CS0-002 Q&As

CompTIA Cybersecurity Analyst (CySA+)

Pass CompTIA CS0-002 Exam with 100% Guarantee

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

https://www.leads4pass.com/cs0-002.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

A security analyst was asked to join an outage call for a critical web application. The web middleware support team determined the web server is running and having no trouble processing requests; however, some investigation has revealed firewall denies to the web server that began around 1.00 a.m. that morning. An emergency change was made to enable the access, but management has asked for a root cause determination. Which of the following would be the BEST next step?

A. Install a packet analyzer near the web server to capture sample traffic to find anomalies.

B. Block all traffic to the web server with an ACL.

C. Use a port scanner to determine all listening ports on the web server.

D. Search the logging servers for any rule changes.

Correct Answer: D

QUESTION 2

A security team identified some specific known tactics and techniques to help mitigate repeated credential access threats, such as account manipulation and brute forcing. Which of the following frameworks or models did the security team MOST likely use to identify the tactics and techniques?

A. MITRE ATTandCK

B. ITIL

C. Kill chain

D. Diamond Model of Intrusion Analysis

Correct Answer: A

Reference: https://attack.mitre.org/techniques/T1110/

QUESTION 3

Management would like to make changes to the company\\'s infrastructure following a recent incident in which a malicious insider was able to pivot to another workstation that had access to the server environment. Which of the following controls would work BEST to prevent this type of event from reoccurring?

A. EDR

B. DLP

C. NAC

D. IPS

Correct Answer: B

QUESTION 4

A small electronics company decides to use a contractor to assist with the development of a new FPGA- based device. Several of the development phases will occur off-site at the contractor\\'s labs.

Which of the following is the main concern a security analyst should have with this arrangement?

A. Making multiple trips between development sites increases the chance of physical damage to the FPGAs.

B. Moving the FPGAs between development sites will lessen the time that is available for security testing.

C. Development phases occurring at multiple sites may produce change management issues.

D. FPGA applications are easily cloned, increasing the possibility of intellectual property theft.

Correct Answer: D

Reference: https://www.eetimes.com/how-to-protect-intellectual-property-in-fpgas-devices-part-1/#

QUESTION 5

Which of the following organizational initiatives would be MOST impacted by data severighty issues?

A. Moving to a cloud-based environment

B. Migrating to locally hosted virtual servers

C. Implementing non-repudiation controls

D. Encrypting local database queries

Correct Answer: A