Attacking the Linux Kernel

Andrey Konovalov

ABSTRACT

This training guides researchers through the field of Linux kernel security. In a series of exercise-driven labs, the training explores the process of finding, assessing, and exploiting kernel bugs in modern Linux distributions on the x86-64 architecture.

Besides providing a foundation for writing Linux kernel exploits, the training covers the no-less important areas of finding kernel bugs and evaluating their security impact. This includes chapters on using dynamic bug-finding tools and writing custom fuzzers.

The training is targeted at beginners but covers a few intermediate topics as well.

Day 1 — Internals, sanitizing, and fuzzing:

- Internals: handling and running the kernel; debugging the kernel and its modules; attack surface; types of vulnerabilities.
- Detecting bugs: KASAN and other bug detectors; using KASAN; KASAN internals; extending KASAN; reading kernel bug reports; assessing impact of kernel bugs.
- Fuzzing: writing kernel-specific fuzzing harnesses; coverage-guided fuzzing; collecting coverage with KCOV; Human-in-the-Loop fuzzing.

Day 2 — Exploiting memory corruptions:

- Escalating privileges: ret2usr; overwriting the cred structure; overwriting modprobe_path.
- Bypassing mitigations: SMEP, SMAP, KPTI, and KASLR; fixating the system; arbitrary read/write primitives; information leaks.
- Exploiting slab corruptions: out-of-bounds and use-after-free bugs; slab spraying; the unlinking attack.
- Beyond: learning advanced exploitation techniques; useful references.

Student requirements

- Working C knowledge.
- Familiarity with x86 architecture and x86 assembly.
- Familiarity with GDB (GNU Debugger).
- Familiarity with common types of vulnerabilities and exploitation techniques for userspace applications.
- No knowledge about Linux kernel internals is required.

Hardware and software requirements

A machine with 100 GB of free disk space, at least 8 GB of RAM, and VMWare Workstation Player installed. A Linux host is recommended.

Bio

Andrey Konovalov is a Security Researcher focusing on the Linux kernel and a Managing Director at Xairy Labs.

Andrey found multiple zero-day bugs in the Linux kernel and published proof-of-concept exploits to demonstrate the impact. Andrey is a contributor to several security-related Linux kernel subsystems and tools: KASAN — a fast dynamic bug detector, syzkaller — a production-grade kernel fuzzer, and Arm Memory Tagging Extension — an exploit mitigation.

Andrey spoke at security conferences such as OffensiveCon, Android Security Symposium, Linux Security Summit, LinuxCon North America, and PHDays. Andrey also maintains a collection of Linux kernel security–related materials at and a channel on Linux kernel security.

See xairy.io for Andrey's articles, talks, and projects.