CertNexus

Exam Questions CFR-410

CyberSec First Responder (CFR) Exam

NEW QUESTION 1
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 2
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 3
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 4
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 5
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 6
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 7
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 8
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 9
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 10
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 10
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 15
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 18
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 22
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 23
During a security investigation, a suspicious Linux laptop is found in the server room. The laptop is processing information and indicating network activity. The investigator is preparing to launch an investigation to determine what is happening with this laptop. Which of the following is the MOST appropriate set of Linux commands that should be executed to conduct the investigation?

A. iperf, traceroute, whois, ls, chown, cat
B. iperf, wget, traceroute, dc3dd, ls, whois
C. lsof, chmod, nano, whois, chown, ls
D. lsof, ifconfig, who, ps, ls, tcpdump

Answer: B

NEW QUESTION 25
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 29
During a log review, an incident responder is attempting to process the proxy server’s log files but finds that they are too large to be opened by any file viewer. Which of the following is the MOST appropriate technique to open and analyze these log files?

A. Hex editor, searching
B. tcpdump, indexing
C. PE Explorer, indexing
D. Notepad, searching

Answer: A

NEW QUESTION 32
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 37
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 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.> /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 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 45
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 48
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 52
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 56
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 57
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 59
.....

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