Topic 1, Exam Pool A

Q1. - (Topic 1)
The network was breached over the weekend. System logs indicate that a single user's account was successfully breached after 500 attempts with a dictionary attack. Which of the following would BEST mitigate this threat?
A. Encryption at rest
B. Account lockout
C. Automatic screen lock
D. Antivirus
Answer: B
Explanation: Account lockout would best mitigate the threat of a dictionary attack1

Q2. - (Topic 1)
Which of the following Wi-Fi protocols is the MOST secure?
A. WPA3
B. WPA-AES
C. WEP
D. WPA-TKIP
Answer: A
Explanation:
https://partners.comptia.org/docs/default-source/resources/comptia-a-220-1102-exam-objectives-(3-0)

Q3. - (Topic 1)
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. Uninstall and reinstall the application
B. Reset the phone to factory settings
C. Install an alternative application with similar functionality
D. Clear the application cache.
Answer: D
Explanation:
The systems administrator should clear the application cache.
If clearing the application cache does not work, the systems administrator should uninstall and reinstall the application.
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

Q4. - (Topic 1)
An architecture firm is considering upgrading its computer-aided design (CAD) software to the newest version that forces storage of backups of all CAD files on the software's cloud server. Which of the following is MOST likely to be of concern to the IT manager?
A. All updated software must be tested with alt system types and accessories
B. Extra technician hours must be budgeted during installation of updates
C. Network utilization will be significantly increased due to the size of CAD files
D. Large update and installation files will overload the local hard drives.
Answer: C
Explanation: The IT manager is most likely to be concerned about network utilization being significantly
increased due to the size of CAD files. Backing up all CAD files to the software’s cloud server can result in a

large amount of data being transferred over the network, which can cause network congestion and slow
down other network traffic.

Q5. - (Topic 1)
A user reports that antivirus software indicates a computer is infected with viruses. The user thinks this happened while browsing the internet. The technician does not recognize the interface with which the antivirus message is presented. Which of the following is the NEXT step the technician should take?
A. Shut down the infected computer and swap it with another computer
B. Investigate what the interface is and what triggered it to pop up
C. Proceed with initiating a full scan and removal of the viruses using the presented interface
D. Call the phone number displayed in the interface of the antivirus removal tool
Answer: B
Explanation: The technician should not proceed with initiating a full scan and removal of the viruses using the presented interface or call the phone number displayed in the interface of the antivirus removal tool
Shutting down the infected computer and swapping it with another computer is not necessary at this point
The technician should not immediately assume that the message is legitimate or perform any actions without knowing what the interface is and what triggered it to pop up. It is important to investigate the issue further, including checking the legitimacy of the antivirus program and the message it is displaying.

Q6. - (Topic 1)
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.

Q7. - (Topic 1)
A change advisory board did not approve a requested change due to the lack of alternative actions if implementation failed. Which of the following should be updated before requesting approval again?
A. Scope of change
B. Risk level
C. Rollback plan
D. End user acceptance
Answer: C
Explanation: The rollback plan should be updated before requesting approval again. A rollback plan is a plan for undoing a change if it causes problems, and it is an important part of any change management process. If the change advisory board did not approve the requested change due to the lack of alternative actions if implementation failed, then updating the rollback plan would be the best way to address this concern.

Q8. - (Topic 1)
Which of the following is the MOST important environmental concern inside a data center?

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

Q9. - (Topic 1)
A change advisory board just approved a change request. Which of the following is the MOST likely next step in the change process?
A. End user acceptance
B. Perform risk analysis
C. Communicate to stakeholders
D. Sandbox testing
Answer: A
Order of change management phases:
1. Request forms
2. Purpose of change
3. Scope of the change
4. Date and Time of the change
5. Affective systems/ impact
6. Risk analysis
7. Change board approval
8. Finally end user acceptance.

Q10. - (Topic 1)
An incident handler needs to preserve evidence for possible litigation. Which of the following will the incident handler MOST likely do to preserve the evidence?
A. Encrypt the files
B. Clone any impacted hard drives
C. Contact the cyber insurance company
D. Inform law enforcement
Answer: B
Explanation: The incident handler should clone any impacted hard drives to preserve evidence for possible
litigation1

Q11. - (Topic 1)
After clicking on a link in an email a Chief Financial Officer (CFO) received the following error:

"X. THERE IS A PROBLEM WITH THIS WEBSITE'S SECURITY CERTIFICATE"

THE SECURITY CERTIFICATE PRESENTED BY THIS WEBSITE WAS NOT ISSUED BY A TRUST CERTIFICATE AUTHORITY

THE SECURITY CERTIFICATE PRESENTED BY THIS WEBSITE WAS ISSUED FOR A DIFFERENT WEBSITE ADDRESS.

SECURITY CERTIFICATE PROBLRMS MAY INDICATE AN ATTEMPT TO FOOL YOU OR INTERCEPT ANY DATA YOU SEND TO THE SERVER."

The CFO then reported the incident to a technician. The link is purportedly to the organization's bank.
Which of the following should the technician perform FIRST?
A. Update the browser's CRLs
B. File a trouble ticket with the bank.
C. Contact the ISP to report the CFCs concern
D. Instruct the CFO to exit the browser
Answer: D
Explanation:

1. **Prevent Further Risk**: Exiting the browser immediately prevents any potential further interaction with the suspicious link or website, which could protect the system from potential malware or phishing attacks.
2. **Mitigate Immediate Threat**: By stopping any interaction with the suspicious site, the risk of data compromise or malware installation is minimized.
3. **Initial Safety Measure**: Ensuring that the CFO is no longer engaging with the potentially malicious link is a crucial first step before investigating further or taking additional actions.

Q12. - (Topic 1)
Upon downloading a new ISO, an administrator is presented with the following string:

59d15a16ce90cBcc97fa7c211b767aB

Which of the following BEST describes the purpose of this string?
A. XSS verification
B. AES-256 verification
C. Hash verification
D. Digital signature verification
Answer: C
Explanation: Hash verification is a process that verifies the integrity of a file by comparing the hash value of the downloaded file to the hash value provided by the source1

Q14. - (Topic 1)
A technician is installing new network equipment in a SOHO and wants to ensure the quipment is secured against external threats on the Internet. Which of the following actions should the technician do FIRST?
A. Lock all devices in a closet.
B. Ensure all devices are from the same manufacturer.
C. Change the default administrative password.
D. Install the latest operating system and patches
Answer: C
Explanation: The technician should change the default administrative password FIRST to ensure the network equipment is secured against external threats on the Internet. Changing the default administrative password is a basic security measure that can help prevent unauthorized access to the network equipment. Locking all devices in a closet is a physical security measure that can help prevent theft or damage to the devices, but it does not address external threats on the Internet. Ensuring all devices are from the same manufacturer is not a security measure and does not address external threats on the Internet. Installing the latest operating system and patches is important for maintaining the security of the network equipment, but it is not the first action the technician should take1

Q15. - (Topic 1)
A user wants to set up speech recognition on a PC. In which of the following Windows Settings tools can the user enable this option?
A. Language
B. System
C. Personalization
D. Ease of Access
Answer: D
Explanation: The user can enable speech recognition on a PC in the Ease of Access settings tool. To set up
Speech Recognition on a Windows PC, the user should open Control Panel, click on Ease of Access, click on Speech Recognition, and click the Start Speech Recognition link. Language settings can be used to change the language of the speech recognition feature, but they will not enable the feature. System settings can be used to configure the hardware and software of the PC, but they will not enable the speech recognition feature. Personalization settings can be used to customize the appearance and behavior of the PC, but they will not enable the speech recognition feature1
Open up ease of access, click on speech, then there is an on and off button for speech recognition.

Q16. - (Topic 1)
A user has requested help setting up the fingerprint reader on a Windows 10 laptop. The laptop is equipped with a fingerprint reader and is joined to a domain Group Policy enables Windows Hello on all computers in the environment. Which of the following options describes how to set up Windows Hello Fingerprint for the user?
A. Navigate to the Control Panel utility, select the Security and Maintenance submenu, select Change
Security and Maintenance settings, select Windows Hello Fingerprint, and have the user place a fingerprint
on the fingerprint reader repeatedly until Windows indicates setup is complete
B. Navigate to the Windows 10 Settings menu, select the Accounts submenu, select Sign in options, select
Windows Hello Fingerprint, and have the user place a fingerprint on the fingerprint reader repeatedly until
Windows indicates setup is complete.
C. Navigate to the Windows 10 Settings menu, select the Update & Security submenu select Windows
Security, select Windows Hello Fingerprint and have the user place a fingerprint on the fingerprint reader
repeatedly until Windows indicates setup is complete
D. Navigate to the Control Panel utility, select the Administrative Tools submenu, select the user account in
the list, select Windows Hello Fingerprint, and have the user place a fingerprint on the fingerprint reader
repeatedly until Windows indicates setup is complete.
Answer: B
Explanation: Navigate to the Windows 10 Settings menu, select the Accounts submenu, select Sign in options, select Windows Hello Fingerprint, and have the user place a fingerprint on the fingerprint reader repeatedly until Windows indicates setup is complete. Windows Hello Fingerprint can be set up by navigating to the Windows 10 Settings menu, selecting the Accounts submenu, selecting Sign in options, and then selecting Windows Hello Fingerprint. The user will then be asked to place a fingerprint on the fingerprint reader repeatedly until Windows indicates that setup is complete. Windows Hello Fingerprint allows the user to log into the laptop using just their fingerprint, providing

an additional layer of security.

Q17. - (Topic 1)
A user receives a notification indicating the antivirus protection on a company laptop is out of date. A technician is able to ping the user's laptop. The technician checks the antivirus parent servers and sees the latest signatures have been installed. The technician then checks the user's laptop and finds the antivirus engine and definitions are current. Which of the following has MOST likely occurred?
A. Ransomware
B. Failed OS updates
C. Adware
D. Missing system files
Answer: B
Explanation: The most likely reason for the antivirus protection on a company laptop being out of date is failed OS updates1. Antivirus software relies on the operating system to function properly. If the operating system is not up to date, the antivirus software may not function properly and may not be able to receive the latest virus definitions and updates2. Therefore, it is important to keep the operating system up-to-date to ensure the antivirus software is functioning properly2.

Q18. - (Topic 1)
A user is having phone issues after installing a new application that claims to optimize performance. The user downloaded the application directly from the vendor's website and is now experiencing high network utilization and is receiving repeated security warnings. Which of the following should the technician perform FIRST to mitigate the issue?
A. Reset the phone to factory settings
B. Uninstall the fraudulent application
C. Increase the data plan limits
D. Disable the mobile hotspot.
Answer: B
Explanation: Installing applications directly from a vendor's website can be risky, as the application may be malicious or fraudulent. Uninstalling the application can help mitigate the issue by removing the source of the problem.

Q19. - (Topic 1)
A technician needs to transfer a large number of files over an unreliable connection. The technician should be able to resume the process if the connection is interrupted. Which of the following tools can be used?
A. afc
B. chkdsk
C. git clone
D. robocopy
Answer: D
Here’s why robocopy is suitable for this task:

Resuming Transfers: robocopy (Robust File Copy) is a command-line tool in Windows that supports resuming interrupted file transfers. It is designed to handle unreliable connections and can retry and resume copying files if the process is interrupted.

Error Recovery: It includes features for retrying on failures, and it can handle network interruptions gracefully, making it a robust choice for large file transfers.

Advanced Options: robocopy provides various options for copying files, including mirroring directories and copying file attributes, making it highly versatile for file management tasks.

Q20. - (Topic 1)
A technician needs to format a USB drive to transfer 20GB of data from a Linux computer to a Windows computer. Which of the following file systems will the technician MOST likely use?
A. FAT32
B. ext4
C. NTFS
D. exFAT
Answer: D
Explanation: exFAT is the most "universally" compatible option of the 4.

exFAT covers all the bases. It supports single file sizes in a size range larger than the largest available consumer disk drives, let alone removeable media. In addition, it's generally compatible with Linux, due to being a simple system overall.

FAT32 only supports file sizes up to 4 GB, which may or may not be acceptable for this transfer, as we don't know if it's a single 20 GB file or multiple 4GB or less files. Because it isn't stated, don't assume multiple files, go only with what is supplied. 20GB, so CompTIA probably wants to see that you know FAT32 doesn't work with files greater than 4GB.

ext4 would work with Linux, but I'll be honest, in over 5 years working in IT, I have never formatted a drive ext4 for desktop level use.

NTFS was developed as a primarily "Windows" file format, and while some version of Linux may work with it, there is the chance for compatibility issues.

Q21. - (Topic 1)
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

Q23. - (Topic 1)
A company wants to remove information from past users’ hard drives in order to reuse the hard drives Witch of the following is the MOST secure method
A. Reinstalling Windows
B. Performing a quick format
C. Using disk-wiping software
D. Deleting all files from command-line interface
Answer: C
Explanation: Using disk-wiping software is the most secure method for removing information from past users’ hard drives in order to reuse the hard drives. Disk-wiping software can help to ensure that all data on the hard drive is completely erased and cannot be recovered.

Q24. - (Topic 1)
A user needs assistance changing the desktop wallpaper on a Windows 10 computer. Which of the

following methods will enable the user to change the wallpaper using a Windows 10 Settings tool?
A. Open Settings, select Accounts, select, your info, click Browse, and then locate and open the image the user wants to use as the wallpaper
B. Open Settings, select Personalization, click Browse, and then locate and open the image the user wants to use as the wallpaper
C. Open Settings, select System, select Display, click Browse, and then locate and open the image the user wants to use as the wallpaper
D. Open Settings, select Apps, select Apps & features, click Browse, and then locate and open the image the user wants to use as the wallpaper.
Answer: B
Explanation: To change the desktop wallpaper on a Windows 10 computer using a Windows 10 Settings tool, the user should open Settings, select Personalization,
click Browse, and then locate and open the image the user wants to use as the wallpape1r
https://www.lifewire.com/change-desktop-background-windows-11-5190733

Q25. - (Topic 1)
Which of the following provide the BEST way to secure physical access to a data cento server room?
(Select TWO).
A. Biometric lock
B. Badge reader
C. USB token
D. Video surveillance
E. Locking rack
F. Access control vestibule
Answer: A,B
Explanation: A biometric lock requires an authorized user to provide a unique biometric identifier, such as a fingerprint, in order to gain access to the server room. A badge reader requires an authorized user to swipe an access card in order to gain access. Both of these methods ensure that only authorized personnel are able to access the server room. Additionally, video surveillance and access control vestibules can be used to further secure the server room. Finally, a locking rack can be used to physically secure the servers, so that they cannot be accessed without the appropriate key.

Q26. - (Topic 1)
A user calls the help desk to report potential malware on a computer. The anomalous activity began after the user clicked a link to a free gift card in a recent email. The technician asks the user to describe any unusual activity, such as slow performance, excessive pop- ups, and browser redirections. Which of the following should the technician do NEXT?
A. Advise the user to run a complete system scan using the OS anti-malware application
B. Guide the user to reboot the machine into safe mode and verify whether the anomalous activities are still
present
C. Have the user check for recently installed applications and outline those installed since the link in the email was clicked
D. Instruct the user to disconnect the Ethernet connection to the corporate network.
Answer: D
Explanation: First thing you want to do is quarantine/disconnect the affected system from the network so whatever malicious software doesn't spread.

Q27. - (Topic 1)
A user is unable to log in to the domain with a desktop PC, but a laptop PC is working properly on the same network. A technician logs in lo the desktop PC with a local account but is unable to

browse to the secure intranet site to get troubleshooting tools. Which of the following is the MOST likely cause of the issue?
A. Time drift
B. Dual in-line memory module failure
C. Application crash
D. Filesystem errors
Answer: A
Explanation: The most likely cause of the issue is a “time drift”. Time drift occurs when the clock on a computer is not synchronized with the clock on the domain controller. This can cause authentication problems when a user tries to log in to the domain. The fact that the technician is unable to browse to the secure intranet site to get troubleshooting tools suggests that there may be a problem with the network connection or the firewall settings on the desktop PC.

Q28. - (Topic 1)
A user reports a computer is running slow. Which of the following tools will help a technician identify the issue?
A. Disk Cleanup
B. Group Policy Editor
C. Disk Management
D. Resource Monitor
Answer: D
Explanation: Resource Monitor is a Windows utility that can be used to monitor and analyze the system resources and processes running on a computer. It can be used to identify and troubleshoot any issues that might be causing the computer to run slowly, such as CPU usage, memory usage, disk I/O, and network usage.

Q29. - (Topic 1)
A technician wants to enable BitLocker on a Windows 10 laptop and is unable to find the BitLocker Drive Encryption menu item in Control Panel. Which of the following explains why the technician unable to find this menu item?
A. The hardware does not meet BitLocker's minimum system requirements.
B. BitLocker was renamed for Windows 10.
C. BitLocker is not included on Windows 10 Home.
D. BitLocker was disabled in the registry of the laptop
Answer: C
Explanation: BitLocker is only available on Windows 10 Pro, Enterprise, and Education editions. Therefore, the technician is unable to find the BitLocker Drive Encryption menu item in Control Panel because it is not included in the Windows 10 Home edition.

Q30. - (Topic 1)
A user reports that a PC seems to be running more slowly than usual. A technician checks system resources, but disk, CPU, and memory usage seem to be fine. The technician sees that GPU temperature is extremely high. Which of the following types of malware is MOST likely to blame?
A. Spyware
B. Cryptominer
C. Ransormvare
D. Boot sector virus
Answer: B
Explanation: The type of malware that is most likely to blame for a PC running more slowly than usual and having an extremely high GPU temperature is a “cryptominer”. Cryptominers are a type of malware that use the resources of a computer to mine cryptocurrency. This can cause the computer to run more slowly than usual and can cause the GPU temperature to rise. Spyware is a type of malware that is used to spy on a user’s activities, but it does not typically cause high GPU

temperatures. Ransomware is a type of malware that encrypts a user's files and demands payment to unlock them, but it does not typically cause high GPU temperatures. Boot sector viruses are a type of malware that infects the boot sector of a hard drive, but they
do not typically cause high GPU temperatures12

Q31. - (Topic 1)
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: A
Here's why a Power user account is appropriate in this scenario:
Advanced Features: Power user accounts are designed to give users more control than a standard user account but less than an administrator account. They can perform tasks such as installing and configuring applications and accessing advanced features without having full administrative privileges.

Least Privilege: While Power user accounts don't have as much control as Administrator accounts, they still provide the necessary access to configure and manage applications effectively. This aligns with the principle of least privilege by providing just enough access for the user to perform their job functions.

Other options and their considerations:

B. Standard account: This account type has limited permissions and may not allow the user to access or configure advanced features of applications.

C. Guest account: This account type is extremely limited and is intended for temporary use or minimal access. It is not suitable for users who need to perform advanced tasks or configurations.

D. Administrator account: While an Administrator account provides full control over the system, it is generally more access than necessary and does not adhere to the principle of least privilege. It should be used only when absolutely required. Placing Windows user accounts in the Power Users security group is a common approach IT organizations take to get users into a least-privilege environment while avoiding the many pains of truly running as a limited user. The Power Users group is able to install software, manage power and time-zone settings, and install ActiveX controls, actions that limited Users are denied.

Q32. - (Topic 1)
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.

Q33. - (Topic 1)
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: C,E
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.

Q34. - (Topic 1)
A technician needs to document who had possession of evidence at every step of the process. Which of the following does this process describe?
A. Rights management
B. Audit trail
C. Chain of custody
D. Data integrity
Answer: C
Explanation: The process of documenting who had possession of evidence at every step of the process is called chain of custody

Q35. - (Topic 1)
A technician has been tasked with installing a workstation that will be used for point-of-sale transactions. The point-of-sale system will process credit cards and loyalty cards. Which of the following encryption technologies should be used to secure the workstation in case of theft?
A. Data-in-transit encryption
B. File encryption
C. USB drive encryption
D. Disk encryption
Answer: D
Explanation: Disk encryption should be used to secure the workstation in case of theft. Disk encryption can help to protect data on the hard drive by encrypting it so that it cannot be accessed without the correct encryption key.

Q36. - (Topic 1)
A technician is investigating an employee's smartphone that has the following symptoms:
• The device is hot even when it is not in use.
•Applications crash, especially when others are launched.
• Certain applications, such as GPS, are in portrait mode when they should be in landscape mode.
Which of the following can the technician do to MOST likely resolve these issues with minimal impact?
(Select TWO).

A. Turn on autorotation
B. Activate airplane mode.
C. Close unnecessary applications
D. Perform a factory reset
E. Update the device's operating system
F. Reinstall the applications that have crashed.
Answer: A, C
Explanation: The technician can close unnecessary applications and turn on autorotation to resolve these issues with minimal impact. Autorotation can help the device to switch between portrait and landscape modes automatically. Closing unnecessary applications can help to free up the device's memory and reduce the device's temperature
Reference:
CompTIA A+ Certification Exam: Core 2 (220-1102) Exam Objectives Version 4.0. Retrieved from https://partners.comptia.org/docs/default-source/resources/comptia-a-220-1102-exam-objectives-(3-0)

Q37. - (Topic 1)
A user purchased a netbook that has a web-based, proprietary operating system. Which of the following operating systems is MOST likely installed on the netbook?
A. macOS
B. Linux
C. Chrome OS
D. Windows
Answer: C
Explanation: 4. Chrome OS. Retrieved from https://en.wikipedia.org/wiki/Chrome_OS 5. What is Chrome OS? Retrieved from https://www.google.com/chromebook/chrome-os/
A netbook with a web-based, proprietary operating system is most likely running Chrome OS. Chrome OS is a web-based operating system developed by Google that is designed to work with web applications and cloud storage. It is optimized for netbooks and other low- power devices and is designed to be fast, secure, and easy to use.

Q38. - (Topic 1)
A technician is setting up a SOHO wireless router. The router is about ten years old. The customer would like the most secure wireless network possible. Which of the following should the technician configure?
A. WPA2 with TKIP
B. WPA2 with AES
C. WPA3withAES-256
D. WPA3 with AES-128
Answer: B
Explanation: This is because WPA2 with AES is the most secure wireless network configuration that is available on a ten-year-old SOHO wireless router.

Q39. - (Topic 1)
A network administrator is deploying a client certificate lo be used for Wi-Fi access for all devices in an organization. The certificate will be used in conjunction with the user's existing username and password. Which of the following BEST describes the security benefits realized after this deployment?
A. Multifactor authentication will be forced for Wi-Fi
B. All Wi-Fi traffic will be encrypted in transit
C. Eavesdropping attempts will be prevented
D. Rogue access points will not connect
Answer: A

Explanation: Multifactor authentication will be forced for Wi-Fi after deploying a client certificate to be used for Wi-Fi access for all devices in an organization3
References:
☞ CompTIA Security+ (Plus) Practice Test Questions | CompTIA. Retrieved from https://www.comptia.org/training/resources/comptia-security-practice-tests

Q40. - (Topic 1)
A technician receives a ticket indicating the user cannot resolve external web pages. However, specific IP addresses are working. Which of the following does the technician MOST likely need to change on the workstation to resolve the issue?
A. Default gateway
B. Host address
C. Name server
D. Subnet mask
Answer: C
Explanation: When a user enters a website name or URL into a web browser, the computer sends a request to a DNS server to resolve the domain name into an IP address that the computer can use to connect to the server hosting the website. This process is called DNS resolution.

If a user can access specific IP addresses but cannot resolve external web pages, it could indicate a problem with the DNS server settings on the user's workstation. The DNS server settings on the workstation could be incorrect or pointing to an invalid DNS server.

In this scenario, the technician would need to change the name server settings on the workstation to point to a valid DNS server that can correctly resolve domain names into IP addresses. The default gateway, host address, and subnet mask settings are not typically related to DNS resolution and would not resolve the issue of not being able to resolve external web pages.

Q41. - (Topic 1)
Which of the following Linux commands would be used to install an application?
A. yum
B. grep
C. ls
D. sudo

Answer: A
Explanation: Here's an overview of why yum is the correct choice and a brief explanation of the other commands:

1. **yum (Yellowdog Updater, Modified)**:
    - **Function**: yum is a package manager used in RPM-based Linux distributions (such as CentOS, Fedora, and Red Hat Enterprise Linux). It handles the installation, updating, and removal of software packages from repositories.
    - **Usage**: To install an application, you would use a command like sudo yum install <package-name>.

Other options and their purposes:

- **B. grep**: grep is a command-line utility used for searching text using patterns. It is not used for installing applications.
- **C. ls**: ls is a command used to list directory contents. It is used for viewing files and directories but not for installing applications.
- **D. sudo**: sudo stands for "superuser do" and is used to execute commands with superuser (root) privileges. While sudo is often used in conjunction with other commands for installing applications (e.g., sudo yum install <package-name>), it itself does not install applications.

Q42. - (Topic 1)
A technician is troubleshooting an issue involving programs on a Windows 10 machine that are loading on startup but causing excessive boot times. Which of the following should the technician do to selectively prevent programs from loading?
A. Right-click the Windows button, then select Run entering shell startup and clicking OK, and then move items one by one to the Recycle Bin
B. Remark out entries listed
HKEY_LOCAL_MACHINE>SOFTWARE>Microsoft>Windows>CurrentVersion>Run
C. Manually disable all startup tasks currently listed as enabled and reboot checking for issue resolution at startup
D. Open the Startup tab and methodically disable items currently listed as enabled and reboot, checking for issue resolution at each startup.
Answer: D
Explanation: This is the most effective way to selectively prevent programs from loading on a Windows 10 machine. The Startup tab can be accessed by opening Task Manager and then selecting the Startup tab.
From there, the technician can methodically disable items that are currently listed as enabled, reboot the machine, and check for issue resolution at each startup. If the issue persists, the technician can then move on to disabling the next item on the list.

Q43. - (Topic 1)
A technician has been tasked with using the fastest and most secure method of logging in to laptops. Which of the following log-in options meets these requirements?
A. PIN
B. Username and password
C. SSO
D. Fingerprint
Answer: D
Explanation: Here's why fingerprint authentication meets the requirements of both speed and security:

1. **Fast**:
    - **Convenience**: Fingerprint authentication is quick and convenient. It typically involves a single touch or swipe, allowing users to access their laptops rapidly without typing a password or PIN.
2. **Secure**:
    - **Biometric Security**: Fingerprints are unique to each individual, making them a strong form of biometric security. They are difficult to replicate or forge compared to traditional passwords or PINs.
    - **Less Vulnerable to Common Attacks**: Unlike passwords or PINs, which can be stolen or guessed, fingerprint data provides a higher level of security due to its uniqueness and the difficulty of duplication.

Here's a brief look at the other options:

- **A. PIN**:
    - **Speed**: PINs can be quick to enter, but they are less secure than biometric options because they can be guessed or stolen, especially if not combined with other security measures.
- **B. Username and password**:
    - **Security**: While secure if properly managed (e.g., using strong, unique passwords), usernames and passwords can be prone to attacks such as phishing, brute-force attacks, and credential theft.
    - **Speed**: Entering a username and password is generally slower compared to biometric authentication.
- **C. SSO (Single Sign-On)**:

- **Speed**: SSO can simplify the login process by allowing users to access multiple systems with a single login. However, SSO is typically used for accessing multiple applications rather than individual laptop logins.
- **Security**: SSO improves convenience but relies on the security of the single authentication method used. If the SSO system is compromised, it could impact access to multiple systems.

Q44. - (Topic 1)
As part of a CYOD policy a systems administrator needs to configure each user's Windows device to require a password when resuming from a period of sleep or inactivity. Which of the following paths will lead the administrator to the correct settings?
A. Use Settings to access Screensaver settings
B. Use Settings to access Screen Timeout settings
C. Use Settings to access General
D. Use Settings to access Display.
Answer: A
Explanation: The systems administrator should use Settings to access Screensaver settings to configure each user's Windows device to require a password when resuming from a period of sleep or inactivity1

Q45. - (Topic 1)
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

Q46. - (Topic 1)
A department has the following technical requirements for a new application:

Quad core processor
250gb HDD
6GB of RAM
Touchscreens

The company plans to upgrade from a 32-bit Windows OS to a 64-bit OS. Which of the following will the company be able to fully take advantage of after the upgrade?
A. CPU
B. Hard drive
C. RAM
D. Touch screen
Answer: C
Explanation: https://www.makeuseof.com/tag/difference-32-bit-64-bit-windows/
After upgrading from a 32-bit Windows OS to a 64-bit OS, the company will be able to fully take advantage of the RAM of the computer. This is because a 64-bit operating system is able to use larger amounts of RAM compared to a 32-bit operating system, which may benefit the system's overall performance if it has more than 4GB of RAM installed

Q47. - (Topic 1)
A company installed a new backup and recovery system. Which of the following types of backups should be completed FIRST?

A. Full
B. Non-parity
C. Differential
D. Incremental
Answer: A
Explanation: The type of backup that should be completed FIRST after installing a new backup and recovery system is a full backup. This is because a full backup is a complete backup of all data and is the foundation for all other backups. After a full backup is completed, other types of backups, such as differential and incremental backups, can be performed.

Q48. - (Topic 1)
Which of the following could be used to implement secure physical access to a data center?
A. Geofence
B. Alarm system
C. Badge reader
D. Motion sensor
Answer: C
Explanation: Badge readers are used to implement secure physical access to a data center. They are used to read the identification information on an employee's badge and grant access to the data center if the employee is authorized2.
This system requires individuals to have an access badge that contains their identification information or a unique code that can be scanned by a reader. After the badge is scanned, the system compares the information on the badge with the authorized personnel database to authenticate if the individual has the required clearance to enter that area. The other options listed, such as a geofence, alarm system, or motion sensor are security measures that may be used in conjunction with badge readers, but do not provide identification and authentication features.

Q49. - (Topic 1)
A technician has spent hours trying to resolve a computer issue for the company's Chief Executive Officer (CEO). The CEO needs the device returned as soon as possible. Which of the following steps should the technician take NEXT?
A. Continue researching the issue
B. Repeat the iterative processes
C. Inform the CEO the repair will take a couple of weeks
D. Escalate the ticket
Answer: D
Explanation: The technician should escalate the ticket to ensure that the CEO's device is returned as soon as possible1

Q50. - (Topic 1)
A call center technician receives a call from a user asking how to update Windows. Which of the following describes what the technician should do?
A. Have the user consider using an iPad if the user is unable to complete updates
B. Have the user text the user's password to the technician.
C. Ask the user to click in the Search field, type Check for Updates, and then press the Enter key
D. Advise the user to wait for an upcoming, automatic patch
Answer: C
Explanation: The technician should guide the user to update Windows through the built-in "Check for Updates" feature. This can be done by having the user click in the Search field, type "Check for Updates", and then press the Enter key. This will bring up the Windows Update function, which will search for any available updates and give the user the option to install them.

Q51. - (Topic 1)

A user reports a computer is running slow. Which of the following tools will help a technician identity the issued.
A. Disk Cleanup
B. Group Policy Editor
C. Disk Management
D. Resource Monitor
Answer: D
Explanation: Resource Monitor will help a technician identify the issue when a user reports a computer is running slow1

Q52. - (Topic 1)
The command cat comptia.txt was issued on a Linux terminal. Which of the following results should be expected?
A. The contents of the text comptia.txt will be replaced with a new blank document
B. The contents of the text comptia.txt would be displayed.
C. The contents of the text comptia.txt would be categorized in alphabetical order.
D. The contents of the text comptia.txt would be copied to another comptia.txt file
Answer: B
Explanation: The command cat cormptia.txt was issued on a Linux terminal. This command would display the contents of the text comptia.txt.

Q53. - (Topic 1)
A user corrects a laptop that is running Windows 10 to a docking station with external monitors when working at a desk. The user would like to close the laptop when it is docked, but the user reports it goes to sleep when it is closed. Which of the following is the BEST solution to prevent the laptop from going to sleep when it is closed and on the docking station?
A. Within the Power Options of the Control Panel utility click the Change Plan Settings button for the enabled power plan and select Put the Computer to Sleep under the Plugged-In category to Never
B. Within the Power Options of the Control Panel utility, click the Change Plan Settings button for the enabled power plan and select Put the Computer to Sleep under the On Battery category to Never
C. Within the Power Options of the Control Panel utility select the option Choose When to Turn Off the Display and select Turn Off the Display under the Plugged-In category to Never
D. Within the Power Options of the Control Panel utility, select the option Choose What Closing the Lid Does and select When I Close the Lid under the Plugged-in category to Do Nothing
Answer: D
Explanation: The laptop has an additional option under power and sleep settings that desktops do not have. Switching to do nothing prevents the screen from turning off when closed.

Q54. - (Topic 1)
During a recent flight an executive unexpectedly received several dog and cat pictures while trying to watch a movie via in-flight Wi-Fi on an iPhone. The executive has no records of any contacts sending pictures like these and has not seen these pictures before. To BEST resolve this issue, the executive should:
A. set AirDrop so that transfers are only accepted from known contacts
B. completely disable all wireless systems during the flight
C. discontinue using iMessage and only use secure communication applications
D. only allow messages and calls from saved contacts
Answer: A
Explanation: To best resolve this issue, the executive should set AirDrop so that transfers are only accepted from known contacts (option A). AirDrop is a feature on iOS devices that allows users to share files, photos, and other data between Apple devices. By setting AirDrop so that it only accepts transfers from known contacts, the executive can ensure that unwanted files and photos are not sent to their device.

Additionally, the executive should ensure that the AirDrop setting is only enabled when it is necessary, as this will protect their device from any unwanted files and photos.

Q55. - (Topic 1)
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.

Q56. - (Topic 1)
A user enabled a mobile device's screen lock function with pattern unlock. The user is concerned someone could access the mobile device by repeatedly attempting random patterns to unlock the device. Which of the following features BEST addresses the user's concern?
A. Remote wipe
B. Anti-malware
C. Device encryption
D. Failed login restrictions
Answer: A
Explanation: The feature that BEST addresses the user's concern is remote wipe. This is because remote wipe allows the user to erase all data on the mobile device if it is lost or stolen, which will prevent unauthorized access to the device1.

Q57. - (Topic 1)
Once weekly a user needs Linux to run a specific open-source application that is not available for the currently installed Windows platform. The user has limited bandwidth throughout the day. Which of the following solutions would be the MOST efficient, allowing for parallel execution of the Linux application and Windows applications?
A. Install and run Linux and the required application in a PaaS cloud environment
B. Install and run Linux and the required application as a virtual machine installed under the Windows OS
C. Use a swappable drive bay for the boot drive and install each OS with applications on its own drive Swap the drives as needed
D. Set up a dual boot system by selecting the option to install Linux alongside Windows
Answer: B
Explanation: The user should install and run Linux and the required application as a virtual machine installed under the Windows OS. This solution would allow for parallel execution of the Linux application and Windows applications2.
The MOST efficient solution that allows for parallel execution of the Linux application and Windows applications is to install and run Linux and the required application as a virtual machine installed under the Windows OS. This is because it allows you to run both Linux and Windows together without the need to keep the Linux portion confined to a VM window 3.

Q58. - (Topic 1)

A Chief Executive Officer has learned that an exploit has been identified on the web server software, and a patch is not available yet. Which of the following attacks MOST likely occurred?
A. Brute force
B. Zero day
C. Denial of service
D. On-path
Answer: B
Explanation: A zero-day attack is an attack that exploits a previously unknown vulnerability in a computer application, meaning that the attack occurs on “day zero” of awareness of the vulnerability
☞ Configuring AAA Services. Retrieved from
https://www.cisco.com/c/en/us/td/docs/routers/crs/software/crs_r4-0/security/configuration/guide/sc40crsb
ook_chapter1.html

Q59. - (Topic 1)
A user reports that text on the screen is too small. The user would like to make the text larger and easier to see. Which of the following is the BEST way for the user to increase the size of text, applications, and other items using the Windows 10 Settings tool?
A. Open Settings select Devices, select Display, and change the display resolution to a lower resolution option
B. Open Settings, select System, select Display, and change the display resolution to a lower resolution option.
C. Open Settings Select System, select Display, and change the Scale and layout setting to a higher percentage.
D. Open Settings select Personalization, select Display and change the Scale and layout setting to a higher percentage
Answer: C
Explanation: Open Settings, select System, select Display, and change the Scale and layout setting to a higher percentage123
Reference: 4. How to Increase the Text Size on Your Computer. Retrieved from https://www.laptopmag.com/articles/increase-text-size-computer 5. How to Change the Size of Text in
Windows 10. Retrieved from https://www.howtogeek.com/370055/how-tochange-the-size-of-text-in-windows-10/ 6. Change the size of text in Windows. Retrieved from https://support.microsoft.com/en-us/windows/change-the-size-of-text-in-windows-1d5830c3-eee3-8eaa-836b-abcc37d99b9a

Q60. - (Topic 1)
A technician is asked to resize a partition on the internal storage drive of a computer running macOS.
Which of the following tools should the technician use to accomplish this task?
A. Consoltf
B. Disk Utility
C. Time Machine
D. FileVault
Answer: B
Explanation: The technician should use Disk Utility to resize a partition on the internal storage drive of a
computer running macOS. Disk Utility is a built-in utility that allows users to manage disks, partitions, and volumes on a Mac. It can be used to resize, create, and delete partitions, as well as to format disks and
volumes.

Q61. - (Topic 1)
A user's smartphone data usage is well above average. The user suspects an installed application is transmitting data in the background. The user would like to be alerted when an application attempts to communicate with the internet. Which of the following BEST addresses the user's concern?
A. Operating system updates
B. Remote wipe
C. Antivirus
D. Firewall
Answer: D
Explanation: A firewall is a security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. In this scenario, the user is concerned about an installed application transmitting data in the background, so a firewall would be the best solution to address their concern. By installing and configuring a firewall, the user can block unauthorized connections to and from the device, and receive alerts whenever an application tries to access the internet.

Q62. - (Topic 1)
A technician needs to recommend the best backup method that will mitigate ransomware attacks. Only a few files are regularly modified, however, storage space is a concern. Which of the following backup methods would BEST address these concerns?
A. Full
B. Differential
C. Off-site
D. Grandfather-father-son
Answer: B
Explanation: The differential backup method would best address these concerns. Differential backups only back up files that have changed since the last full backup, which means that only a few files would be backed up each time. This would help to mitigate the risk of ransomware attacks, as only a few files would be affected if an attack occurred. Additionally, differential backups require less storage space than full
backups.

Q63. - (Topic 1)
A technician found that an employee is mining cryptocurrency on a work desktop. The company has decided that this action violates its guidelines. Which of the following should be updated to reflect this new
requirement?
A. MDM
B. EULA
C. IRP
D. AUP
Answer: D
Explanation: AUP (Acceptable Use Policy) should be updated to reflect this new requirement. The AUP is a document that outlines the acceptable use of technology within an organization. It is a set of rules that employees must follow when using company resources. The AUP should be updated to include a policy on
cryptocurrency mining on work desktops

Q64. - (Topic 1)
A user contacted the help desk to report pop-ups on a company workstation indicating the computer has been infected with 137 viruses and payment is needed to remove them. The user thought the company-provided antivirus software would prevent this issue. The help desk ticket states that the user only receives these messages when first opening the web browser. Which of the following

steps would MOST likely resolve the issue? (Select TWO)
A. Scan the computer with the company-provided antivirus software
B. Install a new hard drive and clone the user's drive to it
C. Deploy an ad-blocking extension to the browser.
D. Uninstall the company-provided antivirus software
E. Click the link in the messages to pay for virus removal
F. Perform a reset on the user's web browser
Answer: C,F
Explanation:
"The user thought the company-provided antivirus software would prevent this issue." The most likely steps to resolve the issue are to deploy an ad-blocking extension to the browser and perform a reset on the user's web browser. Ad-blocking extensions can help to prevent pop-ups and other unwanted content from appearing in the browser, and resetting the browser can help to remove any malicious extensions or
settings that may be causing the issue.

Q65. - (Topic 1)
A technician is setting up a desktop computer in a small office. The user will need to access files on a drive shared from another desktop on the network. Which of the following configurations should the technician employ to achieve this goal?
A. Configure the network as private
B. Enable a proxy server
C. Grant the network administrator role to the user
D. Create a shortcut to public documents
Answer: A
Explanation: The technician should configure the network as private to allow the user to access files on a drive shared from another desktop on the network1

Q66. - (Topic 1)
A wireless network is set up, but it is experiencing some interference from other nearby SSIDs. Which of the following can BEST resolve the interference?
A. Changing channels
B. Modifying the wireless security
C. Disabling the SSIO broadcast
D. Changing the access point name
Answer: A
Explanation: Changing channels can best resolve interference from other nearby SSIDs. Wireless networks operate on different channels, and changing the channel can help to avoid interference from other nearby networks.

Q67. - (Topic 1)
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.

Q68. - (Topic 1)
A technician is unable to join a Windows 10 laptop to a domain Which of the following is the MOST likely reason?
A. The domain's processor compatibility is not met
B. The laptop has Windows 10 Home installed
C. The laptop does not have an onboard Ethernet adapter
D. The Laptop does not have all current Windows updates installed
Answer: C
Explanation:
https://partners.comptia.org/docs/default-source/resources/comptia-a-220-1102-exam-objectives-(3-0)

Q69. - (Topic 1)
A technician needs to format a USB drive to transfer 20GB of data from a Linux computer to a Windows computer. Which of the following filesystems will the technician MOST likely use?
A. FAT32
B. ext4
C. NTFS
D. exFAT
Answer: D
Explanation: exFAT is a file system that is supported by both Linux and Windows and can handle large files1.

Q70. - (Topic 1)
A technician is installing new software on a macOS computer. Which of the following file types will the technician MOST likely use?
A. .deb
B. .vbs
C. .exe
D. .app
Answer: D
Explanation: The file type that the technician will MOST likely use when installing new software on a macOS computer is .app. This is because .app is the file extension for applications on macOS1.

Q71. - (Topic 1)
A user is configuring a new SOHO Wi-Fi router for the first time. Which of the following settings should the user change FIRST?
A. Encryption
B. Wi-Fi channel
C. Default passwords
D. Service set identifier
Answer: C
Explanation: the user should change the default passwords first when configuring a new SOHO Wi-Fi router1

Q72. - (Topic 1)
A user reports that the hard drive activity light on a Windows 10 desktop computer has been steadily lit for more than an hour, and performance is severely degraded. Which of the following tabs in Task Manager would contain the information a technician would use to identify the cause of this issue?
A. Services
B. Processes
C. Performance

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

Q73. - (Topic 1)
A technician installed a known-good, compatible motherboard on a new laptop. However, the motherboard is not working on the laptop. Which of the following should the technician MOST likely have done to prevent damage?
A. Removed all jewelry
B. Completed an inventory of tools before use
C. Practiced electrical fire safety
D. Connected a proper ESD strap
Answer: D
Explanation: The technician should have connected a proper ESD strap to prevent damage to the motherboard. ESD (electrostatic discharge) can cause damage to electronic components, and an ESD strap helps to prevent this by grounding the technician and preventing the buildup of static electricity.
Removing all jewelry is also a good practice, but it is not the most likely solution to this problem.

Q74. - (Topic 1)
A technician suspects a rootkit has been installed and needs to be removed. Which of the following would BEST resolve the issue?
A. Application updates
B. Anti-malware software
C. OS reinstallation
D. File restore
Answer: C
Explanation: If a rootkit has caused a deep infection, then the only way to remove the rootkit is to reinstall the operating system. This is because rootkits are designed to be difficult to detect and remove, and they can hide in the operating system's kernel, making it difficult to remove them without reinstalling the operating system
https://www.minitool.com/backup-tips/how-to-get-rid-of-rootkit-windows-10.html

Q76. - (Topic 1)
An Android user contacts the help desk because a company smartphone failed to complete a tethered OS update A technician determines there are no error messages on the device. Which of the following should the technician do NEXT?
A. Verify all third-party applications are disabled
B. Determine if the device has adequate storage available.
C. Check if the battery is sufficiently charged
D. Confirm a strong internet connection is available using Wi-Fi or cellular data
Answer: C
Explanation: Since there are no error messages on the device, the technician should check if the battery is sufficiently charge1. If the battery is low, the device may not have enough power to complete the update. In this scenario, the technician has already determined that there are no error messages on the device. The next best step would be to check if the battery is sufficiently charged. If the battery is low, it could be preventing the device from completing the update process. Verifying that third-party applications are disabled, determining if the device has adequate storage available,

and confirming a strong internet connection are all important steps in troubleshooting issues with mobile devices. However, since the problem in this scenario is related to a failed OS update, it is important to first check the battery level before
proceeding with further troubleshooting steps.

Q77. - (Topic 1)
Which of the following OS types provides a lightweight option for workstations that need an easy-to-use browser-based interface?
A. FreeBSD
B. Chrome OS
C. macOS
D. Windows
Answer: B
Explanation: Chrome OS provides a lightweight option for workstations that need an easy- to-use browser-based interface1

Q78. - (Topic 1)
An organization is centralizing support functions and requires the ability to support a remote user's desktop.
Which of the following technologies will allow a technician to see the issue along with the user?
A. RDP
B. VNC
C. SSH
D. VPN
Answer: B
Explanation: VNC will allow a technician to see the issue along with the user when an organization is centralizing support functions and requires the ability to support a remote user’s desktop1

Q79. - (Topic 1)
When a user calls in to report an issue, a technician submits a ticket on the user's behalf. Which of the following practices should the technician use to make sure the ticket is associated with the correct user?
A. Have the user provide a callback phone number to be added to the ticket
B. Assign the ticket to the department's power user
C. Register the ticket with a unique user identifier
D. Provide the user with a unique ticket number that can be referenced on subsequent calls.
Answer: D
Explanation: The technician should provide the user with a unique ticket number that can be referenced on subsequent calls to make sure the ticket is associated with the correct user. This is because registering the ticket with a unique user identifier, having the user provide a callback phone number to be added to the ticket, or assigning the ticket to the department’s power user will not ensure that the ticket is associated with the correct user2.

Q80. - (Topic 1)
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: A,B
Explanation: **Here's why these are the best choices:**

1. **Utilizing an ESD strap**:
    - **Prevents Electrostatic Discharge (ESD)**: An Electrostatic Discharge (ESD) strap, or antistatic wrist strap, is crucial for protecting sensitive electronic components from static electricity, which can damage internal parts such as the processor. By grounding yourself through the strap, you minimize the risk of static discharge during the installation.
2. **Disconnecting the computer from the power source**:
    - **Prevents Electrical Shock**: Ensuring the computer is unplugged from the power source prevents the risk of electrical shock and reduces the chance of short circuits while working inside the computer. This step is essential for both safety and protecting the computer's components.

Other options and their relevance:

- **C. Placing the PSU in an antistatic bag**:
    - **Not Essential for Processor Replacement**: The power supply unit (PSU) generally does not need to be removed or placed in an antistatic bag for a processor replacement. This step is more relevant for shipping or storing the PSU.
- **D. Ensuring proper ventilation**:
    - **Not Directly Related**: While proper ventilation is important for overall system cooling and longevity, it does not directly protect the internal components during the installation of a new processor.
- **E. Removing dust from the ventilation fans**:
    - **Good Practice but Not Directly Related**: Removing dust is good practice for maintaining a clean environment inside the computer but does not directly protect components during the processor replacement process.
- **F. Ensuring equipment is grounded**:
    - **Part of ESD Protection**: While ensuring equipment is grounded is related to ESD protection, using an ESD strap (option A) is a more direct and specific method for personal grounding during work. The grounding of the equipment itself is more about preventing damage to the computer's power supply or case.

Q81. - (Topic 1)
A user reports a PC is running slowly. The technician suspects it has a badly fragmented hard drive. Which of the following tools should the technician use?
A. resmon.exe
B. msconfig.exe
C. dfrgui.exe
D. msmfo32.exe
Answer: C
Explanation: The technician should use dfrgui.exe to defragment the hard drive1

Q82. - (Topic 1)
A user is unable to use any internet-related functions on a smartphone when it is not connected to Wi-Fi. When the smartphone is connected to Wi-Fi the user can browse the internet and send and receive email.
The user is also able to send and receive text messages and phone calls when the smartphone is not connected to Wi-Fi. Which of the following is the MOST likely reason the user is unable to use the internet on the smartphone when it is not connected to Wi-Fi?
A. The smartphone's line was not provisioned with a data plan
B. The smartphone's SIM card has failed
C. The smartphone's Bluetooth radio is disabled.

D. The smartphone has too many applications open
Answer: A
Explanation: The smartphone's line was not provisioned with a data plan. The user is unable to use any internet-related functions on the smartphone when it is not connected to Wi-Fi because the smartphone's line was not provisioned with a data plan. The user can send and receive text messages and phone calls when the smartphone is not connected to Wi-Fi because these functions do not require an internet connection1

Q83. - (Topic 1)
A help desk technician is troubleshooting a workstation in a SOHO environment that is running above normal system baselines. The technician discovers an unknown executable with a random string name running on the system. The technician terminates the process, and the system returns to normal operation. The technician thinks the issue was an infected file, but the antivirus is not detecting a threat. The technician is concerned other machines may be infected with this unknown virus. Which of the following is the MOST effective way to check other machines on the network for this unknown threat?
A. Run a startup script that removes files by name.
B. Provide a sample to the antivirus vendor.
C. Manually check each machine.
D. Monitor outbound network traffic.
Answer: C
Explanation: The most effective way to check other machines on the network for this unknown threat is to manually check each machine. This can help to identify any other machines that may be infected with the unknown virus and allow them to be cleaned.

Q84. - (Topic 1)
A customer reported that a home PC with Windows 10 installed in the default configuration is having issues loading applications after a reboot occurred in the middle of the night. Which of the following is the FIRST step in troubleshooting?
A. Install alternate open-source software in place of the applications with issues
B. Run both CPU and memory tests to ensure that all hardware functionality is normal
C. Check for any installed patches and roll them back one at a time until the issue is resolved
D. Reformat the hard drive, and then reinstall the newest Windows 10 release and all applications.
Answer: C
Explanation: The first step in troubleshooting is to check for any installed patches and roll them back one at a time until the issue is resolved. This can help to identify any patches that may be causing the issue and allow them to be removed.

Q85. - (Topic 1)
A technician is configuring a SOHO device Company policy dictates that static IP addresses cannot be used. The company wants the server to maintain the same IP address at all times. Which of the following should the technician use?
A. DHCP reservation
B. Port forwarding
C. DNS A record
D. NAT
Answer: A
Explanation: The technician should use DHCP reservation to maintain the same IP address for the server at all times. DHCP reservation allows the server to obtain an IP address dynamically from the DHCP server, while ensuring that the same IP address is assigned to the server each time it requests an IP address.

Q86. - (Topic 1)

Following the latest Windows update PDF files are opening in Microsoft Edge instead of Adobe Reader. Which of the following utilities should be used to ensure all PDF files open in Adobe Reader?
A. Network and Sharing Center
B. Programs and Features
C. Default Apps
D. Add or Remove Programs
Answer: C
Explanation: Default Apps should be used to ensure all PDF files open in Adobe Reader1

Q87. - (Topic 1)
A technician at a customer site is troubleshooting a laptop. A software update needs to be downloaded but the company's proxy is blocking traffic to the update site. Which of the following should the technician perform?
A. Change the DNS address to 1.1.1.1
B. Update Group Policy
C. Add the site to the client's exceptions list
D. Verity the software license is current.
Answer: C
Explanation: The technician should add the update site to the client’s exceptions list to bypass the proxy.
This can be done through the client’s web browser settings, where the proxy settings can be configured. By adding the update site to the exceptions list, the client will be able to access the site and download the software update.

Q88. - (Topic 1)
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.

Q89. - (Topic 1)
A technician needs to interconnect two offices to the main branch while complying with good practices and security standards. Which of the following should the technician implement?
A. MSRA
B. VNC
C. VPN
D. SSH
Answer: C
Explanation: A technician needs to interconnect two offices to the main branch while complying with good practices and security standards. The technician should implement VPN

Q90. - (Topic 1)

A technician needs to exclude an application folder from being cataloged by a Windows 10 search. Which of the following utilities should be used?
A. Privacy
B. Indexing Options
C. System
D. Device Manager
Answer: B
Explanation: To exclude an application folder from being cataloged by a Windows 10 search, the technician should use the Indexing Options uti1lity