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
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 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 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
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 7
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 8
A security administrator needs to review events from different systems located worldwide. Which of the following is MOST important to ensure that logs can be effectively correlated?

A. Logs should be synchronized to their local time zone.
B. Logs should be synchronized to a common, predefined time source.
C. Logs should contain the username of the user performing the action.
D. Logs should include the physical location of the action performed.

Answer: A

NEW QUESTION 9
During which of the following attack phases might a request sent to port 1433 over a whole company network be seen within a log?

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

Answer: B

NEW QUESTION 10
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 10
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 11
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 14
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 19
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 22
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 27
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 31
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 36
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 41
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 44
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 49
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 54
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 59
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 62
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 63
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 65
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 69
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 73
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 78
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 83
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 86
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 90
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 92
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 93
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 96
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 97
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 100
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 105
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 107
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 110
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 115
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 116
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 121
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 123
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 124
.....

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