Training: OffSec

# OffSec PEN-300 Advanced Evasion Techniques and Breaching Defenses

OffSec Learning Partner

## TRAINING GOALS:

Evasion Techniques and Breaching Defenses (PEN-300) is an advanced penetration testing course. Learners who complete the course and pass the exam will earn the OffSec Experienced Pentester (OSEP) certification. This course builds on the knowledge and techniques taught in Penetration Testing with Kali Linux, teaching learners to perform advanced penetration tests against mature organizations with an established security function and focuses on bypassing security mechanisms that are designed to block attacks. The OSEP is one of three certifications making up the OSCE³ certification along with the OSWE for advanced web attacks and OSED for exploit development.

### Benefits

- Follow up to PEN-200 (PWK)
- Covers evasion and breaching techniques in greater depth
- Prepares learners for real-life Penetration Testing field work

### Who is this course for?

- PEN-300 is an advanced course designed for OSCP-level penetration testers who want to develop their skills against hardened systems
- Job roles like senior penetration tester, security researcher, application penetration tester, and any software developer working on security products could benefit from the course

### Exam

- The PEN-300 course and online lab prepares you for the OSEP certification
- 48-hour exam
- Proctored
- Learn more about the exam https://help.offensive-security.com/hc/en-us/articles/360049781352-OSEP-Exam-FAQ



Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

What competencies will you gain?

- Preparation for more advanced Penetration Testing field work
- Knowledge of breaching network perimeter defenses through client-side attacks, evading antivirus and allow-listing technologies
- How to customize advanced attacks and chain them together

## CONSPECT:

- Evasion Techniques and Breaching Defenses: General Course Information
  - About The PEN300 Course
  - Provided Material
  - Overall Strategies for Approaching the Course
  - About the PEN300 VPN Labs
  - About the OSEP Exam
  - Wrapping Up
- 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
  - Wrapping Up
- Client Side Code Execution With Windows Script Host
  - Creating a Basic Dropper in Jscript
  - Jscript and C#
  - In-memory PowerShell Revisited
  - Wrapping Up
- Process Injection and Migration
  - Finding a Home for Our Shellcode



Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- DLL Injection
- Reflective DLL Injection
- Process Hollowing
- Wrapping Up

- 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
  - Wrapping Up
- 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
  - Wrapping Up
- Application Whitelisting
  - Application Whitelisting Theory and Setup
  - Basic Bypasses
  - Bypassing AppLocker with PowerShell
  - Bypassing AppLocker with C#
  - Bypassing AppLocker with JScript
  - Wrapping Up
- Bypassing Network Filters
  - DNS Filters
  - Web Proxies
  - IDS and IPS Sensors
  - Full Packet Capture Devices
  - HTTPS Inspection
  - Domain Fronting



Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- DNS Tunneling
- Wrapping Up

- Linux Post-Exploitation
  - User Configuration Files
  - Bypassing AV
  - Shared Libraries
  - Wrapping Up
- Kiosk Breakouts
  - Kiosk Enumeration
  - Command Execution
  - Post-Exploitation
  - Privilege Escalation
  - Windows Kiosk Breakout Techniques
  - Wrapping Up
- Windows Credentials
  - Local Windows Credentials
  - Access Tokens
  - 3 Kerberos and Domain Credentials
  - Processing Credentials Offline
  - Wrapping Up
- Windows Lateral Movement
  - Remote Desktop Protocol
  - Fileless Lateral Movement
  - Wrapping Up
- Linux Lateral Movement
  - Lateral Movement with SSH
  - DevOps
  - Kerberos on Linux
  - Wrapping Up
- Microsoft SQL Attacks
  - MS SQL in Active Directory
  - MS SQL Escalation
  - Linked SQL Servers
  - Wrapping Up
- Active Directory Exploitation
  - AD Object Security Permissions



Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Kerberos Delegation
- Active Directory Forest Theory
- Burning Down the Forest
- Going Beyond the Forest
- Compromising an Additional Forest
- Wrapping Up

- Combining the Pieces
  - Enumeration and Shell
  - Attacking Delegation
  - Owning the Domain
  - Wrapping Up
- Trying Harder: The Labs
  - Real Life Simulations
  - Wrapping Up

## REQUIREMENTS:

All learners are required to have completed or have the equivalent knowledge corresponding to PEN-200 Penetration Testing with Kali Linux. Especially:

- Solid ability in enumerating targets to identify vulnerabilities
- The ability to identify and exploit vulnerabilities like SQL injection, file inclusion, and local privilege escalation
- A foundational understanding of Active Directory and knowledge of basic AD attacks

## Difficulty level

## CERTIFICATE:

After passing the OSEP exam, candidates receive a title of OffSec Experienced Pentester (OSEP).

## TRAINER:

Authorized OffSec Trainer



Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

## ADDITIONAL INFORMATION:

Course is available as the e-learning product, in two subscription's models:

- Course & Cert Exam Bundle
- Learn One



Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007