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
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 3
A security investigator has detected an unauthorized insider reviewing files containing company secrets. Which of the following commands could the investigator use to determine which files have been opened by
this user?

A. ls
B. lsof
C. ps
D. netstat

Answer: B

NEW QUESTION 4
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 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
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
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 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 14
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 15
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 19
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 21
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 22
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 25
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 30
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 35
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 37
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 38
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.&gt; /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 41
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 44
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 47
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 52
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 55
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 57
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 59

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 60
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 64
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 65
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 68
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 71
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 73
......