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\(^1\) 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>pwn08</th>
<th>pwn09</th>
<th>pwn10</th>
<th>pwn11</th>
<th>pwn12</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>team404</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>
<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>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>team0xce</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>
<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>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>team205</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>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>team207</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>
<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>
<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>
<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>
<td>❌</td>
<td>❌</td>
</tr>
</tbody>
</table>
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** (about 15 minutes)
- **Hack the other teams’** applications 😊
- Create **Write-Up(s)** about 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?      BBB/01.05.013
Registration

- Solve our **qualification challenge**!
- Available at: **honeynet.sec.in.tum.de:1337**
- Registration **honeynet.sec.in.tum.de/bx**
- **Deadline**: 2022-02-15 (23:59 pm)
- Details: See the course web page after the premeeting
- Registration using the **matching system** (formally required)
- **$2^4$** slots
▶ Contact us at {kilger,peuckert}@sec.in.tum.de
Contact us at {kilger, peuckert}@sec.in.tum.de

Questions?