

## CFR-410 Dumps

### CyberSec First Responder (CFR) Exam

<https://www.certleader.com/CFR-410-dumps.html>



**NEW QUESTION 1**

The incident response team has completed root cause analysis for an incident. Which of the following actions should be taken in the next phase of the incident response process? (Choose two.)

- A. Providing a briefing to management
- B. Updating policies and procedures
- C. Training staff for future incidents
- D. Investigating responsible staff
- E. Drafting a recovery plan for the incident

**Answer:** BE

**NEW QUESTION 2**

A company website was hacked via the following SQL query: email, passwd, login\_id, full\_name FROM members WHERE email = "attacker@somewhere.com"; DROP TABLE members; –" Which of the following did the hackers perform?

- A. Cleared tracks of attacker@somewhere.com entries
- B. Deleted the entire members table
- C. Deleted the email password and login details
- D. Performed a cross-site scripting (XSS) attack

**Answer:** C

**NEW 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

**Answer:** AC

**NEW QUESTION 4**

Nmap is a tool most commonly used to:

- A. Map a route for war-driving
- B. Determine who is logged onto a host
- C. Perform network and port scanning
- D. Scan web applications

**Answer:** C

**NEW QUESTION 5**

A security operations center (SOC) analyst observed an unusually high number of login failures on a particular database server. The analyst wants to gather supporting evidence before escalating the observation to management. Which of the following expressions will provide login failure data for 11/24/2015?

- A. grep 20151124 security\_log | grep –c "login failure"
- B. grep 20150124 security\_log | grep "login\_failure"
- C. grep 20151124 security\_log | grep "login"
- D. grep 20151124 security\_log | grep –c "login"

**Answer:** C

**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**

A government organization responsible for critical infrastructure is being attacked and files on the server been deleted. Which of the following are the most immediate communications that should be made regarding the incident? (Choose two.)

- A. Notifying law enforcement
- B. Notifying the media
- C. Notifying a national compute emergency response team (CERT) or cybersecurity incident response team (CSIRT)
- D. Notifying the relevant vendor

E. Notifying a mitigation expert

**Answer:** CE

#### NEW QUESTION 8

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 9

A Linux system administrator found suspicious activity on host IP 192.168.10.121. This host is also establishing a connection to IP 88.143.12.123. Which of the following commands should the administrator use to capture only the traffic between the two hosts?

- A. # tcpdump -i eth0 host 88.143.12.123
- B. # tcpdump -i eth0 dst 88.143.12.123
- C. # tcpdump -i eth0 host 192.168.10.121
- D. # tcpdump -i eth0 src 88.143.12.123

**Answer:** B

#### NEW QUESTION 10

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 10

During an incident, the following actions have been taken:

- Executing the malware in a sandbox environment
- Reverse engineering the malware
- Conducting a behavior analysis

Based on the steps presented, which of the following incident handling processes has been taken?

- A. Containment
- B. Eradication
- C. Recovery
- D. Identification

**Answer:** A

#### Explanation:

The “Containment, eradication and recovery” phase is the period in which incident response team tries to contain the incident and, if necessary, recover from it (restore any affected resources, data and/or processes).

#### NEW QUESTION 12

A company that maintains a public city infrastructure was breached and information about future city projects was leaked. After the post-incident phase of the process has been completed, which of the following would be PRIMARY focus of the incident response team?

- A. Restore service and eliminate the business impact.
- B. Determine effective policy changes.
- C. Inform the company board about the incident.
- D. Contact the city police for official investigation.

**Answer:** B

#### NEW QUESTION 17

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 18**

A security administrator notices a process running on their local workstation called SvrsScEsdKexzCv.exe. The unknown process is MOST likely:

- A. Malware
- B. A port scanner
- C. A system process
- D. An application process

**Answer:** A

**NEW QUESTION 23**

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 24**

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 25**

When attempting to determine which system or user is generating excessive web traffic, analysis of which of the following would provide the BEST results?

- A. Browser logs
- B. HTTP logs
- C. System logs
- D. Proxy logs

**Answer:** D

**NEW QUESTION 27**

An unauthorized network scan may be detected by parsing network sniffer data for:

- A. IP traffic from a single IP address to multiple IP addresses.
- B. IP traffic from a single IP address to a single IP address.
- C. IP traffic from multiple IP addresses to a single IP address.
- D. IP traffic from multiple IP addresses to other networks.

**Answer:** C

**NEW QUESTION 28**

The Key Reinstallation Attack (KRACK) vulnerability is specific to which types of devices? (Choose two.)

- A. Wireless router
- B. Switch
- C. Firewall
- D. Access point
- E. Hub

**Answer:** AE

**NEW QUESTION 31**

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 36**

Which of the following, when exposed together, constitutes PII? (Choose two.)

- A. Full name
- B. Birth date
- C. Account balance
- D. Marital status
- E. Employment status

**Answer:** AC

**NEW QUESTION 37**

An incident responder discovers that the CEO logged in from their New York City office and then logged in from a location in Beijing an hour later. The incident responder suspects that the CEO's account has been compromised. Which of the following anomalies MOST likely contributed to the incident responder's suspicion?

- A. Geolocation
- B. False positive
- C. Geovelocity
- D. Advanced persistent threat (APT) activity

**Answer:** C

**NEW QUESTION 39**

Which of the following enables security personnel to have the BEST security incident recovery practices?

- A. Crisis communication plan
- B. Disaster recovery plan
- C. Occupant emergency plan
- D. Incident response plan

**Answer:** B

**NEW QUESTION 43**

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 45**

A web server is under a denial of service (DoS) attack. The administrator reviews logs and creates an access control list (ACL) to stop the attack. Which of the following technologies could perform these steps automatically in the future?

- A. Intrusion prevention system (IPS)
- B. Intrusion detection system (IDS)
- C. Blacklisting
- D. Whitelisting

**Answer:** B

**NEW QUESTION 50**

Network infrastructure has been scanned and the identified issues have been remediated. What is the next step in the vulnerability assessment process?

- A. Generating reports
- B. Establishing scope
- C. Conducting an audit
- D. Assessing exposures

**Answer:** C

**NEW QUESTION 54**

.....

## Thank You for Trying Our Product

\* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

\* One year free update

You can enjoy free update one year. 24x7 online support.

\* Trusted by Millions

We currently serve more than 30,000,000 customers.

\* Shop Securely

All transactions are protected by VeriSign!

**100% Pass Your CFR-410 Exam with Our Prep Materials Via below:**

<https://www.certleader.com/CFR-410-dumps.html>