

CompTIA

Exam Questions 220-1102

CompTIA A+ Certification Exam: Core 2



NEW QUESTION 1

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

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

Answer: D

Explanation:

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

NEW QUESTION 2

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

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

Answer: C

Explanation:

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

NEW QUESTION 3

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

TEST QUESTION

[Show Question](#)
[Reset All Answers](#)

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

Assist the executive to help resolve the issue.

INSTRUCTIONS

Select the MOST appropriate statement for each response.

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

Telecom.

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

the latest update, here is a screenshot

IMAP >
SSL >
10.0.200.1 >
100 >

Protocol	IMAP >
Security	SSL >
Server Address	10.0.200.1 >
Port	100 >

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

Thanks for helping.

Which of the following should be done NEXT?

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

Answer: A

NEW QUESTION 4

When trying to access a secure internal network, the user receives an error messaging stating, "There is a problem with this website's security certificate." The user reboots the desktop and tries to access the website again, but the issue persists. Which of the following should the user do to prevent this error from reoccurring?

- A. Reimage the system and install SSL.
- B. Install Trusted Root Certificate.
- C. Select View Certificates and then Install Certificate.
- D. Continue to access the website.

Answer: C

Explanation:

The error message indicates that the website's security certificate is not trusted by the user's device, which may prevent the user from accessing the secure internal network. To resolve this issue, the user can view the certificate details and install it on the device, which will add it to the trusted root certificate store. Reimaging the system and installing SSL, installing Trusted Root Certificate, or continuing to access the website are not recommended solutions, as they may compromise the security of the device or the network.

NEW QUESTION 5

A systems administrator is monitoring an unusual amount of network traffic from a kiosk machine and needs to Investigate to determine the source of the traffic. Which of the following tools can the administrator use to view which processes on the kiosk machine are connecting to the internet?

- A. Resource Monitor
- B. Performance Monitor
- C. Command Prompt
- D. System Information

Answer: A

Explanation:

Resource Monitor is a tool that shows the network activity of each process on a Windows machine, including the TCP connections and the sent and received bytes. Performance Monitor is a tool that shows the performance metrics of the system, such as CPU, memory, disk and network usage. Command Prompt is a tool that allows running commands and scripts on a Windows machine. System Information is a tool that shows the hardware and software configuration of a Windows machine. Verified References:

<https://www.comptia.org/blog/how-to-use-resource-monitor> <https://www.comptia.org/certifications/a>

NEW QUESTION 6

A technician needs to provide recommendations about how to upgrade backup solutions for a site in an area that has frequent hurricanes and an unstable power grid. Which of the following should the technician recommend implementing?

- A. High availability
- B. Regionally diverse backups
- C. On-site backups
- D. Incremental backups

Answer: B

Explanation:

Regionally diverse backups are backups that are stored in different geographic locations, preferably far away from the primary site¹. This way, if a disaster such as a hurricane or a power outage affects one location, the backups in another location will still be available and accessible². Regionally diverse backups can help ensure business continuity and data recovery in case of a disaster³. The other options are not the best backup solutions for a site in an area that has frequent hurricanes and an unstable power grid. High availability is a feature that allows a system to remain operational and accessible even if one or more components fail, but it does not protect against data loss or corruption⁴. On-site backups are backups that are stored in the same location as the primary site, which means they are vulnerable to the same disasters that can affect the primary site. Incremental backups are backups that only store the changes made since the last backup, which means they require less storage space and bandwidth, but they also depend on previous backups to restore data and may not be sufficient for disaster recovery.

NEW QUESTION 7

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 8

A hotel's Wi-Fi was used to steal information on a corporate laptop. A technician notes the following security log:

SRC: 192.168.1.1/secrets.zip Protocol SMB >> DST: 192.168.1.50/capture

The technician analyses the following Windows firewall information:

Port	Status	Direction
1	Open	In/Out
445	Open	In/Out
25	Open	Out
110	Open	In/Out
53	Open	In/Out

Which of the following protocols most likely allowed the data theft to occur?

- A. 1
- B. 53
- C. 110
- D. 445

Answer: D

Explanation:

The protocol that most likely allowed the data theft to occur is SMB over TCP port 445. SMB is a network file sharing protocol that enables access to files, printers, and other resources on a network. Port 445 is used by SMB to communicate directly over TCP without the need for NetBIOS, which is an older and less secure protocol. The security log shows that the source IP address 192.168.1.1 sent a file named secrets.zip using SMB protocol to the destination IP address 192.168.1.50, which captured the file. The Windows firewall information shows that port 445 is enabled for inbound and outbound traffic, which means that it is not blocked by the firewall. Therefore, port 445 is the most likely port that was exploited by the attacker to steal the data from the corporate laptop.

References:

? SMB port number: Ports 445, 139, 138, and 137 explained¹

? What is an SMB Port + Ports 445 and 139 Explained²

? CompTIA A+ Certification Exam Core 2 Objectives³

NEW QUESTION 9

A BSOD appears on a user's workstation monitor. The user immediately presses the power button to shut down the PC, hoping to repair the issue. The user then restarts the PC, and the BSOD reappears, so the user contacts the help desk. Which of the following should the technician use to determine the cause?

- A. Stop code
- B. Event Mewer
- C. Services
- D. System Configuration

Answer: A

Explanation:

When a Blue Screen of Death (BSOD) appears on a Windows workstation, it indicates that there is a serious problem with the operating system. The stop code displayed on the BSOD can provide valuable information to help determine the cause of the issue. The stop code is a specific error code that is associated with the BSOD, and it can help identify the root cause of the problem.

In this scenario, the user has encountered a BSOD and has restarted the PC, only to see the BSOD reappear. This suggests that the problem is persistent and requires further investigation. By analyzing the stop code displayed on the BSOD, a technician can begin to identify the underlying issue and take appropriate actions to resolve it.

NEW QUESTION 10

A user notices a small USB drive is attached to the user's computer after a new vendor visited the office. The technician notices two files named grabber.exe and output.txt. Which of the following attacks is MOST likely occurring?

- A. Trojan
- B. Rootkit
- C. Cryptominer
- D. Keylogger

Answer: D

Explanation:

A keylogger is a type of malware that records the keystrokes of a user and sends them to a remote attacker. A keylogger can be used to steal passwords, credit card numbers, personal information, and other sensitive data. A keylogger can be delivered through a USB drive that contains a malicious executable file, such as grabber.exe, and an output file that stores the captured keystrokes, such as output.txt. The other options are not likely to use this method of attack. References: : <https://www.comptia.org/training/resources/exam-objectives/comptia-a-core-2-exam-objectives> : <https://www.kaspersky.com/resource-center/definitions/keylogger>

NEW QUESTION 10

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

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

Answer: A

Explanation:

Before removing a Trojan virus from a workstation, a technician should disable System Restore. System Restore is a feature that allows users to restore their system to a previous state in case of problems or errors. However, System Restore can also restore infected files or registry entries that were removed by antivirus software or manual actions. By disabling System Restore, a technician can ensure that the Trojan virus is completely removed and does not reappear after a system restore operation. Scheduling a malware scan may help detect and remove some malware but may not be effective against all types of Trojan viruses. Educating the end user may help prevent future infections but does not address the current issue of removing the Trojan virus. Running Windows Update may help

patch some security vulnerabilities but does not guarantee that the Trojan virus will be removed. References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.3

NEW QUESTION 15

A Linux technician needs a filesystem type that meets the following requirements:

- All changes are tracked.
- The possibility of file corruption is reduced.
- Data recovery is easy.

Which of the following filesystem types best meets these requirements?

- ☒ A. FAT32
- ☐ B. ext3
- ☐ C. exFAT
- ☐ D. NTFS

Answer: A

Explanation:

The ext3 file system is a Linux native file system that meets the requirements of the question. It has the following features:

? All changes are tracked. The ext3 file system uses a journaling mechanism that records all changes to the file system metadata in a special log called the journal before applying them to the actual file system. This ensures that the file system can be restored to a consistent state in case of a power failure or system crash¹².

? The possibility of file corruption is reduced. The journaling feature of ext3 also reduces the possibility of file corruption, as it avoids the need for a full file system check after an unclean shutdown. The file system can be quickly replayed from the journal and any inconsistencies can be fixed¹².

? Data recovery is easy. The ext3 file system supports undeletion of files using tools such as ext3grep or extundelete, which can scan the file system for deleted inodes and attempt to recover the data blocks associated with them³⁴.

References:

1: Introduction to Linux File System [Structure and Types] - MiniTool1 2: 7 Ways to Determine the File System Type in Linux (Ext2, Ext3 or Ext4) - Tecmint3 3: How to Recover Deleted Files in Linux with ext3grep 4: How to Recover Deleted Files from ext3 Partitions

NEW QUESTION 19

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

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

Answer: B

Explanation:

The most likely reason that the system is not utilizing all the available RAM is that it is running a 32-bit OS. A 32-bit OS can only address up to 4GB of RAM, and some of that is reserved for hardware and system use¹. Therefore, even if the technician installed 8GB of RAM, the system can only use around 3.5GB of usable RAM. To use the full 8GB of RAM, the technician would need to install a 64-bit OS, which can address much more memory². The system missing updates, the system's memory failing, or the system requiring BIOS updates are not likely to cause this issue.

References: 2: <https://support.microsoft.com/en-us/windows/windows-10-system-requirements-6d4e9a79-66bf-7950-467c-795cf0386715> 1: <https://www.makeuseof.com/tag/unlock-64gb-ram-32-bit-windows-pae-patch/>

NEW QUESTION 20

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

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

Answer: B

Explanation:

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

malware attacks

NEW QUESTION 21

Which of the following filesystem formats would be the BEST choice to ensure read and write compatibility of USB flash drives across several generations of Microsoft operating systems?

- ☐ A. ext4
- ☐ B. APFS
- ☐ C. CDFS
- ☐ D. FAT32

Answer: D

Explanation:

The best filesystem format to ensure read and write compatibility of USB flash drives across several generations of Microsoft operating systems is FAT32. FAT32 stands for File Allocation Table 32-bit and is a filesystem format that organizes and manages files and folders on storage devices using 32-bit clusters. FAT32 is compatible with most Microsoft operating systems since Windows 95 OSR2, as well as other operating systems such as Linux and Mac OS X. FAT32 can support storage devices up to 2TB in size and files up to 4GB in size. APFS stands for Apple File System and is a filesystem format that organizes and manages files and folders on storage devices using encryption, snapshots and cloning features. APFS is compatible with Mac OS X 10.13 High Sierra and later versions but not with Microsoft operating systems natively. Ext4 stands for Fourth Extended File System and is a filesystem format that organizes and manages files and folders on storage devices using journaling, extents and delayed allocation features. Ext4 is compatible with Linux operating systems but not with Microsoft operating systems natively.

NEW QUESTION 25

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 27

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 30

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

- ☐ A. Mastered
- ☐ B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 35

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 (220-1102) Certification Exam Objectives Version 4.0, Domain 1.7

NEW QUESTION 39

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

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

Answer: D

Explanation:

Open-ended questions are questions that require more than a yes or no answer and encourage the customer to provide more details and information. Using open-ended questions can help the support technician to understand the problem better, identify the root cause, and find a suitable solution. Some examples of open-ended questions are:

- ? What exactly is not working on your machine?
- ? When did you notice the problem?
- ? How often does the problem occur?
- ? What were you doing when the problem happened?
- ? What have you tried to fix the problem?

Offering to wipe and reset the device for the customer is not a good option, as it may result in data loss and inconvenience for the customer. It should be used as a last resort only if other troubleshooting steps fail. Advising that the help desk will investigate and follow up at a later date is not a good option, as it may leave the customer unsatisfied and frustrated. It should be used only if the problem requires further research or escalation and cannot be resolved on the first call. Putting the customer on hold and escalating the call to a manager is not a good option, as it may waste time and resources. It should be used only if the problem is beyond the support technician's scope or authority and requires managerial intervention.

NEW QUESTION 42

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 (220-1102) Certification Exam Objectives Version 4.0, Domain 1.5

NEW QUESTION 45

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 network. 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 49

A user attempts to open some files, but a message appears stating that the files are encrypted. The user was able to access these files before without receiving this message and no changes have been made within the company. Which of the following has infected the computer?

- A. Cryptominer
- B. Phishing
- C. Ransomware
- D. Keylogger

Answer: C

Explanation:

Ransomware is malicious software that encrypts files on a computer, making them inaccessible until a ransom is paid. In this case, the user was able to access the files before without issue, and no changes have been made within the company, so it is likely that the computer was infected with ransomware.

NEW QUESTION 51

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

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

Answer: C

Explanation:

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

NEW QUESTION 56

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

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

Answer: C

Explanation:

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

NEW QUESTION 60

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 cleanmgr 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 64

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 (220-1102) Certification Exam Objectives Version 4.0, Domain 3.3

NEW QUESTION 69

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

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

Answer: E

Explanation:

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

NEW QUESTION 71

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

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

Answer: C

Explanation:

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

NEW QUESTION 72

A systems administrator is experiencing Issues connecting from a laptop to the corporate network using PKI. Which to the following tools can the systems administrator use to help remediate the issue?

- A. certmgr.msc
- B. msconfig.exe
- C. lusrmgr.msc
- D. perfmon.msc

Answer: A

Explanation:

certmgr.msc is a tool that can be used to troubleshoot issues with PKI (public key infrastructure) on a Windows machine. It allows a system administrator to view, manage and import certificates, as well as check their validity, expiration and revocation status. msconfig.exe, lusrmgr.msc and perfmon.msc are other tools that can be used for different purposes on a Windows machine, but they are not related to PKI. Verified References: <https://www.comptia.org/blog/what-is-certmgr-msc> <https://www.comptia.org/certifications/a>

NEW QUESTION 77

Windows updates need to be performed on a department's servers. Which of the following methods should be used to connect to the server?

FIP

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

Answer: C

Explanation:

RDP (Remote Desktop Protocol) is a protocol that allows a user to connect to and control a remote computer over a network. RDP can be used to perform Windows updates on a department's servers without physically accessing them.

Reference: CompTIA A+ Core 2 Exam Objectives, Section 5.6

NEW QUESTION 82

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

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

Answer: B

Explanation:

Flashing the BIOS, reformatting the drive, and then reinstalling the OS is the best method

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

NEW QUESTION 85

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

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

Answer: B

Explanation:

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

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

NEW QUESTION 87

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

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

Answer: CE

Explanation:

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

NEW QUESTION 91

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 94

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

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

Answer: B

Explanation:

The best course of action for the technician is to restore the defaults and reimage the corporate OS on the device. This will remove the jailbreak and any unauthorized or malicious apps that may have been installed on the device, as well as restore the security features and policies that the company has set for its devices. This will also ensure that the device can receive the latest updates and patches from the manufacturer and the company, and prevent any data leakage or compromise from the device.

Jailbreaking is a process of bypassing the built-in security features of a device to install software other than what the manufacturer has made available for that device¹. Jailbreaking allows the device owner to gain full access to the root of the operating system and access all the features¹. However, jailbreaking also exposes the device to various risks, such as:

- ? The loss of warranty from the device manufacturers².
- ? Inability to update software until a jailbroken version becomes available².
- ? Increased security vulnerabilities^{3,2}.
- ? Decreased battery life².
- ? Increased volatility of the device².

Some of the signs of a jailbroken device are:

- ? A high number of ads, which may indicate the presence of adware or spyware on the device³.
- ? Receiving data-usage limit notifications, which may indicate the device is sending or receiving data in the background without the user's knowledge or consent³.
- ? Experiencing slow response, which may indicate the device is running unauthorized or malicious apps that consume resources or interfere with the normal functioning of the device³.
- ? Finding apps or icons that the user did not install or recognize, such as Cydia, which is a storefront for jailbroken iOS devices¹.

The other options are not sufficient or appropriate for dealing with a jailbroken device. Running an antivirus and enabling encryption may not detect or remove all the threats or vulnerabilities that the jailbreak has introduced, and may not restore the device to its original state or functionality. Backing up the files and doing a system restore may not erase the jailbreak or the unauthorized apps, and may also backup the infected or compromised files. Undoing the jailbreak and enabling an antivirus may not be possible or effective, as the jailbreak may prevent the device from updating or installing security software, and may also leave traces of the jailbreak or the unauthorized apps on the device.

References:

- ? CompTIA A+ Certification Exam Core 2 Objectives⁴
- ? CompTIA A+ Core 2 (220-1102) Certification Study Guide⁵
- ? What is Jailbreaking & Is it safe? - Kaspersky¹
- ? Is Jailbreaking Safe? The ethics, risks and rewards involved - Comparitech³
- ? Jailbreaking : Security risks and moving past them²

NEW QUESTION 97

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

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

Answer: A

Explanation:

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

NEW QUESTION 98

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 99

A technician is working with a company to determine the best way to transfer sensitive personal information between offices when conducting business. The company currently uses USB drives and is resistant to change. The company's compliance officer states that all media at rest must be encrypted. Which of the following would be the BEST way to secure the current workflow?

- A. Deploy a secondary hard drive with encryption on the appropriate workstation
- B. Configure a hardened SFTP portal for file transfers between file servers
- C. Require files to be individually password protected with unique passwords
- D. Enable BitLocker To Go with a password that meets corporate requirements

Answer: D

Explanation:

The BEST way to secure the current workflow of transferring sensitive personal information between offices when conducting business is to enable BitLocker To Go with a password that meets corporate requirements. This is because BitLocker To Go is a full-disk encryption feature that encrypts all data on a USB drive, which is what the company currently uses, and requires a password to access the data.

NEW QUESTION 101

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. RDP
- ☐ B. VPN
- ☐ 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 103

A homeowner recently moved and requires a new router for the new ISP to function correctly. The internet service has been installed and has been confirmed as functional. Which of the following is the FIRST step the homeowner should take after installation of all relevant cabling and hardware?

- A. Convert the PC from a DHCP assignment to a static IP address.
- B. Run a speed test to ensure the advertised speeds are met.
- C. Test all network sharing and printing functionality the customer uses.
- D. Change the default passwords on new network devices.

Answer: D

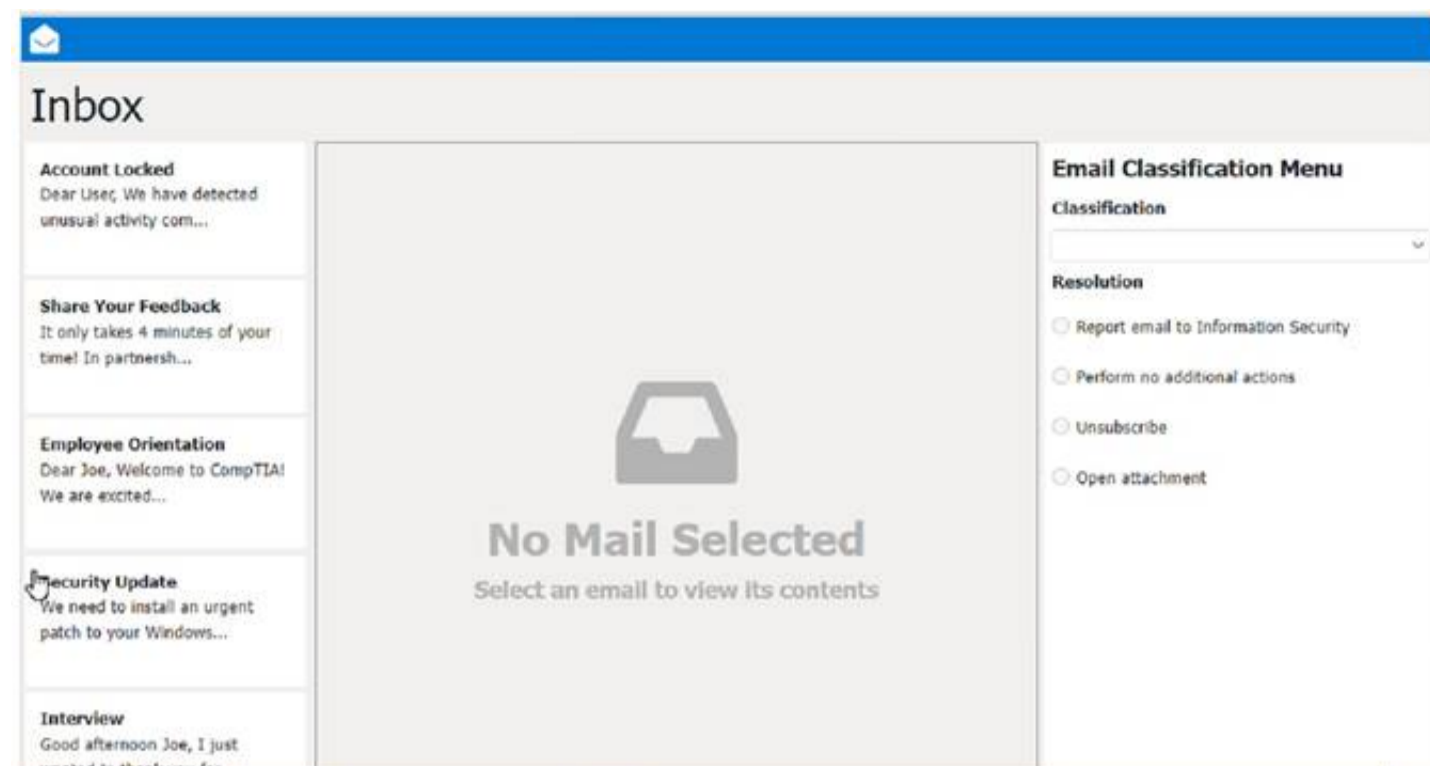
Explanation:

When a homeowner moves and sets up a new router for the new ISP it is important to take appropriate security measures to protect their network from potential security threats. The FIRST step that the homeowner should take after installation of all relevant cabling and hardware is to change the default passwords on new network devices. Most modern routers come with default usernames and passwords that are widely known to potential attackers. If these defaults are not changed, it could make it easier for external attackers to gain unauthorized access to the network. Changing the passwords on new network devices is a simple but effective way to improve the security posture of the network.

NEW QUESTION 108**SIMULATION**

As a corporate technician, you are asked to evaluate several suspect email messages on a client's computer. Corporate policy requires the 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:

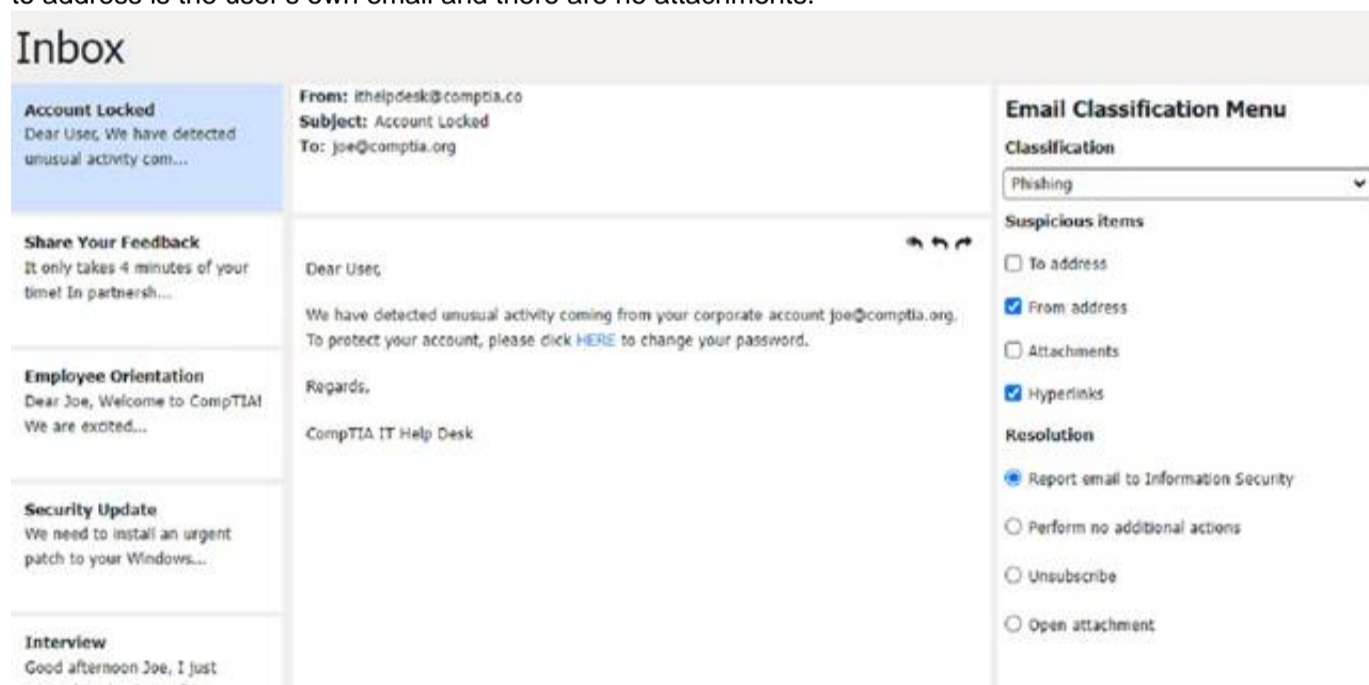
- ? The email has a generic greeting and does not address the user by name.
- ? The email has spelling errors, such as "unusal" and "Locaked".
- ? The email uses a sense of urgency and fear to pressure the user into clicking on the link.
- ? The email does not match the official format or domain of the 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 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.

From: survey@researchco.net
Subject: Share Your Feedback And Get Free Wireless Headphones!
To: joe@comptia.org
Signed By: survey@researchco.net

External Email

It only takes 4 minutes of your time!

In partnership with Research & Co. we are conducting a survey regarding your cellular service. As an expert in your field, we'd love to get your feedback!

This quick survey will only take a few minutes of your time, and as a token of our appreciation for sharing your insight, you will receive a pair of wireless headphones.

Take the Survey [here!](#)

[Manage Email Preferences](#)

Email Classification Menu

Classification

Spam

Resolution

☐ Report email to Information Security


☐ Perform no additional actions

☒ Unsubscribe

☐ Open attachment

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.

From: Human Resources <hr@comptia.org>
Subject: Employee Orientation
To: joe@comptia.org
 Employee_Reference_Guide.PDF

Dear Joe,

Welcome to CompTIA!

We are excited that you are here, and we know you will be a valuable asset to the company.

Please review the attached orientation material to get started with the onboarding experience.

Regards,
CompTIA Human Resources

Email Classification Menu

Classification

Legitimate

Resolution

☐ Report email to Information Security

☒ Perform no additional actions

☐ Unsubscribe

☐ Open attachment

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.

From: CompTIA Information Security <infosec@comptiaa.org>
Subject: Security Update
To: joe@comptia.org
 patch1.exe

We need to install an urgent patch to your Windows Operating System. Please download and run the included attachment to install the security patch as soon as possible!

Regards,
CompTIA Information Security
infosec@comptia.org

Email Classification Menu

Classification

Phishing

Suspicious items

☐ To address

☐ From address

☒ Attachments

☐ Hyperlinks

Resolution

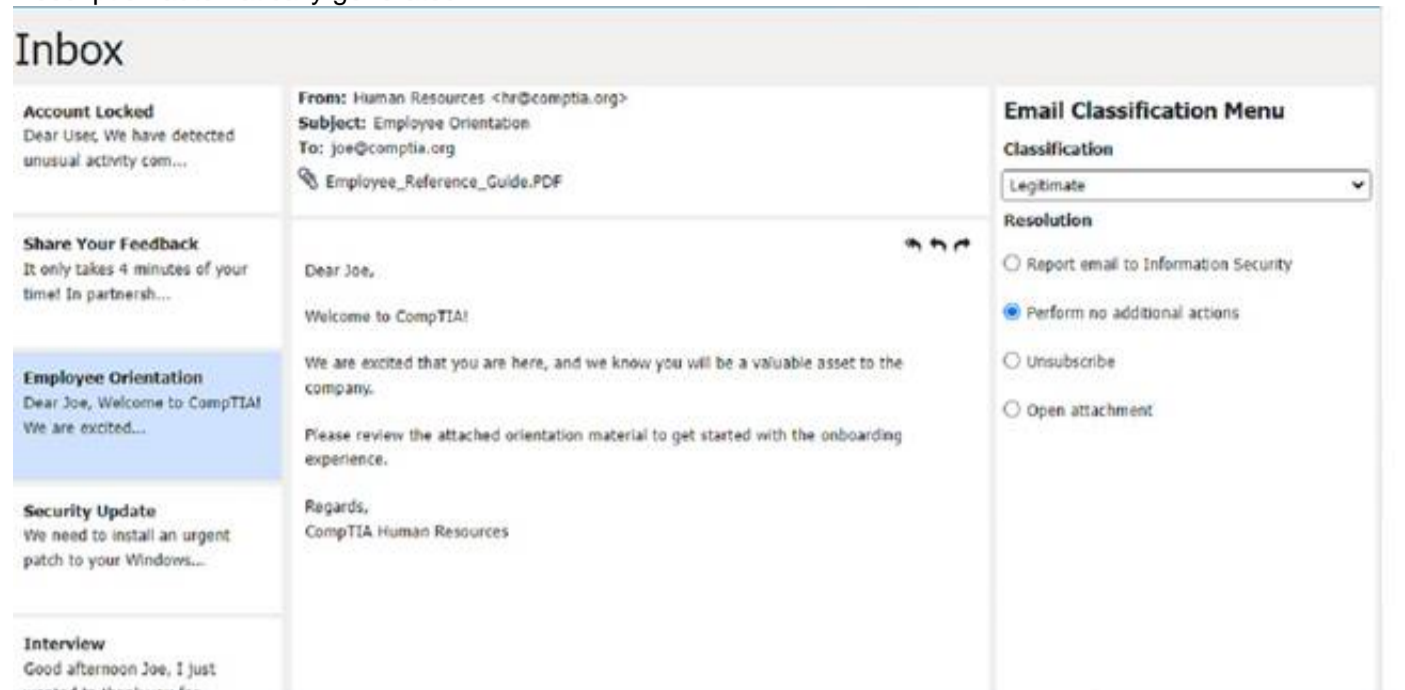
☒ Report email to Information Security

☐ Perform no additional actions

☐ Unsubscribe

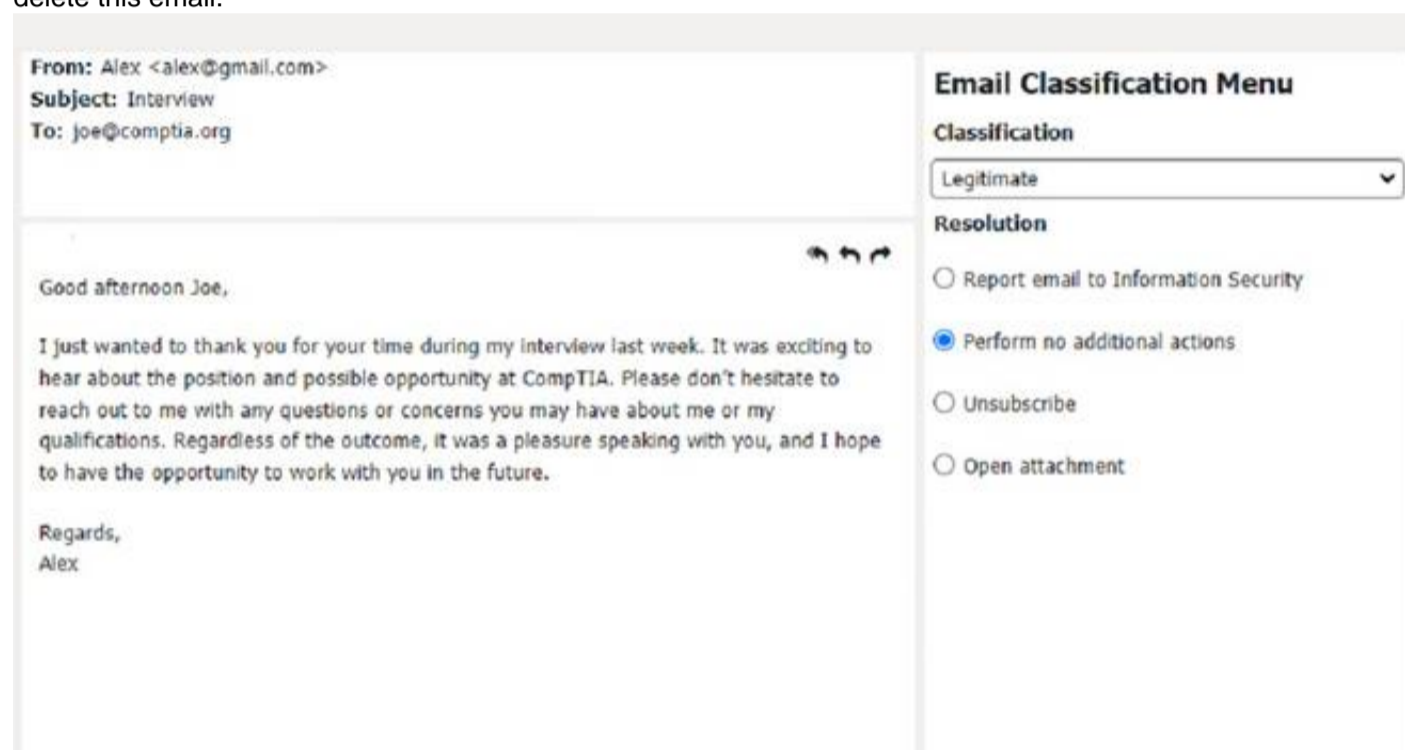
☐ Open attachment

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 111

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 114

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 115

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 116

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

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

Answer: A

Explanation:

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

NEW QUESTION 118

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

- A. Language
- B. System
- C. Personalization
- D. Ease of Access

Answer: D

Explanation:

The user can enable speech recognition on a PC in the Ease of Access settings tool. To set up Speech Recognition on a Windows PC, the user should open Control Panel, click on Ease of Access, click on Speech Recognition, and click the Start Speech Recognition link. Language settings can be used to change the language of the speech recognition feature, but they will not enable the feature. System settings can be used to configure the hardware and software of the PC, but they will not enable the speech recognition feature. Personalization settings can be used to customize the appearance and behavior of the PC, but they will not enable the speech recognition feature.

Open up ease of access, click on speech, then there is an on and off button for speech recognition.

NEW QUESTION 120

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

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

Answer: C

Explanation:

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

NEW QUESTION 125

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 129

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

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

Answer: A

Explanation:

The installation of home edition software on computers at a local office most likely violates the EULA. EULA stands for End User License Agreement and is a legal contract that specifies the terms and conditions for using a software product or service. EULA typically covers topics such as license scope, duration and limitations, rights and obligations of the parties, warranties and disclaimers, liability and indemnity clauses, and termination procedures. EULA may also restrict the use of home edition software to personal or non-commercial purposes only, and prohibit the use of home edition software in business or professional settings. Violating EULA may result in legal actions or penalties from the software vendor or developer. PII stands for Personally Identifiable Information and is any information that can be used to identify or locate an individual, such as name, address, phone number, email address, social security number or credit card number. PII is not related to software installation or licensing but to data protection and privacy. DRM stands for Digital Rights Management and is a technology that controls or restricts the access and use of digital content, such as music, movies, books or games. DRM is not related to software installation or licensing but to content distribution and piracy prevention. Open-source agreement is a type of license that allows users to access, modify and distribute the source code of a software product or service freely and openly. Open-source agreement does not restrict the use of software to home edition only but encourages collaboration and innovation among developers and users. References: CompTIA A+ Core 2 (220-1102) Certification Exam Objectives Version 4.0, Domain 5.1

NEW QUESTION 133

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-\(3-0\)](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 134

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

- ☒ A. Startup
- ☐ B: Performance
- C. Application history
- D. Processes

Answer: D

Explanation:

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

NEW QUESTION 135

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 139

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

- A. c: \minutes
- B. dir
- C. rmdir
- D. md

Answer: D

Explanation:

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

NEW QUESTION 144

Which of the following operating systems is most commonly used in embedded systems?

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

Answer: D

Explanation:

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

NEW QUESTION 148

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

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

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

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

Answer: D

Explanation:

In order to connect to a user's laptop via RDP, the technician should open port 3389 on the Windows firewall. This is because RDP uses port 3389 for communication¹². The other options are not necessary or relevant for establishing an RDP connection.

? Confirming the user can ping the default gateway is not required for RDP, as it

only tests the network connectivity between the user's laptop and the router. RDP works over the internet, so the technician should be able to ping the user's laptop directly using its IP address³.

? Changing the IP address on the user's laptop is not needed for RDP, as long as

the IP address is valid and not conflicting with another device on the network. The user's laptop has a valid IP address of 192.168.0.45, which belongs to the same subnet as the gateway (192.168.0.1) and the subnet mask (255.255.255.0)⁴.

? Changing the subnet mask on the user's laptop is not required for RDP, as long as

the subnet mask matches the network configuration. The user's laptop has a correct subnet mask of 255.255.255.0, which defines a network with 254 possible hosts⁴.

References:

1: [What is RDP and How Does It Work? - CompTIA] 2: CompTIA A+ Certification Exam Core 2 Objectives - CompTIA 3: [Ping (networking utility) - Wikipedia] 4: [IP address - Wikipedia] : What is RDP and How Does It Work? - CompTIA : CompTIA A+ Certification Exam Core 2 Objectives - CompTIA : Ping (networking utility) - Wikipedia) : IP address - Wikipedia

NEW QUESTION 151

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

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

Answer: B

Explanation:

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

NEW QUESTION 152

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 154

The screen on a user's mobile device is not autorotating even after the feature has been enabled and the device has been restarted. Which of the following should the technician do next to troubleshoot the issue?

- A. Calibrate the phone sensors.
- B. Enable the touch screen.
- C. Reinstall the operating system.
- D. Replace the screen.

Answer: A

Explanation:

Calibrating the phone sensors is a step that can troubleshoot the issue of screen not autorotating on a mobile device. Screen autorotation is a feature that automatically adjusts the screen orientation based on the device's position and movement. Screen autorotation relies on sensors such as accelerometer and gyroscope to detect the device's tilt and rotation. Calibrating the phone sensors can help fix any errors or inaccuracies in the sensor readings that may prevent screen autorotation from working properly. Enabling the touch screen, reinstalling the operating system, and replacing the screen are not steps that should be done next to troubleshoot this issue.

NEW QUESTION 157

Which of the following wireless security features can be enabled to allow a user to use login credentials to attach to available corporate SSIDs?

- A. TACACS+
- B. Kerberos
- C. Preshared key
- D. WPA2/AES

Answer: D

Explanation:

WPA2/AES (Wi-Fi Protected Access 2/Advanced Encryption Standard) is a wireless security standard that supports enterprise mode, which allows a user to use login credentials (username and password) to authenticate to available corporate SSIDs (service set identifiers). TACACS+ (Terminal Access Controller Access-Control System Plus) and Kerberos are network authentication protocols, but they are not wireless security features. Preshared key is another wireless security feature, but it does not use login credentials. Verified References: <https://www.comptia.org/blog/wireless-security-standards>
<https://www.comptia.org/certifications/a>

NEW QUESTION 159

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

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

Answer: C

Explanation:

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

References:

- ? Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 15
- ? CompTIA A+ Complete Study Guide: Core 1 Exam 220-1101 and Core 2 Exam ..., page 105

NEW QUESTION 160

Which of the following must be maintained throughout the forensic evidence life cycle when dealing with a piece of evidence?

- A. Acceptable use
- B. Chain of custody
- C. Security policy
- D. Information management

Answer: B

Explanation:

The aspect of forensic evidence life cycle that must be maintained when dealing with a piece of evidence is chain of custody. This is because chain of custody is the documentation of the movement of evidence from the time it is collected to the time it is presented in court, and it is important to maintain the integrity of the evidence

NEW QUESTION 164

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

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

Answer: B

Explanation:

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

NEW QUESTION 167

A technician is setting up a desktop computer in a small office. The user will need to access files on a drive shared from another desktop on the network. Which of the following configurations should the technician employ to achieve this goal?

- A. Configure the network as private
- B. Enable a proxy server
- C. Grant the network administrator role to the user
- D. Create a shortcut to public documents

Answer: A

Explanation:

The technician should configure the network as private to allow the user to access files on a drive shared from another desktop on the network

NEW QUESTION 171

Which of the following helps ensure that a piece of evidence extracted from a PC is admissible in a court of law?

- A. Data integrity form
- B. Valid operating system license
- C. Documentation of an incident
- D. Chain of custody

Answer: D

Explanation:

Chain of custody is a process that helps ensure that a piece of evidence extracted from a PC is admissible in a court of law. Chain of custody refers to the documentation and tracking of who handled, accessed, modified, or transferred the evidence, when, where, why, and how. Chain of custody can help establish the authenticity, integrity, and reliability of the evidence, as well as prevent tampering, alteration, or loss of the evidence. Data integrity form, valid operating system license, and documentation of an incident are not processes that can ensure that a piece of evidence extracted from a PC is admissible in a court of law.

NEW QUESTION 172

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 cache1e2

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 176

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

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

Answer: B

Explanation:

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

NEW QUESTION 177

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

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

Answer: D

Explanation:

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

NEW QUESTION 182

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

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

Answer: C

Explanation:

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

NEW QUESTION 187

Which of the following is a proprietary Cisco AAA protocol?

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

Answer: D

Explanation:

TACACS+ is a proprietary Cisco AAA protocol

NEW QUESTION 190

A company-owned mobile device is displaying a high number of ads, receiving data-usage limit notifications, and experiencing slow response. After checking the

device, a technician notices the device has been jailbroken. Which of the following should the technician do next?

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

Answer: B

Explanation:

Jailbreaking a device exposes it to various security risks, such as malware, data theft, network attacks, and service disruption¹²³⁴. Running an antivirus and enabling encryption may not be enough to remove the threats and restore the device's functionality. Undoing the jailbreak may not be possible or effective, depending on the method used. Backing up the files and doing a system restore may preserve the jailbreak and the associated problems. The best option is to erase the device and reinstall the original operating system that is compatible with the corporate policies and standards. This will ensure that the device is clean, secure, and compliant²⁵.

References: 1 What is Jailbreaking & Is it safe? - Kaspersky(<https://www.kaspersky.com/resource-center/definitions/what-is-jailbreaking>). 2 Jailbreak Detection: Why is jailbreaking a potential security risk? -

Cybersecurity ASEE(<https://cybersecurity.asee.co/blog/what-is-jailbreaking/>). 3 Jailbreaking Information for iOS Devices | University

IT(<https://uit.stanford.edu/service/mydevices/jailbreak>)4 What does it mean to jailbreak your phone—and is it legal? - Microsoft(<https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-jailbreaking-a-phone>).

5 Resetting a corporate laptop back to a personal laptop... Enterprise vs Pro -

Windows 10(<https://community.spiceworks.com/topic/2196812-resetting-a-corporate-laptop-back-to-a-personal-laptop-enterprise-vs-pro>).

NEW QUESTION 195

Remote employees need access to information that is hosted on local servers at the company. The IT department needs to find a solution that gives employees secure access to the company's resources as if the employees were on premises. Which of the following remote connection services should the IT team implement?

- A. SSH
- B. VNC
- C. VPN
- D. RDP

Answer: C

Explanation:

A VPN (Virtual Private Network) is a service that allows remote employees to access the company's network resources securely over the internet as if they were on premises. A VPN encrypts the data traffic between the employee's device and the VPN server, and assigns the employee a virtual IP address that belongs to the company's network. This way, the employee can access the local servers, files, printers, and other resources without exposing them to the public internet. A VPN also protects the employee's privacy and identity by masking their real IP address and location.

NEW QUESTION 196

A technician has just used an anti-malware removal tool to resolve a user's malware issue on a corporate laptop. Which of the following BEST describes what the technician should do before returning the laptop to the user?

- A. Educate the user on malware removal.
- B. Educate the user on how to reinstall the laptop OS.
- C. Educate the user on how to access recovery mode.
- D. Educate the user on common threats and how to avoid them.

Answer: D

Explanation:

educating the user on common threats and how to avoid them (D) would be a good step before returning the laptop to the user. This can help prevent similar issues from happening again.

NEW QUESTION 201

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

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

Answer: C

Explanation:

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

NEW QUESTION 202

A user installed a new application that automatically starts each time the user logs in to a Windows 10 system. The user does not want this to happen and has

asked for this setting to be changed. Which of the following tools would the technician MOST likely use to safely make this change?

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

The technician would most likely use the Task Manager tool to safely make this change¹²

The Task Manager tool can be used to disable applications from starting automatically on Windows 10

The tool that a technician would most likely use to stop an application from automatically starting when a user logs in to a Windows 10 system is the Task Manager. The Task Manager can be used to view and manage processes, including those that are set to automatically start when a user logs in to the system.

NEW QUESTION 205

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

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

Answer: C

Explanation:

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

References: 1: <https://windowsreport.com/mirror-backup-software/>

NEW QUESTION 209

A technician is troubleshooting a PC that has been performing poorly. Looking at the Task Manager, the technician sees that CPU and memory resources seem fine, but disk throughput is at 100%.

Which of the following types of malware is the system MOST likely infected with?

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

Answer: C

Explanation:

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

NEW QUESTION 212

A mobile phone user has downloaded a new payment application that allows payments to be made with a mobile device. The user attempts to use the device at a payment terminal but is unable to do so successfully. The user contacts a help desk technician to report the issue. Which of the following should the technician confirm NEXT as part of the troubleshooting process?

- ☒ A. If airplane mode is enabled
- ☐ B: If Bluetooth is disabled
- ☐ C. If NFC is enabled
- ☐ D. If WiFi is enabled
- ☐ E. If location services are disabled

Answer: C

Explanation:

NFC stands for Near Field Communication, and it is a wireless technology that allows your phone to act as a contactless payment device, among other things².

Payment applications that allow payments to be made with a mobile device usually rely on NFC to communicate with the payment terminal¹. Therefore, if NFC is disabled on the phone, the payment will not work. To enable NFC on an Android phone, you need to follow these steps³:

? On your Android device, open the Settings app.

? Select Connected devices.

? Tap on Connection preferences.

? You should see the NFC option. Toggle it on.

The other options are not directly related to using a payment application with a mobile device. Airplane mode is a setting that disables all wireless communication on the phone, including NFC⁴, but it also affects calls, texts, and internet access. Bluetooth is a wireless technology that allows you to connect your phone with other devices such as headphones or speakers, but it is not used for contactless payments. Wi-Fi is a wireless technology that allows you to access the internet or a local network, but it is also not used for contactless payments. Location services are a feature that allows your phone to determine your geographic location using GPS or other methods, but they are not required for contactless payments.

NEW QUESTION 215

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 217

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 222

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 227

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

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

Answer: B

Explanation:

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

NEW QUESTION 230

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

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

Answer: B

Explanation:

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

NEW QUESTION 234

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 phone.

NEW QUESTION 235

Which of the following is a consequence of end-of-life operating systems?

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

Answer: C

Explanation:

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

NEW QUESTION 237

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

A.

VPN

- B. SMB
- C. RMM
- D. MSRA

Answer: B

Explanation:

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

NEW QUESTION 238

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

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

Answer: A

Explanation:

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

for systems or services. MSRA stands for Microsoft Remote Assistance and is a feature that allows remote access and control of a Windows desktop environment over a network. MSRA is not natively designed for Linux and may not be compatible or supported by Linux systems. RDP stands for Remote Desktop Protocol and is a protocol that allows remote access and control of a Windows desktop environment over a network. RDP is not natively designed for Linux and may not be compatible or supported by Linux systems. References: CompTIA A+ Core 2 (220-1102) Certification Exam Objectives Version 4.0, Domain 1.6

NEW QUESTION 240

A user's corporate laptop with proprietary work Information was stolen from a coffee shop. The user toggled 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 245

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 247

A desktop specialist needs to prepare a laptop running Windows 10 for a newly hired employee. Which of the following methods should the technician use to refresh the laptop?

- A. Internet-based upgrade
- B. Repair installation
- C. Clean install
- D. USB repair
- E.

In place upgrade

Answer: C

Explanation:

The desktop specialist should use a clean install to refresh the laptop. A clean install will remove all data and applications from the laptop and install a fresh copy of Windows 10, ensuring that the laptop is ready for the newly hired employee.

NEW QUESTION 249

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

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

Answer: D

Explanation:

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

NEW QUESTION 252

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

- A. Utilizing an ESD strap
- B. Disconnecting the computer from the power source
- C. Placing the PSU in an antistatic bag

- D. Ensuring proper ventilation
- E. Removing dust from the ventilation fans
- F. Ensuring equipment is grounded

Answer: AC

Explanation:

The two safety procedures that would best protect the components in the PC are:

- ? Utilizing an ESD strap
- ? Placing the PSU in an antistatic bag

<https://www.professormesser.com/free-a-plus-training/220-902/computer-safety-procedures-2/>

<https://www.skillssoft.com/course/comptia-a-core-2-safety-procedures-environmental-impacts-cbdf0f2c-61c0-4f4a-a659-dc98f1f00158>

NEW QUESTION 253

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 255

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

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

Answer: C

Explanation:

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

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

NEW QUESTION 258

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 259

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

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

Answer: A

Explanation:

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

NEW QUESTION 263

A user's permissions are limited to read on a shared network folder using NTFS security settings. Which of the following describes this type of security control?

- A. SMS
- B.

MFA

- C. ACL
- D. MDM

Answer: C

Explanation:

ACL (access control list) is a security control that describes what permissions a user or group has on a shared network folder using NTFS (New Technology File System) security settings. It can be used to grant or deny read, write, modify, delete or execute access to files and folders. SMS (short message service), MFA (multifactor authentication), MDM (mobile device management) are not security controls that apply to shared network folders. Verified References:
<https://www.comptia.org/blog/what-is-an-acl> <https://www.comptia.org/certifications/a>

NEW QUESTION 267

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

- A.

Network & Internet

- B. System
- C. Personalization
- D. Accounts

Answer: A

Explanation:

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

References:

? The Official CompTIA A+ Core 2 Study Guide¹, page 221, 222, 223, 224.

NEW QUESTION 272

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

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

Application crash

- E. Profile rebuild needed

Answer: A

Explanation:

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

NEW QUESTION 277

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

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

Answer: A

Explanation:

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

NEW QUESTION 278

A user receives the following error while attempting to boot a computer.

BOOTMGR is missing

press Ctrl+Alt+Del to restart

Which of the following should a desktop engineer attempt FIRST to address this issue?

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

Answer: A

Explanation:

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

start Windows¹. To fix this error, one of the possible methods is to run Startup Repair from Windows Recovery Environment (WinRE)¹. Startup Repair is a tool that can automatically diagnose and repair problems with the boot process².
References: 1: "Bootmgr is missing Press Ctrl+Alt+Del to restart" error when you start Windows (<https://support.microsoft.com/en-us/topic/-bootmgr-is-missing-press-ctrl-alt-del-to-restart-error-when-you-start-windows-8bc1b94b-d243-1027-5410-aeb04d5cd5e2>) 2: Startup Repair: frequently asked questions (<https://support.microsoft.com/en-us/windows/startup-repair-frequently-asked-questions-f5f412a0-19c4-8e0a-9f68-bb0f17f3daa0>)

NEW QUESTION 280

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

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

Answer: C

Explanation:

The best way to deal with an angry customer who is yelling at a technician is to wait until the customer is done speaking and offer assistance. This shows respect, empathy, and professionalism, and allows the technician to understand the customer's problem and find a solution. According to the CompTIA A+ Core 2 (220-1102) Certification Study Guide¹, some of the steps to handle angry customers are:

- ? Stay calm and do not take it personally.
- ? Listen actively and acknowledge the customer's feelings.
- ? Apologize sincerely and offer to help.
- ? Restate the customer's issue and ask for clarification if needed.
- ? Explain the possible causes and solutions for the problem.
- ? Provide clear and realistic expectations for the resolution.

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

The other options are not appropriate ways to deal with angry customers, as they may worsen the situation or damage the customer relationship. Placing the customer on hold may make them feel ignored or dismissed. Disconnecting the call may make them feel disrespected or abandoned. Escalating the issue to a supervisor may make them feel frustrated or powerless, unless the technician cannot resolve the issue or the customer requests to speak to a supervisor.

References:

? CompTIA A+ Certification Exam Core 2 Objectives2

? CompTIA A+ Core 2 (220-1102) Certification Study Guide1

? How To Deal with Angry Customers (With Examples and Tips)3

? 17 ways to deal with angry customers: Templates and examples4

? Six Ways to Handle Angry Customers5

NEW QUESTION 281

When visiting a particular website, a user receives a message stating, "Your connection is not private." Which of the following describes this issue?

- ☐ A. Malware
- ☐ B: Certificate warning
- ☐ C. JavaScript error
- ☐ D. Missing OS update

Answer: A

Explanation:

A certificate warning is a message that appears when a web browser cannot verify the identity or security of a website. It usually means that there is a problem with the website's SSL certificate, such as expiration, invalidity, or mismatch. A certificate warning can indicate that the website is unsafe or compromised, and that the user's connection is not private123.

References: 1 How to Fix "Your Connection Is Not Private" Errors - How-To Geek(<https://www.howtogeek.com/874436/how-to-fix-your-connection-is-not-private-errors/>)2 How to fix a "Your connection is not private" error - Norton(<https://us.norton.com/blog/how-to/your-connection-is-not-private>)3 "Your Connection Is Not Private" Error: 8 Ways to Fix It - HubSpot Blog(<https://blog.hubspot.com/website/how-to-fix-your-connection-is-not-private>).

NEW QUESTION 283

The audio on a user's mobile device is inconsistent when the user uses wireless headphones and moves around. Which of the following should a technician perform to troubleshoot the issue?

- ☐ A. Verify the Wi-Fi connection status.
- ☐ B. Enable the NFC setting on the device.
- ☐ C. Bring the device within Bluetooth range.
- ☐ D. Turn on device tethering.

Answer: C

Explanation:

Bringing the device within Bluetooth range is the best way to troubleshoot the issue of inconsistent audio when using wireless headphones and moving around. Bluetooth is a wireless technology that allows devices to communicate over short distances, typically up to 10 meters or 33 feet. If the device is too far from the headphones, the Bluetooth signal may be weak or interrupted, resulting in poor audio quality or loss of connection.

NEW QUESTION 284

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

220-1102 Practice Exam Features:

- * 220-1102 Questions and Answers Updated Frequently
- * 220-1102 Practice Questions Verified by Expert Senior Certified Staff
- * 220-1102 Most Realistic Questions that Guarantee you a Pass on Your First Try
- * 220-1102 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The 220-1102 Practice Test Here](#)