Binary Exploitation I — SS 16

Binary Exploitation

Julian Kirsch, Thomas Kittel & Lorenz Panny

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

25 January 2016
Time and place

When? Wednesday, 14:00
Where? 01.05.013
Registration

- Solve our **qualification challenge**!
- Available at: `kirschju.re:55555`
- Details: See the course web page after the premeeting
- Registration using the **matching system** (formally required)
- **14 slots**
Process

Phase I (11 weeks):
  ▶ “Usual” practical course (weekly meetings and introductions to new topics)

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

- **Teams of two**
- Every week: Introduction to a new topic
  - 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

- Development of a vulnerable application
- Creation of an exploit (ab)using the vulnerability/ies
- Short paper
- Presentation
- Break into the other teams’ applications (i.e. "hack" each other 😁)
- Details follow when the time has come
Contents

- Analysis and debugging tools
- Hijacking the control flow abusing buffer overflows
- Shellcode
- Stack- and heap-based buffer overflows
- Bypassing protection mechanisms
- Assume up to 30h of work load per week (But: You reach state-of-the-art knowledge about exploitation of Linux systems)
Questions?