SEC760:™ Advanced Exploit Development for Penetration Testers™

5 Day Program | 40 CPEs | Laptop Required

What You'll Learn

- Advanced reverse engineering techniques
- Complex exploit development methodologies
- Modern fuzzing and vulnerability discovery
- Kernel debugging and exploitation skills
- Windows patch analysis and diffing
- Chrome V8 internals and exploitation
- Advanced heap exploitation techniques

"The hands-on labs in SEC760 were some of the most intense and educational I've ever experienced. I highly recommend this course for serious pen testers."

—K. Nguyen, **Private Cybersecurity Firm**

Advanced Exploit Development: From Zero-Day Discovery to Kernel Exploitation

Vulnerabilities in modern operating systems such as Microsoft Windows 10 and 11, and the latest Linux distributions are often very complex and subtle. Yet, when weaponized by very skilled attackers, these vulnerabilities can undermine an organization's defenses and expose it to significant damage. Few security professionals have the skillset to discover why a complex vulnerability exists and how to write an exploit to compromise it. Conversely, attackers must maintain this skillset regardless of the increased complexity. SANS SEC760: Advanced Exploit Development for Penetration Testers™ teaches the skills required to reverse-engineer applications to find vulnerabilities, perform remote user application and kernel debugging, analyze patches for one-day exploits, perform advanced fuzzing, and write complex exploits against targets such as the Windows kernel and the Linux heap, all while circumventing or working with against cutting-edge exploit mitigations.

Business Takeaways

- Discover zero-day vulnerabilities in programs running on fully patched modern operating systems
- Use the advanced features of IDA Pro and write your own IDAPython scripts
- Perform debugging of Linux and Windows applications
- Understand and exploit Linux heap overflows
- Perform patch diffing against programs, libraries, and drivers to find patched vulnerabilities
- Perform Windows kernel debugging
- Reverse engineer and exploit Windows kernel drivers

Author's Statement

"As a perpetual student of information security, I am excited to offer SEC760: Advanced Exploit Writing for Penetration Testers. Exploit development is a hot topic and will continue to increase in importance moving forward. With all of the modern exploit mitigation controls offered by operating systems such as Windows 11, the number of experts with the skills to produce working exploits is highly limited. Dependence on application development using AI will likely reduce the number of developers and researchers with advanced knowledge of low-level languages.

Many companies are looking to hire professionals with the ability to discover vulnerabilities, determine if those vulnerabilities are exploitable, and carry out general security research. This course was written to help you get into these highly sought-after positions and to teach you cutting-edge tricks to thoroughly evaluate a target, providing you with the skills to improve your exploit development."

—Stephen Sims, SANS Fellow

Section Descriptions

SECTION 1: IDA Pro, Exploit Mitigations, and Windows Kernel Debugging

This section begins working with IDA Pro to look the latest features and techniques. We look at IDA scripting to aid in your reverse engineering workflow and how to leverage AI to assist. Additionally, we cover debugging with IDA, how to create FLIRT signatures, and optimizing your build environment.

TOPICS: Windows Defender Exploit Guard Implementation; Reversing and Debugging Mitigations In-Depth; IDA Pro Fundamentals and Advanced Features; IDA Debugging Capabilities; Lumina, FLIRT, and FLAIR

SECTION 2: Advanced Linux Exploitation

Focusing on sophisticated Linux exploitation techniques, Section 2 builds upon fundamental vulnerability knowledge to address modern attack methodologies. Participants learn to navigate and exploit heap structures, perform browser exploitation, and develop advanced exploitation strategies.

TOPICS: Linux Heap Management Fundamentals; Off-by-One Vulnerability Exploitation; TCache Poisoning Techniques; Chrome V8 Internals; Introduction to JavaScript

SECTION 3: Advanced Fuzzing

Building on basic concepts, this section explores sophisticated fuzzing methodologies for vulnerability discovery. Participants learn to implement coverage-guided fuzzing, develop custom harnesses, and utilize advanced tools like WinAFL for closed-source application testing.

TOPICS: Advanced Fuzzing Architectures; Code Coverage Analysis; Harness Development; Closed-source Application Fuzzing; Full-system Fuzzing Implementation

SECTION 4: Patch Diffing and One-Day Exploitation

Participants learn to analyze vendor patches for vulnerability identification and exploitation. The section covers binary diffing techniques and patch analysis methodologies. You will reverse notable Microsoft patches from the past as well as patches from 2025. Microsoft often changes the way in which patches are packaged up.

TOPICS: Microsoft Patch Management Processes; Binary Diffing Methodologies; Vulnerability Identification Techniques; One-day Exploit Development; BinDiff and Diaphora

SECTION 5: Windows Kernel Debugging and Exploitation

This section teaches Windows 11 kernel debugging and exploitation techniques. Participants learn to navigate kernel complexities, analyze Ring 0 vulnerabilities, and develop working exploits while dealing with modern protection mechanisms.

TOPICS: Windows Kernel Architecture; Modern Kernel Protections; WinDbg Debugging Techniques; Kernel Vulnerability Analysis; Token Manipulation Techniques

Who Should Attend

- Senior network and system penetration testers with exploit development experience
- Secure application developers (C and C++)
- Reverse-engineering professionals
- Senior incident handlers with exploit development experience
- Senior threat analysts with exploit development experience
- Vulnerability researchers
- Security researchers

NICE Framework Work Roles

- Adversary Emulation Specialist/Red Teamer (OPM 541)
- Exploitation Analyst(OPM 121)
- Target Developer (OPM 131)

"SEC760 is the challenge I am looking for. It will be overwhelming, but well worth it."

—William Stott, **Raytheon**

"SEC760 is a kind of training we could not get anywhere else. It is not a theory, we got to implement and to exploit everything we learned."

—Jenny Kitaichit, **Intel**