# OffSec PEN-300 (OSEP) Training

Duration: **5 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

## Overview

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 organisations 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 $OSCE^3$ certification along with the OSWE for advanced web attacks and OSED for exploit development.

## Prerequisites

- 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

## What You Will Learn

- Bypass defences
- Perform advanced attacks while avoiding detection
- Compromise systems configured with security in mind
- Those who complete the course and pass the 48-hour exam earn the Offensive Security Experienced Penetration Tester (OSEP) certification
- Preparation for more advanced field work
- Knowledge of breaching network perimeter defences through client-side attacks, evading antivirus and allow-listing technologies
- How to customise advanced attacks and chain them together

**About the Exam**

- The PEN-300 course and online lab prepares you for the OSEP certification
- 48-hour exam
- Proctored

## Outline

**Module 1 - Operating System and Programming Theory**

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

# OffSec PEN-300 (OSEP) Training

Duration: **5 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

**Module 2 - 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

**Module 3 - Client Side Code Execution With Windows Script Host**

- Creating a Basic Dropper in Jscript
- Jscript and C#
- In-memory PowerShell Revisited
- Wrapping Up

**Module 4 - Process Injection and Migration**

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

**Module 5 - 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 Behaviour
- Office Please Bypass Antivirus
- Hiding PowerShell Inside VBA
- Wrapping Up

**Module 6 - 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

**Module 7 - Application Whitelisting**

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

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com


- Bypassing AppLocker with JScript
- Wrapping Up

**Module 9 - Bypassing Network Filters**

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

**Module 10 - Linux Post-Exploitation**

- User Configuration Files
- Bypassing AV
- Shared Libraries
- Wrapping Up

**Module 11 - Kiosk Breakouts**

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

**Module 12 - Windows Credentials**

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

**Module 13 - Windows Lateral Movement**

- Remote Desktop Protocol
- Fileless Lateral Movement
- Wrapping Up

**Module 14 - Linux Lateral Movement**

- Lateral Movement with SSH
- DevOps
- Kerberos on Linux
- Wrapping Up

**Module 15 - Microsoft SQL Attacks**

- MS SQL in Active Directory

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com


- MS SQL Escalation
- Linked SQL Servers
- Wrapping Up

**Module 16 - 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
- Wrapping Up

**Module 17 - Combining the Pieces**

- Enumeration and Shell
- Attacking Delegation
- Owning the Domain
- Wrapping Up

**Module 18 Trying Harder: The Labs**

- Real Life Simulations
- Wrapping Up