

# Mes Projets

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

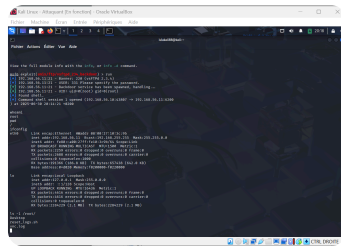
[Retour à l'Accueil](#)

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](#).