Khalil Mzali

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

EXPERIENCE PROFESSIONNELLE

3S (Standard Sharing Software), Tunis, Tunisie — Juillet – Septembre 2024
Stagiaire

- Réalisation d'un audit externe sur toutes les applications web d'un client de 3S, identification, exploitation et rapport de vulnérabilités critiques.
- Réalisation d'un audit interne sur-site, où j'ai identifié et exploité des failles de configuration sur des serveurs et des applications.
- Rédaction d'un rapport détaillé, mettant en évidence plusieurs vulnérabilités critiques et proposant des mesures correctives.

OffensyLab, Tunis, Tunisie — Juin – Juillet 2023
Stagiaire

- Réalisation d'un projet de recherche sur les techniques de contournement d'Antivirus
- Test de plusieurs techniques d'accès incluant l'exploitation par intégration de macros sur des documents Word légitimes avec Powershell Empire

EDUCATION

ESPRIT, Tunis Tunisie — 2020-2025
Diplôme d'ingénieur en cybersécurité

- Moyenne annuelle en 2024: **17.19/20**

Baccalauréat Français Section Scientifique Spécialité Mathématiques – **Mention Très Bien**

CERTIFICATIONS

- **Penetration Testing:** eJPT (eLean Junior Penetration Tester) de eLearnSecurity, Offshore Professional Lab, Zephyr Professional Lab et Dante professional Lab de HackTheBox
- **Blue teaming:** Blue Team Junior Analyst de SecurityBlueTeam et Cisco Cyberops Associate
- **Network security:** NSE 1 et 2 de Fortinet, CCNA 2 et Cisco CCNA Security

PROJETS

Plateforme Next Generation SOC for Banking Organization avec des outils open-source

- Sécurisation du réseau LAN par des firewalls (PfSense) et NIPS (Snort)
- Configuration du SIEM (Wazuh), SIRP (TheHive & Cortex) et DFIR (Velociraptor) dans la zone SOC
- Automatisation du threat intelligence et de la réponse aux incidents par des workflows

Reverse shells en Nim et Go

- Développement de reverse shells en NIM et Go pour le contournement d'Antivirus

Shellcode loaders en C++

- Développement de shellcode loaders en C++ pour le contournement des solutions de sécurité

COMPETENCES

Compétences techniques : Sécurité réseau, Audit des applications Web, exploitation d'Active Directory, Elévation de privilèges sous Windows et Linux, Maitrise des langages de Scripting (Python, NIM, Go) et de programmation (Java, C, C++, C#)
Compétences personnelles : Leadership, autonomie, communication, et travail en équipe

LANGUES

Anglais (Avancé) — **Espagnol** (Intermédiaire)
Français (Avancé) — **Arabe** (Avancé)