EXP-301 OSED

Windows User Mode Exploit Development

EXP-301 (Windows User Mode Exploit Development) is an intermediate course on modern exploit development techniques. Learners gain hands-on experience crafting custom exploits and bypassing security defenses designed to elevate their skills in ethical hacking and vulnerability discovery. It will also provide an introduction to reverse engineering binary applications to help locate vulnerabilities. Completion of this course will prove the learner's 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.

WinDbg Tutorial	Use WinDbg debugger to analyze crashes, investigate memory dumps, and find vulnerabilities in Windows applications
Stack Buffer Overflows	Exploit and gain control of vulnerable programs through stack buffer overflows
Exploiting SEH Overflows	Master techniques to leverage Structured Exception Handler overflows for code execution
Intro to IDA Pro	Reverse engineering software binaries and uncover vulnerabilities with a leading disassembler and debugger (IDA Pro)
Overcoming Space Restrictions	Bypass space limitations in your exploit payloads by locating and executing shellcode with egghunter techniques
Shellcode From Scratch	Perform specific actions on compromised systems by writing custom shellcode
Reverse Engineering Bugs	Identify exploitable vulnerabilities by systematically analysing software binaries
Stack Overflows and DEP/ASLR Bypass	Bypass modern security mitigations to exploit stack overflows using advanced techniques like Data Execution Prevention (DEP) and Address Space Layout Randomization (ASLR)
Format String Specifier Attacks	Exploit format string vulnerabilities and leverage them to read or write arbitrary memory locations
Custom ROP Chains and ROP Payload Decoders	Construct custom Return-Oriented Programming chains to bypass defenses and build ROP payload decoders for stealthy exploitations