**Définition du métier:**

Un pentester est un professionnel de la cybersécurité dont le travail est d’effectuer des tests d’intrusion qui sont des attaques contrôlées sur le réseau informatique du client qui simulent des attaques de hacker, en utilisant les mêmes techniques et qui ont pour but d’évaluer le niveau de sécurité du système, trouver les défauts et failles qu’ils pourraient y avoir et par la suite chercher et proposer des solutions à ces problèmes.

**Comment fonctionne un pentest?:**

Un test d’intrusion peut être divisé en 5 étapes:

1. Planning et reconnaissance: on définit les objectifs du test dont les systèmes qui vont être traités et les méthodes de test que l’on va utiliser.
2. Mapping: rassembler des informations sur la cible afin de mieux comprendre son fonctionnement et de se faire une idée des failles potentielles et des éléments les plus vulnérables.
3. Discovery: une phase d’attaque durant laquelle les pentesters cherchent des vulnérabilités via des recherches manuelles avec le soutien d’outils automatisés dont l’objectif est de découvrir le plus de failles possibles.
4. Exploitation: c’est un test dans lequel le pentester tente d’exploiter les failles identifiées précédemment, cette étape permet d’utiliser les premières failles trouver pour tenter d’en trouver de nouvelles liées à celles trouvées en 1er lieu. Permet d’avoir une évaluation plus complète du niveau de sécurité d’un système.
5. Analyse: les résultats du test sont compilés dans un rapport décrivant les failles exploitées, les données sensibles auxquelles ont à accéder et la durée pendant laquelle le pentester est resté dans le système dans se faire repérer. Ces informations sont analysées pour aider à configurer un pare-feu et corriger les failles pour protéger des futures attaques..

différentes méthodes: blackbox (=simule une attaque en tant que hacker, pentester possède peu ou pas d’infos, il doit prendre le temps d’explorer ce qui peut laisser le tps a la cible de réagir),

whitebox (=pentester en collaboration avec le service de sécurité du client, le pentester possède toutes les infos dont il a besoin, ressemble à un contrôle de sécurité classique )

, greybox (= entre 2, le pentester possède des infos limitées et en cherche pendant l’attaque, permet de simuler des attaques venant de l’intérieur)

exemple d’outil utilisé par les pentester, Nmap= scanner de port qui permet d’analyser un serveur à distance et déterminer quels ports sont ouverts

**Qualité requises pour faire le métier**:

* sens de l’éthique (c’est un hacker qui pirate pour aider et non pas à des fins personnels)
* curiosité
* être réactif (pouvoir s’adapter à toute situation lors d’un test d’intrusion)
* aimer travailler en équipe (
* ne pas avoir peur des défis

**Quels langages/outils dois-je maîtriser?:**

* Compétences avancées en sécurité informatique, architecture(=structure générale d’un système informatique) et systèmes des réseaux informatiques(=les appareils informatiques interconnectés)
* Compétences en programmation (Python, C/C++,...)
* Compétences en langages de programmation web (Java, PHP,...)
* En développement d’applications, de logiciel
* En gestion de systèmes d’exploitation
* Parler anglais
* Suivre de près l’évolution des techniques de hacking

sources:

[Pentester : fiche métier avec les missions, la formation...](https://guardia.school/metiers/pentester.html#competence)

[Qu'est-ce que le pentesting en cybersécurité | Jedha](https://www.jedha.co/formation-cybersecurite/pentesting)

[Métier Pentester : salaire, formation, missions, compétences](https://www.jedha.co/formation-cybersecurite/metier-pentester#quelles-sont-les-qualites-et-competences-dun-pentester)

[What is Penetration Testing | Step-By-Step Process & Methods | Imperva](https://www.imperva.com/learn/application-security/penetration-testing/)

[Test d’intrusion : approche, méthodologie, types de tests et prix](https://www.vaadata.com/blog/fr/test-dintrusion-approche-methodologie-types-de-tests-et-prix/)

[Quels sont les meilleurs outils de pentest ? - GPLExpert](https://gplexpert.com/pentest-meilleurs-outils/)