

# **CertNexus**

## **Exam Questions CFR-410**

CyberSec First Responder (CFR) Exam



#### NEW QUESTION 1

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

**Answer:** AC

#### NEW QUESTION 2

Detailed step-by-step instructions to follow during a security incident are considered:

- A. Policies
- B. Guidelines
- C. Procedures
- D. Standards

**Answer:** C

#### NEW QUESTION 3

A security administrator needs to review events from different systems located worldwide. Which of the following is MOST important to ensure that logs can be effectively correlated?

- A. Logs should be synchronized to their local time zone.
- B. Logs should be synchronized to a common, predefined time source.
- C. Logs should contain the username of the user performing the action.
- D. Logs should include the physical location of the action performed.

**Answer:** A

#### NEW QUESTION 4

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

**Answer:** B

#### NEW QUESTION 5

Tcpdump is a tool that can be used to detect which of the following indicators of compromise?

- A. Unusual network traffic
- B. Unknown open ports
- C. Poor network performance
- D. Unknown use of protocols

**Answer:** A

#### NEW QUESTION 6

Which of the following is an automated password cracking technique that uses a combination of uppercase and lowercase letters, 0-9 numbers, and special characters?

- A. Dictionary attack
- B. Password guessing
- C. Brute force attack
- D. Rainbow tables

**Answer:** C

#### NEW QUESTION 7

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

**Answer:** D

#### NEW QUESTION 8

Recently, a cybersecurity research lab discovered that there is a hacking group focused on hacking into the computers of financial executives in Company A to sell the exfiltrated information to Company B. Which of the following threat motives does this MOST likely represent?

- A. Desire for power
- B. Association/affiliation
- C. Reputation/recognition
- D. Desire for financial gain

**Answer:** D

#### NEW QUESTION 9

Which of the following is a cybersecurity solution for insider threats to strengthen information protection?

- A. Web proxy
- B. Data loss prevention (DLP)
- C. Anti-malware
- D. Intrusion detection system (IDS)

**Answer:** B

#### NEW QUESTION 10

An incident handler is assigned to initiate an incident response for a complex network that has been affected by malware. Which of the following actions should be taken FIRST?

- A. Make an incident response plan.
- B. Prepare incident response tools.
- C. Isolate devices from the network.
- D. Capture network traffic for analysis.

**Answer:** D

#### NEW QUESTION 10

A network administrator has determined that network performance has degraded due to excessive use of social media and Internet streaming services. Which of the following would be effective for limiting access to these types of services, without completely restricting access to a site?

- A. Whitelisting
- B. Web content filtering
- C. Network segmentation
- D. Blacklisting

**Answer:** B

#### NEW QUESTION 11

A security engineer is setting up security information and event management (SIEM). Which of the following log sources should the engineer include that will contain indicators of a possible web server compromise? (Choose two.)

- A. NetFlow logs
- B. Web server logs
- C. Domain controller logs
- D. Proxy logs
- E. FTP logs

**Answer:** BC

#### NEW QUESTION 13

After imaging a disk as part of an investigation, a forensics analyst wants to hash the image using a tool that supports piecewise hashing. Which of the following tools should the analyst use?

- A. md5sum
- B. sha256sum
- C. md5deep
- D. hashdeep

**Answer:** A

#### NEW QUESTION 18

To minimize vulnerability, which steps should an organization take before deploying a new Internet of Things (IoT) device? (Choose two.)

- A. Changing the default password
- B. Updating the device firmware
- C. Setting up new users
- D. Disabling IPv6
- E. Enabling the firewall

**Answer:**

BE

**NEW QUESTION 19**

Which common source of vulnerability should be addressed to BEST mitigate against URL redirection attacks?

- A. Application
- B. Users
- C. Network infrastructure
- D. Configuration files

**Answer:** A

**NEW QUESTION 22**

Which of the following types of attackers would be MOST likely to use multiple zero-day exploits executed against high-value, well-defended targets for the purposes of espionage and sabotage?

- A. Cybercriminals
- B. Hacktivists
- C. State-sponsored hackers
- D. Cyberterrorist

**Answer:** C

**NEW QUESTION 27**

Which of the following characteristics of a web proxy strengthens cybersecurity? (Choose two.)

- A. Increases browsing speed
- B. Filters unwanted content
- C. Limits direct connection to Internet
- D. Caches frequently-visited websites
- E. Decreases wide area network (WAN) traffic

**Answer:** AD

**NEW QUESTION 30**

In which of the following attack phases would an attacker use Shodan?

- A. Scanning
- B. Reconnaissance
- C. Gaining access
- D. Persistence

**Answer:** A

**NEW QUESTION 35**

An organization recently suffered a data breach involving a server that had Transmission Control Protocol (TCP) port 1433 inadvertently exposed to the Internet. Which of the following services was vulnerable?

- A. Internet Message Access Protocol (IMAP)
- B. Network Basic Input/Output System (NetBIOS)
- C. Database
- D. Network Time Protocol (NTP)

**Answer:** C

**NEW QUESTION 39**

If a hacker is attempting to alter or delete system audit logs, in which of the following attack phases is the hacker involved?

- A. Covering tracks
- B. Expanding access
- C. Gaining persistence
- D. Performing reconnaissance

**Answer:** A

**NEW QUESTION 44**

Which of the following are legally compliant forensics applications that will detect an alternative data stream (ADS) or a file with an incorrect file extension? (Choose two.)

- A. Disk duplicator
- B. EnCase
- C. dd
- D. Forensic Toolkit (FTK)
- E. Write blocker

**Answer:**

BD

**NEW QUESTION 45**

Which of the following data sources could provide indication of a system compromise involving the exfiltration of data to an unauthorized destination?

- A. IPS logs
- B. DNS logs
- C. SQL logs
- D. SSL logs

**Answer:** A

**NEW QUESTION 49**

A system administrator identifies unusual network traffic from outside the local network. Which of the following is the BEST method for mitigating the threat?

- A. Malware scanning
- B. Port blocking
- C. Packet capturing
- D. Content filtering

**Answer:** C

**NEW QUESTION 54**

An incident response team is concerned with verifying the integrity of security information and event management (SIEM) events after being written to disk. Which of the following represents the BEST option for addressing this concern?

- A. Time synchronization
- B. Log hashing
- C. Source validation
- D. Field name consistency

**Answer:** A

**NEW QUESTION 57**

According to Payment Card Industry Data Security Standard (PCI DSS) compliance requirements, an organization must retain logs for what length of time?

- A. 3 months
- B. 6 months
- C. 1 year
- D. 5 years

**Answer:** C

**NEW QUESTION 58**

.....

## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### CFR-410 Practice Exam Features:

- \* CFR-410 Questions and Answers Updated Frequently
- \* CFR-410 Practice Questions Verified by Expert Senior Certified Staff
- \* CFR-410 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* CFR-410 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The CFR-410 Practice Test Here](#)**