APPLIED TECHNOLOGY ACADEMY

800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

# OffSec Advanced Windows Exploitation EXP-401 (OSEE) Training

**OffSec Authorized Training · Applied Technology Academy**

We are a premier provider of EXP-401 Offensive Security OSEE Training. Modern exploits for Windows-based platforms require modern bypass methods to circumvent Microsoft's defenses. In Advanced Windows Exploitation, our expert instructors will challenge students to develop creative solutions that work in today's increasingly difficult exploitation environment.

| LEVEL | DURATION | EXPERIENCE | AVERAGE SALARY | LABS |
|---|---|---|---|---|
| **Advanced** | **5 Days** | **4 years: Advanced Windows Exploitation** | **$120,634** | **Yes** |

## Course Overview

The OSEE is the most difficult exploit development certification you can earn. We recommend completing the 300- level certifications before registering for this course.

Students who complete EXP-401 and pass the exam will earn the Offensive Security Exploitation Expert (OSEE) certification. The OSEE exam assesses not only the course content, but also the ability to think laterally and adapt to new challenges.

The virtual lab environment has a limited number of target systems. The software within contains specific, unknown vulnerabilities. Students have 72 hours to develop and document exploits. The exam requires a stable, high-speed internet connection.

You must submit a comprehensive penetration test report as part of the exam. It should contain in-depth notes and screenshots detailing the steps taken and the exploit methods used.

- Custom Shellcode Creation
- Writing Exploit Code
- Shellcode Framework Creation
- Reverse Shell
- VMware Workstation Guest-To-Host Escape
- Data Execution Prevention (DEP)
- VMware Workstation Guest-To-Host Escape
- Driver Callback Overwrite
- Address Space Layout Randomization
- VMware Workstation Internals
- The Windows Heap Memory Manager

800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

- Low Fragmentation Heap
- Restoring the Execution Flow
- Windows Defender Exploit Guard
- ROP Mitigations
- Unsanitized User-mode Callback
- Course Materials
- Active Student Forums
- Access to Home Lab Setup

## Course Outline

- **Lesson 1: Introduction**
- **Lesson 2: Custom Shellcode Creation**
- **Lesson 3: VMware Workstation Guest-To-Host Escape**
- **Lesson 4: Microsoft Edge Type Confusion**
- **Lesson 5: Driver Callback Overwrite**
- **Lesson 6: Unsanitized User-mode Callback**

## Intended Audience

Advanced Windows Exploitation is NOT an entry level course. We expect students to have previous exploitation experience in a Windows environment and understand their way around a debugger. This is the hardest course Offensive Security offers.

## Prerequisites

All students are required to have:

Experience in developing windows exploits and understand how to operate a debugger. Familiarity with WinDBG, x86_64 assembly, IDA Pro and basic C/C++ programming is highly recommended. A willingness to work and put in real effort will greatly help students succeed in this security training course.

A laptop that is able to run three VMs with ease. Please do not bring netbooks or other low-resolution systems. The only supported host operating system is Windows 10.

- VMware Workstation 15 or higher
- 64-bit CPU with a minimum of 4 cores along with support for NX, SMEP, VT-d/IOMMU and VT-x/EPT
- At least 160 GB HD free
- At least 16 GB of RAM

## Features

Our EXP-401 course includes:

- Instructor-Led Training with our advanced practitioner instructor team.
- Comprehensive EXP-401 Courseware Binder with all of the most recent course updates!
- All of the EXP-401 VMs to help launch you in to execution!
- An OSEE Exam Voucher

**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.