DUMPSARENA

CyberSec First Responder (CFR) Exam

CertNexus CFR-410

Version Demo

Total Demo Questions: 10

Total Premium Questions: 100

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

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: B D

QUESTION NO: 2

An incident at a government agency has occurred and the following actions were taken:

- Users have regained access to email accounts

- Temporary VPN services have been removed

- Host-based intrusion prevention system (HIPS) and antivirus (AV) signatures have been updated

- Temporary email servers have been decommissioned

Which of the following phases of the incident response process match the actions taken?

A. Containment

B. Post-incident

C. Recovery

D. Identification

ANSWER: A

QUESTION NO: 3

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

ANSWER: B C

QUESTION NO: 4

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

QUESTION NO: 5

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: B E

QUESTION NO: 6

A network security analyst has noticed a flood of Simple Mail Transfer Protocol (SMTP) traffic to internal clients. SMTP traffic should only be allowed to email servers. Which of the following commands would stop this attack? (Choose two.)

A. iptables -A INPUT -p tcp –dport 25 -d x.x.x.x -j ACCEPT

B. iptables -A INPUT -p tcp –sport 25 -d x.x.x.x -j ACCEPT

C. iptables -A INPUT -p tcp –dport 25 -j DROP

D. iptables -A INPUT -p tcp –destination-port 21 -j DROP

E. iptables -A FORWARD -p tcp –dport 6881:6889 -j DROP

ANSWER: A C

QUESTION NO: 7

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

QUESTION NO: 8

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

QUESTION NO: 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: C E

QUESTION NO: 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