CompTIA

Exam Questions 220-1102

CompTIA A+ Certification Exam: Core 2

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
A user is no longer able to start the OS on a computer and receives an error message indicating there is no OS found. A technician reviews the audit logs and notes that the user's system posted a S.M.A.R.T. error just days before this issue. Which of the following is the MOST likely cause of this issue?

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

Answer: C

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

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

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

Answer: EG

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

NEW QUESTION 3
Which of the following 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 4
A technician installed a new application on a workstation. For the program to function
properly, it needs to be listed in the Path Environment Variable. Which of the following Control Panel utilities should the technician use?

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

Answer: A

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

NEW QUESTION 5
A new spam gateway was recently deployed at a small business However; users still occasionally receive spam. The management team is concerned that users will open the messages and potentially
infect the network systems. Which of the following is the MOST effective method for dealing with this Issue?

A. Adjusting the spam gateway
B. Updating firmware for the spam appliance

C. Adjusting AV settings
D. Providing user training

Answer: D

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

NEW QUESTION 6
An administrator has submitted a change request for an upcoming server deployment. Which of the following must be completed before the change can be approved?

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

Answer: A

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

NEW QUESTION 7
A user connected a smartphone to a coffee shop's public Wi-Fi and noticed the smartphone started sending unusual SMS messages and registering strange network activity A technician thinks a virus or other malware has infected the device. Which of the following should the technician suggest the user do to best address these security and privacy concerns? (Select two).

A. Disable Wi-Fi autoconnect.
B. Stay offline when in public places.
C. Uninstall all recently installed applications.
D. Schedule an antivirus scan.
E. Reboot the device
F. Update the OS

Answer: CD

Explanation:
The best way to address the security and privacy concerns caused by a malware infection on a smartphone is to uninstall all recently installed applications and schedule an antivirus scan. Uninstalling the applications that may have introduced the malware can help remove the source of infection and prevent further damage. Scheduling an antivirus scan can help detect and remove any remaining traces of malware and restore the device's functionality. References: CompTIA A+ Core 2 (220-1102) Certification Study Guide, Chapter 5: Mobile Devices, Section 5.3: Mobile Device Security1

NEW QUESTION 8
A technician is securing a new Windows 10 workstation and wants to enable a Screensaver lock. Which of the following options in the Windows settings should the technician use?

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

Answer: C

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

NEW QUESTION 9
Which of the following is the most likely reason a filtration system is critical for data centers?

A. Plastics degrade over time.
B. High humidity levels can rust metal.
C. Insects can invade the data center.
D. Dust particles can clog the machines.

Answer: B

Explanation:
A filtration system is critical for data centers because it can control the humidity and temperature levels in the environment. High humidity levels can cause condensation and corrosion on the metal components of the servers and other equipment, leading to malfunction and damage. A filtration system can also prevent dust, dirt, and other contaminants from entering the data center and clogging the machines or causing overheating.

NEW QUESTION 10
A technician is troubleshooting a mobile device that was dropped. The technician finds that the screen (ails to rotate, even though the settings are correctly applied. Which of the following pieces of hardware should the technician replace to resolve the issue?

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

Answer: C

Explanation:
The piece of hardware that the technician should replace to resolve the issue of the screen failing to rotate on a mobile device that was dropped is the accelerometer. The accelerometer is a sensor that detects the orientation and movement of the mobile device by measuring the acceleration forces acting on it. The accelerometer allows the screen to rotate automatically according to the position and angle of the device. If the accelerometer is damaged or malfunctioning, the screen may not rotate properly or at all, even if the settings are correctly applied. LCD stands for Liquid Crystal Display and is a type of display that uses liquid crystals and backlight to produce images on the screen. LCD is not related to the screen rotation feature but to the quality and brightness of the display. Battery is a component that provides power to the mobile device by storing and releasing electrical energy. Battery is not related to the screen rotation feature but to the battery life and performance of the device. Digitizer is a component that converts touch inputs into digital signals that can be processed by the mobile device. Digitizer is not related to the screen rotation feature but to the touch sensitivity and accuracy of the display. References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.5

NEW QUESTION 10
A user requires a drive to be mapped through a Windows command line. Which of the following command-line tools can be utilized to map the drive?

A. gpupdate
B. net use
C. hostname
D. dir

Answer: B

Explanation:
Net use is a command-line tool that can be used to map a drive in Windows. Mapping a drive means assigning a drive letter to a network location or a local folder, which allows the user to access it more easily and quickly. Net use can also be used to disconnect a mapped drive, display information about mapped drives, or connect to shared resources on another computer. Gpupdate, hostname, and dir are not command-line tools that can be used to map a drive.

NEW QUESTION 12
Antivirus software indicates that a workstation is infected with ransomware that cannot be quarantined. Which of the following should be performed first to prevent further damage to the host and other systems?

A. Turn off the machine.
B. Run a full antivirus scan.
C. Remove the LAN card.
D. Install a different endpoint solution.

Answer: A

Explanation:
Turning off the machine is the first and most urgent step to prevent further damage to the host and other systems. Ransomware can encrypt files, steal data, and spread to other devices on the network if the infected machine remains online. Turning off the machine will stop the ransomware process and isolate the machine from the network12. The other options are either ineffective or risky. Running a full antivirus scan may not detect or remove the ransomware, especially if it is a new or unknown variant. Removing the LAN card may disconnect the machine from the network, but it will not stop the ransomware from encrypting or deleting files on the local drive. Installing a different endpoint solution may not be possible or helpful if the ransomware has already compromised the system or blocked the installation.
References: 1 3 steps to prevent and recover from ransomware(https://www.microsoft.com/en-us/security/blog/2021/09/07/3-steps-to-prevent- and-recover-from-ransomware/)2 #StopRansomware Guide | CISA(https://www.cisa.gov/stopransomware/ransomware-guide).

NEW QUESTION 17
An office is experiencing constant connection attempts to the corporate Wi-Fi. Which of the following should be disabled to mitigate connection attempts?

A. SSID
B. DHCP
C. Firewall
D. SSD

Answer: A

Explanation:
The SSID (Service Set Identifier) is the name of a wireless network that is broadcasted by the router or the Wi-Fi base station. The SSID helps nearby devices to

identify and connect to the available networks. However, broadcasting the SSID also exposes the network to potential connection attempts from unauthorized or malicious users. Therefore, disabling the SSID can mitigate connection attempts by making the network invisible or hidden to the devices that are not already connected to it. To connect to a hidden network, the user would need to know the exact SSID and enter it manually. The other options are not related to mitigating connection attempts to the corporate Wi-Fi. DHCP (Dynamic Host Configuration Protocol) is a protocol that assigns IP addresses to the devices on a network. Firewall is a software or hardware device that filters the incoming and outgoing network traffic based on predefined rules. SSD (Solid State Drive) is a type of storage device that uses flash memory to store data. Disabling any of these options would not prevent connection attempts to the Wi-Fi network, and may cause other problems or issues for the network functionality and performance.
References:
? What is SSID + how to find (and change) it1
? Choosing an SSID2
? SSID Meaning: Finding Your Network's Name3

NEW QUESTION 20
An Android user contacts the help desk because a company smartphone failed to complete a tethered OS update A technician determines there are no error messages on the device Which of the following should the technician do NEXT?

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

Answer: C

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

NEW QUESTION 25
Which of the following features allows a technician to configure policies in a Windows 10 Professional desktop?

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

Answer: A

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

NEW QUESTION 29
A technician is modifying the default home page of all the workstations in a company. Which of the following will help to implement this change?

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

Answer: A

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

NEW QUESTION 33
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 36
A technician is setting up a new laptop. The company's security policy states that users cannot install virtual machines. Which of the following should the technician implement to prevent users from enabling virtual technology on their laptops?

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

Answer: B

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

NEW QUESTION 40
A company acquired a local office, and a technician is attempting to join the machines at the office to the local domain. The technician notes that the domain join option appears to be missing. Which of the following editions of Windows is MOST likely installed on the machines?

A. Windows Professional
B. Windows Education
C. Windows Enterprise
D. Windows Home

Answer: D

Explanation:
Windows Home is the most likely edition of Windows installed on the machines that do not have the domain join option. Windows Home is a consumer-oriented edition that does not support joining a domain or using Group Policy. Only Windows Professional, Education, and Enterprise editions can join a domain

NEW QUESTION 44
Which of the following would MOST likely be deployed to enhance physical security for a building? (Select TWO).

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

Answer: BE

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

NEW QUESTION 49
A salesperson's computer is unable to print any orders on a local printer that is connected to the computer Which of the following tools should the salesperson use to restart the print spooler?

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

Answer: D

Explanation:

The correct answer is D. Services. The print spooler is a service that manages the print queue and sends print jobs to the printer. To restart the print spooler, the salesperson can use the Services app, which allows them to stop and start the service. Alternatively, they can also use the Task Manager or the Command Prompt to restart the print spooler.
References and Explanation
? The Services app is a tool that displays all the services that are running on the
computer. It can be accessed by typing services.msc in the Run window or by searching for Services in the Start menu. The Services app allows users to start, stop, restart, or configure any service, including the print spooler123.
? The Task Manager is a tool that shows information about the processes,
applications, and services that are running on the computer. It can be accessed by pressing Ctrl + Shift + Esc or by right-clicking on the taskbar and selecting Task Manager. The Task Manager allows users to start, stop, or restart any service by going to the Services tab and right-clicking on the service name12.
? The Command Prompt is a tool that allows users to execute commands and
perform tasks using text input. It can be accessed by typing cmd in the Run window or by searching for Command Prompt in the Start menu. The Command Prompt allows users to start, stop, or restart any service by using the net command with the service name. For example, to restart the print spooler, users can type net stop spooler and then net start spooler1.
? The Control Panel is a tool that provides access to various settings and options for
the computer. It can be accessed by typing control panel in the Run window or by searching for Control Panel in the Start menu. The Control Panel does not allow users to restart the print spooler directly, but it can be used to access other tools such as Devices and Printers, Troubleshooting, or Administrative Tools2.
? The Processes tab is a part of the Task Manager that shows information about the
processes that are running on the computer. It can be accessed by opening the Task Manager and selecting the Processes tab. The Processes tab does not allow users to restart the print spooler directly, but it can be used to end any process that is related to printing or causing problems with the print spooler2.
? The Startup tab is a part of the Task Manager that shows information about the
programs that run automatically when the computer starts. It can be accessed by opening the Task Manager and selecting the Startup tab. The Startup tab does not allow users to restart the print spooler directly, but it can be used to disable or enable any program that affects printing or interferes with the print spooler2.

NEW QUESTION 52
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 53
A technician has verified a computer is infected with malware. The technician isolates the system and updates the anti-malware software. Which of the following should the technician do next?

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 54
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 56
A desktop technician has received reports that a user's PC is slow to load programs and saved files. The technician investigates and discovers an older HDD with adequate free space. Which of the following should the technician use to alleviate the issue first?

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

Answer: B

Explanation:
Disk Defragment is a tool that can be used to improve the performance of a hard disk drive (HDD). HDDs store data in sectors and clusters on spinning platters. Over time, as data is written, deleted, and moved, the data may become fragmented, meaning that it is spread across different locations on the disk. This causes the HDD to take longer to access and load data, resulting in slower performance. Disk Defragment consolidates the fragmented data and rearranges it in a contiguous manner, which reduces the seek time and increases the speed of the HDD. Disk Management, Disk Cleanup, and Device Manager are not tools that can alleviate the issue of slow HDD performance.

NEW QUESTION 58
A technician is troubleshooting application crashes on a Windows workstation. Each time the workstation user tries to open a website in a browser, the following message is displayed:
crypt32.d11 is missing not found
Which of the following should the technician attempt FIRST?

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

Answer: D

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

NEW QUESTION 61
A technician downloads a validated security tool and notes the vendor hash of a58e87a2. When the download is complete, the technician again validates the hash, but the value returns as 2a876a7d3. Which of the following is the MOST likely cause of the issue?

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

Answer: C

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

NEW QUESTION 63
A remote user is experiencing issues with Outlook settings and asks a technician to review the settings. Which of the following can the technician use to access the user's computer remotely?

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

Answer: B

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

NEW QUESTION 64
A user calls the help desk to report that none of the files on a PC will open. The user also indicates a program on the desktop is requesting payment in exchange for file access A technician verifies the user's PC is infected with ransorrrware. Which of the following should the technician do FIRST?

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

Answer: C

Explanation:
The technician should quarantine the system first1 Reference:
CompTIA A+ Certification Exam: Core 2 Objectives Version 4.0. Retrieved from https://partners.comptia.org/docs/default-source/resources/comptia-a-220-1102-exam- objectives-(3-0)

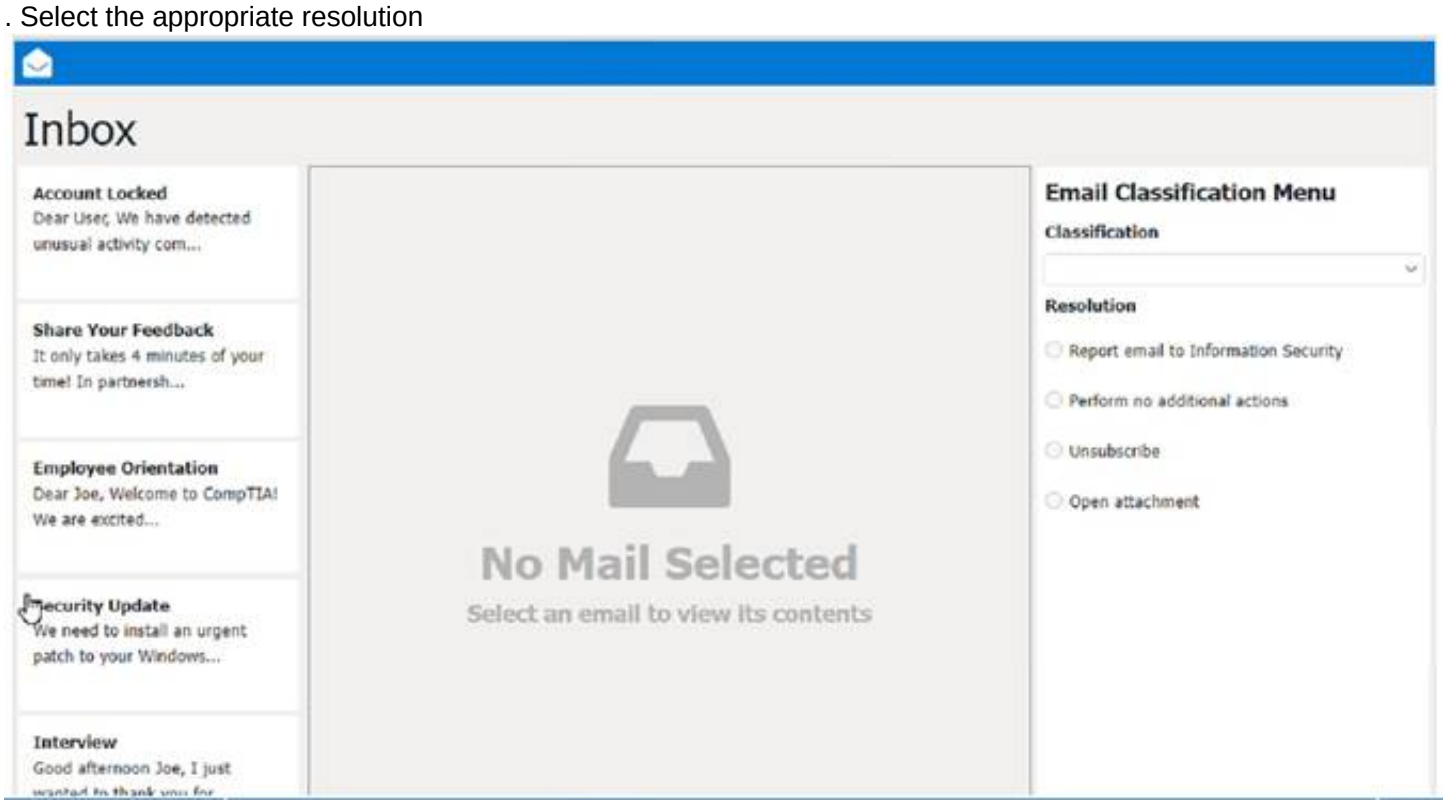
NEW QUESTION 68
A company is deploying mobile phones on a one-to-one basis, but the IT manager is concerned that users will root/jailbreak their phones. Which of the following technologies can be implemented to prevent this issue?

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 69
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

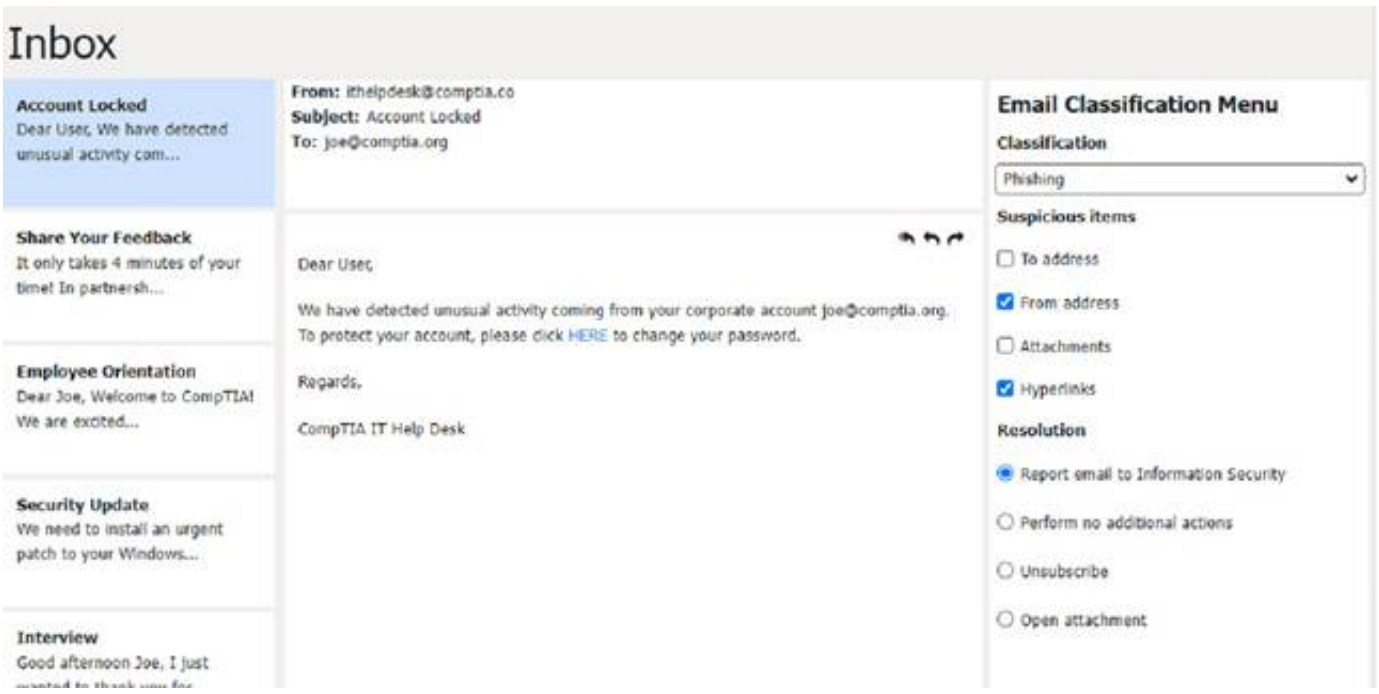


Answer:
See the Full solution in Explanation below.

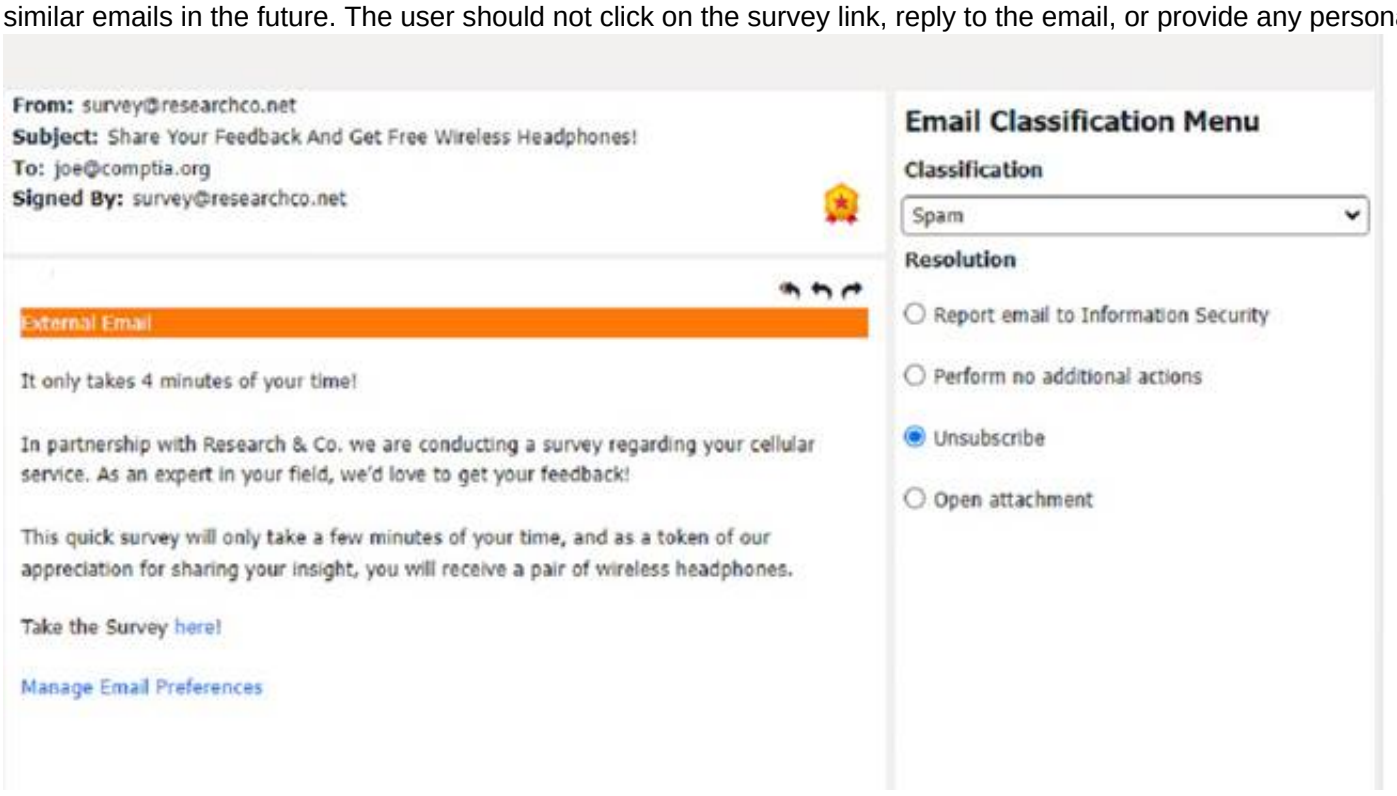
A. Mastered
B. Not Mastered

Answer: A

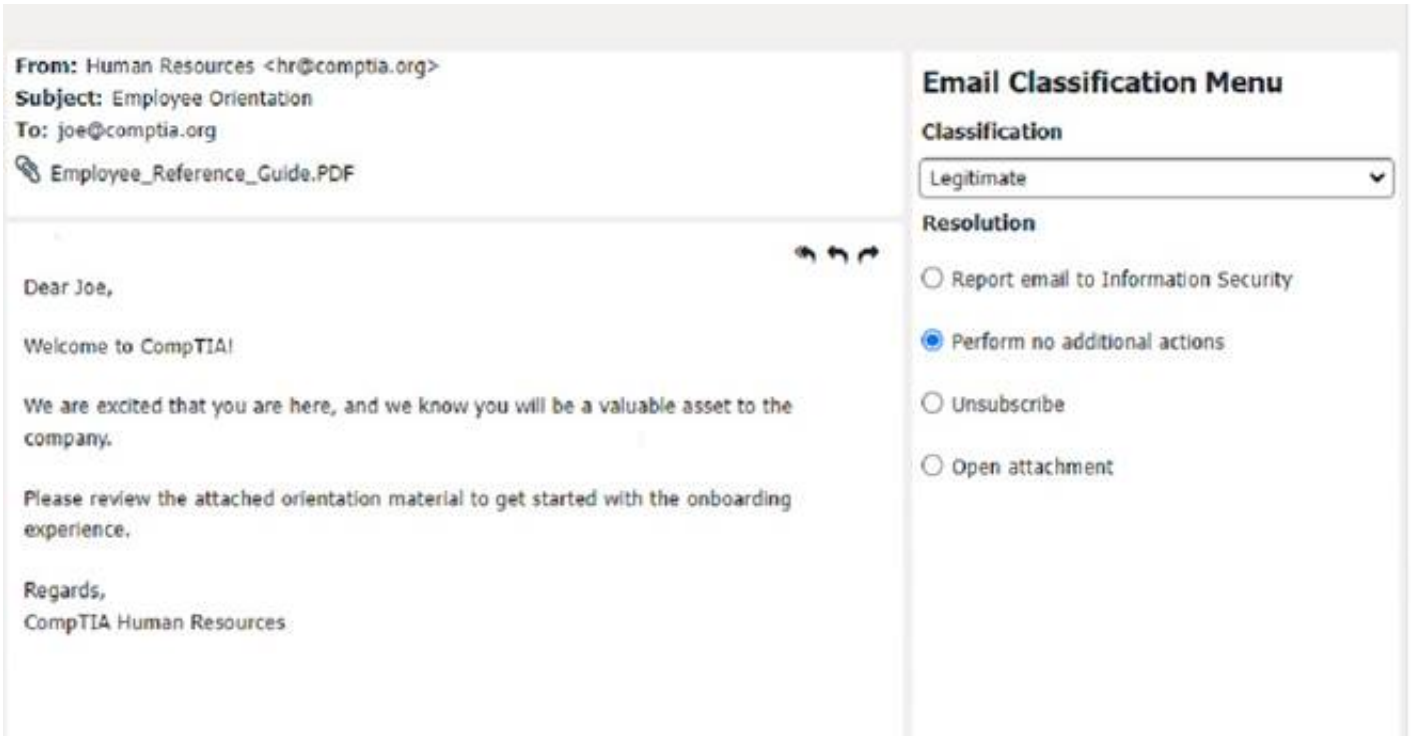
Explanation:
Classification: a) Phishing
This email is a phishing attempt, as it tries to trick the user into clicking on a malicious link that could compromise their account or personal information. Some suspicious items in this email are:
? The email has a generic greeting and does not address the 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.



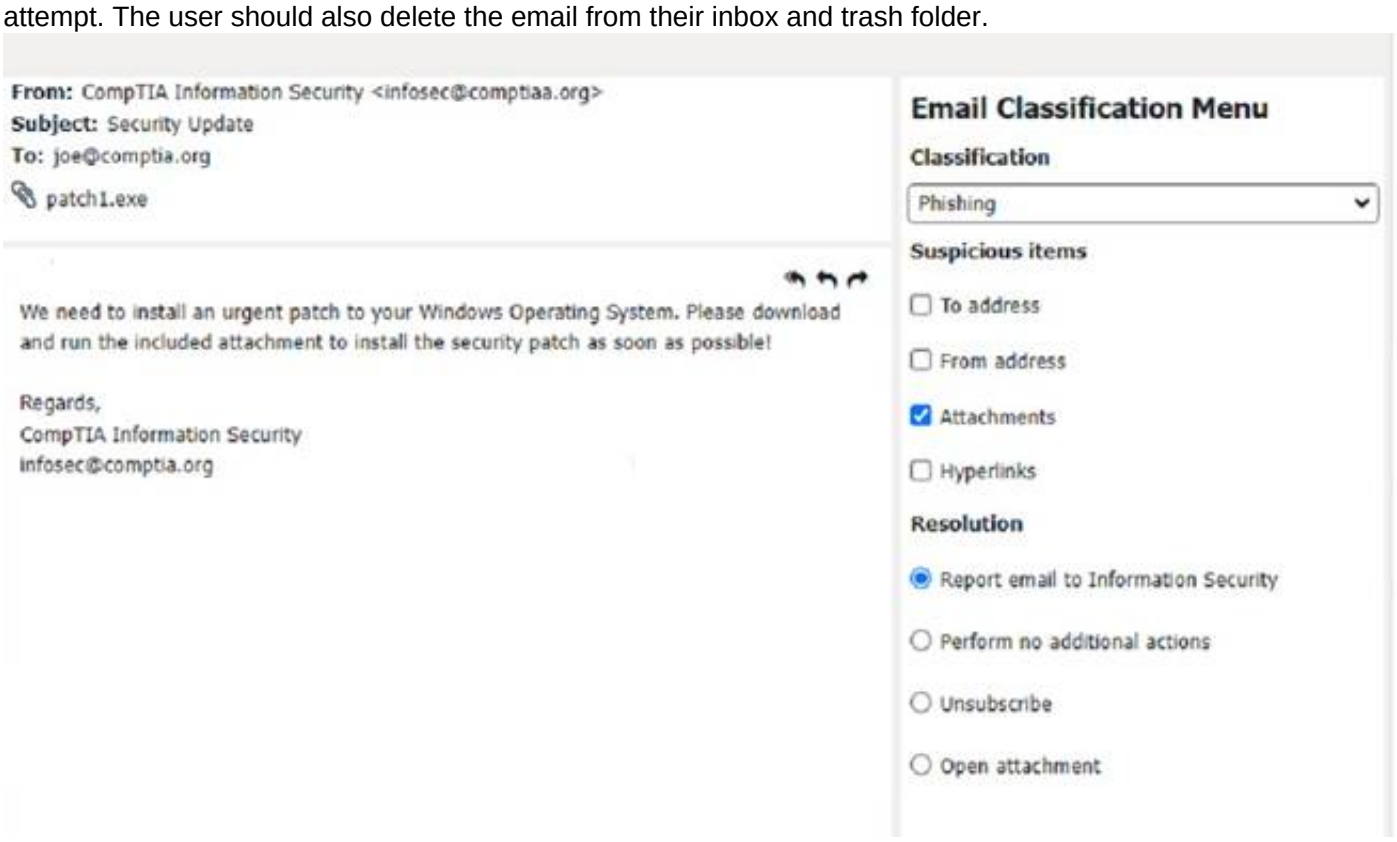
Classification: b) Spam
This email is a spam email, as it is an unsolicited and unwanted message that tries to persuade the user to participate in a survey and claim a reward. Some suspicious items in this email are:
? The email offers a free wireless headphone as an incentive, which is too good to
be 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.



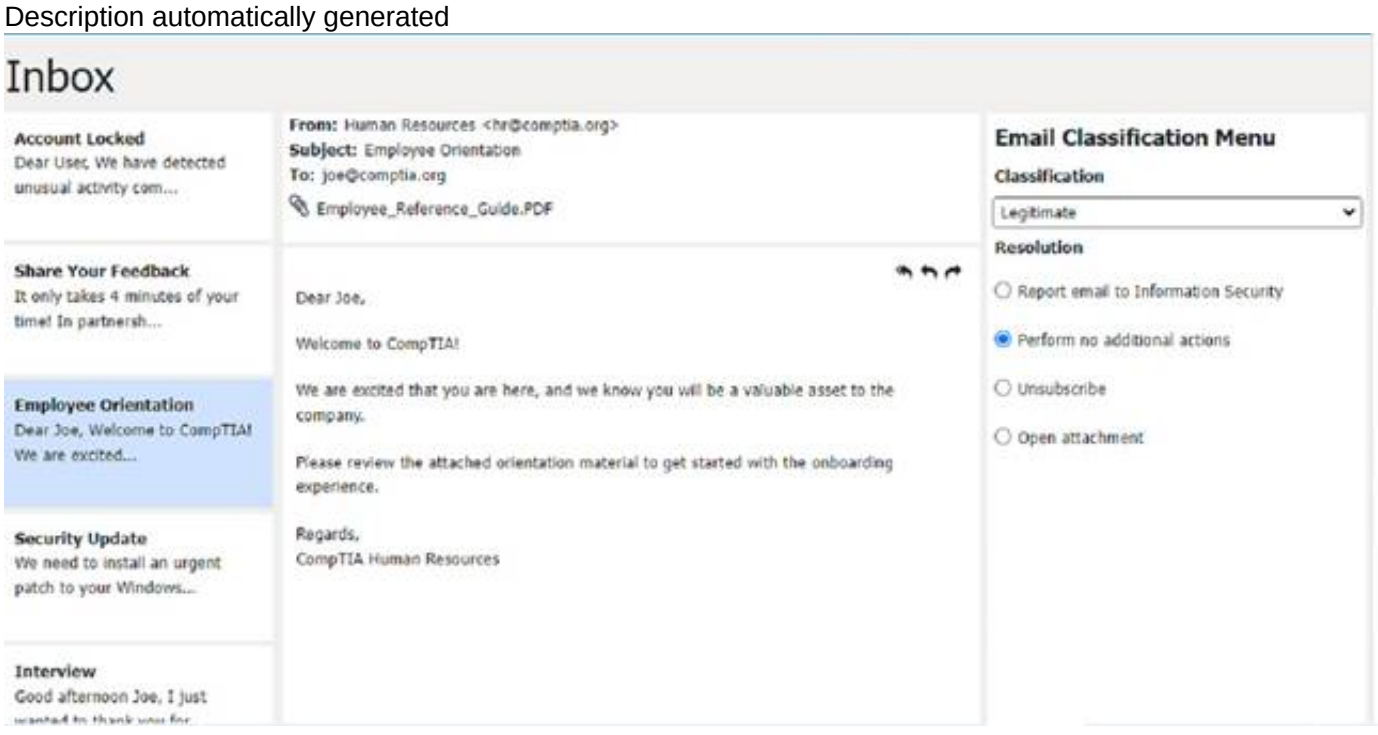
Classification: c) Legitimate
This email is a legitimate email, as it is from a trusted source and has a valid purpose. There are no suspicious items in this email, as the from address, the to address, the attachment, and the email body are all consistent and relevant. The appropriate resolution for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

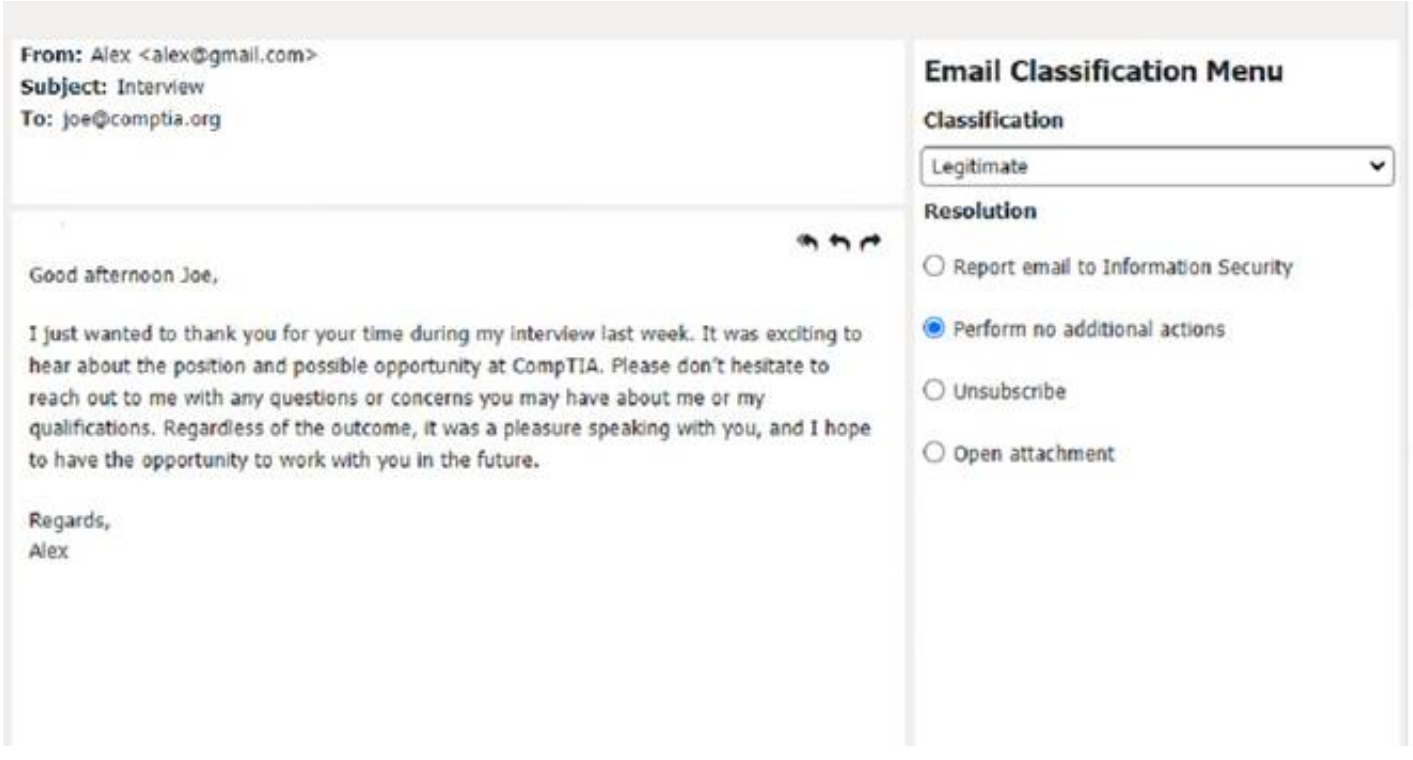


A screenshot of a computer
Description automatically generated



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 74
An IT security team is implementing a new Group Policy that will return a computer to the login after three minutes. Which of the following BEST describes the change in policy?

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

Answer: B

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

NEW QUESTION 78
Which of the following is MOST likely used to run .vbs files on Windows devices?

A. winmgmt.exe
B. powershell.exe
C. cscript.exe
D. explorer.exe

Answer: C

Explanation:
A .vbs file is a Virtual Basic script written in the VBScript scripting language. It contains code that can be executed within Windows via the Windows-based script host (Wscript.exe), to perform certain admin and processing functions1. Cscript.exe is a command-line version of the Windows Script Host that provides command-line options for setting script properties. Therefore, cscript.exe is most likely used to run .vbs files on Windows devices. References: 1: https://fileinfo.com/extension/vbs : https://docs.microsoft.com/en-us/windows-server/administration/windows- commands/cscript

NEW QUESTION 79
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 84
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 86
A help desk technician determines a motherboard has failed. Which of the following is the most logical next step in the remediation process?

A. Escalating the issue to Tier 2
B. Verifying warranty status with the vendor
C. Replacing the motherboard
D. Purchasing another PC

Answer: B

Explanation:
Verifying warranty status with the vendor is the most logical next step in the remediation process after determining that a motherboard has failed. A warranty is a guarantee from the vendor that covers the repair or replacement of defective or faulty products within a specified period of time. Verifying warranty status with the vendor can help the technician determine if the motherboard is eligible for warranty service and what steps to take to obtain it. Escalating the issue to Tier 2, replacing the motherboard, and purchasing another PC are not the most logical next steps in the remediation process.

NEW QUESTION 90
Which of the following options should MOST likely be considered when preserving data from a hard drive for forensic analysis? (Select TWO).

A. Licensing agreements
B. Chain of custody
C. Incident management documentation
D. Data integrity
E. Material safety data sheet
F. Retention requirements

Answer: B

Explanation:
Chain of custody and data integrity are two options that should most likely be considered when preserving data from a hard drive for forensic analysis. Chain of custody refers to the documentation and tracking of who has access to the data and how it is handled, stored, and transferred. Data integrity refers to the assurance that the data has not been altered, corrupted, or tampered with during the preservation process

NEW QUESTION 93
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 98
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 100
A user's computer unexpectedly shut down immediately after the user plugged in a USB headset. Once the user turned the computer back on, everything was functioning properly, including the headset. Which of the following Microsoft tools would most likely be used to determine the root cause?

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

Answer: A

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

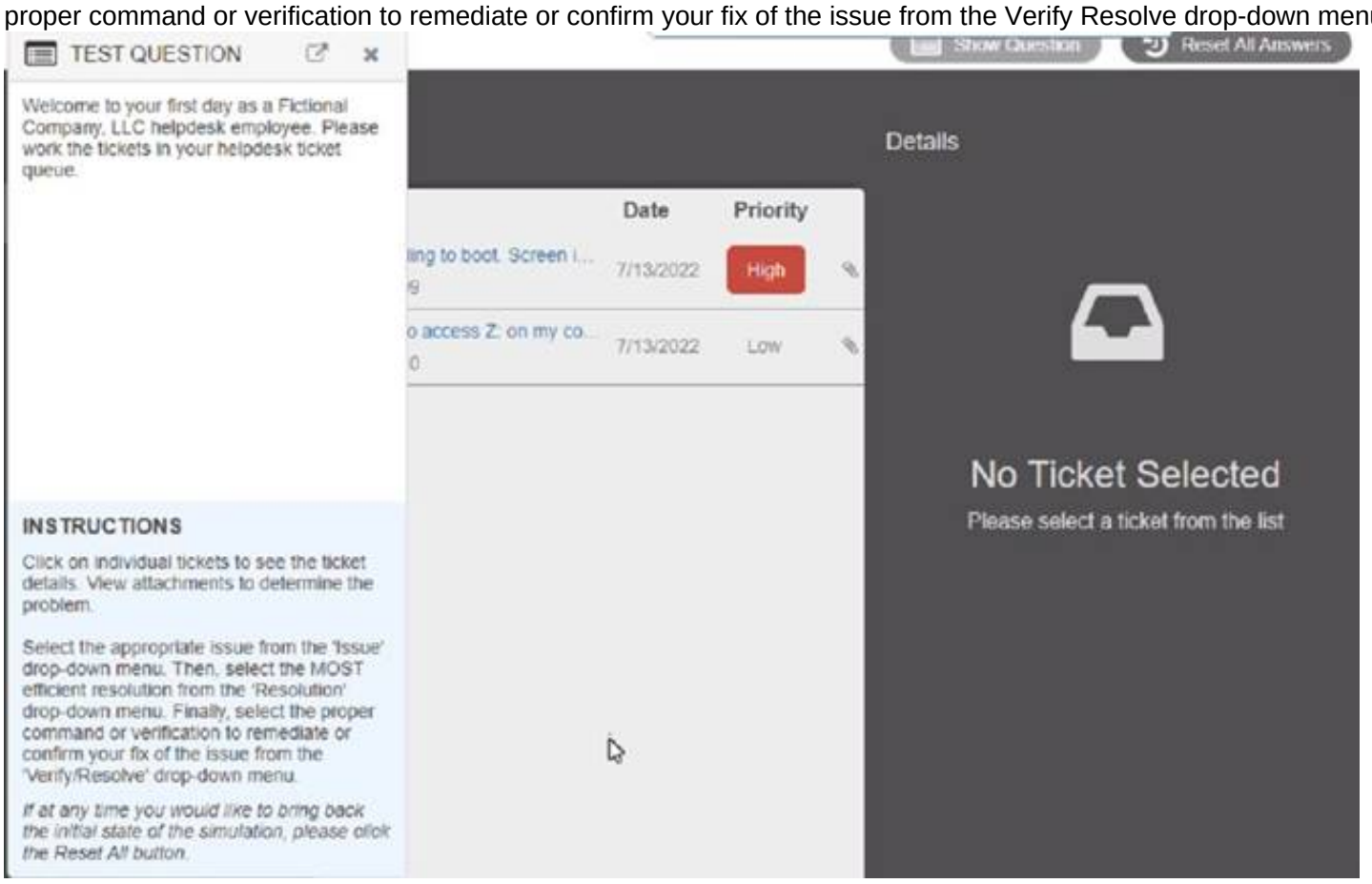
NEW QUESTION 101
A technician downloaded software from the Internet that required the technician to scroll through a text box and at the end of the text box, click a button labeled Accept Which of the following agreements IS MOST likely in use?

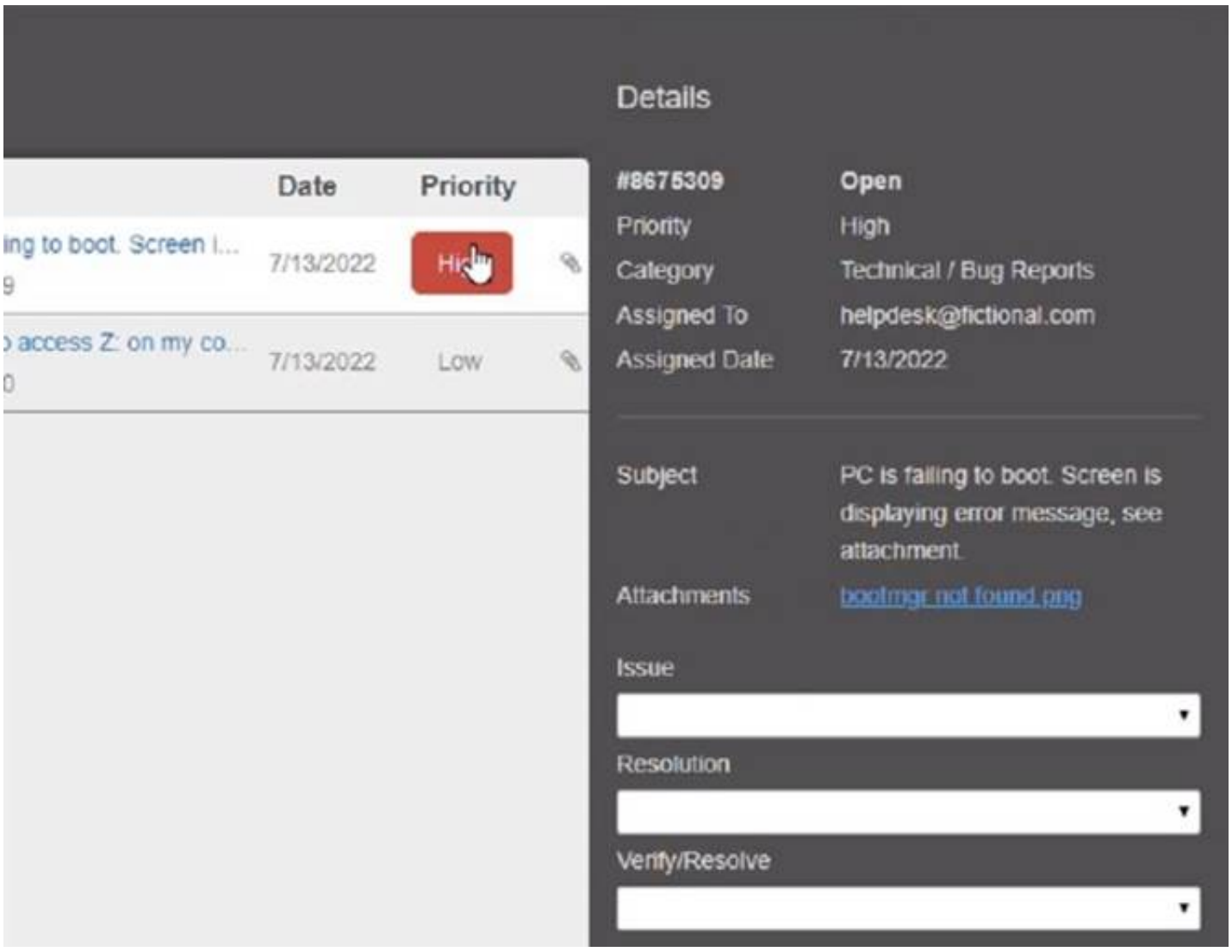
A. Mastered
B. Not Mastered

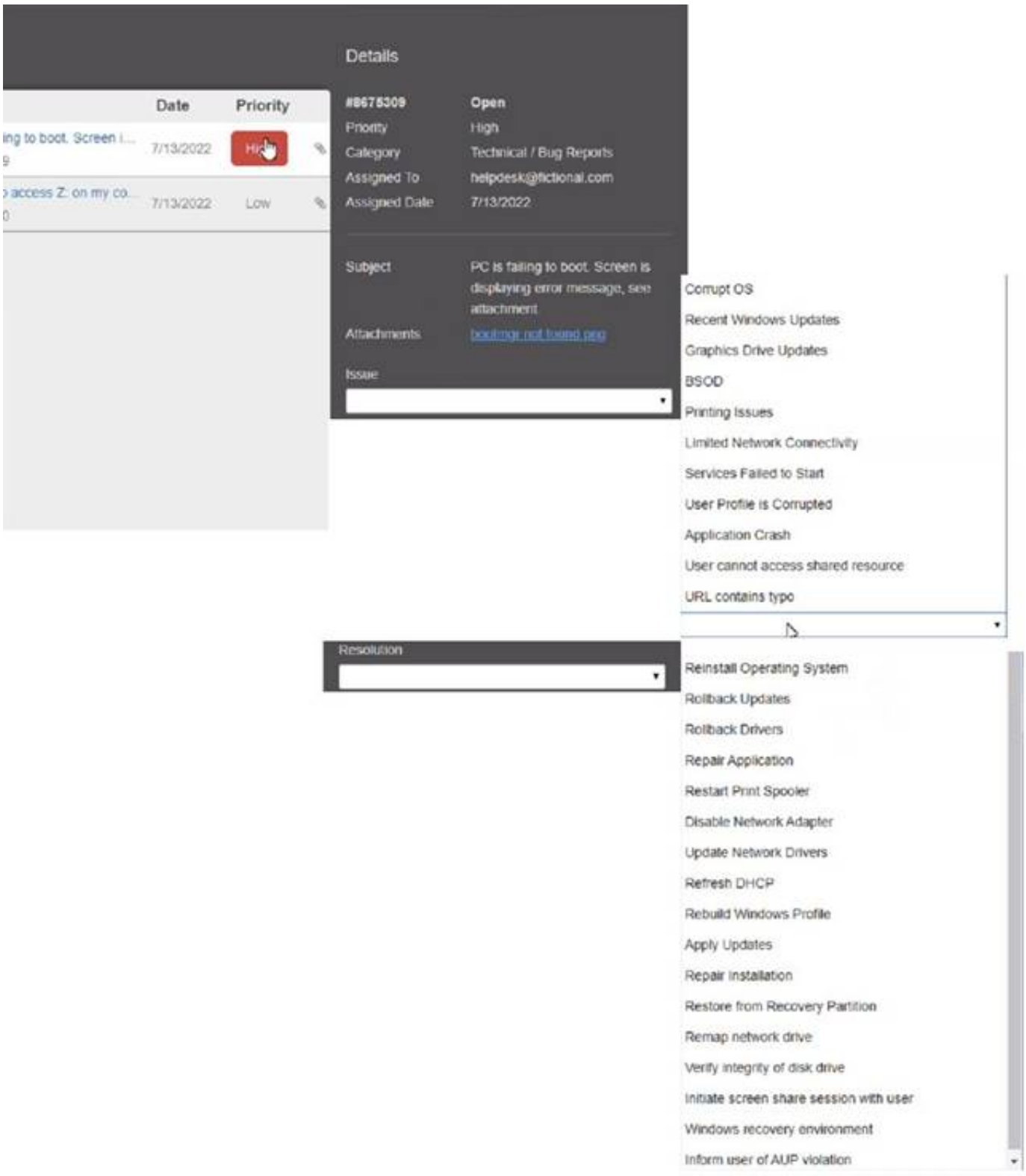
Answer: A

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

NEW QUESTION 106
HOTSPOT
Welcome to your first day as a Fictional Company. LLC helpdesk employee. Please work the tickets in your helpdesk ticket queue.
Click on individual tickers to see the ticket details. View attachments to determine the problem.
Select the appropriate issue from the 'issue' drop-down menu. Then, select the MOST efficient resolution from the 'Resolution' drop-down menu. Finally, select the proper command or verification to remediate or confirm your fix of the issue from the Verify Resolve drop-down menu.



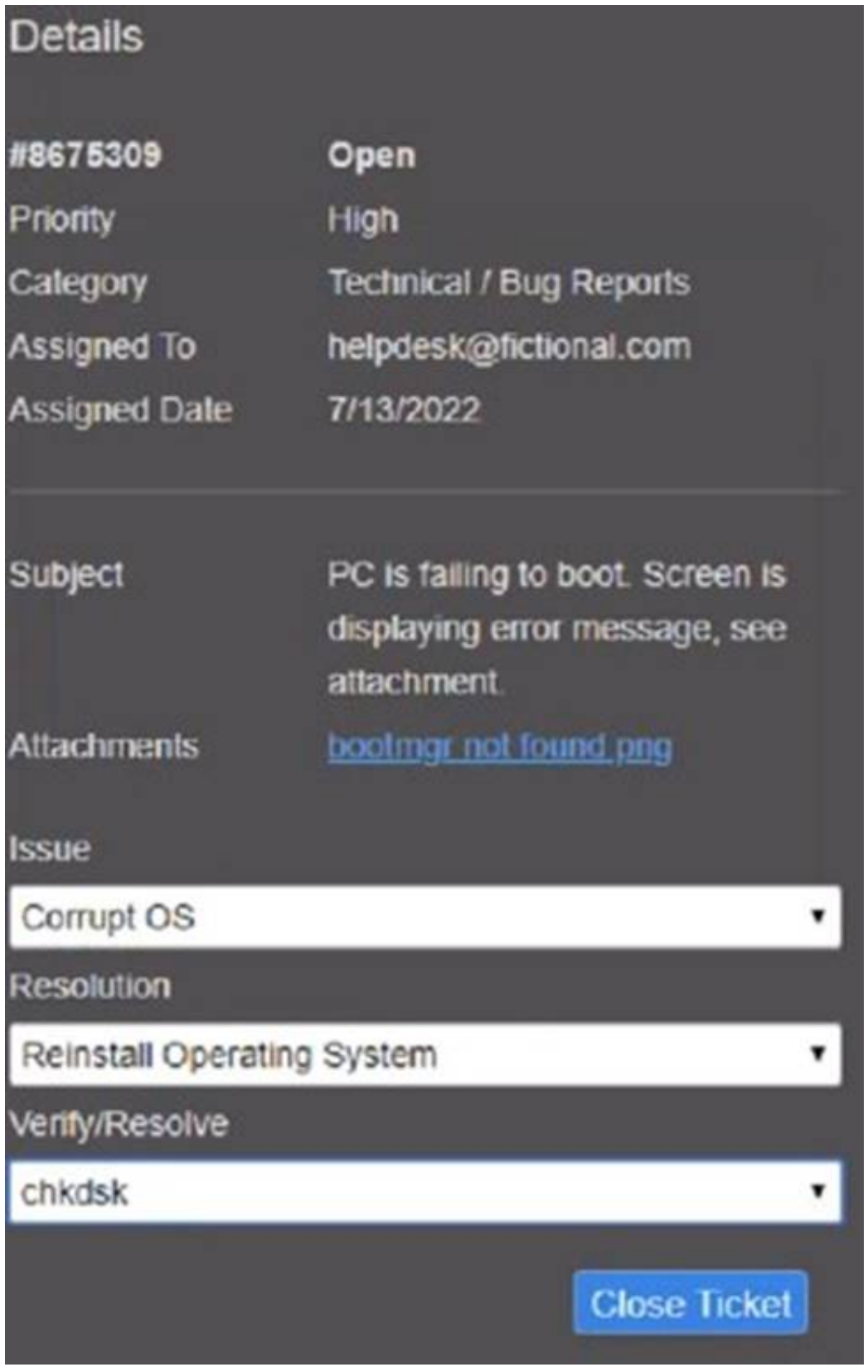

Details
Date
Priority
ing to boot. Screen i...
9
7/13/2022
Hi
access Z: on my co...
0
7/13/2022
Low
#8675309
Open
Priority
High
Category
Technical / Bug Reports
Assigned To
helpdesk@fictional.com
Assigned Date
7/13/2022
Subject
PC is failing to boot. Screen is displaying error message, see attachment
Attachments
bootmgr not found.png
Issue
Resolution
Verify/Resolve



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 108
Which of the following default system tools can be used in macOS to allow the technician to view the screen simultaneously with the user?

A. Remote Assistance
B. Remote Desktop Protocol
C. Screen Sharing
D. Virtual Network Computing

Answer: C

Explanation:
Screen Sharing is the default system tool that can be used in macOS to allow the technician to view the screen simultaneously with the user. Screen Sharing is a built-in app that lets users share their Mac screen with another Mac on the network. The user can enable screen sharing in the System Preferences > Sharing pane, and then allow other users to request or enter a password to access their screen1. The technician can launch the Screen Sharing app from the Spotlight search or the Finder sidebar, and then enter the user's name, address, or Apple ID to connect to their screen2. Remote Assistance is a Windows feature that allows users to invite someone to help them with a problem on their PC3. Remote Desktop Protocol (RDP) is a protocol that allows users to connect to a remote computer over a network4. Virtual Network Computing (VNC) is a technology that allows users to share their screen with other devices using a VNC viewer app1. These are not default system tools in macOS, although they can be used with third-party software or settings.
References: 1: https://support.apple.com/guide/mac-help/share-the-screen-of-another-mac-mh14066/mac 2: https://www.howtogeek.com/449239/how-to-share-your-macs-screen-with-another-mac/ 3: https://support.microsoft.com/en-us/windows/solve-pc-problems-over-a-remote-connection-b077e31a-16f4-2529-1a47-21f6a9040bf3 4: https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/clients/remote-desktop-protocol

NEW QUESTION 109
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.

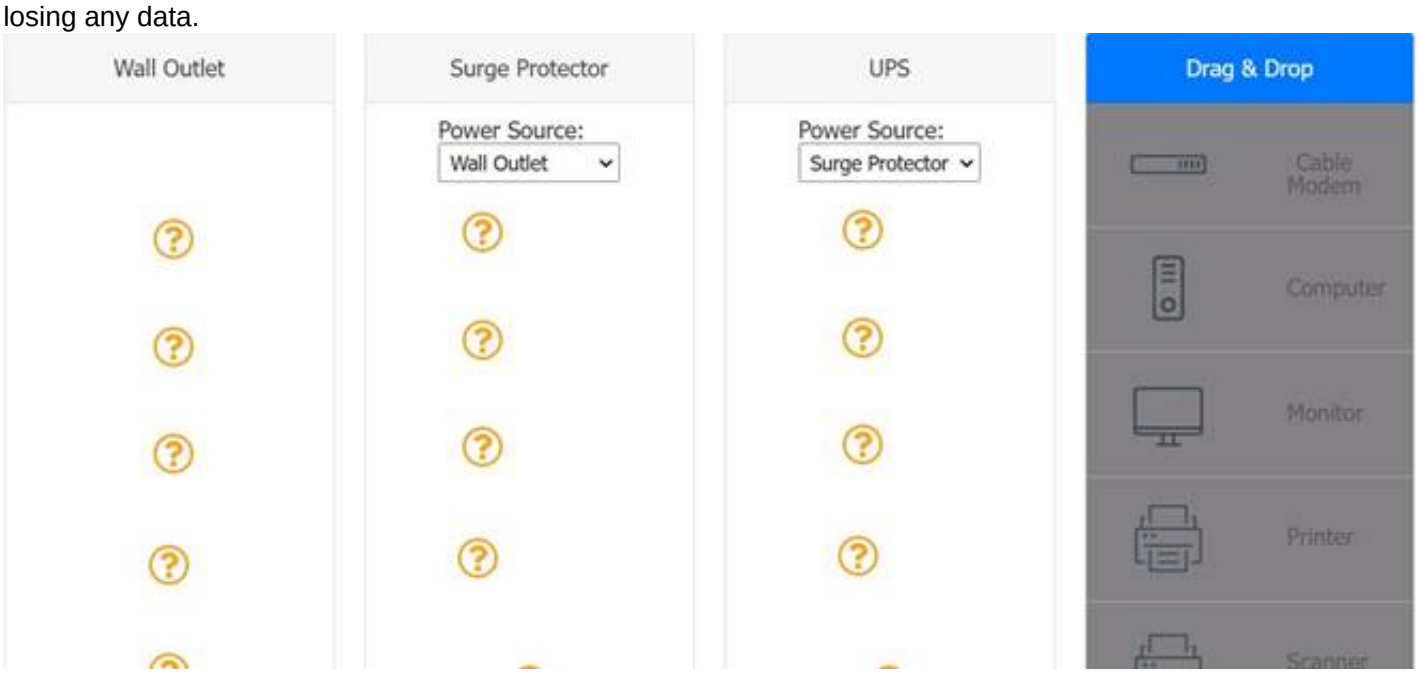
NEW QUESTION 113
A technician is unable to completely start up a system. The OS freezes when the desktop background appears, and the issue persists when the system is restarted. Which of the following should the technician do next to troubleshoot the issue?

A. Disable applicable BIOS options.
B. Load the system in safe mode.
C. Start up using a flash drive OS and run System Repair.
D. Enable Secure Boot and reinstall the system.

Answer: B

Explanation:
Loading the system in safe mode is a common troubleshooting step that allows the technician to isolate the problem by disabling unnecessary drivers and services. This can help determine if the issue is caused by a faulty device, a corrupted system file, or a malware infection.

NEW QUESTION 115
DRAG DROP
A customer recently experienced a power outage at a SOHO. The customer does not think the components are connected properly. A print job continued running for several minutes after the power failed, but the customer was not able to interact with the computer. Once the UPS stopped beeping, all functioning devices also turned off. In case of a future power failure, the customer wants to have the most time available to save cloud documents and shut down the computer without losing any data.



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 120
A technician is unable to access the internet or named network resources. The technician receives a valid IP address from the DHCP server and can ping the default gateway. Which of the following should the technician check next to resolve the issue?

A. Verify the DNS server settings.
B. Turn off the Windows firewall.
C. Confirm the subnet mask is correct.
D. Configure a static IP address.

Answer: A

Explanation:
The correct answer is A. Verify the DNS server settings. This is because the DNS server is responsible for resolving domain names to IP addresses, which is necessary for accessing the internet or named network resources. If the DNS server settings are incorrect or the DNS server is down, the technician will not be able to access these resources even if they have a valid IP address and can ping the default gateway1.
1: CompTIA A+ Certification Exam: Core 2 Objectives, page 16, section 1.10.

NEW QUESTION 121
A technician is creating a location on a Windows workstation for a customer to store meeting minutes. Which of the following commands should the technician use?

A. c: \minutes
B. dir

rmdir

C. md

Answer: D

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

NEW QUESTION 123
Which of the following filesystem types does macOS use?

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

Answer: D

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

NEW QUESTION 128
An organization is updating the monitors on kiosk machines. While performing the upgrade, the organization would like to remove physical input devices. Which of the following utilities in the Control Panel can be used to turn on the on-screen keyboard to replace the physical input devices?

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

Answer: B

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

NEW QUESTION 132
A user's smartphone data usage is well above average. The user suspects an installed application is transmitting data in the background. The user would like to be alerted when an application attempts to communicate with the internet. Which of the following BEST addresses the user's concern?

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

Answer: D

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

NEW QUESTION 133
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 136
A systems administrator needs to reset a users password because the user forgot it. The systems administrator creates the new password and wants to further protect the user's account Which of the following should the systems administrator do?

A. Require the user to change the password at the next log-in.
B. Disallow tie user from changing the password.
C. Disable the account
D. Choose a password that never expires.

Answer: A

Explanation:
This will ensure that the user is the only one who knows their password, and that the new password is secure.
The CompTIA A+ Core 2 220-1002 exam covers this topic in the domain 1.4 Given a scenario, use appropriate data destruction and disposal methods.

NEW QUESTION 139
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 141
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 145
An Android user reports that when attempting to open the company's proprietary mobile application it immediately doses. The user states that the issue persists, even after rebooting the phone. The application contains critical information that cannot be lost. Which of the following steps should a systems administrator attempt FIRST?

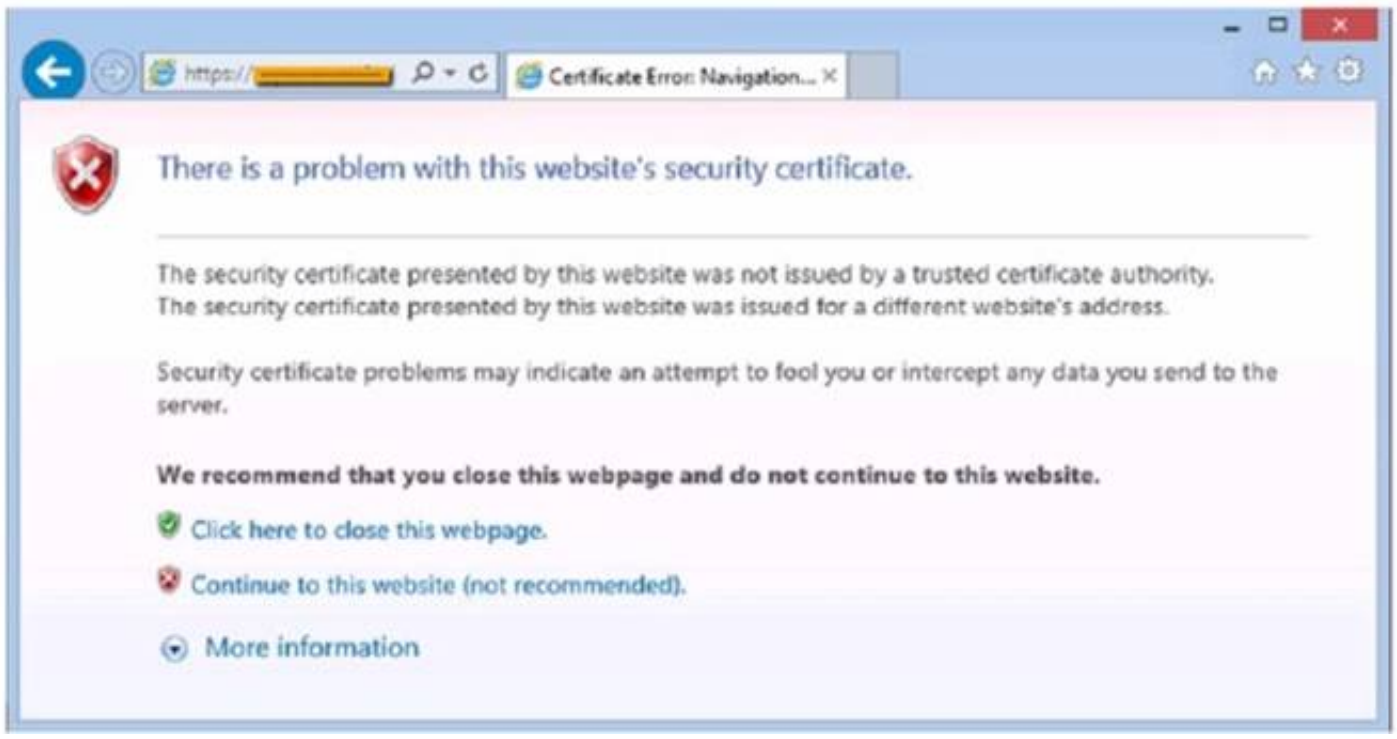
A. Mastered
B. Not Mastered

Answer: A

Explanation:
The systems administrator should clear the application cach1e2

If clearing the application cache does not work, the systems administrator should uninstall and reinstall the application12
Resetting the phone to factory settings is not necessary at this point12
Installing an alternative application with similar functionality is not necessary at this point12

NEW QUESTION 146
After clicking on a link in an email a Chief Financial Officer (CFO) received the following error:



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

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

Answer: A

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

NEW QUESTION 151
Which of the following protocols supports fast roaming between networks?

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

Answer: B

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

NEW QUESTION 152
Which of the following protects a mobile device against unwanted access when it is left unattended?

A. PIN code
B. OS updates
C. Antivirus software
D. BYOD policy

Answer: A

Explanation:
A PIN code is a numeric password that protects a mobile device against unwanted access when it is left unattended. It requires the user to enter the correct code before unlocking the device. OS updates, antivirus software and BYOD policy are other security measures for mobile devices, but they do not prevent unauthorized access when the device is left unattended. Verified References: https://www.comptia.org/blog/mobile- device-security https://www.comptia.org/certifications/a

NEW QUESTION 154

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

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

Answer: D

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

NEW QUESTION 157
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 158
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 160
A user contacted the help desk to report pop-ups on a company workstation indicating the computer has been infected with 137 viruses and payment is needed to remove them. The user thought the company-provided antivirus software would prevent this issue. The help desk ticket states that the user only receives these messages when first opening the web browser. Which of the following steps would MOST likely resolve the issue? (Select TWO)

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 162
An administrator is designing and implementing a server backup system that minimizes the capacity of storage used. Which of the following is the BEST backup approach to use in conjunction with synthetic full backups?

A. Differential
B. Open file
C. Archive
D. Incremental

Answer: D

Explanation:
Incremental backups are backups that only include the changes made since the last backup, whether it was a full or an incremental backup. Incremental backups minimize the capacity of storage used and are often used in conjunction with synthetic full backups, which are backups that combine a full backup and subsequent incremental backups into a single backup set.
Reference: CompTIA A+ Core 2 Exam Objectives, Section 3.3

NEW QUESTION 166
A user receives a notification indicating the data plan on the user's corporate phone has reached its limit. The user has also noted the performance of the phone is abnormally slow. A technician discovers a third-party GPS application was installed on the phone. Which of the following is the MOST likely cause?

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

Answer: B

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

NEW QUESTION 170
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 173
Maintaining the chain of custody is an important part of the incident response process. Which of the following reasons explains why this is important?

A. To maintain an information security policy
B. To properly identify the issue
C. To control evidence and maintain integrity
D. To gather as much information as possible

Answer: C

Explanation:
Maintaining the chain of custody is important to control evidence and maintain integrity. The chain of custody is a process that documents who handled, accessed, or modified a piece of evidence, when, where, how, and why. The chain of custody ensures that the evidence is preserved, protected, and authenticated throughout the incident response process. Maintaining the chain of custody can help prevent tampering, alteration, or loss of evidence, as well as establish its reliability and validity in legal proceedings. Maintaining an information security policy, properly identifying the issue, and gathering as much information as possible are not reasons why maintaining the chain of custody is important. Maintaining an information security policy is a general practice that defines the rules and guidelines for securing an organization's information assets and resources. Properly identifying the issue is a step in the incident response process that involves analyzing and classifying the incident based on its severity, impact, and scope. Gathering as much information as possible is a step in the incident response process that involves collecting and documenting relevant data and evidence from various sources, such as logs, alerts, or witnesses. References:
? Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 26

NEW QUESTION 175
Which of the following best describes when to use the YUM command in Linux?

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

Answer: A

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

NEW QUESTION 176
Which of the following would MOST likely be used to change the security settings on a user's device in a domain environment?

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

Answer: C

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

NEW QUESTION 178
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 182
A user's corporate laptop with proprietary work Information was stolen from a coffee shop. The user togged in to the laptop with a simple password. and no other security mechanisms were in place. Which of the following would MOST likely prevent the stored data from being recovered?

A. Biometrics
B. Full disk encryption
C. Enforced strong system password
D. Two-factor authentication

Answer: B

Explanation:
Full disk encryption is a security mechanism that encrypts the entire data on a hard drive, making it unreadable without the correct decryption key or password. It can prevent the stored data from being recovered by unauthorized persons who steal or access the laptop. Biometrics, enforced strong system password and two-factor authentication are other security mechanisms, but they only protect the login access to the laptop, not the data on the hard drive. Verified References: https://www.comptia.org/blog/what-is-full-disk- encryption https://www.comptia.org/certifications/a

NEW QUESTION 183
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 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 187
A technician has identified malicious traffic originating from a user's computer. Which of the following is the best way to identify the source of the attack?

A. Investigate the firewall logs.
B. Isolate the machine from the network.
C. Inspect the Windows Event Viewer.

D. Take a physical inventory of the device.

Answer: B

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

NEW QUESTION 191
Which of the following operating systems is considered closed source?

A. Ubuntu
B. Android
C. CentOS
D. OSX

Answer: D

Explanation:
OSX (now macOS) is an operating system that is considered closed source, meaning that its source code is not publicly available or modifiable by anyone except its

developers. It is owned and maintained by Apple Inc. Ubuntu, Android and CentOS are operating systems that are considered open source, meaning that their source code is publicly available and modifiable by anyone who wants to contribute or customize them. Verified References: https://www.comptia.org/blog/open-source-vs-closed-source-software https://www.comptia.org/certifications/a

NEW QUESTION 193

Which of the following should be used to control security settings on an Android phone in a domain environment?

A. MDM
B. MFA
C. ACL

D. SMS

Answer: A

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

NEW QUESTION 195

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

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

Answer: C

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

NEW QUESTION 199
A PC is taking a long time to boot. Which of the following operations would be best to do to resolve the issue at a minimal expense? (Select two).

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

Answer: BD

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

NEW QUESTION 200
Which of the following file extensions should a technician use for a PowerShell script?

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

Answer: A

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

NEW QUESTION 204
A user is setting up a computer for the first time and would like to create a secondary login with permissions that are different than the primary login. The secondary login will need to be protected from certain content such as games and websites. Which of the following Windows settings should the user utilize to create the secondary login?

A. Privacy
B. Accounts
C. Personalization
D. Shared resources

Answer: B

Explanation:
To create a secondary login with different permissions in Windows 10, the user should utilize the Accounts setting. Here are the steps to create a new user account with different permissions:
? Right-click the Windows Start menu button.
? Select Control Panel.
? Select User Accounts.
? Select Manage another account.
? Select Add a new user in PC settings.
? Use the Accounts dialog box to configure a new account.1

NEW QUESTION 208
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:
An unattended installation is a method of installing Windows 10 that does not require any user input or interaction during the installation process. An unattended installation can be performed by using an answer file, which is a file that contains all the configuration settings and preferences for the installation, such as the product key, the language, the partition size, and the user accounts. An unattended installation can be the fastest way to install Windows 10, as it automates and streamlines the installation process. Factory reset, System Restore, and in-place upgrade are not methods of installing Windows 10.

NEW QUESTION 211
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 216
Which of the following would cause a corporate-owned iOS device to have an Activation Lock issue?

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

Answer: B

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

NEW QUESTION 218
During a recent flight an executive unexpectedly received several dog and cat pictures while trying to watch a movie via in-flight Wi-Fi on an iPhone. The executive has no records of any contacts sending pictures like these and has not seen these pictures before. To BEST resolve this issue, the executive should:

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

Answer: A

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

NEW QUESTION 222
A department manager submits a help desk ticket to request the migration of a printer's port utilization from USB to Ethernet so multiple users can access the printer. This will be a new network printer, thus a new IP address allocation is required. Which of the following should happen immediately before network use is authorized?

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

Answer: B

Explanation:

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

NEW QUESTION 226
A technician needs to ensure that USB devices are not suspended by the operating system Which of the following Control Panel utilities should the technician use to configure the setting?

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

Answer: B

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

NEW QUESTION 229
A change advisory board authorized a setting change so a technician is permitted to Implement the change. The technician successfully implemented the change. Which of the following should be done next?

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

Answer: A

Explanation:
The correct answer is A. Document the date and time of change. After implementing a change, the technician should document the date and time of change in the change log or record. This helps to track the change history, monitor the change performance, and identify any issues or incidents related to the change. Documenting the date and time of change is also a good practice for auditing and compliance purposes. Documenting the purpose of the change (B) and the risk level © are steps that should be done before implementing the change, not after. These are important information that help to justify, prioritize, and plan the change. The purpose of the change should explain why the change is needed and what benefits it will bring to the organization. The risk level should assess the potential impact and probability of the change causing any problems or disruptions to the business.
Documenting the findings of the sandbox test (D) is also a step that should be done before implementing the change, not after. A sandbox test is a way of testing the change in an isolated environment that mimics the production environment. This helps to verify that the change works as expected and does not cause any errors or conflicts with other systems or processes. The findings of the sandbox test should be documented and reviewed by the change advisory board (CAB) before approving the change for implementation. References:
? What is a Change Advisory Board? (Overview, Roles, and Responsibilities)
? Best Practices in Change Management
? 10 Top change management best practices

NEW QUESTION 234
A technician is investigating an employee's smartphone that has the following symptoms
• The device is hot even when it is not in use.
•Applications crash, especially when others are launched.
• Certain applications, such as GPS, are in portrait mode when they should be in landscape mode.
Which of the following can the technician do to MOST likely resolve these issues with minimal impact? (Select TWO).

A. Mastered
B. Not Mastered

Answer: A

Explanation:
The technician can close unnecessary applications and turn on autorotation to resolve these issues with minimal impact. Autorotation can help the device to switch between portrait and landscape modes automatically. Closing unnecessary applications can help to free up the device's memory and reduce the device's temperature1
Reference:
CompTIA A+ Certification Exam: Core 2 (220-1102) Exam Objectives Version 4.0. Retrieved from https://partners.comptia.org/docs/default-source/resources/comptia-a-220- 1102-exam-objectives-(3-0)

NEW QUESTION 236
A technician sees a file that is requesting payment to a cryptocurrency address. Which of the following should the technician do first?

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

Answer: A

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

NEW QUESTION 239
A technician has been tasked with troubleshooting audiovisual issues in a conference room. The meeting presenters are unable to play a video with sound. The following error is received:

The Audio Driver is not running.

Which of the following will MOST likely resolve the issue?

A. compmgmt.msc
B. regedit.exe
C. explorer.exe
D. taskmgt.exe
E. gpmc.msc
F. services.msc

Answer: F

Explanation:
services.msc is a tool that can be used to resolve the issue of “The Audio Driver is not running” on a Windows machine. It allows a technician to view, start, stop and configure the services that run on the system, such as the Windows Audio service. compmgmt.msc, regedit.exe, explorer.exe, taskmgt.exe and gpmc.msc are other tools that can be used for different purposes on a Windows machine, but they are not related to audio drivers or services. Verified References: https://www.comptia.org/blog/what-is- services-msc https://www.comptia.org/certifications/a

NEW QUESTION 244

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

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

Answer: C

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

NEW QUESTION 245
Which of the following is the most likely to use NTFS as the native filesystem?

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

Answer: C

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

NEW QUESTION 250
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 254
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 258
A user enabled a mobile device's screen lock function with pattern unlock. The user is concerned someone could access the mobile device by repeatedly attempting random patterns to unlock the device. Which of the following features BEST addresses the user's concern?

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

Answer: A

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

NEW QUESTION 259
An implementation specialist is replacing a legacy system at a vendor site that has only one wireless network available. When the specialist connects to Wi-Fi. the specialist realizes the insecure network has open authentication. The technician needs to secure the vendor's sensitive data. Which of the following should the specialist do FIRST to protect the company's data?

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

Answer: B

Explanation:
The first thing that the specialist should do to protect the company’s data on an insecure network with open authentication is to connect to the vendor’s network using a VPN. A VPN stands for Virtual Private Network and is a technology that creates a secure and encrypted connection over a public or untrusted network. A VPN can protect the company’s data by preventing eavesdropping, interception or modification of the network traffic by unauthorized parties. A VPN can also provide access to the company’s internal network and resources remotely. Manually configuring an IP address, a subnet mask and a default gateway may not be necessary or possible if the vendor’s network uses DHCP to assign network configuration parameters automatically. Manually configuring an IP address, a subnet

mask and a default gateway does not protect the company's data from network attacks or threats. Changing the network location to private may not be advisable or effective if the vendor's network is a public or untrusted network. Changing the network location to private does not protect the company's data from network attacks or threats. Configuring MFA on the network may not be feasible or sufficient if the vendor's network has open authentication and does not support or require MFA. Configuring MFA on the network does not protect the company's data from network attacks or threats. References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 3.3

NEW QUESTION 263
When a user calls in to report an issue, a technician submits a ticket on the user's behalf. Which of the following practices should the technician use to make sure the ticket is associated with the correct user?

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

Answer: D

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

NEW QUESTION 267
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 269
Once weekly a user needs Linux to run a specific open-source application that is not available for the currently installed Windows platform. The user has limited bandwidth throughout the day. Which of the following solutions would be the MOST efficient, allowing for parallel execution of the Linux application and Windows applications?

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

Answer: B

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

NEW QUESTION 273
.....

Relate Links

100% Pass Your 220-1102 Exam with Exambible Prep Materials

https://www.exambible.com/220-1102-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/