PEN-300: Advanced Evasion Techniques and Breaching Defenses

Duration: **90 Days**

Course Description:

Building on the skills acquired in PEN-200, OffSec's PEN-300 course explores advanced penetration testing techniques against hardened targets. Learners gain hands-on experience bypassing security defenses and crafting custom exploits in real-world scenarios, enhancing their expertise in ethical hacking and vulnerability assessment.

This self-paced course culminates in a challenging exam, leading to the OffSec Experienced Penetration Tester (OSEP) certification. Achieving the OSEP certification distinguishes professionals with advanced penetration testing skills, making them highly sought-after experts in securing organizations from sophisticated threats.

Course Outlines:

Operating System and Programming Theory

- This comprehensive module provides a deep understanding of the inner workings of operating systems and fundamental programming concepts. You'll study memory management, process scheduling, file systems, and other essential OS components, gaining a solid foundation for understanding and exploiting vulnerabilities.

Client-Side Code Execution with Office

- This module focuses on leveraging known vulnerabilities in Microsoft Office applications (Word, Excel, PowerPoint) to craft malicious documents that trigger code execution on a victim's machine, gaining unauthorized access and control.

Client-Side Code Execution with Jscript

- Learn how to exploit Jscript, a scripting language used in Windows environments, for code execution attacks, gaining unauthorized access and control on a victim's machine.

Process Injection and Migration

- In this module, you'll master the art of stealth and persistence by injecting your malicious code into legitimate running processes. You'll also learn how to migrate between processes to evade detection and maintain control even if one process is terminated.

Introduction to Antivirus Evasion

- This module introduces basic techniques to bypass or evade antivirus software, such as obfuscation and packing, allowing you to create malware that goes undetected.

Advanced Antivirus Evasion

- Learn more sophisticated methods like signature-based and heuristic-based evasion, enabling you to create malware that goes undetected by even the most sophisticated antivirus solutions.

Application Whitelisting

- Learn how to circumvent application whitelisting, a security measure that restricts the execution of unauthorized software.

Bypassing Network Filters

- Discover various techniques to bypass network filters and firewalls, gaining access to restricted resources and networks.

Linux post-exploitation

- This module covers a wide range of techniques for maintaining access and escalating privileges on compromised Linux systems. You'll learn how to navigate file systems, manipulate user accounts, extract sensitive information, and establish persistent backdoors for future access.

Windows post-exploitation

- Learn various techniques for maintaining access and escalating privileges on compromised Windows systems, including navigating file systems, manipulating user accounts, extracting sensitive information, and establishing persistent backdoors.