Leads4Pass

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

An organization developed a comprehensive incident response policy. Executive management approved the policy and its associated procedures. Which of the following activities would be MOST beneficial to evaluate personnel\\'s familiarity with incident response procedures?

A. A simulated breach scenario involving the incident response team

B. Completion of annual information security awareness training by all employees

C. Tabletop activities involving business continuity team members

D. Completion of lessons-learned documentation by the computer security incident response team

E. External and internal penetration testing by a third party

Correct Answer: A

QUESTION 2

Which of the following sources will provide the MOST relevant threat intelligence data to the security team of a dental care network?

A. H-ISAC

B. Dental forums

C. Open threat exchange

D. Dark web chatter

Correct Answer: A

Reference: https://h-isac.org/

QUESTION 3

A technician is troubleshooting a desktop computer with low disk space. The technician reviews the following information snippets:

Disk Allocation Report
350Gb − C:\Users\user1\movies\movies

Network Stats

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:8080	0.0.0.0:0	LISTENING movieDB
TCP	192.168.1.10:8080	172.16.34.77:1200	TIME_WAIT

Which of the following should the technician do to BEST resolve the issue based on the above information? (Choose two.)

A. Delete the movies/movies directory

B. Disable the movieDB service

C. Enable OS auto updates

D. Install a file integrity tool

E. Defragment the disk

Correct Answer: BE

QUESTION 4

Which of the following is a vulnerability that is specific to hypervisors?

A. DDoS

B. VLAN hopping

C. Weak encryption

D. WMescape

Correct Answer: D

QUESTION 5

A security analyst is generating a list of recommendations for the company\\'s insecure API.

Which of the following is the BEST parameter mitigation...?

A. Implement parameterized queries.

B. Use effective authentication and authorization methods.

C. Validate all incoming data.

D. Use TLs for all data exchanges.

Correct Answer: D