Pentesting Lab

Organizational

Possegger, Prodinger, Schauklies, Schwarzl

04.03.2024

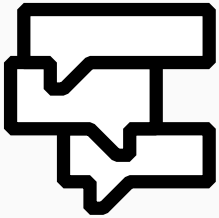
Summer 2023/24, www.iaik.tugraz.at/ptl

- Lecturers




+ 3 Guest lecturers!

Organizational

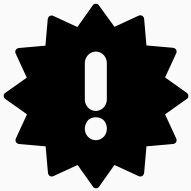


- Website: www.iaik.tugraz.at/ptl
- Discord: https://discord.gg/Nm6rM5Da
  - Announcements and possible clarifications
  - Reading is mandatory!
  - Ask your own questions, especially if relevant for other students
  - Do not post any solutions!

Seminar Mode

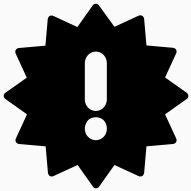
- Practical **assignments**
  - Group size = 1
  - You can work together
  - Deliver until 31st of May, 2024
- **Tutorium** session / question hours
  - Not mandatory but highly recommended
- **Discord** channel for Q&A
  - Mandatory to read (announcements, clarifications ...)
- Final **oral exam**
  - Mandatory
  - First week of June

Timeline I



- 4.3.2024: Kickoff + Pentesting 101
- 10.3.2024: Enumeration Techniques
- 18.3.2024: UNIX Privilege Escalation
- 8.4: Advanced Web Application Security
- 15.4: Test system exploitation / Docker Security
- 22.4: Linux Kernel exploitation

Timeline II



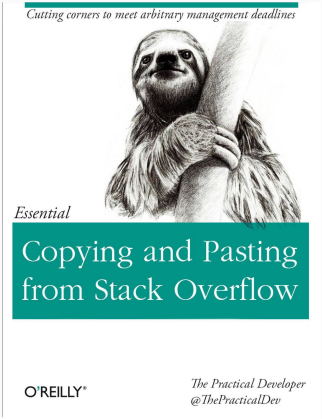
- 27.4.2024: Optional Question Hour
- 6.5: Windows Privilege Escalation
- 13.5: Post-Exploitation
- 20.5: Active Directory
- 27.5: Bonus lecture
- First week of June: Oral exam

Oral exam

- Mandatory
- First week of June
- There will be multiple time slots
- You need to be able to:
  - Answer questions to each assignment and the tasks you fulfilled
  - Insufficient answers will yield to point deduction
    - and can even yield a negative grade
  - More information will be given with each assignment

- No plagiarism will be tolerated!
- We check for plagiarism!
  - If we suspect plagiarism, affected students are questioned
  - All students involved in plagiarism will receive 0 points
  - At least one student: Ungültig/Täuschung with all its consequences

Plagiarism

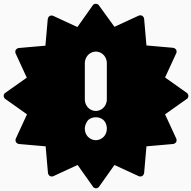


- 👎 No copying from the internet or other sources without showing the reference
- 👎 No sharing of source code / solutions with other students
- 👉 Protect your results from unintended access of others
- 👍 Discussions with other students are highly appreciated
- 👍 Exchange ideas, hints, and pitfalls but no code snippets, solutions, etc.
- 👍 We want everyone to learn and understand for themselves

Assignments

Deliverables

- Create a writeup template for one finding
- Solve lecture challenges
  - CTFd link will be announced
- Solve 1 Windows pentesting challenge
- Solve 1 Linux pentesting challenge
- Deliver writeup
  - Use template
  - Include full attack chain

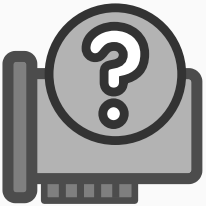


- Final Report:

  Deadline: 31st of May 2024

Expectations

What we expect from you



- Be active and bring up questions/topics
- Time management
- Basic scripting knowledge
- Basic OS knowledge
- Willingness to try and learn

Any Questions?