Jacopo Rossi

MSc Student in Computer Science & AI Engineering · AI & Data Security

Rome, Italy · rossijacopo002@gmail.com · jacoporossi.com · linkedin.com/in/jacopo-rossi-software-engineer · github.com/enoughpaladin00 · Hack The Box

PROFILE

Final-year MSc student at Sapienza (GPA 28.28/30) focused on the security of AI systems and data. Finalist in CyberX Mind4Future, the CTF and red-teaming competition run by Leonardo and Cyber 4.0. I built an ML-driven intrusion detection system that blocks attackers in real time, and I want to bring this attacker's mindset to protecting AI platforms and data.

EDUCATION

MSc in Engineering in Computer Science and Artificial Intelligence — Sapienza University of Rome 2025 – expected July 2027
GPA 28.28/30 · taught entirely in English

- Completed: Cybersecurity (30/30), Machine Learning (30/30), Artificial Intelligence (30/30), Advanced Cryptography (28/30), Algorithm Design (28/30)
- In progress: Machine Learning Security, Malware Analysis, Network Infrastructures, Mobile, Edge and Cloud Computing, Secure Computation
- Planned thesis: Machine Learning Security or Malware Analysis

BSc in Computer and Control Engineering — Sapienza University of Rome 2021 – 2025
Final grade 98/110 · Thesis: Guardaloo, design and development of a digital guide for film enthusiasts

PROJECTS AND COMPETITIONS

CyberX Mind4Future — Finalist · Leonardo & Cyber 4.0 National Competence Centre 2024 – 2025

- Completed an advanced cybersecurity training phase taught by faculty from the partner universities
- Qualified as a finalist in the Capture the Flag and red-teaming challenges against simulated real-world systems

NetInfect — ML-driven network IDS with active response github.com/enoughpaladin00/NetInfect

- Emulated a three-zone enterprise network (WAN, DMZ, LAN) with Kathará and Docker, monitored by Zeek on the gateway
- Built a hybrid detection pipeline: an Isolation Forest anomaly score feeds a Random Forest classifier (scikit-learn, pandas)
- Generated labelled data by scripting multi-stage attacks: port scanning, SSH brute force, SQLi/XSS, HTTP flood, Slowloris, data exfiltration
- Real-time response: a controller injects iptables rules to drop attacker IPs, plus a regex-based L7 WAF, a Streamlit dashboard and offline PCAP analysis

Secure Dice Game · Cybersecurity course github.com/enoughpaladin00/dice-game

- Fair two-party game with no trusted third party: SHA-256 commit-then-reveal and XOR seed derivation, each player in its own Docker container

ECHO · Laboratory of Advanced Programming github.com/enoughpaladin00/2003424_ECHO

- Distributed, fault-tolerant platform that processes and classifies real-time seismic sensor streams (Python)

Guardaloo · BSc thesis, team project · **FAT file system in C** · Operating Systems course

- Full-stack web app for film enthusiasts (Ruby on Rails) for the Software Architecture and Cybersecurity Lab; FAT-based file system handling low-level memory and on-disk structures

TECHNICAL SKILLS

Security: Burp Suite, Nmap, Metasploit, Wireshark, Zeek, iptables, IDA, Gobuster, John the Ripper, Hydra · ongoing practice on Hack The Box
AI / ML: PyTorch, scikit-learn, pandas, supervised and unsupervised learning, anomaly detection, adversarial machine learning (coursework)
Programming: Python, C/C++, Java, JavaScript/TypeScript, PHP, SQL, x86 Assembly · Solidity and Circom (zero-knowledge circuits)
Systems and tools: UNIX/Linux, Docker, Kubernetes, Kathará, Git, PostgreSQL, MySQL, Streamlit

OTHER EXPERIENCE

Private Tutor · Self-employed, Rome Sep 2022 – May 2025
Tutored high-school students in mathematics, physics, natural sciences and English, building an individual study plan for each student.

Warehouse Assistant · Bancolibri Sulla Strada srls, Rome Summers 2024 and 2025

LANGUAGES AND INTERESTS

Italian: native · **English:** fluent, daily academic use in an MSc taught entirely in English; Cambridge First Certificate (B2), 2019 · **Driving licence:** B
Interests: cinema (technical director of an independent short film, 2025), amateur football (often team captain), photography, literature

I authorise the processing of my personal data pursuant to Regulation (EU) 2016/679 (GDPR).