Exam Questions 220-1102

CompTIA A+ Certification Exam: Core 2

https://www.2passeasy.com/dumps/220-1102/

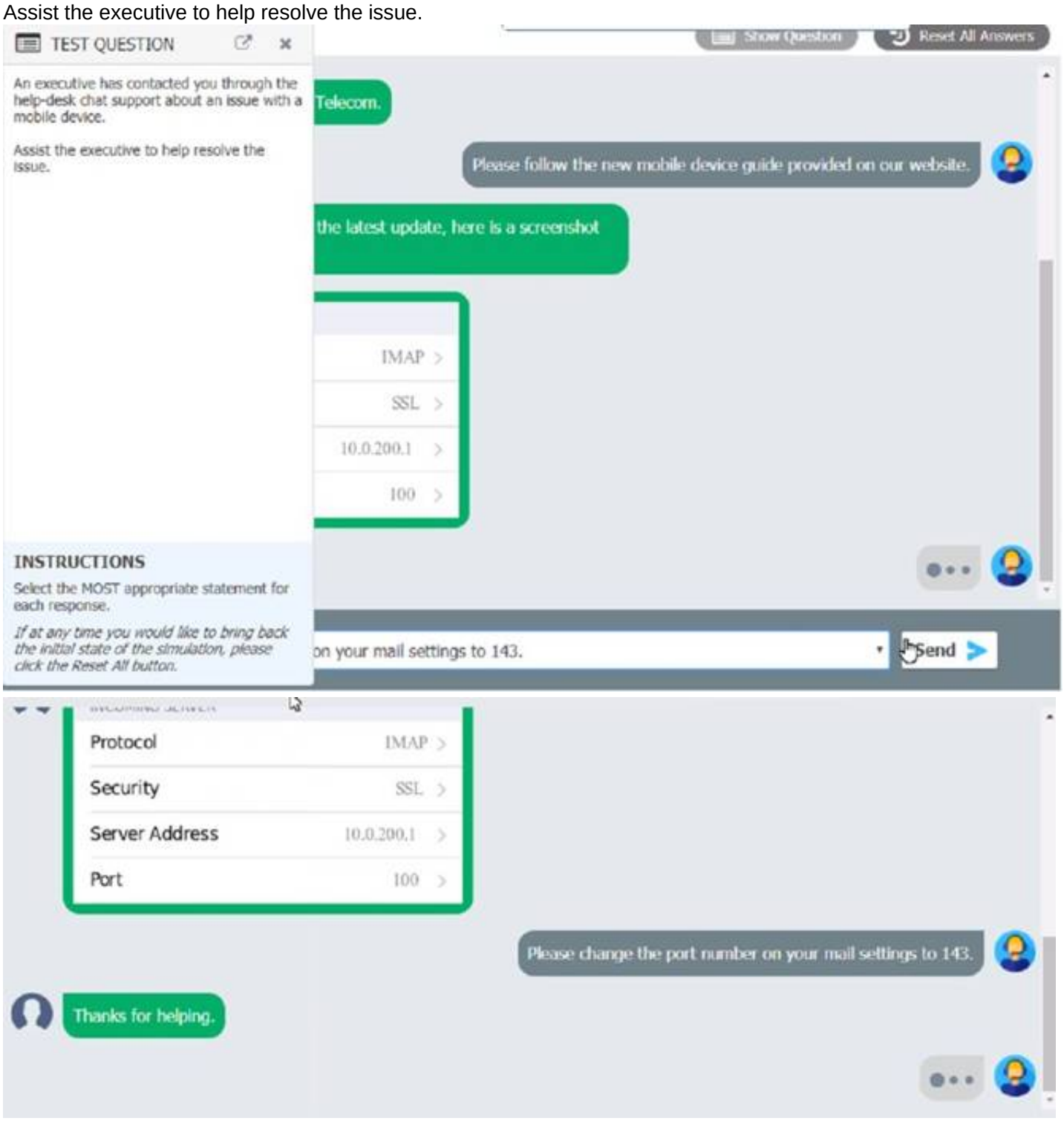
NEW QUESTION 1
After a failed update, an application no longer launches and generates the following error message: Application needs to be repaired. Which of the following Windows 10 utilities should a technician use to address this concern?

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

Answer: D

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

NEW QUESTION 2
An executive has contacted you through the help-desk chat support about an issue with a mobile device.
Assist the executive to help resolve the issue.



Which of the following should be done NEXT?

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

Answer: A

NEW QUESTION 3
A company recently experienced a security incident in which a USB drive containing malicious software was able to covertly install malware on a workstation.
Which of the following actions should be taken to prevent this incident from happening again? (Select two).

A. Install a host-based IDS.
B. Restrict log-in times.
C. Enable a BIOS password.

D. Update the password complexity.
E. Disable AutoRun.
F. Update the antivirus definitions.
G. Restrict user permissions.

Answer: EG

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

NEW QUESTION 4
A user reports that the pages flash on the screen two or three times before finally staying open when attempting to access banking web pages. Which of the following troubleshooting steps should the technician perform NEXT to resolve the issue?

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

Answer: B

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

NEW QUESTION 5
Which of the following data is MOST likely to be regulated?

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

Answer: B

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

NEW QUESTION 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 technician is troubleshooting a Windows 10 PC that is unable to start the GUI. A new SSD and a new copy of Windows were recently installed on the PC. Which of the following is the most appropriate command to use to fix the issue?

A. msconfig
B. chkdsk
C. sfc
D. diskpart
E. mstsc

Answer: C

Explanation:
The sfc command is a tool for scanning and repairing system files that are corrupted or missing on Windows operating systems12. System files are essential files that are required for the proper functioning of the operating system, such as the GUI, drivers, services, and applications. If system files are damaged or deleted, the operating system may fail to start or run properly, causing errors, crashes, or blue screens.
The sfc command can be used to fix the issue of the PC that is unable to start the GUI, assuming that the problem is caused by corrupted or missing system files. The sfc command can be run from the command prompt, which can be accessed by booting the PC from the installation media, choosing the repair option, and selecting the command prompt option3. The sfc command can be used with different switches, such as /scannow, /verifyonly, /scanfile, or /offbootdir, depending on the situation and the desired action4. The most common switch is /scannow, which scans all the system files and repairs any problems that are found5. The syntax of the sfc command with the /scannow switch is: sfc /scannow
The sfc command will then scan and repair the system files, and display the results on the screen. If the sfc command is able to fix the system files, the PC should be able to start the GUI normally after rebooting. If the sfc command is unable to fix the system files, the PC may need further troubleshooting or a clean installation of Windows.
References1: CompTIA A+ Certification Exam Core 2 Objectives, page 10 2: CompTIA A+ Core 2 (220-1102) Complete Video Course, Lesson 26 Documentation 3: How to use SFC Scannow to repair Windows system files 4: SFC Command (System File Checker) 5: How to Repair Windows 10 using Command Prompt

NEW QUESTION 9
A large university wants to equip all classrooms with high-definition IP videoconferencing equipment. Which of the following would most likely be impacted in this situation?

A. SAN
B. LAN
C. GPU
D. PAN

Answer: B

Explanation:
LAN is the most likely option to be impacted in this situation. LAN stands for Local Area Network, and it is a network that connects devices within a limited area, such as a building or a campus. Installing high-definition IP videoconferencing equipment in all classrooms would require a high bandwidth and reliable LAN infrastructure to support the video and audio transmission. The LAN would also need to be configured with proper security, quality of service, and multicast protocols to ensure the optimal performance of the videoconferencing system. SAN, GPU, and PAN are not directly related to this scenario. SAN stands for Storage Area Network, and it is a network that provides access to consolidated storage devices. GPU stands for Graphics Processing Unit, and it is a hardware component that handles graphics rendering and computation. PAN stands for Personal Area Network, and it is a network that connects devices within a short range, such as Bluetooth or infrared. References:
? Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 20
? CompTIA A+ Complete Study Guide: Core 1 Exam 220-1101 and Core 2 Exam …, page 104

NEW QUESTION 10
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 user is unable to access files on a work PC after opening a text document. The text document was labeled "URGENT PLEASE READ.txt - In active folder, .txt file titled urgent please read". Which of the following should a support technician do FIRST?

A. Quarantine the host in the antivirus system.
B. Run antivirus scan tor malicious software.
C. Investigate how malicious software was Installed.
D. Reimage the computer.

Answer: B

Explanation:
Running an antivirus scan for malicious software is the first step that a support technician should do when a user reports a virus on a PC. The antivirus scan can detect and remove the virus, as well as prevent further damage or infection. Quarantining the host, investigating how the malware was installed and reimaging the computer are possible steps that can be done after running the antivirus scan, depending on the situation and the results of the scan. Verified References: https://www.comptia.org/blog/how-to- remove-a-virus https://www.comptia.org/certifications/a

NEW QUESTION 12
A systems administrator is configuring centralized desktop management for computers on a domain. The management team has decided that all users' workstations should have the same network drives, printers, and configurations. Which of the following should the administrator use to accomplish this task?

A. Network and Sharing Center
B. net use
C. User Accounts
D. regedit
E. Group Policy

Answer: E

Explanation:
Group Policy is a feature of Windows that allows administrators to centrally manage and apply policies and settings to computers and users on a domain3. Group Policy can be used to configure network drives, printers, security settings, desktop preferences, and other configurations for all users' workstations3. Network and Sharing Center, net use, User Accounts, and regedit are not tools that can accomplish this task.

NEW QUESTION 13
After a security event, a technician removes malware from an affected laptop and disconnects the laptop from the network. Which of the following should the technician do to prevent the operating system from automatically returning to an infected state?

A. Enable System Restore.
B. Disable System Restore.
C. Enable antivirus.
D. Disable antivirus.
E. Educate the user.

Answer: B

Explanation:
System Restore is a feature that allows the user to revert the system to a previous state. However, this can also restore the malware that was removed by the technician. Disabling System Restore can prevent the operating system from automatically returning to an infected state. Enabling antivirus, educating the user, and enabling System Restore are good preventive measures, but they do not address the question. Disabling antivirus can make the system more vulnerable to malware attacks

NEW QUESTION 14
A customer called the help desk to report that a machine that was recently updated is no longer working. The support technician checks the latest logs to see what updates were deployed, but nothing was
deployed in more than three weeks. Which of the following should the support technician do to BEST resolve the situation?

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

Answer: D

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

NEW QUESTION 18
A technician is investigating options to secure a small office's wireless network. One requirement is to allow automatic log-ins to the network using certificates instead of passwords. Which of the following should the wireless solution have in order to support this feature?

A. RADIUS
B. AES
C. EAP-EKE

D. MFA

Answer: A

Explanation:
RADIUS is the correct answer for this question. RADIUS stands for Remote Authentication Dial-In User Service, and it is a protocol that provides centralized authentication, authorization, and accounting for wireless networks. RADIUS can support certificate-based authentication, which allows users to log in to the network automatically without entering passwords. RADIUS also provides other benefits, such as enforcing security policies, logging user activities, and managing network access. AES, EAP-EKE, and MFA are not wireless solutions, but rather encryption algorithms, authentication methods, and security factors, respectively.
References:
? Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 23
? CompTIA A+ Core 1 (220-1101) and Core 2 (220-1102) Cert Guide, page 459

NEW QUESTION 23
A technician suspects the boot disk of a user's computer contains bad sectors. Which of the following should the technician verify in the command prompt to address the issue without making any changes?

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

Answer: C

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

NEW QUESTION 28
A user reports a virus is on a PC. The user installs additional real-lime protection antivirus software, and the PC begins performing extremely slow. Which of the following steps should the technician take to resolve the issue?

A. Uninstall one antivirus software program and install a different one.
B. Launch Windows Update, and then download and install OS updates
C. Activate real-time protection on both antivirus software programs
D. Enable the quarantine feature on both antivirus software programs.
E. Remove the user-installed antivirus software program.

Answer: E

Explanation:
Removing the user-installed antivirus software program is the best way to resolve the issue of extremely slow performance caused by installing additional real-time protection antivirus software on a PC. Having more than one antivirus software program running at the same time can cause conflicts, resource consumption and performance degradation. Uninstalling one antivirus software program and installing a different one, activating real-time protection on both antivirus software programs, enabling the quarantine feature on both antivirus software programs and launching Windows Update are not effective ways to resolve the issue. Verified References: https://www.comptia.org/blog/why- you-shouldnt-run-multiple-antivirus-programs-at-the-same-time https://www.comptia.org/certifications/a

NEW QUESTION 33
A user has requested help setting up the fingerprint reader on a Windows 10 laptop. The laptop is equipped with a fingerprint reader and is joined to a domain Group Policy enables Windows Hello on all computers in the environment. Which of the following options describes how to set up Windows Hello Fingerprint for the user?

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

Answer: B

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

NEW QUESTION 35
A computer on a corporate network has a malware infection. Which of the following would be the BEST method for returning the computer to service?

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

E. flashing the BIOS, and then scanning with on-premises antivirus

Answer: B

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

NEW QUESTION 37
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 38
A help desk technician needs to remotely access and control a customer's Windows PC by using a secure session that allows the technician the same control as the customer. Which of the following tools provides this type of access?

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

Answer: B

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

NEW QUESTION 43
A user's mobile phone has become sluggish A systems administrator discovered several malicious applications on the device and reset the phone. The administrator installed MDM software. Which of the following should the administrator do to help secure the device against this threat in the future? (Select TWO).

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

Answer: CE

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

NEW QUESTION 46
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 47
Which of the following often uses an SMS or third-party application as a secondary method to access a system?

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

Answer: A

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

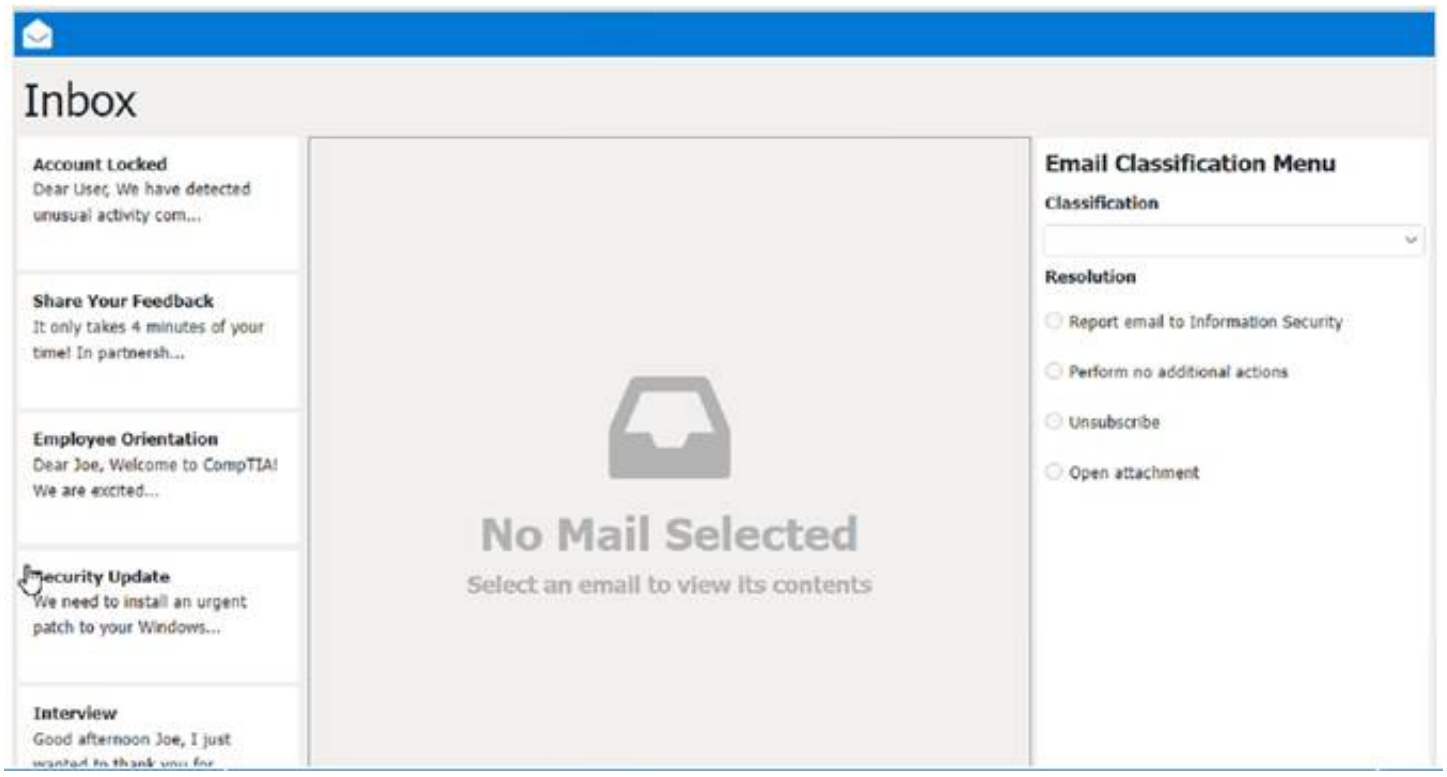
NEW QUESTION 49
A company is deploying mobile phones on a one-to-one basis, but the IT manager is concerned that users will root/jailbreak their phones. Which of the following technologies can be implemented to prevent this issue?

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

Answer: D

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

NEW QUESTION 53
SIMULATION
As a corporate technician, you are asked to evaluate several suspect email messages on a client's computer. Corporate policy requires he following:
. All phishing attempts must be reported.
. Future spam emails to users must be prevented. INSTRUCTIONS
Review each email and perform the following within the email:
. Classify the emails
. Identify suspicious items, if applicable, in each email
. Select the appropriate resolution

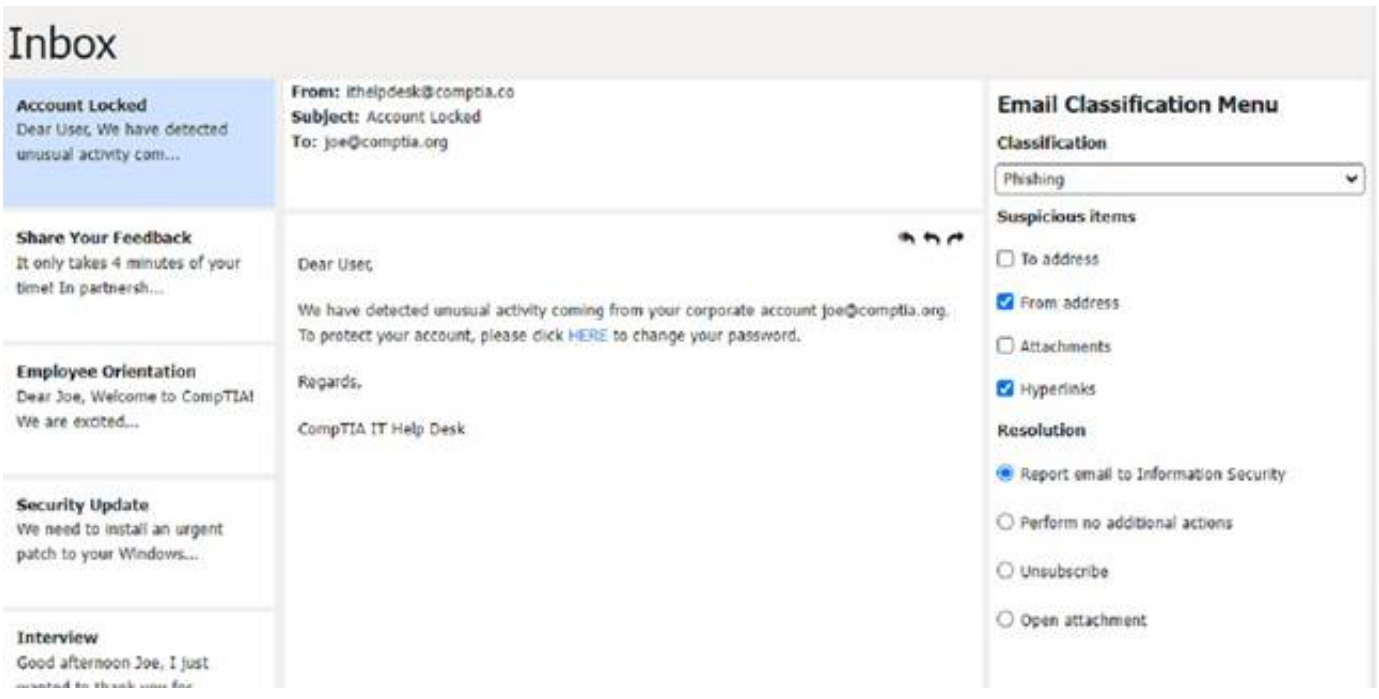


Answer:
See the Full solution in Explanation below.

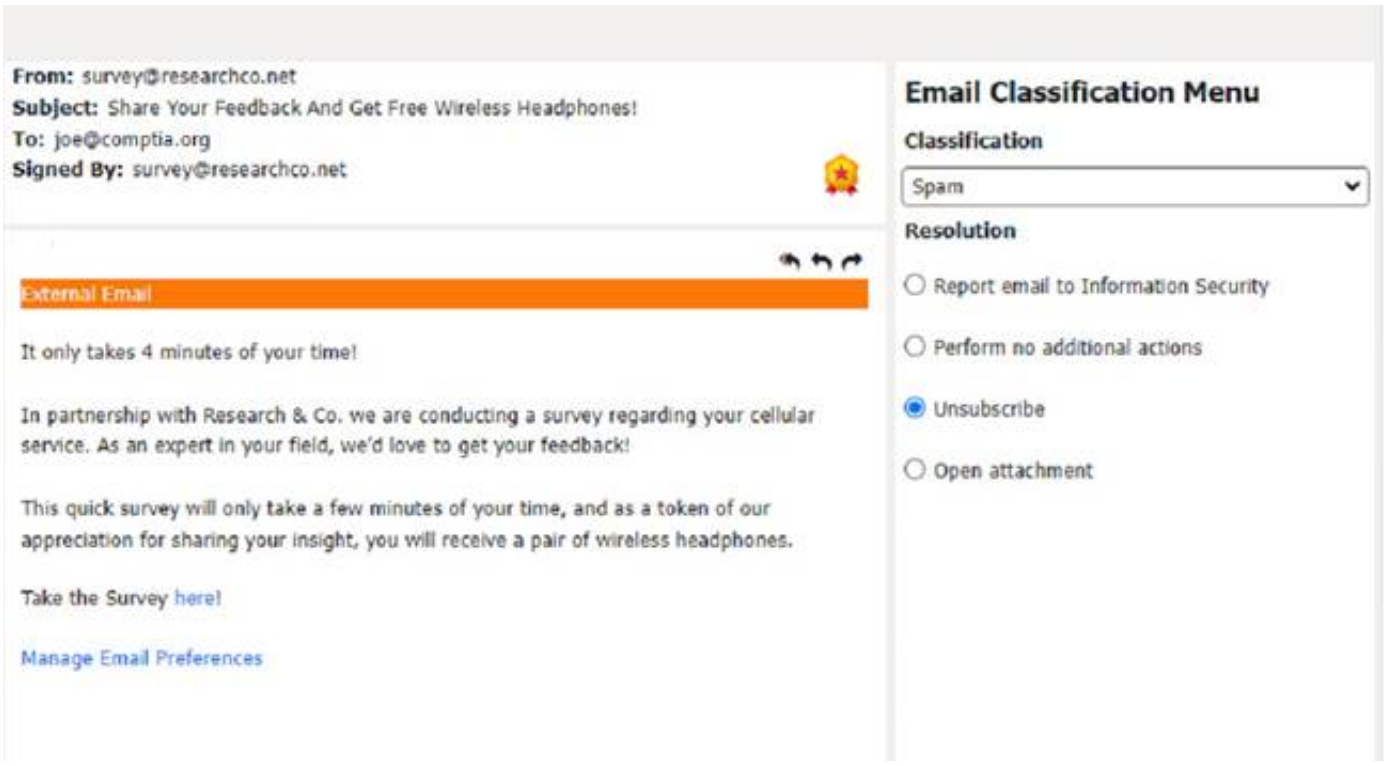
A. Mastered
B. Not Mastered

Answer: A

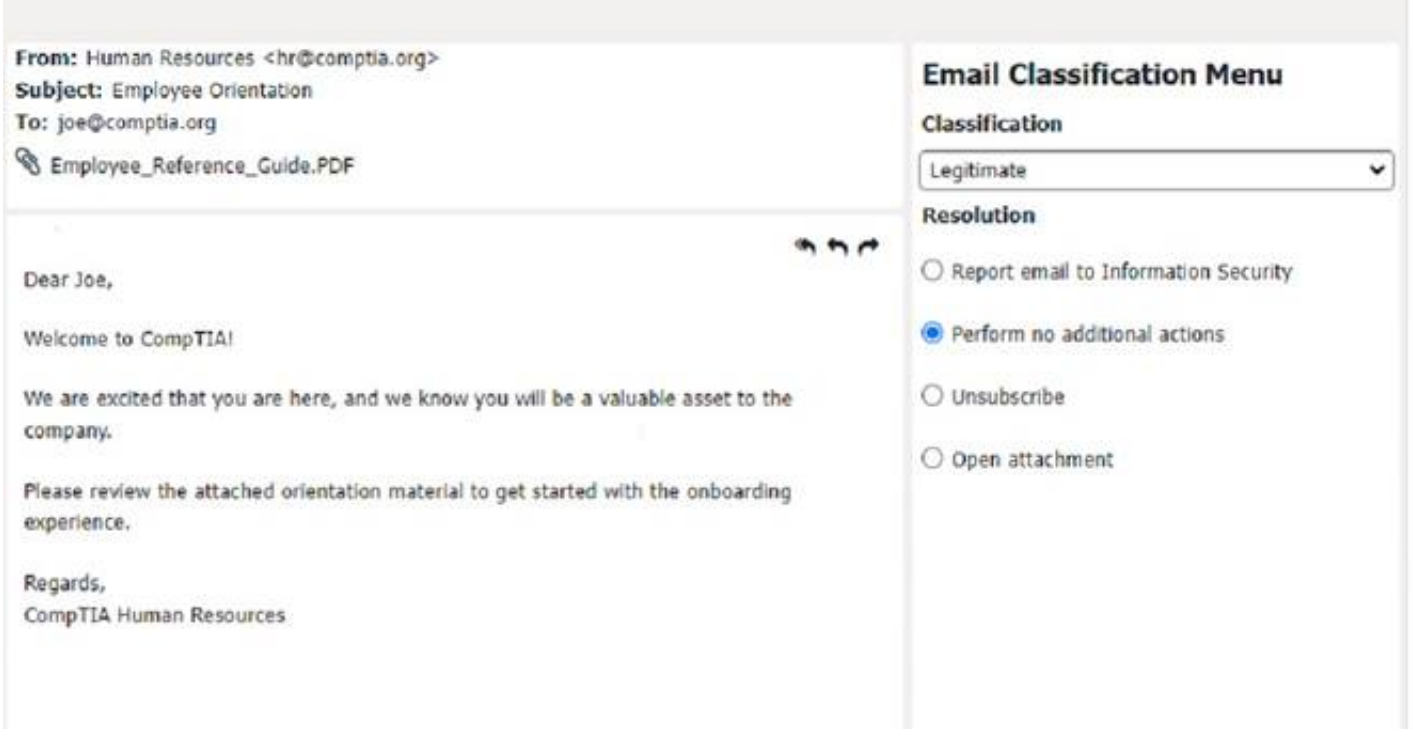
Explanation:
Classification: a) Phishing
This email is a phishing attempt, as it tries to trick the user into clicking on a malicious link that could compromise their account or personal information. Some suspicious items in this email are:
? The email has a generic greeting and does not address the user by name.
? The email has spelling errors, such as “unusal” and “Locaked”.
? The email uses a sense of urgency and fear to pressure the user into clicking on the link.
? The email does not match the official format or domain of the IT Help Desk at CompTIA.
? The email has two black bat icons, which are not related to CompTIA or IT support.
The appropriate resolution for this email is A. Report email to Information Security. The user should not click on the link, reply to the email, or provide any personal or account information. The user should forward the email to the Information Security team or use a professional email form to report the phishing attempt. The user should also delete the email from their inbox and trash folder.
The suspicious items to select are:
? b) From address
? d) Hyperlinks
These items indicate that the email is not from a legitimate source and that the link is potentially malicious. The other items are not suspicious in this case, as the to address is the user’s own email and there are no attachments.



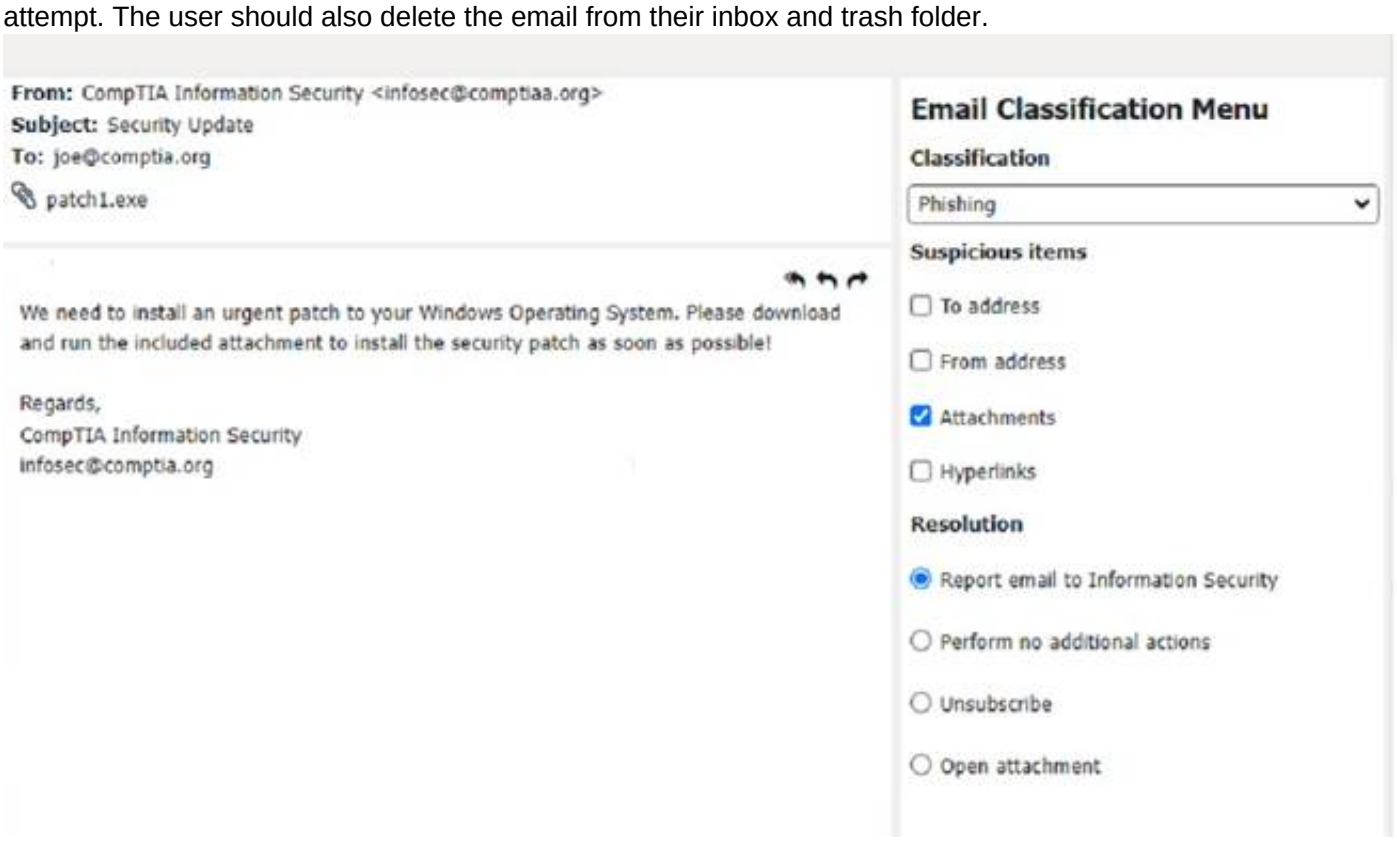
Classification: b) Spam
This email is a spam email, as it is an unsolicited and unwanted message that tries to persuade the user to participate in a survey and claim a reward. Some suspicious items in this email are:
? The email offers a free wireless headphone as an incentive, which is too good to
be true.
? The email does not provide any details about the survey company, such as its name, address, or contact information.
? The email contains an external survey link, which may lead to a malicious or fraudulent website.
? The email does not have an unsubscribe option, which is required by law for commercial emails.
The appropriate resolution for this email is C. Unsubscribe. The user should look for an unsubscribe link or button at the bottom of the email and follow the instructions to opt out of receiving future emails from the sender. The user should also mark the email as spam or junk in their email client, which will help filter out similar emails in the future. The user should not click on the survey link, reply to the email, or provide any personal or financial information.



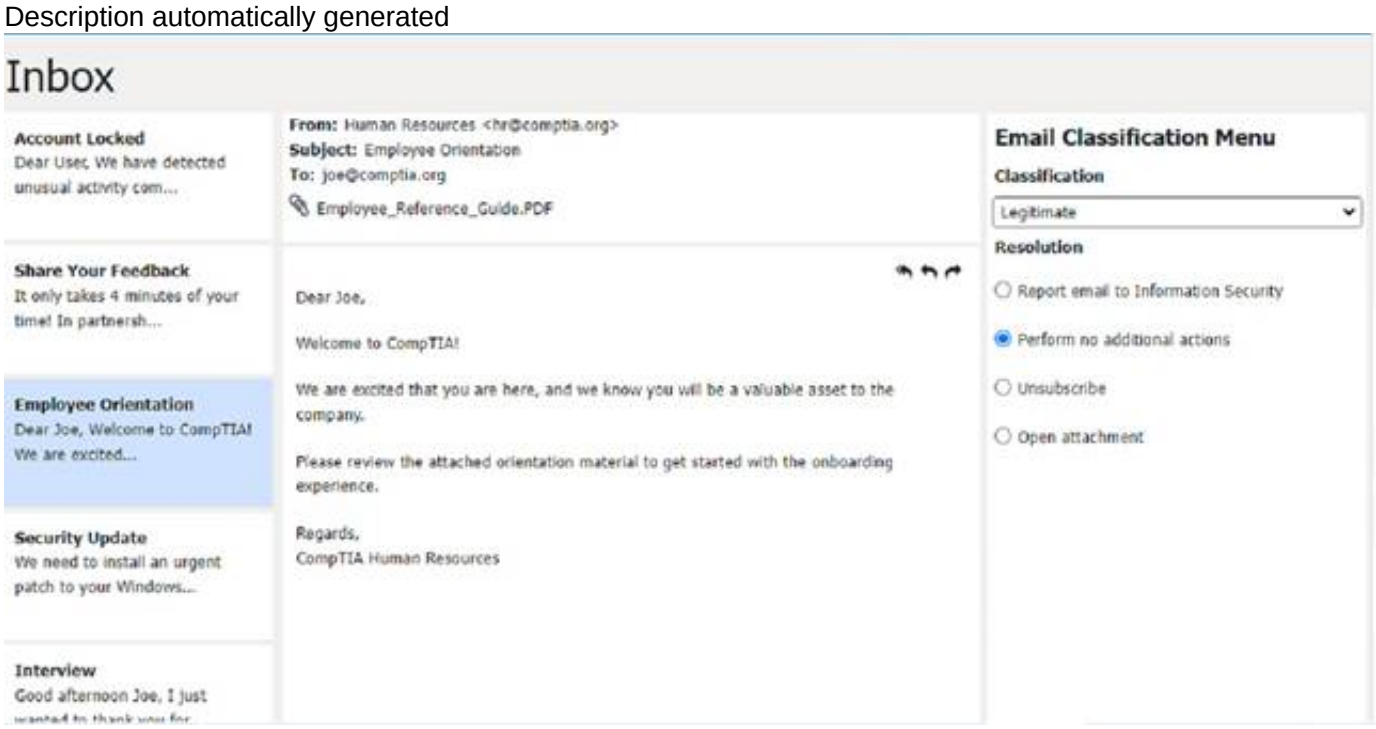
Classification: c) Legitimate
This email is a legitimate email, as it is from a trusted source and has a valid purpose. There are no suspicious items in this email, as the from address, the to address, the attachment, and the email body are all consistent and relevant. The appropriate resolution for this email is B. Perform no additional actions. The user can open the attachment and review the orientation material as instructed. The user does not need to report, unsubscribe, or delete this email.



A screenshot of a computer
Description automatically generated
Classification: a) Phishing
This email is a phishing attempt, as it tries to deceive the user into downloading and running a malicious attachment that could compromise their system or data. Some suspicious items in this email are:
? The email has a generic greeting and does not address the user by name or username.
? The email has an urgent tone and claims that a security patch needs to be installed immediately.
? The email has an attachment named “patch1.exe”, which is an executable file that could contain malware or ransomware.
? The email does not match the official format or domain of CompTIA Information Security.
The appropriate resolution for this email is A. Report email to Information Security. The user should not open the attachment, reply to the email, or provide any personal or account information. The user should forward the email to the Information Security team or use a professional email form to report the phishing attempt. The user should also delete the email from their inbox and trash folder.



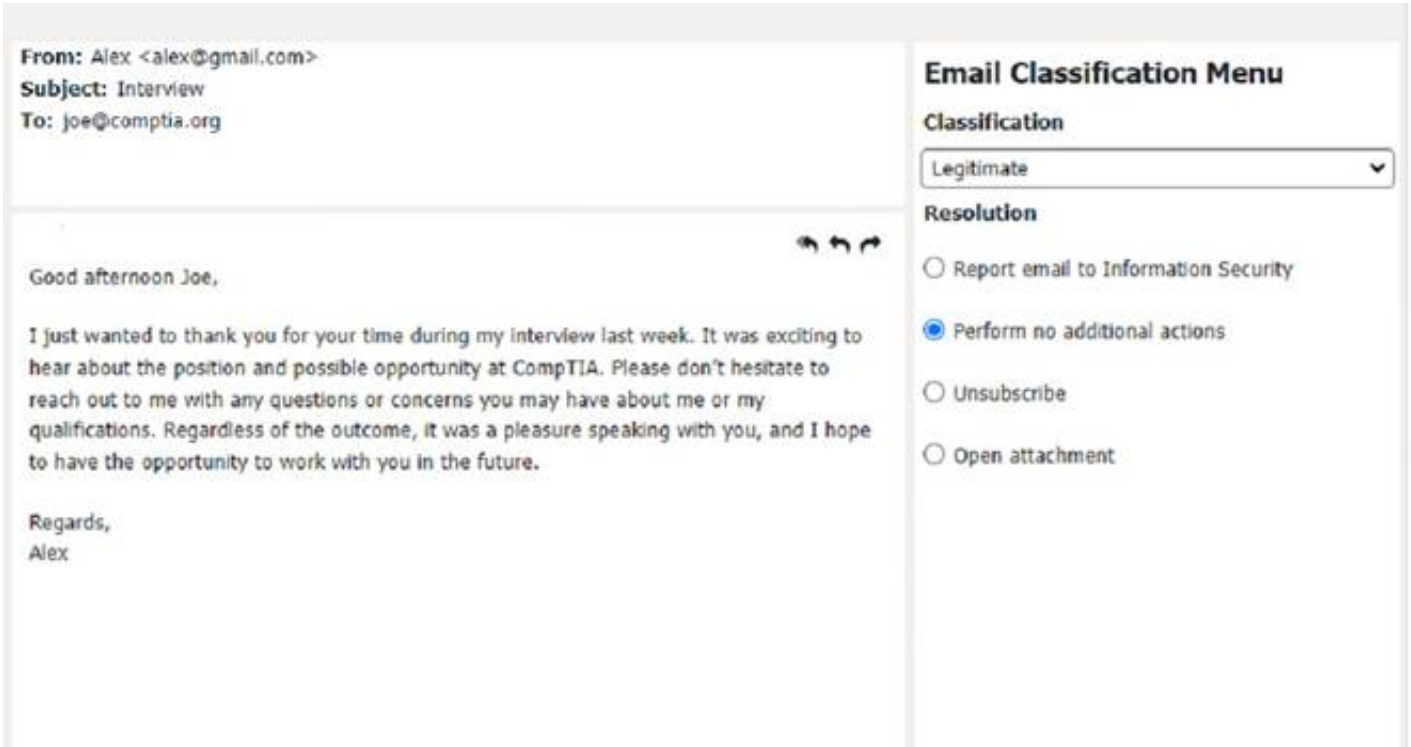
A screenshot of a computer
Description automatically generated



Classification: c) Legitimate

This email is a legitimate email, as it is from a trusted source and has a valid purpose. There are no suspicious items in this email, as the from address, the to address, and the email body are all consistent and relevant. The appropriate resolution for this email is B.

Perform no additional actions. The user can reply to the email and thank the sender for the interview opportunity. The user does not need to report, unsubscribe, or delete this email.



A screenshot of a computer
Description automatically generated

NEW QUESTION 55
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 60
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
Backups
F.

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 61
A user reported that a laptop's screen turns off very quickly after silting for a few moments and is also very dim when not plugged in to an outlet Everything else seems to be functioning normally. Which of the following Windows settings should be configured?

A. Power Plans
B. Hibernate
C. Sleep/Suspend
D. Screensaver

Answer: A

Explanation:
Power Plans are Windows settings that allow a user to configure how a laptop's screen behaves when plugged in or running on battery power. They can adjust the screen brightness and the time before the screen turns off due to inactivity. Hibernate, Sleep/Suspend and Screensaver are other Windows settings that affect how a laptop's screen behaves, but they do not allow changing the screen brightness or turning off time. Verified References: https://www.comptia.org/blog/windows-power-plans https://www.comptia.org/certifications/a

NEW QUESTION 65
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 70
A user recently purchased a second monitor and wants to extend the Windows desktop to the new screen. Which of the following Control Panel options should a technician adjust to help the user?

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

Answer: D

NEW QUESTION 73
A technician has verified that a user's computer has a virus and the antivirus software is out of date. Which of the following steps should the technician take next?

A. Quarantine the computer.
B. Use a previous restore point.
C. Educate the end user about viruses.
D. Download the latest virus definitions.

Answer: D

Explanation:
The first step in removing a virus from a computer is to update the antivirus software with the latest virus definitions. Virus definitions are files that contain information about the characteristics and behavior of known viruses and malware. They help the antivirus software to identify and remove the malicious threats from the computer. Without the latest virus definitions, the antivirus software may not be able to detect or remove the virus that infected the user's computer. Therefore, the technician should download the latest virus definitions from the antivirus vendor's website or use the update feature in the antivirus program before scanning the computer for viruses.
References:
? How to remove malware or viruses from my Windows 10 PC, section 21
? How to Remove a Virus From a Computer in 2023, section 32

? The Official CompTIA A+ Core 2 Study Guide (220-1102), page 2193

NEW QUESTION 77
A junior administrator is responsible for deploying software to a large group of computers in an organization. The administrator finds a script on a popular coding website to automate this distribution but does not understand the scripting language. Which of the following BEST describes the risks in running this script?

A. The instructions from the software company are not being followed.
B. Security controls will treat automated deployments as malware.
C. The deployment script is performing unknown actions.
D. Copying scripts off the internet is considered plagiarism.

Answer: C

Explanation:
The risks in running this script are that the deployment script is performing unknown actions. Running the script blindly could cause unintended actions, such as deploying malware or deleting important files, which could negatively impact the organization's network and data1.

NEW QUESTION 80
The findings from a security audit indicate the risk of data loss from lost or stolen laptops is high. The company wants to reduce this risk with minimal impact to users who want to use their laptops when not on the network. Which of the following would BEST reduce this risk for Windows laptop users?

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

Answer: D

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

NEW QUESTION 82
A user's corporate phone was stolen, and the device contains company trade secrets. Which of the following technologies should be implemented to mitigate this risk? (Select TWO).

A. Remote wipe
B. Firewall
C. Device encryption
D. Remote backup
E. Antivirus
F. Global Positioning System

Answer: AC

Explanation:
Remote wipe is a feature that allows data to be deleted from a device or system remotely by an administrator or owner1. It is used to protect data from being compromised if the device is lost, stolen, or changed hands1. Device encryption is a feature that helps protect the data on a device by making it unreadable to unauthorized users2. It requires a key or a password to access the data2. Both features can help mitigate the risk of losing company trade secrets if a corporate phone is stolen.
References: 1: How to remote wipe Windows laptop (https://www.thewindowsclub.com/remote-wipe-windows-10) 2: Device encryption in Windows (https://support.microsoft.com/en-us/windows/device-encryption-in-windows-ad5dcf4b-dbe0-2331-228f-7925c2a3012d)

NEW QUESTION 86
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 90
A user reports an issue when connecting a mobile device to Bluetooth. The user states the mobile device's Bluetooth is turned on. Which of the following steps should the technician take NEXT to resolve the issue?

A. Restart the mobile device.
B. Turn on airplane mode.
C. Check that the accessory is ready to pair.
D. Clear all devices from the phone's Bluetooth settings.

Answer: C

Explanation:
The first step in troubleshooting a Bluetooth connection issue is to check that the accessory is ready to pair with the mobile device. Some accessories may have a button or a switch that needs to be pressed or turned on to initiate pairing mode. If the accessory is not ready to pair, the mobile device will not be able to detect it.
Reference: CompTIA A+ Core 2 Exam Objectives, Section 2.4

NEW QUESTION 95
A user in a corporate office reports the inability to connect to any network drives. No other users have reported this issue. Which of the following is the MOST likely reason the user is having this issue?

A. Mastered
B. Not Mastered

Answer: A

NEW QUESTION 96
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 99
A technician, who is working at a local office, has found multiple copies of home edition software installed on computers. Which of the following does this MOST likely violate?

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

Answer: A

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

NEW QUESTION 102
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 104
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 107
A Windows workstation that was recently updated with approved system patches shut down instead of restarting. Upon reboot, the technician notices an alert stating the workstation has malware in the root OS folder. The technician promptly performs a System Restore and reboots the workstation, but the malware is still detected. Which of the following BEST describes why the system still has malware?

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

Answer: D

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

NEW QUESTION 109
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 111
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 112
A systems administrator is setting up a Windows computer for a new user Corporate policy requires a least privilege environment. The user will need to access advanced features and configuration settings for several applications. Which of the following BEST describes the account access level the user will need?

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

Answer: B

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

NEW QUESTION 116
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 117
A developer's Type 2 hypervisor is performing inadequately when compiling new source code. Which of the following components should the developer upgrade to improve the hypervisor’s performance?

A. Amount of system RAM
B. NIC performance
C. Storage IOPS
D. Dedicated GPU

Answer: A

Explanation:
The correct answer is A. Amount of system RAM. A Type 2 hypervisor is a virtualization software that runs on top of a host operating system, which means it shares the system resources with the host OS and other applications. Therefore, increasing the amount of system RAM can improve the performance of the hypervisor and the virtual machines running on it. RAM is used to store data and instructions that are frequently accessed by the CPU, and having more RAM can reduce the need for swapping data to and from the storage device, which is slower than RAM.
NIC performance, storage IOPS, and dedicated GPU are not as relevant for improving the hypervisor’s performance in this scenario. NIC performance refers to the speed and quality of the network interface card, which is used to connect the computer to a network. Storage IOPS refers to the number of input/output operations per second that can be performed by the storage device, which is a measure of its speed and efficiency. Dedicated GPU refers to a separate graphics processing unit that can handle complex graphics tasks, such as gaming or video editing. These components may affect other aspects of the computer’s performance, but they are not directly related to the hypervisor’s ability to compile new source code.

NEW QUESTION 120
The network was breached over the weekend System logs indicate that a single user's account was successfully breached after 500 attempts with a dictionary attack. Which of the following would BEST mitigate this threat?

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

Answer: B

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

NEW QUESTION 125
A user rotates a cell phone horizontally to read emails, but the display remains vertical, even though the settings indicate autorotate is on. VT1ich of the following will MOST likely resolve the issue?

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

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 126
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 131
Which of the following Is a package management utility for PCs that are running the Linux operating system?

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

Answer: B

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

NEW QUESTION 136
Which of the following is a proprietary Cisco AAA protocol?

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

Answer: D

Explanation:
TACACS+ is a proprietary Cisco AAA protocol

NEW QUESTION 141
A systems administrator is creating periodic backups of a folder on a Microsoft Windows machine. The source data is very dynamic, and files are either added or deleted regularly. Which of the following utilities can be used to 'mirror the source data for the backup?

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

Answer: C

Explanation:
Robocopy is a command-line utility that can be used to mirror the source data for the backup. It can copy files and folders with various options, such as copying only changed files, preserving attributes and permissions, and retrying failed copies. Robocopy is more powerful and flexible than copy or xcopy, which are simpler commands that can only copy files and folders without mirroring or other advanced features. Copy-Item is a PowerShell cmdlet that can also copy files and folders, but it is not a native Windows utility and it requires PowerShell to run1.
References: 1: https://windowsreport.com/mirror-backup-software/

NEW QUESTION 146
A technician is troubleshooting a PC that has been performing poorly. Looking at the Task Manager, the technician sees that CPU and memory resources seem fine, but disk throughput is at 100%.
Which of the following types of malware is the system MOST likely infected with?

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

Answer: C

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

NEW QUESTION 151
A user's antivirus software reports an infection that it is unable to remove. Which of the following is the most appropriate way to remediate the issue?

A. Disable System Restore.
B. Utilize a Linux live disc.
C. Quarantine the infected system.
D. Update the anti-malware.

Answer: C

Explanation:
Quarantining the infected system is the most appropriate way to remediate the issue of an infection that the antivirus software cannot remove. Quarantining means isolating the system from the network and other devices to prevent the infection from spreading or causing further damage. Quarantining also allows the technician to perform further analysis and removal of the infection without risking the security of other systems or data.
Some of the steps involved in quarantining an infected system are:
? Disconnect the system from the internet and any local network connections, such as Wi-Fi, Ethernet, Bluetooth, or USB.
? Disable any file-sharing or remote access services on the system, such as Windows File Sharing, Remote Desktop, or TeamViewer.
? Use a separate device to download and update the antivirus software and any other tools that may be needed to remove the infection, such as malware scanners, rootkit removers, or bootable rescue disks.
? Transfer the updated antivirus software and tools to the infected system using a removable media, such as a CD, DVD, or USB flash drive. Scan the removable media for any infections before and after using it on the infected system.
? Run the antivirus software and tools on the infected system and follow the instructions to delete or quarantine the infection. If the infection is persistent or complex, it may require booting the system from a rescue disk or using a Linux live disc to access and clean the system files.
? After the infection is removed, restore the system to a previous clean state using
System Restore, backup, or recovery partition. Scan the system again to ensure that it is clean and secure. Reconnect the system to the network and update the system and the antivirus software.
References:
? How to Identify and Repair Malware or Virus Infected Computers, section 31
? Uninstalling Antivirus Software, the Clean Way: 40 Removal Tools & Instructions, section 22
? How to manually remove an infected file from a Windows computer3
? The Official CompTIA A+ Core 2 Study Guide (220-1102), page 2194

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 158
A customer calls a service support center and begins yelling at a technician about a feature for a product that is not working to the customer's satisfaction. This feature is not supported by the service support center and requires a field technician to troubleshoot. The customer continues to demand service. Which of the following is the BEST course of action for the support center representative to take?

A. Inform the customer that the issue is not within the scope of this department.
B. Apologize to the customer and escalate the issue to a manager.
C. Ask the customer to explain the issue and then try to fix it independently.
D. Respond that the issue is something the customer should be able to fix.

Answer: B

Explanation:
Apologizing to the customer and escalating the issue to a manager is the best course of action for the support center representative to take. This shows empathy and professionalism and allows the manager to handle the situation and provide the appropriate service or resolution for the customer.

NEW QUESTION 160
A technician is installing new software on a macOS computer. Which of the following file types will the technician MOST likely use?

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

Answer: D

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

NEW QUESTION 164
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 168
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 169
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 174
The command cac cor.ptia. txt was issued on a Linux terminal. Which of the following results should be expected?

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

Answer: B

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

NEW QUESTION 179
A technician needs to remotely connect to a Linux desktop to assist a user with troubleshooting. The technician needs to make use of a tool natively designed for Linux. Which of the following tools will the technician MOST likely use?

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

Answer: A

Explanation:
The tool that the technician will most likely use to remotely connect to a Linux desktop is VNC. VNC stands for Virtual Network Computing and is a protocol that allows remote access and control of a graphical desktop environment over a network. VNC is natively designed for Linux and can also support other operating systems, such as Windows and Mac OS. VNC can be used to assist users with troubleshooting by viewing and interacting with their desktops remotely. MFA stands for Multi-Factor Authentication and is a method of verifying identity using two or more factors, such as something you know, something you have or something you are. MFA is not a tool that can be used to remotely connect to a Linux desktop but a technique that can be used to enhance security

for systems or services. MSRA stands for Microsoft Remote Assistance and is a feature that allows remote access and control of a Windows desktop environment over a network. MSRA is not natively designed for Linux and may not be compatible or supported by Linux systems. RDP stands for Remote Desktop Protocol and is a protocol that allows remote access and control of a Windows desktop environment over a network. RDP is not natively designed for Linux and may not be compatible or supported by Linux systems. References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.6

NEW QUESTION 182
An application user received an email indicating the version of the application currently in use will no longer be sold. Users with this version of the application will no longer receive patches or updates either. Which of the following indicates a vendor no longer supports a product?

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

Answer: C

Explanation:
EOL (end-of-life) is a term that indicates a vendor no longer supports a product. It means that the product will no longer be sold, updated or patched by the vendor, and that the users should migrate to a newer version or alternative product. AUP (acceptable use policy), EULA (end-user license agreement) and UAC (user account control) are not terms that indicate a vendor no longer supports a product. Verified References: https://www.comptia.org/blog/what-is-end-of-life https://www.comptia.org/certifications/a

NEW QUESTION 184
A company would like to implement multifactor authentication for all employees at a minimal cost. Which of the following best meets the company's requirements?

A. Biometrics
B. Soft token
C. Access control lists
D. Smart card

Answer: B

Explanation:
A soft token, also known as a software token or an OTP (one-time password) app, is a type of multifactor authentication that generates a temporary code or password on a user’s device, such as a smartphone or a tablet. The user must enter this code or password along with their username and password to access their account or service. A soft token can help improve security by adding an extra layer of verification and preventing unauthorized access even if the user’s

credentials are compromised. A soft token can also be implemented at a minimal cost, as it does not require any additional hardware or infrastructure. Biometrics, access control lists, and smart card are not types of multifactor authentication that can be implemented at a minimal cost.

NEW QUESTION 186
Which of the following is used to explain issues that may occur during a change implementation?

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

Answer: C

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

NEW QUESTION 189
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 193

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 198
A neighbor successfully connected to a user's Wi-Fi network. Which of the following should the user do after changing the network configuration to prevent the neighbor from being able to connect again?

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

Answer: A

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

NEW QUESTION 199
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 203
A technician is finalizing a new workstation for a user. The user's PC will be connected to the internet but will not require the same private address each time. Which of the following protocols will the technician MOST likely utilize?

A. DHCP
B. SMTP
C. DNS
D. RDP

Answer: A

Explanation:
DHCP stands for Dynamic Host Configuration Protocol and it is used to assign IP addresses and other network configuration parameters to devices on a network automatically. This is useful for devices that do not require the same private address each time they connect to the internet.

NEW QUESTION 207
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 209
A macOS user reports seeing a spinning round cursor on a program that appears to be frozen. Which of the following methods does the technician use to force the program to close in macOS?

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

Answer: D

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

NEW QUESTION 213
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 217
A user updates a mobile device's OS. A frequently used application becomes consistently unresponsive immediately after the device is launched. Which of the following troubleshooting steps should the user perform FIRST?

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

Answer: B

Explanation:
Checking for application updates is the first troubleshooting step that the user should perform, because the application may not be compatible with the new OS version and may need an update to fix the issue. Deleting the application's cache, rolling back the OS update, or uninstalling and reinstalling the application are possible solutions, but they are more time-consuming and disruptive than checking for updates. References: : https://www.comptia.org/training/resources/exam-objectives/comptia-a-core-2-exam- objectives : https://www.lifewire.com/how-to-update-apps-on-android-4173855

NEW QUESTION 222
A user attempts to install additional software and receives a UAC prompt. Which of the following is the BEST way to resolve this issue?

A. Add a user account to the local administrator's group.
B. Configure Windows Defender Firewall to allow access to all networks.
C. Create a Microsoft account.
D. Disable the guest account.

Answer: A

Explanation:
A user account that belongs to the local administrator's group has the permission to install software on a Windows machine. If a user receives a UAC (user account control) prompt when trying to install software, it means the user does not have enough privileges and needs to enter an administrator's password or switch to an administrator's account. Adding the user account to the local administrator's group can resolve this issue. Configuring Windows Defender Firewall, creating a Microsoft account and disabling the guest account are not related to this issue. Verified References: https://www.comptia.org/blog/user-account-control https://www.comptia.org/certifications/a

NEW QUESTION 223
Which of the following should be done NEXT?

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

Answer: D

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

NEW QUESTION 226
A technician requires graphical remote access to various Windows, Linux, and macOS desktops on the company LAN. The security administrator asks the technician to utilize a single software solution that does not require an external internet connection. Which of the following remote access tools is the technician most likely to install?

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

Answer: A

Explanation:
VNC (Virtual Network Computing) is a remote access tool that allows the technician to access and control various Windows, Linux, and macOS desktops on the company LAN using a graphical user interface. VNC does not require an external internet connection, as it works over a local network or a VPN. VNC uses a client-

server model, where the server runs on the remote desktop and the client connects to it from another device. VNC can transmit the keyboard and mouse events from the client to the server, and the screen updates from the server to the client, enabling the technician to interact with the remote desktop as if it were local12.
VNC is a better option than the other choices because:
? RMM (Remote Monitoring and Management) (B) is not a single software solution, but a category of software solutions that enable IT professionals to remotely monitor, manage, and troubleshoot multiple devices and networks. RMM software may include remote access tools, but also other features such as patch management, backup and recovery, security, reporting, and automation. RMM software may require an external internet connection, as it often relies on cloud-based services or web-based consoles34.
? RDP (Remote Desktop Protocol) © is a remote access tool that allows the technician to access and control Windows desktops on the company LAN using a graphical user interface. However, RDP is not compatible with Linux or macOS desktops, unless they have third-party software installed that can emulate or translate the RDP protocol. RDP also has some security and performance issues, such as encryption vulnerabilities, bandwidth consumption, and latency problems56.
? SSH (Secure Shell) (D) is a remote access tool that allows the technician to access and control various Windows, Linux, and macOS desktops on the company LAN using a command-line interface. SSH does not require an external internet connection, as it works over a local network or a VPN. SSH uses encryption and authentication to secure the communication between the client and the server. However, SSH does not provide a graphical user interface, which may limit the functionality and usability of the remote desktop7 .
References:
1: What is VNC? - Definition from Techopedia1 2: How VNC Works - RealVNC2 3: What is Remote Monitoring and Management (RMM)? - Definition from Techopedia3 4: What is RMM Software? - NinjaRMM4 5: What is Remote Desktop Protocol (RDP)? - Definition from Techopedia5 6: Remote Desktop Protocol: What it is and how to secure it - CSO Online6 7: What is Secure Shell (SSH)? - Definition from Techopedia7 : How to Use SSH to Access a Remote Server in Linux or Windows - Hostinger Tutorials

NEW QUESTION 229
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 232
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 Agreenment Reference: https://www.youtube.com/watch?v=Ru77iZxuElA&list=PLG49S3nxzAnna96gzhJrzkii4hH_mgW4b&index=59

NEW QUESTION 235
A remote user is having issues accessing an online share. Which of the following tools would MOST likely be used to troubleshoot the Issue?

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

Answer: A

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

NEW QUESTION 240
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 243
A technician is trying to encrypt a single folder on a PC. Which of the following should the technician use to accomplish this task?

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

Answer: D

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

NEW QUESTION 248
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 250
A macOS user is installing a new application. Which of the following system directories is the software MOST likely to install by default?

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

Answer: B

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

NEW QUESTION 251
A user receives a notification indicating the antivirus protection on a company laptop is out of date. A technician is able to ping the user's laptop. The technician checks the antivirus parent servers and sees the latest signatures have been installed. The technician then checks the user's laptop and finds the antivirus engine and definitions are current. Which of the following has MOST likely occurred?

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

Answer: B

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

NEW QUESTION 255
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 259
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 261
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 263
A user receives an error message from an online banking site that states the following:
Your connection is not private. Authority invalid.
Which of the following actions should the user take NEXT?

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

Answer: C

Explanation:
The error message “Your connection is not private. Authority invalid.” means that the web browser cannot verify the identity or security of the website’s SSL certificate. This could indicate that the website has been compromised, has a configuration error, or has an expired or invalid certificate. The user should not proceed to the site or use a different browser, as this could expose their sensitive information to potential attackers. The user should also not reinstall the browser, as this is unlikely to fix the error and could cause data loss. The best action for the user to take is to report the error to the bank and wait for them to resolve it. References: : How to Fix “Your Connection Is Not Private” Errors (https://www.howtogeek.com/874436/how-to-fix-your-connection-is-not-private-errors/) : Fix connection errors (https://support.google.com/chrome/answer/6098869?hl=en)

NEW QUESTION 264
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 266
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 268
A technician successfully removed malicious software from an infected computer after running updates and scheduled scans to mitigate future risks. Which of the following should the technician do next?

A. Educate the end user on best practices for security.
B. Quarantine the host in the antivirus system.
C. Investigate how the system was infected with malware.
D. Create a system restore point.

Answer: A

Explanation:
Educating the end user on best practices for security is the next step that the technician should take after successfully removing malicious software from an infected computer. Educating the end user on best practices for security is an important part of preventing future infections and mitigating risks. The technician should explain to the end user how to avoid common sources of malware, such as phishing emails, malicious websites, or removable media. The technician should also advise the end user to use strong passwords, update software regularly, enable antivirus and firewall protection, and backup data frequently. Educating the end user on best practices for security can help the end user become more aware and responsible for their own security and reduce the likelihood of recurrence of malware infections. Quarantining the host in the antivirus system, investigating how the system was infected with malware, and creating a system restore point are not the next steps that the technician should take after successfully removing malicious software from an infected computer. Quarantining the host in the antivirus system is a step that the technician should take before removing malicious software from an infected computer. Quarantining the host in the antivirus system means isolating the infected computer from the network or other devices to prevent the spread of malware. Investigating how the system was infected with malware is a step that the technician should take during or after removing malicious software from an infected computer. Investigating how the system was infected with malware means identifying the source, type, and impact of malware on the system and documenting the findings and actions taken. Creating a system restore point is a step that the technician should take before removing malicious software from an infected computer. Creating a system restore point means saving a snapshot of the system’s configuration and settings at a certain point in time, which can be used to restore the system in case of failure or corruption. References:
? Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 15
? CompTIA A+ Core 1 (220-1101) and Core 2 (220-1102) Cert Guide, page 458

NEW QUESTION 270
A user connected an external hard drive but is unable to see it as a destination to save files. Which of the following tools will allow the drive to be formatted?

A. Disk Management
B. Device Manager
C. Disk Cleanup
D. Disk Defragmenter

Answer: A

Explanation:
Disk Management is a tool that allows users to create, format, delete, shrink, extend, and manage partitions on hard drives. If the external hard drive is not formatted or has an incompatible filesystem type, Disk Management can be used to format it with a supported filesystem type such as NTFS, FAT32, or exFAT. Device Manager, Disk Cleanup, and Disk Defragmenter are not tools that can format a hard drive.

NEW QUESTION 271
A user reports seeing random, seemingly non-malicious advertisement notifications in the Windows 10 Action Center. The notifications indicate the advertisements are coming from a web browser. Which of the following is the best solution for a technician to implement?

A. Disable the browser from sending notifications to the Action Center.
B. Run a full antivirus scan on the computer.
C. Disable all Action Center notifications.
D. Move specific site notifications from Allowed to Block.

Answer: A

Explanation:

The best solution for a technician to implement is to disable the browser from sending notifications to the Action Center. This will prevent the random advertisement notifications from appearing in the Windows 10 Action Center, which can be annoying and distracting for the user. The technician can follow these steps to disable the browser notifications1:
? Open the browser that is sending the notifications, such as Microsoft Edge, Google Chrome, or Mozilla Firefox.
? Go to the browser settings or options menu, and look for the privacy and security section.
? Find the option to manage site permissions or notifications, and click on it.
? You will see a list of sites that are allowed or blocked from sending notifications to the browser and the Action Center. You can either block all sites from sending notifications, or select specific sites that you want to block or allow.
? Save the changes and close the browser settings. This solution is better than the other options because:
? Running a full antivirus scan on the computer (B) is not necessary, as the advertisement notifications are not malicious or harmful, and they are not caused by a virus or malware infection. Running a scan will not stop the notifications from appearing, and it will consume system resources and time.
? Disabling all Action Center notifications © is not advisable, as the Action Center is a useful feature that shows notifications and alerts from various apps and system events, such as email, calendar, security, updates, etc. Disabling all notifications will make the user miss important information and reminders, and reduce the functionality of the Action Center.
? Moving specific site notifications from Allowed to Block (D) is not the best solution, as it will only stop the notifications from some sites, but not from others. The user may still receive advertisement notifications from other sites that are not blocked, or from new sites that are added to the Allowed list. This solution will also require the user to manually manage the list of sites, which can be tedious and time- consuming.
References:
1: How to Disable Annoying Browser Notifications - PCMag

NEW QUESTION 274
A technician is selling 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:
An unattended installation is the fastest way to install Windows 10 on a newly built computer. It uses an answer file that contains all the configuration settings and preferences for the installation, such as language, product key, partition size, etc. It does not require any user interaction or input during the installation process. Factory reset, System Restore and in-place upgrade are not methods of installing Windows 10 on a new computer, but ways of restoring or updating an existing Windows installation. Verified References: https://www.comptia.org/blog/what-is-an-unattended-installation https://www.comptia.org/certifications/a

NEW QUESTION 276
A call center handles inquiries into billing issues for multiple medical facilities. A security analyst notices that call center agents often walk away from their workstations, leaving patient data visible for anyone to see. Which of the following should a network administrator do to BEST prevent data theft within the call center?

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

Answer: B

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

NEW QUESTION 281
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 220-1102 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 220-1102 Product From:

https://www.2passeasy.com/dumps/220-1102/

Money Back Guarantee

220-1102 Practice Exam Features:

* 220-1102 Questions and Answers Updated Frequently

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

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

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