Bypassing advanced protection mechanisms

Real-world vulnerabilities

Exploitation of operating systems other than Linux
  - Windows
  - OpenBSD

Exploitation of architectures other than x86(_64)
  - ARM
  - MIPS

Exploitation of targets outside of boring userspace
  - Browser
  - Kernel
  - Hypervisor

But most importantly: Ub3r l33t h4x0r sk1llz
Bypassing advanced protection mechanisms

Real-world vulnerabilities

Exploitation of operating systems other than Linux
  - Windows
  - OpenBSD

Exploitation of architectures other than x86(64)
  - ARM
  - MIPS

Exploitation of targets outside of boring userspace
  - Browser
  - Kernel
  - Hypervisor

But most importantly:
Bypassing advanced protection mechanisms

Real-world vulnerabilities

Exploitation of operating systems other than Linux
  - Windows
  - OpenBSD

Exploitation of architectures other than x86(_64)
  - ARM
  - MIPS

Exploitation of targets outside of boring userspace
  - Browser
  - Kernel
  - Hypervisor

But most importantly:
Ub3r l33t h4x0r sk1llz
Recap

From bx1 you already know:
Recap

From bx1 you already know:

➤ **How 2 highjack control flow via:**
  ➤ Stack- and heap-based buffer overflows
  ➤ Format string vulnerabilities
  ➤ Exploiting heap-management logic
  ➤ . . .
Recap

From bx1 you already know:

- **How to highjack control flow via:**
  - Stack- and heap-based buffer overflows
  - Format string vulnerabilities
  - Exploiting heap-management logic
  - ...

- **How to bypass common exploit mitigations**
  - ASLR
  - PIE
  - Stack canary
  - Heap sanity checks
  - ...

Process

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

Phase II (4 weeks):
  ▶ Final project (short report and presentation)
Process — Phase I

▶ Teams of two
▶ Each week: Introduction to a new topic
  ▶ Submission of solutions until the following week before the meeting
  ▶ Public presentations and discussion of solutions during the meeting
Final project

- Details follow when the time has come
- Short report
- Presentation
Registration

▶ Send an e-mail to kilger@sec.in.tum.de until 2023-07-19, 23:59. Include the following information:
  ▶ the name of the course
  ▶ your name and matriculation number
  ▶ the semester in which you graduated from bx1
    ▶ alternatively: proof of passing a similar course at a different university incl. proof of the courses syllabus

▶ **Additionally**: Registration using the **matching system**

▶ **30** slots
Former bx1 graduates register via e-mail and matching system:

- kilger@sec.in.tum.de until 2023-07-19, 23:59
- the name of the course
- your name and matriculation number
- the semester in which you graduated from bx1
- alternatively: proof of passing a similar course at a different university incl. proof of the courses syllabus