GIAC Penetration Tester (GPEN)

The topic areas for each exam part follow:

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 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.