CENTER FOR CYBER SECURITY TRAINING

Linux Kernel Internals & Development

Abstract

The goal of this course is to enable students to develop and debug loadable kernel modules that extend the functionality of the modern 64-bit version Linux kernel. LKID focuses on the skills of investigating the internals of the Linux kernel and the development and debugging of Linux loadable kernel modules. Students learn how to use built in tools to peer into the internals of the Linux kernel, call Linux kernel programming interfaces and build, test and debug Linux loadable kernel modules.

Learning Objectives

Students will:

- Describe the different components of the Linux kernel.
- Develop, build, test and debug Linux kernel modules.
- Implement security related functionality in kernel modules.
- Identify the kernel programming interfaces to solve a given development task.
- Retrieve information from the kernel using various commands.
- Examine crash dumps and identify the cause of the crash.
- Build the foundation to attend the Linux Kernel Exploitation and Rootkit training (LKXR).

Students' Knowledge Pre-Requisites:

- Proficient in C programming language.
- Knowledge 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.

- Knowledge of operating system concepts such as process, thread, virtual memory, heaps, stacks, files, system calls, daemons etc.

Course Outline:

Topics

- Kernel Development Environment
- Kernel Module Development
- Kernel Execution
- User-Kernel Interface
- Device Drivers
- Memory Management I
- Memory Management II
- Synchronization
- Debugging