220-1102$^{\text{Q\&As}}$

CompTIA A+ Certification Exam: Core 2

Pass CompTIA 220-1102 Exam with 100% Guarantee

QUESTION 1

Which of the following common security vulnerabilities can be mitigated by using put validation?

A. Brute-force attack

B. Cross-site scripting

C. SQL injection

D. Cross-site request forgery

Correct Answer: C

Put is the same as applying data, probably short for input. SQL injections often happen when a specific code injection on a page, program, or directory has not been patched out, allowing for attacker to use code to interject a new line to receive a yes to let them access, or manipulate page they are on. https://support.microsoft.com/en-us/office/apply-data-validation-to-cells-29fecbcc-d1b9-42c1-9d76-eff3ce5f7249

QUESTION 2

A user\\'s Windows desktop has low disk space. A technician thinks some upgrade files were never removed. Which of the following tools should the technician use to correct the issue?

A. devmgmt.msc

B. cleanmgr.exe

C. dfrgui.exe

D. diskmgmt.mac

Correct Answer: B

The correct tool to use for removing upgrade files and freeing up disk space on a Windows desktop is cleanmgr.exe, which stands for Disk Cleanup. Disk Cleanup is a maintenance utility included in Microsoft Windows designed to free up disk space on a computer\\'s hard drive. The utility scans and analyzes the hard drive for files that are no longer of any use, and then removes the unnecessary files. It can delete temporary files, system files, empty the Recycle Bin, and remove a variety of system files and other items that you might no longer need.

QUESTION 3

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

A. Delete the application\\'s cache.

B. Check for application updates.

C. Roll back the OS update.

D. Uninstall and reinstall the application.

Correct Answer: B

Sometimes, an OS update can cause compatibility issues with some applications that are not optimized for the new version of the OS. To fix this, the user should check if there are any updates available for the application that can resolve the

issue. The user can check for application updates by following these steps:

On an Android device, open the Google Play Store app and tap on the menu icon in the top left corner. Then tap on My apps and games and look for any updates available for the application. If there is an update, tap on Update to install it. On

an iOS device, open the App Store app and tap on the Updates tab at the bottom. Then look for any updates available for the application. If there is an update, tap on Update to install it.

QUESTION 4

A technician needs to configure security settings on a Windows 10 workstation. Which of the following should the technician configure to limit password attempts?

A. Account Lockout Policy

B. User Access Control

C. System Protection

D. Firewall

Correct Answer: A

Configuring the Account Lockout Policy in Windows 10 is the appropriate action to limit password attempts. This security setting determines the number of failed login attempts that will trigger a lockout, preventing unauthorized access due to repeated password guessing. It is an effective measure to enhance security by deterring brute-force attacks.

QUESTION 5

A client wants a technician to set up a proxy server in a branch office to manage internet access. This involves configuring the workstations to use the new proxy server. Which of the following Internet Options tabs in Control Panel would be most appropriate for the technician to use to configure the settings?

A. Privacy

B. Advanced

C. Content

D. Connections

E. Security

Correct Answer: D

The Connections tab in Internet Options allows the technician to configure the proxy server settings for the workstations. The technician can enter the proxy server address and port number, and specify which websites to bypass the proxy server for. The other tabs are not relevant for configuring the proxy server settings. References: CompTIA A+ Certification ore 2 Objectives, page 9, section 1.7; CompTIA A+ Core 2 (220- 1102) Certification Study Guide, page 140, section 1.7.

QUESTION 6

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

Correct Answer: C

The process of documenting who had possession of evidence at every step of the process is called chain of custody

QUESTION 7

Which of the following is the proper way for a technician to dispose of used printer consumables?

A. Proceed with the custom manufacturer\\'s procedure.

B. Proceed with the disposal of consumables in standard trash receptacles.

C. Empty any residual ink or toner from consumables before disposing of them in a standard recycling bin.

D. Proceed with the disposal of consumables in standard recycling bins.

Correct Answer: A

When it comes to disposing of used printer consumables , it is important to follow the manufacturer\\'s instructions or guidelines for proper disposal, as different types of consumables may require different disposal procedures. Some manufacturers provide specific instructions for proper disposal, such as sending the used consumables back to the manufacturer or using special recycling programs. Therefore, the proper way for a technician to dispose of used printer consumables is to proceed with the custom manufacturer\\'s procedure , if provided. This option ensures that the disposal is handled in an environmentally friendly and safe manner.

QUESTION 8

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

A. Use a key combination to lock the computer when leaving.

B. Ensure no unauthorized personnel are in the area.

C. Configure a screensaver to lock the computer automatically after approximately 30 minutes of inactivity.

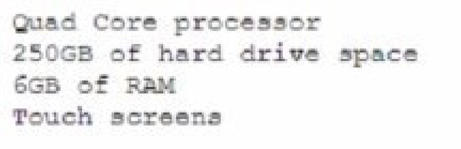
D. Turn off the monitor to prevent unauthorized visibility of information.

Correct Answer: A

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

QUESTION 9

A department has the following technical requirements for a new application:



```
Quad Core processor
250GB of hard drive space
6GB of RAM
Touch screens
```

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

Correct Answer: C

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

QUESTION 10

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.

Correct Answer: B

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.

QUESTION 11

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

Correct Answer: B

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

QUESTION 12

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

A. Signed system images

B. Antivirus

C. SSO

D. MDM

Correct Answer: D

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

QUESTION 13

Which of the following is the STRONGEST wireless configuration?

A. WPS

B. WPA3

C. WEP

D. WMN

Correct Answer: B

The strongest wireless configuration is B. WPA3. WPA3 is the most up-to-date wireless encryption protocol and is the most secure choice. It replaces PSK with SAE, a more secure way to do the initial key exchange. At the same time, the session key size of WPA3 increases to 128-bit in WPA3-Personal mode and 192-bit in WPA3-Enterprise, which makes the password harder to crack than the previous Wi-Fi security standards https://www.makeuseof.com/tag/wep-wpa-wpa2wpa3-explained/

QUESTION 14

A user calls the help desk and reports a workstation is infected with malicious software. Which of the following tools should the help desk technician use to remove the malicious software? (Choose two.)

A. Local Network Connection

B. User Account Control

C. Windows Backup and Restore

D. Windows Firewall

E. Windows Defender

F. Network Packet Analyzer

Correct Answer: EF

E. Windows Defender: Windows Defender is a built-in antivirus and antimalware solution in Windows operating systems. It can scan the system for malicious software and attempt to remove or quarantine it.

F. Network Packet Analyzer: A network packet analyzer, also known as a network sniffer or packet capture tool, allows the technician to capture and inspect network traffic. This tool can help identify any suspicious or malicious network activity that may be related to the infection.

It\\'s important to note that the other options (A. Local Network Connection, B. User Account Control, C. Windows Backup and Restore, and D. Windows Firewall) are not directly related to removing malicious software from a workstation. Instead, they pertain to network connectivity, security permissions, data backup and recovery, and network traffic filtering, respectively.

QUESTION 15

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

A. Biometrics

B. Soft token

C. Access control lists

D. Smart card

Correct Answer: B