Federico **Zanca**

federico.zanca@mail.polimi.it | federico-zanca

Summary

Master's student in Computer Science and Engineering at Politecnico di Milano, passionate about low-level stuff, with a strong focus on binary exploitation and reverse engineering. Active CTF player with Tower of Hanoi, continuously learning through hands-on challenges and projects. Currently exploring Linux kernel exploitation as my main area of interest. Enthusiastic about low-level systems and breaking things down to better understand them. Drawn to problems that feel like puzzles, whether in security, programming, or logic-driven challenges. Interests also extend to cryptography, its mathematical foundations, and side-channel attacks. Always eager to learn, experiment, and dive deeper into security research.

Education

Politecnico di Milano (Polytechnic University of Milan)

Milan, Italy

MSc in Computer Science and Engineering — *Sep. 2023 - Present*

- Currently pursuing my Laurea Magistrale at Politecnico di Milano
- Specializing in Computer Security
- Current GPA: 29.1/30

Politecnico di Milano (Polytechnic University of Milan)

Milan, Italy

BSc in Computing Systems Engineering — *Sep. 2020 - July 2023*

Liceo Scientifico delle Scienze Applicate E. Fermi

Mantova, Italy

High School Diploma — *Sep. 2015 - July 2020*

Mater Academy, Miami

Online

USA High School Diploma — *Sep. 2015 - July 2019*

- Completed alongside my Italian high school diploma in a dual diploma program.

Capture The Flag (CTF) Activities

CTF Team - Tower of Hanoi & mhackeroni

Active Player — *2023 - Present*

- Regularly playing CTFs as a member of **Tower of Hanoi**, the CTF team of Politecnico di Milano, which merges with other Italian teams to form **mhackeroni** for DEFCON.
- Focusing on pwn challenges
- Playing under the handle **amuro**

CyberChallenge.IT 2024

National Finalist — *Feburary - July, 2024*

- Participated in **CyberChallenge.IT**, Italy's national cybersecurity training program, which serves as a selection pathway for the European Cybersecurity Challenge (ECSC).
- Qualified for and competed in the national finals held at the ONU ITCILO Campus in Turin from July 3 to 6, 2024.

Projects

Disclaimer: Certain repositories may currently be private due to academic policy. They will be published as soon as permitted.

Ongoing Projects

Linux Kernel Vulnerability Pivoting (UAF to OOB)

Project for Advanced Operating Systems course

- Exploit a UAF CVE and pivot it to an OOB or another more powerful vulnerability to escalate privileges.
- Bypass kernel mitigations like KASLR to demonstrate the attack chain.
- https://github.com/federico-zanca/KernelExploit-UAF-to-OOB

Python Library for Power Analysis Side-Channel Attacks

- Developing a Python library to analyze power traces for passive side-channel attacks.
- The library aims to include implementations of key power analysis attacks of different types such as Differential Power Analysis (DPA), Simple Power Analysis (SPA), and Correlation Power Analysis (CPA).
- Aims to extract cryptographic keys from a victim device by analyzing power consumption patterns.
- https://github.com/federico-zanca/power-analysis-attacks

Completed Projects

ECDSA Lattice Attacks Tool

Project for Cryptography and Architectures for Cybersecurity course

- Developed a SageMath tool to perform lattice-based attacks on ECDSA signatures with partial nonce leakage, given signatures and the leak.
- The tool allows recovering the private key from the leaked bits of the nonce and some signatures.
- Implemented in Sagemath and Python
- https://github.com/federico-zanca/ECDSA-partially-known-nonce-attack

Nailed It (Videogame)

Videogame Design and Programming course

- Collaborated in a team to design and develop 'Nailed It', an original (and unusual) game where players use a unique nailing mechanic to navigate levels.
- Contributed to game mechanics design, programming, and level development.
- The game was ranked 1st in the course's game ranking.
- Available to play for free at https://polimi-game-collective.itch.io/nailed-it

Distributed P2P Group Chat with Causal Ordering

Project for Distributed Systems course

- Developed a fully distributed group chat application ensuring high availability and causal message ordering.
- Implemented in Java using a peer-to-peer architecture without reliance on a central server.
- Features include resilience to network failures and the ability to operate during temporary disconnections.
- https://github.com/federico-zanca/P2P-Causal-Chat

Certifications & Awards

CyberChallenge.IT 2024

Participant to the Training Phase and National Finalist

- Participated in CyberChallenge.IT 2024, Italy's leading cybersecurity training program for young talents, focused on defensive and offensive cybersecurity skills.
- Gained hands-on experience in various cybersecurity domains, including binary exploitation, reverse engineering, cryptography and web security.

Dual Diploma Program

Mater Academy, Miami

- Completed a dual diploma program in parallel, studying for the USA High School Diploma while pursuing an Italian education.
- Recognized as equivalent to a C1-level English proficiency certification, demonstrating advanced language skills.
- GPA: 4.0/4.0

TOEIC English Certification

Educational Testing Service (ETS)

- Achieved proficiency in English as assessed by TOEIC, focusing on communication in professional and everyday contexts.
- Demonstrated strong command of both written and spoken English in academic and business settings.
- Score: 955/990

Relevant Coursework

- **Offensive and Defensive Cybersecurity** – 30/30 with honors (Prof. Mario Polino)
- **Computer Security** - 30/30 with honors (Prof. Alessandro Barenghi)
- **Cryptography and Architectures for Cybersecurity** – 30/30 (Prof. G. Pelosi, Prof. A. Barenghi)

Other Skills

Programming Languages	Java, Python, C, C++, C#, SageMath, JavaScript, PHP, VHDL, x86, ARM, and other assembly languages
Operating Systems	Linux, Android, Windows
Database Management	SQL, MySQL, PostgreSQL
Web Technologies	HTML, CSS, JSP, JSTL, Thymeleaf
Version Control	Git
Testing & Optimization	JUnit, Code Optimization, Computational Theory
GUI Development	JavaFX, Java Swing, Pygame, VPython
Unity Game Development	C#, Unity Engine 2D/3D Game Development
Machine Learning	Keras, TensorFlow, Neural Networks, Deep Learning Models
Mathematical Concepts	Theory of Computation, Calculus, Abstract Algebra, Number Theory, Algorithmic Complexity