Clément Arki
Alexandre Fernandes
BTS SIO 1

Exposé : Pentester

1. Description du poste, rôle dans l'organisation

Un pentester est un professionnel de la sécurité informatique qui a une éthique, qui est un expert technique avec de l'expérience, qui est cultivé et découvre les vulnérabilités pas encore connues et non publiées, c'est -à -dire les 0 days. Ils font des tests complets visant à déterminer leur vulnérabilité aux attaques en utilisant des méthodes et techniques qui sont mises en place par de vrais attaquants ou pirates (un pirate est une personne qui va chercher à piller un système informatique en détruisant ses protections). Il essaye aussi de pénétrer dans un système sans autorisation et permet ainsi de découvrir des faiblesses et mieux évaluer les risques potentiels. Ils doivent suivre des méthodologies référencées et utiliser des outils de reporting pour répertorier les incidents détectés. D'après la Loi pour la confiance en l'économie numérique ce sont des personnes légales car il existe d'autres hackers qui sont hors la loi comme les Blacks hats, les Crackers White Hats etc.
Souvent les Pentesters étaient des White Hats dont leur but est d'aider à la sécurisation du système, sans en tirer profit et ainsi divulguer totalement leur découverte et prévenir les propriétaires. Les Pentester qui étaient des White hats font de leur passion un métier pour en vivre afin qu'il gagne leur vie en tant qu'hacker légal. Un hacker est un bidouilleur, fouineur et passionné qui est spécialiste de la sécurité informatique. Il utilise ses connaissances par envie d'en savoir plus pour diffuser l'information.
Leur rôle dans l'organisation en tant que professionnel de la cybersécurité est de limiter et anticiper les failles d'intrusions malveillantes dans le système informatique de l'entreprise. Il va faire des tests d'intrusion pour vérifier la sécurité informatique de l'entreprise et fournir des solutions pour réduire la vulnérabilité des systèmes.

2. Diplômes, Formations, Écoles

Pour devenir Pentester, après le baccalauréat, il faut suivre une spécialisation dans la Cybersécurité. Il existe plusieurs types de cursus en cybersécurité pour les BAC+2, les BAC+3 et les BAC+5 qui veulent faire de la cybersécurité. Des écoles qui font des formations dans les métiers de la cybersécurité le permettent comme IPPSI, HETIC, Guardia School ou alors des écoles d'ingénieurs comme l'ISEN Lille ou l'IMT Douai, mais aussi des facultés.
Il existe une formation BAC+2 en cybersécurité qui est le BTS SN (Système numérique) Option Informatique et réseaux parcours Cyberdéfense qui à été créée en 2017. Cela à été mis en place pour répondre à la demande croissante de spécialistes de la protection numérique dans l'informatique.
Pour une formation en BAC+3 (en fac ou en école) qui est en liaison avec la cybersécurité on peut faire une licence professionnelle informatique, une licence générale d'informatique parcours cyberdéfense ou un Bachelor en informatique spécialisé "Sécurité informatique".

Pour faire une formation en BAC+5 en cybersécurité on peut faire un Master informatique spécialité cyberdéfense et sécurité de l'information (CDSI) ou spécialité Ingénierie des réseaux de communications mobiles et sécurité, un MBA (maîtrise des affaires de l'administration) management de la sécurité des données numériques, un Mastère spécialisé cybersécurité ou alors un MSc (maîtrise en science) Cybersécurité.

3. Secteur d'activité d'embauche

Le métier de pentester s'exerce directement au sein des entreprises informatique, de l'administration ou des cabinets de conseils spécialisés en Sécurité des Systèmes d'informations dans les grands groupes comme les startups.
Il peut aussi s'exercer dans divers secteurs industriels, de services ou encore dans le secteur public. Il évolue ainsi dans les secteurs suivants tels que les logiciels, informatiques et numérique, bancaire, télécommunication ou encore santé.
Les entreprises qui recrutent des pentesters sont toujours plus nombreuses à rechercher des profils experts en cybersécurité, ils y travaillent pour Airbus, Orange Cyberdéfense ou encore Yes we hack (qui est une plateforme permettant la mise en contact entre des entreprises et des hackers éthiques).
Le pentester à la possibilité de s'exercer en tant que freelance, ce qui représente de la rigueur, de l'organisation, un sens de la communication et une maîtrise du sujet (pour les clients).

4. Salaire d'embauche et salaire moyen

Le salaire d'embauche pour un pentester débutant se situe au moins à 3000€ par mois et peut voir son salaire à plus de 5000€ en tant que pentester confirmé. Dans d'autres pays du monde comme aux Etats-Unis, le salaire annuel moyen d'un pentester est d'environ 110 000 dollars.
Le salaire moyen d'un pentester en France se situe entre 36 000€ par an et 48 000€ par an en fonction de son expérience.
Un pentester qui travaille en freelance à un tarif journalier moyen qui peut varier de 400€ à 1500€, en fonction de ses expériences et références en entreprise.

Le salaire médian pour les emplois pentester (basé sur 187 salaires) en France est de 55 000€ par an, soit 4580€ par mois ou alors 30 € par heure. Sur les 187 salaires, les postes de niveau débutant commencent avec un salaire environnant 42 500€ par an (soit environ 3540€ par mois) tandis que les travailleurs qui sont plus expérimentés gagnent jusqu'à 89 500€ par an (soit 7460€ par mois).

5. Compétences nécessaires, Qualités requises

Les compétences nécessaires pour exercer en tant que pentester demande des compétences nombreuses et étendues.
Il faut avoir la capacité de compréhension des menaces cybersécurité, la capacité à exploiter des sources ouvertes de manière sécurisée, la mise en place de plans de veille sur un ou plusieurs secteurs déterminants. Il y a aussi la détection, qualification et analyse d'informations pertinentes et enfin connaître le droit et les réglementations en vigueur en matière de cybersécurité.
Alexandre: Il s'ajoute aussi à de très nombreuses connaissances pratiques qui ne peuvent s'acquérir que par l'expérience.
Ce métier nécessite des connaissances solides en réseau, de sécurité informatique (c'est-à-dire tout ce qui est de la cryptographie, système de codage, audit de sécurité réseau et web), de développement logiciel et systèmes informatiques (par exemple systèmes embarqués ou industriel).
Des compétences en programmation tel que le Python, C, C++... y compris les langages de programmation web (JavaScript, Php) sont donc indispensables car les tests d'intrusion sont réalisés le plus souvent de manières automatisées grâce à ces langages.
L'expérience de ceci peut être acquise, notamment grâce à des événements comme le "Capture the flag" qui consistent à exploiter les déficiences d'un système pour s'y introduire afin de récupérer un drapeau qui est dont la preuve de réussite de l'intrusion.

Les qualités requises pour un Pentester professionnel de la cybersécurité sont qu'il doit avoir une Éthique et être légal, curieux, cultivé, qui est un expert technique et avec de l'expérience, dynamique, réactif, créatif, disponible, il doit faire preuve de confidentialité, il

doit avoir une bonne maîtrise de l'anglais, il doit aimer le travail en équipe et enfin il doit avoir le goût du défi.
Enfin le pentester doit avoir une bonne qualité humaine

6.Outils technologiques utilisés

Pour exercer sa profession, le pentester à divers outils technologiques à sa disposition, il utilise notamment beaucoup de logiciels comme : Nmap, Open Vas ou encore la distribution Linux Kali.

Il faut savoir que Kali Linux est une distribution Linux intégrant tous les outils nécessaires à la réalisation de tests d'intrusion. Plus de 300 outils de sécurité sont à la disposition du pentester qui peut ainsi vérifier les vulnérabilités d'un système à une offensive. Ces outils sont recommandés et utilise par les pentester au quotidien.

7.Responsabilités, Risques

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.

Concernant les risques le Pentester a la lourde responsabilité de traiter chacun de ses dossiers avec la plus grande vigilance, en effet chaque erreurs ou fautes peut avoir des impacts qui seront cruciaux pour l'organisation dans laquelle il y travaille ou pour ses clients.

8.Avantages et inconvénients

Avantage :

Salaire
Profession qui devient indispensable donc le secteur recrute
Passionnant: C'est un métier dans lequel on relève des challenges et où l'on résout des cases tête, faire du pentest votre métier sera pour vous tout sauf ennuyant !
Néanmoins, il faut savoir que le pentester, contrairement à l'imaginaire collectif qui gravite autour de son métier, n'est pas un geek solitaire et insociable.

Inconvénients :

Charge de travail qui reste très élevé
Pression : 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.

9.Évolution de carrière possible.....

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 l'hacker éthique semblent être étroitement liés de par 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.

10.Vidéo interview

Une histoire de talents - Pentester | Orange Cyberdefense - Bing video

Source :

https://guardia.school/metiers/pentester.html#mission

https://diplomeo.com/formations-cybersecurite

https://www.cidj.com/metiers/pentester#:~:text=Le%20pentester%20exerce%20directement%20au,S%C3%A9curit%C3%A9%20des%20Syst%C3%A8mes%20d'informations.

https://www.hetic.net/debouches-insertions/metiers-web-internet/pentester#:~:text=Pour%20devenir%20pentester%2C%20le%20candidat,ad%C3%A9quation%20pour%20atteindre%20cet%20objectif

https://fr.talent.com/salary?job=pentester

https://www.cyberjobs.fr/metiers-cybersecurite/fiche-metier-pentester