Linux Kernel Exploitation & Rootkits (LKXR)

Abstract

The goal of this course is to provide a good understanding of offensive and defensive software development in the Linux kernel and the knowledge to detect malicious activity in the kernel and defend against it. LKXR focuses on the skills of developing and detecting techniques used by Linux kernel mode rootkits at every stage of their execution. Students learn how to exploit kernel vulnerabilities, use and abuse kernel subsystems and programming interfaces to implement various stages of rootkits, and identify rootkits artifacts in modern 64-bit Linux systems. Students also learn about the security functionality and mitigations available in the latest Linux 5.x kernel.

Learning Objectives

Students will:

- Identify kernel components and programming interfaces used to compromise a system.
- Develop shellcode that executes in the kernel.
- Develop linux kernel modules that provide offensive security functionality.
- Implement key components of a kernel rootkit.
- Recognize security related enhancements in the modern Linux kernel.
- Analyze a Linux system to identify malicious activity.
- Configure a Linux system to improve the system's security posture.

Students' Knowledge Pre-Requisites:

- Proficient in C programming language.
- Knowledgeable of C programming constructors such as pointers, structures, arrays and linked lists. Comfortable with Linux command line tools.
- Familiar with Linux development tools such as gcc and make and gdb commands.

- Knowledge of operating system concepts such as process, thread, virtual memory, heaps, stacks, files, system calls, daemons etc.
- Knowledge of Linux kernel internals, kernel module development and debugging.

Course Outline:

Topics

- CPU Architecture
- Kernel Shellcoding
- Kernel Security Mitigations
- Kernel Exploitation
- Privilege Escalation
- Code Flow Subversion
- Stealth and Persistence
- Covert Communication
- Detection and case studies