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 cybersecurity analyst is dissecting an intrusion down to the specific techniques and wants to organize them in a logical manner. Which of the following frameworks would BEST apply in this situation?

A. Pyramid of Pain

B. MITRE ATTandCK

C. Diamond Model of Intrusion Analysts

D. CVSS v3.0

Correct Answer: B

QUESTION 2

While preparing for a third-party audit, the vice president of risk management and the vice president of information technology have stipulated that the vendor may not use offensive software during the audit. This is an example of:

A. organizational control.

B. service-level agreement.

C. rules of engagement.

D. risk appetite

Correct Answer: C

QUESTION 3

In SIEM software, a security analysis selected some changes to hash signatures from monitored files during the night followed by SMB brute-force attacks against the file servers.

Based on this behavior, which of the following actions should be taken FIRST to prevent a more serious compromise?

A. Fully segregate the affected servers physically in a network segment, apart from the production network.

B. Collect the network traffic during the day to understand if the same activity is also occurring during business hours

C. Check the hash signatures, comparing them with malware databases to verify if the files are infected.

D. Collect all the files that have changed and compare them with the previous baseline

Correct Answer: A

QUESTION 4

An organization has a policy prohibiting remote administration of servers where web services are running. One of the Nmap scans is shown here:

```
Starting Nmap 4.67 (http://nmap.org) at 2011-11-03 18:32 EDT
Nmap scan report for 192.168.1.13
Host is up (0.00066s latency).
/>Not shown: 992 closed ports
PORT       STATE      SERVICE
22/tcp     open       ssh
80/tcp     open       http
111/tcp    open       rpcbind
139/tcp    open       netbios-ssn
3306       open       mysql

MAC Address: 01:AA:FB:23:21:45
Nmap done: 1 IP address (1 host up) scanned in 4.22 seconds
```

Given the organization\\'s policy, which of the following services should be disabled on this server?

A. rpcbind

B. netbios-ssn

C. mysql

D. ssh

E. telnet

Correct Answer: D

QUESTION 5

A vulnerability scanner has identified an out-of-support database software version running on a server. The software update will take six to nine months to complete. The management team has agreed to a one-year extended support contract with the software vendor. Which of the following BEST describes the risk treatment in this scenario?

A. The extended support mitigates any risk associated with the software.

B. The extended support contract changes this vulnerability finding to a false positive.

C. The company is transferring the risk for the vulnerability to the software vendor.

D. The company is accepting the inherent risk of the vulnerability.

Correct Answer: D