Ethical Hacking

MSc Degree in Cybersecurity
2024-2025

Dr. Alessandro Brighente
Department of Mathematics
University of Padua
alessandro.brighente@unipd.it
https://www.math.unipd.it/~abrighen/

Dr. Eleonora Losiouk
Department of Mathematics
University of Padua
elosiouk@math.unipd.it
https://www.math.unipd.it/~elosiouk/

Teaching Assistant

Francesco Marchiori
francesco.marchiori@math.unipd.it
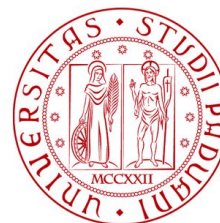
UNIVERSITÀ
DEGLI STUDI
DI PADOVA

SPRITZ
SECURITY & PRIVACY
RESEARCH GROUP

DIPARTIMENTO
MATEMATICA

Basic Information

- **Language:**

- **Credits:** 6 CFU

- **Schedule:** I semester (course schedule is published [HERE](#)).

- **Lectures mode:** due to the highly practical nature of the course, we highly recommend live attendance

Course Content

- **Network Security** (~20% of the course)
  - Sniffing and spoofing
  - Traffic analysis
  - Attacks to transport layer protocols
  - Firewall

- **Blockchain Security**(~20% of the course)
  - How Blockchains work
  - How smart contracts work
  - Attacks to smart contracts

- **Web Security** (~20% of the course)
  - Cross-site scripting
  - Cross-site request forgery
  - HTTP request smuggling
  - SQL Injection

Course Content

- **Reverse** (~20% of the course)
  - Static analysis, reversing in x86
  - Reversing, patching
  - gdb, calling conventions, debuggers
  - Symbolic execution, angr

- **Pwning** (~20% of the course)
  - Shellcode attack
  - Buffer overflow attack
  - Return-to-libc attack
  - Format string attack
  - Race Condition Vulnerability

Lecture Structure
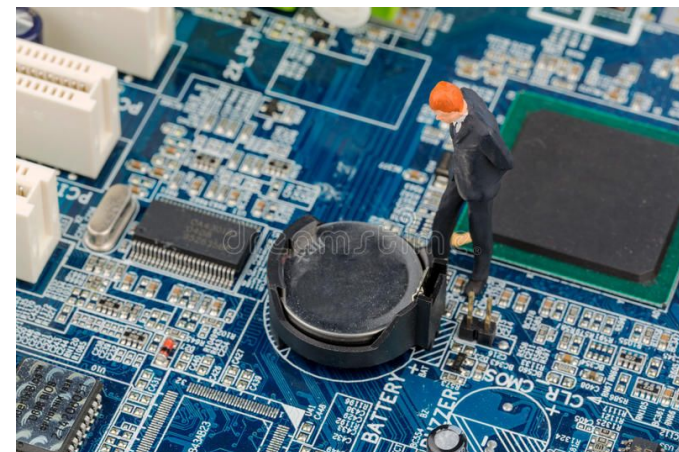
- **Theory**
  - We will provide you video lectures on the course content
  - We will assess at the beginning of each lecture what you got from the videos (does not contribute to the final grade)

- **Practice**
  - You will be divided into groups to solve challenges related to the content of the videos
  - A group will be selected to present the solution to the others during the successive lecture
  - A nice presentation is worth an extra point for the final grade

Grading criteria

- The final exam will be composed by multiple choice questions:
    - Theoretical aspects (18 points)
    - Code snippets + Mini attacks (15 points)

- Grading for the multiple choice test allows to reach the maximum score

- We will add to the exam score the extra points gained with the presentations during the course