CompTIA

Exam Questions 220-1102

CompTIA A+ Certification Exam: Core 2

NEW QUESTION 1
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.

Answer: C

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.
References5: Malware: what it is, how it works, and how to stop it - Norton6: How to Prevent Malware: 15 Best Practices for Malware Prevention7: 10 Security Tips for How to Prevent Malware Infections - Netwrix

NEW QUESTION 2
A company recently experienced a security incident in which a USB drive containing malicious software was able to covertly install malware on a workstation. Which of the following actions should be taken to prevent this incident from happening again? (Select two).

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

Answer: EG

Explanation:
AutoRun is a feature of Windows that automatically executes a program or file when a removable media such as a USB drive is inserted into the computer. Disabling AutoRun can prevent a USB drive containing malicious software from covertly installing malware on a workstation, as it would require the user to manually open the drive and run the file. Restricting user permissions can also prevent a USB drive containing malicious software from covertly installing malware on a workstation, as it would limit the user's ability to execute or install unauthorized programs or files. Installing a host-based IDS, restricting log-in times, enabling a BIOS password, updating the password complexity, and updating the antivirus definitions are not actions that can directly prevent this incident from happening again.

NEW QUESTION 3
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 4
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

Answer: B

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.

NEW QUESTION 5
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

Answer: C

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.

NEW QUESTION 6
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

Answer: B

Explanation:
A name on a medical diagnosis (B) is most likely to be regulated. This is because it falls under the category of protected health information (PHI), which is subject to regulations such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States. These regulations aim to protect the privacy and security of individuals' health information.

NEW QUESTION 7
A technician at a customer site is troubleshooting a laptop A software update needs to be downloaded but the company's proxy is blocking traffic to the update site. Which of the following should the technician perform?

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

Answer: C

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

NEW QUESTION 8
A technician is in the process of installing a new hard drive on a server but is called away to another task. The drive has been unpackaged and left on a desk. Which of the following should the technician perform before leaving?

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

Answer: C

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

NEW QUESTION 9
Which of the following Is used to identify potential issues with a proposed change poor lo implementation?

A. Request form
B. Rollback plan
C. End-user acceptance
D. Sandbox testing

Answer: D

Explanation:

Sandbox testing is a method of identifying potential issues with a proposed change prior to implementation. It involves creating a simulated or isolated environment that mimics the real system and applying the change to it. This can help to verify that the change works as expected and does not cause any errors or conflicts. Request form, rollback plan and end-user acceptance are other components of a change management process, but they do not involve identifying issues with a change. Verified References: https://www.comptia.org/blog/what-is-sandbox-testing https://www.comptia.org/certifications/a

NEW QUESTION 10
A remote user is experiencing issues connecting to a corporate email account on a laptop. The user clicks the internet connection icon and does not recognize the connected Wi-Fi. The help desk technician, who is troubleshooting the issue, assumes this is a rogue access point. Which of the following is the first action the technician should take?

A. Restart the wireless adapter.
B. Launch the browser to see if it redirects to an unknown site.
C. Instruct the user to disconnect the Wi-Fi.
D. Instruct the user to run the installed antivirus software.

Answer: C

Explanation:
Instructing the user to disconnect the Wi-Fi is the first action the technician should take if they suspect a rogue access point. A rogue access point is an unauthorized wireless network that could be used to intercept or manipulate network traffic, compromise security, or launch attacks. Disconnecting the Wi-Fi would prevent further exposure or damage to the user's device or data. Restarting the wireless adapter, launching the browser, or running the antivirus software are possible actions to take after disconnecting the Wi-Fi, but they are not as urgent or effective as the first step. References:
? Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 22
? CompTIA A+ Core 1 (220-1101) and Core 2 (220-1102) Cert Guide, page 456

NEW QUESTION 10
A new spam gateway was recently deployed at a small business However; users still occasionally receive spam. The management team is concerned that users will open the messages and potentially
infect the network systems. Which of the following is the MOST effective method for dealing with this Issue?

A. Adjusting the spam gateway
B. Updating firmware for the spam appliance
C. Adjusting AV settings
D. Providing user training

Answer: D

Explanation:
The most effective method for dealing with spam messages in a small business is to provide user training1. Users should be trained to recognize spam messages and avoid opening them1. They should also be trained to report spam messages to the IT department so that appropriate action can be taken1. In addition, users should be trained to avoid clicking on links or downloading attachments from unknown sources1. By providing user training, the management team can reduce the risk of users opening spam messages and potentially infecting the network systems1.

NEW QUESTION 12
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

Answer: C

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. References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.7

NEW QUESTION 13
A customer called the help desk to report that a machine that was recently updated is no longer working. The support technician checks the latest logs to see what updates were deployed, but nothing was
deployed in more than three weeks. Which of the following should the support technician do to BEST resolve the situation?

A. Offer to wipe and reset the device for the customer.
B. Advise that the help desk will investigate and follow up at a later date.
C. Put the customer on hold and escalate the call to a manager.
D. Use open-ended questions to further diagnose the issue.

Answer: D

Explanation:

Open-ended questions are questions that require more than a yes or no answer and encourage the customer to provide more details and information. Using open-ended questions can help the support technician to understand the problem better, identify the root cause, and find a suitable solution. Some examples of open-ended questions are:
? What exactly is not working on your machine?
? When did you notice the problem?
? How often does the problem occur?
? What were you doing when the problem happened?
? What have you tried to fix the problem?
Offering to wipe and reset the device for the customer is not a good option, as it may result in data loss and inconvenience for the customer. It should be used as a last resort only if other troubleshooting steps fail. Advising that the help desk will investigate and follow up at a later date is not a good option, as it may leave the customer unsatisfied and frustrated. It should be used only if the problem requires further research or escalation and cannot be resolved on the first call. Putting the customer on hold and escalating the call to a manager is not a good option, as it may waste time and resources. It should be used only if the problem is beyond the support technician's scope or authority and requires managerial intervention.

NEW QUESTION 18
Which of the following is used as a password manager in the macOS?

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

Answer: D

Explanation:
Keychain is a feature of macOS that securely stores passwords, account numbers, and other confidential information for your Mac, apps, servers, and websites1. You can use the Keychain Access app on your Mac to view and manage your keychains and the items stored in them1. Keychain can also sync your passwords across your devices using iCloud Keychain1. Keychain can be used as a password manager in macOS to help you keep track of and protect your passwords. References: 1: Manage passwords using keychains on Mac (https://support.apple.com/guide/mac-help/use-keychains-to-store-passwords- mchlf375f392/mac)

NEW QUESTION 19
A technician is creating a tunnel that hides IP addresses and secures all network traffic. Which of the following protocols is capable of enduring enhanced security?

A. DNS
B. IPS
C. VPN
D. SSH

Answer: C

Explanation:
A VPN (virtual private network) is a protocol that creates a secure tunnel between two devices over the internet, hiding their IP addresses and encrypting their traffic. DNS (domain name system) is a protocol that translates domain names to IP addresses. IPS (intrusion prevention system) is a device that monitors and blocks malicious network traffic. SSH (secure shell) is a protocol that allows remote access and command execution on another device. Verified References: https://www.comptia.org/blog/what-is-a-vpn
https://www.comptia.org/certifications/a

NEW QUESTION 20
A salesperson's computer is unable to print any orders on a local printer that is connected to the computer Which of the following tools should the salesperson use to restart the print spooler?

A. Control Panel
B. Processes
C. Services
D. Startup

Answer: D

Explanation:
The correct answer is D. Services. The print spooler is a service that manages the print queue and sends print jobs to the printer. To restart the print spooler, the salesperson can use the Services app, which allows them to stop and start the service. Alternatively, they can also use the Task Manager or the Command Prompt to restart the print spooler.
References and Explanation
? The Services app is a tool that displays all the services that are running on the computer. It can be accessed by typing services.msc in the Run window or by searching for Services in the Start menu. The Services app allows users to start, stop, restart, or configure any service, including the print spooler123.
? The Task Manager is a tool that shows information about the processes, applications, and services that are running on the computer. It can be accessed by pressing Ctrl + Shift + Esc or by right-clicking on the taskbar and selecting Task Manager. The Task Manager allows users to start, stop, or restart any service by going to the Services tab and right-clicking on the service name12.
? The Command Prompt is a tool that allows users to execute commands and perform tasks using text input. It can be accessed by typing cmd in the Run window or by searching for Command Prompt in the Start menu. The Command Prompt allows users to start, stop, or restart any service by using the net command with the service name. For example, to restart the print spooler, users can type net stop spooler and then net start spooler1.
? The Control Panel is a tool that provides access to various settings and options for the computer. It can be accessed by typing control panel in the Run window or by searching for Control Panel in the Start menu. The Control Panel does not allow users to restart the print spooler directly, but it can be used to access other tools such as Devices and Printers, Troubleshooting, or Administrative Tools2.
? The Processes tab is a part of the Task Manager that shows information about the processes that are running on the computer. It can be accessed by opening the Task Manager and selecting the Processes tab. The Processes tab does not allow

users to restart the print spooler directly, but it can be used to end any process that is related to printing or causing problems with the print spooler2.
? The Startup tab is a part of the Task Manager that shows information about the
programs that run automatically when the computer starts. It can be accessed by opening the Task Manager and selecting the Startup tab. The Startup tab does not allow users to restart the print spooler directly, but it can be used to disable or enable any program that affects printing or interferes with the print spooler2.

NEW QUESTION 25

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.

Answer: B

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.

NEW QUESTION 26
A help desk technician needs to remotely access and control a customer's Windows PC by using a secure session that allows the technician the same control as the customer. Which of the following tools provides this type of access?

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

Answer: B

Explanation:
RDP stands for Remote Desktop Protocol, which is a proprietary protocol developed by Microsoft that allows a user to remotely access and control another computer over a network. RDP provides a secure session that encrypts the data between the client and the host, and allows the user to see and interact with the desktop and applications of the remote computer as if they were sitting in front of it. RDP also supports features such as audio, video, clipboard, printer, and file sharing, as well as multiple monitor support and session recording. To use RDP, the host computer must have Remote Desktop enabled and configured, and the client computer must have a Remote Desktop client software installed. The client can connect to the host by entering its IP address, hostname, or domain name, and providing the login credentials of a user account on the host. RDP is commonly used for remote administration, technical support, and remote work scenarios

NEW QUESTION 30
A company-owned mobile device is displaying a high number of ads, receiving data-usage limit notifications, and experiencing slow response. After checking the device, a technician notices the device has been jailbroken. Which of the following should the technician do next?

A. Run an antivirus and enable encryption.
B. Restore the defaults and reimage the corporate OS.
C. Back up the files and do a system restore.
D. Undo the jailbreak and enable an antivirus.

Answer: B

Explanation:
The best course of action for the technician is to restore the defaults and reimage the corporate OS on the device. This will remove the jailbreak and any unauthorized or malicious apps that may have been installed on the device, as well as restore the security features and policies that the company has set for its devices. This will also ensure that the device can receive the latest updates and patches from the manufacturer and the company, and prevent any data leakage or compromise from the device.
Jailbreaking is a process of bypassing the built-in security features of a device to install software other than what the manufacturer has made available for that device1. Jailbreaking allows the device owner to gain full access to the root of the operating system and access all the features1. However, jailbreaking also exposes the device to various risks, such as:
? The loss of warranty from the device manufacturers2.
? Inability to update software until a jailbroken version becomes available2.
? Increased security vulnerabilities32.
? Decreased battery life2.
? Increased volatility of the device2.
Some of the signs of a jailbroken device are:
? A high number of ads, which may indicate the presence of adware or spyware on the device3.
? Receiving data-usage limit notifications, which may indicate the device is sending or receiving data in the background without the user's knowledge or consent3.
? Experiencing slow response, which may indicate the device is running unauthorized or malicious apps that consume resources or interfere with the normal functioning of the device3.
? Finding apps or icons that the user did not install or recognize, such as Cydia, which is a storefront for jailbroken iOS devices1.
The other options are not sufficient or appropriate for dealing with a jailbroken device. Running an antivirus and enabling encryption may not detect or remove all

the threats or vulnerabilities that the jailbreak has introduced, and may not restore the device to its original state or functionality. Backing up the files and doing a system restore may not erase the jailbreak or the unauthorized apps, and may also backup the infected or compromised files. Undoing the jailbreak and enabling an antivirus may not be possible or effective, as the jailbreak may prevent the device from updating or installing security software, and may also leave traces of the jailbreak or the unauthorized apps on the device.
References:
? CompTIA A+ Certification Exam Core 2 Objectives4
? CompTIA A+ Core 2 (220-1102) Certification Study Guide5
? What is Jailbreaking & Is it safe? - Kaspersky1
? Is Jailbreaking Safe? The ethics, risks and rewards involved - Comparitech3
? Jailbreaking : Security risks and moving past them2

NEW QUESTION 35
A remote user is experiencing issues with Outlook settings and asks a technician to review the settings. Which of the following can the technician use to access the user's computer remotely?

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

Answer: B

Explanation:
One of the possible ways to access the user’s computer remotely is to use RDP, which stands for Remote Desktop Protocol. RDP is a protocol that allows a user to connect to another computer over a network and use its graphical interface. RDP is commonly used for remote desktop software, such as Microsoft Remote Desktop Connection1. To use RDP, the user’s computer must run RDP server software, and the technician must run RDP client software. The technician can then enter the user’s IP address or hostname, and provide the appropriate credentials to log in to the user’s computer. Once connected, the technician can view and control the user’s desktop, and review the Outlook settings.

NEW QUESTION 38
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 Reference:
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)

NEW QUESTION 40
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

Answer: D

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.

NEW QUESTION 43
A team of support agents will be using their workstations to store credit card data. Which of the following should the IT department enable on the workstations in order to remain compliant with common regulatory controls? (Select TWO).

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

Answer: AF

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

NEW QUESTION 48
A user recently purchased a second monitor and wants to extend the Windows desktop to the new screen. Which of the following Control Panel options should a technician adjust to help the user?

A. Color Management
B. System
C. Troubleshooting
D. Device Manager
E. Administrative Tools

Answer: D

NEW QUESTION 50
A technician suspects a rootkit has been installed and needs to be removed. Which of the following would BEST resolve the issue?

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 53
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.

Answer: A

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 inactivity1

NEW QUESTION 54
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 55
A company is experiencing a ODDS attack. Several internal workstations are the source of the traffic Which of the following types of infections are the workstations most likely experiencing? (Select two)

A. Zombies
B. Keylogger
C. Adware
D. Botnet
E. Ransomvvare
F. Spyware

Answer: AD

Explanation:
The correct answers are A and D. Zombies and botnets are types of infections that allow malicious actors to remotely control infected computers and use them to launch distributed denial-of-service (DDoS) attacks against a target. A DDoS attack is a type of cyberattack that aims to overwhelm a server or a network with a large volume of traffic from multiple sources, causing it to slow down or crash.
A keylogger is a type of malware that records the keystrokes of a user and sends them to a remote server, often for the purpose of stealing passwords, credit card numbers, or other sensitive information.
Adware is a type of software that displays unwanted advertisements on a user's computer, often in the form of pop-ups, banners, or redirects. Adware can also collect user data and compromise the security and performance of the system.
Ransomware is a type of malware that encrypts the files or locks the screen of a user's computer and demands a ransom for their restoration. Ransomware can also threaten to delete or expose the user's data if the ransom is not paid.

Spyware is a type of software that covertly monitors and collects information about a user's online activities, such as browsing history, search queries, or personal data. Spyware can also alter the settings or functionality of the user's system without their consent.

NEW QUESTION 58
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

Answer: A

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

NEW QUESTION 60
A user reports a workstation has been performing strangely after a suspicious email was opened on it earlier in the week. Which of the following should the technician perform FIRST?

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 64
A user's application is unresponsive. Which of the following Task Manager tabs will allow the user to address the situation?

A. Startup
B: Performance
C. Application history
D. Processes

Answer: D

Explanation:
The Processes tab in the Task Manager shows all the running processes on the computer, including applications and background services. The user can use this tab to identify the unresponsive application and end its process by right-clicking on it and selecting End task. This will free up the system resources and close the application. The other tabs in the Task Manager do not allow the user to address the situation. The Startup tab shows the programs that run when the computer starts, the Performance tab shows the system resource usage and statistics, and the Application history tab shows the resource usage of the applications over time

NEW QUESTION 67
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

Answer: D

Explanation:
The command md stands for make directory and is used to create a new directory or folder in the current location. In this case, the technician can use md minutes to create a folder named minutes in the C: drive. The other commands are not relevant for
this task. c: \minutes is not a command but a path to a folder. dir is used to display a list of files and folders in the current directory. rmdir is used to remove or delete an existing directory or folder.

NEW QUESTION 69

A technician is hardening a company file server and needs to prevent unauthorized LAN devices from accessing stored files. Which of the following should the technician use?

A. Software firewall
B. Password complexity
C. Antivirus application
D. Anti-malware scans

Answer: A

Explanation:
A software firewall is a program that monitors and controls the incoming and outgoing network traffic on a computer or a server. A software firewall can help prevent unauthorized LAN devices from accessing stored files on a company file server by applying rules and policies that filter the network packets based on their source, destination,
protocol, port, or content. A software firewall can also block or allow specific applications or services from communicating with the network, and alert the administrator of any
suspicious or malicious activity12.
A software firewall is a better option than the other choices because:
? Password complexity (B) is a good practice to protect the file server from
unauthorized access, but it is not sufficient by itself. Password complexity refers to the use of strong passwords that are hard to guess or crack by attackers, and that are changed frequently and securely. Password complexity can prevent brute force attacks or credential theft, but it cannot stop network attacks that exploit vulnerabilities in the file server software or hardware, or that bypass the authentication process34.
? Antivirus application © and anti-malware scans (D) are important tools to protect
the file server from viruses and malware that can infect, damage, or encrypt the stored files. However, they are not effective in preventing unauthorized LAN devices from accessing the files in the first place. Antivirus and anti-malware tools can only detect and remove known threats, and they may not be able to stop zero- day attacks or advanced persistent threats that can evade or disable
them. Moreover, antivirus and anti-malware tools cannot control the network traffic or the file server permissions, and they may not be compatible with all file server platforms or configurations56.
References:
1: What is a Firewall and How Does it Work? - Cisco1 2: How to Harden Your Windows Server - ServerMania2 3: Password Security: Complexity vs. Length - Norton7 4: Password Hardening: 5 Ways to Protect Your Passwords - Infosec 5: What is Antivirus Software and How Does it Work? - Kaspersky 6: What is Anti-Malware? - Malwarebytes

NEW QUESTION 73
An organization is updating the monitors on kiosk machines. While performing the upgrade, the organization would like to remove physical input devices. Which of the following utilities in the Control Panel can be used to turn on the on-screen keyboard to replace the physical input devices?

A. Devices and Printers
B. Ease of Access
C. Programs and Features
D. Device Manager

Answer: B

Explanation:
Ease of Access is a utility in the Control Panel that allows users to adjust various accessibility settings on Windows, such as the on-screen keyboard, magnifier, narrator, high contrast, etc. The on-screen keyboard can be turned on by going to Ease of Access > Keyboard and toggling the switch to On12. Alternatively, the on-screen keyboard can be opened by pressing Windows + Ctrl + O keys or by typing osk.exe in the Run dialog box3.
References: 1 Use the On-Screen Keyboard (OSK) to type(https://support.microsoft.com/en-us/windows/use-the-on-screen-keyboard-osk-to-type- ecbb5e08-5b4e-d8c8-f794-81dbf896267a)2 How to Enable or Disable the On-Screen Keyboard in Windows 10 - Lifewire(https://www.lifewire.com/enable-or-disable-on-screen-keyboard-in-windows-10-5180667)3 On-Screen Keyboard Settings, Tips and Tricks in Windows 11/10(https://www.thewindowsclub.com/windows-onscreen-keyboard).

NEW QUESTION 75
A technician is installing RAM in a new workstation and needs to protect against electrostatic discharge. Which of the following will best resolve this concern?

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

Answer: C

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

NEW QUESTION 78
A technician is concerned about a large increase in the number of whaling attacks happening in the industry. The technician wants to limit the company's risk to avoid any issues. Which of the following items should the technician implement?

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

Answer: C

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

NEW QUESTION 79
A user wants to back up a Windows 10 device. Which of the following should the user select?

A. Devices and Printers
B. Email and Accounts
C. Update and Security
D. Apps and Features

Answer: C

Explanation:
Update and Security is the section in Windows 10 Settings that allows the user to back up their device. Backing up a device means creating a copy of the data and settings on the device and storing it in another location, such as an external drive or a cloud service. Backing up a device can help the user restore their data and settings in case of data loss, corruption, or theft. Devices and Printers, Email and Accounts, and Apps and Features are not sections in Windows 10 Settings that allow the user to back up their device.

NEW QUESTION 82
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

Answer: A

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

NEW QUESTION 84
Which of the following Is a package management utility for PCs that are running the Linux operating system?

A. chmod
B. yum
C. man
D. grep

Answer: B

Explanation:
yum (Yellowdog Updater Modified) is a package management utility for PCs that are running the Linux operating system. It can be used to install, update and remove software packages from repositories. chmod (change mode) is a command that changes the permissions of files and directories in Linux. man (manual) is a command that displays the documentation of other commands in Linux. grep (global regular expression print) is a command that searches for patterns in text files in Linux. Verified References: https://www.comptia.org/blog/linux-package-management https://www.comptia.org/certifications/a

NEW QUESTION 87
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 89
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

Answer: C

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.

NEW QUESTION 91
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.

Answer: D

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.

NEW QUESTION 95
The Chief Executive Officer at a bark recently saw a news report about a high-profile cybercrime where a remote-access tool that the bank uses for support was also used in this crime. The report stated that attackers were able to brute force passwords to access systems. Which of the following would BEST limit the bark's risk? (Select TWO)

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

Answer: AF

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

NEW QUESTION 96
Which of the following Linux commands would be used to install an application?

A. yum
B. grep
C. Is
D. sudo

Answer: D

Explanation:
The Linux command used to install an application is sudo. The sudo command allows users to run programs with the security privileges of another user, such as the root user. This is necessary to install applications because it requires administrative privileges1

NEW QUESTION 98
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. Mastered
B. Not Mastered

Answer: A

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 103
Which of the following file types allows a user to easily uninstall software from macOS by simply placing it in the trash bin?

A. .exe
B. .dmg
C. . app
D. . rpm
E. .pkg

Answer: C

Explanation:
app files are application bundles that contain all the necessary files and resources for a Mac app. They can be easily deleted by dragging them to the Trash or using Launchpad12. Other file types, such as .exe, .dmg, .rpm, and .pkg, are either not compatible with macOS or require additional steps to uninstall34. References: 1 Uninstall apps on your Mac - Apple Support(https://support.apple.com/en- us/102610)2 How to Uninstall Apps on a Mac (and Make Sure Leftover Files Are
…(https://www.pcmag.com/how-to/uninstall-delete-apps-from-mac)3 How to install and uninstall software on a Mac - Laptop Mag(https://www.laptopmag.com/articles/install- unininstall-mac-software)4 How to completely uninstall an app on a Mac and delete all junk files(https://www.xda-developers.com/how-to-uninstall-app-mac/).

NEW QUESTION 108
The command cac cor.ptia. 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 compti
C. txt would be displayed.
D. The contents of the text comptia.txt would be categorized in alphabetical order.
E. The contents of the text compti
F. txt would be copied to another compti
G. txt file

Answer: B

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

NEW QUESTION 112
A user is unable to access a web-based application. A technician verifies the computer cannot access any web pages at all. The computer obtains an IP address from the DHCP server. Then, the technician verifies the user can ping localhost. the gateway, and known IP addresses on the interne! and receive a response. Which of the following Is the MOST likely reason tor the Issue?

A. A firewall is blocking the application.
B. The wrong VLAN was assigned.
C. The incorrect DNS address was assigned.
D. The browser cache needs to be cleared

Answer: C

Explanation:
DNS (domain name system) is a protocol that translates domain names to IP addresses. If the computer has an incorrect DNS address assigned, it will not be able to

resolve the domain names of web-based applications and access them. A firewall, a VLAN (virtual local area network) and a browser cache are not the most likely reasons for the issue, since the computer can ping known IP addresses on the internet and receive a response. Verified References: https://www.comptia.org/blog/what-is-dns https://www.comptia.org/certifications/a

NEW QUESTION 117
A PC is taking a long time to boot. Which of the following operations would be best to do to resolve the issue at a minimal expense? (Select two).

A. Installing additional RAM
B. Removing the applications from startup
C. Installing a faster SSD
D. Running the Disk Cleanup utility
E. Defragmenting the hard drive
F. Ending the processes in the Task Manager

Answer: BD

Explanation:
Removing the applications from startup can improve the boot time of a PC by reducing the number of programs that load automatically when the PC starts. Some applications may add themselves to the startup list without the user's knowledge or consent, which can slow down the PC's performance. Running the Disk Cleanup utility can also improve the boot time of a PC by deleting unnecessary or temporary files that take up disk space and affect the PC's speed. Disk Cleanup can also remove old system files that may cause conflicts or errors during booting. Installing additional RAM, installing a faster SSD, defragmenting the hard drive, and ending the processes in the Task Manager are not operations that would be best to do to resolve the issue of slow boot time at a minimal expense, as they may require purchasing new hardware or software, or may have negative impacts on other aspects of the PC's performance.

NEW QUESTION 118
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

Answer: D

Explanation:
To accomplish this task, the technician should use a Full backup meth1od
A full backup only requires two sets of tapes to restore because it backs up all the data from the workstation. With a differential backup, the backups need to be taken multiple times over a period of time, so more tapes would be needed to restore the data1

NEW QUESTION 121
A customer calls desktop support and begins yelling at a technician. The customer claims to have submitted a support ticket two hours ago and complains that the issue still has not been resolved. Which of the following describes how the technician should respond?

A. Place the customer on hold until the customer calms down.
B. Disconnect the call to avoid a confrontation.
C. Wait until the customer is done speaking and offer assistance.
D. Escalate the issue to a supervisor.

Answer: C

Explanation:
The best way to deal with an angry customer who is yelling at a technician is to wait until the customer is done speaking and offer assistance. This shows respect, empathy, and professionalism, and allows the technician to understand the customer's problem and find a solution. According to the CompTIA A+ Core 2 (220-1102) Certification Study Guide1, some of the steps to handle angry customers are:
? Stay calm and do not take it personally.
? Listen actively and acknowledge the customer's feelings.
? Apologize sincerely and offer to help.
? Restate the customer's issue and ask for clarification if needed.
? Explain the possible causes and solutions for the problem.
? Provide clear and realistic expectations for the resolution.

? Follow up with the customer until the issue is resolved.

The other options are not appropriate ways to deal with angry customers, as they may worsen the situation or damage the customer relationship. Placing the customer on hold may make them feel ignored or dismissed. Disconnecting the call may make them feel disrespected or abandoned. Escalating the issue to a supervisor may make them feel frustrated or powerless, unless the technician cannot resolve the issue or the customer requests to speak to a supervisor.
References:
? CompTIA A+ Certification Exam Core 2 Objectives2
? CompTIA A+ Core 2 (220-1102) Certification Study Guide1
? How To Deal with Angry Customers (With Examples and Tips)3
? 17 ways to deal with angry customers: Templates and examples4
? Six Ways to Handle Angry Customers5

NEW QUESTION 125
An engineer is configuring a new server that requires a bare-metal installation. Which of the following installation methods should the engineer use if installation media is not available on site?

A. Image deployment
B. Recovery partition installation
C. Remote network installation
D. Repair installation

Answer: C

Explanation:
Remote network installation is the best option for configuring a new server that requires a bare-metal installation without installation media on site. A remote network installation is a method of installing an operating system or an application over a network connection, such as LAN, WAN, or Internet. A remote network installation can use various protocols, such as PXE, HTTP, FTP, or SMB, to access the installation files from a server or a cloud service. A remote network installation can also use various tools, such as Windows Deployment Services, Microsoft Deployment Toolkit, or Red Hat Kickstart, to automate and customize the installation process. A remote network installation can save time and resources by eliminating the need for physical media and allowing centralized management of multiple installations. Image deployment, recovery partition installation, and repair installation are not correct answers for this question. Image deployment is a method of installing an operating system or an application by copying a preconfigured image file to a target device. Image deployment requires an existing image file and a compatible device. Recovery partition installation is a method of restoring an operating system or an application from a hidden partition on the hard disk that contains the original factory settings. Recovery partition installation requires an existing recovery partition and a functional hard disk. Repair installation is a method of fixing an operating system or an application that is corrupted or damaged by replacing or repairing the system files without affecting the user data or settings. Repair installation requires an existing operating system or application and a working device. References:
? Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 16
? CompTIA A+ Complete Study Guide: Core 1 Exam 220-1101 and Core 2 Exam …, page 106

NEW QUESTION 129
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

Answer: A

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.

NEW QUESTION 132
A department manager submits a help desk ticket to request the migration of a printer's port utilization from USB to Ethernet so multiple users can access the

printer. This will be a new network printer, thus a new IP address allocation is required. Which of the following should happen immediately before network use is authorized?

A. Document the date and time of the change.
B. Submit a change request form.
C. Determine the risk level of this change.
D. Request an unused IP address.

Answer: B

Explanation:
A change request form is a document that describes the proposed change, the reason for the change, the impact of the change, and the approval process for the change. A change request form is required for any planned changes to the network, such as adding a new network printer, to ensure that the change is authorized, documented, and communicated to all stakeholders. Submitting a change request form should happen immediately before network use is authorized, as stated in the Official CompTIA A+ Core 2 Study Guide. The other options are either too late (documenting the date and time of the change) or too early (determining the risk level of the change and requesting an unused IP address) in the change management process.

NEW QUESTION 134
A technician needs to ensure that USB devices are not suspended by the operating system Which of the following Control Panel utilities should the technician use to configure the setting?

A. System
B. Power Options
C. Devices and Printers
D. Ease of Access

Answer: B

Explanation:
The correct answer is B. Power Options. The Power Options utility in the Control Panel allows you to configure various settings related to how your computer uses and saves power, such as the power plan, the sleep mode, the screen brightness, and the battery status. To access the Power Options utility, you can follow these steps:
? Go to Control Panel > Hardware and Sound > Power Options.
? Click on Change plan settings for the power plan you are using.
? Click on Change advanced power settings.
? Expand the USB settings category and then the USB selective suspend setting subcategory.
? Set the option to Disabled for both On battery and Plugged in.
? Click on OK and then on Save changes.
This will prevent the operating system from suspending the USB devices to save power . System, Devices and Printers, and Ease of Access are not the utilities that should be used to configure the setting. System is a utility that provides information about your computer’s hardware and software, such as the processor, memory, operating system, device manager, and system protection. Devices and Printers is a utility that allows you to view and manage the devices and printers connected to your computer, such as adding or removing devices, changing device settings, or troubleshooting problems. Ease of Access is a utility that allows you to customize your computer’s accessibility options, such as the narrator, magnifier, high contrast, keyboard, mouse, and speech recognition. None of these utilities have any option to configure the USB selective suspend setting.

NEW QUESTION 135
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.

Answer: C

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.

NEW QUESTION 139
A remote user is having issues accessing an online share. Which of the following tools would MOST likely be used to troubleshoot the Issue?

A. Screen-sharing software
B. Secure shell
C. Virtual private network
D. File transfer software

Answer: A

Explanation:
Screen-sharing software is a tool that allows a technician to remotely view and control a user’s screen over the internet. It can be used to troubleshoot issues with accessing an online share, as well as other problems that require visual inspection or guidance. Secure shell (SSH) is a protocol that allows remote access and command execution on another device, but it does not allow screen-sharing. Virtual private network (VPN) is a protocol that creates a secure tunnel between two devices over the internet, but it does not allow remote troubleshooting. File transfer software is a tool that allows transferring files between two devices over the internet, but it does not allow screen- sharing. Verified References: https://www.comptia.org/blog/what-is-screen-sharing- software https://www.comptia.org/certifications/a

NEW QUESTION 144
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 145
A technician is trying to encrypt a single folder on a PC. Which of the following should the technician use to accomplish this task?

A. FAT32
B. exFAT
C. BitLocker
D. EFS

Answer: D

Explanation:
EFS (Encrypting File System) is a feature that allows a user to encrypt a single folder or file on a Windows PC. It uses a public key encryption system to protect the data from unauthorized access. FAT32 and exFAT are file system formats that do not support encryption. BitLocker is a feature that encrypts the entire drive, not a single folder or file. Verified References: https://www.comptia.org/blog/what-is-efs https://www.comptia.org/certifications/a

NEW QUESTION 148
A macOS user is installing a new application. Which of the following system directories is the software MOST likely to install by default?

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

Answer: B

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

NEW QUESTION 152
Once weekly a user needs Linux to run a specific open-source application that is not available for the currently installed Windows platform. The user has limited bandwidth throughout the day. Which of the following solutions would be the MOST efficient, allowing for parallel execution of the Linux application and Windows applications?

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

Answer: B

Explanation:
The user should install and run Linux and the required application as a virtual machine installed under the Windows OS. This solution would allow for parallel execution of the Linux application and Windows applications2.
The MOST efficient solution that allows for parallel execution of the Linux application and Windows applications is to install and run Linux and the required application as a virtual machine installed under the Windows OS. This is because it allows you to run both Linux and Windows together without the need to keep the Linux portion confined to a VM window 3.

NEW QUESTION 153
A company implemented a BYOD policy and would like to reduce data disclosure caused by malware that may infect these devices. Which of the following should the company deploy to address these concerns?

A. UAC
B. MDM

C. LDAP
D. SSO

Answer: B

Explanation:
MDM stands for mobile device management, which is a type of software solution that allows remote management and security of mobile devices. MDM can help a company reduce data disclosure caused by malware that may infect these devices by enforcing security policies, such as encryption, password protection, antivirus software, and remote wipe. MDM can also monitor and control the access of personal devices to corporate data and networks. UAC stands for user account control, which is a feature of Windows that prompts users for permission or an administrator password before making changes that affect the system. UAC may not be effective in preventing malware infection or data disclosure on personal devices. LDAP stands for lightweight directory access protocol, which is a protocol for accessing and managing information stored in a directory service, such as user names and passwords. LDAP does not directly address the issue of malware infection or data disclosure on personal devices. SSO stands for single sign-on, which is a feature that allows users to access multiple applications or services with one set of credentials. SSO may not prevent malware infection or data disclosure on personal devices, and may even increase the risk if the credentials are compromised.
https://www.nist.gov/news-events/news/2021/03/mobile-device-security-bring-your-own-device-byod-draft-sp-1800-22

NEW QUESTION 157
A technician is installing a program from an ISO file. Which of the following steps should the technician take?

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

Answer: A

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

NEW QUESTION 159
A branch office suspects a machine contains ransomware. Which of the following mitigation steps should a technician take first?

A. Disable System Restore.
B. Remediate the system.
C. Educate the system user.
D. Quarantine the system.

Answer: D

Explanation:
The first mitigation step that a technician should take when a machine is suspected to contain ransomware is to quarantine the system. This means isolating the infected machine from the network and other devices, to prevent the ransomware from spreading and encrypting more data. The technician can quarantine the system by disconnecting the network cable, turning off the wireless adapter, or using firewall rules to block the traffic from and to the machine12.
This step is more important than the other options because:
? Disabling System Restore (A) is not a priority, as it will not stop the ransomware from running or spreading. System Restore is a feature that allows users to restore their system to a previous state, but it may not work if the ransomware has encrypted or deleted the restore points. Moreover, disabling System Restore may prevent the user from recovering some data or settings in the future13.
? Remediating the system (B) is the ultimate goal, but it cannot be done before quarantining the system. Remediating the system means removing the ransomware, restoring the data, and fixing the vulnerabilities that allowed the attack. However, this process requires careful analysis, planning, and execution, and it may not be possible if the ransomware is still active and communicating with the attackers. Therefore, the technician should first isolate the system and then proceed with the remediation steps12.
? Educating the system user © is a preventive measure, but it is not a mitigation step. Educating the system user means raising awareness and providing training on how to avoid ransomware attacks, such as by recognizing phishing emails, avoiding suspicious links or attachments, and updating and patching the system regularly. However, this step will not help if the system is already infected, and it may not be effective if the user is not willing or able to follow the best practices. Therefore, the technician should focus on resolving the current incident and then educate the user as part of the recovery plan14.
References:
1: How to Mitigate Ransomware Attacks in 10 Steps - Heimdal Security1 2: 3 steps to prevent and recover from ransomware | Microsoft Security Blog3 3: How to use System Restore on Windows 10 | Windows Central5 4: Ransomware Mitigation | Prevention and Mitigation Strategies - Delinea4

NEW QUESTION 160
An organization's Chief Financial Officer (CFO) is concerned about losing access to very sensitive, legacy unmaintained PII on a workstation if a ransomware outbreak occurs. The CFO has a regulatory requirement to retain this data for many years. Which of the following backup methods would BEST meet the requirements?

A. A daily, incremental backup that is saved to the corporate file server
B. An additional, secondary hard drive in a mirrored RAID configuration
C. A full backup of the data that is stored of site in cold storage
D. Weekly, differential backups that are stored in a cloud-hosting provider

Answer: C

Explanation:
According to CompTIA A+ Core 2 objectives, a full backup stored off-site provides the greatest protection against data loss in the event of a ransomware attack or other data disaster. By storing the backup in a separate physical location, it is less likely to be affected by the same event that could cause data loss on the original system. Cold storage is a term used for data archiving, which typically refers to a long-term storage solution that is used for retaining data that is infrequently accessed, but still needs to be kept for regulatory or compliance reasons.

NEW QUESTION 164
Which of the following Wi-Fi protocols is the MOST secure?

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 167
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

Answer: A

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. References1: BitLocker overview - Windows Security | Microsoft Learn2: Device encryption in Windows - Microsoft Support3: Can You Turn on BitLocker on Windows 10 Home?4: How to enable device encryption on Windows 10 Home

NEW QUESTION 170
A technician needs to ensure that USB devices are not suspended by the operating system. Which of the following Control Panel utilities should the technician use to configure the setting?

A. System
B. Power Options
C. Devices and Printers
D. Ease of Access

Answer: B

Explanation:
Power Options is a Control Panel utility that allows users to configure the power settings of their computer, such as when to turn off the display, when to put the computer to sleep, and how to manage the battery life. Power Options also allows users to configure the USB selective suspend setting, which is a feature that automatically suspends the power supply to USB devices that are not in use, in order to save energy. A user can disable this setting if they want to ensure that USB devices are not suspended by the operating system. System, Devices and Printers, and Ease of Access are not Control Panel utilities that can be used to configure the USB selective suspend setting.

NEW QUESTION 171
A user's Windows computer seems to work well at the beginning of the day. However, its performance degrades throughout the day, and the system freezes when several applications are open. Which of the following should a technician do to resolve the issue? (Select two).

A. Install the latest GPU drivers.
B. Reinstall the OS.
C. Increase the RAM.
D. Increase the hard drive space.
E. Uninstall unnecessary software.
F. Disable scheduled tasks.

Answer: CE

Explanation:
The most likely causes of the user's Windows computer performance degradation and freezing are insufficient RAM and excessive software running in the background. Therefore, the technician should do the following to resolve the issue:
? Increase the RAM. RAM is the memory that the computer uses to store and run applications and processes. If the RAM is not enough to handle the workload, the computer will use the hard drive as a virtual memory, which is much slower and can cause performance issues. Increasing the RAM will allow the computer to run more applications and processes smoothly and avoid freezing. The technician should check the system requirements of the applications that the user needs to run, and install additional RAM modules that are compatible with the motherboard and the existing RAM. The technician should also make sure that the system is managing the page file size automatically, or adjust it manually to optimize the virtual memory usage12.
? Uninstall unnecessary software. Software that the user does not need or use can take up valuable disk space and system resources, and can interfere with the performance of other applications. Some software may also run in the background or start automatically when the computer boots up, which can slow down the system and cause freezing. The technician should help the user to identify and uninstall unnecessary software from the control panel or the settings app, and disable unnecessary startup programs from the task manager or the system configuration tool. The technician should also check for and remove viruses and malware that may affect the system performance134.
References:
1: Tips to improve PC performance in Windows - Microsoft Support1 2: How to Upgrade or Install RAM on Your Windows PC - Lifewire5 3: How to Uninstall Programs on Windows 10
- PCMag6 4: How to Fix a Windows Computer that Hangs or Freezes - wikiHow

NEW QUESTION 172
Which of the following would most likely be used in a small office environment?

A. Print server
B. Virtualization
C. Domain access
D. Workgroup

Answer: D

Explanation:
A workgroup is a network configuration that allows computers to communicate and share resources with each other without requiring a centralized server or domain controller. A workgroup is suitable for small office environments where there are only a few computers and users who need simple file and printer sharing. A workgroup does not have centralized management or security policies, which may be desirable for larger or more complex networks. Print server, virtualization, and domain access are not network configurations that are most likely used in a small office environment.

NEW QUESTION 175
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.

Answer: B

Explanation:
To change the desktop wallpaper on a Windows 10 computer using a Windows 10 Settings tool, the user should open Settings, select Personalization, click Browse, and then locate and open the image the user wants to use as the wallpape1r https://www.lifewire.com/change-desktop-background-windows-11-5190733

NEW QUESTION 176
A user installed a new computer game. Upon starting the game, the user notices the frame rates are low. Which of the following should the user upgrade to resolve the issue?

A. Hard drive
B. Graphics card
C. Random-access memory
D. Monitor

Answer: B

Explanation:
A graphics card, also known as a video card or a GPU (graphics processing unit), is a component that can affect the performance of a computer game. A graphics card is responsible for rendering and displaying graphics on the screen, such as images, animations, and effects. A computer game may require a high level of graphics processing power to run smoothly and achieve high frame rates, which are the number of frames per second (FPS) that the game can display. Upgrading to a better graphics card can improve the performance of a computer game by increasing its graphics quality and frame rates. Hard drive, random-access memory, and monitor are not components that can directly
improve the performance of a computer game.

NEW QUESTION 180
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 184
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.

Answer: D

Explanation:
The issue is specific to the user's profile, so the technician should rebuild the
profile. Rebuilding the profile will create a new profile and transfer the user's data to the new profile1

NEW QUESTION 189
A technician is working on a Windows 10 PC that has unwanted applications starting on boot. Which of the following tools should the technician use to disable applications on startup?

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 192
A technician is working on a way to register all employee badges and associated computer IDs. Which of the following options should the technician use in order to achieve this objective?

A. Database system
B. Software management
C. Active Directory description
D. Infrastructure as a Service

Answer: A

Explanation:
A database system is a software application that allows storing, organizing, and managing data in a structured way. A database system can be used to register all employee badges and associated computer IDs by creating a table or a record for each employee that contains their badge number, computer ID, name, and other relevant information. A database system can also facilitate searching, updating, and deleting data as needed. Software management is a general term that refers to the process of planning, developing, testing, deploying, and maintaining software applications. It does not directly address the issue of registering employee badges and computer IDs. Active Directory description is a field in Active Directory that can be used to store additional information about an object, such as a user or a computer. It is not a software application that can be used to register employee badges and computer IDs by itself. Infrastructure as a Service (IaaS) is a cloud computing model that provides servers, storage, networking, and software over the internet. It does not directly address the issue of registering employee badges and computer IDs either.
https://www.idcreator.com/
https://www.alphacard.com/photo-id-systems/card-type/employee-badges

NEW QUESTION 197
A technician needs to establish a remote access session with a user who has a Windows workstation. The session must allow for simultaneous viewing of the workstation by both the user and technician. Which of the following remote access technologies should be used?

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

Answer: D

Explanation:
MSRA (Microsoft Remote Assistance) is a remote access technology that allows a technician to establish a session with a user who has a Windows workstation. The session allows for simultaneous viewing of the workstation by both the user and technician, as well as remote control and file transfer capabilities. RDP (remote desktop protocol) is another remote access technology, but it does not allow simultaneous viewing by default. VPN (virtual private network) and SSH (secure shell) are protocols that create secure tunnels between two devices over the internet, but they do not allow remote access sessions. Verified References: https://www.comptia.org/blog/what-is-msra https://www.comptia.org/certifications/a

NEW QUESTION 201
Which of the following should be used to secure a device from known exploits?

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

Answer: C

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

NEW QUESTION 204
A change advisory board authorized a setting change so a technician is permitted to implement the change. The technician successfully implemented the change. Which of the following should be done NEXT?

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

Answer: A

Explanation:
After implementing a change authorized by the change advisory board (CAB), the technician should document the date and time of change as part of the post-implementation review. This helps to track the change history, verify the success of the change, and identify any issues or incidents caused by the change1. Documenting the purpose of the change, the risk level, and the findings of the sandbox test are all part of the pre-implementation activities that should be done before submitting the change request to the CAB2.
References: 2: https://www.manageengine.com/products/service-desk/itil-change-management/cab-change-advisory-board.html 1: https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/success/quick-answer/change-advisory-board-setup.pdf

NEW QUESTION 207
A PC is taking a long time to boot Which of the following operations would be best to do to resolve the issue at a minimal expense? (Select two).

A. Installing additional RAM
B. Removing the applications from startup
C. Installing a faster SSD
D. Running the Disk Cleanup utility
E. Defragmenting the hard drive
F. Ending the processes in the Task Manager

Answer: BD

Explanation:
The best operations to do to resolve the issue of a long boot time at a minimal expense are B. Removing the applications from startup and D. Running the Disk Cleanup utility. These are two simple and effective ways to speed up your PC's boot time without spending any money on hardware upgrades.
Removing the applications from startup means preventing unnecessary programs from launching automatically when you turn on your computer. This can reduce the load on your system resources and make the boot process faster. You can do this in Windows 10 by pressing Ctrl + Alt + Esc to open the Task Manager, and going to the Startup tab. There, you can see a list of programs that start with your computer, and their impact on the startup performance. You can disable any program that you don't need by right-clicking on it and choosing Disable12.
Running the Disk Cleanup utility means deleting temporary files, system files, and other unnecessary data that may be taking up space and slowing down your computer. This can free up some disk space and improve the performance of your system. You can do this in Windows 10 by typing disk cleanup in the search box and selecting the Disk Cleanup app. There, you can choose which files you want to delete, such as Recycle Bin, Temporary Internet Files, Thumbnails, etc. You can also click on Clean up system files to delete more files, such as Windows Update Cleanup, Previous Windows installation(s), etc34.

NEW QUESTION 212
An Internet cafe has several computers available for public use. Recently, users have reported the computers are much slower than they were the previous week. A technician finds the CPU is at 100% utilization, and antivirus scans report no current infection. Which of the following is MOST likely causing the issue?

A. Spyware is redirecting browser searches.
B. A cryptominer is verifying transactions.
C. Files were damaged from a cleaned virus infection.
D. A keylogger is capturing user passwords.

Answer: B

Explanation:
A cryptominer is a malicious program that uses the CPU resources of a computer to generate cryptocurrency, such as Bitcoin or Ethereum. This can cause the CPU to run at 100% utilization and slow down the system. Spyware, virus and keylogger are other types of malware, but they do not necessarily cause high CPU usage. Verified References: https://www.comptia.org/blog/what-is-cryptomining https://www.comptia.org/certifications/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 220
Which of the following is used to integrate Linux servers and desktops into Windows Active Directory environments?

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

Answer: C

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

NEW QUESTION 225
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 227
A Microsoft Windows PC needs to be set up for a user at a targe corporation. The user will need access to the corporate domain to access email and shared drives. Which of the following versions of Windows would a technician MOST likely deploy for the user?

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

Answer: B

Explanation:
The Windows Professional Edition is the most likely version that a technician would deploy for a user at a target corporation. This version of Windows is designed for business use and provides the necessary features and capabilities that a user would need to access the corporate domain, such as email and shared drives.

NEW QUESTION 229
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 234
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

Answer: B

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.

NEW QUESTION 236
During a network outage, a technician discovers a new network switch that was not listed in the support documentation. The switch was installed during a recent change window when a new office was added to the environment. Which of the following would most likely prevent this type of mismatch after next month's change window?

A. Performing annual network topology reviews
B. Requiring all network changes include updating the network diagrams
C. Allowing network changes once per year
D. Routinely backing up switch configuration files

Answer: B

Explanation:
This would ensure that the support documentation reflects the current state of the network and prevents any confusion or mismatch during a network outage. Updating the network diagrams is also one of the best practices for network documentation, as stated in the Official CompTIA A+ Core 2 Study Guide1. The other options are not as effective or feasible as option B. Performing annual network topology reviews is too infrequent and may not capture recent changes. Allowing network changes once per year is too restrictive and may not meet the business needs. Routinely backing up switch configuration files is important, but it does not help with identifying new switches or devices on the network.

NEW QUESTION 240
A user is attempting to make a purchase at a store using a phone. The user places the phone on the payment pad, but the device does not recognize the phone. The user attempts to restart the phone but still has the same results. Which of the following should the user do to resolve the issue?

A. Turn off airplane mode while at the register.
B. Verify that NFC is enabled.
C. Connect to the store's Wi-Fi network.
D. Enable Bluetooth on the phone.

Answer: B

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

NEW QUESTION 241
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 244
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 vmgm
D. msc
E. diskmgmt.msc

Answer: C

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

NEW QUESTION 249
A department manager submits a help desk ticket to request the migration of a printer's port utilization from USB to Ethernet so multiple users can access the printer. This will be a new network printer; thus a new IP address allocation is required. Which of the following should happen immediately before network use is authorized?

A. Document the date and time of the change.
B. Submit a change request form.
C. Determine the risk level of this change.
D. Request an unused IP address.

Answer: D

Explanation:
An IP address is a unique identifier that allows a device to communicate with other devices on a network. A network printer needs an IP address to be accessible by multiple users on the network. Requesting an unused IP address from the network administrator or using an IP address scanner is the step that should happen immediately before network use is authorized, as it ensures that there is no IP address conflict or duplication on the network. Documenting the date and time of the change, submitting a change request form, and determining the risk level of this change are steps that should happen before requesting an unused IP address.

NEW QUESTION 251
A user is setting up backups on a workstation. The user wants to ensure that the restore process is as simple as possible. Which of the following backup types should the user select?

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

Answer: A

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

NEW QUESTION 252
Which of the following does MFA provide?
? Security enhancement
? Encryption
? Digital signature

A. Public key infrastructure

Answer: A

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

NEW QUESTION 254
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

Answer: BE

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.

NEW QUESTION 258
Which of the following is the MOST cost-effective version of Windows 10 that allows remote access through Remote Desktop?

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

Answer: D

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

NEW QUESTION 261
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 262
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?

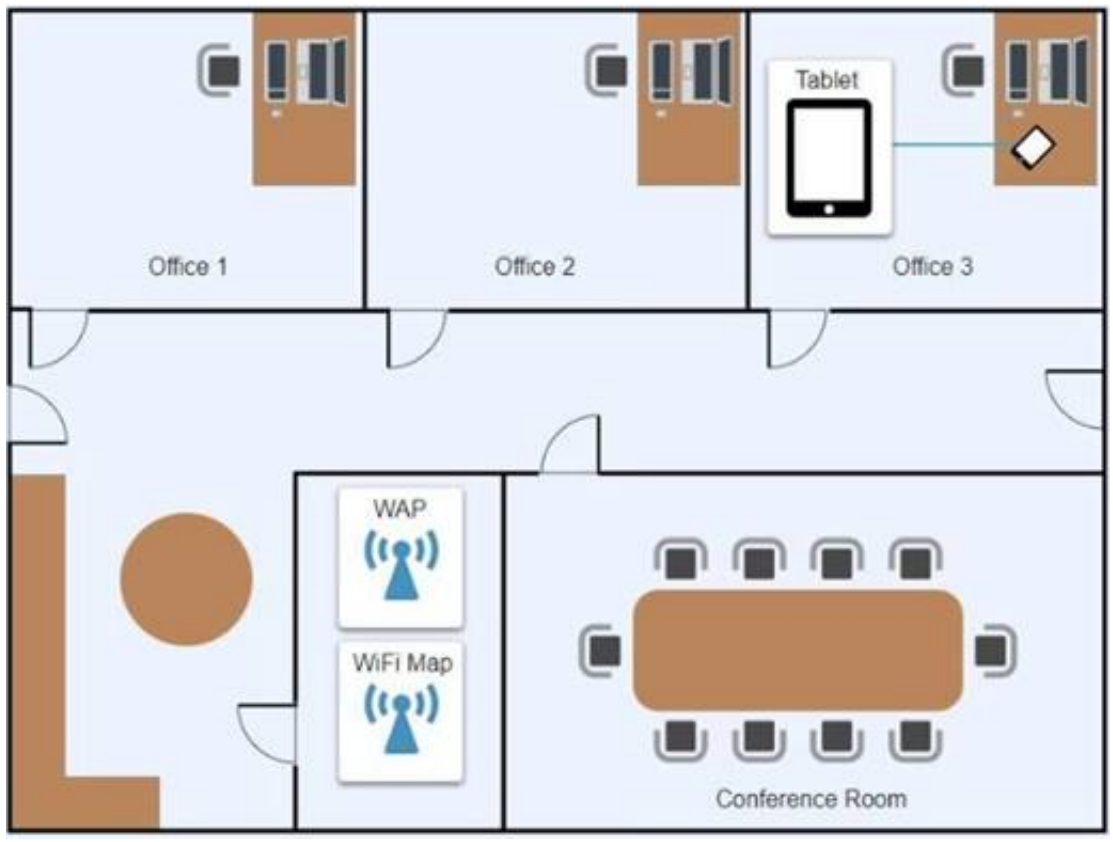
A. Requiring employees to enter their usernames and passwords
B. Setting up facial recognition for each employee
C. Using a PIN and providing it to employees
D. Requiring employees to use their fingerprints

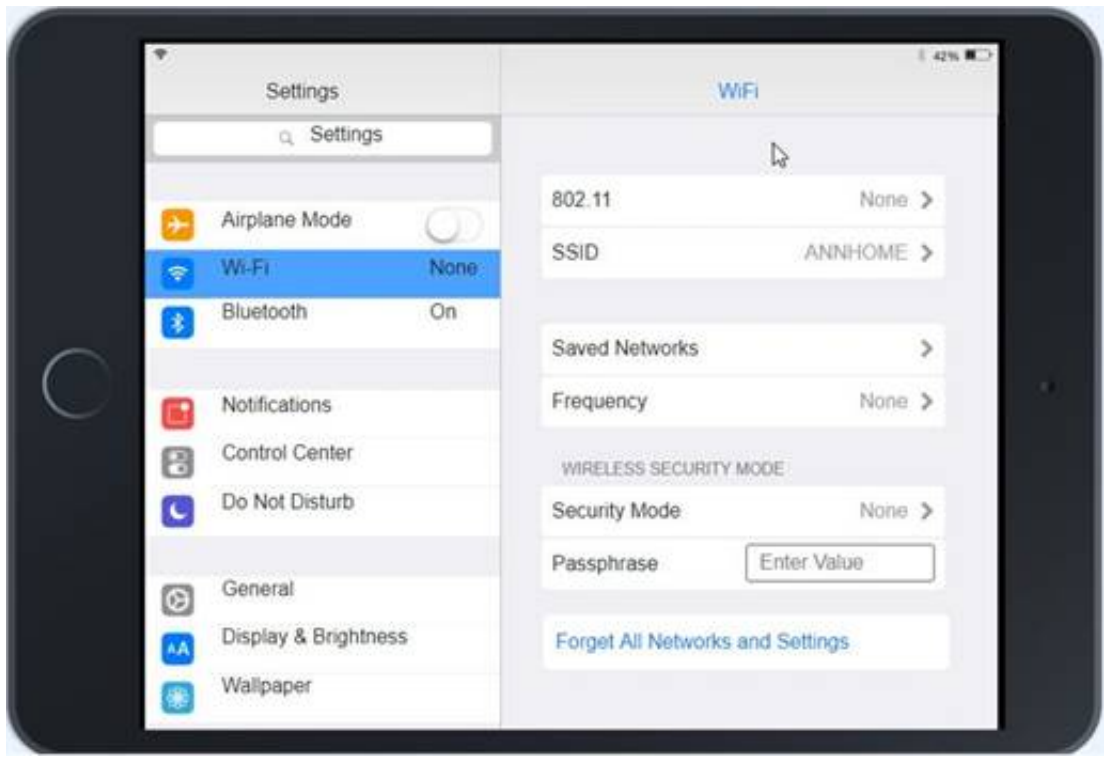
Answer: C

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.
References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 3.3

NEW QUESTION 263
SIMULATION
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

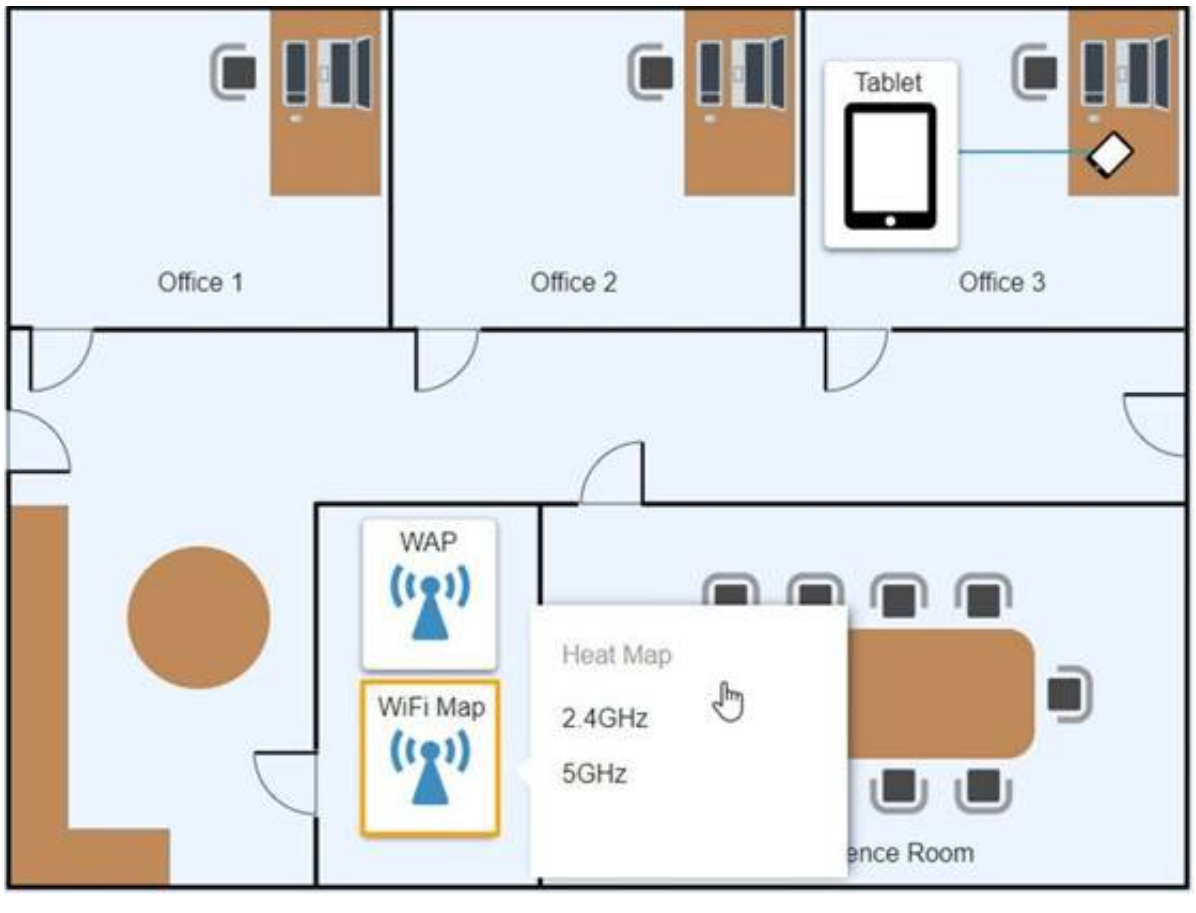

Settings
WiFi
Settings
Airplane Mode
Wi-Fi None
Bluetooth On
Notifications
Control Center
Do Not Disturb
General
Display & Brightness
Wallpaper
802.11 None
SSID ANNHOME
Saved Networks
Frequency None
WIRELESS SECURITY MODE
Security Mode None
Passphrase Enter Value
Forget All Networks and Settings


Settings
Wi-Fi 802.11
Settings
Airplane Mode
Wi-Fi None
Bluetooth On
Notifications
Control Center
Do Not Disturb
General
Display & Brightness
Wallpaper
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
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
Security Mode
OPEN
WEP
WPA
WPA2

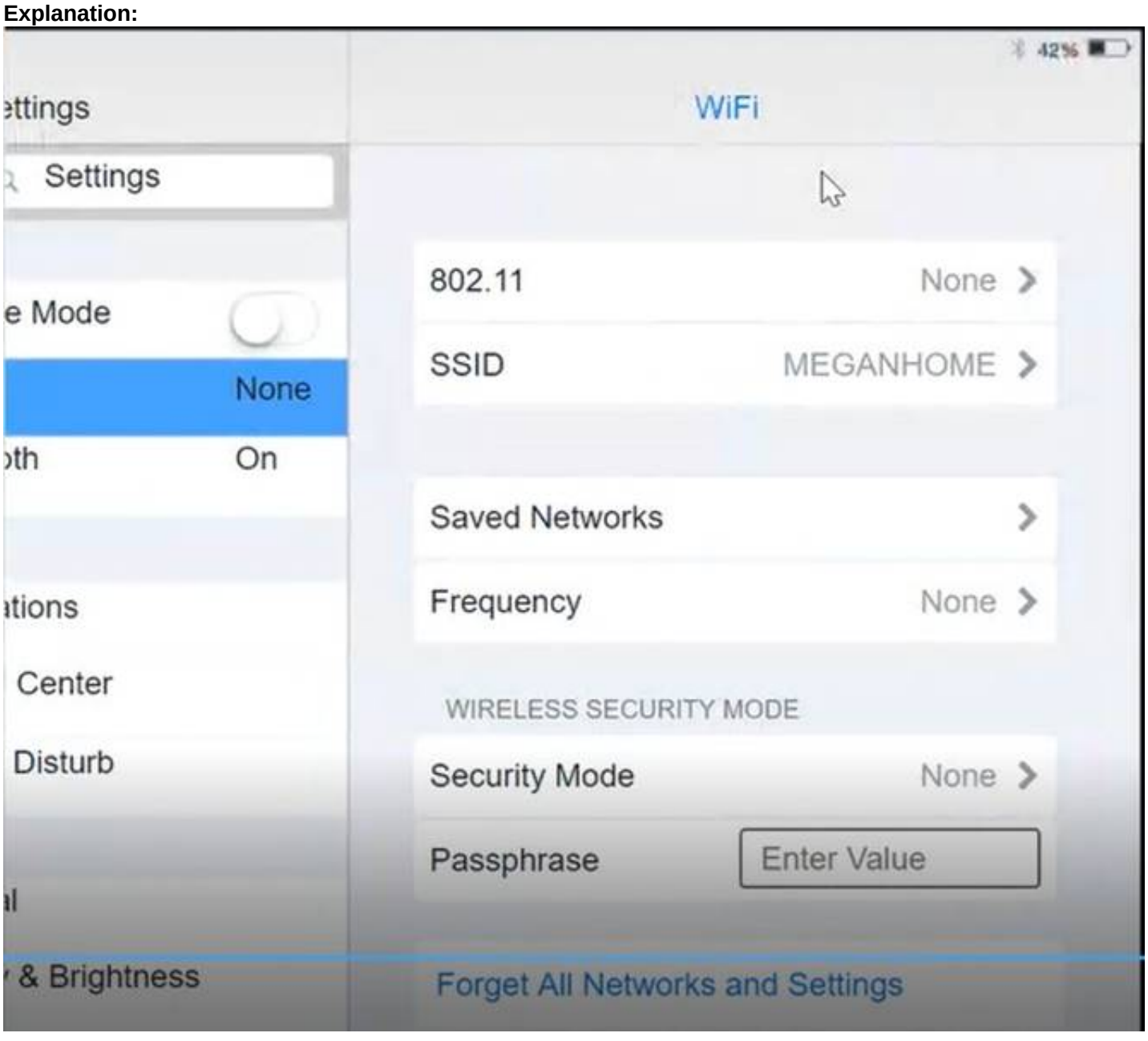

Settings
Site
Wireless Networks
Networks
Guest Control
Admins
User Groups
VOIP
Controller
Cloud Access
Maintenance
Wireless Networks
SSID
Frequency
Security
Totally Secure!
CORP
2.4GHz/5GHz
WPA2
Corpsecure1
BYOD
2.4GHz/5GHz
WPA-PSK
TotallySecure!
Create New Wireless Network



A. Mastered
B. Not Mastered

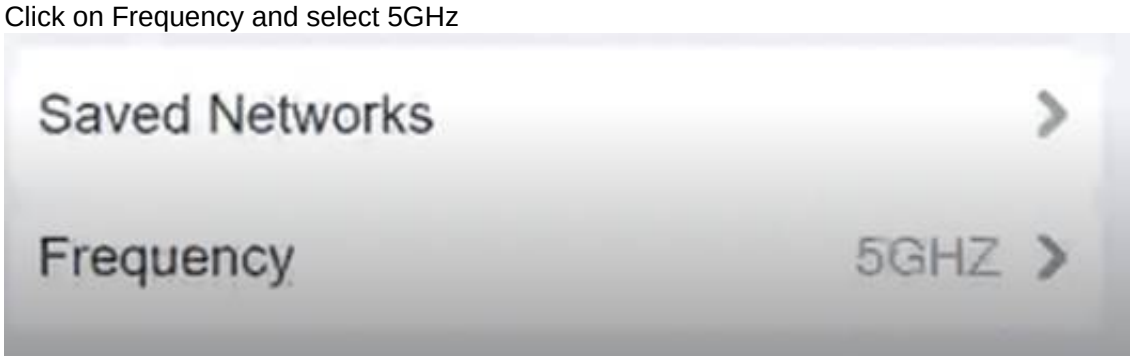
Answer: A

Explanation:



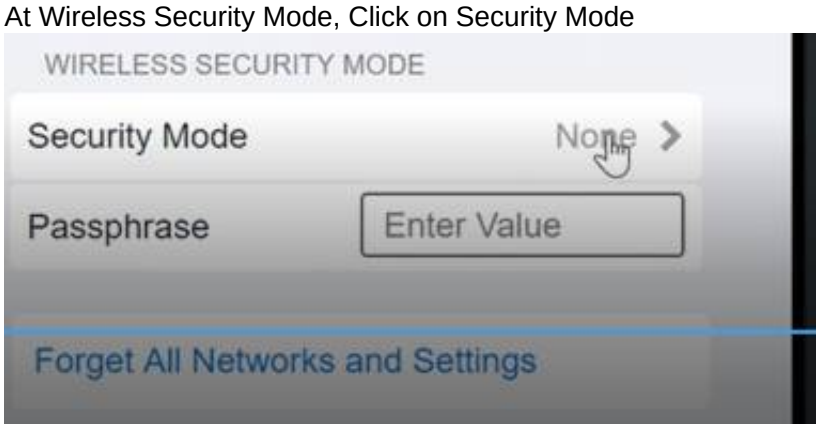
Graphical user interface, application
Description automatically generated
Click on 802.11 and Select ac

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

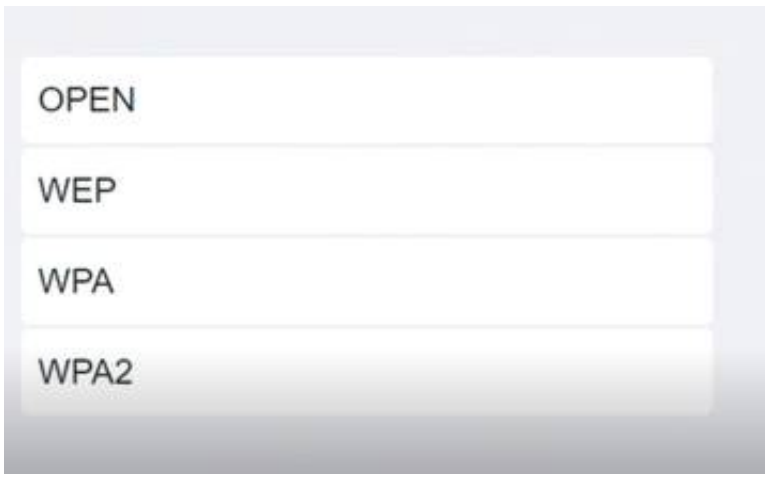


Graphical user interface, text, application, Teams
Description automatically generated
Click on Frequency and select 5GHz

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 267
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

220-1102 Practice Exam Features:

* 220-1102 Questions and Answers Updated Frequently

* 220-1102 Practice Questions Verified by Expert Senior Certified Staff

* 220-1102 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 220-1102 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year