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.geekcert.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 company\\'s data is still being exfiltered to business competitors after the implementation of a DLP solution. Which of the following is the most likely reason why the data is still being compromised?

A. Printed reports from the database contain sensitive information

B. DRM must be implemented with the DLP solution

C. Users are not labeling the appropriate data sets

D. DLP solutions are only effective when they are implemented with disk encryption

Correct Answer: B

Reference: https://www.vaultize.com/blog/-enterprise-drm-and-dlp-are-amazing-together.html

QUESTION 2

An analyst is detecting Linux machines on a Windows network. Which of the following tools should be used to detect a computer operating system?

A. whois

B. netstat

C. nmap

D. nslookup

Correct Answer: C

QUESTION 3

A SIEM solution alerts a security analyst of a high number of login attempts against the company\\'s webmail portal. The analyst determines the login attempts used credentials from a past data breach. Which of the following is the BEST mitigation to prevent unauthorized access?

A. Single sign-on

B. Mandatory access control

C. Multifactor authentication

D. Federation

E. Privileged access management

Correct Answer: C

QUESTION 4

A security analyst is reviewing port scan data that was collected over the course of several months. The following data represents the trends:

	Number of devices with open ports					
Port	Month 1	Month 2	Month 3	Month 4	Month 5	Month 6
445	8	8	8	8	8	8
8443	7	9	10	13	16	19
22	6	6	7	6	8	6

Which of the following is the BEST action for the security analyst to take after analyzing the trends?

A. Review the system configurations to determine if port 445 needs to be open.

B. Assume there are new instances of Apache in the environment.

C. Investigate why the number of open SSH ports varied during the six months.

D. Raise a concern to a supervisor regarding possible malicious use Of port 8443.

Correct Answer: C

According to the CompTIA CySA+ Certification Exam Study guide, the best action for the security analyst to take after analyzing the trends is to investigate why the number of open SSH ports varied during the six months. This could indicate that malicious actors are attempting to gain access to the system, and it would be important to find out the root cause of this activity in order to prevent further intrusions. Additionally, raising a concern to a supervisor regarding possible malicious use of port 8443 would also be a prudent step, as this port is often used by attackers. As stated in the study guide, "Monitoring network ports and traffic can provide insight into suspicious activity and may be necessary to identify malicious activities". Additionally, "Ports can be used to gain unauthorized access to a system, so it is important to monitor the ports and to take steps to ensure that only necessary ports are open".

QUESTION 5

A security analyst discovers a standard user has unauthorized access to the command prompt, PowerShell, and other system utilities. Which of the following is the BEST action for the security analyst to take?

A. Disable the appropriate settings in the administrative template of the Group Policy.

B. Use AppLocker to create a set of whitelist and blacklist rules specific to group membership.

C. Modify the registry keys that correlate with the access settings for the System32 directory.

D. Remove the user\\'s permissions from the various system executables.

Correct Answer: A

Latest CS0-002 Dumps CS0-002 PDF Dumps CS0-002 VCE Dumps