Pentester

Autres appellations en français :

- **Auditeur Cybersécurité**

Autres appellations en anglais:

- **Penetration Tester**
- **Ethical Hackers**

Définition :

Le Pentester se met dans la peau d'un hacker potentiel et réalise des tests d'intrusion (« penetration test ») afin d'évaluer la sécurité d'un système informatique. Le rôle de ce professionnel de la sécurité informatique est de trouver toutes les failles de sécurité d'un système puis de procéder à des tests d'intrusion, autrement dit des attaques contrôlées grandeur nature.
Le métier de pentester consiste à contrôler la sécurité de tout un ensemble d'applications web. On peut citer les applications mobiles, le back end de sites web qui enregistrent des numéros de cartes de crédits etc.

Le Pentester est chargé principalement :

- **Rechercher** des informations sur Internet au sujet de sa cible, reconnaissance passive.
- **Vérifier** les demandes d'assistance de la société sur le WEB (des posts sur Github par exemple)
- **Scanner** le serveur cible à la recherche de son adresse IP, des ports ouverts etc.
- **Définir** le niveau de criticité des failles trouvées et mettre l'accent sur certaines d'entre elles
- **Préparer** un test d'intrusion sous la forme d'un proof of concept, prouver la faille dans un cadre sécurisé
- **Réaliser un rapport de l'intrusion**
- **P**résenter ses conclusions à l'équipe responsable du serveur
- **Orienter** les équipes techniques quant aux correctifs ou palliatifs à mettre en œuvre pour sécuriser le réseau et les systèmes informatiques

Activités complémentaires :

- **Assurer** une veille technique sur les menaces actuelles et la cyberdéfense
- **Connaître** les langages de programmation (Python,Java, Scala…).
- Maîtriser Linux et ses distributions axées sécurité (ex : Kali Linux)
- Participer à des événements « Capture the flag », où l'objectif est de trouver et d'exploiter les vulnérabilités d'un système afin de s'y introduire.
- **Connaître** les systèmes auxquels on va s'attaquer !

Travaillé en NSI :

- *Terminale et 1ère – Architectures matérielles, systèmes d'exploitation réseaux*
- *1ère – Interactions entre l'homme et la machine sur le Web*

Études Post-bac :

diplômé Bac +5 d'une école d'Ingénieur ou équivalent avec une spécialisation principale dans le domaine de la sécurité ou alors dans de rare cas des autodidactes

Principales compétences :

- Réseau et sécurité
- Rigueur et Organisation
- Savoir programmer
- Résistant au Stress
- Curieux et Autonome
- Aimer apprendre par soi-même