Rootkit Programming — WS 15/16

Julian Kirsch, Thomas Kittel & Jonas Jelten

Chair for IT Security / I20
Prof. Dr. Claudia Eckert
Technische Universität München

7 July 2015
Time and place

When? Tuesday, 16:00
Where? 01.05.013
Registration

- Send an e-mail to \{kirschju,kittel,jelten\}@sec.in.tum.de until 10 July, 23:59
- Prove you’re qualified by solving a C programming challenge provided by us (do so until 18 July 23:59, details soon on the course webpage).
- Registration using the matching system
- 14 slots
Rootkits

- A **kit** (i.e., group of programs or functions) that allows an attacker to **maintain** root access.
- Provides **backdoor** into the system.
- **Hides** files, connections, etc. that provide this backdoor.
Process

Phase I (12 weeks):
▶ “Usual” practical course (weekly meetings and exercise sheets)

Phase II (3 weeks):
▶ Final project (short paper and presentation)
Process — Phase I

- **Teams of two**
- Every week: Introduction to a new topic
  - System call hooking
  - File-, process-, module-, socket-, network traffic hiding
  - Privilege Escalation
- **Weekly exercise sheets**
  - Submission of solutions until the following week *before* the meeting
  - Private demonstration and short explanation of solution during the meeting
Process — Phase II

Final project

- Preparation of a VM image infected with your rootkit
- Forensic analysis of other teams’ VM images
- Short paper
- Presentation
- Details follow when the time has come
Questions?