



# Bahaeddine Melki

Cybersecurity Student at Eurecom | Seeking an end of studies internship in OffSec / AI red teaming

📍 Antibes, France 📞 +33 605 703 683 @ bahaeddine.melki@eurecom.fr

Profiles	<div><a href="#">in LinkedIn</a></div> <div><a href="#">Github</a></div> <div><a href="#">K4v0r1_0x</a></div> <div><a href="#">Portfolio</a></div>			
Summary	Double-degree Post-Master's student at EURECOM with a telecom engineering background from Sup'Com. Hands-on with web/binary exploitation and AD attack paths; comfortable building small lab environments to reproduce TTPs and generate IoCs. Looking to contribute to a Red Team/AppSec internship by turning findings into clear, actionable fixes.			
Experience	<b>KPMG Tunisia</b> Summer Intern		<b>July 2023 - September 2023</b> Tunis, Tunisia	
	<ul style="list-style-type: none"><li>Resolved technical issues for different users in the enterprise.</li><li>Managed network troubleshooting and user privileges, ensuring security and access control.</li></ul>			
	<b>IEEE Tunisia Section (Remote)</b> Summer Intern		<b>June 2023 - September 2023</b> Tunis, Tunisia	
	<ul style="list-style-type: none"><li>Collected, cleaned and added labels to receipt data.</li><li>Trained CNN models and classification models to extract labels and verify the validity of the receipt.</li></ul>			
Education	<b>EURECOM</b> Security in Computer Systems and Communications		<b>2024 - 2026</b> Post Master's degree	
	<b>SUP'COM</b> ICT Engineering		<b>2022 - 2024</b> National Engineering Degree	
	<b>Preparatory Institute for Engineering Studies - El-Manar (IPEIEM)</b> Math and Physics		<b>2020 - 2022</b> Pre-Engineering Diploma	
Projects	<b>Red-Team RAT (Discord C2) — Personal project</b>		<b>August 2025</b>	
	<ul style="list-style-type: none"><li>Built a lab-only Remote Access Tool (RAT) proof-of-concept that used Discord as a simulated command-and-control channel for controlled red-team research.</li><li>Designed modular capabilities—remote command execution, file-transfer simulation and telemetry generation—used to validate detection engineering, produce IoCs, and test SOC playbooks.</li></ul>			
	<b>LLM-Guided Deepfake Detection (ASVspoof Challenge)</b>		<b>March 2025 – July 2025</b>	
	<ul style="list-style-type: none"><li>Built a detection pipeline that transcribed spoofed and bonafide speech using Wav2Vec2 and fine-tuned DistilBERT and Whisper models for one-class classification.</li><li>Benchmarked performance across multiple spoofing techniques from the latest ASVspoof dataset, highlighting the effectiveness of LLM-based approaches for audio security.</li></ul>			
	<b>Pentest Home Lab</b>		<b>February 2025</b>	
	<ul style="list-style-type: none"><li>Built a lab environment with an Active Directory domain controller and vulnerable Linux hosts (Metasploitable 2 &amp; 3) in a segmented network.</li><li>Used it to emulate attack paths (credential harvesting, Kerberos abuse, lateral movement).</li></ul>			
	<b>Zero-Knowledge SNARK Implementation</b>		<b>October 2024 – January 2025</b>	
	<ul style="list-style-type: none"><li>Implemented a zero-knowledge polynomial commitment scheme in Rust, incorporating the Fiat–Shamir transform for non-interactive proofs.</li><li>Demonstrated the end-to-end construction of a zk-SNARK pipeline, from commitment to verification, as part of cryptography research.</li></ul>			
Skills	<b>Ethical Hacking</b> Penetration Testing, Web Exploitation, Binary Exploitation, AD Pentest	<b>Cybersecurity</b> Digital Forensics, Cryptography, Systems Security, GRC, Reverse Engineering	<b>Programming Languages</b> Python, C++, C, PHP, Rust, Java	<b>AI</b> Machine Learning, Deep Learning, Time Series, Pytorch, TensorFlow, LLMs
Certifications	<b>CPTS - Certified Penetration Testing Specialist</b> Hack The Box		<b>Ongoing</b>	
	<b>Junior Penetration Tester (PT1)</b> TryHackMe		<b>June 2025</b>	
	<b>E-learn Security Junior Penetration Tester (eJPT)</b> INE		<b>March 2025</b>	
	<b>Certified in Cybersecurity (CC)</b> ISC2		<b>February 2025</b>	
	<b>TOEIC</b> ETS		<b>March 2024</b>	
Languages	<b>English</b> C2	<b>French</b> B2	<b>German</b> A1	<b>Arabic</b> Native