

Exam Questions CFR-410

CyberSec First Responder (CFR) Exam

<https://www.2passeasy.com/dumps/CFR-410/>



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

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 4

A security investigator has detected an unauthorized insider reviewing files containing company secrets. Which of the following commands could the investigator use to determine which files have been opened by this user?

- A. ls
- B. lsof
- C. ps
- D. netstat

Answer: B

NEW QUESTION 5

Which of the following is the GREATEST risk of having security information and event management (SIEM) collect computer names with older log entries?

- A. There may be duplicate computer names on the network.
- B. The computer name may not be admissible evidence in court.
- C. Domain Name System (DNS) records may have changed since the log was created.
- D. There may be field name duplication when combining log files.

Answer: D

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

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 8

An administrator believes that a system on VLAN 12 is Address Resolution Protocol (ARP) poisoning clients on the network. The administrator attaches a system to VLAN 12 and uses Wireshark to capture traffic. After reviewing the capture file, the administrator finds no evidence of ARP poisoning. Which of the following actions should the administrator take next?

- A. Clear the ARP cache on their system.
- B. Enable port mirroring on the switch.
- C. Filter Wireshark to only show ARP traffic.
- D. Configure the network adapter to promiscuous mode.

Answer: D

NEW QUESTION 9

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 10

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 10

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 11

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 14

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 17

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 18

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 19

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 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 26

A company help desk is flooded with calls regarding systems experiencing slow performance and certain Internet sites taking a long time to load or not loading at all. The security operations center (SOC) analysts who receive these calls take the following actions:

- Running antivirus scans on the affected user machines
- Checking department membership of affected users
- Checking the host-based intrusion prevention system (HIPS) console for affected user machine alerts
- Checking network monitoring tools for anomalous activities

Which of the following phases of the incident response process match the actions taken?

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

Answer: A

NEW QUESTION 28

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 30

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 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 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 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 44

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 49

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 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 55

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 56

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 58

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 62

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 65

Which of the following is susceptible to a cache poisoning attack?

- A. Domain Name System (DNS)
- B. Secure Shell (SSH)
- C. Hypertext Transfer Protocol Secure (HTTPS)
- D. Hypertext Transfer Protocol (HTTP)

Answer: A

NEW QUESTION 67

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 70

When performing an investigation, a security analyst needs to extract information from text files in a Windows operating system. Which of the following commands should the security analyst use?

- A. findstr
- B. grep
- C. awk
- D. sigverif

Answer: C

NEW QUESTION 71

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 76

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 79

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CFR-410 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CFR-410 Product From:

<https://www.2passeasy.com/dumps/CFR-410/>

Money Back Guarantee

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