Rootkit Programming

Premeeting

Fabian Franzen & Ludwig Peuckert

Chair of IT-Security (I20)
Prof. Dr. Claudia Eckert
Technische Universität München

July 14, 2020

What is a Rootkit?

> A rootkit is a collection of computer software, typically malicious, designed to enable access to a computer or an area of its software that is not otherwise allowed (for example, to an unauthorized user) and often masks its existence or the existence of other software.
> — Wikipedia

Course Contents

In this course you will create your **own rootkit** with the following features...

- hide files on disk
- hide network traffic
  - in Wireshark
  - hide open ports to root and external hosts
- escalate privileges to root

Even more we will focus on the **detection of rootkits** using

- Virtual Machine Introspection (VMI)

Your rootkit will target the **latest** Debian stable kernel (4.19).

Teaching goals

- Linux kernel hacking
  - How to create your **own kernel module**
  - How the Linux kernel tracing system works
  - Getting familiar with **fundamental linux subsystems**
- Details about the linux kernel boot process (e.g. initramfs)
- How the kernel, the loader and the libc interact to start a program
- How a Hypervisor can **interact** and **inspect** its running VMs

Prerequisites

We **do not** have formal requirements for students who want to join the course.

However, we **strongly recommend** being familiar with the following...

- how to write **a C program** and how **pointers** work
- what a **Syscall** is
- how an operating system works in general (as taught in IN0009)

Having seen or worked with **assembly** is a plus!

Orga stuff

- the course has **16 slots**
- we will meet once a week
- you will get **weekly** exercises, which are discussed and graded in the upcoming week (there are exceptions for large tasks!)
  - you have therefore to be present in class!
  - your final grade will be primarily based on this
- You will work with a partner in teams of **two**
- We may finish with a **project**, depending on your interests
  - e.g creating the most awesome rootkit or detection toolkit

Registration

Awesome! How can I join?

We want to make sure that motivated students get places!

- **no** letter of motivation
- instead solve a **small qualification task**
  - create a driver for a PCI device as Linux Kernel Module, that reads out a secret value (flag).[1]
  - due at **21.07.2020 23:59** (end of matching)
  - submit the flag at `https://rk.sec.in.tum.de`
  - more information about the challenge setup can also be found there!
- Nonetheless, do not forget to **register** your self in the **matching system**!

[1] actually it's not a real device, but an emulated one by QEMU

Q & A

We are now happy to answer your questions :)