



**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

An administrator investigating intermittent network communication problems has identified an excessive amount of traffic from an external-facing host to an unknown location on the Internet. Which of the following BEST describes what is occurring?

- A. The network is experiencing a denial of service (DoS) attack.
- B. A malicious user is exporting sensitive data.
- C. Rogue hardware has been installed.
- D. An administrator has misconfigured a web proxy.

**Answer:** B

#### NEW QUESTION 3

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 4

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 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

It was recently discovered that many of an organization's servers were running unauthorized cryptocurrency mining software. Which of the following assets were being targeted in this attack? (Choose two.)

- A. Power resources
- B. Network resources
- C. Disk resources
- D. Computing resources
- E. Financial resources

**Answer:** AB

#### NEW QUESTION 7

While reviewing some audit logs, an analyst has identified consistent modifications to the sshd\_config file for an organization's server. The analyst would like to investigate and compare contents of the current file with archived versions of files that are saved weekly. Which of the following tools will be MOST effective during the investigation?

- A. `cat * | cut -d ' ' -f 2,5,7`
- B. `more * | grep`
- C. `diff`
- D. `sort *`

**Answer:** C

#### NEW QUESTION 8

A first responder notices a file with a large amount of clipboard information stored in it. Which part of the MITRE ATT&CK matrix has the responder discovered?

- A. Collection
- B. Discovery
- C. Lateral movement
- D. Exfiltration

**Answer:** D

#### NEW QUESTION 9

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 10

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 10

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 13

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 14

Which of the following attacks involves sending a large amount of spoofed User Datagram Protocol (UDP) traffic to a router's broadcast address within a network?

- A. Land attack
- B. Fraggle attack
- C. Smurf attack
- D. Teardrop attack

**Answer:** C

#### NEW QUESTION 17

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 22

A Windows system administrator has received notification from a security analyst regarding new malware that executes under the process name of “armageddon.exe” along with a request to audit all department workstations for its presence. In the absence of GUI-based tools, what command could the administrator execute to complete this task?

- A. ps -ef | grep armageddon
- B. top | grep armageddon
- C. wmic process list brief | find “armageddon.exe”
- D. wmic startup list full | find “armageddon.exe”

**Answer:** C

#### NEW QUESTION 27

A security administrator is investigating a compromised host. Which of the following commands could the investigator use to display executing processes in real time?

- A. ps
- B. top
- C. nice
- D. pstree

**Answer:** B

#### NEW QUESTION 30

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 35

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 36

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 41

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 44

During a malware-driven distributed denial of service attack, a security researcher found excessive requests to a name server referring to the same domain name and host name encoded in hexadecimal. The malware author used which type of command and control?

- A. Internet Relay Chat (IRC)
- B. Dnscat2

- C. Custom channel
- D. File Transfer Protocol (FTP)

**Answer:** D

#### NEW QUESTION 48

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 53

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 57

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 61

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 63

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 66

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 71

Which of the following are part of the hardening phase of the vulnerability assessment process? (Choose two.)

- A. Installing patches
- B. Updating configurations
- C. Documenting exceptions
- D. Conducting audits
- E. Generating reports

**Answer:** AB

#### NEW QUESTION 72

An organization recently suffered a breach due to a human resources administrator emailing employee names and Social Security numbers to a distribution list. Which of the following tools would help mitigate this risk from recurring?

- A. Data loss prevention (DLP)
- B. Firewall
- C. Web proxy
- D. File integrity monitoring

**Answer:** A

#### NEW QUESTION 73

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 75

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 78

While performing routing maintenance on a Windows Server, a technician notices several unapproved Windows Updates and that remote access software has been installed. The technician suspects that a malicious actor has gained access to the system. Which of the following steps in the attack process does this activity indicate?

- A. Expanding access
- B. Covering tracks
- C. Scanning
- D. Persistence

**Answer:** A

#### NEW QUESTION 81

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 85

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 87**

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

**Answer:** C

**NEW QUESTION 91**

Which of the following security best practices should a web developer reference when developing a new web- based application?

- A. Control Objectives for Information and Related Technology (COBIT)
- B. Risk Management Framework (RMF)
- C. World Wide Web Consortium (W3C)
- D. Open Web Application Security Project (OWASP)

**Answer:** D

**NEW QUESTION 93**

Which of the following are well-known methods that are used to protect evidence during the forensics process? (Choose three.)

- A. Evidence bags
- B. Lock box
- C. Caution tape
- D. Security envelope
- E. Secure rooms
- F. Faraday boxes

**Answer:** ACD

**NEW QUESTION 97**

.....

## 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](#)**