SY0-701 Q&As

CompTIA Security+ 2024

Pass CompTIA SY0-701 Exam with 100% Guarantee

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

https://www.geekcert.com/sy0-701.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Which of the following enables the use of an input field to run commands that can view or manipulate data?

A. Cross-site scripting

B. Side loading

C. Buffer overflow

D. SQL injection

Correct Answer: D

SQL injection is a type of attack that enables the use of an input field to run commands that can view or manipulate data in a database. SQL stands for Structured Query Language, which is a language used to communicate with databases.

By injecting malicious SQL statements into an input field, an attacker can bypass authentication, access sensitive information, modify or delete data, or execute commands on the server. SQL injection is one of the most common and

dangerous web application vulnerabilities.

References: CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 5, page 195. CompTIA Security+ SY0-701 Exam Objectives, Domain 1.1, page 8.

QUESTION 2

Which of the following would be most useful in determining whether the long-term cost to transfer a risk is less than the impact of the risk?

A. ARO

B. RTO

C. RPO

D. ALE

E. SLE

Correct Answer: D

QUESTION 3

Which of the following control types is AUP an example of?

A. Physical

B. Managerial

C. Technical

D. Operational

Correct Answer: B

An Acceptable Use Policy (AUP) is an example of a managerial control. Managerial controls are policies and procedures that govern an organization\\'s operations, ensuring security through directives and rules. The AUP defines acceptable behavior and usage of company resources, setting guidelines for employees. Physical controls refer to security measures like locks, fences, or security guards. Technical controls involve security mechanisms such as firewalls or encryption. Operational controls are procedures for maintaining security, such as backup and recovery plans.

QUESTION 4

An administrator needs to perform server hardening before deployment. Which of the following steps should the administrator take? (Select two).

A. Disable default accounts.

B. Add the server to the asset inventory.

C. Remove unnecessary services.

D. Document default passwords.

E. Send server logs to the SIEM.

F. Join the server to the corporate domain.

Correct Answer: AC

To perform server hardening before deployment, the administrator should disable default accounts and remove unnecessary services. These steps are crucial to reducing the attack surface and enhancing the security of the server. Disable

default accounts: Default accounts often come with default credentials that are well-known and can be exploited by attackers. Disabling these accounts helps prevent unauthorized access. Remove unnecessary services: Unnecessary

services can introduce vulnerabilities and be exploited by attackers. Removing them reduces the number of potential attack vectors.

Add the server to the asset inventory: Important for tracking and management but not directly related to hardening.

Document default passwords: Documentation is useful, but changing or disabling default passwords is the hardening step.

Send server logs to the SIEM: Useful for monitoring and analysis but not a direct hardening step.

Join the server to the corporate domain: Part of integration into the network but not specific to hardening.

Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 1.1 - Compare and contrast various types of security controls (Server hardening).

QUESTION 5

Since a recent upgrade to a WLAN infrastructure, several mobile users have been unable to access the internet from the lobby. The networking team performs a heat map survey of the building and finds several WAPs in the area. The WAPs are using similar frequencies with high power settings. Which of the following installation considerations should the security team evaluate next?

A. Channel overlap

B. Encryption type

C. New WLAN deployment

D. WAP placement

Correct Answer: A

When multiple Wireless Access Points (WAPs) are using similar frequencies with high power settings, it can cause channel overlap, leading to interference and connectivity issues. This is likely the reason why mobile users are unable to access the internet in the lobby. Evaluating and adjusting the channel settings on the WAPs to avoid overlap is crucial to resolving the connectivity problems. References: CompTIA Security+ SY0-701 study materials, particularly the domain on Wireless and Mobile Security, which covers WLAN deployment considerations.