Hacker-Praktikum — SS 15
Binary Exploitation

Sebastian Vogl, Julian Kirsch & Lorenz Panny

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

28 January 2015
When? Tuesday, 13:00
Where? 01.05.013
Registration

- Short **letter of motivation** (about one page)
  - Submit to \{kirschju,vogls,panny\}@sec.in.tum.de until 8 February, 23:59
  - What is your previous experience related to exploitation and low-level programming (C, Assembler)?
  - What do you expect to learn in the practical course?
  - Why are you particularly interested in *this* practical course?

- Registration using the **matching system**

- **14** slots
Process

Phase I (11 weeks):
▶ “Usual” practical course (weekly meetings and exercise sheets)

Phase II (2 weeks):
▶ Final project (short paper and presentation)
Process — Phase I

- Teams of two
- Every week: Introduction to a new topic
- Weekly exercise sheets (10 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

- Development of a vulnerable application
- Creation of an exploit (ab)using the vulnerability/ies
- Short paper
- Presentation
- Details follow when the time has come
Contents

- Analysis and debugging tools
- Hijacking the control flow abusing buffer overflows
- Stack and heap-based buffer overflows
- Shellcode
- Bypassing protection mechanisms