Bahaeddine Melki

Post-Master's Cybersecurity Student at EURECOM | Seeking End-of-Studies Internship in Red Teaming / Application Security

⊙ Antibes, France ☎ +33 605 703 683 @ bahaeddine.melki@eurecom.fr

Profiles			
in LinkedIn	○ Github	☁ K4v0r1_0x	☠ Portfolio

Summary

Post-Master's student at EURECOM specializing in offensive security, with a background in telecommunication engineering. Experienced with web and binary exploitation and Active Directory attack paths. Holder of eJPT and PT1 certifications, seeking a 6-month Red Team or Application Security internship starting February 2026.

Education

EURECOM — 2024 - 2026
Security in Computer Systems and Communications — Post Master's degree

International institution accredited to deliver a specialized engineering degree (post-master) in digital security and communications.

SUP'COM — 2022 - 2024
ICT Engineering — National Engineering Degree

Recognized among Tunisia's top engineering schools and leading in telecommunications education.

Preparatory Institute for Engineering Studies - El-Manar (IPEIEM) — 2020 - 2022
Math and Physics — Pre-Engineering Diploma

Ranked in the top 5 % nationally in the entrance exam for engineering schools.

Experience

KPMG Tunisia — July 2023 - September 2023
Summer Intern — Tunis, Tunisia

- Assisted the IT department with network troubleshooting and user privilege management within the Active Directory (AD) environment.
- Resolved technical issues for end-users and supported the implementation of secure access controls.

IEEE Tunisia Section (Remote) — June 2023 - September 2023
Summer Intern — Tunis, Tunisia

- Processed and labeled 10 000+ receipt images to train computer-vision models for automated document verification.
- Trained and evaluated CNN-based classification models to detect mislabeled or fraudulent receipts.

Projects

Red-Team RAT (Discord C2) — Personal project — August 2025

- Developed a remote access tool (RAT) for red-team simulation using the Discord API as a command-and-control channel.
- Implemented modular features for remote command execution and file transfer in a controlled lab environment for detection engineering purposes.

LLM-Based Deepfake Detection (ASVspoof Challenge) — March 2025 – July 2025

- Built an audio deepfake detection pipeline leveraging Wav2Vec2 and DistilBERT for spoofed-speech classification.
- Benchmarked performance across multiple attack types from the ASVspoof dataset to evaluate model robustness.

Pentest Home Lab — February 2025

- Designed a virtualized penetration-testing lab with Windows AD and Linux vulnerable hosts (Metasploitable 2/3).
- Practiced credential harvesting, Kerberos abuse, and lateral movement using tools such as BloodHound and Evil-WinRM.

Zero-Knowledge SNARK Implementation — October 2024 – January 2025

- Implemented a zero-knowledge proof system in Rust, applying the Fiat–Shamir transform for non-interactive verification.
- Demonstrated end-to-end construction of a zk-SNARK pipeline from polynomial commitment to proof validation.

Skills

Offensive Security
Web Exploitation, Binary Exploitation, Network Exploitation, Active Directory Attacks, Privilege Escalation, Detection Evasion

Tools & Frameworks
Evil-WinRM, Burp Suite, Metasploit, Nmap, Wireshark, BloodHound, Ghidra, IDA Free, Docker, Git

Programming Languages
Python, C++, C, PHP, Rust, Java

Certifications

CPTS - Certified Penetration Testing Specialist — Ongoing
Hack The Box

Junior Penetration Tester (PT1) — June 2025
TryHackMe

E-learn Security Junior Penetration Tester (eJPT) — March 2025
INE

Certified in Cybersecurity (CC) — February 2025
ISC2

TOEIC — March 2024
ETS

Languages

English	French	German	Arabic
C2	C1	A1	Native