

EM

# EL ISLAH MHOMA

Analyste de Données & Futurs Expert en Cybersécurité

Introduction

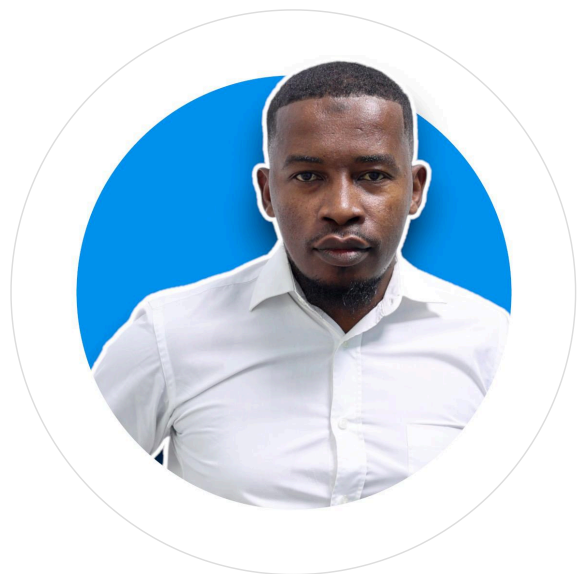
Compétences

Parcours

Contact

## Bienvenue

Analyste de Données en spécialisation Cybersécurité, je mets mes compétences en mathématiques et informatique au service de la protection des systèmes d'information. Passionné par la résolution de problèmes complexes, je suis à la recherche d'une alternance pour contribuer activement à la sécurité de votre organisation.



## Mes Compétences



### Cybersécurité & Systèmes

Panorama de la SSI (ANSSI), Sécurité du poste de travail, Analyse de logs, Gestion des incidents, Windows, Hygiène numérique.

### Analyse de Données & Gestion de Projet

Modélisation Statistique, Traitement de Données, Pilotage de projets d'innovation, Gestion d'équipe, Google Analytics.

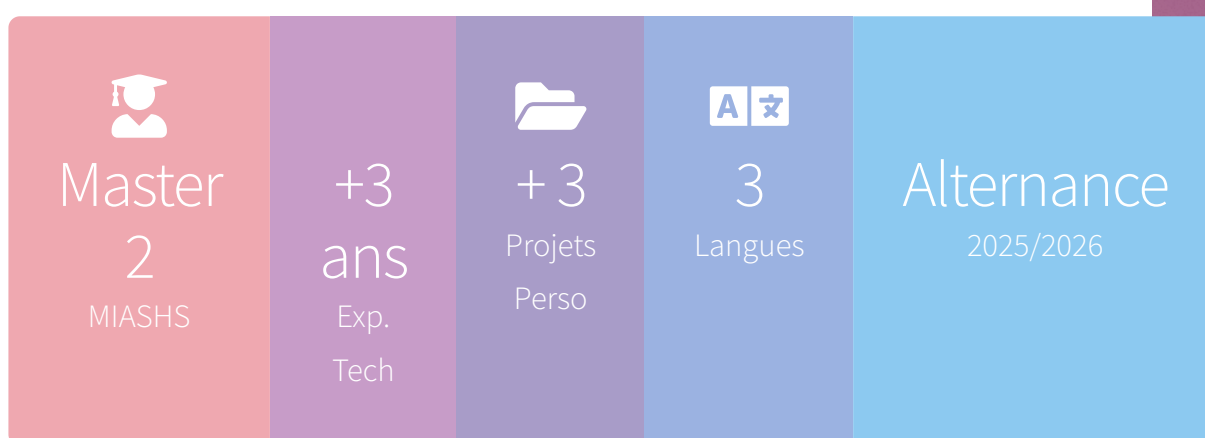
### Compétences Humaines

Esprit d'analyse, Rigueur et discipline, Autonomie, Travail en équipe, Adaptabilité et sens des responsabilités.

# Mon Parcours

---

Un parcours solide en analyse de données, complété par des expériences variées en gestion de projet et support technique, aujourd'hui tourné vers la cybersécurité



De la gestion de projets d'innovation au PNUD à la supervision d'infrastructures chez ANADEN, en passant par le support utilisateur, chaque expérience a renforcé ma capacité à résoudre des problèmes techniques et organisationnels. Mon Master en Mathématiques et Informatique m'a doté d'un esprit analytique rigoureux, que je mets aujourd'hui au service de ma spécialisation en cybersécurité.

## Prêt à Collaborer ?

---

Intéressé par mon profil pour une alternance ou un projet ?  
N'hésitez pas à me contacter via le formulaire ci-dessous ou sur  
LinkedIn.

## De la Théorie à la Pratique

Je suis convaincu que la meilleure façon de maîtriser une compétence est de la mettre en pratique. Découvrez les projets que j'ai menés pour transformer la connaissance en expertise.

[Voir mes Projets](#)

## Coordonnées

**Localisation** Rouen, 76000 •  
France

**Téléphone** (+33) 7 85 94 85 44

**Email** [el.islah.mhoma@gmail.com](mailto:el.islah.mhoma@gmail.com)



# Mes Projets

Démonstration de mes compétences pratiques en cybersécurité et analyse de données.

[Retour à l'Accueil](#)

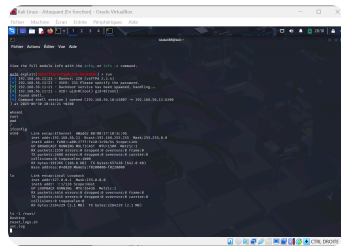
Voici une sélection de projets personnels qui démontrent ma démarche d'apprentissage actif et mon intérêt pour la cybersécurité pratique. Chaque projet est une opportunité pour moi d'appliquer des concepts théoriques à des cas concrets.

---

Projet 1 : Mise en Place et Exploitation d'un Laboratoire de Pentesting

**Objectif :** Construire un environnement virtualisé, isolé et sécurisé pour mener un test d'intrusion





complet, de la reconnaissance initiale à l'obtention d'un accès administrateur sur une machine cible.

## Démarche et Compétences Mises en Œuvre :


1. **Configuration de l'Environnement** : J'ai déployé deux machines virtuelles sous **Oracle VirtualBox**. La machine attaquante est une installation de **Kali Linux**, et la cible une machine **Metasploitable2**, connue pour ses vulnérabilités pédagogiques.
2. **Isolation Réseau** : Pour garantir la sécurité, j'ai configuré les deux VMs sur un **Réseau Interne** dédié, avec un adressage IP statique ( `192.168.56.0/24` ), les coupant ainsi de tout accès extérieur.
3. **Phase de Reconnaissance** : Depuis Kali, j'ai utilisé **Nmap** pour scanner la machine cible. Le scan a révélé plusieurs services ouverts, dont le serveur FTP vulnérable `vsftpd 2.3.4` sur le port 21.
4. **Phase d'Exploitation** : J'ai ensuite utilisé le **Metasploit Framework** ( `msfconsole` ) pour rechercher, configurer et lancer l'exploit `exploit/unix/ftp/vsftpd_234_backdoor` ciblant cette vulnérabilité spécifique.

5. **Résultat** : L'exploitation a réussi, me donnant un **shell** avec les privilèges `root` sur la machine Metasploitable, validant ainsi la réussite complète du cycle de test d'intrusion.

**Outils Maîtrisés** : VirtualBox, Kali Linux, Nmap, Metasploit Framework, Ligne de commande Bash.

---

## Projet 2 : Analyse de Logs de Sécurité

**Objectif** : Appliquer mes  Graphique d'analyse de logs de données (issues de mon Master MIAHS) à une problématique de cybersécurité.

**Description** : En utilisant un jeu de données public de logs de serveur web, j'ai développé des scripts pour parser et analyser les informations. Le but était d'identifier des anomalies telles que des tentatives de connexion par force brute, des balayages de ports ou des requêtes suspectes (injections SQL). Ce projet m'a permis de comprendre l'importance de l'analyse de logs dans la détection d'incidents.

**Outils utilisés :** Excel pour une première analyse, Python (bibliothèque Pandas) pour le traitement avancé.

---

## Projet 3 : Challenges Capture The Flag (CTF)



Profil de la  
plateforme Root-  
Me

**Objectif :** Maintenir une veille technique constante et me mesurer à des problématiques de sécurité variées et réalistes.

**Description :** Je participe régulièrement à des challenges sur des plateformes comme Root-Me. Cela me permet de développer ma créativité et ma rigueur dans la résolution de problèmes en web, forensic, réseau, etc. C'est un excellent moyen de rester à jour et d'apprendre en continu.

**Mon Profil :** Vous pouvez suivre ma progression sur mon [profil Root-Me](#).