APPLIED TECHNOLOGY ACADEMY

800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

OffSec Windows User Mode Exploit Development EXP-301 (OSED) Training

OffSec Authorized Training · Applied Technology Academy

Invest in a secure future with offensive security training from the developers of Kali Linux. OffSec certifications are the most well-recognized and respected in the industry. Our courses focus on real-world skills and applicability, preparing you for real-life challenges and offensive security expertise!

LEVEL	DURATION	EXPERIENCE	AVERAGE SALARY	LABS
Intermediate	**5 Days**	**2 years: Debuggers/ Python**	**$127,000**	**Yes**

Course Overview

EXP-301 is an intermediate course that teaches the skills necessary to bypass DEP and ASLR security mitigations, create advanced custom ROP chains, reverse-engineer a network protocol and even create read and write primitives by exploiting format string specifiers.

Windows User Mode Exploit Development (EXP-301) is a course that teaches learners the basics of modern exploit development. Despite being a fundamental course, it is at the 300 level because it relies on substantial knowledge of assembly and low level programming. It begins with basic buffer overflow attacks and builds into learning the skills needed to crack the critical security mitigations protecting enterprises. Learners who complete the course and pass the exam earn the OffSec Exploit Developer (OSED) certification. The OSED is one of three certifications making up the OSCE3 certification along with the OSEP for advanced penetration testing and OSWE for web application security. Course Objectives:

- Learn the fundamentals of reverse engineering
- Create custom exploits
- Develop the skills to bypass security mitigations
- Write handmade Windows shellcode
- Adapt older techniques to more modern versions of Windows

Course Outline

- **Lesson 1: Windows User Mode Exploit Development: General Course Information**
  - About the EXP301 Course
  - Provided Materials
  - Overall Strategies for Approaching the Course
  - About the EXP301 VPN Labs
  - About the OSED Exam

800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

  - Wrapping Up
- **Lesson 2: WinDbg and x86 Architecture**
  - Introduction to x86 Architecture
  - Introduction to Windows Debugger
  - Accessing and Manipulating Memory from WinDbg
  - Controlling the Program Execution in WinDbg
  - Additional WinDbg Features
  - Wrapping Up
- **Lesson 3: Exploiting Stack Overflows**
  - Stack Overflows Introduction
  - Installing the Sync Breeze Application
  - Crashing the Sync Breeze Application
  - Win32 Buffer Overflow Exploitation
  - Wrapping Up
- **Lesson 4: Exploiting SEH Overflows**
  - Installing the Sync Breeze Application
  - Crashing Sync Breeze
  - Analyzing the Crash in WinDbg
  - Introduction to Structured Exception Handling
  - Structured Exception Handler
  - Overflows
  - Wrapping Up
- **Lesson 5: Introduction to IDA Pro**
  - IDA Pro 101
  - Working with IDA Pro
  - Wrapping Up
- **Lesson 6: Overcoming Space Restrictions: Egghunters**
  - Crashing the Savant Web Server
  - Analyzing the Crash in WinDbg
  - Detecting Bad Characters
  - Gaining Code Execution
  - Finding Alternative Places to Store
  - Large Buffers
  - Finding our Buffer - The Egghunter
  - Approach
  - Improving the Egghunter Portability Using SEH
  - Wrapping Up

800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

- **Lesson 7: Creating Custom Shellcode**
  - Calling Conventions on x86
  - The System Call Problem
  - Finding kernel32.dll
  - Resolving Symbols
  - NULLFree Position-Independent Shellcode PIC
  - Reverse Shell
  - Wrapping Up
- **Lesson 8: Reverse Engineering for Bugs**
  - Installation and Enumeration
  - Interacting with Tivoli Storage
  - Manager
  - Reverse Engineering the Protocol
  - Digging Deeper to Find More Bugs
  - Wrapping Up
- **Lesson 9: Stack Overflows and DEP Bypass**
  - Data Execution Prevention
  - Return Oriented Programming
  - Gadget Selection
  - Bypassing DEP
  - Wrapping Up
- **Lesson 10: Stack Overflows and ASLR Bypass**
  - ASLR Introduction
  - Finding Hidden Gems
  - Expanding our Exploit ASLR Bypass)
  - Bypassing DEP with WriteProcessMemory
  - Wrapping Up
- **Lesson 11: Format String Specifier Attack Part I**
  - Format String Attacks
  - Attacking IBM Tivoli FastBackServer
  - Reading the Event Log
  - Bypassing ASLR with Format Strings
- **Lesson 12: Format String Specifier Attack Part II**
  - Write Primitive with Format Strings
  - Overwriting EIP with Format Strings
  - Locating Storage Space
  - Getting Code Execution

800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

  - Wrapping Up
- **Lesson 13: Trying Harder: The Labs**
  - Challenge 1
  - Challenge 2
  - Challenge 3
  - Wrapping Up

Intended Audience

Windows User Mode Exploit Development is an intermediate course designed for those who want to learn about exploit development skills

Job roles like penetration testers, exploit developers, security researchers, Malware analysts, and software developers working on security products, could benefit from the course

- Job Roles
- Penetration Testers
- Exploit Developers
- Security Researchers
- Malware Analysts
- Software Developers Working On Security Products

Prerequisites

All students should have the following prerequisite skills before starting the course:

- Familiarity with debuggers (ImmunityDBG, OllyDBG)
- Familiarity with basic exploitation concepts on 32-bit
- Familiarity with writing Python 3 code
- The following optional skills are recommended: Ability to read and understand C code at a basic level
- Ability to read and understand 32-bit Assembly code at a basic level
- *The prerequisite skills can be obtained by taking our Penetration Testing with Kali Linux course.

Follow-On Courses

- EXP-312: Advanced macOS Control Bypasses
- EXP-401: Advanced Windows Exploitation

Features

- Course Materials
- Active Student Forums

- Access to Home Lab Setup
- Learn One Package – $2,749
- One course
- 365 days of lab access
- Two exam attempts
- Plus exclusive content
- OR
- Learn Unlimited Package – $6,099
- All courses
- 365 days of lab access
- Unlimited exam attempts
- Plus exclusive content

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.