SY0-601 Q&As

CompTIA Security+

Pass CompTIA SY0-601 Exam with 100% Guarantee

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

https://www.passapply.com/sy0-601.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

After a phishing scam for 9 user\\'s credentals, the red team was able to craft a payload to deploy on @ server. The attack allowed the installaton of malicious software that intiates @ new remote session.

Which of the following types of attacks has occurred?

A. Privilege escalation

B. Session replay

C. Application programming interface

D. Directory traversal

Correct Answer: A

Privilege escalation DOES NOT always mean you are escalating to elevated permissions. Privilege escalations can also be horiztonal movements. In this case, the red team compromises a user\\'s account through the phising attack. The red team then deploys payload on the server through the comprised user account. The malware then initiates a new remote session, enabling the hackers to access the server directly. The comprised account is User A and the red team directly connected as a result of the malware can be thought of as User B. In this case, privilege escalation refers to user B being able to access user A resources.

QUESTION 2

Which of the following ensures an organization can continue to do business with minimal interruption in the event of a major disaster?

A. Business recovery plan

B. Incident response plan

C. Communication plan

D. Continuity of operations plan

Correct Answer: D

COOP is similar to BCP, but a federal initiative that intends to encourage organizations to address how critical operations will continue under a broad range of negative circumstances. it addresses emergencies from all hazard approach instead of focusing on a specific event.

QUESTION 3

The manager who is responsible for a data set has asked a security engineer to apply encryption to the data on a hard disk. The security engineer is an example of a:

A. data controller.

B. data owner

C. data custodian.

D. data processor

Correct Answer: C

From the official CompTIA Security+ Study Guide glossary:

data custodian - An individual who is responsible for managing the system on which data assets are stored, including being responsible for enforcing access control, encryption, and backup/recovery measures.

QUESTION 4

An organization that is located in a flood zone is MOST likely to document the concerns associated with the restoration of IT operation in a:

A. business continuity plan

B. communications plan.

C. disaster recovery plan.

D. continuity of operations plan

Correct Answer: C

A disaster recovery plan (DRP) is a documented and structured approach that outlines the processes and procedures to recover and restore IT systems and operations after a disruptive event, such as a flood or other disaster In the flood zone, a disaster recovery plan would address the specific concerns and considerations related to the restoration of IT operations after a flood. While a business continuity plan (Option A) is closely related to a disaster recovery plan, it typically has a broader scope and encompasses the overall strategies and actions to ensure the continuity of business operations in the face of various disruptions including floods. Option B focuses on establishing effective communication channels during emergencies. A continuity of operations plan (Option D) is generally associated with government agencies and outlines procedures to ensure the continuous performance of essential functions during a wide range of emergencies.

QUESTION 5

A financial institution recently joined a bug bounty program to identify security issues in the institution\\'s new public platform. Which of the following best describes who the institution is working with to identify security issues?

A. Script kiddie

B. Insider threats

C. Malicious actor

D. Authorized hacker

Correct Answer: D

An authorized hacker, also known as an ethical hacker or a white hat hacker, is someone who uses their skills and knowledge to find and report security issues in a system or application with the permission of the owner. An authorized

hacker follows the rules and guidelines of the bug bounty program and does not cause any harm or damage to the system or its users.