CertNexus

Exam Questions CFR-410

CyberSec First Responder (CFR) Exam

NEW QUESTION 1
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 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 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
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 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
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 10
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 10
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 15
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 20
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 25
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 30
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 31
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 36
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 39
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 44
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 45
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 50
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 52
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 57
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 61
A company that maintains a public city infrastructure was breached and information about future city projects was leaked. After the post-incident phase of the process has been completed, which of the following would be PRIMARY focus of the incident response team?

A. Restore service and eliminate the business impact.
B. Determine effective policy changes.
C. Inform the company board about the incident.
D. Contact the city police for official investigation.

Answer: B

NEW QUESTION 62
An automatic vulnerability scan has been performed. Which is the next step of the vulnerability assessment process?

A. Hardening the infrastructure
B. Documenting exceptions
C. Assessing identified exposures
D. Generating reports

Answer: D

NEW QUESTION 64
To minimize vulnerability, which steps should an organization take before deploying a new Internet of Things (IoT) device? (Choose two.)

A. Changing the default password
B. Updating the device firmware
C. Setting up new users
D. Disabling IPv6
E. Enabling the firewall

Answer: BE

NEW QUESTION 69
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 72
A security administrator notices a process running on their local workstation called SvrsScEsdKexzCv.exe. The unknown process is MOST likely:

A. Malware
B. A port scanner

C. A system process
D. An application process

Answer: A

NEW QUESTION 74
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 75
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 79
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 80
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 83
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 87
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 91
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 96
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 97
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 102
.....

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