



CS0-003^{Q&As}

CompTIA Cybersecurity Analyst (CySA+)

Pass CompTIA CS0-003 Exam with 100% Guarantee

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

<https://www.geekcert.com/cs0-003.html>

100% Passing Guarantee
100% Money Back Assurance

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

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers





QUESTION 1

A recent penetration test discovered that several employees were enticed to assist attackers by visiting specific websites and running downloaded files when prompted by phone calls. Which of the following would best address this issue?

- A. Increasing training and awareness for all staff
- B. Ensuring that malicious websites cannot be visited
- C. Blocking all scripts downloaded from the internet
- D. Disabling all staff members' ability to run downloaded applications

Correct Answer: A

QUESTION 2

After running the `cat file01.bin | hexdump -C` command, a security analyst reviews the following output snippet: Which of the following digital-forensics techniques is the analyst using?

```
00000000 ff d8 ff e0 00 10 4a 46 49 46 00 01 01 00 00 01 |.....JFIF.....|
```

- A. Reviewing the file hash
- B. Debugging the binary file
- C. Implementing file carving
- D. Verifying the file type
- E. Utilizing reverse engineering

Correct Answer: D

QUESTION 3

A company is deploying new vulnerability scanning software to assess its systems. The current network is highly segmented, and the networking team wants to minimize the number of unique firewall rules. Which of the following scanning techniques would be most efficient to achieve the objective?

- A. Deploy agents on all systems to perform the scans
- B. Deploy a central scanner and perform non-credentialed scans
- C. Deploy a cloud-based scanner and perform a network scan



D. Deploy a scanner sensor on every segment and perform credentialed scans

Correct Answer: D

QUESTION 4

Which of the following phases of the Cyber Kill Chain involves the adversary attempting to establish communication with a successfully exploited target?

- A. Command and control
- B. Actions on objectives
- C. Exploitation
- D. Delivery

Correct Answer: A

Command and control (C2) is a phase of the Cyber Kill Chain that involves the adversary attempting to establish communication with a successfully exploited target. C2 enables the adversary to remotely control or manipulate the target system or network using various methods, such as malware callbacks, backdoors, botnets, or covert channels. C2 allows the adversary to maintain persistence, exfiltrate data, execute commands, deliver payloads, or spread to other systems or networks.

QUESTION 5

A systems administrator receives reports of an internet-accessible Linux server that is running very sluggishly. The administrator examines the server, sees a high amount of memory utilization, and suspects a DoS attack related to half-open TCP sessions consuming memory. Which of the following tools would best help to prove whether this server was experiencing this behavior?

- A. Nmap
- B. TCPDump
- C. SIEM
- D. EDR

Correct Answer: B

In this scenario, where the administrator suspects a DoS attack related to half-open TCP sessions consuming memory, TCPDump would be the best tool to use. It can help prove whether the server is experiencing this behavior by capturing and analyzing the network packets to identify patterns consistent with half-open TCP sessions.