Binary Exploitation I — WS 2017
Practical Course

Julian Kirsch & Clemens Jonischkeit

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

03. July 2017
What is this?

Exploiting buggy C programs on modern x86_64 Linux systems.
What is this?

Exploiting buggy C programs\(^1\) on modern x86\_64 Linux systems.

\(^1\)Disclaimer: There might be a little C++ as well...
What is this?

Exploiting buggy C programs\(^1\) on modern x86\(_{64}\)\(^2\) Linux systems.

---

\(^1\)Disclaimer: There might be a little C++ as well...

\(^2\)Disclaimer: There might be a little 32-bit x86 as well...
What is this?

Exploiting buggy C programs\textsuperscript{1} on modern x86\textsubscript{64}\textsuperscript{2} Linux\textsuperscript{3} systems.

\textsuperscript{1}Disclaimer: There might be a little C++ as well...
\textsuperscript{2}Disclaimer: There might be a little 32-bit x86 as well...
\textsuperscript{3}Just kidding — no Windows (yet). We kindly refer you to abx.😊
You should...

- ...understand how computers work
- ...know the basics of the Intel x86 assembly language
- ...have a reasonable grasp of the C programming language

...but most importantly:
You should...

- understand **how computers work**
- know the basics of the Intel x86 **assembly language**
- have a reasonable grasp of the **C programming language**

...but **most importantly**:
- enjoy **banging your head against tough challenges**
Process

Phase I (∼ 10 weeks):
  ▶ “Usual” practical course (weekly meetings and assignments)

Phase II (∼ 4 weeks):
  ▶ Final project (vulnerable program, exploit and presentation)
### Scores

| #  | Team       | x1 | x2 | x3 | s0 | s1 | s2 | s3 | s4 | s5 | s6 | s7 | s8 | 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | Σ  |
|-----|------------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 1   | team205    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    | 93 |
| 2   | team2012   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    | 83 |
| 3   | PwnRM      |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    | 73 |
| 4   | /or/aget_flag |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    | 63 |
| 5   | -_-        |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    | 55 |
| 6   | team267    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    | 49 |
| 7   | 1337011D45 |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    | 12 |
| 8   | hunter2    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    | 11 |
| 9   | XORX35     |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |  3 |

### Graphs

![Graph Image](image-url)
Process — Phase I

- Teams of two
- Every week: Introduction to a new topic
  - Submission of solutions before the following week’s meeting
  - Private explanation of the solution during that meeting
Process — Phase II

Final project

- Development of a **vulnerable application**
- Creation of an **exploit** (ab)using the vulnerability/ies
- **Presentation**
- **Hack the other teams’ applications 😊**
- Details follow when the time has come
Contents

- Analysis and debugging tools
- Hijacking the control flow
- Shellcode
- Format string vulnerabilities
- Stack- and heap-based buffer overflows
- Exploiting heap management logic
- Bypassing protection mechanisms
Don’t say we didn’t warn you

- Assume up to 30h of workload per week
- (But: You reach state-of-the-art uber 1337 h4x0r skillz knowledge about binary exploitation techniques on Linux systems)
When? Wednesday, 14:00
Where? 01.05.013
Registration

- Solve our qualification challenge!
- Available at: kirschju.re:55556
- Description and registration https://kirschju.re/bx17w
- **Deadline**: 2017-07-19 (11:59 pm)
- Details: See the course web page after the premeeting
- Registration using the matching system (formally required)
- **14 slots**
Contact us at {kirschju,jonischk}@sec.in.tum.de

PGP fingerprints:
- F949 CFBD 140A 6DD0 71E9 0B8C DC24 396B 6D45 1038
- A903 76D1 65F3 25F9 8594 280A 2BA0 1592 EFAC B551
Contact us at \{kirschju, jonischk\}@sec.in.tum.de

PGP fingerprints:
- F949 CFBD 140A 6DD0 71E9 0B8C DC24 396B 6D45 1038
- A903 76D1 65F3 25F9 8594 280A 2BA0 1592 EFAC B551

Questions?