**MÉTIER**

Professionnel de la cybersécurité, le pentester contrôle la sécurité des réseaux informatiques en opérant des tests d’intrusion ou “penetration test” en anglais, d’où l’intitulé de son métier. Il identifie ainsi les vulnérabilités et propose des actions pour les corriger.

**MISSIONS DU PENTESTER**

Les entreprises de plus en plus sujettes aux cybermenaces doivent se doter d’experts en cybersécurité capables de raisonner de la même manière que leurs potentiels attaquants, ceci afin de limiter et anticiper au maximum les failles et intrusions malveillantes dans leur système informatique.

Le pentester est ce professionnel de la sécurité informatique dont la mission consiste à infiltrer « volontairement » un réseau ou une application informatique afin d’en évaluer le niveau de sécurité.

Son approche s’apparente à celle du pirate informatique, utilisant les mêmes techniques et approches que le hacker malveillant, mais en les détournant au bénéfice de l’entreprise.

Le pentester réalise des tests d’intrusion pour vérifier la sécurité informatique de l’entreprise

Le pentester va ainsi effectuer des tests d’intrusion pour vérifier la sécurité informatique de l’entreprise et fournir des solutions pour réduire la vulnérabilité des systèmes.

## TESTS D’INTRUSIONS, SCANS DE VULNÉRABILITÉ ET AUDITS

Un test d’intrusion, ou test de pénétration, ou encore pentest, est une méthode qui consiste à analyser une cible en se mettant dans la peau d’un attaquant.

Cette cible peut être une IP, une application, un serveur web, ou un réseau complet.

Le scan de vulnérabilité, différent du test d’intrusion, est en fait une composante du test d’intrusion, c’est-à-dire une sous-partie. C’est plus précisément un scan de la cible qui permet d’énumérer les vulnérabilités, sans tenter de les qualifier ou de vérifier si elles sont exploitables.

Les tests d’intrusion ont des objectifs clairs :

* Identifier les vulnérabilités du SI ou de son application
* Évaluer le degré de risque de chaque faille identifiée
* Proposer des correctifs de manière priorisée

Grâce au test d’intrusion, le pentester peut qualifier la sévérité de la vulnérabilité, la complexité de la correction, et l’ordre de priorité qu’il faut donner aux corrections.

Afin de sécuriser l’infrastructure ou l’application, les tests d’intrusion peuvent être réalisés à différents moments de la vie d’une entreprise. Ainsi, ces derniers peuvent être initiés lors de la conception du projet, afin d’anticiper les éventuelles attaques, pendant la phase d’utilisation, à intervalle régulier et enfin, suite à une cyberattaque afin que celle-ci ne se reproduise plus .

Le test d’intrusion peut se faire de l’extérieur (test d’intrusion externe). Ce test d’intrusion pourra être réalisé de n’importe quelle connexion Internet.

Le test d’intrusion peut également se faire de l’intérieur de l’infrastructure (test d’intrusion interne). Dans ce cas, le test sera opéré sur le LAN (réseau interne de l’entreprise).

Grâce à ces dispositions, le pentester évalue les failles et essaye d’attaquer le système. Les systèmes de défense à savoir l’antivirus et les firewalls sont contournés par les outils mis en avant pour l’intrusion.

Enfin, les missions du pentester peuvent aller au-delà d’un test d’intrusion de système informatique. Elles peuvent concerner la totalité des équipements dont dispose son terrain d’intervention au sein de l’entreprise. Ainsi, le pentester pourra également réaliser des audits complets pour l’entreprise. Il en existe plusieurs types :

* Audits de code : le code source d’une application est analysé afin de relever toute faille de sécurité.
* Audits de configuration :  la configuration d’un système ou d’un équipement réseau est fournie au pentester qui compare ensuite ces données à des référentiels officiels (CIS, guides de l’ANSSI…) pour relever tout écart de conformité.
* Audits d’architecture:  le pentester vérifie la robustesse de l’architecture d’un système d’information face à différentes menaces. Cela est réalisé à partir des documents d’architecture client et d’entretiens.
* Audit organisationnel: le pentester vérifie l’organisation mise en place par le client d’un point de vue sécurité, de la création d’une équipe dédiée à la gestion des incidents, à partir des documents disponibles et des entretiens avec le client.

**RESPONSABILITÉS DU PENTESTER**

S’introduire légalement dans les systèmes et les réseaux d’une entreprise nécessite pour le pentester de se conformer à un code de conduite et à une discipline stricte.

Le pentester devra documenter le chemin d’attaque qu’il communique à l’organisation, signer un accord de confidentialité et traiter toutes les informations de l’entreprise avec la plus grande prudence. Le pentester devra signaler immédiatement à l’organisation toute violation de sécurité. Enfin, il devra effacer toutes les traces de tests de vulnérabilités pour éviter toute exploitation malveillante des failles précédemment identifiées.

**COMPÉTENCES**

Exercer comme pentester demande des compétences nombreuses et étendues :

* Capacité de compréhension des menaces cybersécurité
* Capacité à exploiter des sources ouvertes de manière sécurisée
* Mise en place de plans de veille sur un ou plusieurs secteurs déterminés
* Détection, qualification et analyse d’informations pertinentes
* Connaître le droit et les réglementations en vigueur en matière de cybersécurité

A cette base théorique, il faut ajouter de très nombreuses connaissances pratiques qui ne peuvent s’acquérir que par l’expérience. Un bon moyen de commencer consiste à participer à des événements tels que « Capture the flag », où l’objectif est de trouver et d’exploiter les vulnérabilités d’un système afin de s’y introduire.

**QUALITÉS**

Le pentester est un professionnel de la cybersécurité dont les missions visent à limiter et anticiper au maximum les failles et intrusions malveillantes dans le système informatique de l’entreprise. Si ses compétences sont bien un atout, ses qualités doivent suivre aussi. Les unes ne vont pas sans les autres. Cela se traduit par être :

* Ethique et légal
* Curieux
* Dynamique
* Réactif
* Créatif
* Disponibile
* Faire preuve de confidentialité
* Aimer le travail en équipe
* Avoir le goût du défi
* Le pentester fournit des solutions de sécurité à l’entreprise afin de l’aider dans la lutte contre les cybermenaces

## ÉTUDES ET FORMATIONS

* Pour devenir pentester , vous devrez justifier d’un diplôme en informatique de niveau Bac +3 à 5 avec une spécialisation en cybersécurité. Une école dans les métiers de la cybersécurité le permet. Des certifications en sécurité/produit seront demandées parfois.
* A savoir que certains pentesters se sont formés en autodidactes puisqu’il s’agit d’un nouveau métier qui passionne les génies de l’informatique. D’ailleurs, des hackers pirates (dans l’illégalité) ont choisi de retrouver “le droit chemin » en devenant pentester au sein de grands groupes et sociétés.

## QUELLE FORMATION CHOISIR ?

En intégrant le Master of Science, vous obtiendrez les compétences nécessaires pour rejoindre les équipes d’attaque et d’intrusion d’une entreprise. Cette formation permettra aux futurs pentester de comprendre les problématiques techniques d’architecture réseau, de gestion des données et de détection de failles des systèmes. Des projets seront à réaliser tout au long de votre cursus sans oublier des stages et rencontres avec des professionnels du milieu.

[Pour en savoir plus sur la formation…](https://guardia.school/formations-cybersecurite.html)

## SALAIRE

La rémunération d’un pentester varie en fonction de la taille de l’entreprise qui l’emploie, de son expérience et du lieu de travail.

En moyenne, un étant débutant en France, il touchera 3 000 euros par mois et peut voir son salaire à plus de 5 000 euros en tant que sénior.

Aux États-Unis, le salaire annuel moyen d’un pentester avoisine les 110 000 dollars.

Le salaire d’un pentester peut presque dépasser les 100 000 dollars de l’autre côté de l’Altantique

**DANS QUEL SECTEUR TRAVAILLER ?**

Le pentester peut exercer dans divers secteurs industriels, de services ou encore dans le secteur public. Il peut aussi évoluer dans les secteur suivants :

* Logiciel, informatique et numérique
* Bancaire
* Télécommunications
* Santé

**ENTREPRISES QUI RECRUTENT DES PENTESTERS**

Elles sont toujours plus nombreuses à rechercher des profils experts en cybersécurité et le métier de pentesters n’échappe pas à la règle. Où travailler alors ? Réponse :

* Airbus
* Orange Cyberdéfense
* Yes we hack
* Sopra Steria

Des offres d’emploi pour exercer en tant que pentester sont disponibles sur des sites généralistes ou spécialisés :

* Cyberjobs.fr
* Monster.fr
* Jobrapido.com
* LinkedIn
* Simplyhired.fr
* Wizbii.com
* Indeed.com
* Jooble.org
* Apec.fr
* Glassdoor.fr

**PENTESTER FREELANCE**

Le pentester peut exercer en tant que freelance. Le tarif journalier moyen peut alors varier de 400 à 1 500 euros, en fonction de ses expériences et références en entreprise. Choisir ce statut, c’est être conscient des enjeux qui reposent sur vos épaules puisque vous devrez maîtriser le sujet, faire preuve de rigueur, d’organisation et d’un sens de la communication. Tout le monde ne peut ainsi pas devenir indépendant.

**EVOLUTION DE CARRIÈRE**

Aux vues de la hausse et de la diversité des menaces cybercriminelles, le pentester devient un expert de plus en plus recherché en entreprise.

En France, les pentesters sont souvent, à la base, des experts en systèmes d’information ou des experts sécurité et réseaux formés par la suite en cybercriminalité. Néanmoins, des formations dédiées au métier de pentester se développent de plus en plus et laissent entendre que le métier a de beaux jours devant lui.

Le pentester et le hacker éthique semblent être étroitement liés de part leurs missions et les deux termes sont souvent utilisés de façon interchangeable . Pourtant, les deux métiers présentent quelques différences.

Ainsi, le pentester met beaucoup plus l’accent sur les étapes ou les processus  permettant de trouver des failles de sécurité sur un système d’information alors que le hacker éthique va plus loin et essaie d’améliorer la sécurité du système cible.

Un hacker éthique est donc un pentester dont la mission est de trouver les moyens pérennes d’améliorer la sécurité du système d’information cible. Après avoir exercé plusieurs années comme pentester, il est donc possible de se spécialiser ensuite en hacking éthique.

**LES AVANTAGES ET INCONVÉNIENTS**

Si vous aimez les puzzles, les casse-têtes et autres challenges, faire du pentest votre métier sera pour vous tout sauf ennuyant !

Néanmoins, sachez que le pentester, contrairement à l’imaginaire collectif qui gravite autour de son métier, n’est pas un geek solitaire et insociable.

C’est avant tout un consultant qui doit s’adapter à son auditoire en vulgarisant parfois, et qui doit savoir s’exprimer aussi bien à l’oral qu’à l’écrit . Il ne faut donc pas avoir peur de s’exprimer auprès de cibles variées, direction, équipes, clients, etc.

Le métier est exigeant, il faut savoir se mettre au niveau rapidement, réaliser un travail de veille important et constant car les technologies et les vulnérabilités évoluent aussi vite que les missions du pentester.

**DEVENIR PENTESTER**

**Quelles sont les missions du pentester ?**

En résumé, le pentester est un professionnel de la cybersécurité dont les missions visent à limiter et anticiper au maximum les failles et intrusions malveillantes dans le système informatique de l’entreprise.

Le pentester va ainsi effectuer des tests d’intrusion pour vérifier la sécurité informatique de l’entreprise et fournir des solutions pour réduire la vulnérabilité des systèmes.

**Quel est le salaire du pentester ?**

En moyenne, le pentester débutant qui exerce en France touchera  3 000 euros par mois à 5 000 euros pour un profil sénior.

**Quel niveau d’étude pour devenir pentester ?**

Pour devenir pentester, vous devrez justifier d’un diplôme informatique de niveau Bac +3 à Bac+ 5 avec une spécialisation en cybersécurité.

**Quel Bac choisir ?**

Au lycée, nous vous conseillons de suivre un Bac général ou technologique et d’opter pour l’une des spécialités suivantes en mathématiques, sciences de l’ingénieur ou sciences informatiques.

**Quelle est la formation pour devenir pentester ?**

A Guardia Cybersecurity School, le Master of Science en deux ans accorde une place importante à l’expertise cyber aussi bien dans la maîtrise technique que dans le déploiement de stratégie et le développement personnel. Une formation dont votre niveau de compétences à la sortie sera élevé. De quoi vous permettre de travailler pour des entreprises qui cherchent des experts.

Nous recherchons un pentester/ingénieur sécurité pour une mission de plusieurs mois sur Toulouse :  
  
descriptif détaillé de la prestation : Réalisation des tests d'intrusion applicatif et infrastructure dans l’objectif d’identifier les failles potentielles  
Environnement technique : Montée en puissance des pratiques de sécurisation des développements  
Renforcement de l'équipe CERT en construction.  
Travail en équipe.  
  
Connaissance de la sécurité dans les développements, vulnérabilités, méthodes de développement sécurisé (OWASP…)  
Connaissances en Pentests notamment applicatif  
Connaissance des méthodes, outils de tests d'intrusion notamment applicatif  
Connaissance des architectures et langages de développement Web et mobile. (HTML, JavaScript, API, IOS, Androïd, Java, .Net…)  
Certifications : CEH  
CISSP  
SECWEB  
GWEB  
GWAPT  
  
Des travaux complémentaires seront réalisés avec une participation sur des sujets d'automatisation (outil BIRT)

## Définition du Pentester/Ethical Hacker

Pentester est un terme qui provient de la contraction des deux mots anglais "Penetration" et "Testing".

Le pentester est un professionnel qui assure la sécurité des réseaux informatiques au moyen de tests d'intrusion qui consistent à trouver les failles de sécurité d'un système et procéder à des attaques contrôlées.

Ces failles ne concernent pas uniquement les brèches au niveau de la sécurité, qui rendent possible le contrôle à distance d'une machine. Elles concernent également la simple divulgation d'information par un système qui peut alerter un pirate informatique et le mener à lancer une attaque ou hacking. Le pentester permet à son client **d'appréhender en toute objectivité le niveau actuel de sécurité de son système et l'assiste en vue de son amélioration**.

Ce professionnel est également appelé **Ethical Hacker** même si de subtiles différences sont à noter entre ces deux termes. Le Ethical Hacker, aussi appelé White Hat Hacker, base ses actions sur l'éthique du hacker : mettre en avant la liberté des informations et l'amélioration des qualités de vie. On parle ainsi d'Ethical Hacking pour désigner un ensemble de techniques de piratage et d'attaques qui permet de détecter des failles de sécurité sous réserve du consentement du propriétaire.

## Le rôle et les missions du Pentester

La principale mission d'un Pentester est d'assurer la **sécurité informatique des systèmes** de ses clients. Dans cette optique, il se base sur sa connaissance des techniques d'hacking pour :

* identifier les vulnérabilités du système de sécurité,
* évaluer le risque d'attaque associé à chaque faille identifiée,
* proposer des solutions adaptées de manière priorisée.

Le Pentester, grâce au test d'intrusion, parvient ainsi à évaluer avec précision la sévérité de la brèche identifiée, la complexité des corrections à apporter et leur ordre de priorité.

Le test d'intrusion peut être effectué de l'extérieur à partir d'une simple connexion internet ou de l'intérieur de l'infrastructure sur le réseau interne de l'entreprise.

Les missions du Pentester ou de l'Ethical Hacker vont également bien au-delà du test d'intrusion. Elles peuvent également concerner d'autres aspects comme **les audits complets pour son entreprise cliente**. Ceux-ci peuvent être de différents types :

* audit de code source : permettent d'analyser le code source d'une application dans le but d'identifier d'éventuelles failles de sécurité,
* audit d'architecture : consistent à vérifier la robustesse d'un système d'information face à des menaces de sécurité,
* audit de configuration : fournissent au Pentester la configuration d'un équipement réseau. Il se charge alors de les comparer avec des référentiels officiels afin d'identifier tout écart de conformité.

Dans son travail, le Pentester peut avoir accès à des informations sensibles, voire confidentielles. Or, il ne peut en aucun cas s'en servir. Il est tenu de **respecter scrupuleusement la législation en vigueur et les règles fixées par les auditeurs**. Au cours de son introduction légale dans le système et les réseaux de son client, le Pentester se doit de documenter le chemin d'attaque qu'il lui communique.

Les Pentesters signent le plus souvent uneclause de confidentialité très spécifique. Ils doivent également signaler de suite à leur client toute violation de sécurité et effacer toutes les traces de tests afin d'éviter leur exploitation à des fins malveillantes.

## Les compétences et qualités d'un Pentester

### Les compétences du Pentester

La profession de Pentester exige une très bonne compréhension de **techniques de hacking, du développement logiciel et des systèmes informatiques.** **De solides connaissances en réseau et en sécurité informatique**(système de codage, cryptographie, audit de sécurité…) sont également nécessaires.

De même, un véritable Pentester doit disposer de réelles **compétences en programmation et langage de programmation web** comme le Java et le PHP. Et pour cause, les tests d'intrusion sont le plus souvent réalisés de manière automatisée avec desapplications logicielles. Posséder des connaissances en Linux et en particulier ses distributions orientées sécurité à l'instar de Kali Linux est également recommandé.

Cependant, cette base théorique n'est pas suffisante : des connaissances pratiques doivent également être acquises.

Elles ne peuvent se faire que par l'expérience. **La participation à des évènements de type Capture the flag ou capture de drapeau en français est une expérience très enrichissante.** Bon nombre de Pentesters ou Ethical Hackers y prennent d'ailleurs part. L'objectif est d'identifier et d'exploiter la vulnérabilité d'un système pour s'y introduire. Les drapeaux qui sont la preuve de l'intrusion sont alors récupérés. Réussir ce type de compétition nécessite la connaissance de nombreuses astuces hacking et la capacité à les réutiliser au bon moment.

### Les qualités

Les compétences et la seule connaissance de techniques d'hacking ne suffisent pas pour devenir un bon Pentester ou Ethical Hacker. À cela s'ajoutent également des qualités incontournables comme la curiosité, le dynamisme et la réactivité.

Faire preuve d'éthique est également une qualité que doit posséder tout Pentester qui souhaite évoluer dans le domaine de la sécurité informatique.

L'éthique et la confidentialité règnent en effet en maître absolu dans son secteur et**c'est d'ailleurs ce qui le distingue principalement des pirates informatiques**. De plus, faire preuve de disponibilité et avoir le goût du défi sont des qualités recherchées chez un Pentester.

## Salaire et évolution de carrière pour le Pentester

Au début de sa carrière, le salaire d'un Pentester est au minimum de 3000 euros par mois, soit **36OOO euros par an**. En fonction de son expertise et de son expérience, le salaire moyen annuel peut atteindre 48 000 euros. Les Pentesters comme d'autres professionnels peuvent également connaître une évolution dans leur carrière. Après quelques années d'expérience, ils peuvent **devenir responsables d'intrusion et se spécialiser dans un système particulier** (pentest de systèmes industriels par exemple). Ils sont également libres de se mettre à leur propre compte en créant un cabinet de conseil en sécurité informatique.

‍

## Les formations pour devenir Pentester

Pour développer les nombreuses connaissances en hacking et compétences nécessaires pour exercer cette activité, une formation de qualité s'impose.

Notre formation Cybersécurité Essentials délivre ces connaissances car elle couvre de nombreuses thématiques comme le **monitoring des menaces systèmes**et**les tests de pénétration**. Elle permet au Pentester ou à l'Ethical Hacker en devenir de **comprendre les problématiques des architectures réseau, de l'identification des failles de sécurité et de la gestion des données**.

Devenir un Pentester nécessite un **bon niveau en informatique**. Pour y parvenir, il est possible de suivre une école d'ingénieur en informatique avec une spécialisation en cybersécurité. Un cursus niveau Bac + 5 ou BAC + 3 suffit également pour faire carrière dans ce métier passionnant qui en est encore à ses débuts. Certaines entreprises exigent également des certifications de sécurité pour recruter leurs pentesters. Il est donc pratique au-delà de la formation de pouvoir disposer de certifications de tests d'intrusion comme le CEH et l'OSCP.

Un CEH ou **Certified Ethical Hacker** est un professionnel qualifié de la sécurité informatique. Un Pentester certifié CEH dispose des outils et techniques d'hacking les plus utilisées par les pirates afin de devenir un hacker éthique. L'OSCP ou certification Offensive Security Certified Professional se focalise, tout comme le CEH, sur les tests d'intrusion et le piratage informatique. De même, de nombreux Pentesters sont de véritables autodidactes qui se sont formés seuls à l'informatique et aux techniques d'hacking. Certains anciens hackers ont même pu devenir Pentester après avoir retrouvé le droit chemin.

### **Réf : Ingénieur Cyber-sécurité / Pentester (H/F)**

**Safari Technologies :** Entreprise spécialisée dans les infrastructures système réseau et sécurité opérant dans la France entière, nous avons mis en place un management à visage humain, proche de nos collaborateurs, assurant un suivi adapté et une réactivité face à vos demandes, recherche Ingénieur sécurité possédant 3 ans d’expérience et plus dans l’exploitation et le maintien en conditions opérationnelles des infrastructures réseau et sécurité, orienté vers des technologies innovantes telles que Cisco, Firewall, FW JUNIPER, IBM IPS , IBM Scanner, Juniper, SIEM.  
 **Vous devrez  :**

Présenter à différents niveaux hiérarchiques les résultats  
Apporter des conseils et recommandations adaptés aux problèmes de sécurité rencontrés par des clients.  
Définir les besoins nécessaires à la bonne réalisation des audits et tests des solutions  
Maintenir et tester les méthodologies d’audit

Expérience demandée :  
Diplômé Bac+5 ou plus dans le secteur de l’informatique et de la sécurité, justifiez d’une expérience de 3 à 5 ans dans un poste équivalent sur ces différents aspects :

Bonne connaissance du monde Unix et Windows (Seven, 2008, 2012 ?)  
Connaissance en Sécurité : principe généraux, Firewall, IDS, IPS, cryptographie, authentification, audits, mobile  
Connaissance en Réseaux : TCP/IP, Ethernet, wifi  
Connaissances de base en développement C, Scripting, .NET & J2EE  
Certification attendues CEH, OSCP, CISA, GIAC/GPEN-GXPN  
Connaissances des standards OWASP, CIS Benchmarks, NIST