CFR-410 Q&As

CyberSec First Responder (CFR)

Pass CertNexus CFR-410 Exam with 100% Guarantee

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

https://www.pass4itsure.com/cfr-410.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

During which of the following attack phases might a request sent to port 1433 over a whole company network be seen within a log?

A. Reconnaissance

B. Scanning

C. Gaining access

D. Persistence

Correct Answer: B

Reference: https://blog.stealthbits.com/finding-microsoft-sql-server-targets-sql-attacks/

QUESTION 2

During the forensic analysis of a compromised computer image, the investigator found that critical files are missing, caches have been cleared, and the history and event log files are empty. According to this scenario, which of the following techniques is the suspect using?

A. System hardening techniques

B. System optimization techniques

C. Defragmentation techniques

D. Anti-forensic techniques

Correct Answer: D

QUESTION 3

A network security analyst has noticed a flood of Simple Mail Transfer Protocol (SMTP) traffic to internal clients. SMTP traffic should only be allowed to email servers. Which of the following commands would stop this attack? (Choose two.)

A. iptables -A INPUT -p tcp –dport 25 -d x.x.x.x -j ACCEPT

B. iptables -A INPUT -p tcp –sport 25 -d x.x.x.x -j ACCEPT

C. iptables -A INPUT -p tcp –dport 25 -j DROP

D. iptables -A INPUT -p tcp –destination-port 21 -j DROP

E. iptables -A FORWARD -p tcp –dport 6881:6889 -j DROP

Correct Answer: AC

QUESTION 4

When tracing an attack to the point of origin, which of the following items is critical data to map layer 2 switching?

A. DNS cache

B. ARP cache

C. CAM table

D. NAT table

Correct Answer: B

The host that owns the IP address sends an ARP reply message with its physical address. Each host machine maintains a table, called ARP cache, used to convert MAC addresses to IP addresses. Since ARP is a stateless protocol, every time a host gets an ARP reply from another host, even though it has not sent an ARP request for that reply, it accepts that ARP entry and updates its ARP cache. The process of updating a target host\\'s ARP cache with a forged entry is referred to as poisoning.

Reference: https://www.researchgate.net/publication/221056734_Securing_Layer_2_in_Local_Area_Networks

QUESTION 5

During which phase of a vulnerability assessment would a security consultant need to document a requirement to retain a legacy device that is no longer supported and cannot be taken offline?

A. Conducting post-assessment tasks

B. Determining scope

C. Identifying critical assets

D. Performing a vulnerability scan

Correct Answer: C