

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 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.

Answer: A

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

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 5

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 6

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 7

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 8

Which of the following could be useful to an organization that wants to test its incident response procedures without risking any system downtime?

- A. Blue team exercise
- B. Business continuity exercise
- C. Tabletop exercise
- D. Red team exercise

Answer: B

NEW QUESTION 9

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 10

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 10

A Linux system administrator found suspicious activity on host IP 192.168.10.121. This host is also establishing a connection to IP 88.143.12.123. Which of the following commands should the administrator use to capture only the traffic between the two hosts?

- A. # tcpdump -i eth0 host 88.143.12.123
- B. # tcpdump -i eth0 dst 88.143.12.123
- C. # tcpdump -i eth0 host 192.168.10.121
- D. # tcpdump -i eth0 src 88.143.12.123

Answer: B

NEW QUESTION 15

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 20

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 25

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 28

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 31

Which of the following is the FIRST step taken to maintain the chain of custody in a forensic investigation?

- A. Security and evaluating the electronic crime scene.
- B. Transporting the evidence to the forensics lab
- C. Packaging the electronic device
- D. Conducting preliminary interviews

Answer: C

NEW QUESTION 32

When attempting to determine which system or user is generating excessive web traffic, analysis of which of the following would provide the BEST results?

- A. Browser logs
- B. HTTP logs
- C. System logs
- D. Proxy logs

Answer: D

NEW QUESTION 35

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 37

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 41

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 44

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions 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

100% Actual & Verified — Instant Download, Please Click
[Order The CFR-410 Practice Test Here](#)