CS0-003 Q&As

CompTIA Cybersecurity Analyst (CySA+)

Pass CompTIA CS0-003 Exam with 100% Guarantee

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

https://www.pass4itsure.com/cs0-003.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

QUESTION 1

A company is deploying new vulnerability scanning software to assess its systems. The current network is highly segmented, and the networking team wants to minimize the number of unique firewall rules. Which of the following scanning techniques would be most efficient to achieve the objective?

A. Deploy agents on all systems to perform the scans

B. Deploy a central scanner and perform non-credentialed scans

C. Deploy a cloud-based scanner and perform a network scan

D. Deploy a scanner sensor on every segment and perform credentialed scans

Correct Answer: D

QUESTION 2

A security analyst s monitoring a company\\'s network traffic and finds ping requests going to accounting and human resources servers from a SQL server. Upon investigation, the analyst discovers a technician responded to potential network connectivity issues. Which of the following is the best way for the security analyst to respond?

A. Report this activity as a false positive, as the activity is legitimate.

B. Isolate the system and begin a forensic investigation to determine what was compromised.

C. Recommend network segmentation to the management team as a way to secure the various environments.

D. Implement host-bases firewalls on all systems to prevent ping sweeps in the future.

Correct Answer: A

QUESTION 3

A security analyst is reviewing a packet capture in Wireshark that contains an FTP session from a potentially compromised machine. The analyst sets the following display filter: ftp. The analyst can see there are several RETR requests with 226 Transfer complete responses, but the packet list pane is not showing the packets containing the file transfer itself. Which of the following can the analyst perform to see the entire contents of the downloaded files?

A. Change the display filter to f cp. accive. pore

B. Change the display filter to tcg.port=20

C. Change the display filter to f cp-daca and follow the TCP streams

D. Navigate to the File menu and select FTP from the Export objects option

Correct Answer: C

The best way to see the entire contents of the downloaded files in Wireshark is to change the display filter to ftp-data and follow the TCP streams. FTP-data is a protocol that is used to transfer files between an FTP client and server using TCP port 20. By filtering for ftp-data packets and following the TCP streams, the analyst can see the actual file data that was transferred during the FTP session

QUESTION 4

A forensic analyst is conducting an investigation on a compromised server Which of the following should the analyst do first to preserve evidence\\'\\'

A. Restore damaged data from the backup media

B. Create a system timeline

C. Monitor user access to compromised systems

D. Back up all log files and audit trails

Correct Answer: D

A forensic analyst is conducting an investigation on a compromised server. The first step that the analyst should do to preserve evidence is to back up all log files and audit trails. This will ensure that the analyst has a copy of the original data that can be used for analysis and verification. Backing up the log files and audit trails will also prevent any tampering or modification of the evidence by the attacker or other parties. The other options are not the first steps or may alter or destroy the evidence. CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0- 002), page 16; https://www.nist.gov/publications/guide-collection-and-preservation-digital-evidence

QUESTION 5

A new zero-day vulnerability was released. A security analyst is prioritizing which systems should receive deployment of compensating controls deployment first. The systems have been grouped into the categories shown below:

Group	Vulnerability present	Mitigating controls	Asset value
Group A	No	No	High
Group B	Yes	Yes	Med
Group C	Yes	No	Med
Group D	Yes	Yes	High

Which of the following groups should be prioritized for compensating controls?

A. Group A

B. Group B

C. Group C

D. Group D

Correct Answer: C