Mohamed Khalil Mzali

Cybersecurity Engineer

+216 28216384 | cyber.mzali@gmail.com | linkedin.com/in/khalil-mzali | https://cyberkmz.github.io

PROFESSIONAL EXPERIENCE

Keystone, Tunis, Tunisia December – June 2025

End-of-Studies Internship

- Designed and developed Guardian, a PowerShell-based automation tool for Windows system security hardening and compliance auditing aligned with CIS Benchmarks.
- Implemented three core modules: Backup (exports current system and group policy configurations), Protect (applies 23 CIS-aligned security policy categories), and Audit (evaluates compliance and assigns security scores).

3S (Standard Sharing Software), Tunis, Tunisia July – September 2024

Internship

- Performed an external audit on one of 3S client's web applications for two weeks, uncovered and reported medium severity vulnerabilities.
- Performed an internal audit on-site inside the client's organization, uncovered and reported several critical and high severity vulnerabilities.
- Provided recommendations to mitigate the reported vulnerabilities based on the internal and external assessment results.

OffensyLab, Tunis, Tunisia

Internship June – July 2023

- Performed security research on antivirus bypass techniques.
- Tested various initial access delivery techniques such as embedded malicious macros on word documents with Powershell Empire.

EDUCATION

ESPRIT - Honoris United Universities Group (British Universities Holding), Tunisia 2020-2025

- Engineering Degree in Cybersecurity – **Graduated with Highest Honors**

French Baccalaureate – Scientific Section (Mathematics)

- **Graduated with Honors**

CERTIFICATIONS

- **CRTO (Certified Red Team Operator)** from Zero-Point Security
- **eJPT (eLearn Junior Penetration Tester)** from eLearnSecurity
- **Dante, Zephyr and Offshore Professional Labs** from HackTheBox
- **Blue Team Junior Analyst** from Security Blue Team
- **Scrum Master** from the International Scrum Institute

PROJECTS

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

- Configuration of the LAN network with firewalls (PfSense) and NIPS solutions (Snort).
- Configuration of the SIEM (Wazuh), SIRP (TheHive & Cortex) and DFIR (Velociraptor) solutions inside the SOC area.
- Automation of threat intelligence and incident response with workflows.

Reverse shells in Nim and Go

- Development of reverse shell scripts on NIM and Go that circumvent Antivirus detection.

Shellcode Loaders

- Development of shellcode loaders in C++ (Process Injection, DLL Injection).

SKILLS

Technical Skills: Network Security, Web Application Testing, Active Directory exploitation, Python, NIM, Go, Java, C, C++, C#
Soft Skills: Leadership, Analytical Skills, Problem-Solving, Communication, Teamwork

LANGUAGES

English (TOEFL C1**)**
French (Full Professional proficiency**)**
Spanish (Limited Working proficiency**)**
Arabic (Native**)**