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.pass2lead.com/cs0-002.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 command line utilities would an analyst use on an end-user PC to determine the ports it is listening on?

A. tracert

B. ping

C. nslookup

D. netstat

Correct Answer: D

QUESTION 2

A customer notifies a security analyst that a web application is vulnerable to information disclosure The analyst needs to indicate the seventy of the vulnerability based on its CVSS score, which the analyst needs to calculate When analyzing the vulnerability the analyst realizes that tor the attack to be successful, the Tomcat configuration file must be modified.

Which of the following values should the security analyst choose when evaluating the CVSS score?

A. Network

B. Physical

C. Adjacent

D. Local

Correct Answer: D

QUESTION 3

A small business does not have enough staff in the accounting department to segregate duties. The controller writes the checks for the business and reconciles them against the ledger. To ensure there is no fraud occurring, the business conducts quarterly reviews in which a different officer in the business compares all the cleared checks against the ledger. Which of the following BEST describes this type of control?

A. Deterrent

B. Preventive

C. Compensating

D. Detective

Correct Answer: C

A compensating control, also called an alternative control, is a mechanism that is put in place to satisfy the requirement for a security measure that is deemed too difficult or impractical to implement at the present time. "Compensating controls are additional security measures that you take to address a vulnerability without remediating the underlying issue."

QUESTION 4

The Chief Information Security Officer (CISO) asks a security analyst to write a new SIEM search rule to determine if any credit card numbers are being written to log files. The CISO and security analyst suspect the following log snippet contains real customer card data:

```
RecordError - dumping affected entry:
CustomerName: John Doe
Card1RawString: 0413555577814399
Card2RawString: 0444719465780100
CVV: not-stored
CustomerID: 1234-5678
```

Which of the following expressions would find potential credit card numbers in a format that matches the log snippet?

A. ^[0-9](16)$

B. (0-9) x 16

C. "1234-5678"

D. "04*"

Correct Answer: A

QUESTION 5

An analyst is responding to an incident within a cloud infrastructure Based on the logs and traffic analysis, the analyst thinks a container has been compromised.

Which of the following should Ihe analyst do FIRST?

A. Perform threat hunting in other areas of the cloud infrastructure

B. Contact law enforcement to report the incident

C. Perform a root cause analysis on the container and the service logs

D. Isolate the container from production using a predefined policy template

Correct Answer: D

Latest CS0-002 Dumps CS0-002 PDF Dumps CS0-002 Braindumps