220-1102 Q&As

CompTIA A+ Certification Exam: Core 2

Pass CompTIA 220-1102 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/220-1102.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

QUESTION 1

Which of the following operating systems can allow users to have access to the source code, can host various server applications, and can be command line only?

A. Windows

B. macOS

C. Linux

D. Chrome OS

Correct Answer: C

QUESTION 2

Users access files in the department share. When a user creates a new subfolder, only that user can access the folder and its files. Which of the following will MOST likely allow all users to access the new folders?

A. Assigning share permissions

B. Enabling inheritance

C. Requiring multifactor authentication

D. Removing archive attribute

Correct Answer: B

QUESTION 3

Sensitive data was leaked from a user\\'s smartphone. A technician discovered an unapproved application was installed, and the user has full access to the device\\'s command shell.

Which of the following is the NEXT step the technician should take to find the cause of the leaked data?

A. Restore the device to factory settings.

B. Uninstall the unapproved application.

C. Disable the ability to install applications from unknown sources.

D. Ensure the device is connected to the corporate WiFi network.

Correct Answer: B

The technician should disable the user\\'s access to the device\\'s command shell. This will prevent the user from accessing sensitive data and will help to prevent further data leaks. The technician should then investigate the unapproved application to determine if it is the cause of the data leak. If the application is found to be the cause of the leak, the technician should uninstall the application and restore the device to factory settings. If the application is not the

cause of the leak, the technician should investigate further to determine the cause of the leak. Disabling the ability to install applications from unknown sources can help to prevent future data leaks, but it is not the next step the technician should take in this scenario. Ensuring the device is connected to the corporate WiFi network is not relevant to this scenario

QUESTION 4

A user is trying to use a third-party USB adapter but is experiencing connection issues. Which of the following tools should the technician use to resolve this issue?

A. taskschd.msc

B. eventvwr.msc

C. de vmgmt. msc

D. diskmgmt.msc

Correct Answer: C

The tool that the technician should use to resolve the connection issues with the third-party USB adapter is devmgmt.msc. Devmgmt.msc is a command that opens the Device Manager, which is a utility that allows users to view and manage the hardware devices and drivers installed on a computer. The technician can use the Device Manager to check the status, properties and compatibility of the USB adapter and its driver, and perform actions such as updating, uninstalling or reinstalling the driver, enabling or disabling the device, or scanning for hardware changes. Taskschd.msc is a command that opens the Task Scheduler, which is a utility that allows users to create and manage tasks that run automatically at specified times or events. The Task Scheduler is not relevant or useful for resolving connection issues with the USB adapter. Eventvwr.msc is a command that opens the Event Viewer, which is a utility that allows users to view and monitor the system logs and events. The Event Viewer may provide some information or clues about the connection issues with the USB adapter, but it does not allow users to manage or troubleshoot the device or its driver directly. Diskmgmt.msc is a command that opens the Disk Management, which is a utility that allows users to view and manage the disk drives and partitions on a computer. The Disk Management is not relevant or useful for resolving connection issues with the USB adapter. References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.6

QUESTION 5

A technician receives a call from a user who is on vacation. The user provides the necessary credentials and asks the technician to log in to the users account and read a critical email that the user has been expecting. The technician refuses because this is a violation of the:

A. acceptable use policy.

B. regulatory compliance requirements.

C. non-disclosure agreement

D. incident response procedures

Correct Answer: A

Logging into a user\\'s account without their explicit permission is a violation of the acceptable use policy, which outlines the rules and regulations by which a user must abide while using a computer system. By logging into the user\\'s

account without their permission, the technician would be violating this policy. Additionally, this action could be seen as a breach of confidentiality, as the technician would have access to information that should remain confidential.

QUESTION 6

Which of the following should be used to secure a device from known exploits?

A. Encryption

B. Remote wipe

C. Operating system updates

D. Cross-site scripting

Correct Answer: C

Operating system updates are used to secure a device from known exploits. Operating system updates are patches or fixes that are released by the vendor to address security vulnerabilities, bugs, or performance issues. Operating system updates can also provide new features or enhancements to the device. It is important to keep the operating system updated to prevent attackers from exploiting known flaws or weaknesses.

QUESTION 7

Which of the following defines the extent of a change?

A. Scope

B. Purpose

C. Analysis

D. Impact

Correct Answer: A

The term that defines the extent of a change is scope. Scope is a measure of the size, scale and boundaries of a project or an activity. Scope defines what is included and excluded in the project or activity, such as goals, requirements, deliverables, tasks and resources. Scope helps determine the feasibility, duration and cost of the project or activity. Scope also helps manage the expectations and needs of the stakeholders involved in the project or activity. Purpose is the reason or objective for doing a project or an activity. Purpose defines why the project or activity is important or necessary, such as solving a problem, meeting a need or achieving a goal. Purpose helps provide direction, motivation and justification for the project or activity. Analysis is the process of examining, evaluating and interpreting data or information related to a project or an activity. Analysis helps identify, understand and prioritize issues, risks, opportunities and solutions for the project or activity. Impact is the effect or outcome of a project or an activity on something or someone else. Impact defines how the project or activity affects or influences other factors, such as performance, quality, satisfaction or value. Impact helps measure the success and effectiveness of the project or activity. References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 5.2

QUESTION 8

A user\\'s system is infected with malware. A technician updates the anti-malware software and runs a scan that removes the malware. After the user reboots the system, it once again becomes infected with malware.

Which of the following will MOST likely help to permanently remove the malware?

A. Enabling System Restore

B. Educating the user

C. Booting into safe mode

D. Scheduling a scan

Correct Answer: B

Although updating the anti-malware software and running scans are important steps in removing malware, they may not be sufficient to permanently remove the malware if the user keeps engaging in behaviors that leave the system vulnerable, such as downloading unknown files or visiting malicious websites. Therefore, educating the user on safe computing practices is the best way to prevent future infections and permanently remove the malware. Enabling System Restore, Booting into safe mode, and scheduling a scan are not the most efficient ways to permanently remove the malware. Enabling System Restore and Booting into safe mode may help in some cases, but they may not be sufficient to permanently remove the malware. Scheduling a scan is also important for detecting and removing malware, but it may not be sufficient to prevent future infections.

https://partners.comptia.org/docs/default-source/resources/comptia-a-220-1102-exam-objectives-(3-0)

QUESTION 9

A server administrator, Anne, has set up a new server on the company\\'s network to provide centralized user and access management. The file permissions on the server have been shared over the network based on user groups divided into departments and do not have administrative rights. This practice is called which of the following?

A. Logical separation of data

B. User segregation

C. Administrative overhead

D. Principle of least privilege

Correct Answer: D

QUESTION 10

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.

Correct Answer: C

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.

QUESTION 11

A user states that they see a warning on their screen about an IP conflict. Which of the following is MOST likely the cause?

A. A static IP address is assigned to the workstation

B. A bad router

C. A bad switch

D. The computer is getting an APIPA address

Correct Answer: A

QUESTION 12

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

Correct Answer: C

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

QUESTION 13

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

Correct Answer: A

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

QUESTION 14

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.

Correct Answer: D

First thing you want to do is quarantine/disconnect the affected system from the network so whatever malicious software doesn\\'t spread.

QUESTION 15

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.

Correct Answer: A

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