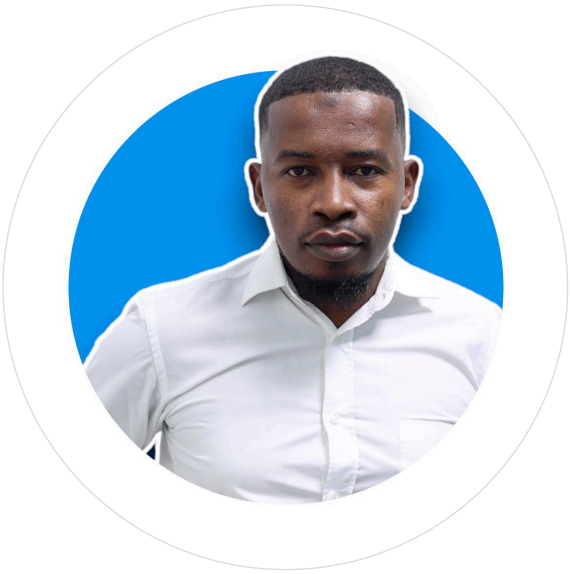
EM

EL ISLAH MHOMA

Analyste de Données & Futurs Expert en Cybersécurité

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.



Découvrir mes projets

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

Master 2	+3 ans	+ 3	3	Alternance
MIASHS	Exp. Tech	Projets Perso	Langues	2025/2026

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

Mes Projets

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

Retour à l'Accueil

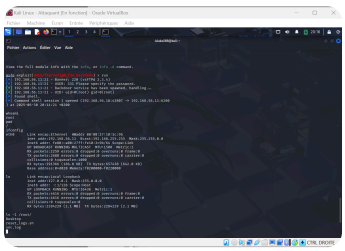
Voici une sélection de projets personnels qui démontrent ma démarche d'apprentissage actif et mon intérêt pour la cybersécurité pratique. Chaque projet est une opportunité pour moi d'appliquer des concepts théoriques à des cas concrets.

Projet 1 : Étude de Cas Complète - Intrusion en Environnement Contrôlé

Ce projet illustre l'intégralité d'un cycle de test d'intrusion, depuis la construction d'un

laboratoire sécurisé jusqu'à l'obtention d'un contrôle administratif total sur la machine cible. L'objectif est de démontrer une maîtrise méthodologique des outils et des concepts fondamentaux du hacking éthique.

Partie 1 : Construction du Laboratoire de Pentesting

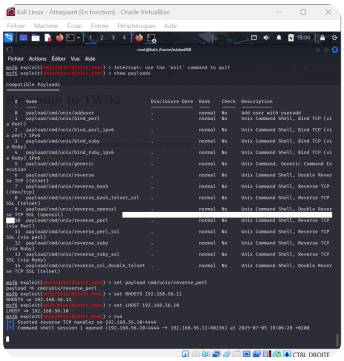


La première étape a été de créer un environnement de travail isolé pour mener mes expériences sans aucun risque.

- **Virtualisation :** J'ai utilisé **Oracle VirtualBox** pour déployer deux machines virtuelles : une machine attaquante **Kali Linux** et une machine cible **Metasploitable2**.
- **Isolation Réseau :** Les deux VMs ont été configurées sur un **"Réseau Interne"** (`intnet`), créant un réseau local virtuel totalement coupé du monde extérieur pour une sécurité maximale.

Partie 2 : Intrusion Initiale via une Vulnérabilité Réseau

Une fois le laboratoire opérationnel, j'ai procédé à l'attaque en suivant une méthodologie structurée.

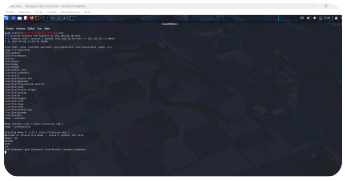


1. **Reconnaissance & Énumération :**
   Un scan Nmap (`nmap -sV`) a révélé un service `distcc v1` vulnérable, connu pour une faille d'exécution de code à distance (RCE).

2. **Exploitation et Résolution de Problème :**
   J'ai utilisé le module `exploit/unix/misc/distcc_exec` de Metasploit. Face à un échec du payload par défaut, j'ai sélectionné un payload plus fiable (`cmd/unix/reverse_perl`) pour établir une connexion inversée.

3. **Résultat & Accès Initial :**
   Après configuration (`RHOSTS` , `LHOST`), l'exploitation a réussi, me donnant un shell avec les privilèges de l'utilisateur `daemon` .

Partie 3 : Escalade de Privilèges via une Faille SUID



L'accès initial en tant que `daemon` étant limité, l'étape suivante était d'obtenir les privilèges administrateur (`root`).

1. **Énumération Locale :**
   Une fois sur la machine cible, une recherche de permissions SUID (`find / -perm -u=s ...`) a révélé que le binaire `nmap` pouvait être exécuté avec des droits élevés.

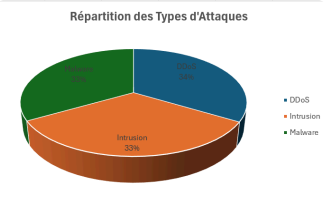
2. **Exploitation de la Mauvaise Configuration :**
   Les anciennes versions de Nmap disposent d'un mode interactif. En lançant `nmap --interactive` , j'ai pu accéder à une console Nmap qui s'exécutait en tant que `root`.

3. **Obtention du Shell Root :**
   Depuis cette console, la commande `!sh` permet d'exécuter un shell système. Cet interpréteur de commandes a hérité des privilèges de Nmap, me donnant ainsi un accès `root` complet, comme confirmé par la commande `whoami` .

Compétences Transversales Démontrées :

`Virtualisation (VirtualBox)` `Configuration Réseau` `Nmap (Scanning)` `Metasploit Framework` `Analyse de Vulnérabilités` `Résolution de Problèmes` `Post-Exploitation` `Escalade de Privilèges (SUID)`

Projet 2 : Détection d'Anomalies par l'Analyse de Logs de Serveur Web



Objectif : Mettre en application mon double profil en utilisant les techniques d'analyse de données de mon Master MIASHS pour résoudre un problème de cybersécurité : la détection d'activités malveillantes dans un grand volume de logs.

Démarche et Résultats :

À partir d'un jeu de données public de logs de serveur Apache, ma méthodologie s'est déroulée en quatre étapes clés :

1. **Parsing et Structuration :**
   La première étape a consisté à écrire un script Python pour "parser" chaque ligne de log et extraire les informations clés (IP, date, requête, code statut, etc.) dans un tableau de données structuré.

2. **Analyse Statistique et Détection de Signaux Faibles :**
   J'ai ensuite analysé les données pour identifier des anomalies. J'ai notamment pu détecter :

   - Des tentatives de **force brute** sur des pages d'authentification (pics d'erreurs 401 depuis certaines IP).
   - Des **scans de vulnérabilités** (grand nombre d'erreurs 404 depuis les mêmes sources).
   - Des tentatives d'**injection de code** (présence de motifs SQL ou XSS dans les URLs des requêtes).

3. **Visualisation des Données (Data Viz) :**
   Pour synthétiser mes résultats, j'ai créé plusieurs visualisations, dont un tableau de bord présentant le top 10 des adresses IP suspectes et un graphique montrant l'évolution des attaques dans le temps.

Compétences Démontrées : `Analyse de Données`, `Python (Pandas)`, `Analyse de Logs`, `Data Visualization`, `Détection d'Incidents`, `Threat Hunting`.

Projet 3 : Apprentissage Continu via Challenges (CTF)

Objectif : Maintenir une veille technique constante, développer ma créativité et renforcer ma rigueur dans la résolution de problèmes de sécurité variés et réalistes.

Démarche : Je suis un participant actif sur la plateforme de hacking éthique **Root-Me**. Cette pratique régulière me permet d'aborder une grande diversité de challenges dans des domaines comme l'analyse de systèmes, le web, ou la cryptographie.

Au-delà des points, chaque challenge est une opportunité d'apprendre une nouvelle technique, de comprendre une nouvelle vulnérabilité et d'aiguiser mes réflexes d'analyste. C'est la démonstration de mon engagement personnel à

rester à jour dans un domaine en perpétuelle évolution.

Mon Profil : Vous pouvez suivre ma progression et les challenges que je valide directement sur mon profil public.

Voir mon Profil Root-Me

Prêt à Collaborer ?

Mon profil vous intéresse ? N'hésitez pas à me contacter directement ou à

Coordonnées

Localisation Rouen, 76000 • France

Téléphone (+33) 7 85 94 85 44

Email el.islah.mhoma@gmail.co

consulter mes profils professionnels pour en savoir plus.

Me Contacter