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 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 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
A security professional discovers a new ransomware strain that disables antivirus on the endpoint during an infection. Which location would be the BEST place for the security professional to find technical information about this malware?

A. Threat intelligence feeds
B. Computer emergency response team (CERT) press releases
C. Vulnerability databases
D. Social network sites

Answer: A

NEW QUESTION 5
A security analyst is required to collect detailed network traffic on a virtual machine. Which of the following tools could the analyst use?

A. nbtstat
B. WinDump
C. fport
D. netstat

Answer: D

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
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 8
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 9
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 10
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 11
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 12
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 13
An incident responder has collected network capture logs in a text file, separated by five or more data fields. Which of the following is the BEST command to use if the responder would like to print the file (to terminal/ screen) in numerical order?

A. cat | tac
B. more
C. sort –n
D. less

Answer: C

NEW QUESTION 14
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 15
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 16
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 17
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 18
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 19
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 20
According to Payment Card Industry Data Security Standard (PCI DSS) compliance requirements, an organization must retain logs for what length of time?

A. 3 months
B. 6 months
C. 1 year
D. 5 years

Answer: C

NEW QUESTION 21
......