ECHAHBOUNI ISSAM

Étudiant en Cybersécurité – Stage d'Initiation 2026

M'diq, Maroc (Tétouan / Tanger) • +212 675 23 40 46 • issam.echahbouni@etu.uae.ac.ma • linkedin.com/in/issam-echahbouni

PROFIL PROFESSIONNEL

Étudiant en 1ère année DUT Cybersécurité (EST Tétouan), passionné par la détection des menaces et la sécurisation des infrastructures réseau. Expérience pratique en lab : déploiement SIEM/NIDS (Wazuh, Suricata, Snort) et simulations Red Team. Participant actif aux compétitions CTF. Disponible pour un stage d'initiation fin 2026.

FORMATION

DUT Cybersécurité – EST Tétouan, Maroc *2025 – En cours*

Cours clés : Réseaux & Sécurité (OSI/TCP-IP, Pare-feux, VPN, IDS/IPS) • Windows Server (AD, GPO) • Python • C • SQL

Baccalauréat Sciences Physiques (option français), mention Bien – Lycée Abdelkhalek Torres, Tétouan

CERTIFICATIONS

Getting Started with Cisco Packet Tracer – Cisco Networking Academy *Mai 2026*
Introduction to Cybersecurity – Cisco Networking Academy *Avril 2026*
Foundations of Cybersecurity – Google / Coursera *Avril 2026*

COMPÉTENCES TECHNIQUES

Sécurité & SIEM : Wazuh SIEM, Suricata NIDS, Snort IDS/IPS, Zabbix
Outils Offensifs : Nmap, Hydra, Nikto, SQLMap, hping3 (environnement lab)
Systèmes : Kali Linux, Linux Mint, Ubuntu, Debian, Windows Server 2012 R2
Langages : Python (POO, Scripting), C, SQL
Virtualisation : VMware, VirtualBox, Cisco Packet Tracer

PROJETS ACADÉMIQUES & PERSONNELS

Architecture Wazuh SIEM & Suricata NIDS *Projet Académique*

- Déployé une architecture Wazuh complète (Manager + Agents) avec intégration Suricata NIDS pour l'analyse des alertes EVE JSON.
- Campagnes Red Team simulées : scans Nmap, brute force SSH/FTP/RDP (Hydra), injections SQL (SQLMap), DoS SYN flood (hping3) depuis Kali Linux.
- Corrélé et analysé les événements de sécurité pour valider la couverture de détection et l'efficacité des règles.

Implémentation Snort IDS/IPS *Lab Personnel*

- Installé Snort 3 ; développé des règles personnalisées pour la détection ICMP, brute force SSH et scans Nmap SYN.
- Configuré Snort en mode IPS inline (NFQ) pour le blocage actif du trafic malveillant incluant les injections SQL.

Plateforme CTF – Capture The Flag *Projet Académique*

- Développé et déployé une plateforme web CTF fonctionnelle en Python (POO), hébergée en production sur Railway.

COMPÉTITIONS CTF

ENSI 2K26 CTF (Cyberspace x ENSI) – 11 flags validés (Mai 2026)
NorthSec 2026 – 6 flags validés (Avril 2026)
Compétences acquises : Forensique numérique, exploitation web, reverse engineering.

LANGUES

Arabe : Langue maternelle **Français :** Courant (études) **Anglais :** Opérationnel (technique)

SOFT SKILLS & CENTRES D'INTÉRÊT

Soft Skills : Esprit d'analyse et résolution de problèmes (CTF), Travail en équipe (simulations Red/Blue team), Autonomie et curiosité technique.

Centres d'intérêt : Musculation (discipline, force & hypertrophie), Jeux vidéo de simulation/automobile (Euro Truck Simulator 2, Forza Horizon 5).

Disponible pour un stage d'initiation – Fin 2026 • Régions Tétouan & Tanger