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
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 3
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 4
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 5
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 6
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 7
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 8
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 9
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 10
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 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 15
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 19
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 24
Which of the following would MOST likely make a Windows workstation on a corporate network vulnerable to remote exploitation?

A. Disabling Windows Updates
B. Disabling Windows Firewall
C. Enabling Remote Registry
D. Enabling Remote Desktop

Answer: D

NEW QUESTION 26
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
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
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 40
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 42
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 45

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 49
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 51
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 54
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 55
.....

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