ABIR MAJDI

Elève ingénieure en Génie de Développement Numérique et Cybersécurité

+212704845990 abir.majdi@usmba.ac.ma N 152 rue 31 lotissement JBL THRAT 2 FEZ

OBJECTIF PROFESSIONNEL

Étudiante en deuxième année de Génie du Développement Numérique et Cybersécurité, passionnée par la sécurité informatique et les nouvelles technologies. À la recherche d'un stage d'application de deux mois (1er Juillet – 31 Août 2026) afin de mettre en pratique mes connaissances en sécurité informatique, développement sécurisé et administration des systèmes et bases de données.

FORMATIONS

ENSA Fez | 2023-2027

Diplôme : Génie du Développement Numérique et Cybersécurité

Doroub El Maarifa | 2022

Baccalauréat Sciences Physiques, Mention Très Bien

EXPÉRIENCES

CHU | Juillet 2025

Stage d'initiation – Centre Hospitalier Universitaire Hassan II de Fès

- Découverte du fonctionnement des systèmes d'information hospitaliers.
- Étude des bonnes pratiques de sécurité appliquées aux bases de données médicales.
- Contribution à la mise en place d'un système de détection et journalisation des accès anormaux dans MySQL.
- Participation à l'analyse des logs et détection des requêtes suspectes.

PROJETS ACADÉMIQUES

Développement d'un protocole sécurisé type TLS

- Implémentation d'un protocole inspiré de TLS en Python (architecture client-serveur)
- Mise en place d'un handshake sécurisé avec échange de clés Diffie-Hellman
- Chiffrement symétrique des communications et dérivation de clé de session

Simulation d'attaques et hardening d'une application web (OWASP A02)

- Déploiement d'une application FastAPI/Nginx Dockerisée volontairement vulnérable
- Identification et exploitation de misconfigurations critiques (credentials en clair, debug activé, directory listing)
- Hardening complet (gestion sécurisée des secrets, sécurisation Nginx, headers OWASP)
- Validation par scans Nmap/Nikto et script automatisé – réduction du risque ~85%

Déploiement d'un Honeypot SSH avec centralisation des logs

- Conception d'un honeypot SSH Dockerisé pour détecter les tentatives de brute force et scans
- Collecte et analyse des logs via ELK stack (Logstash & Elasticsearch)
- Mise en place de mécanismes de confinement (AppArmor, seccomp) pour sécuriser l'environnement

CERTIFICATIONS & FORMATIONS EN LIGNE

- Introduction to cryptography (great learning)
- Manipulate MAC addresses, execute MiTM attacks, develop RAT | PYCEH Hacking (udemy)
- Database programming with SQL (Oracle)
- Learn SQLMap for Ethical Hacking: Explore Automated SQL Injection Testing (udemy)

CENTRES D'INTÉRET

- pentesting sur une machine virtuelle
- IA & Sécurité

LANGUES

- arabe natif
- Français Intermédiaire B2
- Anglais Avancé C1