

# DUMPSBOSS.

## CyberSec First Responder (CFR) Exam

CertNexus CFR-410

Version Demo

Total Demo Questions: 10

Total Premium Questions: 100

Buy Premium PDF

<https://dumpsboss.co>

[support@dumpsboss.co](mailto:support@dumpsboss.co)

support@dumpsboss.co  
dumpsboss.co

## QUESTION NO: 1

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**

## QUESTION NO: 2

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: 3

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: A E**

## QUESTION NO: 4

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**

## QUESTION NO: 5

Malicious code designed to execute in concurrence with a particular event is BEST defined as which of the following?

- A. Logic bomb
- B. Rootkit
- C. Trojan
- D. Backdoor

**ANSWER: A**

## QUESTION NO: 6

It was recently discovered that many of an organization's servers were running unauthorized cryptocurrency mining software. Which of the following assets were being targeted in this attack? (Choose two.)

- A. Power resources
- B. Network resources
- C. Disk resources
- D. Computing resources
- E. Financial resources

**ANSWER: A B**

## QUESTION NO: 7

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).

Reference: <https://blog.rapid7.com/2017/01/11/introduction-to-incident-response-life-cycle-of-nist-sp-800-61/>

## QUESTION NO: 8

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**

## QUESTION NO: 9

A cybersecurity expert assigned to be the IT manager of a middle-sized company discovers that there is little endpoint security implementation on the company’s systems. Which of the following could be included in an endpoint security solution? (Choose two.)

- A. Web proxy

- B. Network monitoring system
- C. Data loss prevention (DLP)
- D. Anti-malware
- E. Network Address Translation (NAT)

**ANSWER: A B**

## QUESTION NO: 10

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: D E**