Advanced Binary Exploitation — Summer 2019

Advanced Binary Exploitation

Clemens Jonischkeit & Julian Kirsch

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

2019-01-29

Time and place

When?	**Wednesday, 16:00-17:30**
Where?	**01.08.033**

Registration

- Send an e-mail to `{jonischk,kirschju}@sec.in.tum.de` until 2019-02-13, 23:59. Include the following information:
  - your matriculation number
  - the semester in which you graduated from `bx1`
  - *optional*: topic suggestions
- Additionally: Registration using the matching system
- 14 slots

Process

Phase I (10 weeks):

- “Usual” practical course (weekly meetings and exercise sheets)

Phase II (3 weeks):

- Final project (short paper and presentation)

Process — Phase I

- **Teams of two**
- Eeach week: Introduction to a new topic
  - Submission of solutions until the following week **before** the meeting
  - Private demonstration and short explanation of solution during the meeting

Process — Phase II

Final project

- Development of a vulnerable application
- Creation of an exploit (ab)using the vulnerability/ies
- Short paper
- Presentation
- Details follow when the time has come

Contents

- Bypassing advanced protection mechanisms
- Real-world vulnerabilities
- Exploitation of platforms other than x86(_64)
- Exploitation of operating systems other than Linux
- (your suggestions?)

Contents

- Bypassing advanced protection mechanisms
- Real-world vulnerabilities
- Exploitation of platforms other than x86(_64)
- Exploitation of operating systems other than Linux
- (your suggestions?)
- But *most importantly*:

Contents

- Bypassing advanced protection mechanisms
- Real-world vulnerabilities
- Exploitation of platforms other than x86(_64)
- Exploitation of operating systems other than Linux
- (your suggestions?)
- But *most importantly*:
- **Ub3r l33t h4x0r sk1llz w1th hxp**

Questions?

Questions?

tl;dr:

Former `bx1` graduates register via e-mail *and* matching system:

- `{jonischk,kirschju}@sec.in.tum.de` until **2019-02-13, 23:59**
  - your matriculation number
  - the semester in which you graduated from `bx1`
  - *optional*: Topic suggestions