CertNexus

Exam Questions CFR-410

CyberSec First Responder (CFR) Exam

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 network security analyst has noticed a flood of Simple Mail Transfer Protocol (SMTP) traffic to internal clients. SMTP traffic should only be allowed to email servers. Which of the following commands would stop this attack? (Choose two.)

A. iptables -A INPUT -p tcp –dport 25 -d x.x.x.x -j ACCEPT
B. iptables -A INPUT -p tcp –sport 25 -d x.x.x.x -j ACCEPT
C. iptables -A INPUT -p tcp –dport 25 -j DROP
D. iptables -A INPUT -p tcp –destination-port 21 -j DROP
E. iptables -A FORWARD -p tcp –dport 6881:6889 -j DROP

Answer: AC

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
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 6
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 7
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 8
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 9
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 10
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 15
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 18
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 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 23
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
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 32
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 34
A suspicious script was found on a sensitive research system. Subsequent analysis determined that proprietary data would have been deleted from both the local server and backup media immediately following a specific administrator's removal from an employee list that is refreshed each evening. Which of the following BEST describes this scenario?

A. Backdoor
B. Rootkit
C. Time bomb
D. Login bomb

Answer: A

NEW QUESTION 37
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 40
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 43
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 46
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
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 54
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 55
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 56
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 61

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 64
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 67
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 70
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 71
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 75
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 77
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 82
Which of the following are part of the hardening phase of the vulnerability assessment process? (Choose two.)

A. Installing patches
B. Updating configurations
C. Documenting exceptions
D. Conducting audits
E. Generating reports

Answer: AB

NEW QUESTION 86
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 88
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 93
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 98
Which of the following, when exposed together, constitutes PII? (Choose two.)

A. Full name
B. Birth date
C. Account balance
D. Marital status
E. Employment status

Answer: AC

NEW QUESTION 100
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 104
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 106
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 109
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 112
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 115
A web server is under a denial of service (DoS) attack. The administrator reviews logs and creates an access control list (ACL) to stop the attack. Which of the following technologies could perform these steps automatically in the future?

A. Intrusion prevention system (IPS)
B. Intrusion detection system (IDS)
C. Blacklisting
D. Whitelisting

Answer: B

NEW QUESTION 116
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 118
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 123
Which of the following are well-known methods that are used to protect evidence during the forensics process? (Choose three.)

A. Evidence bags
B. Lock box
C. Caution tape
D. Security envelope
E. Secure rooms
F. Faraday boxes

Answer: ACD

NEW QUESTION 127
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

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