

Exam Questions CFR-410

CyberSec First Responder (CFR) Exam

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



NEW QUESTION 1

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 2

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 3

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 4

Which asset would be the MOST desirable for a financially motivated attacker to obtain from a health insurance company?

- A. Transaction logs
- B. Intellectual property
- C. PII/PHI
- D. Network architecture

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 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 8

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 9

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 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

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 11

Which of the following describes United States federal government cybersecurity policies and guidelines?

- A. NIST
- B. ANSI
- C. NERC
- D. GDPR

Answer: A

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 20

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 25

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 27

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 32

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 34

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 35

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 38

To minimize vulnerability, which steps should an organization take before deploying a new Internet of Things (IoT) device? (Choose two.)

- A. Changing the default password
- B. Updating the device firmware

- C. Setting up new users
- D. Disabling IPv6
- E. Enabling the firewall

Answer: BE

NEW QUESTION 39

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 40

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 41

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 45

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 50

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 51

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 56

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.> /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 57

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 58

A cybersecurity expert assigned to be the IT manager of a middle-sized company discovers that there is little endpoint security implementation on the company's systems. Which of the following could be included in an endpoint security solution? (Choose two.)

- A. Web proxy
- B. Network monitoring system
- C. Data loss prevention (DLP)
- D. Anti-malware
- E. Network Address Translation (NAT)

Answer: AB

NEW QUESTION 59

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 60

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 63

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 66

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 71

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 74

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 77

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 78

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 83

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 85

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 90

.....

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