Youssef Charfeddine

youssef.charfeddine@insat.ucar.tn | LinkedIn | GitHub | Portfolio | +216 53 922 372

Résumé

Étudiant en Génie Réseaux et Télécommunications à l'INSAT, spécialisé en Digital Forensics, Incident Response (DFIR) et Malware Analysis. Combine une solide base en infrastructure réseau et administration système avec une expérience avancée et pratique en threat intelligence et analyse bas niveau. A démontré une rigueur technique en rétro-ingéniant manuellement et en documentant plus de 60 échantillons de malware réels. Contributeur actif à la communauté et concepteur de challenges CTF nationaux et internationaux pour Securinets INSAT.

Compétences Techniques

Reverse Engineering & DFIR : x86 Assembly, IDA Pro, x64dbg, Manual Unpacking (OEP/IAT Reconstruction, Scylla), IDAPython Tooling, C2 Network Interception, Procmon.

Offensive Security : Web Penetration Testing, OWASP, Burp Suite, Nmap, Metasploit.

Machine Learning & Développement : Python, C/C++, Bash, Classical ML, .NET Core, Angular.

Réseaux & Infrastructure : TCP/IP, SIEM, Linux, GNS3, Docker, QEMU/KVM.

Formation

Diplôme d'Ingénieur en Réseaux et Télécommunications – INSAT, Tunisie 2022 – Présent
Formation axée sur l'administration réseau, la cybersécurité, la gestion d'infrastructures IT et l'analyse système bas niveau.

Expérience Pertinente

Auteur de Challenges CTF (Malware & DFIR) – Securinets INSAT Sep 2024 – Présent
Conception et déploiement de plusieurs challenges DFIR et Malware Analysis, touchant plus de 1000 participants lors de compétitions nationales et internationales en cybersécurité.

Stagiaire Web Pentest – Keystone Jul 2025 – Aug 2025
Réalisation d'un test d'intrusion complet sur l'environnement de laboratoire *UNSAFE Bank*, identification et reporting de 13 vulnérabilités critiques, avec recommandations de remédiation exploitables.

Stagiaire Développeur Web – MS Solutions Group (Monetics Services Solutions) Jun 2023 – Jul 2023
Conception de solutions full-stack incluant le développement d'une plateforme e-commerce responsive et d'une application de gestion de livres avec Angular et .NET Core, ainsi que l'implémentation d'APIs backend sécurisées. Développement d'un outil autonome de gestion de tournois en C#.

Projets & Recherche Indépendante

Malware Persistence Maturity Model (Projet académique - En cours) : Développement d'un projet de recherche en sécurité structuré en 4 niveaux, cartographiant le "Persistence Spectrum" de Windows, des artefacts User-Mode jusqu'aux implants firmware supportés par le matériel.

Practical Malware Analysis : Reverse engineering manuel et documentation exhaustive de plus de 60 échantillons de malware réels sur une période de 4 mois.

Plateforme SIEM : Conception et déploiement d'une solution SIEM complète, intégrant différentes sources de logs et création de règles de détection personnalisées afin de réduire le temps hypothétique de réponse à incident.

ISLP (Introduction to Statistical Learning with Python) : Résolution et documentation de plus de 50 exercices complexes en apprentissage statistique, avec application de différents modèles de machine learning.