EXP-301: Windows User Mode Exploit Development

Duration: 90 Days

Course Description:

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 a self-paced 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.

Course Outlines:

WinDbg Tutorial

- Master the powerful WinDbg debugger to effectively analyze crashes, investigate memory dumps, and identify vulnerabilities in Windows applications.

Stack Buffer Overflows

- Understand the mechanics of stack buffer overflows and learn how to exploit them to gain control of vulnerable programs.

Exploiting SEH Overflows

- Delve into Structured Exception Handler (SEH) overflows, a specific type of buffer overflow, and master techniques to leverage them for code execution.

Intro to IDA Pro

- Familiarize yourself with IDA Pro, a leading disassembler and debugger, essential for reverse engineering software binaries and uncovering vulnerabilities.

Overcoming Space Restrictions

- Egghunters: Learn how to bypass space limitations in your exploit payloads by utilizing egghunter techniques to locate and execute shellcode.

Shellcode From Scratch

- Develop the skills to write your own custom shellcode, enabling you to perform specific actions on compromised systems.

Reverse-Engineering Bugs

- Learn how to systematically analyze software binaries to identify and understand vulnerabilities that can be exploited.

Stack Overflows and DEP/ASLR Bypass

- Master advanced techniques for exploiting stack overflows while bypassing modern security mitigations such as Data Execution Prevention (DEP) and Address Space Layout Randomization (ASLR).

Format String Specifier Attacks

- Understand and exploit format string vulnerabilities, which can be leveraged to read or write arbitrary memory locations.

Custom ROP Chains and ROP Payload Decoders

- Learn how to construct custom Return-Oriented Programming (ROP) chains to bypass security defenses and build ROP payload decoders for stealthy exploitation.