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
A company website was hacked via the following SQL query: email, passwd, login_id, full_name FROM members WHERE email = “attacker@somewhere.com”; DROP TABLE members; –” Which of the following did the hackers perform?

A. Cleared tracks of attacker@somewhere.com entries
B. Deleted the entire members table
C. Deleted the email password and login details
D. Performed a cross-site scripting (XSS) attack

Answer: C

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 analyst is required to collect detailed network traffic on a virtual machine. Which of the following tools could the analyst use?

A. nbtstat
B. WinDump
C. fport
D. netstat

Answer: D

NEW QUESTION 5
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 6
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 7
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 8
A Linux administrator is trying to determine the character count on many log files. Which of the following command and flag combinations should the administrator use?

A. tr -d
B. uniq -c
C. wc -m
D. grep -c

Answer: C

NEW QUESTION 9
Senior management has stated that antivirus software must be installed on all employee workstations. Which of the following does this statement BEST describe?

A. Guideline
B. Procedure
C. Policy
D. Standard

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 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 15
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
After a security breach, a security consultant is hired to perform a vulnerability assessment for a company’s web application. Which of the following tools would the consultant use?

A. Nikto
B. Kismet
C. tcpdump
D. Hydra

Answer: A

NEW QUESTION 19
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 21
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 22
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 27
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 32
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 34
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 36
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 39
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 42
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 45
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 51
In which of the following attack phases would an attacker use Shodan?

A. Scanning
B. Reconnaissance
C. Gaining access
D. Persistence

Answer: A

NEW QUESTION 55
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 60
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 64
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 65
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 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 70
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
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 78
An incident responder was asked to analyze malicious traffic. Which of the following tools would be BEST for this?

A. Hex editor
B. tcpdump
C. Wireshark
D. Snort

Answer: C

NEW QUESTION 79
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 83
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 85
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 87
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 92
Which of the following technologies would reduce the risk of a successful SQL injection attack?

A. Reverse proxy
B. Web application firewall
C. Stateful firewall
D. Web content filtering

Answer: B

NEW QUESTION 97
......

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