PEN-300: Advanced Evasion Techniques and Breaching Defenses (OSEP)

Course Overview

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 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.

Prerequisites

While there are no formal certification prerequisites, a strong understanding of operating systems, networking, and scripting (e.g., Python, Bash) is highly recommended. Additionally, familiarity with the concepts and techniques covered in PEN-200 (Penetration Testing with Kali Linux) is highly recommended for success in this course.

Target Audience

- Web Penetration Testers
- Pentesters
- Web Application Developers
- Application Security Analysts
- Application Security Architects
- SOC Analysts
- Blue team members

Course Objectives

Upon completing PEN-300 and successfully passing the OSEP exam, you'll have mastered advanced penetration testing skills, including:

- In-depth vulnerability analysis and exploitation
- Custom exploit development
- Bypassing modern security defenses
- Exploiting authentication and authorization flaws
- Attacking Active Directory and cloud environments
- Post-exploitation techniques for maintaining access and escalating privileges

Duration

5 Days

Certifications

OSEP

Contact Us

☎ 800.674.3550

📍 2151 W. Hillsboro Blvd.
Suite 210
Deerfield Beach, FL 33442

Connect with us

APPLIED TECHNOLOGY ACADEMY

Sign Up Today!

AppliedTechnologyAcademy.com

PEN-300: Advanced Evasion Techniques and Breaching Defenses (OSEP)

Course Outline

Evasion Techniques and Breaching Defenses: General Course Information

- About the PEN-300 Course
- Provided Material
- Overall Strategies for Approaching the Course
- About the PEN-300 VPN Labs
- About the OSEP Exam

Operating System and Programming Theory

- Programming Theory
- Operating System and Programming Theory
- Client-Side Code Execution with Office

Client-Side Code Execution with Office

- Will You Be My Dropper
- Phishing with Microsoft Office
- Keeping Up Appearances
- Executing Shellcode in Word Memory
- PowerShell Shellcode Runner
- Keep That PowerShell in Memory
- Talking to the Proxy

Client-Side Code Execution with Windows Script Host

- Creating a Basic Dropper in JScript
- JScript and C#
- In-memory PowerShell Revisited

Process Injection and Migration

- Finding a Home for Our Shellcode
- DLL Injection
- Reflective DLL Injection
- Process Hollowing

Introduction to Antivirus Evasion

- Antivirus Software Overview
- Simulating the Target Environment
- Locating Signatures in Files
- Bypassing Antivirus with Metasploit
- Bypassing Antivirus with C#
- Messing with Our Behavior
- Office Please Bypass Antivirus
- Hiding PowerShell Inside VBA

Advanced Antivirus Evasion

- Intel Architecture and Windows 10
- Antimalware Scan Interface
- Bypassing AMSI With Reflection in PowerShell
- Wrecking AMSI in PowerShell
- UAC Bypass vs Microsoft Defender
- Bypassing AMSI in JScript

Application Whitelisting

- Application Whitelisting Theory and Setup
- Basic Bypasses
- Bypassing AppLocker with PowerShell
- Bypassing AppLocker with C#
- Bypassing AppLocker with JScript

Bypassing Network Filters

- DNS Filters
- Web Proxies
- IDS and IPS Sensors
- Full Packet Capture Devices
- HTTPS Inspection
- Domain Fronting
- DNS Tunneling

Linux Post-Exploitation

- User Configuration Files
- Bypassing AV
- Shared Libraries

Kiosk Breakouts

- Kiosk Enumeration
- Command Execution
- Post-Exploitation
- Privilege Escalation
- Windows Kiosk Breakout Techniques

Windows Credentials

- Local Windows Credentials
- Access Tokens
- 3 Kerberos and Domain Credentials
- Processing Credentials Offline

Windows Lateral Movement

- Remote Desktop Protocol
- Fileless Lateral Movement

Linux Lateral Movement

- Lateral Movement with SSH
- DevOps
- Kerberos on Linux

Microsoft SQL Attacks

- MS SQL in Active Directory
- MS SQL Escalation
- Linked SQL Servers

Active Directory Exploitation

- AD Object Security Permissions
- Kerberos Delegation
- Active Directory Forest Theory
- Burning Down the Forest
- Going Beyond the Forest
- Compromising an Additional Forest

Combining the Pieces

- Enumeration and Shell
- Attacking Delegation
- Owning the Domain

Trying Harder: The Labs

- Real Life Simulations
- Wrapping Up