



CERTSWARRIOR

# G/AC

*GRTP*  
*GIAC Red Team Professional*

## Questions & Answers PDF

**For More Information:**

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

## Features:

- 90 Days Free Updates
- 30 Days Money Back Guarantee
- Instant Download Once Purchased
- 24/7 Online Chat Support
- Its Latest Version

---

# Latest Version: 6.0

## Question: 1

What are effective strategies for the initial reconnaissance phase?

(Choose two)

Response:

- A. Social engineering to gather intel from company employees
- B. Deploying a wide range of automated scanning tools against the target
- C. Reviewing publicly available information about the target
- D. Physically breaking into the target's premises to gather intel

**Answer: A,C**

## Question: 2

Why is it important to use both direct and indirect C2 channels in an attack infrastructure?

Response:

- A. To ensure redundancy in case one communication channel is detected or disrupted
- B. To provide different bandwidth options for data exfiltration
- C. To comply with international cyber warfare conventions
- D. To facilitate the segmentation of the compromised network

**Answer: A**

## Question: 3

Which of the following are common methods for escalating privileges on a Linux system?

(Choose two)

Response:

- A. Exploiting vulnerable services or daemons
- B. Cracking passwords using brute force attacks
- C. Modifying file permissions as a regular user
- D. Abusing misconfigured network services

**Answer: A,D**

---

### Question: 4

Adversary emulation differs from penetration testing primarily in that it:

Response:

- A. Focuses solely on the exploitation of physical security controls
- B. Is an unstructured approach to identifying vulnerabilities
- C. Emulates an adversary's actions based on real-world incidents and TTPs
- D. Is typically performed without any prior knowledge of the environment

**Answer: C**

### Question: 5

During the enumeration phase, why is it important to identify the domain controllers in an Active Directory environment?

Response:

- A. To locate the physical servers in the data center
- B. To target the primary sources of authentication and policy enforcement
- C. To assess the environmental temperature controls
- D. To determine the brand of hardware being used

**Answer: B**

### Question: 6

What is the primary purpose of a Golden Ticket attack within an Active Directory environment?

Response:

- A. To modify Active Directory schema
- B. To obtain persistent access and impersonate the domain's Kerberos Ticket Granting Ticket (TGT)
- C. To disrupt the availability of Active Directory services
- D. To extract plaintext passwords from the Active Directory database

**Answer: B**

### Question: 7

Which technique is indicative of ransomware behavior within a network?

---

Response:

- A. Incremental backups of essential files
- B. Encryption of files with a demand for payment for decryption keys
- C. Broadcasting SSID from the compromised system
- D. Port scanning the internal network for open services

**Answer: B**

### Question: 8

In network discovery, which types of information are typically gathered using SNMP enumeration?  
(Choose two)

Response:

- A. Network device types and roles
- B. Usernames and passwords
- C. Running services and processes
- D. Network interface and routing information

**Answer: A,D**



# CERTSWARRIOR

## *FULL PRODUCT INCLUDES:*

Money Back Guarantee



Instant Download after Purchase



90 Days Free Updates



PDF Format Digital Download



24/7 Live Chat Support



Latest Syllabus Updates



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

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

**16 USD Discount Coupon Code: U89DY2AQ**