EDUSUM

#1 Online Certification Guide

GIAC GRTP

GIAC Red Team Professional Certification Questions & Answers

Exam Summary – Syllabus –Questions

GRTP

GIAC Red Team Professional (GRTP)

75 Questions Exam – 76% Cut Score – Duration of 120 minutes

Table of Contents:

Know Your GRTP Certification Well:

The GRTP is best suitable for candidates who want to gain knowledge in the GIAC Offensive Operations, Pen Testing, and Red Teaming. Before you start your GRTP preparation you may struggle to get all the crucial GIAC Red Team Professional materials like GRTP syllabus, sample questions, study guide.

But don't worry the GRTP PDF is here to help you prepare in a stress free manner.
The PDF is a combination of all your queries like-

- What is in the GRTP syllabus?
- How many questions are there in the GRTP exam?
- Which Practice test would help me to pass the GRTP exam at the first attempt?

Passing the GRTP exam makes you GIAC Red Team Professional (GRTP). Having the GIAC Red Team Professional certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

GRTP GIAC Red Team Professional Certification Details:

Exam Name	GIAC Red Team Professional (GRTP)
Exam Code	GRTP
Exam Price	$979 (USD)
Duration	120 mins
Number of Questions	75
Passing Score	76%
Books / Training	**SEC565: Red Team Operations and Adversary Emulation**
Schedule Exam	**Pearson VUE**
Sample Questions	**GIAC GRTP Sample Questions**
Practice Exam	**GIAC GRTP Certification Practice Exam**

GRTP Syllabus:

Topic	Details
Adversary Emulation Fundamentals	- The candidate will have an understanding of common terminology, frameworks, and methodology associated with adversary emulation.
Attacking Active Directory	- The candidate will have an understanding of Active Directory objects, the different authentication methods offered within an Active Directory environment, and the techniques used to attack those authentication methods.
Command and Control infrastructure	- The candidate will have an understanding of command-and-control deployments, uses, channels and tools including Empire and Cobalt Strike.
Creating the Attack infrastructure	- The candidate will have an understanding how to create and manage an adversary infrastructure to include, an adversary domain, DNS, and an understanding of redirection and pivoting.
Discovery and Enumeration	- The candidate will have an understanding of how to perform network and Active Directory discovery and enumeration as well as how to acquire available credentials within the target environment.
Enumerating and Attacking Privileges	- The candidate will understand how to determine privileges within the environment and how to escalate to the required privileges to achieve their objectives including Linux attacks and performing privilege recon remotely.
Gaining Access	- The candidate will have an understanding on how to perform reconnaissance on a target, how to create and test a malicious payload, and how to deliver the malicious payload ensuring access to the target environment.
Leveraging the Domain	- The candidate will have an understanding of how to move within the target environment in order to achieve the objectives of the engagement.
Persistence and Exfiltration	- The candidate will have an understanding on different methods to gain persistence in a environment and how to exploit that persistence to complete the objectives of the engagement including, gaining access to a database, staging data for exfiltration, and emulating ransomware.
Red Team Engagement Planning and Reporting	- The candidate will be able to plan an engagement including tasks such as adversary profiling, scoping the

Topic	Details
	engagement, and red team creation. The candidate will also be able to understand how to close the engagement including data consolidation, revealing the red teams actions, producing an engagement report, and determining if retesting will be completed.

GIAC GRTP Sample Questions:

Question: 1

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

a) To locate the physical servers in the data center
b) To determine the brand of hardware being used
c) To assess the environmental temperature controls
d) To target the primary sources of authentication and policy enforcement

Answer: d

Question: 2

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

a) To modify Active Directory schema
b) To extract plaintext passwords from the Active Directory database
c) To disrupt the availability of Active Directory services
d) To obtain persistent access and impersonate the domain's Kerberos Ticket Granting Ticket (TGT)

Answer: d

Question: 3

Which of the following are common methods for escalating privileges on a Linux system? (Choose two)

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

What are effective strategies for the initial reconnaissance phase?

(Choose two)

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: 5

How should the success criteria of a red team engagement be determined?

a) By the number of vulnerabilities found
b) By achieving the predefined objectives without being detected
c) By the amount of time it takes to breach the system
d) By the feedback received from the organization's employees

Answer: b

Question: 6

Which technique is indicative of ransomware behavior within a network?

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: 7

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

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: 8

In the context of persistence, what is the purpose of creating a hidden user account on the compromised system?

a) To enable the legitimate users to have enhanced privileges
b) To facilitate remote support and troubleshooting
c) To ensure the attacker can regain access even if other accounts are discovered or removed
d) To provide an account for guest users

Answer: c

Question: 9

Adversary emulation differs from penetration testing primarily in that it:

a) Focuses solely on the exploitation of physical security controls
b) Emulates an adversary's actions based on real-world incidents and TTPs
c) Is an unstructured approach to identifying vulnerabilities
d) Is typically performed without any prior knowledge of the environment

Answer: b

Question: 10

In network discovery, which types of information are typically gathered using SNMP enumeration?

(Choose two)

a) Network device types and roles
b) Usernames and passwords
c) Running services and processes
d) Network interface and routing information

Answer: a, d

Study Guide to Crack GIAC Red Team Professional GRTP Exam:

- Getting details of the GRTP syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the GRTP exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the GIAC provided training for GRTP exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the GRTP sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on GRTP practice tests is must. Continuous practice will make you an expert in all syllabus areas.