EXP-301 - Windows User Mode Exploit Development (WUMED/OSED)

Durée: 5 Jours **Réf de cours: GK840107** **Méthodes d'apprentissage: Intra-entreprise & sur-mesure**

Résumé:

OffSec's Windows User-Mode Exploit Development (EXP-301) course provides a comprehensive understanding of modern exploit development techniques. Learners gain hands-on experience crafting custom exploits and bypassing security defenses in an environment designed to elevate their skills in ethical hacking and vulnerability discovery.
Successful completion of the online training course and passing the associated exam earns the OffSec Exploit Developer (OSED) certification. This certification validates expertise in advanced exploit development techniques, including reverse engineering, writing shellcode, and bypassing modern mitigations, making certified professionals invaluable for identifying and addressing vulnerabilities in software applications.
Upd Apr2025

Company Events

These events can be delivered exclusively for your company at our locations or yours, specifically for your delegates and your needs. The Company Events can be tailored or standard course deliveries.

Public visé:

The EXP-301 course is ideal for individuals with a solid foundation in penetration testing and programming who are seeking to master exploit development techniques, ultimately earning the OSED certification.

Objectifs pédagogiques:

- Upon completing EXP-301 and passing the OSED exam, youll have mastered exploit development skills, including:
- In-depth vulnerability analysis and exploitation in Windows user-mode applications
- Custom exploit development for stack, heap, and integer overflows, as well as format string and use-after-free vulnerabilities
- Bypassing modern Windows security mitigations like DEP, ASLR, and CFG
- Writing reliable shellcode from scratch
- Reverse engineering to uncover vulnerabilities

Pré-requis:

While there are no formal prerequisites, a strong understanding of C programming, assembly language, operating system internals (Windows), and debugging tools (such as WinDbg and Immunity Debugger) is highly recommended.

Test et certification

Contenu:

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

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

Exploiting Stack Overflows

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

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

Introduction to IDA Pro

- IDA Pro 101
- Working with IDA Pro

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

Creating Custom Shellcode

- Calling Conventions on x86
- The System Call Problem
- Finding kernel32.dll
- Resolving Symbols
- NULLFree Position-Independent Shellcode PIC
- Reverse Shell

Reverse Engineering for Bugs

- Installation and Enumeration
- Interacting with Tivoli Storage Manager
- Reverse Engineering the Protocol
- Digging Deeper to Find More Bugs

Stack Overflows and DEP Bypass

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

Stack Overflows and ASLR Bypass

- ASLR Introduction
- Finding Hidden Gems
- Expanding our Exploit ASLR Bypass)
- Bypassing DEP with WriteProcessMemory

Format String Specifier Attack Part I

- Format String Attacks
- Attacking IBM Tivoli FastBackServer
- Reading the Event Log
- Bypassing ASLR with Format Strings

Format String Specifier Attack Part II

- Write Primitive with Format Strings
- Overwriting EIP with Format Strings
- Locating Storage Space
- Getting Code Execution

Trying Harder: The Labs

- Challenge 1
- Challenge 2
- Challenge 3

Méthodes pédagogiques :

Official course book provided to participants. Course materials in english

Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans