Binary Exploitation I — Winter 2020
Practical Course

Clemens Jonischkeit & Julian Kirsch

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

2020-07-13
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...
Exploiting buggy C programs\textsuperscript{1} on modern x86\_64\textsuperscript{2} Linux 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...
What is this?

Exploiting buggy C programs\(^1\) on modern x86\(_{64}\)\(^2\) Linux\(^3\) systems.

\(^{1}\)Disclaimer: There might be a little C++ as well...
\(^{2}\)Disclaimer: There might be a little 32-bit x86 as well...
\(^{3}\)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)
<table>
<thead>
<tr>
<th>Team</th>
<th>pwn00</th>
<th>pwn01</th>
<th>pwn02</th>
<th>pwn03</th>
<th>pwn04</th>
<th>pwn05</th>
<th>pwn06</th>
<th>pwn07</th>
<th>pwn09</th>
<th>pwn10</th>
<th>pwn11</th>
<th>pwn13</th>
<th>pwn14</th>
<th>pwn15</th>
<th>pwn16</th>
<th>pwn17</th>
<th>pwn18</th>
<th>pwn19</th>
<th>pwn20</th>
<th>pwn21</th>
<th>pwn22</th>
<th>pwn23</th>
<th>pwn24</th>
</tr>
</thead>
<tbody>
<tr>
<td>w0rmi_b0is</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>0xdeadbeef</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>team208</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td># whoami</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>team202</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>0x400000</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Mantasr0x</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>team203</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>team209</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>team210</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>

**Graphs**

![Graphs](image)

- **x-axis**: Date and Time (02.11.01:00 to 11.11.01:00)
- **y-axis**: Position in Top 8
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
- Short paper (about 5 pages)
- **Presentation** (about 15 minutes)
- **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)
Time and place

When? Tuesday, 14:00
Where? Online
Registration

- Solve our **qualification challenge**!
- Available at: bxqual.sec.in.tum.de:55555
- Description [https://www.sec.in.tum.de/i20/teaching/ws2020/binary-exploitation](https://www.sec.in.tum.de/i20/teaching/ws2020/binary-exploitation)
- **Deadline**: 2020-07-26 (23:59 pm)
- Details: See the course web page after the premeeting
- Registration using the **matching system** (formally required)
- **2^4** slots
Contact me at jonischk@sec.in.tum.de

PGP fingerprint:

A903 76D1 65F3 25F9 8594 280A 2BA0 1592 EFAC B551
Contact me at jonischk@sec.in.tum.de
PGP fingerprint:
- A903 76D1 65F3 25F9 8594 280A 2BA0 1592 EFAC B551

Questions?