

CertNexus

Exam Questions CFR-410

CyberSec First Responder (CFR) Exam



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

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 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

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 5

A security professional discovers a new ransomware strain that disables antivirus on the endpoint during an infection. Which location would be the BEST place for the security professional to find technical information about this malware?

- A. Threat intelligence feeds
- B. Computer emergency response team (CERT) press releases
- C. Vulnerability databases
- D. Social network sites

Answer: A

NEW QUESTION 6

While planning a vulnerability assessment on a computer network, which of the following is essential? (Choose two.)

- A. Identifying exposures
- B. Identifying critical assets
- C. Establishing scope
- D. Running scanning tools
- E. Installing antivirus software

Answer: AC

NEW QUESTION 7

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 8

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 9

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 10

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 10

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 13

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 18

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 21

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 22

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 25

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 29

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 32

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 34

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 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 37

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 40

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 log review, an incident responder is attempting to process the proxy server's log files but finds that they are too large to be opened by any file viewer. Which of the following is the MOST appropriate technique to open and analyze these log files?

- A. Hex editor, searching
- B. tcpdump, indexing
- C. PE Explorer, indexing
- D. Notepad, searching

Answer: A

NEW QUESTION 45

Malicious code designed to execute in concurrence with a particular event is BEST defined as which of the following?

- A. Logic bomb
- B. Rootkit
- C. Trojan
- D. Backdoor

Answer: A

NEW QUESTION 46

As part of an organization's regular maintenance activities, a security engineer visits the Internet Storm Center advisory page to obtain the latest list of blacklisted host/network addresses. The security engineer does this to perform which of the following activities?

- A. Update the latest proxy access list
- B. Monitor the organization's network for suspicious traffic
- C. Monitor the organization's sensitive databases
- D. Update access control list (ACL) rules for network devices

Answer: D

NEW QUESTION 48

An incident responder has collected network capture logs in a text file, separated by five or more data fields. Which of the following is the BEST command to use if the responder would like to print the file (to terminal/ screen) in numerical order?

- A. cat | tac
- B. more
- C. sort -n
- D. less

Answer: C

NEW QUESTION 50

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 51

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 54

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 58

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 61

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 62

Which of the following methods are used by attackers to find new ransomware victims? (Choose two.)

- A. Web crawling
- B. Distributed denial of service (DDoS) attack
- C. Password guessing
- D. Phishing
- E. Brute force attack

Answer: DE

NEW QUESTION 67

A security analyst has discovered that an application has failed to run. Which of the following is the tool MOST likely used by the analyst for the initial discovery?

- A. syslog
- B. MSConfig
- C. Event Viewer
- D. Process Monitor

Answer: C

NEW QUESTION 68

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 72

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 74

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 75

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 76

.....

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](#)