

CSOC Practice Test Questions and Answers

1. What is a 'zero-day vulnerability'?

- A) A vulnerability that is unknown to the software vendor and for which no patch is yet available
- B) A vulnerability that was discovered on the first day of a software release
- C) A vulnerability that takes zero days to exploit once discovered
- D) A vulnerability that only affects systems with zero days of uptime

2. What is a 'grey box' penetration test?

- A) A test where the tester is given partial knowledge of the target system, simulating an attacker with some internal information
- B) A test conducted on systems that are partially operational and not fully deployed
- C) A penetration test conducted between a 'black box' and 'white box' test in terms of regulatory compliance
- D) A test that focuses only on the network perimeter without testing internal systems

3. What is a 'honeypot' in network security?

- A) A decoy system designed to attract attackers and observe their tactics, techniques, and procedures
- B) A secure storage vault for sensitive cryptographic keys
- C) A network segment containing systems with the highest security controls
- D) A software tool that automatically patches vulnerable systems in the network

4. What is a 'denial of service' (DoS) attack?

- A) An attack that overwhelms a system or network with traffic to make it unavailable to legitimate users
- B) An attack that denies a specific user access to their account
- C) An attack that destroys data on a system to deny the owner access to their files
- D) An attack where the attacker denies any involvement in a cybersecurity incident

Answers: 1-A 2-A 3-A 4-A

For More CSOC Questions and Answers FREE, CSOC Online Prep Training, CSOC Exam, CSOC Study Guide, CSOC Flashcards, CSOC Quizzes visit:

CSOC Practice Test