Université Paris-est est Créteil

Faculté des Sciences et Technologies

UPEC
Connaissance - Action

UNIVERSITÉ
PARIS-EST CRÉTEIL
VAL DE MARNE

Pentester

Lawrence AL RAYYAN
L1 Informatique
Groupe n° 2

Vincent Ronach
21 / 04 / 2022

La page de remerciements

- Je remercie le chargé de notre TP projet professionnel M. Ronach Vincent pour toutes les informations pertinentes pour notre rapport mais également enrichissantes dans le cadre de notre avenir professionnel
- Je remercie la chargée de notre TP technique d'expression Mme. Sonnia Marquez pour ses cours de français
- Je remercie mes deux co-équipiers Raphael et Yassine qui m'ont fait découvrir ce métier
- Je remercie le professionnel Scrow-Hacking pour le temps qu'il m'a accordé afin de réaliser l'interview

Sommaire :

Liste des abréviations, sigles et acronymes 4

I. Introduction 5

II. Matériel et méthode 6
A. L'équipe….....6
B. La documentation 6
C. Les entretiens 6

III. Résultats 7
A. Le travail en équipe 7
B. Les informations recueillies 7
1) Le métier en bref 7
2) Etudes et débouchées 7
3) Evolution de carrière ….....8
4) Le secteur …….....8
5) Le salaire ……..9

IV. Conclusion 9

Liste des Annexe.....10
Annexes.....11

Liste des abréviations, sigles et acronymes

- CIDJ = Le Centre d'information et de documentation jeunesse.
- OSCP = Offensive security certified professional.

I. Introduction

Pentester est un mot anglais peu connu en France, il vient de « penetration test » en français « test d'intrusion ».
C'est une personne chargée de tester la sécurité d'un système informatique.

Nous nous sommes orientés vers ce métier chacun pour une raison différente.
D'une part, Raphaël souhaite exercer ce métier à l'avenir. D'autre part, Yassine connaissait déjà l'existence du métier de Pentester et le trouve intéressant malgré le fait qu'il ne souhaite pas se lancer dans ce domaine.

Pour ma part, je ne connaissais pas le métier et le découvrir m'intéresse personnellement. J'ai choisi ce métier car c'est un champ important à connaitre dans tous les domaines de l'informatique. Découvrir cela est important pour mieux sécuriser mon prochain travail et savoir comment je pourrais éviter au maximum de laisser des portes ouvertes en particulier à notre époque où les pirates sont devenus nombreux.

L'analyse de ce métier m'a énormément interrogé au début de ce projet, notamment, sur des questions très simples qui pourraient s'adapter à n'importe quel autre métier.

Qu'est-ce que c'est un pentester ?

Quelle étude faut-il réaliser afin de pouvoir pratiquer ce métier ?

Quelles compétences sont nécessaires ?

Quel type d'entreprise empoche ?

Quel est le salaire moyen pour un junior ?

Mes deux camarades se posèrent des questions un peu plus techniques, vu qu'ils connaissaient déjà ce corps de métier, telles que :

Comment se passe un audit ?

Quelles sont les failles les plus fréquentes ?

II. Matériel et méthode

A. L'équipe :

Nous constituons une équipe hétérogène avec une personne possédant de bonnes connaissances sur le métier de pentester, une autre personne avec une moyenne connaissance et moi sans connaissance. Cette différence de connaissance vis-à-vis de ce métier a été une force pour notre équipe. En effet, cela nous a permis d'aborder ce projet sous différents points de vue et ainsi de mieux le découvrir.

B. La documentation :

Pour trouver des informations concernant le métier de pentester, nous avons majoritairement utilisé internet. Ce type de documentation se justifie par le fait que ce métier est assez récent et peu de livres évoquent ce métier. Nous avons pu avancer nos recherches particulièrement grâce à des sites d'emploi comme Indeed, des sites de centre d'informations comme CIDJ et des sites gouvernementaux comme Pôle emploi.

C. Les entretiens :

Grâce aux interviews, et aux questions que nous avons pu poser aux professionnels, nous avons pu recouper ces informations avec celles trouvées sur des sites internet et ainsi attester ou non de leur véracité. C'est au contact de ces professionnels et des entretiens menés, c'est-à-dire, à la proximité du terrain que nous en avons appris le plus.

Pour la recherche des professionnels, certains ont contacté des entreprises comme Orange ou cherché auprès de leurs connaissances. De mon côté, j'ai effectué mes recherches de contacts via les réseaux sociaux et grâce à cela j'ai pu trouver la personne correspondante aux spécifications que je recherchais.

III- Résultats

- Le travail en équipe

Au début du projet, nous ne savions pas dans quelle direction partir. Beaucoup de questions et d'hésitations sont apparues. Etant donné que ce type de métier est récent et peu développé, nous ne savions pas par où commencer ni par où chercher, les ressources étaient minces. Après réflexion, nous avons débuté le travail en collectif, nous avons partagé nos idées et ensuite les tâches ont été réparties entre l'équipe afin d'approfondir davantage nos recherches, puis nous avons mis en commun notre travail. Grâce à cette organisation, nous avons pu récolter ces interviews.

- Les informations recueillies

1. Le métier en bref

Le pentester est un professionnel de la sécurité informatique.
Son rôle est de contrôler la sécurité des applications (mobiles, back end des sites web qui enregistrent des données confidentielles comme les numéros de cartes bancaires par exemple…) et des réseaux informatiques (réseaux industriels : chaine de montage aéronautique…) en opérant des tests d'intrusion (attaques contrôlées). D'où son nom : **pentester** est la contraction de "**penetration test**".

Une fois les failles de sécurité repérées, il définit le niveau de criticité et de vulnérabilité. Il propose des conclusions et préconise des solutions techniques pour y remédier ou renforcer la sécurité des systèmes informatiques.

2. Etudes et débouchées :

Le métier de pentester nécessite diverses compétences telles que la rigueur, la patience et l'esprit de recherche mais surtout il exige un bon niveau en informatique.

Exemples de formations :

Niveau bac + 3

- Licence professionnelle métier de l'informatique : administration et sécurité des systèmes et des réseaux
  Différents parcours : cybersécurité (Université de Bourgogne)
- BUT Informatique

Niveau bac + 5

- Diplôme d'ingénieur (Isep....)
- Master en informatique avec spécialisation en cybersécurité

Des certifications en sécurité/produits peuvent être parfois exigées.
Parmi les plus courantes : OSCP.
Comme beaucoup de nouveaux métiers, il y a aussi nombreux autodidactes passionnés par l'informatique qui exercent ce métier.

3. Evolution de carrière

Après quelques années d'expériences, le pentester peut évoluer vers un poste de responsable d'intrusion. Il peut également se spécialiser sur un système particulier ou encore créer son cabinet de conseil en sécurité informatique.

Certains pentesters sont en freelance ce qui comporte des avantages mais aussi des inconvénients.
Il en est ressorti de l'interview avec un professionnel en freelance, que cela permet d'effectuer ce métier plus par passion. Il a expliqué que le travail en entreprise tue la passion. Seulement la freelance est plus compliquée sur la sécurité. De plus, le salaire n'est pas fixe et oscille en fonction des missions données ce qui engendre des salaires variant d'un mois à l'autre et une certaine instabilité financière, on ne sait pas combien d'argent on va faire ce mois-ci.

4. Secteurs

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

- Logiciel, informatique et numérique
- Bancaire

- Télécommunication
- Santé

5. Salaire :

Le salaire moyen d'un pentester en France se situe entre 36 000 euros par an et 48 000 euros brut par an en fonction de son expérience, mais comme beaucoup d'autres métiers le salaire varie beaucoup en fonction de la taille de l'entreprise et du lieu de travail.

IV- Conclusion :

Pour conclure, ce rapport a vraiment été une expérience très enrichissante malgré mon manque de connaissance qui a parfois posé problème. L'équipe a toujours été présente pour m'expliquer et me fournir des solutions pour mener à bien les différentes missions qui m'étaient confiées.

Ce projet nous a permis d'être en immersion totale dans le fonctionnement et la réalisation d'un projet et des rôles spécifiques pour chacun. Cela nous a apporté une expérience dans le déroulement d'un projet, le travail en équipe, l'écoute des pairs, la responsabilité et le partage d'idées.

Cela va beaucoup nous aider pour le projet tutoré à venir mais également pour notre avenir lorsque que nous serons en entreprise.

Ce rapport a vraiment confirmé mes ambitions futures de vouloir continuer les études d'informatique.

Liste des annexes :

Annexe 1 : Fiche « Choix de thème », 1 page

Annexe 2 : Fiche État des lieux, 2 pages

Annexe 3 : Fiches Carnet de bord, 1 page

Annexe 4 : Interview, 3 pages

Annexe 5 : Le Mail envoyé au professionnelle, 1 page

Annexe 6 : Compétence, 2 pages

- Savoir-faire
- Savoir être

Annexe 1 : Fiche « Choix de thème »

PROJET PROFESSIONNEL – L1

Formulaire « Choix de thème »

Informations Personnelles

NOM (en majuscules) :
…… ALRAYYAN……..……
Prénom (en Minuscules) :
…… Lawrence ……..……..……..……...
Numéro étudiant :
…… 31901910 ……
Tel Mobile (obligatoire) :
…… 0758491691……..……..
E-mail :
…… Lawrence.al-rayyan@etu.u-pec.fr ……
Groupe de TD:
…….Groupe 2 ……..……..……..……..……..……..……

Projet Professionnel : Indiquez le ou les thèmes choisis (métier, domaine d'activité, centres d'intérêt) Numérotez-les si vous avez un ordre de préférence.

Pentester

Co-équipiers :
……Yassine……..
……Raphael ……..

Annexe 2 :

Fiche État des lieux (à distribuer aux étudiants)

Vous allez réfléchir, en équipe, sur ce que vous savez ou croyez savoir sur le thème que vous avez choisi lors de la séance d'amphi. Formulez par écrit le bilan du « remue-méninges » de votre équipe. Cette feuille vous ***servira*** *en fin de semestre pour rédiger l'introduction et la conclusion votre rapport individuel.*

Thème choisi (recopiez ce que vous avez écrit sur la fiche « Choix de thème » remplie en amphi)

Pentester

Ce que je sais ou crois savoir de ce thème

* Est-ce un métier, une fonction, un secteur d'activité1, une discipline, un centre d'intérêt ?

C'est un métier.

* Cadre dans lequel s'exerce cette activité

Activité salariée, profession libérale, fonction publique

Ça peut être des activités salariées ou bien profession libérale

Autres types d'employeurs, types d'entreprises

Ingénieur en cybersécurité

Réseaux de professionnels

Ce que je sais ou crois savoir sur la nature de cette activité

Niveau de formation, études, diplômes

Bac +5

Compétences (savoir, savoir-faire)

- Parallèlement des compétences en programmation (Python, C/C++…)
- Programmation web (Java, PHP …) sont indispensables

1 *Secteur d'activité (= secteur économique) : exemples : sidérurgie, textile, automobile, assurances, industrie chimique, santé, éducation, action sociale, transports et télécommunications, construction, commerce, etc.*

- Cryptographie, systèmes de codage, audit de sécurité réseau et web

Qualités personnelles (savoir-être)

Son sens de l'éthique doit être irréprochable car ce métier amène à faire des actions normalement illégales, à accéder à des informations sensibles et confidentielles

Niveau de rémunération

50 000€ annuel

Évolution dans la carrière

Ouvrir son propre cabinet.

Annexe 3 :

Fiche Carnet de Bord (à distribuer aux étudiants)

NOM et prénom de l'étudiant AL RAYYAN Lawrence

Parcours Informatique Groupe de TP de projet pro GROUPE 2

NOM et mail de l'intervenant qui encadre votre groupe de projet pro

Vincent Ronach
vincent.ronach@u-pec.fr

Coordonnées des membres de votre équipe			
NOM Prénom	**Adresse postale**	**mail**	**tél. portable**
AL RAYYAN Lawrence	11 rue delaunoy	Lawrence.al-rayyan@etu.u-pec.fr	0758491691
FEKIH HASSEN Yassine	7 Rue du Docteur laennec	Yassine.fekih-hassen@etu.u-pec.fr	0782998532
BATICLE Raphael	8 rue de la Garenne Varennes Jarcy	Raphael.baticle@etu.u-pec.fr	0768114860

RENCONTRES DE L'ÉQUIPE

Pour chaque rencontre, indiquer quel membre de l'équipe a pris l'initiative de la rencontre, la date de la rencontre, le lieu et la forme (rencontre directe, internet, sms, Teams …), l'ordre du jour, quels membres de l'équipe étaient présents, quels étaient les absents excusés (et le motif de leur absence).

Entre le TP1 et le TP2

Choisir un thème

Entre le TP2 et le TP3

Chercher des professionnels .

Entre le TP3 et le TP4

Mise en commun de nos recherches

Entre le TP4 et le TP

Préparation de notre oral pour la soutenance

Pour la préparation de la soutenance

Annexe 4 :

L'Interview :

Site du professionnel : (Hacking for noobs (hacking-for-noobs.com))

1. En quoi consiste le métier de pentester ?

Le job de pentester consiste à chercher des vulnérabilités sur des sites web/applications/réseaux pour des entreprises clientes.

Il s'agit de sécurité offensive, on se met à la place d'un "attaquant" pour tenter de compromettre le serveur cible, d'usurper la session d'un utilisateur,

d'un admin, d'uploader des fichiers malveillants, de contourner les protections, etc...

L'objectif est ensuite de remettre un rapport (et de faire une restitution) sur toutes les vulnérabilités détectées afin qu'ils puissent corriger en interne avec ses équipes (dev), et ainsi se prémunir de "vraies" cyberattaques.

2. Quelles études avez-vous fait ?

J'ai fait une classe prépa scientifique, puis une école d'ingé en électronique et enfin un mastère spécialisé en sécurité des systèmes d'information dans une seconde école d'ingénieur.

Mais le parcours "classique" est bien souvent une école d'informatique avec une spécialisation en cybersécurité.

3. Quelle est votre journée type ?

Cela dépend des missions, il n'y a pas réellement de journée type. Mais comme à présent j'ai quelques années d'expérience, dans mes journées bien souvent j'alterne entre chefferie de projets (pilotage de mission, réunions et management d'équipe) et du delivery (donc de l'audit technique, pentest).

4.Quelle est la différence entre le faire en freelance ou en entreprise ?

En tant que freelance il y a également à gérer toute la partie commerciale, trouver des clients, se faire connaître, etc.

Pour ma part je trouve que travailler dans une entreprise est plus "stable", notamment en termes de salaire, de vacances, cotisation retraite et mutuelle et moins chronophage également.

5. Quelles difficultés avez-vous rencontrées quand vous avez débuté ?

Je dirais l'adaptation au métier, les missions sont quand différentes de ce que l'on peut trouver en "ctf" (capture the flag).

Il y a également les autres phases de la mission que je découvrais : qualification avec le client (besoin, cdg, prérequis), la rédaction du rapport et la restitution finale.

6. Quel est le salaire mensuel approximativement ?

Dans la région parisienne un pentester peut espérer un salaire de 38-40K annuel à ses débuts, cela peut augmenter par la suite en fonction de son expérience et de ses responsabilités.

7. Quels sont les avantages et les inconvénients du métier ?

Avantages : le fait de toujours apprendre, il n'y a pas de monotonie dans ce métier.

La stimulation intellectuelle, l'émulation avec les collègues et l'aspect "challenge" des missions. Le télétravail et les horaires qui sont assez libres.

Inconvénients : Certaines missions sont beaucoup moins intéressantes que d'autres, notamment lorsqu'il s'agit d'environnement sécurisé et que nous ne trouvons pas grand-chose...

8. Comment se passe un audit ?

Il y a plusieurs phases : proposition commerciale, qualification des besoins, kickoff (présentation aux clients de la méthodologie, et des prérequis nécessaires : compte d'accès, ...), audit technique, rédaction du livrable, restitution

9. Quelles sont les failles les plus fréquentes ?

C'est que l'on appelle le TOP 10 OWASP (mauvais contrôle d'accès, injections, XSS, mauvaises configurations, ...)

10. Quelle est votre pire peur / expérience dans ce métier ?

Les missions vont grandement dépendre du relationnel avec les clients, donc en fonction des attentes et du caractère cela peut assez mal se passer.

Annexe 5 :

Mail envoyé au professionnel .

Demande d'interview

AL **Al Rayyan Lawrence <lawrence.al-rayyan@etu.u-pec.fr>**
13/03/2022 21:01

À : scrowhacking@gmail.com

Bonjour,

Je me présente, je m'appelle Lawrence AL RAYYAN et je suis étudiant à l'université de Paris-est Créteil en Informatique en première année.
J'ai vu votre compte sur Instagram et j'ai vu que vous étiez pentester, cela m'intéresse. J'ai aussi parcouru votre site qui est très enrichissant.
Je vous explique la raison pour laquelle je vous écris ce mail.
Nous avons un cours de projet professionnel et nous devons choisir un métier sur lequel un rapport professionnel doit être réalisé. Le vôtre m'attire tout particulièrement.

Je me permets de vous demander qu'on puisse faire un interview ensemble que cela soit en présentiel si vous êtes sur Paris ou bien soit en distanciel.

Les questions seront les suivantes :

1. En quoi consiste le métier de pentester ?
2. Quelles études avez-vous fait ?
3. Quelle est votre journée type ?
4. Quelle est la différence entre le faire en freelance ou en entreprise ?
5. Quelles difficultés avez-vous rencontrées quand vous avez débuté ?
6. Quel est le salaire mensuel approximativement ?
7. Quels sont les avantages et les inconvénients du métier ?
8. Comment se passe un audit ?
9. Quelles sont les failles les plus fréquentes ?
10. Quelle est votre pire peur / expérience dans ce métier ?

Je tiens compte que vous aviez déjà répondu à presque toutes ces questions sur votre site et sur votre réseau social cependant cela est important que vous répondez aux questions de nouveau et laisser votre signature afin de pouvoir avoir une trace de vous dans mon rapport.
Je vous remercie pour le temps que vous pourriez m'accorder.
Cordialement
Al Rayyan Lawrence
07 58 49 16 91

Annexe 6 :

Compétence

Tout d'abord, il faut savoir que le savoir-être fait partie des compétences professionnelles avec le savoir et le savoir-faire. Ces trois notions se complètent et sont interdépendantes. Le savoir correspond à ce que nous savons, nos connaissances théoriques. Le savoir-faire correspond à ce que nous savons faire, à nos compétences. Le savoir-être correspond à des qualités personnelles et professionnelles qui représentent la façon dont vous vous comportez dans un milieu professionnel avec autrui ou non.

- **Savoir-faire**

C'est les connaissances techniques de la personne

Le métier de pentester nécessite des connaissances solides :

- En réseau, Sécurité informatique (cryptographie, systèmes de codage, audit de sécurité réseau et web)
- Développement logiciel et systèmes informatique (systèmes embarqués, systèmes industriels …)
- Parallèlement des compétences en programmation (Python, C/C++…)
- Programmation web (Java, PHP …) sont indispensables

https://www.cidj.com/metiers/pentester#:~:text=Description%20m%C3%A9tier&text=D'o%C3%B9%20son%20nom%20%3A%20pentester,la%20s%C3%A9curit%C3%A9%20des%20syst%C3%A8mes%20informatiques.

- **Savoir-être :**

Le **savoir-être** correspond aux qualités personnelles et comportementales d'un individu au sein d'un domaine professionnel. Autrement dit, à la capacité d'agir par rapport à un environnement de travail (entreprise, clients, collaborateurs, freelance). Ce sont des compétences qui ne s'acquiert pas grâce à l'école ou à une formation, mais que l'on va utiliser chaque jour.

- Le pentester doit savoir s'exprimer aussi bien à l'écrit qu'à l'oral (y compris en anglais)

- Être fin pédagogue et psychologue lorsqu'il est face aux concepteurs d'un système dont il a trouvé des failles.
- Son sens de l'éthique doit être irréprochable car ce métier amène à faire des actions normalement illégales, à accéder à des informations sensibles et confidentielles.