Ibrahim Mounir

Technicien Spécialisé en Infrastructure Digitale Option Cybersécurité

☎ **+212 779 900 321** **brahimmounir555@gmail.com** **linkedin.com/in/ibrahimmounir** **imounir.tech** **Khenifra, Morocco**

EDUCATION

Technicien Spécialisé : Infrastructure Digitale & Cybersécurité (IDoCS) | Institut Spécialisé de Technologie Appliquée (ISTA)
Khenifra, Morocco *Sep. 2024 – 2026*

– Coursework : Sécurité Réseau, Administration Systèmes Linux/Windows, Virtualisation (VMware), Active Directory, Tests d'intrusion, Cryptographie

Baccalauréat — Sciences Physiques Khenifra, Morocco *2023*

EXPÉRIENCE & PROJETS

Stagiaire en Cybersécurité | Maroc Datacenter (MDC) Temara, Rabat-Salé-Kénitra, Morocco ***Mar. 2026 · 1 mois***

– Stage technique au sein de l'équipe Réseau et Sécurité, focalisé sur la gestion de l'infrastructure Data Center.

– Firewall & VPN : Participation à la configuration des règles de sécurité et à la gestion des accès distants sécurisés via VPN IPsec/SSL.

– Switching : Configuration de VLANs et monitoring des ports pour assurer la segmentation et la performance du réseau.

– Servers : Administration et maintenance de serveurs (installation, configuration d'IP statiques et gestion des services).

– Monitoring : Surveillance active de l'état des équipements pour garantir une haute disponibilité.

Projet de Fin d'Études (PFE) — Infrastructure Réseau Sécurisée avec Monitoring Centralisé | ISTA Khenifra *2025 – 2026*

– Conception d'une topologie dual-firewall (FortiGate + Sophos XG) avec segmentation VLAN (Clients, Servers, Admins, DMZ).
– Déploiement d'Active Directory (Windows Server 2019, domaine pfe.local) avec GPO et jonction de postes clients.
– Mise en place de Wazuh SIEM pour le monitoring centralisé des événements de sécurité.
– Configuration de règles firewall avancées (NAT, VIP, ACL) et serveur Web en DMZ.

Laboratoire — Simulation d'Audit de Sécurité (Active Directory) | Projet Académique

– Déploiement d'une infrastructure complète (Windows Server 2019 + Windows 10).
– Mise en place de stratégies de groupe (GPO) pour sécuriser les accès.
– Simulation d'attaques (Mimikatz, Responder) pour tester la résilience du réseau.
– Rédaction d'un rapport technique détaillant les vulnérabilités identifiées.

CTF & Cybersécurité Offensive — SecDojo Competitions | Compétitions en ligne

– Résolution de labs : exploitation MCP (command/prompt injection), RCE N8N avec Docker socket escape.
– Attaques MLflow/Jupyter (pickle deserialization), énumération Active Directory en pentest.

Développement Web — Projets Pratiques | Projets Académiques

– Création de sites web (HTML/CSS) et conception d'interfaces graphiques interactives.
– Analyse de sécurité statique d'applications web : identification de vulnérabilités (xmlrpc.php, REST API enumeration, version disclosure).

COMPÉTENCES TECHNIQUES

Sécurité: Pare-feu (FortiGate, Sophos XG), SIEM Wazuh, Active Directory, GPO, Tests d'intrusion, Cryptographie
Réseaux: VLAN, NAT, ACL, VPN, Routage, Segmentation réseau, Protocoles TCP/IP
Systèmes: Administration Linux & Windows Server, VMware Workstation/ESXi, GNS3
Langages: Python, Bash/Shell, HTML, CSS, SQL
Outils: Wireshark, Mimikatz, Responder, Nmap, Git, Word, Excel, PowerPoint

CERTIFICATIONS & FORMATIONS

Cisco CCNA Training | Python Essentials 1 & 2 | Jr Penetration Tester (TryHackMe)

LANGUES

Arabe : Langue maternelle | **Français :** Niveau intermédiaire | **Anglais :** Niveau intermédiaire