



Check Point[®]
SOFTWARE TECHNOLOGIES LTD.

Workshop in Information Security

Building a Firewall within the Linux Kernel

Course overview

Lecturer: Eran Tromer

Teaching assistant: Ariel Haviv

Advisor: Assaf Harel

Goals

- Become familiar with the Linux kernel, and how to extend it using kernel modules.
- Understand the TCP/IP protocol, and how it is processed in the Linux kernel.
- Understand concepts in packet inspection and parsing, and rule-based enforcement.
- Introduction to network attack techniques, detection and prevention.
- Gain experience in designing and implementing a modular system.

Assignments

There will be about 5 "Hands-on" assignments in the following subjects:

- TCP/IP traffic recording and crafting
- Protocol enforcement
- Linux user-kernel interface
- Packet filtering
- Attack protection

Linux Kernel

- Write C code intended to compile into a module kernel.
- Debug the kernel module, when it's inserted to the kernel.
- Read Linux man pages to learn about functions.
- Read Linux C headers, to figure out how to use kernel APIs.
- Tackle problems, use web resources

VMs

- Create several Ubuntu virtual machines.
- Install packages on these machines.
- Create virtual networks to connect the machines.
- Make the machines communicate with each other.
- Work with Linux CLI (command line interface).
 - Get to know important Linux commands.
 - Read man pages (yes, again) to learn about CLI tools.

Tools

- C development environment (e.g. Geany) to manage the code.
- Create traffic with:
 - Linux CLI: nc, hping3
 - Programming languages: C, Python or any of your favorite.
- Monitor traffic: Wireshark
- Miscellaneous tasks: Ubuntu GUI and CLI.

Expectations & Guidelines

- We love reading beautiful code. Make us happy.
- Comprehensible modular design. Logical units must be separated, play their unique role, and have clean, well-specified interfaces.
- Show off your innovation. We expect pleasant surprises unique to every team. Such surprises will probably attract our attention, and extra points to the grade.

Comments

- This workshop is going to be intense, challenging and rewarding.
- A lot of self learning will be expected of you.
- You will acquire skills important in the industry.
- Take it only if you are up to it.