



CERTSWARRIOR

# GIAC GRTP

## GIAC Red Team Professional

Questions&AnswersPDF

ForMoreInformation:

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

## Features:

- 90DaysFreeUpdates
- 30DaysMoneyBackGuarantee
- InstantDownloadOncePurchased
- 24/7OnlineChat Support
- ItsLatestVersion

# Latest Version: 6.0

## Question: 1

Which tool is widely used for lateral movement within Windows domains?

Response:

- A. BloodHound
- B. PsExec
- C. Wireshark
- D. Hydra

**Answer: B**

## Question: 2

Which two techniques are used to perform lateral movement within a Windows domain?

(Choose two)

Response:

- A. Remote code execution via PsExec
- B. DNS tunneling
- C. Exploiting misconfigured file shares
- D. DNS spoofing

**Answer: A,C**

## Question: 3

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: 4

What are key considerations when forming a red team for an engagement?

Multiple Correct Answers

Response:

- A. The skills and expertise of each team member
- B. The availability of advanced hacking tools
- C. Ensuring a diversity of perspectives and capabilities
- D. The ability to work undetected within the target organization

**Answer: A,C**

### Question: 5

How can an attacker leverage scheduled tasks for persistence?

Response:

- A. By scheduling system reboots to disrupt user activity
- B. By creating tasks that initiate the attacker's payload at system startup or at a specified time
- C. By deleting all scheduled tasks to cover tracks
- D. By scheduling legitimate system updates to gain user trust

**Answer: B**

### Question: 6

What is the purpose of scoping a red team engagement?

Response:

- A. To identify all vulnerabilities in the environment
- B. To define the objectives, rules, and boundaries of the engagement
- C. To determine the number of testers needed
- D. To plan for social engineering activities

**Answer: B**

### Question: 7

What is the primary function of a Command and Control (C2) infrastructure in adversary emulation?

Response:

- A. To capture and store network traffic
- B. To establish communication between compromised systems and attackers
- C. To block incoming network traffic
- D. To encrypt all system data

**Answer: B**

### Question: 8

After gaining initial access, what are the key next steps an attacker should take?

Multiple Correct Answers

Response:

- A. Establishing persistence in the system
- B. Immediately exfiltrating all accessible data
- C. Conducting further reconnaissance within the network
- D. Strengthening the security of the system to lock out other potential attackers

**Answer: A,C**

### Question: 9

What is the purpose of performing Pass-the-Hash (PtH) attacks in a domain environment?

Response:

- A. To sniff network traffic
- B. To exploit weak passwords
- C. To authenticate without knowing the plaintext password
- D. To identify unpatched systems

**Answer: C**

### Question: 10

Which of the following attacks can be used to escalate privileges in an Active Directory environment?

Multiple Correct Answers

Response:

- A. Pass-the-Hash attack
- B. ARP poisoning

- C. Kerberoasting
- D. DNS spoofing

**Answer: A,C**



# 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**