Ethical Hacking

Prof. Luca Pajola and Pier Paolo Tricomi

Outcomes

- Understand the basic principles of ethical hacking …
    - … in practice!
- We cover several area of cybersecurity
- And play with toy-sh application

Lesson Structure

- Small theoretical introduction (~20 minutes)
- Practical exercises (the rest of the lesson)
- The exercises use a ***Capture The Flag (CTF)*** style
  - You have an application to brake
  - You use what we learn so far to crack it
  - If you successfully hack it, you see a flag message
    - E.g., smactCTF{your_first_exercise}

Topics

- Cryptography (Luca)
    - Ciphers; hash functions; symmetric/asymmetric encryption
- Web Vulnerabilities (Luca)
    - Bad programming practices; injections; language vulnerabilities
- Reverse Engineering (Pier)
    - Reversing techniques; patching; anti-debug
- Pawning (Pier)
    - Buffer overflow; defenses; Return Oriented Programming; Global Offset Table

Exam

- At the end of the course we have 4 hours of exams
- 4 CTF exercises in crypto, web, reverse, pwn
- Each exercise gives you some points (e.g., 8)
- We give you some hints to help you solving the problem which cost you some points (e.g., -2)

Whoami

- ITIS Rovigo -IT degree (2008 - 2013)
- Bachelor Degree in Computer Science (2013 - 2016)
    - University of Ferrara, Italy
- Master Degree in Computer Science (2016 - 2018)
    - University of Padova, Italy
- Erasmus at the University of Helsinki, Finland (2017 - 2018)
- Research assistant at Aalto University, Finland (2018)
- Research assistant at Dartmouth College, USA (2019)
- PhD Students in Brain, Mind & Computer Science - University of Padova (Oct 2019 - on going)

Whoami

- Part of the SPRITZ group
  - We are a research team in cybersecurity
  - Lead by prof. Mauro Conti
- My research focuses in the interaction between AI and CyberSecurity