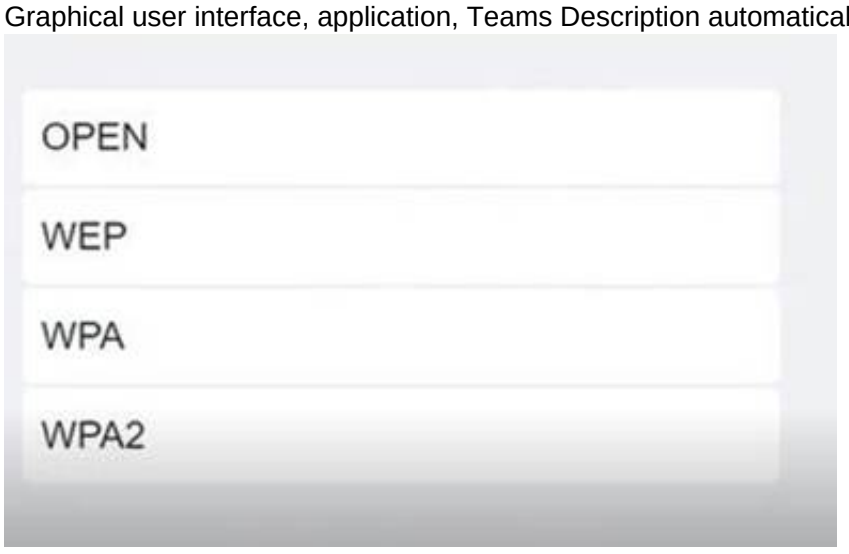


Click on Frequency and select 5GHz
A picture containing background pattern Description automatically generated



At Wireless Security Mode, Click on Security Mode
Graphical user interface, text, application Description automatically generated

Select the WPA2
Graphical user interface, application, Teams Description automatically generated with medium confidence



Ann needs to connect to the BYOD SSID, using 2.4GHZ. The selected security method chose should be WPA PSK, and the password should be set to TotallySecret.
Graphical user interface, application Description automatically generated

NEW QUESTION 118
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

Answer: D

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

NEW QUESTION 123
An administrator has received approval for a change request for an upcoming server deployment. Which of the following steps should be completed NEXT?

A. Perform a risk analysis.

B. Implement the deployment.
C. Verify end user acceptance
D. Document the lessons learned.

Answer: A

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

NEW QUESTION 126
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

Answer: A

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

NEW QUESTION 130
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

Answer: B

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

NEW QUESTION 133
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

Answer: C

Explanation:
The technician should change the default administrative password FIRST to ensure the network equipment is secured against external threats on the Internet. Changing the default administrative password is a basic security measure that can help prevent unauthorized access to the network equipment. Locking all devices in a closet is a physical security measure that can help prevent theft or damage to the devices, but it does not address external threats on the Internet. Ensuring all devices are from the same manufacturer is not a security measure and does not address external threats on the Internet. Installing the latest operating system and patche is important for maintaining the security of the network equipment, but it is not the first action the technician should take1

NEW QUESTION 137
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?

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

Answer: C

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.

NEW QUESTION 141
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

Answer: D

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

NEW QUESTION 142
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.

Answer: B

Explanation:
The GPS application contains malware. The third-party GPS application is likely the cause of the slow performance of the phone. The application may contain malware that is using up system resources and slowing down the phone. The user should uninstall the application and run a malware scan on the phon1e

NEW QUESTION 145
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

Answer: A

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

NEW QUESTION 150
A technician receives a call from a user who is on vacation. The user provides the necessary credentials and asks the technician to log in to the users account and read a critical email that the user has been expecting. The technician refuses because this is a violation of the:

A. acceptable use policy.
B. regulatory compliance requirements.
C. non-disclosure agreement
D. incident response procedures

Answer: A

Explanation:
Logging into a user's account without their explicit permission is a violation of the acceptable use policy, which outlines the rules and regulations by which a user must abide while using a computer system. By logging into the user's account without their permission, the technician would be violating this policy. Additionally, this action could be seen as a breach of confidentiality, as the technician would have access to information that should remain confidential.

NEW QUESTION 154
Which of the following is the MOST basic version of Windows that includes BitLocker?

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

Answer: D

Explanation:
The most basic version of Windows that includes BitLocker is Windows Pro. BitLocker is a feature of Windows Pro that provides full disk encryption for all data on a storage drive [1]. It helps protect data from unauthorized access or theft and can help secure data from malicious attacks. Pro for Workstations includes this feature, as well as other features such as support for up to 6 TB of RAM and ReFS.

NEW QUESTION 155
A suite of security applications was installed a few days ago on a user's home computer. The user reports that the computer has been running slowly since the installation. The user notices the hard drive activity light is constantly solid. Which of the following should be checked FIRST?

A. Services in Control Panel to check for overutilization
B. Performance Monitor to check for resource utilization
C. System File Checker to check for modified Windows files
D. Event Viewer to identify errors

Answer: C

Explanation:
System File Checker to check for modified Windows files. System File Checker (SFC) is a Windows utility that can be used to scan for and restore corrupt Windows system files. SFC can be used to detect and fix any modified or corrupted system files on a computer, and thus should be checked first when a user reports that their computer has been running slowly since the installation of security applications [1][2]. By checking SFC, any modified or corrupted system files can be identified and fixed, potentially improving the overall performance of the computer.

NEW QUESTION 160
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

Answer: D

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.

NEW QUESTION 163
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

Answer: C

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

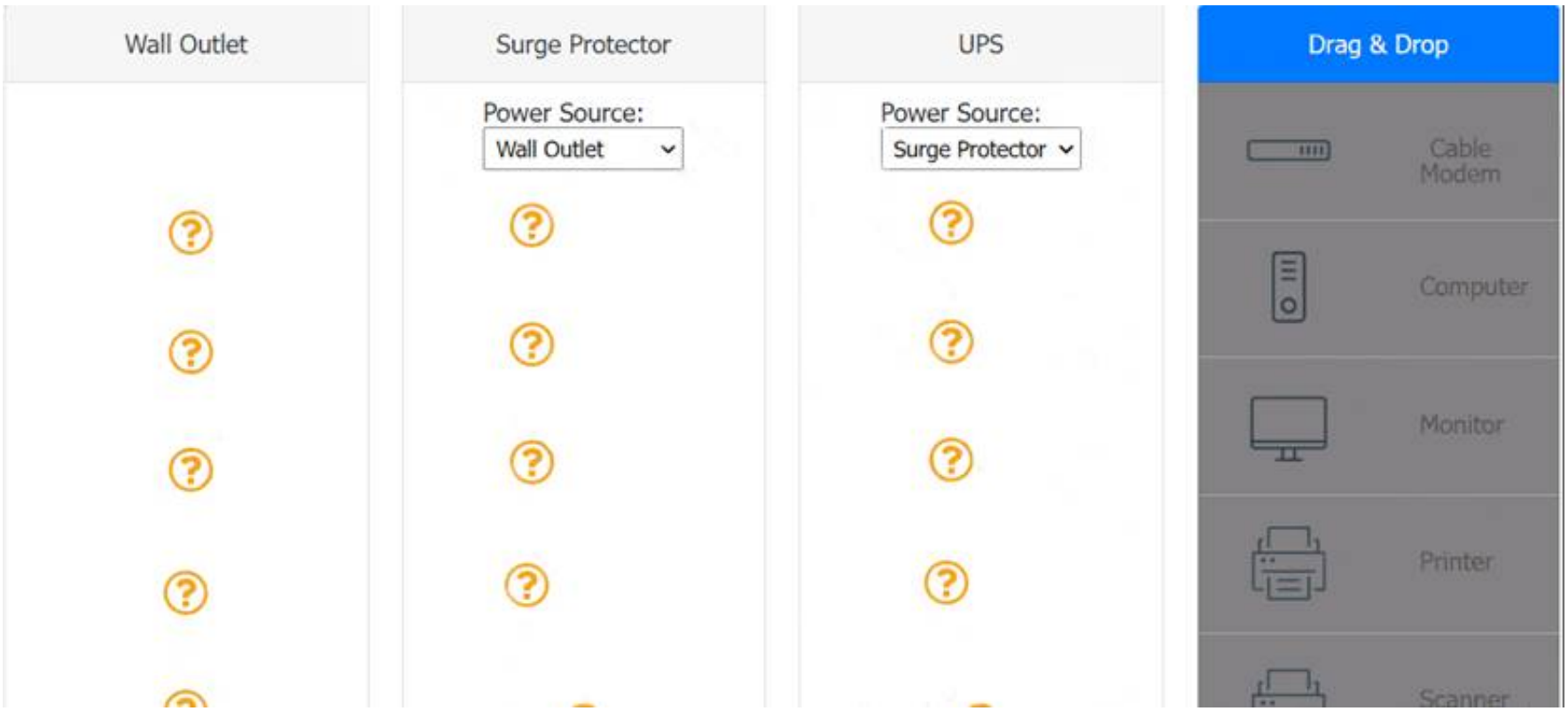
NEW QUESTION 164
A user calls the help desk to report that none of the files on a PC will open. The user also indicates a program on the desktop is requesting payment in exchange for file access A technician verifies the user's PC is infected with ransorrrware. Which of the following should the technician do FIRST?

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

Answer: C

Explanation:
The technician should quarantine the system first1

NEW QUESTION 168
A customer recently experienced a power outage at a SOHO. The customer does not think the components are connected properly. A print job continued running for several minutes after the power failed, but the customer was not able to interact with the computer. Once the UPS stopped beeping, all functioning devices also turned off. In case of a future power failure, the customer wants to have the most time available to save cloud documents and shut down the computer without losing any data.



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 172
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

Answer: D

Explanation:
Shredding is the most effective method to securely dispose of data stored on optical discs12 References: 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/

NEW QUESTION 175
A technician is configuring a new Windows laptop Corporate policy requires that mobile devices make use of full disk encryption at all limes Which of the following encryption solutions should the technician choose?

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

Answer: A

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

NEW QUESTION 180
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

Answer: C

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

NEW QUESTION 183
A user has a license for an application that is in use on a personal home laptop. The user approaches a systems administrator about using the same license on multiple computers on the corporate network. Which of the following BEST describes what the systems administrator should tell the user?

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

Answer: B

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

NEW QUESTION 188
A user reports a computer is running slow. Which of the following tools will help a technician identify the issue?

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

Answer: D

Explanation:
Resource Monitor is a Windows utility that can be used to monitor and analyze the system resources and processes running on a computer. It can be used to identify and troubleshoot any issues that might be causing the computer to run slowly, such as CPU usage, memory usage, disk I/O, and network usage.

NEW QUESTION 189
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

Answer: B

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

NEW QUESTION 191
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.

Answer: D

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.

NEW QUESTION 196
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

Answer: B

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

NEW QUESTION 198
A laptop user is visually impaired and requires a different cursor color. Which of the following OS utilities is used to change the color of the cursor?

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

Answer: C

Explanation:
The OS utility used to change the color of the cursor in Windows is Ease of Access Cente1r2
The user can change the cursor color by opening the Settings app, selecting Accessibility in the left sidebar selecting Mouse pointer and touch under Vision, and choosing one of the cursor options. The user can
select Custom to pick a color and use the Size slider to make the cursor larger or 1sm2 aller
The Ease of Access Center in the Windows OS provides accessibility options for users with disabilities or impairments. One of these options allows the user to change the color and size of the cursor, making it more visible and easier to locate on the screen. The Keyboard and Touchpad settings do not offer the option to change cursor color, and Display Settings are used to adjust the resolution and other properties of the display. Therefore, C is the best answer. This information is covered in the Comptia A+ Core2 documents/guide under the Accessibility section.

NEW QUESTION 201
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

Answer: AB

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.

NEW QUESTION 205
A small business owner wants to install newly purchased software on all networked PCs. The network is not configured as a domain, and the owner wants to use the easiest method possible. Which of the following is the MOST deficient way lor the owner to install the application?

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

Answer: B

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

NEW QUESTION 209
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

Answer: C

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.

NEW QUESTION 210
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.

Answer:

A

NEW QUESTION 215
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

Answer: C

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

NEW QUESTION 216
A customer reported that a home PC with Windows 10 installed in the default configuration is having issues loading applications after a reboot occurred in the middle of the night. Which of the following is the FIRST step in troubleshooting?

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

Answer: C

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

NEW QUESTION 221
Which of the following change management documents includes how to uninstall a patch?

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

Answer: B

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

NEW QUESTION 226
A manager reports that staff members often forget the passwords to their mobile devices and applications. Which of the following should the systems administrator do to reduce the number of help desk tickets submitted?

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

Answer: A

Explanation:
Multifactor authentication (MFA) is a security measure that requires users to provide multiple pieces of evidence when logging in to an account or system. This can include a combination of something the user knows (e.g. a password or PIN), something the user has (e.g. a security token or smartphone) and something the user is (e.g. biometrics such as a fingerprint or face scan). By enabling MFA, the systems administrator can ensure that users are required to provide multiple pieces of evidence when logging in, making it more difficult for unauthorized users to gain access to the system. This can help reduce the number of help desk tickets submitted due to forgotten passwords.

NEW QUESTION 230
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

Answer: D

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

NEW QUESTION 235
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 impac
B. Most Voted
C. A risk assessment can be performed to determine if the software is needed.
D. End users can be aware of the scope of the change.
E. A rollback plan can be implemented in case the software breaks an application.

Answer: A

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.

NEW QUESTION 240
A user connected a laptop to a wireless network and was tricked into providing login credentials for a website. Which of the following threats was used to carry out the attack?

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

Answer: B

Explanation:
Vishing, also known as voice phishing, is a type of social engineering attack where the attacker tricks the victim into divulging sensitive information over the phone. In this case, the attacker tricked the user into providing login credentials for a website.

NEW QUESTION 243
Someone who is fraudulently claiming to be from a reputable bank calls a company employee. Which of the following describes this incident?

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

Answer: C

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

NEW QUESTION 246
A technician is setting up a new laptop. The company's security policy states that users cannot install virtual machines. Which of the following should the technician implement to prevent users from enabling virtual technology on their laptops?

A. UEFI password
B. Secure boot
C. Account lockout
D. Restricted user permissions

Answer: B

Explanation:
A technician setting up a new laptop must ensure that users cannot install virtual machines as the company's security policy states One way to prevent users from enabling virtual technology is by implementing Secure Boot. Secure Boot is a feature of UEFI firmware that ensures the system only boots using firmware that is trusted by the manufacturer. It verifies the signature of all bootloaders, operating systems, and drivers before running them, preventing any unauthorized modifications to the boot process. This will help prevent users from installing virtual machines on the laptop without authorization.

NEW QUESTION 250
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

Answer: B

Explanation:
To exclude an application folder from being cataloged by a Windows 10 search, the technician should use the Indexing Options uti1lity

NEW QUESTION 252
A technician is attempting to mitigate micro power outages, which occur frequently within the area of operation. The outages are usually short, with the longest occurrence lasting five minutes. Which of the following should the technician use to mitigate this issue?

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

Answer: B

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

NEW QUESTION 256
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

Answer: C

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

NEW QUESTION 257
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

Answer: A

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

NEW QUESTION 261
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.

Answer: C

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.

NEW QUESTION 262
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your 220-1102 Exam with Our Prep Materials Via below:

https://www.certleader.com/220-1102-dumps.html