APPLIED TECHNOLOGY ACADEMY

800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

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

OffSec Authorized Training · Applied Technology Academy

We are a premier provider of PEN-300 OffSec OSEP Training. PEN-300 teaches the skills necessary to bypass many different types of defenses while performing advanced attacks that avoid detection. Students who complete the course and pass the exam earn the OffSec Experienced Penetration Tester (OSEP) certification, demonstrating their ability to perform advanced penetration tests against mature organizations.

LEVEL	DURATION	EXPERIENCE	AVERAGE SALARY	LABS
Advanced	**5 Days**	**3 years: Offensive Security**	**$119,895**	**Yes**

Course Overview

PEN-300 builds on the knowledge and techniques taught in PEN-200, teaching learners to perform advanced penetration tests against mature organizations with an established security function and bypassing security mechanisms that are designed to block attacks.

This is an advanced-level course designed for OSCP-level penetration testers who want to develop their skills against hardened systems and for job roles such as senior penetration tester, security researcher, application penetration tester, and any software developer working on security products.

Learners who complete the course and pass the exam earn the OffSec Experienced Penetration Tester (OSEP) certification and are prepared for more advanced penetration testing fieldwork.

- Evasion techniques and Breaching Defenses: General Course Information
- Operating System and Programming Theory
- Phishing with Microsoft Office
- Phishing with Calendars
- Phishing with Jscript
- Reflective PowerShell
- Reflective Code Execution in Client Side Attacks
- Process Injection and Migration
- Introduction to Antivirus Evasion
- Advanced Antivirus Evasion
- Application Whitelisting
- Bypassing Network Filters
- Linux Post-Exploitation

800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

- Kiosk Breakouts
- Windows Credentials
- Windows Lateral Movement
- Linus Lateral Movement
- Microsoft SQL Attacks
- Active Directory Exploitation
- Attacking Active Directory
- Combining the Pieces
- Trying Harder: The Labs

Course Outline

- **Lesson 1: Evasion Techniques and Breaching Defenses: General Course Information**
- **Lesson 2: Operating System and Programming Theory**
- **Lesson 3: Phishing with Microsoft Office**
- **Lesson 4: Phishing with Calendars**
- **Lesson 5: Phishing with Jscript**
- **Lesson 6: Reflective PowerShell**
- **Lesson 7: Reflective Code Execution in Client Side Attacks**
- **Lesson 8: Process Injection and Migration**
- **Lesson 9: Introduction to Antivirus Evasion**
- **Lesson 10: Advanced Antivirus Evasion**
- **Lesson 11: Application Whitelisting**
- **Lesson 12: Bypassing Network Filters**
- **Lesson 13: Linux Post-Exploitation**
- **Lesson 14: Kiosk Breakouts**
- **Lesson 15: Windows Credentials**
- **Lesson 16: Windows Lateral Movement**
- **Lesson 17: Linux Lateral Movement**
- **Lesson 18: Microsoft SQL Attacks**
- **Lesson 19: Active Directory Exploitation**
- **Lesson 20: Attacking Active Directory**
- **Lesson 21: Combining the Pieces**
- **Lesson 22: Trying Harder: The Labs**

800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

Intended Audience

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

Prerequisites

We strongly suggest that students taking PEN-300 have either taken PWK and passed the OSCP certification or have equivalent knowledge and skills in the following areas:

- Working familiarity with Kali Linux command line
- Solid ability run enumerating targets to identify vulnerabilities
- Basic scripting abilities in Bash, Python and PowerShell
- Identifying and exploiting vulnerabilities like SQL injection, file inclusion and local privilege escalation
- Foundational understanding of Active Directory and knowledge of basic AD attacks
- Familiarity with C# programming is a plus

Follow-On Courses

- Advanced Web Attacks with Kali Linux (WEB-200)
- Advanced Web Attacks with Exploitation (WEB-300)

Features

Also available in On-Demand formats below:

- Learn One Package – $2,749
- 1 year of access to the course of your choice
- 2 exam attempts during your subscription
- 365 days of lab access
- Access to all 100-level content for 1 year
- 1 year of unlimited access to all fundamental content and OffSec curated Learning Paths
- PEN-103 + 1 KLCP exam attempt
- PEN-210 + 1 OSWP exam attempt
- Proving Grounds Practice labs
- Learn More
- OR
- Learn Unlimited Package – $6,099

- 1 year of access to unlimited course & content
- Unlimited exam attempts during your subscription
- 365 days of lab access
- 1 year of unlimited access to all fundamental content and OffSec curated Learning Paths
- Access to all 100-level content for 1 year
- PEN-103 + unlimited KLCP exam attempts
- PEN-210 + unlimited OSWP exam attempts
- Proving Grounds Practice labs
- 3 downloads of course material
- Learn More

Ready to enroll? Call 800.674.3550 or email Info@AppliedTechAc.com — private team cohorts, GSA MAS purchasing, military credentialing funding, VA GI Bill and VR&E and student financing available.