

MAROUAN BEN HMED

JUNIOR PENETRATION TESTER

 m0rgxn.me |  [MarwenOnGit](https://github.com/MarwenOnGit) |  [HackTheBox](https://www.hackthebox.com/profile/104544) |  marouan.benhmed@etudiant-enit.utm.tn |  +216 44 650 180 |  Tunis, Tunisia

PROFILE

Final-year computer engineering student in offensive security, with hands-on experience across web application, Active Directory, and Azure assessments. I build practical offensive tooling and hybrid attack labs, and I am ranked Top 5 nationally on HackTheBox. Available for a 12-week research internship between May and October 2027.

Areas of expertise: offensive security, Active Directory, cloud security, attack simulation, detection

EDUCATION

Engineering Degree in Computer Science	Sept 2023 - present
<i>National Engineering School of Tunis</i>	El Manar, Tunisia
Preparatory Studies for Engineering in Physics and Technology	Sept 2020 - Jul 2023
<i>Preparatory Institute for Engineering Studies El Manar</i>	El Manar, Tunisia
- Ranked top 8% in the National Entrance Exam to Engineering Schools	

PROFESSIONAL EXPERIENCE

Azure Red Team Intern @ Keystone Group (Tunis, Tunisia)	Jul 2026 - Sep 2026
- Developed offensive tooling targeting Azure services by exploiting common cloud security misconfigurations. - Researched privilege-escalation paths involving Azure RBAC, managed identities, and service principals.	
White Box Penetration Tester (Engagement)	Aug 2026
- Led a white-box security assessment of a production web application, identifying and validating high-impact vulnerabilities. - Delivered a technical report with remediation guidance and proof-of-concept demonstrations for confirmed findings.	
Data Science Summer Intern @ MAS Enterprise (Tunis, Tunisia)	Jun 2025 - Aug 2025
Developed NLP models and data pipelines with monitoring dashboards for model performance, with a focus on reliability and secure handling of enterprise data.	

PROJECTS & ACHIEVEMENTS

Fenrir - Azure Managed Identity Attack-Path Tool (github.com/MarwenOnGit/fenrir)	Jul 2026 - present
- Built a Python CLI that automates the Azure managed-identity attack chain: tenant recon, IMDS token theft across VM, App Service, Logic App, Container, and Automation hosts, and tenant-wide post-exploitation. - Designed a conservative go/no-go readiness verdict that models privilege-escalation primitives as data, so a single rule set drives both the report and the JSON output. - Published three research writeups on Azure managed-identity attacks at m0rgxn.me: modeling privilege escalation as an attack graph, the design of Fenrir, and an attacker's analysis of the credential-less identity model.	
Independent Offensive Security Research	Mar 2025 - present
Reached Top 5 nationally in Tunisia on HackTheBox (70+ machines), publishing in-depth technical writeups of attack paths and remediation at m0rgxn.me.	
Hybrid Environment Setup & Red Team Infrastructure	Mar 2025 - present
- Designed a large enterprise hybrid environment integrating on-premises Active Directory with EntraID. - Stood up full Red Team infrastructure on AWS, including Mythic C2, redirectors, and OPSEC-safe tooling. - Ran attack simulations covering lateral movement and privilege escalation across monitored Windows/Linux agents.	

SKILLS

Penetration Testing: Enumeration, Lateral Movement, Active Directory, Web Application Testing
Tools: Burpsuite, Mythic C2, Wireshark, Metasploit, Nmap, Sliver C2, Chisel, Proxychains, Impacket Scripts
Programming: Python, Bash, JavaScript, Java (<i>proficient</i>); C, C++, C#, .NET (<i>familiar</i>)
DevOps & Cloud: Docker, Terraform, Ansible, GitHub Actions, AWS, Azure/EntraID, Git/GitHub
Application Development: React, Next.js, Node.js, Flask
Languages: French (<i>fluent</i>), English (<i>fluent</i>), Arabic (<i>native</i>)

CERTIFICATIONS

HackTheBox CPTS (<i>In Progress</i>)	Expected completion 2027
HackTheBox Prolab: Puppet (<i>Completed</i>)	Writeup
HTB University CTF 2025	Ranked 77/1200 teams