Training: OffSec
OffSec EXP-301 Windows User Mode Exploit Development

TRAINING GOALS:

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.

Benefits

Learners will:

- 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

Who is this course for?

- 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

Exam

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

- The EXP-301 course and online lab prepares you for the OSED certification
- 48-hour exam
- Proctored
- Learn more about the exam https://help.offsec.com/hc/en-us/articles/360052977212-EXP-301-Windows-User-Mode-Exploit-Development-OSED-Exam-Guide

What competencies will you gain?

- Using WinDbg
- Writing your own shellcode
- Bypassing basic security mitigations, including DEP and ASLR
- Exploiting format string specifiers
- The necessary foundations for finding bugs in binary applications to create custom exploits

CONSPECT:

- 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
  - Wrapping Up
- 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
- Exploiting Stack Overflows
  - Stack Overflows Introduction
  - Installing the Sync Breeze Application
  - Crashing the Sync Breeze Application
  - Win32 Buffer Overflow Exploitation

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

- Wrapping Up
- Exploiting SHE 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
- Introduction to IDA Pro
  - IDA Pro 101
  - Working with IDA Pro
  - Wrapping Up
- 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
- 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
- Reverse Engineering for Bugs
  - Installation and Enumeration
  - Interacting with Tivoli Storage Manager
  - Reverse Engineering the Protocol
  - Digging Deeper to Find More Bugs
  - Wrapping Up
- Stack Overflows and DEP Bypass

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

- Data Execution Prevention
- Return Oriented Programming
- Gadget Selection
- Bypassing DEP
- Wrapping Up

- Stack Overflows and ASLR Bypass
  - ASLR Introduction
  - Finding Hidden Gems
  - Expanding our Exploit ASLR Bypass)
  - Bypassing DEP with WriteProcessMemory
  - Wrapping Up
- Format String Specifier Attack Part I
  - Format String Attacks
  - Attacking IBM Tivoli FastBackServer
  - Reading the Event Log
  - Bypassing ASLR with Format Strings
  - Wrapping Up
- Format String Specifier Attack Part II
  - Write Primitive with Format Strings
  - Overwriting EIP with Format Strings
  - Locating Storage Space
  - Getting Code Execution
  - Wrapping Up
- Trying Harder: The Labs
  - Challenge 1
  - Challenge 2
  - Challenge 3
  - Wrapping Up

REQUIREMENTS:

All learners are required to have completed or have the equivalent knowledge corresponding to EXP-100 Exploit Development Essentials. Especially:

- Familiarity with debuggers (ImmunityDBG, OllyDBG)
- Familiarity with basic exploitation concepts on 32-bit
- Familiarity with writing Python 3 code

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

- Ability to read and understand C code at a basic level
- Ability to read and understand 32-bit Assembly code at a basic level

Difficulty level

CERTIFICATE:

After passing the OSED exam, candidates receive a title of OffSec Exploit Developer (OSED).

TRAINER:

Authorized OffSec Trainer

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