

Binary Exploitation — Winter 24/25

Practical Course

Fabian Kilger & Manuel Andreas
Julian Kirsch & Clemens Jonischkeit

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

2024-07-02

What is this?

Exploiting buggy C programs on modern x86_64 Linux systems.

What is this?

Exploiting buggy C programs¹ on modern x86_64 Linux systems.

¹Disclaimer: There might be a little C++ as well...

What is this?

Exploiting buggy C programs¹ on modern x86_64² Linux systems.

¹Disclaimer: There might be a little C++ as well...

²Disclaimer: There might be a little 32-bit x86 as well...

What is this?

Exploiting buggy C programs¹ on modern x86_64² Linux³ systems.

¹Disclaimer: There might be a little C++ as well...

²Disclaimer: There might be a little 32-bit x86 as well...

³Just 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):

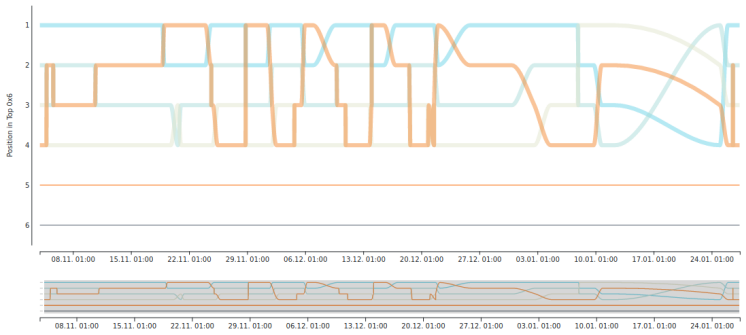
- ▶ “Usual” practical course (weekly meetings and assignments)

Phase II (~ 4 weeks):

- ▶ Final project (vulnerable program, exploit and presentation)

Team	pwn00	pwn01	pwn02	pwn03	pwn04	pwn05	pwn06	pwn07	pwn08	pwn09	pwn10	pwn11	pwn12	pwn13	pwn14	pwn15	pwn16	pwn17	pwn18	pwn19	pwn20	pwn21	pwn22	pwn23	pwn24	
team404	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
team203	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
(!@#\$%^&*) ↑↓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
team0xcce	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
team202	✓	✓	✗	✓	✓	✓	✗	✗	✗	✓	✓	✓	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗	✓	✓	✗
team205	✓	✗	✗	✓	✗	✗	✓	✓	✗	✓	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	
team207	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	
team208	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	
team209	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	
team210	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	

🔄 Graphs



Process — Phase I

- ▶ **Teams of two**
- ▶ Every week: Introduction to a new topic
 - ▶ Submission of solutions **before** the following week's meeting
 - ▶ Presentation 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 20 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? Wednesday, 14:00

Where? TBA

Registration

- ▶ Solve our **qualification challenge individually!**
 - ▶ Connect via **netcat** or in Python via **socket** module
 - ▶ **GDB** might be helpful
 - ▶ Dockerfile provided, but not strictly necessary
 - ▶ You will **not** need to do any **heap** exploitation

Registration

- ▶ Solve our **qualification challenge individually!**
 - ▶ Connect via **netcat** or in Python via **socket** module
 - ▶ **GDB** might be helpful
 - ▶ Dockerfile provided, but not strictly necessary
 - ▶ You will **not** need to do any **heap** exploitation
- ▶ Available at:
`courses.sec.in.tum.de:22019`
- ▶ Registration `courses.sec.in.tum.de/bx`
- ▶ **Deadline**: 2024-07-16 (23:59 pm)
- ▶ Registration using the **matching system** (formally required)
- ▶ **26** slots - no further prioritization from our side

▶ Contact us at `{kilger, andreas}@sec.in.tum.de`

▶ Contact us at `{kilger, andreas}@sec.in.tum.de`

Questions?