Mohamed Aziz Haddadi

azizhaddadi10@gmail.com | LinkedIn | github.com/aziz-haddadi | pulgaa.com

Summary

Cybersecurity student specializing in **Digital Forensics & Incident Response (DFIR)**, malware analysis, and Blue Team operations. Active CTF competitor ranked **Top 1% globally on TryHackMe** with multiple podium finishes including **1st place at QnQSec CTF**. Published security research including RAT reverse engineering and packer detection tooling. Currently seeking security internships in SOC, forensics, or threat intelligence roles.

Education

National Institute of Applied Science and Technology (INSAT) Tunis, Tunisia

Software Engineering — Focus: Cybersecurity & Digital Forensics *2023 – Present*

- Relevant coursework: Computer Networks, Operating Systems, Databases, Algorithms, Software Architecture, Web Development.
- Member of **Securinets** (Technical Team) and **MOJO-JOJO** CTF team.

Technical Skills

DFIR & Forensics: Volatility 3, Autopsy, FTK Imager, Wireshark, KAPE, Velociraptor, Regripper, Registry Explorer, PhotoRec/TestDisk
Blue Team & SOC: Splunk, YARA, Snort, ELK Stack, Sysmon, TheHive, FakeNet-NG, MITRE ATT&CK Framework
Malware Analysis & RE: Ghidra, IDA Pro, dnSpy, x64dbg, Detect It Easy, CyberChef, any.run, VirusTotal, PE/COFF format analysis
Programming: Python (PyCryptodome, Scapy, argparse, struct), Bash, PowerShell, JavaScript, SQL, C
Platforms & Tools: Linux (Kali, Ubuntu), FlareVM, Docker, Git, Burp Suite, Node.js, Nmap

Projects

XWorm v3.1 — Malware Analysis & Config Decryption Mar 2026

- Reverse-engineered AES-256-ECB config encryption of XWorm RAT (VB.NET, 54/66 VT detections) using dnSpy; wrote a Python decryptor replicating the MD5 key derivation to extract C2 host, port, mutex, and encryption key.
- Mapped full kill chain across static & dynamic analysis in FlareVM: reflective loading, 3 persistence mechanisms, raw TCP C2 protocol, 20+ command dispatcher, and keylogger. Authored a YARA rule covering v3.0–5.0 variants.

PackDetect — Packer Detection & Unpacking Tool Jan 2026

- Built a Python CLI detecting packed PE malware via Shannon entropy, a 9-packer signature database, and 5 structural heuristics (EP anomaly, missing IAT, virtual-only sections). Auto-unpacks UPX/MPRESS with JSON export and batch scanning.
- Validated on real MalwareBazaar samples at 97% confidence; 26 unit tests with synthetic PE binaries — zero external dependencies for PE parsing.

ZipKrack — ZIP Password Cracker Mar 2026

- Zero-dependency Python CLI for dictionary-based ZIP cracking with real-time feedback, auto-extraction, timestamped password logging, and dual interactive/CLI modes.

DFIR Automation Scripts In Development

- Python toolkit automating Windows artifact parsing (EVTX, Prefetch, registry hives), IOC extraction from memory dumps, VirusTotal API integration, and HTML/PDF triage reports.

CTF Competitions & Community

Placements: 1st — QnQSec CTF | Top 4 — Securinets Quals (5th North Africa) | Top 5 — Darkest Hour 2026 | Top 7 — Securinets Finals | 1st — Advanced Cybersphere CTF
Ranking: Top 1% globally on TryHackMe | Published writeups on memory forensics, disk forensics, malware analysis, and DNS exfiltration
Securinets INSAT: Technical Team Member — CTF organization, workshops, and security awareness (2024–Present)
MOJO-JOJO: Core player & DFIR challenge author — design forensics challenges for national CTFs (2025–Present)

Certifications

Google Cybersecurity Professional Certificate — *Google (Coursera)* 2024

SOC Level 1 Learning Path — *TryHackMe* Certified

TryHackMe Top 1% — *Global Platform Ranking* 2026