Exam Questions CFR-410

CyberSec First Responder (CFR) Exam

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

NEW QUESTION 1
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 2
A security professional discovers a new ransomware strain that disables antivirus on the endpoint during an infection. Which location would be the BEST place for the security professional to find technical information about this malware?

A. Threat intelligence feeds
B. Computer emergency response team (CERT) press releases
C. Vulnerability databases
D. Social network sites

Answer: A

NEW QUESTION 3
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 4
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 5
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 6
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 7
It was recently discovered that many of an organization’s servers were running unauthorized cryptocurrency mining software. Which of the following assets were being targeted in this attack? (Choose two.)

A. Power resources
B. Network resources
C. Disk resources
D. Computing resources
E. Financial resources

Answer: AB

NEW QUESTION 8
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 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 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 10
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 12
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 14
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 19
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 20
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 21
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 23
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 25
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 27
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 30
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 33
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 37
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 40
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 44
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 45
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 49
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 51
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 53
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 56
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 57
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 60
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 62
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 66
Which of the following does the command nmap –open 10.10.10.3 do?

A. Execute a scan on a single host, returning only open ports.
B. Execute a scan on a subnet, returning detailed information on open ports.
C. Execute a scan on a subnet, returning all hosts with open ports.
D. Execute a scan on a single host, returning open services.

Answer: D

NEW QUESTION 71
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 73
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 76
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
A system administrator identifies unusual network traffic from outside the local network. Which of the following is the BEST method for mitigating the threat?

A. Malware scanning
B. Port blocking
C. Packet capturing
D. Content filtering

Answer: C

NEW QUESTION 83
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 84
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 88
Which of the following is a method of reconnaissance in which a ping is sent to a target with the expectation of receiving a response?

A. Active scanning
B. Passive scanning
C. Network enumeration
D. Application enumeration

Answer: C

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 93
.....

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