

CFR-410 Dumps

CyberSec First Responder (CFR) Exam

<https://www.certleader.com/CFR-410-dumps.html>



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

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

Nmap is a tool most commonly used to:

- A. Map a route for war-driving
- B. Determine who is logged onto a host
- C. Perform network and port scanning
- D. Scan web applications

Answer: C

NEW QUESTION 5

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 6

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 7

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 8

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 9

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

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 10

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 13

After successfully enumerating the target, the hacker determines that the victim is using a firewall. Which of the following techniques would allow the hacker to bypass the intrusion prevention system (IPS)?

- A. Stealth scanning
- B. Xmas scanning
- C. FINS scanning
- D. Port scanning

Answer: C

NEW QUESTION 14

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 17

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 21

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 23

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 24

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 26

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 29

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 30

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 35

Organizations considered “covered entities” are required to adhere to which compliance requirement?

- A. Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- B. Payment Card Industry Data Security Standard (PCI DSS)
- C. Sarbanes-Oxley Act (SOX)
- D. International Organization for Standardization (ISO) 27001

Answer: A

NEW QUESTION 37

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 41

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your CFR-410 Exam with Our Prep Materials Via below:

<https://www.certleader.com/CFR-410-dumps.html>