Fiche - Les étapes d’un Pentest (Test d'intrusion)

1. Phase 1 : Reconnaissance (Information Gathering)

➤ Objectif : Collecter un maximum d’informations sur la cible.

Deux types :

- **Passive** : sans interagir directement (whois, OSINT, moteurs de recherche, Shodan…)
- **Active** : en interrogeant directement la cible (ping, traceroute, DNS, port scanning léger)

But : connaître le domaine, les IP, les services visibles, les technologies utilisées.

2. Phase 2 : Scan & Cartographie

➤ Objectif : Identifier les portes d’entrée (ports, services, OS, etc.)

- **Scan de ports** : avec Nmap, Masscan…
- **Détection de services** (bannières, versions logicielles)
- **Scan de vulnérabilités** : avec Nessus, Nikto, OpenVAS, etc.

But : établir une **cartographie réseau + logicielle** de la cible

3. Phase 3 : Exploitation

➤ Objectif : Exploiter les failles détectées (accès non autorisé, élévation de privilèges…)

- Injection SQL, XSS, faille RCE, bruteforce, attaque réseau…
- Utilisation de Metasploit, scripts maison, ou attaques manuelles.

🎯 But : prouver que la faille est **réellement exploitable, obtenir un shell, une session ou un accès au système**.

4. Phase 4 : Post-Exploitation

➤ Objectif : Comprendre l’impact d’une compromission réussie

- Maintien de l’accès (backdoor, shell inversé…)
- Mouvement latéral (propagation sur d’autres machines)
- Récupération d'infos sensibles (mots de passe, mails, documents internes)

🎯 But : Comprendre et montrer ce que l'on peut faire avec l'accès.

5. Phase 5 : Restauration & Remédiation (si demandé)

En pentest **boîte blanche / collaborative**, on peut :

- **Aider à corriger** les failles,
- **Supprimer les accès** utilisés pour l'exploitation.

🎯 But : ne rien laisser derrière soi, et parfois **aider les équipes à corriger**.

6. Phase 6 : Rapport (Reporting)

➤ Objectif : Documenter l'ensemble du test

- Résumé exécutif pour la direction
- Détail technique pour les équipes IT
- Gravité des vulnérabilités (CVSS)
- Preuves (captures, logs)
- **Recommandations de correction**

🎯 But : **apporter de la valeur au client** et lui permettre d'améliorer sa sécurité.

Et souvent une Phase 7 : Retest (optionnelle)

Une fois les failles corrigées, un **test de validation** peut être demandé pour confirmer que les vulnérabilités sont bien bouchées.