Pentesting Lab

Organizational

Felix, Possegger, Pongratz, Prodinger, Schauklies, Schwarzl

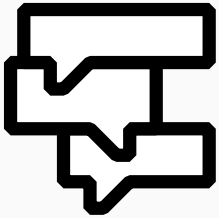
03.03.2025

Summer 2025, www.isec.tugraz.at/ptl

- Lecturers

Organizational

Communication & Support

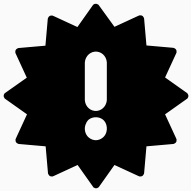


- Website: https://www.isec.tugraz.at/ptl
- Discord: https://discord.gg/Nm6rM5Da
  - Announcements and possible clarifications
  - Reading is mandatory!
  - Ask your own questions, especially if relevant for other students
  - Do not post any solutions!

Seminar Mode

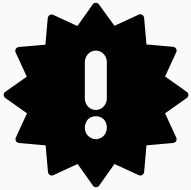
- Practical **assignments**
  - Group size = ~~1~~ 2
  - You can work together
  - Deliver until 31st of May, 2025
- **Tutorium** session / question hours
  - Not mandatory but highly recommended
- **Discord** channel for Q&A
  - Mandatory to read (announcements, clarifications ...)
- Final **oral exam**
  - Mandatory
  - First week of June

Timeline I



- 3.3: Kickoff + Pentesting 101
- 10.3: Enumeration Techniques
- 17.3: Windows AD Fundamentals
- 25.3: Windows AD II + Post Exploitation
- 31.3: Windows PrivEsc
- 07.4: Question Hour

Timeline II



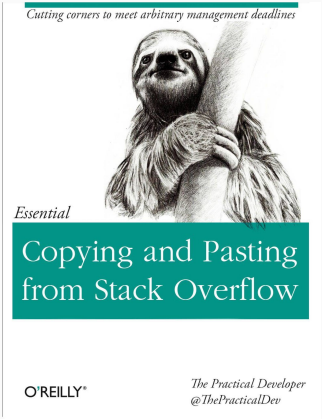
- 14.4-27.04: Easter Break
- 28.4: PrivEsc UNIX
- 5.5: Cloud Security Test system exploitation / Docker Security
- 12.5: Advanced Web Exploitation
- 19.5: Kernel Exploitation
- 26.5: Bonus
- First week of June: Oral exam

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

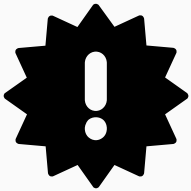


- 👎 No copying from the internet or other sources without showing the reference
- 👎 No sharing of source code / solutions with other students
- 👉 Protect your results from unintended access of others
- 👍 Discussions with other students are highly appreciated
- 👍 Exchange ideas, hints, and pitfalls but 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 2025

Expectations

- Be active and bring up questions/topics
- Time management
- Basic web security (InfoSec) knowledge
- Basic scripting knowledge
- Basic OS knowledge
- Willingness to try and learn

Any Questions?