

# CREST CCRTS

**CREST Red Team Specialist**

**For More Information – Visit link below:**

**<https://www.examsempire.com/>**

**Product Version**

- 1. Up to Date products, reliable and verified.**
- 2. Questions and Answers in PDF Format.**



**<https://examsempire.com/>**

**Visit us at: <https://www.examsempire.com/ccrts>**

# Latest Version: 6.0

## Question: 1

Which of the following best reflects operational security (OPSEC) in red team exercises?

Response:

- A. Encrypting client credentials post-engagement
- B. Preventing detection during engagement to preserve realism
- C. Using VPNs for all outbound traffic
- D. Running attacks only during working hours

**Answer: B**

## Question: 2

When sensitive data is accessed during an engagement, it must be handled in accordance with \_\_\_\_\_ regulations.

Response:

- A. GDPR
- B. DMZ
- C. SPF
- D. CIDR

**Answer: A**

## Question: 3

Malicious Microsoft Office documents often use embedded \_\_\_\_\_ to execute payloads when opened.

Response:

- A. VBA macros
- B. bash aliases
- C. HTML comments
- D. SHA-1 signatures

**Answer: A**

### Question: 4

Scenario: You are asked to review a script written by a previous red teamer. You find hardcoded credentials and cleartext tokens in the source. What should you do before using it in your engagement?

Response:

- A. Strip credentials and use environment variables
- B. Encrypt the file with base64
- C. Convert the script to compiled binary
- D. Upload the script to GitHub for version control

**Answer: A**

### Question: 5

Scenario: Your C2 traffic is detected due to repetitive, non-browser-like headers in requests. What should you modify?

Response:

- A. Use Base64 payloads
- B. Spoof User-Agent and Accept headers
- C. Switch to DNS-only C2
- D. Send binary data directly in URL paths

**Answer: B**

### Question: 6

The process of impersonating a domain admin account using a captured ticket is known as a \_\_\_\_\_ attack.

Response:

- A. Pass-the-Ticket
- B. Replay
- C. NTLM Downgrade
- D. OAuth2 Abuse

**Answer: A**

### Question: 7

Publicly available repositories, social media, and breach data all contribute to effective \_\_\_\_\_ gathering.

Response:

- A. Open-Source Intelligence (OSINT)
- B. Payload
- C. Pivoting
- D. DDoS

**Answer: A**

### Question: 8

Which DNS misconfigurations could provide attackers with an internal view of the organization's structure?

Response:

- A. Open zone transfers
- B. Public SPF records
- C. Wildcard A records
- D. TXT records for DKIM

**Answer: A,B**

### Question: 9

Credential stuffing relies on \_\_\_\_\_ passwords being reused across multiple sites.

Response:

- A. breached
- B. random
- C. rotated
- D. long

**Answer: A**

### Question: 10

Why might a red team script be obfuscated?

Response:

- A. To ensure it runs faster
- B. To reduce file size
- C. To evade detection by defensive tools
- D. To improve code readability

**Answer: C**

**Thank You for Trying Our Product**

**Special 16 USD Discount Coupon: NSZUBG3X**

**Email:** [support@examsempire.com](mailto:support@examsempire.com)

**Check our Customer Testimonials and ratings  
available on every product page.**

**Visit our website.**

**<https://examsempire.com/>**