Mohamed Khalil MZALI

Born on 29th December 2002

• +216-28-216-384 • mzalimohamedkhalil@gmail.com • linkedin.com/in/khalil-mzali
• medium.com/@mzalimohamedkhalil • mohamedkhalilmzali.github.io

CyberSecurity Student from **ESPRIT (Ecole Supérieure Privée d'Ingénierie et de Technologies)**

EDUCATION

- High School French Baccalaureate **with Honors** - **Math Specialty**
- Cybersecurity Degree at ESPRIT (2020-2025):

Annual score 2023: 17.19/20 (GPA 4.0) – Annual score 2024: 17,23/20 (GPA 4.0)

CERTIFICATIONS

- Offshore Professional Lab from HackTheBox (August 2024)
- Zephyr Professional Lab from HackTheBox (June 2024)
- Blue Team Junior Analyst from Security Blue Team (May 2024)
- Cisco CCNA Security (February 2024)
- Cisco CyberOps Associate (February 2024)
- Dante Professional Lab from HackTheBox (September 2023)
- NSE 2 from Fortinet (July 2023)
- Introduction to OSINT from Security Blue Team (July 2023)
- CCNA: Switching, Wireless and Routing Essentials from Cisco (July 2023)
- AWS Security Fundamentals (July 2023)
- NSE 1 from Fortinet (June 2023)
- Introduction To DarkWeb Operations from Security Blue Team (June 2023)
- Android Bug Bounty Hunting: Hunt Like a Rat from EC-Council (June 2023)
- TryHackMe Offensive Pentesting Learning Path (August 2022)
- ISO/IEC 27001 Information Security Associate (August 2022)
- TryHackMe Jr Penetration Tester Learning Path (August 2022)
- Foundations of operationalizing MITRE ATT&CK (July 2022)
- Scrum Master Certification (July 2022)
- eJPT (eLearn Junior Penetration Tester) (June 2022)
- TryHackMe Web Fundamentals Learning Path (July 2022)

PROJECTS

Next Generation SOC Platform for Banking Organization using open-source Tools

- Provided a comprehensive perspective to grasp the business context of the proposed solution.
- Identified critical assets, potential threats, vulnerabilities, and delineated the repercussions of a security incident.
- Designed and provided a layered architecture that modularizes the SOC components.
- Deployed, configured, and integrated appropriate security solutions for both physical and virtual infrastructures.
- Prepared and customized the solution by focusing on the development of tailored playbooks and automation scripts.
- Tested the effectiveness and efficiency of the deployed SOC solution against internal and external attacks.
- Provided a comprehensive review of the organization's adherence to regulatory compliance

Automated Web Application Reconnaissance

- Designed a shell script that automates and facilitates the reconnaissance stage of a web application.

PROFESSIONAL EXPERIENCE

TryHackme CTF Competition Platform **(2022-2024)**

- Gained valuable experience in penetration testing, by enriching my theoretical and practical knowledge with Web application, network and Active Directory exploitation techniques.

HackTheBox CTF Competition Platform **(2023-Present)**

- Participated in Dante Professional Lab, which simulates a real-world penetration testing of a corporate network of 14 machines with latest technologies. I had the opportunity to practice my enumeration, exploitation, post-exploitation and lateral movement skills to gain access to dependent machines that include Linux and Windows web servers, domain-joined windows machines and Domain controllers.

VulnLab CTF Competition Platform **(2024-Present)**

- Participated at the compromise of two machines that expose real-world vulnerabilities such as log4j vulnerability and unsecure LDAP directories.
- Published writeups explaining my methodology when solving these machines on my medium blog (https://medium.com/@mzalimohamedkhalil)

Penetration Testing internship at OffensyLab **(July 2023)**

OffensyLab is a Tunisian Cybersecurity startup specializing in providing offensive security services.

During my internship at OffensyLab, I had the opportunity to contribute significantly to various projects, including:

- **Created a shell script** that automates the reconnaissance phase of web application assessments, significantly reducing manual effort and improving efficiency.
- **Conducted penetration testing** of Windows environments using Metasploit and PowerShell Empire. Identified and exploited vulnerabilities to enhance system security.
- **Practiced exploitation techniques** targeting OWASP Top 10 vulnerabilities on vulnerable lab environments, gaining hands-on experience in mitigating common security risks.

Network Management internship at SOTETEL **(July 2021)**

SOTETEL is a key player in the field of telecommunications operating since 1981 on the Tunisian market and abroad, recognized for its expertise in the implementation and maintenance of telecommunications networks.

During my internship at SOTETEL, I gained practical experience in network management and infrastructure development, including:

- **Implemented a network infrastructure**, contributing to the setup and optimization of network components.
- **Learned and understood the Physical Layer Components**, gaining insights into the foundational elements of network architecture.
- **Participated in the configuration of Routers and switches**, assisting in the setup and maintenance of network devices to ensure optimal performance.

ACTIVITIES

SECURINETS ESPRIT **(2021-2022)**

Actively contributed to a cybersecurity club focused on knowledge sharing, participating in workshops, and collaborating with peers to solve challenges in the cybersecurity domain.

ATIDE (Association Tunisienne pour l'Intégrité et la Démocratie des Elections) **(25 July 2022)**

Participated as an observer during the Tunisian Constitution Referendum.

SKILLS

Technical Skills

- Network Security
- Web Application Testing
- Active Directory exploitation
- Privilege escalation techniques on Windows and Linux
- Scripting Languages (Python, Bash Scripting)
- Programming Languages (Java, C, C++, C#)

Soft Skills

- Leadership
- Analytical Skills
- Problem-Solving
- Communication
- Teamwork

LANGUAGES

- **English** (Full Professional Proficiency)
- **French** (Full Professional Proficiency)
- **Spanish** (Limited Working Proficiency)
- **Arabic** (Native)