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

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

Answer: C

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

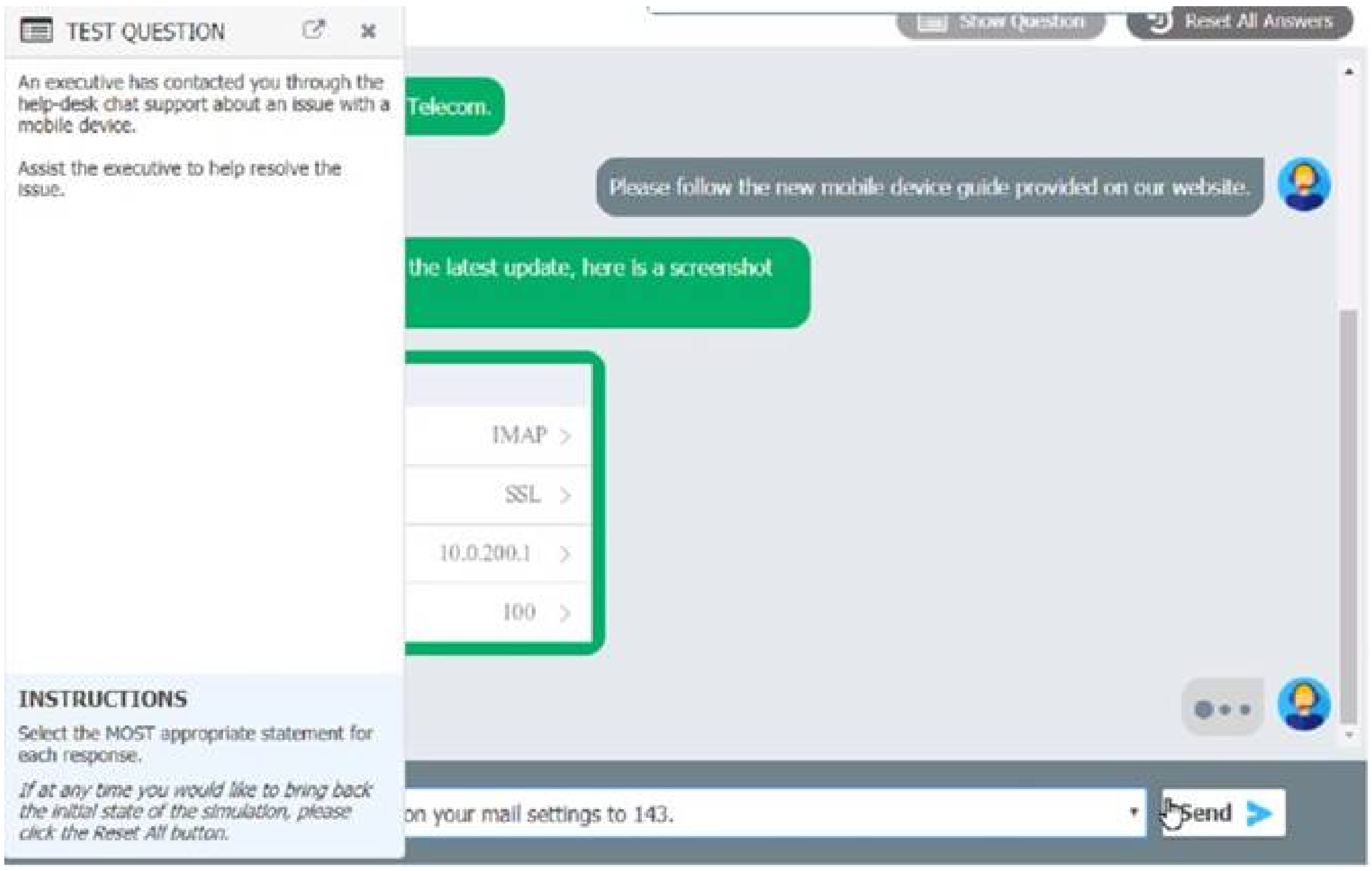
NEW QUESTION 3
Which of the following is the MOST basic version of Windows that includes BitLocker?

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

Answer: D

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

NEW QUESTION 4
An executive has contacted you through the help-desk chat support about an issue with a mobile device.
Assist the executive to help resolve the issue.



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

Assist the executive to help resolve the issue.

Telecom.

Please follow the new mobile device guide provided on our website.

the latest update, here is a screenshot

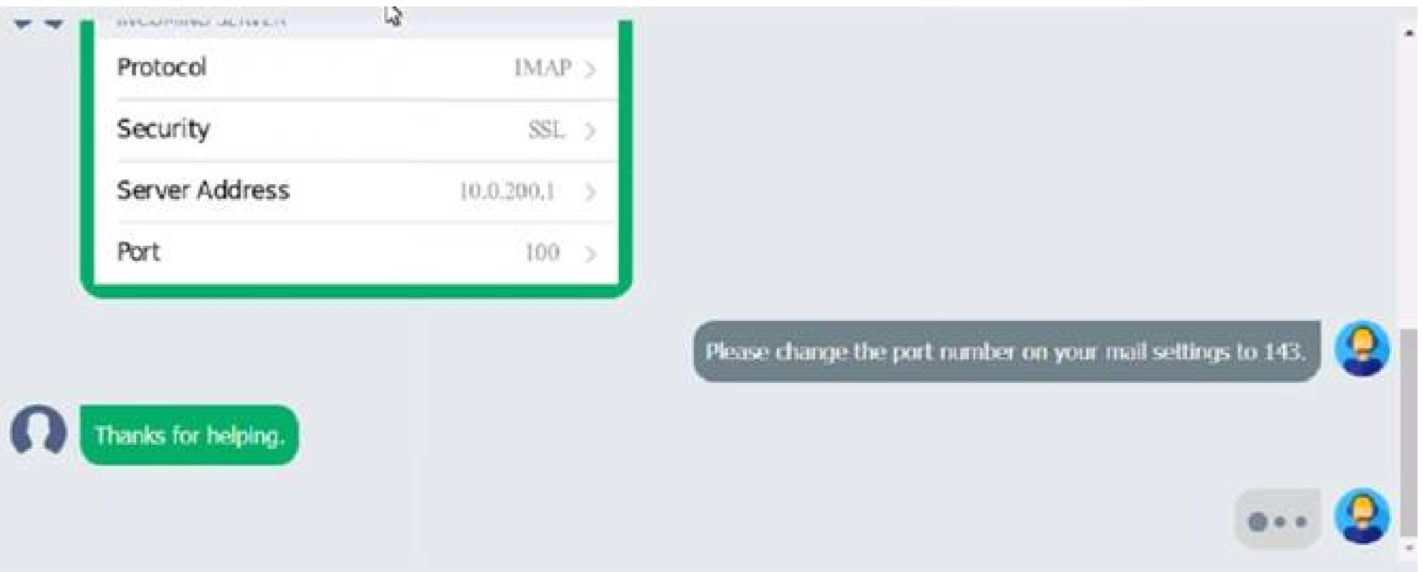
IMAP
SSL
10.0.200.1
100

INSTRUCTIONS

Select the MOST appropriate statement for each response.

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

on your mail settings to 143.



Protocol	IMAP
Security	SSL
Server Address	10.0.200.1
Port	100

Please change the port number on your mail settings to 143.

Thanks for helping.

Which of the following should be done NEXT?

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

Answer: A

NEW QUESTION 5
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
macOS
C.
D: Windows

Answer: B

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

NEW QUESTION 6
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 7
A technician installs specialized software on a workstation. The technician then attempts to run the software. The workstation displays a message indicating the software is not authorized to run. Which of the following should the technician do to most likely resolve the issue?

A. Install the software in safe mode.
B. Attach the external hardware token.
C. Install OS updates.
D. Restart the workstation after installation.

Answer: B

Explanation:
A hardware token is a physical device that provides an additional layer of security for software authorization. Some specialized software may require a hardware token to be attached to the workstation in order to run. A hardware token may contain a cryptographic key, a password, or a one-time code that verifies the user's identity or permission. Installing the software in safe mode, installing OS updates, and restarting the workstation after installation are not likely to resolve the issue of software authorization.

NEW QUESTION 8
A user calls the help desk to report that Windows installed updates on a laptop and rebooted overnight. When the laptop started up again, the touchpad was no longer working. The technician thinks the software that controls the touchpad might be the issue. Which of the following tools should the technician use to make adjustments?

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

Answer: D

Explanation:
The technician should use devmgmt.msc tool to make adjustments for the touchpad issue after Windows installed updates on a laptop. Devmgmt.msc is a command that opens the Device Manager, which is a utility that allows users to view and manage the hardware devices and drivers installed on a computer. The technician can use the Device Manager to check the status, properties and compatibility of the touchpad device and its driver, and perform actions such as updating, uninstalling or reinstalling the driver, enabling or disabling the device, or scanning for hardware changes. Eventvwr.msc is a command that opens the Event Viewer, which is a utility that allows users to view and monitor the system logs and events. The Event Viewer may provide some information or clues about the touchpad issue, but it does not allow users to manage or troubleshoot the device or its driver directly. Perfmon.msc is a command that opens the Performance Monitor, which is a utility that allows users to measure and analyze the performance of the system

NEW QUESTION 9
A user added a second monitor and wants to extend the display to it. In which of the following Windows settings will the user MOST likely be able to make this change?

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 10
A technician is preparing to remediate a Trojan virus that was found on a workstation. Which of the following steps should the technician complete BEFORE removing the virus?

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

Answer: A

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

NEW QUESTION 10

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

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

Answer: B

Explanation:
The most likely reason that the system is not utilizing all the available RAM is that it is running a 32-bit OS. A 32-bit OS can only address up to 4GB of RAM, and some of that is reserved for hardware and system use1. Therefore, even if the technician installed 8GB of RAM, the system can only use around 3.5GB of usable RAM. To use the full 8GB of RAM, the technician would need to install a 64-bit OS, which can address much more memory2. The system missing updates, the system's memory failing, or the system requiring BIOS updates are not likely to cause this issue.
References: 2: https://support.microsoft.com/en-us/windows/windows-10-system-requirements-6d4e9a79-66bf-7950-467c-795cf0386715 1: https://www.makeuseof.com/tag/unlock-64gb-ram-32-bit-windows-pae-patch/

NEW QUESTION 12
A technician installed a new application on a workstation. For the program to function
properly, it needs to be listed in the Path Environment Variable. Which of the following Control Panel utilities should the technician use?

A. System
B. Indexing Options
C. Device Manager
D. Programs and Features

Answer: A

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

NEW QUESTION 14
An administrator has submitted a change request for an upcoming server deployment. Which of the following must be completed before the change can be approved?

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

Answer: A

Explanation:
Risk analysis is the process of identifying and evaluating the potential threats and impacts of a change on the system, network, or service. It is an essential step before approving a change request, as it helps to determine the level of risk, the mitigation strategies, and the contingency plans. Risk analysis also helps to prioritize the change requests based on their urgency and importance12.
References: 1 The Change Request Process and Best Practices(https://www.processmaker.com/blog/it-change-request-process-best- practices/)2 Risk Assessment and Analysis Methods: Qualitative and Quantitative(https://www.isaca.org/resources/isaca-journal/issues/2021/volume-2/risk- assessment-and-analysis-methods).

NEW QUESTION 17
A small-office customer needs three PCs to be configured in a network with no server. Which of the following network types is the customer's BEST choice for this environment?

A. Mastered
B. Not Mastered

Answer: A

Explanation:
A workgroup network is a peer-to-peer network where each PC can share files and resources with other PCs without a central server. A public network is a network that is accessible to anyone on the internet. A wide area network is a network that spans a large geographic area, such as a country or a continent. A domain network is a network where a server controls the access and security of the PCs. Verified References: https://www.comptia.org/blog/network-types https://www.comptia.org/certifications/a

NEW QUESTION 22
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 27
An Android user contacts the help desk because a company smartphone failed to complete a tethered OS update A technician determines there are no error messages on the device Which of the following should the technician do NEXT?

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

Answer: C

Explanation:
Since there are no error messages on the device, the technician should check if the battery is sufficiently charge1d
If the battery is low, the device may not have enough power to complete the update2
In this scenario, the technician has already determined that there are no error messages on the device. The next best step would be to check if the battery is sufficiently charged. If the battery is low, it could be preventing the device from completing the update process. Verifying that third-party applications are disabled, determining if the device has adequate storage available, and confirming a strong internet connection are all important steps in troubleshooting issues with mobile devices. However, since the problem in this scenario is related to a failed OS update, it is important to first check the battery level before proceeding with further troubleshooting steps.

NEW QUESTION 32
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 and other secure information across your devices using iCloud Keychain1. Keychain can be used as a password manager in macOS to help you keep track of and protect your passwords. References: 1: Manage passwords using keychains on Mac (https://support.apple.com/guide/mac-help/use-keychains-to-store-passwords- mchlf375f392/mac)

NEW QUESTION 36
The courts determined that a cybercrimes case could no longer be prosecuted due to the agency's handling of evidence. Which of the following was MOST likely violated during the investigation?

A. Open-source software
B. EULA
C. Chain of custody
D. AUP

Answer: C

Explanation:
Chain of custody is a process that documents how evidence is collected, handled, stored and transferred during a cybercrime investigation. It ensures that the evidence is authentic, reliable and admissible in court. If the chain of custody is violated during an investigation, it can compromise the integrity of the evidence and lead to the case being dismissed. Open-source software, EULA (end-user license agreement) and AUP (acceptable use policy) are not related to cybercrime investigations or evidence handling. Verified References: https://www.comptia.org/blog/what-is-chain-of-custody https://www.comptia.org/certifications/a

NEW QUESTION 40
A technician is modifying the default home page of all the workstations in a company. Which of the following will help to implement this change?

A. Group Policy
B. Browser extension
C. System Configuration
D. Task Scheduler

Answer: A

Explanation:

Group Policy is a feature of Windows that allows administrators to centrally manage and configure the settings of computers and users in a domain network. Group Policy can be used to modify the default home page of all the workstations in a company by creating and applying a policy that specifies the desired URL for the home page. This way, the change will be automatically applied to all the workstations that are joined to the domain and receive the policy.

NEW QUESTION 41
Which of the following would MOST likely be deployed to enhance physical security for a building? (Select TWO).

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

Answer: BE

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

NEW QUESTION 46
A company needs employees who work remotely to have secure access to the corporate intranet. Which of the following should the company implement?

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

Answer: C

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

NEW QUESTION 50
A technician has verified a computer is infected with malware. The technician isolates the system and updates the anti-malware software. Which of the following should the technician do next?

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Malware is malicious software that can cause damage or harm to a computer system or network4. A technician has verified a computer is infected with malware by observing unusual behavior, such as slow performance, pop-ups, or unwanted ads. The technician isolates the system and updates the anti-malware software to prevent further infection or spread of the malware. The next step is to run repeated remediation scans until the malware is removed. A remediation scan is a scan that detects and removes malware from the system. Running one scan may not be enough to remove all traces of malware, as some malware may hide or regenerate itself.

NEW QUESTION 55
A company is looking lot a solution that provides a backup for all data on the system while providing the lowest impact to the network. Which of the following backup types will the company MOST likely select?

A. Off-site
B. Synthetic
C. Full
D. Differential

Answer: B

Explanation:
A synthetic backup is a backup type that provides a backup for all data on the system while providing the lowest impact to the network. It combines a full backup with one or more incremental backups to create a single backup set, without requiring access to the original data source. Off-site is a backup location, not a backup type. Full and differential are backup types, but they have a higher impact on the network than synthetic. Verified References:

https://www.comptia.org/blog/what-is-a-synthetic-backup https://www.comptia.org/certifications/a

NEW QUESTION 59
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 61
While trying to repair a Windows 10 OS, a technician receives a prompt asking for a key. The technician tries the administrator password, but it is rejected. Which of the following does the technician need in order to continue the OS repair?

A. SSL key
B. Preshared key
C. WPA2 key
D. Recovery key

Answer: D

Explanation:
A recovery key is a code that can be used to unlock a BitLocker-encrypted drive when the normal authentication methods (such as password or PIN) are not available or have been forgotten. BitLocker is a feature of Windows that encrypts the entire drive to protect data from unauthorized access. If a technician is trying to repair a Windows 10 OS that has BitLocker enabled, they will need the recovery key to access the drive and continue the OS repair. SSL key, preshared key, and WPA2 key are not keys that are related to BitLocker or OS repair.

NEW QUESTION 63
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 64
An IT security team is implementing a new Group Policy that will return a computer to the login after three minutes. Which of the following BEST describes the change in policy?

A. Login times
B. Screen lock
C. User permission
D. Login lockout attempts

Answer: B

Explanation:
Screen lock is a feature that returns a computer to the login screen after a period of inactivity, requiring the user to enter their credentials to resume their session. Screen lock can be configured using Group Policy settings, such as Screen saver timeout and Interactive logon: Machine inactivity limit. Screen lock can help prevent unauthorized access to a computer when the user is away from their desk. Login times are not a feature that returns a computer to the login screen, but a measure of how long it takes for a user to log in to a system. User permission is not a feature that returns a computer to the login screen, but a set of rights and privileges that determine what a user can do on a system. Login lockout attempts are not a feature that returns a computer to the login screen, but a security policy that locks out a user account after a number of failed login attempts. https://woshub.com/windows-lock-screen-after-idle-via-gpo/

NEW QUESTION 68
A company is experiencing a DDoS 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. Ransomware
F. Spyware

Answer: AD

Explanation:
Zombies and botnets are terms that describe the types of infections that can cause internal workstations to participate in a DDoS (distributed denial-of-service) attack. A DDoS attack is a malicious attempt to disrupt the normal functioning of a website or a network by overwhelming it with a large amount of traffic from multiple sources. Zombies are infected computers that are remotely controlled by hackers without the owners' knowledge or consent. Botnets are networks of zombies that are coordinated by hackers to launch DDoS attacks or other malicious activities. Keylogger, adware, ransomware, and spyware are not types of infections that can cause internal workstations to participate in a DDoS attack.

NEW QUESTION 70
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 74
Which of the following should be documented to ensure that the change management plan is followed?

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

Answer: A

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

NEW QUESTION 77
A new employee was hired recently. Which of the following documents will the new employee need to sign before being granted login access to the network?

A. Mastered

B. Not Mastered

Answer: A

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

NEW QUESTION 80
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
System
B.
C. Troubleshooting
D. Device Manager
E. Administrative Tools

Answer: D

NEW QUESTION 81
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 85
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 87
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 has taken the appropriate action by not taking the call and setting the phone to silent in order to avoid any distractions and remain focused on the task at hand. This is a good example of how to maintain focus and productivity when working on a customer's PC, and will help to ensure that the job is completed in a timely and efficient manner.

NEW QUESTION 89
A user wants to set up speech recognition on a PC. In which of the following Windows Settings tools can the user enable this option?

A. Language
B. System

C. Personalization
D. Ease of Access

Answer: D

Explanation:
The user can enable speech recognition on a PC in the Ease of Access settings tool. To set up Speech Recognition on a Windows PC, the user should open Control Panel, click on Ease of Access, click on Speech Recognition, and click the Start Speech Recognition link. Language settings can be used to change the language of the speech recognition feature, but they will not enable the feature. System settings can be used to configure the hardware and software of the PC, but they will not enable the speech
recognition feature. Personalization settings can be used to customize the appearance and behavior of the PC, but they will not enable the speech recognition feature1
Open up ease of access, click on speech, then there is an on and off button for speech recognition.

NEW QUESTION 92
A user's computer unexpectedly shut down immediately after the user plugged in a USB headset. Once the user turned the computer back on, everything was functioning properly, including the headset. Which of the following Microsoft tools would most likely be used to determine the root cause?

A. Event Viewer
B. System Configuration
C. Device Manager
D. Performance Monitor

Answer: A

Explanation:
Event Viewer is a Microsoft tool that records and displays system events, errors, warnings, and information. Event Viewer can help troubleshoot and diagnose problems, such as unexpected shutdowns, by showing the details of what happened before, during, and after the incident. Event Viewer can also show the source of the event such as an application, a service, a driver, or a hardware device. By using Event Viewer, a technician can identify the root cause of the unexpected shutdown, such as a power failure, a thermal event, a driver conflict, or a malware infection.

NEW QUESTION 97
A user received the following error upon visiting a banking website:
The security presented by website was issued a different website' s address . A technician should instruct the user to:

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

Answer: A

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

NEW QUESTION 101
A user reports a workstation has been performing strangely after a suspicious email was opened on it earlier in the week. Which of the following should the technician perform FIRST?

A. 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 103
A user reports that the hard drive activity light on a Windows 10 desktop computer has been steadily lit for more than an hour, and performance is severely degraded. Which of the following tabs in Task Manager would contain the information a technician would use to identify the cause of this issue?

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

Answer: B

Explanation:
Processes tab in Task Manager would contain the information a technician would use to identify the cause of this issue. The Processes tab in Task Manager displays all the processes running on the computer, including the CPU and memory usage of each process. The technician can use this tab to identify the process that is causing the hard drive activity light to remain lit and the performance degradation1

NEW QUESTION 108
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 111
Which of the following operating systems is most commonly used in embedded systems?

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

Answer: D

Explanation:
Linux is the most commonly used operating system in embedded systems because it is open source, free, customizable, and supports a wide range of architectures and devices. Linux also offers many advantages for embedded development, such as real- time capabilities, modularity, security, scalability, and reliability. Linux can run on embedded systems with limited resources, such as memory, storage, or power, and can be tailored to the specific needs of the application. Linux also has a large and active community of developers and users who contribute to its improvement and
innovation. Some examples of embedded systems that use Linux are smart TVs, routers,
drones, robots, smart watches, and IoT devices

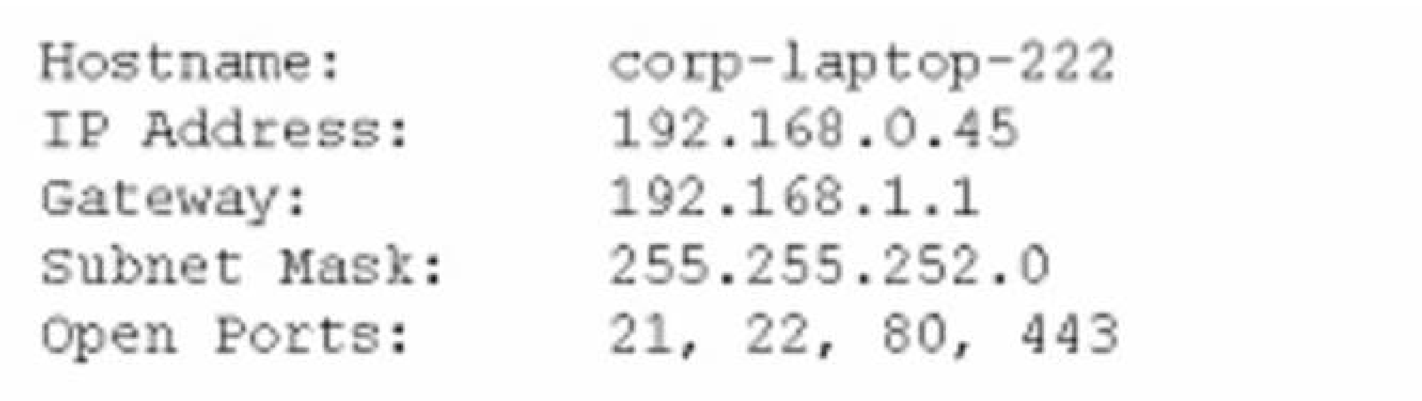
NEW QUESTION 113
A technician is hardening a company file server and needs to prevent unauthorized LAN devices from accessing stored files. Which of the following should the technician use?

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 115
A technician is trying to connect to a user's laptop in order to securely install updates. Given the following information about the laptop:



```
Hostname:           corp-laptop-222
IP Address:         192.168.0.45
Gateway:            192.168.1.1
Subnet Mask:        255.255.252.0
Open Ports:         21, 22, 80, 443
```

Which of the following should the technician do to connect via RDP?

A. Confirm the user can ping the default gateway.
B. Change the IP address on the user's laptop.
C. Change the subnet mask on the user's laptop.
D. Open port 3389 on the Windows firewall.

Answer: D

Explanation:
In order to connect to a user's laptop via RDP, the technician should open port 3389 on the Windows firewall. This is because RDP uses port 3389 for communication12. The other options are not necessary or relevant for establishing an RDP connection.
? Confirming the user can ping the default gateway is not required for RDP, as it only tests the network connectivity between the user's laptop and the router. RDP works over the internet, so the technician should be able to ping the user's laptop directly using its IP address3.
? Changing the IP address on the user's laptop is not needed for RDP, as long as the IP address is valid and not conflicting with another device on the network. The user's laptop has a valid IP address of 192.168.0.45, which belongs to the same subnet as the gateway (192.168.0.1) and the subnet mask (255.255.255.0)4.
? Changing the subnet mask on the user's laptop is not required for RDP, as long as the subnet mask matches the network configuration. The user's laptop has a correct subnet mask of 255.255.255.0, which defines a network with 254 possible hosts4.
References:
1: [What is RDP and How Does It Work? - CompTIA] 2: CompTIA A+ Certification Exam Core 2 Objectives - CompTIA 3: [Ping (networking utility) - Wikipedia] 4: [IP address - Wikipedia] : What is RDP and How Does It Work? - CompTIA : CompTIA A+ Certification Exam Core 2 Objectives - CompTIA : Ping (networking utility) - Wikipedia) : IP address - Wikipedia

NEW QUESTION 119
Which of the following filesystem types does macOS use?

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

Answer: D

Explanation:
APFS stands for Apple File System and it is the default filesystem type for macOS since High Sierra (10.13) version1. APFS is optimized for flash storage and supports features such as encryption, snapshots, cloning, and space sharing1.

NEW QUESTION 123
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 124
A user's smartphone data usage is well above average. The user suspects an installed application is transmitting data in the background. The user would like to be alerted when an application attempts to communicate with the internet. Which of the following BEST addresses the user's concern?

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

D. Firewall

Answer: D

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

NEW QUESTION 125
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 126
A company is recycling old hard drives and wants to quickly reprovision the drives for reuse. Which of the following data destruction methods should the company use?

A. Degaussing
B. Standard formatting
C. Low-level wiping
D. Deleting

Answer: C

Explanation:
Low-level wiping is the best data destruction method for recycling old hard drives for reuse. Low-level wiping is a process that overwrites every bit of data on a hard drive with zeros or random patterns, making it impossible to recover any data from the drive. Low-level wiping also restores the drive to its factory state, removing any bad sectors or errors that may have accumulated over time. Low-level wiping can be done using specialized software tools or hardware devices that connect to the drive. Degaussing, standard formatting, and deleting are not suitable data destruction methods for recycling old hard drives for reuse. Degaussing is a process that exposes a hard drive to a strong magnetic field, destroying both the data and the drive itself. Degaussing renders the drive unusable for reuse. Standard formatting is a process that erases the data on a hard drive by removing the file system structure, but it does not overwrite the data itself. Standard formatting leaves some data recoverable using forensic tools or software utilities. Deleting is a process that removes the data from a hard drive by marking it as free space, but it does not erase or overwrite the data itself. Deleting leaves most data recoverable using undelete tools or software utilities.
References:
? Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 15
? CompTIA A+ Complete Study Guide: Core 1 Exam 220-1101 and Core 2 Exam …, page 105

NEW QUESTION 131
A manager called the help desk to ask for assistance with creating a more secure environment for the finance department- which resides in a non-domain environment. Which of the following would be the BEST method to protect against unauthorized use?

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

Answer: B

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

NEW QUESTION 135
An IT services company that supports a large government contract replaced the Ethernet cards on several hundred desktop machines to comply With regulatory requirements. Which of the following disposal methods for the non-compliant cards is the MOST environmentally friendly?

A. incineration
B. Resale
C. Physical destruction
D. Dumpster for recycling plastics

Answer: D

Explanation:
When disposing of non-compliant Ethernet cards, the most environmentally friendly option is to use a dumpster for recycling plastics. This method is the most effective way to reduce the amount of waste that is sent to landfills, and it also helps to reduce the amount of energy used in the production of new materials. Additionally, recycling plastics helps to reduce the amount of toxic chemicals that can be released into the environment. According to CompTIA A+ Core 2 documents, "The most environmentally friendly disposal method for non-compliant Ethernet cards is to use a dumpster for recycling plastics. This method is the most effective way to reduce the amount of waste that is sent to landfills, and it also helps to reduce the amount of energy used in the production of new materials." https://sustainability.yale.edu/blog/how-sustainably-dispose-your-technological-waste

NEW QUESTION 137
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 141
A user rotates a cell phone horizontally to read emails, but the display remains vertical, even though the settings indicate autorotate is on. VT1ich of the following will MOST likely resolve the issue?

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

Answer: D

Explanation:
When a user rotates a cell phone horizontally to read emails and the display remains vertical, even though the settings indicate autorotate is on, this is typically due to a problem with the phone's accelerometer. The accelerometer is the sensor that detects changes in the phone's orientation and adjusts the display accordingly. If the accelerometer is not calibrated correctly, the display may not rotate as expected.

Recalibrating the accelerometer is the most likely solution to this issue. The process for recalibrating the accelerometer can vary depending on the specific device and operating system, but it typically involves going to the device's settings and finding the option to calibrate or reset the sensor. Users may need to search their device's documentation or online resources to find specific instructions for their device.

NEW QUESTION 146
A technician is setting up a newly built computer. Which of the following is the fastest way for the technician to install Windows 10?

A. Factory reset
B. System Restore
C. In-place upgrade
D. Unattended installation

Answer: D

Explanation:
Windows 10

The correct answer is D. Unattended installation. An unattended installation is a way of installing Windows 10 without requiring any user input or interaction. It uses a configuration file called answer file that contains the settings and preferences for the installation, such as the product key, language, partition, and network settings. An unattended installation can be performed by using a bootable USB flash drive or DVD that contains the Windows 10 installation files and the answer file1. This is the fastest way for the technician to install Windows 10 on a newly built computer, as it automates the whole process and saves time. A factory reset is a way of restoring a computer to its original state by deleting all the data and applications and reinstalling the operating system. A factory reset can be performed by using the recovery partition or media that came with the computer, or by using the Reset this PC option in Windows 10 settings2. A factory reset is not a way of installing Windows 10 on a newly built computer, as it requires an existing operating system to be present.

A system restore is a way of undoing changes to a computer’s system files and settings by using a restore point that was created earlier. A system restore can be performed by using the System Restore option in Windows 10 settings or by using the Advanced Startup Options menu3. A system restore is not a way of installing Windows 10 on a newly built computer, as it requires an existing operating system and restore points to be present.

An in-place upgrade is a way of upgrading an existing operating system to a newer version without losing any data or applications. An in-place upgrade can be performed by using the Windows 10 Media Creation Tool or by running the Setup.exe file from the Windows 10 installation media. An in-place upgrade is not a way of installing Windows 10 on a newly built computer, as it requires an existing operating system to be present.

NEW QUESTION 147
A systems administrator is tasked with configuring desktop systems to use a new proxy server that the organization has added to provide content filtering. Which of the following Windows utilities IS the BEST choice for accessing the necessary configuration to complete this goal?

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

Answer: D

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

NEW QUESTION 148
An architecture firm is considering upgrading its computer-aided design (CAD) software to the newest version that forces storage of backups of all CAD files on the software's cloud server. Which of the following is MOST likely to be of concern to the IT manager?

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

Answer: C

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

NEW QUESTION 149
A user reports that a workstation is operating sluggishly Several other users operate on the same workstation and have reported that the workstation is operating normally. The systems administrator has validated that the workstation functions normally. Which of the following steps should the systems administrator most likely attempt NEXT?

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

Answer: C

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

NEW QUESTION 152
Which of the following protocols supports fast roaming between networks?

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

Answer: B

Explanation:
WPA2 is the only protocol among the options that supports fast roaming between
networks. Fast roaming, also known as IEEE 802.11r or Fast BSS Transition (FT), enables a client device to roam quickly in environments implementing WPA2 Enterprise security, by ensuring that the client device does not need to re-authenticate to the RADIUS server
every time it roams from one access point to another1. WEP, WPA, LEAP, and PEAP do not support fast roaming and require the client device to perform the full authentication process every time it roams, which can cause delays and interruptions in the network service.
References:
? The Official CompTIA A+ Core 2 Study Guide2, page 263.
? WiFi Fast Roaming, Simplified3

NEW QUESTION 153
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 155
A technician is editing the hosts file on a few PCs in order to block certain domains. Which of the following would the technician need to execute after editing the hosts file?

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

Answer: D

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

NEW QUESTION 156
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 158
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 161
A user has a computer with Windows 10 Home installed and purchased a Windows 10 Pro license. The user is not sure how to upgrade the OS. Which of the following should the technician do to apply this license?

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

Answer: B

Explanation:
Redeeming the included activation key card for a product key is the correct way to apply a Windows 10 Pro license to a computer that has Windows 10 Home installed. The activation key card is a physical or digital card that contains a 25-digit code that can be used to activate Windows 10 Pro online or by phone. Copying the windows.lie file, inserting a Windows USB hardware dongle and activating with the digital license are not valid methods of applying a Windows 10 Pro license. Verified References: https://www.comptia.org/blog/how-to-upgrade-windows-10-home-to-pro https://www.comptia.org/certifications/a

NEW QUESTION 166
Which of the following macOS utilities uses AES-128 to encrypt the startup disk?

A. fdisk
B. Diskpart
C. Disk Utility
D. FileVault

Answer: D

Explanation:
FileVault is a macOS utility that uses AES-128 (Advanced Encryption Standard) to encrypt the startup disk of a Mac computer. It protects the data from unauthorized access if the computer is lost or stolen. fdisk and Diskpart are disk partitioning utilities for Linux and Windows, respectively. Disk Utility is another macOS utility that can perform disk management tasks, such as formatting, resizing, repairing, etc. Verified References: https://www.comptia.org/blog/what-is-filevault https://www.comptia.org/certifications/a

NEW QUESTION 168
A user receives a notification indicating the data plan on the user's corporate phone has reached its limit. The user has also noted the performance of the phone is abnormally slow. A technician discovers a third-party GPS application was installed on the phone. Which of the following is the MOST likely cause?

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

Answer: B

Explanation:
The GPS application contains malware. The third-party GPS application is likely the cause of the slow performance of the phone. The application may contain malware that is using up system resources and slowing down the phone. The user should uninstall the application and run a malware scan on the phone1

NEW QUESTION 173
Which of the following is a consequence of end-of-lite operating systems?

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

Answer: C

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

NEW QUESTION 174
A technician needs administrator access on a Windows workstation to facilitate system changes without elevating permissions. Which of the following would best accomplish this task?

A. Group Policy Editor
B. Local Users and Groups
C. Device Manager
D. System Configuration

Answer: B

Explanation:

Local Users and Groups is the best option to accomplish this task. Local Users and Groups is a tool that allows managing the local user accounts and groups on a Windows workstation. The technician can use this tool to create a new user account with administrator privileges or add an existing user account to the Administrators group. This way, the technician can log in with the administrator account and make system changes without elevating permissions. Group Policy Editor, Device Manager, and System Configuration are not correct answers for this question. Group Policy Editor is a tool that allows configuring policies and settings for users and computers in a domain environment. Device Manager is a tool that allows managing the hardware devices and drivers on a Windows workstation. System Configuration is a tool that allows modifying the startup options and services on a Windows workstation. None of these tools can directly grant administrator access to a user account. 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 177
Which of the following best describes when to use the YUM command in Linux?

A. To add functionality
B. To change folder permissions
C. To show documentation
D. To list file contents

Answer: A

Explanation:
YUM stands for Yellowdog Updater Modified and it is a command-line tool that allows users to install, update, remove, and manage software packages in Linux. YUM can be used to add functionality to a Linux system by installing new software packages or updating existing ones. To change folder permissions, show documentation, or list file contents, other commands such as chmod, man, or ls can be used in Linux.

NEW QUESTION 178
A technician needs to transfer a file to a user's workstation. Which of the following would BEST accomplish this task utilizing the workstation's built-in protocols?

A.

VPN
B. SMB
C. RMM
D. MSRA

Answer: B

Explanation:
SMB stands for Server Message Block, which is a network file sharing protocol that allows applications on a computer to read and write to files and to request services from server programs in a computer network. SMB is a built-in protocol in Windows operating systems and can be used to transfer files between computers over a network. The technician can use SMB to access a file share on the user's workstation and copy the file to or from it. VPN stands for virtual private network, which is a technology that creates a secure and encrypted connection over a public network. VPN is not a built-in protocol in Windows operating systems and does not directly transfer files between computers. RMM stands for remote monitoring and management, which is a type of software solution that allows remote management and monitoring of devices and networks. RMM is not a built-in protocol in Windows operating systems and does not directly transfer files between computers. MSRA stands for Microsoft Remote Assistance, which is a feature that allows a user to invite another user to view or control their computer remotely. MSRA is not a protocol, but an application that uses Remote Desktop Protocol (RDP) to establish a connection. MSRA does not directly transfer files between computers. https://www.pcmag.com/picks/the-best-desktop-workstations

NEW QUESTION 183
Which of the following would MOST likely be used to change the security settings on a user's device in a domain environment?

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

Answer: C

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

complexity, account lockout, firewall rules, encryption settings, etc.

NEW QUESTION 187
A network technician is deploying a new machine in a small branch office that does not have a DHCP server. The new machine automatically receives the IP address of 169.254.0.2 and is unable to communicate with the rest of the network. Which of the following would restore communication?

A. Static entry
B. ARP table
C.

APIPA address

D. NTP specification

Answer: A

Explanation:
A static entry is the best option to restore communication for the new machine in a small branch office that does not have a DHCP server. A static entry means manually configuring the IP address, subnet mask, default gateway, and DNS server for the network adapter of the machine. A static entry ensures that the machine has a valid and unique IP address that matches the network configuration and can communicate with the rest of the network.
The new machine automatically receives the IP address of 169.254.0.2 because it uses APIPA (Automatic Private IP Addressing), which is a feature that enables computers to self-assign an IP address when a DHCP server is not available. However, APIPA only works for local communication within the same subnet, and does not provide a default gateway or a DNS server. Therefore, the new machine is unable to communicate with the rest of the network, which may be on a different subnet or require a gateway or a DNS server to access.
The other options are not related to restoring communication for the new machine. ARP table is a cache that stores the mapping between IP addresses and MAC addresses for the devices on the network. NTP specification is a protocol that synchronizes the clocks of the devices on the network.
References:
? CompTIA A+ Certification Exam Core 2 Objectives1
? CompTIA A+ Core 2 (220-1102) Certification Study Guide2
? What is APIPA (Automatic Private IP Addressing)? - Study-CCNA3
? How to Configure a Static IP Address in Windows and OS X4

NEW QUESTION 191
Which of the following physical security controls can prevent laptops from being stolen?

A. Encryption
B. LoJack
C. Multifactor authentication
D. Equipment lock
E. Bollards

Answer: D

Explanation:
An equipment lock is a physical security device that attaches a laptop to a fixed object, such as a desk or a table, with a cable and a lock. This can prevent the laptop from being stolen by unauthorized persons. Encryption, LoJack, multifactor authentication and bollards are other security measures, but they do not physically prevent theft. Verified References: https://www.comptia.org/blog/physical-security https://www.comptia.org/certifications/a

NEW QUESTION 194
A technician wants to install Developer Mode on a Windows laptop but is receiving a "failed to install package" message. Which of the following should the technician do first?

A.

Ensure internet connectivity.
B. Check for Windows updates.
C. Enable SSH.
D. Reboot computer.

Answer: A

Explanation:
Developer Mode on Windows 10 is a feature that allows developers to test and debug their applications on their devices, as well as sideload apps and access other developer tools12. To enable Developer Mode, the user needs to go to the Settings app, select Update & Security, choose For Developers, and switch to Developer Mode123. However, enabling Developer Mode requires internet connectivity, as Windows will download and install a package of features, such as Windows Device Portal and SSH services, that are
necessary for Developer Mode124. If the user does not have internet connectivity, they will receive a “failed to install package” message when trying to enable Developer Mode4. Therefore, the first thing that the technician should do is to ensure that the laptop has internet access, either through Wi-Fi or Ethernet, and then try to enable Developer Mode again4

NEW QUESTION 197
A technician is replacing the processor in a desktop computer prior to opening the computer, the technician wants to ensure the internal components are protected. Which of the following safety procedures would BEST protect the components in the PC? (Select TWO).

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

Answer: AC

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

https://www.professormesser.com/free-a-plus-training/220-902/computer-safety- procedures-2/
https://www.skillsoft.com/course/comptia-a-core-2-safety-procedures-environmental-impacts-cbdf0f2c-61c0-4f4a-a659-dc98f1f00158

NEW QUESTION 198
A technician has identified malicious traffic originating from a user's computer. Which of the following is the best way to identify the source of the attack?

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

Answer: B

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

NEW QUESTION 200
A technician is troubleshooting boot times for a user. The technician attempts to use MSConfig to see which programs are starting with the OS but receives a message that it can no longer be used to view startup items. Which of the following programs can the technician use to view startup items?

A. msinfo32
B. perfmon
C. regedit
D. taskmgr

Answer: D

Explanation:
When troubleshooting boot times for a user, a technician may want to check which programs are starting with the operating system to identify any that may be slowing down the boot process. MSConfig is a tool that can be used to view startup items on a Windows system, but it may not always be available or functional. In this scenario, the technician receives a message that MSConfig cannot be used to view startup items. As an alternative, the technician can use Task Manager (taskmgr), which can

also display the programs that run at startup. To access the list of startup items in Task Manager, the technician can follow these steps:
? Open Task Manager by pressing Ctrl+Shift+Esc.
? Click the "Startup" tab.
? The list of programs that run at startup will be displayed.

NEW QUESTION 205
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 208
All the desktop icons on a user's newly issued PC are very large. The user reports that the PC was working fine until a recent software patch was deployed. Which of the following would BEST resolve the issue?

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

Answer: A

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

NEW QUESTION 210

Which of the following is the best reason for sandbox testing in change management?

A. To evaluate the change before deployment
B. To obtain end-user acceptance
C. To determine the affected systems
D. To select a change owner

Answer: A

Explanation:
Sandbox testing is a method of testing changes in a simulated environment that mimics the real one, without affecting the actual production system. Sandbox testing is useful for change management because it allows the testers to evaluate the change before deployment, and ensure that it works as intended, does not cause any errors or conflicts, and meets the requirements and expectations of the stakeholders. Sandbox testing also helps to protect the investment in the existing system, as it reduces the risk of introducing bugs or breaking functionality that could harm the customer experience or the business operations. Sandbox testing also gives the testers more control over the customer experience, as they can experiment with different scenarios and configurations, and optimize the change for the best possible outcome.
References:
1: Change Management and Sandbox - Quickbase1 2: Embracing change: Build, test, and adapt in a sandbox environment - Zendesk3

NEW QUESTION 211
A user is setting up a new Windows 10 laptop. Which of the following Windows settings should be used to input the SSID and password?

A.

Network & Internet
B. System
C. Personalization

D. Accounts

Answer: A

Explanation:
The Network & Internet settings in Windows 10 allow the user to input the SSID and password of a Wi-Fi network, as well as manage other network-related options, such as airplane mode, mobile hotspot, VPN, proxy, etc1. To access the Network & Internet settings, the user can select the Start button, then select Settings > Network & Internet2. Alternatively, the user can right-click the Wi-Fi icon on the taskbar and click "Open Network & Internet Settings"3.
The System settings in Windows 10 allow the user to configure the display, sound, notifications, power, storage, and other system-related options1. The Personalization settings in Windows 10 allow the user to customize the background, colors, lock screen, themes, fonts, and other appearance-related options1. The Accounts settings in Windows 10 allow the user to manage the user accounts, sign-in options, sync settings, and other account-related options1. None of these settings can be used to input the SSID and password of a Wi-Fi network.
References:
? The Official CompTIA A+ Core 2 Study Guide1, page 221, 222, 223, 224.

NEW QUESTION 214
A technician wants to enable BitLocker on a Windows 10 laptop and is unable to find the BitLocker Drive Encryption menu item in Control Panel. Which of the following explains why the technician unable to find this menu item?

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

Answer: C

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

NEW QUESTION 219
A user is unable to log in to the network. The network uses 802.1X with EAP-TLS to authenticate on the wired network. The user has been on an extended leave and has not logged in to the computer in several months. Which of the following is causing the login issue?

A. Expired certificate
B. OS update failure
C. Service not started
D.

Application crash
E. Profile rebuild needed

Answer: A

Explanation:
EAP-TLS is a method of authentication that uses certificates to establish a secure tunnel between the client and the server3. The certificates have a validity period and must be renewed before they expire1. If the user has been on an extended leave and has not logged in to the computer in several months, it is possible that the certificate on the client or the server has expired and needs to be renewed2. The other options are not directly related to EAP-TLS authentication or 802.1X network access.

NEW QUESTION 220
Which of the following file extensions should a technician use for a PowerShell script?

A.

.ps1
B. .py
C. .sh
D. .bat
E. .cmd

Answer: A

Explanation:
A PowerShell script is a plain text file that contains one or more PowerShell commands. Scripts have a .ps1 file extension and can be run on your computer or in a remote session. PowerShell scripts can be used to automate tasks and change settings on Windows devices. To create and run a PowerShell script, you need a text editor (such as Visual Studio Code or Notepad) and the PowerShell Integrated Scripting Environment (ISE) console. You also need to enable the correct execution policy to allow scripts to run on your system

NEW QUESTION 225
A user receives the following error while attempting to boot a computer.
BOOTMGR is missing
press Ctrl+Alt+Del to restart
Which of the following should a desktop engineer attempt FIRST to address this issue?

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

Answer: A

Explanation:
The error “BOOTMGR is missing” indicates that the boot sector is damaged or missing1
. The boot sector is a part of the hard disk that contains the code and information needed to

start Windows1. To fix this error, one of the possible methods is to run Startup Repair from Windows Recovery Environment (WinRE)1. Startup Repair is a tool that can automatically diagnose and repair problems with the boot process2.
References: 1: “Bootmgr is missing Press Ctrl+Alt+Del to restart” error when you start Windows (https://support.microsoft.com/en-us/topic/-bootmgr-is-missing-press-ctrl-alt-del- to-restart-error-when-you-start-windows-8bc1b94b-d243-1027-5410-aeb04d5cd5e2) 2: Startup Repair: frequently asked questions

(https://support.microsoft.com/en- us/windows/startup-repair-frequently-asked-questions-f5f412a0-19c4-8e0a-9f68- bb0f17f3daa0)

NEW QUESTION 227
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 229
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 234
Which of the following would cause a corporate-owned iOS device to have an Activation Lock issue?

A. A forgotten keychain password
B. An employee's Apple ID used on the device
C. An operating system that has been jailbroken
D. An expired screen unlock code

Answer: B

Explanation:
Activation Lock is a feature that prevents anyone from erasing or activating an iOS device without the owner's Apple ID and password. If a corporate-owned iOS device is linked to an employee's Apple ID, it will have an Activation Lock issue when the employee leaves the company or forgets their Apple ID credentials.
Reference: CompTIA A+ Core 2 Exam Objectives, Section 4.1

NEW QUESTION 237
Which of the following is an advantage of using WPA2 instead of WPA3?

A. Connection security
B. Encryption key length
C. Device compatibility
D. Offline decryption resistance

Answer: C

Explanation:
Device compatibility is an advantage of using WPA2 instead of WPA3. WPA2 is the previous version of the Wi-Fi Protected Access protocol, which provides security and encryption for wireless networks. WPA3 is the latest version, which offers improved security features, such as stronger encryption, enhanced protection against brute-force attacks, and easier configuration. However, WPA3 is not backward compatible with older devices that only support WPA2 or earlier protocols. Therefore, using WPA3 may limit the range of devices that can connect to the wireless network. Connection security, encryption key length, and offline decryption resistance are advantages of using WPA3 instead of WPA2. References:
? Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 24
? CompTIA A+ Certification All-in-One Exam Guide (Exams 220-1101 & …, page 1000

NEW QUESTION 239
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 243
A technician sees a file that is requesting payment to a cryptocurrency address. Which of the following should the technician do first?

A. Quarantine the computer.
B. Disable System Restore.
C. Update the antivirus software definitions.
D. Boot to safe mode.

Answer: A

Explanation:
Quarantining the computer means isolating it from the network and other devices to prevent the spread of malware or ransomware. Ransomware is a type of malware that encrypts the files on a computer and demands payment (usually in cryptocurrency) to restore them. If a technician sees a file that is requesting payment to a cryptocurrency address, it is likely that the computer has been infected by ransomware. Quarantining the computer should be the first step to contain the infection and prevent further damage. Disabling System Restore, updating the antivirus software definitions, and booting to safe mode are not steps that should be done before quarantining the computer.

NEW QUESTION 246
Which of the following could be used to implement secure physical access to a data center?

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

Answer: C

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

NEW QUESTION 251
Which of the following is the most likely to use NTFS as the native filesystem?

A. macOS
B. Linux
C. Windows
D. Android

Answer: C

Explanation:
NTFS stands for New Technology File System, which is a proprietary file system developed by Microsoft4. NTFS is the default file system for the Windows NT family of operating systems, which includes Windows 10, Windows Server 2019, and other versions5. NTFS provides features such as security, encryption, compression, journaling, and large volume support45. NTFS is not the native file system for other operating systems, such as macOS, Linux, or Android, although some of them can read or write to NTFS volumes with third-party drivers or tools

NEW QUESTION 252
An analyst needs GUI access to server software running on a macOS server. Which of the following options provides the BEST way for the analyst to access the macOS server from the Windows workstation?

A. RDP through RD Gateway
B. Apple Remote Desktop
C. SSH access with SSH keys
D. VNC with username and password

Answer: B

Explanation:
Apple Remote Desktop is a remote access solution that allows a user to access and control another macOS computer from their Windows workstation. It provides a graphical user interface so that the analyst can easily access the server software running on the macOS server. Apple Remote Desktop also supports file transfers, so the analyst can easily transfer files between the two computers. Additionally, Apple Remote Desktop supports encryption, so data is secure during transmission.

NEW QUESTION 253
A change advisory board just approved a change request. Which of the following is the MOST likely next step in the change process?

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

Answer: D

Explanation:
The risk analysis should be performed before it's taken to the board. The step after the board approves the change is End User Agreement Reference: https://www.youtube.com/watch?v=Ru77iZxuElA&list=PLG49S3nxzAnna96gzhJrzkii4hH_mgW4b&index=59

NEW QUESTION 255
A user enabled a mobile device's screen lock function with pattern unlock. The user is concerned someone could access the mobile device by repeatedly attempting random patterns to unlock the device. Which of the following features BEST addresses the user's concern?

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

Answer: A

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

NEW QUESTION 259
Which of the following is an example of MFA?

A. Fingerprint scan and retina scan
B. Password and PIN
C. Username and password
D. Smart card and password

Answer: D

Explanation:
Smart card and password is an example of two-factor authentication (2FA), not multi-factor authentication (MFA). MFA requires two or more authentication factors. Smart card and password is an example of two-factor authentication (2FA2)

NEW QUESTION 261
When a user calls in to report an issue, a technician submits a ticket on the user's behalf. Which of the following practices should the technician use to make sure the ticket is associated with the correct user?

A. Have the user provide a callback phone number to be added to the ticket
B. Assign the ticket to the department's power user
C. Register the ticket with a unique user identifier
D. Provide the user with a unique ticket number that can be referenced on subsequent calls.

Answer: D

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

NEW QUESTION 262
A change advisory board did not approve a requested change due to the lack of alternative actions if implementation failed. Which of the following should be updated before requesting approval again?

A. Scope of change
Risk level
B.
C. Rollback plan
D. End user acceptance

Answer: C

Explanation:
The rollback plan should be updated before requesting approval again. A rollback plan is a plan for undoing a change if it causes problems, and it is an important part of any change management process. If the change advisory board did not approve the requested change due to the lack of alternative actions if implementation failed, then updating the rollback plan would be the best way to address this concern.

NEW QUESTION 267
Which of the following is the MOST important environmental concern inside a data center?

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

Answer: D

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

NEW QUESTION 271
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 275
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 279
A bank would like to enhance building security in order to prevent vehicles from driving into the building while also maintaining easy access for customers. Which of the following BEST addresses this need?

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

Answer: B

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

NEW QUESTION 280
A user tries to access commonly used web pages but is redirected to unexpected websites. Clearing the web browser cache does not resolve the issue. Which of the following should a technician investigate NEXT to resolve the issue?

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

Answer: B

Explanation:

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

NEW QUESTION 281
A user requires local administrative access to a workstation. Which of the following Control Panel utilities allows the technician to grant access to the user?

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

Answer: C

Explanation:
User Accounts is a Control Panel utility that allows the technician to manage user accounts and groups on a workstation1. The technician can use User Accounts to grant local administrative access to a user by adding the user to the Administrators group1. The Administrators group has full control over the workstation and can perform tasks such as installing software, changing system settings, and accessing all files.
References: 1: User Accounts (Control Panel) (https://docs.microsoft.com/en-us/windows/win32/shell/user-accounts) : Local Users and Groups (https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/local-users-and-groups)

NEW QUESTION 285
A technician is attempting to mitigate micro power outages, which occur frequently within the area of operation. The outages are usually short, with the longest occurrence lasting five minutes. Which of the following should the technician use to mitigate this issue?

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

Answer: B

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

NEW QUESTION 290
During an enterprise rollout of a new application, a technician needs to validate compliance with an application's EULA while also reducing the number of licenses to manage. Which of the following licenses would best accomplish this goal?

A. Personal use license
B. Corporate use license
C. Open-source license
D. Non-expiring license

Answer: B

Explanation:
A corporate use license, also known as a volume license, is a type of software license that allows an organization to purchase and use multiple copies of a software product with a single license key. A corporate use license can help validate compliance with an application’s EULA (end-user license agreement), which is a legal contract that defines the terms and conditions of using the software. A corporate use license can also reduce the number of licenses to manage, as it eliminates the need to activate and track individual licenses for each copy of the software. Personal use license, open-source license, and non-expiring license are not types of licenses that can best accomplish this goal.

NEW QUESTION 295
A technician is asked to resize a partition on the internal storage drive of a computer running macOS. Which of the followings tools should the technician use to accomplish this task?

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

Answer: B

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

NEW QUESTION 299
A user calls the help desk to report that mapped drives are no longer accessible. The technician verifies that clicking on any of the drives on the user's machine results in an error message. Other users in the office are not having any issues. As a first step, the technician would like to remove and

attempt to reconnect the drives. Which of the following command-line tools should the technician use?

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

Answer: A

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

NEW QUESTION 303
A police officer often leaves a workstation for several minutes at a time. Which of the following is the BEST way the officer can secure the workstation quickly when walking away?

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

Answer: A

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

NEW QUESTION 305
Which of the following would allow physical access to a restricted area while maintaining a record of events?

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Access control vestibule is the correct answer for this question. An access control vestibule is a physical security device that consists of two doors that form an enclosed space between them. The first door opens only after verifying the identity of the person entering, such as by using a card reader, biometric scanner, or keypad. The second door opens only after the first door closes, creating a buffer zone that prevents unauthorized access or tailgating. An access control vestibule also maintains a record of events, such as who entered or exited, when, and how. Hard token, key fob, and door lock are not sufficient to meet the requirements of this question. A hard token is a device that generates a one-time password or code for authentication purposes. A key fob is a small device that can be attached to a key ring and used to unlock doors or start vehicles remotely. A door lock is a mechanism that secures a door from opening without a key or a code. References:
? Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 25

NEW QUESTION 308
A technician needs to access a Windows 10 desktop on the network in a SOHO using RDP. Although the connection is unsuccessful, the technician is able to ping the computer successfully. Which of the following is MOST likely preventing the connection?

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

Answer: A

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

NEW QUESTION 310
Which of the following is command options is used to display hidden files and directories?

A. -a
B. -s
C. -lh
D. -t

Answer: A

Explanation:
The -a option is used to display hidden files and directories in a command- line interface. Hidden files and directories are those that start with a dot (.) and are normally not shown by default. The -a option stands for “all” and shows all files and directories, including the hidden ones. The -a option can be used with

commands such as ls, dir, or find to list or search for hidden files and directories. The -s, -lh, and -t options are not used to display hidden files and directories. The -s option stands for “size” and shows the size of files or directories in bytes. The -lh option stands for “long human-readable” and shows the size of files or directories in a more readable format, such as KB, MB, or GB. The -t option stands for “time” and sorts the files or directories by modification time. References:
? Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 17
? CompTIA A+ Complete Study Guide: Core 1 Exam 220-1101 and Core 2 Exam …, page 107

NEW QUESTION 311
......