OffSec

PEN-300 OSEP

Evasion Techniques and Breaching Defenses

PEN-300 is an advanced course for penetration testers, building on the skills and techniques learned within PEN-200. This course explores advanced penetration testing techniques against hardened targets in mature organizations with an established security function. Within this course, you will go beyond the use of existing tools and skills and be encouraged to develop new techniques and tools. By taking on this course, learners will be proving their advanced phishing skills, advanced antivirus evasion tactics, and establishing attack vectors that leverage or disclose Windows credentials.

Operating System and Programming Theory	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	Focus on leveraging known vulnerabilities in Microsoft Office applications to craft malicious documents that trigger code execution on a victim's machine, gaining unauthorized access and control
Client-Side Code Execution with Jscript	Exploit Jscript for code execution attacks, gaining unauthorized access and control of machines in Windows environments
Process Injection and Migration	Master the art of stealth and persistence by injecting malicious code into legitimate running processes, migrating between processes to evade detection and maintain control when processes are terminated
Introduction to Antivirus Evasion	Create malware that goes undetected with basic techniques like obfuscation and packing to bypass and evade antivirus software
Advanced Antivirus Evasion	Use advanced methods like signature-based and heuristic-based evasion to create malware that goes undetected by complex antivirus solutions
Application Whitelisting	Bypass security measures intended to restrict the execution of unauthorized software
Bypassing Network Filters	Gain access to restricted resources and networks with different techniques for bypassing network filters and firewalls
Linux Post Exploitation	Navigate file systems, manipulate user accounts, extract sensitive information, and establish persistent backdoors on compromised Linux systems
Windows Post Exploitation	Navigate file systems, manipulate user accounts, extract sensitive information, and establish persistent backdoors on compromised Windows systems
Kiosk Breakouts	Break out of restricted kiosk environments like ATMs or point-of-sale terminals to gain control of their operating systems

Windows Credentials	Use different methods and techniques to extract valuable credentials like passwords and hashes from Windows systems
Windows Lateral Movement	Exploit trust relationships, leverage vulnerabilities in services and protocols with tools like PsExec and Mimikatz to gain access to systems throughout a compromised Windows network
Linux Lateral Movement	Exploit trust relationships, leverage vulnerabilities in services and protocols to gain access to systems throughout a compromised Linux network
Microsoft SQL Attacks	Attack vulnerabilities in Microsoft SQL Server databases to extract sensitive data, escalate privileges, and gain control over entire systems
Active Directory Exploitation	Exploit vulnerabilities in Active Directory to compromise domains in Windows networks
Combining the Pieces	Combine multiple exploits, techniques, and tools to create complex, multi-stage attacks to bypass multiple layers of security
Trying Harder	Apply your knowledge and skills in challenging, real-world scenarios with complex network environments, hardened security measures, and realistic attack scenarios