HAMZA SALIH

Security Engineer | Offensive Security and Detection Engineering

Tangier, Morocco · +212 7 76 68 17 78 · hamza-salih-pro@proton.me

github.com/hamza-salih · linkedin.com/in/hamza-salih-181a5038b

PROFESSIONAL SUMMARY

Security Engineer with a State Engineering Degree in Cybersecurity and detection engineering experience at APM Terminals. Strong in security monitoring, Python, Linux, networking and web security assessment, and building deeper offensive-security capability through ongoing practical training.

PROFESSIONAL EXPERIENCE

APM Terminals — Tangier Med, Morocco March 2026 – September 2026

Cybersecurity Intern

- Designed and built an agentless Insider Threat Detection System that flags anomalous user activity from existing logs, with no endpoint agents deployed.
- Built a five-signal risk engine combining Z-score deviation, Isolation Forest, role-based peer comparison, shift context and attack-chain analysis.
- Produced explainable alerts using SHAP attribution, local Mistral/Ollama briefs and MITRE ATT&CK mapping, on a stack of Python, FastAPI, Streamlit, PostgreSQL, Redis, WebSockets and Docker.

National Ports Agency (ANP) — Tangier, Morocco September 2024 – October 2024

Information Systems Intern

- Maintained the port-management databases and investigated internal user incidents to resolution.
- Provided user support, documented technical procedures and contributed to validation testing.

SELECTED PROJECTS

Containerized SSH Honeypot and Attack Analysis

- Deployed a Cowrie honeypot with Docker Compose and built a Filebeat/Logstash pipeline into Elasticsearch with GeoIP enrichment and four Kibana dashboards.
- Configured Watcher alerts and analyzed attacker commands and brute-force behavior, mapping relevant activity to MITRE ATT&CK.

Automated Web Vulnerability Scanner

- Built a Python and OWASP ZAP workflow producing candidate SQL injection, XSS, open redirect and missing security-header findings that require manual validation.
- Enriched findings with severity, OWASP Top 10 category and target URL, stored them in Elasticsearch with Kibana dashboards, and ran isolated scans in scheduled containers.

EDUCATION

École des Nouvelles Sciences et Ingénierie (ENSI) — Tangier, Morocco 2021 – 2026

State Engineering Degree in Cybersecurity

PROFESSIONAL DEVELOPMENT

Offensive Security Engineering — independent practical training in progress

TECHNICAL SKILLS

Security & Detection	ELK Stack (Elasticsearch, Logstash, Kibana, Filebeat), Wazuh, Cowrie, Watcher, MITRE ATT&CK, anomaly detection, Isolation Forest, SHAP
Security Assessment	Burp Suite, OWASP ZAP, Nmap, Wireshark, OWASP Top 10, HTTP request analysis, vulnerability validation, packet and protocol analysis
Systems & Networking	Linux, Windows, Active Directory fundamentals, TCP/IP, IPv4/IPv6, DNS, HTTP/HTTPS, TLS/PKI, routing, Docker, Docker Compose
Development & Automation	Python, Bash, PowerShell, C/C++, Git, FastAPI, REST APIs, WebSockets, scheduled automation
Data Platforms	PostgreSQL, Redis, Elasticsearch, MySQL, MongoDB

LANGUAGES

Arabic — Native | French — Intermediate | English — Intermediate