

# Binary Exploitation I — Winter 2022/23

## Practical Course

Fabian Kilger & Ludwig Peuckert &  
Julian Kirsch & Clemens Jonischkeit

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

2022-07-13

What is this?

Exploiting buggy C programs on modern x86\_64 Linux systems.

# What is this?

Exploiting buggy C programs<sup>1</sup> on modern x86\_64 Linux systems.

---

<sup>1</sup>Disclaimer: There might be a little C++ as well...

# What is this?

Exploiting buggy C programs<sup>1</sup> on modern x86\_64<sup>2</sup> Linux systems.

---

<sup>1</sup>Disclaimer: There might be a little C++ as well...

<sup>2</sup>Disclaimer: There might be a little 32-bit x86 as well...

# What is this?

Exploiting buggy C programs<sup>1</sup> on modern x86\_64<sup>2</sup> Linux<sup>3</sup> systems.

---

<sup>1</sup>Disclaimer: There might be a little C++ as well...

<sup>2</sup>Disclaimer: There might be a little 32-bit x86 as well...

<sup>3</sup>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)





# 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?** Wednesday, 14:00

**Where?** 01.05.013

# Registration

- ▶ Solve our **qualification challenge!**
- ▶ Available at:  
`honeynet.sec.in.tum.de:1337`
- ▶ Registration `honeynet.sec.in.tum.de/bx`
- ▶ **Deadline:** 2022-07-27 (23:59 pm)
- ▶ Details: See the course web page after the premeeting
- ▶ Registration using the **matching system** (formally required)
- ▶ **2<sup>4</sup>** slots

▶ Contact me at [kilger@sec.in.tum.de](mailto:kilger@sec.in.tum.de)



▶ Contact me at [kilger@sec.in.tum.de](mailto:kilger@sec.in.tum.de)

Questions?