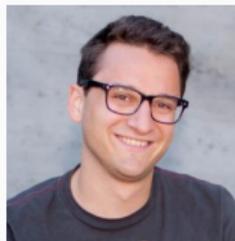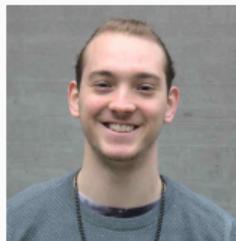# Pentesting Lab

Organizational

Ostermayer, Possegger, Pongratz, Schauklies, Schwarzl

02.03.2026

Summer 2026, www.isec.tugraz.at/ptl

- Lecturers

Organizational

- Website: https://www.isec.tugraz.at/ptl
- Discord: https://discord.gg/b7dMkJAfrw
- Tube: https://tube.tugraz.at/portal/courses/
  6062b365-13b0-4da8-ac22-ca8eed32daa7
 - Announcements and possible clarifications
  - Reading is mandatory!
  - Ask your own questions, especially if relevant for other students
  - Do not post any solutions!

- Practical **assignments**
  - Group size = ~~1~~ 2
  - You can work together
  - Deliver until 31st of May, 2026
- **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
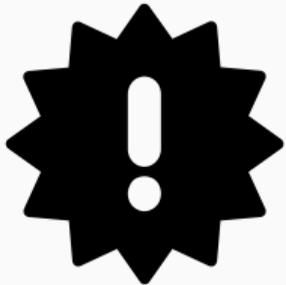
- 2.3: Kickoff + Pentesting 101
- 9.3: Enumeration Techniques
- 16.3: Windows AD Fundamentals
- 23.3: Windows AD II + Post Exploitation
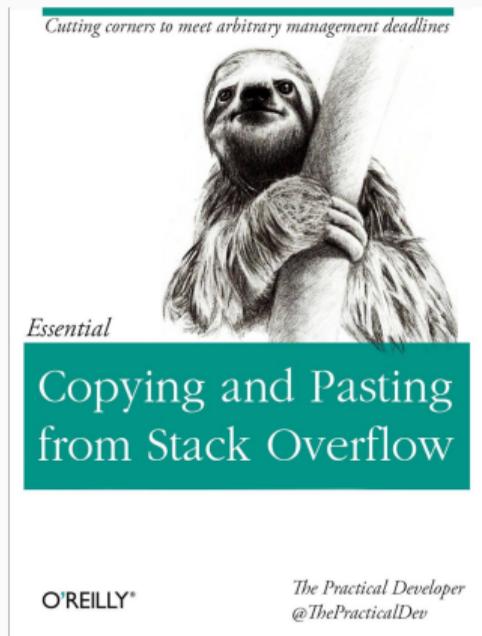- 30.3-12.04: Easter Break
- 13.4: Windows PrivEsc
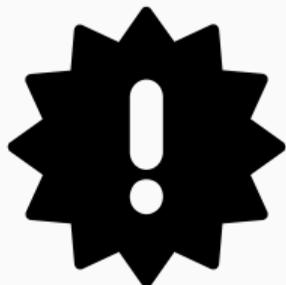
- 15.4: Question Hour - To be confirmed
- 20.4: PrivEsc UNIX
- 27.4: Cloud Security Test system exploitation / Docker Security
- 4.5: Miscellaneous Application Security Topics
- 11.5: Kernel Exploitation
- ??.6: Bonus
- First week of June: Oral exam

- 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

Cutting corners to meet arbitrary management deadlines

Essential

Copying and Pasting from Stack Overflow

O'REILLY®

The Practical Developer
@ThePracticalDev

- 👎 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

- 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
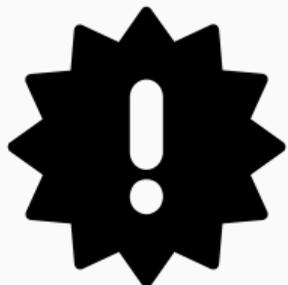
- Final Report:
    Deadline: 31st of May 2026

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

- This is not just capturing flags
- Do not just provide a walkthrough
- Be as complete as possible → report anything that draws your attention
- Pentesting is about showing impact. Documenting vulnerabilities is as important as finding them.
- Do not stop after you found the first critical issue
- Report should contain at least what the https://shorturl.at/A3H6F

Any Questions?