CFR-410 Q&As

CyberSec First Responder (CFR)

Pass CertNexus CFR-410 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/cfr-410.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CertNexus Official Exam Center

QUESTION 1

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.

Correct Answer: A

QUESTION 2

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.

Correct Answer: D

Reference: https://www.tutorialspoint.com/ethical_hacking/ethical_hacking_arp_poisoning.htm

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.

Correct Answer: B

QUESTION 4

During the forensic analysis of a compromised computer image, the investigator found that critical files are missing, caches have been cleared, and the history and event log files are empty. According to this scenario, which of the following techniques is the suspect using?

A. System hardening techniques

B. System optimization techniques

C. Defragmentation techniques

D. Anti-forensic techniques

Correct Answer: D

QUESTION 5

In which of the following attack phases would an attacker use Shodan?

A. Scanning

B. Reconnaissance

C. Gaining access

D. Persistence

Correct Answer: A

Reference: https://books.google.com.pk/books?id=3bzPDwAAQBAJandpg=PA41andlpg=PA41anddq=attack+phases+would+an+attacker+use +Shodanandsource=blandots=phUbfR8BOYandsig=ACfU3U1sg5J67s_sL_Ixpr3OiqdCIraKUwandhl=enandsa=Xandved=2ahUKEwjazaKCssXpAhUC4YUKHcJ5CVwQ6AEwAXoECBMQAQ#v=onepageandq=attack%20phases%20would%20an%20attacker %20use%20Shodanandf=false

QUESTION 6

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

Correct Answer: A

Reference: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf

QUESTION 7

Detailed step-by-step instructions to follow during a security incident are considered:

A. Policies

B. Guidelines

C. Procedures

D. Standards

Correct Answer: C

QUESTION 8

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

Correct Answer: B

Reference: https://www.ciscopress.com/articles/article.asp?p=345618

QUESTION 9

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

Correct Answer: BC

Reference: https://www.techrepublic.com/blog/data-center/top-three-indicators-of-compromised-web-servers/

QUESTION 10

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

Correct Answer: C

Reference: https://kb.iu.edu/d/afjb

QUESTION 11

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

Correct Answer: D

QUESTION 12

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

Correct Answer: AE

Reference: https://www.kaspersky.com/blog/krackattack/19798/

QUESTION 13

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

Correct Answer: A

Reference: https://blog.qualys.com/securitylabs/2016/01/07/open-redirection-a-simple-vulnerability-threatens-your-web-applications

QUESTION 14

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

Correct Answer: C

Reference: https://nmap.org/book/firewall-subversion.html

QUESTION 15

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

Correct Answer: A