

# CertNexus

## Exam Questions CFR-410

CyberSec First Responder (CFR) Exam



#### NEW QUESTION 1

Various logs are collected for a data leakage case to make a forensic analysis. Which of the following are MOST important for log integrity? (Choose two.)

- A. Hash value
- B. Time stamp
- C. Log type
- D. Modified date/time
- E. Log path

**Answer:** AB

#### NEW QUESTION 2

After a hacker obtained a shell on a Linux box, the hacker then sends the exfiltrated data via Domain Name System (DNS). This is an example of which type of data exfiltration?

- A. Covert channels
- B. File sharing services
- C. Steganography
- D. Rogue service

**Answer:** A

#### 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

A common formula used to calculate risk is: + Threats + Vulnerabilities = Risk. Which of the following represents the missing factor in this formula?

- A. Exploits
- B. Security
- C. Asset
- D. Probability

**Answer:** C

#### NEW QUESTION 5

According to company policy, all accounts with administrator privileges should have suffix \_ja. While reviewing Windows workstation configurations, a security administrator discovers an account without the suffix in the administrator's group. Which of the following actions should the security administrator take?

- A. Review the system log on the affected workstation.
- B. Review the security log on a domain controller.
- C. Review the system log on a domain controller.
- D. Review the security log on the affected workstation.

**Answer:** B

#### NEW QUESTION 6

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

**Answer:** B

#### Explanation:

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.

#### NEW QUESTION 7

A company has noticed a trend of attackers gaining access to corporate mailboxes. Which of the following would be the BEST action to take to plan for this kind of attack in the future?

- A. Scanning email server for vulnerabilities
- B. Conducting security awareness training
- C. Hardening the Microsoft Exchange Server
- D. Auditing account password complexity

**Answer:** A

#### NEW QUESTION 8

Which of the following are common areas of vulnerabilities in a network switch? (Choose two.)

- A. Default port state
- B. Default credentials
- C. Default protocols
- D. Default encryption
- E. Default IP address

**Answer:** AB

#### NEW QUESTION 9

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 10

A suspicious script was found on a sensitive research system. Subsequent analysis determined that proprietary data would have been deleted from both the local server and backup media immediately following a specific administrator's removal from an employee list that is refreshed each evening. Which of the following BEST describes this scenario?

- A. Backdoor
- B. Rootkit
- C. Time bomb
- D. Login bomb

**Answer:** A

#### NEW QUESTION 10

A user receives an email about an unfamiliar bank transaction, which includes a link. When clicked, the link redirects the user to a web page that looks exactly like their bank's website and asks them to log in with their username and password. Which type of attack is this?

- A. Whaling
- B. Smishing
- C. Vishing
- D. Phishing

**Answer:** D

#### NEW QUESTION 13

Which of the following could be useful to an organization that wants to test its incident response procedures without risking any system downtime?

- A. Blue team exercise
- B. Business continuity exercise
- C. Tabletop exercise
- D. Red team exercise

**Answer:** B

#### NEW QUESTION 16

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 21

An attacker intercepts a hash and compares it to pre-computed hashes to crack a password. Which of the following methods has been used?

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

**Answer:** C

#### NEW QUESTION 25

Which of the following would MOST likely make a Windows workstation on a corporate network vulnerable to remote exploitation?

- A. Disabling Windows Updates
- B. Disabling Windows Firewall
- C. Enabling Remote Registry
- D. Enabling Remote Desktop

**Answer:** D

#### NEW QUESTION 26

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 27

During a security investigation, a suspicious Linux laptop is found in the server room. The laptop is processing information and indicating network activity. The investigator is preparing to launch an investigation to determine what is happening with this laptop. Which of the following is the MOST appropriate set of Linux commands that should be executed to conduct the investigation?

- A. iperf, traceroute, whois, ls, chown, cat
- B. iperf, wget, traceroute, dc3dd, ls, whois
- C. lsof, chmod, nano, whois, chown, ls
- D. lsof, ifconfig, who, ps, ls, tcpdump

**Answer:** B

#### NEW QUESTION 32

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 33

An automatic vulnerability scan has been performed. Which is the next step of the vulnerability assessment process?

- A. Hardening the infrastructure
- B. Documenting exceptions
- C. Assessing identified exposures
- D. Generating reports

**Answer:** D

#### NEW QUESTION 35

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 38

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 40

A secretary receives an email from a friend with a picture of a kitten in it. The secretary forwards it to the ~COMPANYWIDE mailing list and, shortly thereafter, users across the company receive the following message:

“You seem tense. Take a deep breath and relax!”

The incident response team is activated and opens the picture in a virtual machine to test it. After a short analysis, the following code is found in C:

```
\Temp\chill.exe:Powershell.exe –Command “do {(for /L %i in (2,1,254) do shutdown /r /m Error! Hyperlink reference not valid.&gt; /f /t / 0 /c “You seem tense. Take a deep breath and relax!”);Start-Sleep –s 900) } while(1)”
```

Which of the following BEST represents what the attacker was trying to accomplish?

- A. Taunt the user and then trigger a shutdown every 15 minutes.
- B. Taunt the user and then trigger a reboot every 15 minutes.
- C. Taunt the user and then trigger a shutdown every 900 minutes.
- D. Taunt the user and then trigger a reboot every 900 minutes.

**Answer: B**

#### NEW QUESTION 42

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 43

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 48

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 52

.....

## 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](#)**