Youssef Charfeddine

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

Summary

Network and Telecommunications Engineering student at INSAT specializing in Digital Forensics, Incident Response (DFIR), and Malware Analysis. Combines a strong foundation in network infrastructure and system administration with advanced, hands-on experience in threat intelligence and low-level execution. Demonstrated technical rigor by manually reverse-engineering and documenting over 60 real-world malware samples. Active community contributor and architect of national and international CTF challenges for Securinets INSAT.

Technical Skills

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 & Development: Python, C/C++, Bash, Classical ML, .NET Core, Angular.

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

Education

Engineering Degree in Networks and Telecommunications – INSAT, Tunisia 2022 – Present
Focused on network administration, cybersecurity, IT infrastructure management, and low-level system analysis.

Relevant Experience

CTF Challenge Author (Malware & DFIR) – Securinets INSAT Sep 2024 – Present
Architected and deployed multiple DFIR and malware analysis challenges, reaching over 1000 participants in national and international cybersecurity competitions.

Web Pentest Intern – Keystone Jul 2025 – Aug 2025
Conducted a full penetration test on the *UNSAFE Bank* lab environment, identifying and reporting 13 critical security vulnerabilities and providing actionable remediation steps.

Web Developer Intern – MS Solutions Group (Monetics Services Solutions) Jun 2023 – Jul 2023
Engineered full-stack solutions by developing a responsive e-commerce platform and a book management application using Angular and .NET Core, while implementing secure backend APIs. Built a standalone C# tournament management tool.

Projects & Independent Research

Malware Persistence Maturity Model (Academic Project - Ongoing): Developing a comprehensive 4-tier security research project mapping the Windows ”Persistence Spectrum” from User-Mode artifacts to Hardware-backed firmware implants.

Practical Malware Analysis: Manually reverse-engineered and exhaustively documented over 60 real-world malware samples over a 4-month period.

SIEM Platform: Designed and deployed a complete SIEM solution, integrating distinct log sources and creating custom detection rules to reduce hypothetical incident response time.

ISLP (Introduction to Statistical Learning with Python): Solved and recorded over 50 complex statistical learning exercises, applying distinct machine learning models.