Hacker-Praktikum — SS 15
Advanced Binary Exploitation

Julian Kirsch, Thomas Kittel & Lorenz Panny

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

6 Juli 2015
Time and place

When?  Wednesday, 16:00
Where?  01.05.013
Registration

- Send an e-mail to {kirschju, kittel, panny}@sec.in.tum.de until 10 July, 23:59
- Prove you’re qualified by (choose one):
  - a successful participation at Binary Exploitation 1.
  - solving a Binary Exploitation Challenge provided by us (do so until 18 July 23:59, details soon on the course webpage).
- Registration using the matching system
- **14 slots**
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
- Weekly exercise sheets
  - Submission of solutions until the following week before the meeting
  - Private demonstration and short explanation of solution during the meeting
- Scoreboard: https://pwning.sec.in.tum.de
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

- Bypassing advanced protection mechanisms
- Real-world vulnerabilities
- Exploitation of platforms other than x86(_64)
- Exploitation of operating systems other than Linux
- Kernel and browser exploitation
- (your suggestions?)
Questions?