# ABDELAAZIZ BELKHAIR

Élève-Ingénieur Cybersécurité

Pessac, France — +33 6 15 24 33 25 — abelkhair002@bordeaux-inp.fr
Portfolio — GitHub

*Élève-ingénieur en Télécommunications passionné par la cybersécurité. Expérience en sécurité offensive (pentest, analyse de malware), développement d'outils de sécurité et cryptographie. Recherche un stage de fin d'études de 6 mois à partir de février 2026.*

## Formation

**ENSEIRB-MATMECA – École Nationale Supérieure d'Électronique, Informatique, Télécommunications**
*Diplôme d'Ingénieur Télécommunications – Spécialisation Cybersécurité* 2023 – 2026
Réseaux et protocoles, cryptographie, sécurité des systèmes, développement logiciel

**Classes Préparatoires aux Grandes Écoles**
*MPSI/MP – Mathématiques, Physique, Sciences de l'Ingénieur* 2021 – 2023
Fès, Maroc

## Certifications & Langues

**Certifications**

- EC-Council Pentesting Agent – Beginner/Intermediate
- Pratique CTF sur Root-Me (Web, Réseau, Reverse, Forensic)

**Langues**

- Français : Courant
- Anglais : B2/C1 – **TOEIC 945/990**
- Allemand : A2

## Expérience Professionnelle

**Stage Ingénieur R&D – AM Advisory** (Conseil IT) Juin – Septembre 2025
*Développement de SecureDevKit – Plateforme SAST basée sur l'Intelligence Artificielle*

- Conception d'un moteur SAST hybride intégrant analyse statique et modèles IA (CodeBERT, Phi)
- Développement d'un système de génération automatique de correctifs avec fine-tuning de LLMs
- Optimisation des modèles par quantization pour déploiement à faible latence
- Benchmarking de performance (latence, CPU, mémoire) et études de solutions du marché
- Livrables : documentation technique, dashboards de suivi, rapports de synthèse

## Compétences Techniques

**Sécurité Offensive**
- Pentest, exploitation
- Analyse de malware
- Reverse-engineering
- Attaques Active Directory
- MITRE ATT&CK

**Cryptographie**
- Post-quantique (Kyber, Dilithium)
- AES-GCM, HKDF
- PKI, certificats
- TLS, SSH

**Réseaux & Protocoles**
- TCP/IP, DNS, HTTP
- Kerberos, NTLM, LDAP
- OAuth 2.0, OIDC
- MQTT, CoAP, LoRaWAN

**Développement**
- Python (avancé)
- C (avancé)
- Bash, PowerShell
- SQL

**IA / Machine Learning**
- PyTorch, Scikit-learn
- Fine-tuning LLMs
- Détection d'anomalies
- Pandas

**Infrastructure**
- Docker
- Microsoft Azure
- Windows Server, Linux
- Active Directory

**Outils :** Metasploit, Burp Suite, Wireshark, Nmap, Scapy, BloodHound, PingCastle, Responder

## Projets

**Framework d'Analyse et Déobfuscation de Malware**

Framework modulaire pour l'analyse automatique de binaires ELF obfusqués. Analyse statique (parsing), déobfuscation (unpacking, décryptage), analyse dynamique (traçage) et extraction d'IoC. Génération de rapports multi-formats (JSON, Markdown, HTML).
*Technologies : Python, reverse-engineering*

### Net-Aware Auth Auditor

Outil d'audit réseau avec reconnaissance passive/active et analyse de protocoles d'authentification (Kerberos, NTLM, TLS, LDAP). Détection de faiblesses de configuration et génération de rapports d'audit structurés.
*Technologies : Python, Scapy*

### Système Honeypot avec Détection ML

Infrastructure honeypot multi-services (SSH, HTTP) pour capture et analyse de trafic d'attaques en temps réel. Détection d'anomalies par machine learning, logging centralisé et génération de métriques de menaces.
*Technologies : Python, Scikit-learn*

### PQ-Secure Sync – Synchronisation Post-Quantique

Système de synchronisation sécurisé par cryptographie post-quantique. Handshake avec KEM Kyber768 et signatures Dilithium3 (latence  1ms). Gestion de clés persistantes avec TOFU, dérivation HKDF-SHA256 et chiffrement AES-GCM. Benchmarking exhaustif des algorithmes PQ.
*Technologies : Python, cryptographie post-quantique*

### Architecture Cloud Sécurisée Azure

Infrastructure cloud avec approche Zero Trust : gestion des identités (Azure AD), contrôle d'accès RBAC, monitoring centralisé (Log Analytics), dashboards de supervision et audit des habilitations.
*Technologies : Microsoft Azure, Docker*

### Système de Stockage Distribué et Chiffré

Architecture distribuée avec réplication et tolérance aux pannes. Passerelle, nœuds de stockage et base de métadonnées. Chiffrement bout-en-bout et déploiement complet via Docker (Infrastructure as Code).
*Technologies : Docker, Python*

### Système de Mémoire Partagée Distribuée

Espace mémoire synchronisé entre processus distribués via sockets TCP/IP. Programmation en C avec gestion de la cohérence et des accès concurrents.
*Technologies : C, sockets TCP/IP*

## Centres d'Intérêt

**Cybersécurité :** Veille active, CTF (Root-me, Tryhackme)
**Technologies :** Cryptographie post-quantique, IA appliquée à la sécurité, sécurité OT/IoT