PENTEST STEPS

Bien sûr ! Tu parles visiblement des **étapes d’un pentest (test d'intrusion)**, et plus précisément de la phase finale : **"Cover Tracks"** (effacer ses traces).

Voici les **5 grandes étapes classiques d’un pentest éthique**, avec une explication simple et claire pour chaque étape. Ces phases sont souvent utilisées dans les tests d’intrusion professionnels, notamment en cybersécurité offensive.

🔍 Les 5 étapes du Pentest (Information Gathering à Cover Tracks)

1. Reconnaissance / Information Gathering

🔍 **Objectif :** Collecter un maximum d'informations sur la cible avant l’attaque.

📌 Ce que tu fais :

- Recherche passive (sans interagir directement avec la cible) :
  - WHOIS lookup
  - DNS lookup (dig, nslookup)
  - Google Dorking
  - OSINT (Open Source Intelligence)
- Recherche active (en interagissant avec la cible) :
  - Scan réseau (nmap)
  - Enumeration de services (FTP, SSH, SMB, etc.)
  - Recherche de sous-domaines

🛠️ Outils utiles :

- `nmap`, `theHarvester`, `dnsenum`, `recon-ng`, `Shodan`, `Maltego`

---

2. Scanning / Enumeration

📡 **Objectif :** Identifier les ports ouverts, services vulnérables, utilisateurs, partages, etc.

📌 Ce que tu fais :

- Scan de ports et détection de services (`nmap`)
- Enumeration des utilisateurs, partages réseaux, vulnérabilités
- Détection de versions logicielles
- Recherche de vulnérabilités connues (CVE)

🛠️ Outils utiles :

- `nmap`, `enum4linux`, `smbclient`, `nikto`, `dirb`, `gobuster`

---

3. Gaining Access (Accès)

🔓 **Objectif :** Exploiter les vulnérabilités trouvées pour obtenir un accès à la machine.

📌 Ce que tu fais :

- Utiliser des exploits (avec Metasploit, exploit-db, etc.)
- Brute-force de mots de passe
- Injection SQL, XSS, RCE, etc.
- Upload de payloads personnalisés

🛠️ Outils utiles :

- `Metasploit Framework`, `sqlmap`, `hydra`, `msfvenom`, `nc`, `netcat`

---

4. Maintaining Access (Persistance)

🔐 **Objectif :** Maintenir un accès persistant à la machine compromise.

📌 Ce que tu fais :

- Installer un backdoor ou reverse shell persistant
- Créer un utilisateur malveillant
- Modifier des scripts de démarrage

- Activer des services cachés

🛠️ Outils utiles :

- Reverse shells personnalisés
- `Meterpreter` (dans Metasploit)
- Scripts de démarrage (Linux : `.bashrc`, Windows : `Startup` folder)

---

5. Cover Tracks (Effacer ses traces)

🧼 **Objectif :** Supprimer les preuves de ton intrusion pour ne pas être détecté.

📌 Ce que tu fais :

- Supprimer les logs système (ex: `/var/log/auth.log`)
- Effacer les fichiers temporaires ou payloads
- Nettoyer les traces d'exécution (historique bash, PowerShell, etc.)
- Désactiver les alertes ou journaux d'événements
- Éviter les outils bruyants qui génèrent du trafic suspect

> ⚠️ Attention légale : Cette étape est réservée aux tests éthiques autorisés. En vrai hacking illégal, effacer des logs est puni par la loi.

🛠️ Outils / Techniques :

- `logcleaner` (scripts personnalisés)
- `timestomp` (pour modifier les timestamps de fichiers)
- Effacement manuel des logs
- Utilisation de rootkits (avancé)

🧪 Résumé Visuel :

Phase	Objectif
1. **Information Gathering**	Collecter des informations passives/actives
2. **Scanning & Enumeration**	Identifier les ports/services/vulnérabilités

3. **Gaining Access**	Exploiter une vulnérabilité pour prendre le contrôle
4. **Maintaining Access**	Maintenir un accès persistant
5. **Cover Tracks**	Effacer les traces pour rester discret

📚 Pour t'entraîner :

Tu peux pratiquer ces étapes sur des plateformes comme :

- TryHackMe
- Hack The Box
- OverTheWire
- VulnHub
- CTFtime pour des challenges CTF

Souhaites-tu que je te montre un exemple concret de pentest étape par étape sur une machine virtuelle vulnérable ? 😎