



# Plan de progression cybersécurité – 3 mois

---



## Objectif final

À la fin des 3 mois, tu auras :

- Un **lab complet**
  - Des **scripts utiles en Python/Bash**
  - Plusieurs **rapports de tests de vulnérabilité**
  - Des **write-ups de CTF**
  - Un **portfolio en ligne**
- 



## Mois 1 – Mise en place & fondamentaux



### Semaine 1 : Création du lab

- Installer VirtualBox
- Créer un réseau interne
- Installer Kali Linux, Metasploitable 2 et une VM Windows (évaluation)
- Documenter l'installation (fichier PDF ou Markdown pour le portfolio)



#### Livable :

Création d'un lab local de cybersécurité prêt pour les tests d'exploitation, l'analyse réseau et la détection d'intrusions.

---



### Semaine 2 : Reconnaissance réseau

- Utilisation de Nmap : scans TCP, UDP, OS detection
- Utiliser **enum4linux**, **whatweb**, **nikto** sur Metasploitable
- Écriture d'un petit rapport de scan



#### Livable :

Audit réseau de Metasploitable avec Nmap, Nikto, Enum4linux

---



### Semaine 3 : Exploitation basique

- Utiliser Metasploit pour exploiter une faille (vsftpd, samba, etc.)
- Comprendre les payloads, les reverse shells
- Post-exploitation : **whoami**, **uname**, extraction des utilisateurs



#### Livable :

Exploitation d'un service vulnérable avec Metasploit : étude de cas

---

## Semaine 4 : Scripts de base en Python

- Créer un **scanner de port simple** (socket, threading)
- Créer un **extracteur de bannière**
- Documenter ton code (README + commentaires)

### Livrable :

Outils de reconnaissance réseau en Python – scanner de port et bannière

---

## Mois 2 – Sécurisation et détection

### Semaine 5 : fail2ban et logs

- Installer et configurer fail2ban sur un serveur SSH
- Générer des logs d'attaque (via Hydra ou script)
- Observer et expliquer le fonctionnement

### Livrable :

Détection et protection contre le brute-force SSH avec fail2ban

---

### Semaine 6 : Audit Linux

- Créer un script Bash/Python pour auditer :
  - Droits des fichiers `/etc/passwd`, `/etc/shadow`
  - Services en écoute (`ss -tulnp`)
  - Sécurité SSH (`PermitRootLogin`, `PasswordAuthentication`)
- Comparer avec `Lynis`

### Livrable :

Audit de sécurité d'un système Fedora avec script personnalisé

---

### Semaine 7 : Capture réseau avec Wireshark

- Capturer une session HTTP (login non chiffré)
- Identifier les paquets, reconstituer les requêtes
- Étudier un handshake TCP et une résolution DNS

### Livrable :

Analyse réseau : observation d'une session HTTP et DNS avec Wireshark

---

### Semaine 8 : Premier CTF complet

- Choisir une box facile (TryHackMe : "Intro to Pentesting", "Mr Robot")
- Suivre les étapes :

- Scanning
- Exploitation
- Prise de flag
- Faire un write-up clair

#### **Livable :**

Write-up CTF : Mr Robot (TryHackMe)

---

## Mois 3 – Projets concrets et portfolio

### Semaine 9 : Honeypot simple

- Installer Cowrie (ou T-Pot si tu es à l'aise)
- Observer les connexions SSH
- Analyser les logs et les commandes exécutées

#### **Livable :**

Mise en place d'un honeypot SSH avec Cowrie

---

### Semaine 10 : Pare-feu & sécurité réseau

- Configurer **iptables** ou **nftables**
- Règles simples :
  - Bloquer certains ports
  - Autoriser SSH depuis IP fixe
  - Drop par défaut
- Tester via scan

#### **Livable :**

Politique de pare-feu personnalisée pour serveur Linux

---

### Semaine 11 : Portfolio en ligne

- Créer un site web ou un GitHub Pages
- Organiser les projets :
  - Introduction
  - Capture d'écran
  - Liens vers GitHub
  - PDF des rapports
- (Optionnel) version anglaise

#### **Livable :**

Portfolio cybersécurité en ligne – version 1.0

---

## Semaine 12 : Projet libre ou 2e CTF





- Refaire un CTF ou approfondir un sujet vu
- Créer un **rapport d'analyse plus complet**
- Corriger et relire tout ton portfolio

### Livrable :

Deuxième CTF ou projet bonus : approfondissement

---

## Conseils pratiques

-  **Tenir un carnet de bord** (Notion, Obsidian ou fichier Markdown)
-  **Uploader les scripts et write-ups sur GitHub**
-  **Faire des captures d'écran propres**
-  **Ajouter une section "Leçons apprises" à chaque projet**