PENTESTING

Tests d'intrusion — Guide de référence

Qu'est-ce que le pentesting ?

Le **pentesting** (ou **test d'intrusion**) a été créé pour tester les failles de sécurité d'un réseau, d'un site internet, d'un ordinateur ou, plus généralement, de tout système informatique.

Il consiste à faire intervenir un **hacker éthique**, mandaté par une entreprise, afin de simuler une attaque réelle de manière légale et contrôlée.

Une fois l'attaque effectuée, le **pentester** doit informer l'entreprise de toutes les failles trouvées et proposer des recommandations pour renforcer sa sécurité.

Les types de hackers

On distingue généralement trois types de hackers, dont certains pratiquent le pentesting :

♡ White Hat — Chapeau blanc

Hackers éthiques agissant avec l'autorisation de l'entreprise.
Rémunérés légalement pour tester et renforcer les systèmes.

Gray Hat — Chapeau gris

Situés entre légalité et illégalité.
Peuvent découvrir des failles sans autorisation, mais sans nuire intentionnellement.
Méthodes juridiquement discutables.

♥ Black Hat — Chapeau noir

Hackers malveillants aux actions illégales.
Objectifs : vol, destruction, revente de données ou extorsion.

Le processus d'un pentest

Le déroulement d'un pentest peut varier selon le professionnel, mais suit généralement les étapes ci-dessous :

1

Reconnaissance

Collecte d'informations sur la cible : organisation, employés, adresses e-mail, technologies utilisées, infrastructure, etc.
Ces données aident à identifier des points faibles (mots de passe, failles humaines…).

2

Analyse et scan

Cartographie et analyse du réseau.
Utilisation d'outils de scan pour détecter les services ouverts, vulnérabilités et mauvaises configurations.

3

Exploitation

Tentatives d'intrusion pour exploiter les failles détectées.
Techniques : bruteforce, injections, escalade de privilèges, etc.
Objectif : démontrer concrètement les risques.

4

Post-exploitation

Évaluation de l'impact réel de la compromission.
Jusqu'où l'attaquant peut aller : accès aux données, contrôle du système, mouvements latéraux…

5

Rapport final

Rédaction d'un compte rendu complet comprenant :

- les failles trouvées et leur niveau de gravité
- les preuves d'exploitation
- les recommandations de correction

Se former au pentesting

Il existe plusieurs plateformes pour s'entraîner légalement au pentesting :

- ▶ **TryHackMe**
- ▶ **Root-Me**
- ▶ **Hack The Box**
- ▶ **PortSwigger Web Security Academy**

Ces sites proposent des laboratoires pratiques pour apprendre les techniques d'attaque et de défense.