EDUSUM

#1 Online Certification Guide

GIAC GPEN

GIAC Penetration Tester Certification Questions & Answers

Exam Summary – Syllabus –Questions

GPEN

GIAC Penetration Tester (GPEN)

82-115 Questions Exam – 75% Cut Score – Duration of 82-115 minutes

Table of Contents:

Know Your GPEN Certification Well:

The GPEN is best suitable for candidates who want to gain knowledge in the GIAC Penetration Testing. Before you start your GPEN preparation you may struggle to get all the crucial Penetration Tester materials like GPEN syllabus, sample questions, study guide.

But don't worry the GPEN 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 GPEN syllabus?
- How many questions are there in the GPEN exam?
- Which Practice test would help me to pass the GPEN exam at the first attempt?

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

GIAC GPEN Penetration Tester Certification Details:

Exam Name	GIAC Penetration Tester (GPEN)
Exam Code	GPEN
Exam Price	$2499 (USD)
Duration	180 mins
Number of Questions	82-115
Passing Score	75%
Schedule Exam	**Pearson VUE**
Sample Questions	**GIAC GPEN Sample Questions**
Practice Exam	**GIAC GPEN Certification Practice Exam**

GPEN Syllabus:

Topic	Details
Advanced Password Attacks	- The candidate will be able to use additional methods to attack password hashes and authenticate.
Attacking Password Hashes	- The candidate will be able to obtain and attack password hashes and other password representations.
Domain Escalation and Persistence Attacks	- The candidate will demonstrate an understanding of common Windows privilege escalation attacks and Kerberos attack techniques that are used to consolidate and persist administrative access to Active Directory.
Escalation and Exploitation	- The candidate will be able to demonstrate the fundamental concepts of exploitation, data exfiltration from compromised hosts and pivoting to exploit other hosts within a target network.
Exploitation Fundamentals	- The candidate will be able to demonstrate the fundamental concepts associated with the exploitation phase of a pentest.
Kerberos Attacks	- The candidate will demonstrate an understanding of attacks against Active Directory including Kerberos attacks.
Metasploit	- The candidate will be able to use and configure the Metasploit Framework at an intermediate level.
Moving Files with Exploits	- The candidate will be able to use exploits to move files between remote systems.
Password Attacks	- The candidate will understand types of password attacks, formats, defenses, and the circumstances under which to use each password attack variation. The candidate will be able to conduct password guessing attacks.
Password Formats and Hashes	- The candidate will demonstrate an understanding of common password hashes and formats for storing password data.
Penetration Test Planning	- The candidate will be able to demonstrate the fundamental concepts associated with pen-testing, and utilize a process-oriented approach to penetration testing and reporting.
Penetration Testing with PowerShell and the Windows Command Line	- The candidate will demonstrate an understanding of the use of advanced Windows command line skills during a penetration test, and demonstrate an understanding of the use of advanced Windows Power Shell skills during a penetration test.
Reconnaissance	- The candidate will understand the fundamental concepts of reconnaissance and will understand how to obtain basic, high level information about the target organization and network, often considered information leakage, including but not limited to technical and non technical

Topic	Details
	public contacts, IP address ranges, document formats, and supported systems.
Scanning and Host Discovery	- The candidate will be able to use the appropriate technique to scan a network for potential targets, and to conduct port, operating system and service version scans and analyze the results.
Vulnerability Scanning	- The candidate will be able to conduct vulnerability scans and analyze the results.
Web Application Injection Attacks	- The candidate will demonstrate an understanding of how injection attacks work against web applications and how to conduct them.
Web Application Reconnaisance	- The candidate will demonstrate an understanding of the use of tools and proxies to discover web application vulnerabilities.

GIAC GPEN Sample Questions:

Question: 1

Which two key elements will help to properly scope a penetration test?

a) Areas of concern
b) Rules of engagement
c) Statement of work
d) Type of test
e) Status meetings

Answer: a, d

Question: 2

Which of the following protocols can offer a secure transport mechanism for delivering the report to the customer?

(Select all that apply.)

a) HTTP
b) SFTP
c) FTP
d) HTTPS

Answer: b, d

Question: 3

During a web application penetration test, you find a possible blind SQL injection point in a form. You are limited in

time and need an automated way of gathering data from the back-end database. Which tool can help you accomplish this task?

a) sqldump
b) masscan
c) sqlmap
d) dbmapper

Answer: c

Question: 4

In a meterpreter session, which of the following commands dumps the keystroke buffer from a Windows 7 target?

a) keyscan_dump
b) keyboard_send
c) keyevent
d) keyscan_stop

Answer: a

Question: 5

From a computer security perspective, which of the following are benefits of password hashing with a salt value?

(Select all that apply.)

a) No two users will have the same password.
b) Confidentiality of the password is ensured.
c) No two users will have the same password hash.
d) The password cannot be cracked.

Answer: b, c

Question: 6

_____ is the process of researching, collecting, and analyzing data that is available from public or open sources of information.

a) Active scanning
b) Fingerprinting
c) OSINT gathering
d) Web scraping

Answer: c

Question: 7

You want to start capturing a target user's clipboard activity on a Windows target. Which Metasploit extension will you

need to load inside your meterpreter session in order to make use of the clipboard commands?

a) load kiwi
b) load clipboard
c) load extapi
d) load clipbrd

Answer: c

Question: 8

Which two commands can you use on a Windows system to list known Layer 2 addresses?

a) arp --all-neighbors
b) arp -a
c) Get-NetNeighbor
d) Get-ArpNeighbor

Answer: b, c

Question: 9

NTLM offers a family of security protocols that can provide which of the following for authenticating users and computers based on a challenge-response mechanism? (Select all that apply.)

a) Integrity
b) Authentication
c) Confidentiality
d) All of the above

Answer: d

Question: 10

You are running the SharpHound ingestor with the Default collection method. Which of the following sets of data will not be collected? (Select all that apply.)

a) Session information
b) RDP information
c) DCOM data
d) Group membership
e) Domain trust information

Answer: b, c

Study Guide to Crack GIAC Penetration Tester GPEN Exam:

- Getting details of the GPEN 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 GPEN 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 GPEN 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 GPEN 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 GPEN practice tests is must. Continuous practice will make you an expert in all syllabus areas.