Ryan Agin

Présentation Personnelle

Je m'appelle Ryan Agin, et je suis actuellement en première année de BUT Informatique à l'Université Paris 13, au sein de l'IUT de Villetaneuse. Depuis l'âge de 13 ans, lorsque j'ai eu mon premier PC, j'ai développé une passion pour l'informatique et ainsi avoir une vision différente des autres par rapport à l'informatique , ce qui m'a naturellement conduit à ce domaine.

Passionné par le hacking et la cybersécurité, je me destine à une carrière dans le pentesting. Mes études m'ont permis d'acquérir des compétences solides en programmation, en gestion de bases de données, et en réseaux informatiques. En parallèle, je m'intéresse particulièrement à l'éthique du hacking et aux techniques de pénétration sécurisée, domaines dans lesquels je me forme activement.

Pour atteindre cet objectif, je me suis particulièrement intéressé au domaine des réseaux. J'ai déjà réalisé plusieurs projets orientés vers les réseaux et la collecte de données. De plus, je prévois d'installer "Kali Linux", une célèbre distribution de Linux spécialisée dans le pentesting, avec des outils de hacking directement intégrés. Cela me permettra de me familiariser rapidement avec l'environnement du hacking.

Mon objectif professionnel est de devenir un expert en cybersécurité, capable de protéger les systèmes d'information contre les menaces et les vulnérabilités. Je suis motivé par les défis et toujours à la recherche de nouvelles opportunités pour approfondir mes connaissances et contribuer à des projets innovants dans ce domaine crucial.

Gestion de bases de données : Compétence solide en conception, manipulation, et optimisation de bases de données relationnelles, acquise à travers divers projets académiques où j'ai géré des bases de données complexes.

Réseaux informatiques : Connaissance approfondie des protocoles réseau et de la configuration des équipements réseau. J'ai, par exemple, mis en place un réseau local sécurisé pour un projet de collecte de données ou même l’utilisation d’analyse trame pour récolter des informations .

Cybersécurité et Pentesting : Passionné par le hacking éthique, je me forme activement aux techniques de pénétration sécurisée. J'ai réalisé des audits de

sécurité pour des projets académiques, utilisant des outils de Kali Linux pour identifier et corriger les vulnérabilités.

Écoute et respect : Je suis une personne très à l'écoute et respectueuse, ce qui me permet de créer un environnement de travail chaleureux et collaboratif avec mes collègues.

Altruisme : Mon sens de l'altruisme me permet d'aider les autres sans hésitation. Je suis toujours prêt à offrir mon soutien, ce qui renforce la cohésion et l'efficacité au sein de l'équipe.

Esprit d'équipe : J'ai travaillé sur plusieurs projets en groupe, où la collaboration et la communication étaient essentielles pour atteindre nos objectifs communs.

Résolution de problèmes : Mon approche analytique et méthodique me permet de résoudre efficacement des problèmes complexes, comme lors de la mise en place de mesures de sécurité pour des systèmes informatiques.

Autonomie et initiative : Je suis proactif dans l'apprentissage de nouvelles compétences et technologies. Par exemple, j'ai pris l'initiative d'apprendre et d'installer Kali Linux pour me familiariser avec les outils de pentesting.

j’ai aussi un rapport d’un test de personnalité fait , que je peux envoyer pour avoir un aperçu de ma personnalité .

Pourquoi l'informatique

L'informatique représente bien plus qu'une simple compétence technique dans le monde actuel . C'est devenu une clé essentielle pour comprendre et influencer notre société interconnectée. Ma décision de me spécialiser dans ce domaine découle de plusieurs facteurs.

Raisons factuelles : L'informatique est omniprésente et essentielle dans notre quotidien moderne. Des applications mobiles aux services bancaires en ligne, notre dépendance à la technologie ne cesse de croître. Maîtriser les bases de données, la programmation et la sécurité informatique est non seulement pertinent mais indispensable pour répondre aux besoins croissants de sécurité et de fiabilité.

Vision personnelle : Mon intérêt pour l'informatique est profondément ancré dans ma volonté d'appréhender les défis contemporains avec rigueur et innovation. En explorant les nuances de la cybersécurité, j'ai réalisé que chaque ligne de code peut renforcer la protection de nos informations sensibles. Cette responsabilité et cette opportunité de contribuer à un monde plus sûr sont des motivations clés dans mon parcours professionnel.

Expérience pratique : Mes expériences concrètes, telles que la gestion de réseaux locaux sécurisés et la participation à des projets de développement logiciel, m'ont permis de voir l'impact direct et tangible de l'informatique dans divers domaines. Ces réalisations renforcent ma conviction que l'informatique est le terrain où mes compétences et mes aspirations convergent.

En conclusion, choisir l'informatique comme voie professionnelle est pour moi bien plus qu'une simple inclination technique. C'est une passion pour la sécurité, l'innovation et l'impact sociétal positif, motivée par une compréhension approfondie des enjeux du monde actuel et des opportunités offertes par ce domaine en constante évolution.

le métier de pentester en cybersécurité

Définition et Principes

Le métier de pentester, ou testeur d'intrusion, est au cœur de la cybersécurité moderne. Son rôle principal est de détecter et d'exploiter les vulnérabilités potentielles dans les systèmes informatiques, réseaux ou applications, afin d'évaluer leur sécurité. Contrairement aux cybercriminels, les pentesters agissent de manière éthique et légale pour identifier les failles avant qu'elles ne soient exploitées par des tiers malveillants. Leur travail consiste à simuler des attaques réelles pour aider les organisations à renforcer leur posture de sécurité.

Cadre et Applications

Les pentesters travaillent souvent au sein d'équipes de sécurité informatique au sein d'entreprises, d'organisations gouvernementales, ou en tant que consultants indépendants. Leur champ d'action peut inclure des tests sur des réseaux locaux, des applications web, des infrastructures cloud, et même des objets connectés (IoT). Ils utilisent une variété d'outils spécialisés et de techniques avancées pour mener à bien leurs missions et produire des rapports détaillés sur les vulnérabilités découvertes.

Comment exercer ce métier

Formation et Compétences Requises : Pour devenir pentester, il est essentiel de posséder une solide formation en informatique, souvent à travers un diplôme universitaire en sécurité informatique, en informatique, ou en génie logiciel. Des certifications spécifiques telles que Certified Ethical Hacker (CEH), Offensive Security Certified Professional (OSCP), ou GIAC Certified Penetration Tester (GPEN) sont également très valorisées dans le secteur.

Les compétences requises incluent une expertise en programmation, une bonne compréhension des réseaux informatiques, des connaissances approfondies en systèmes d'exploitation, et une capacité à penser de manière créative pour contourner les défenses de sécurité. La maîtrise des outils de hacking éthique comme Kali Linux est souvent indispensable.

Intérêt Personnel

Le métier de pentester m'intéresse particulièrement en raison de sa nature dynamique et de son impact direct sur la sécurité des systèmes informatiques. Lors de mon entretien mené au premier semestre, j'ai découvert que ce métier allie

parfaitement ma passion pour la technologie avec un fort engagement éthique. Voici un extrait pertinent de cet entretien :

"J'ai toujours été fasciné par les défis que représente la cybersécurité. En tant que pentester, je pourrais utiliser mes compétences techniques pour trouver des failles et aider les entreprises à se protéger contre les cyberattaques. C'est gratifiant de savoir que mon travail contribuerait directement à renforcer la sécurité des données et des infrastructures essentielles en plus de ça faire un métier de hacker qui de base est illégal et le transformer en légale et en plus de ça être payer ."

Focus sur une technologie

Veille Professionnelle sur la Cybersécurité et le Métier de Pentester

Sources de Veille Utilisées

Ma veille professionnelle s'appuie sur plusieurs sources fiables et variées pour rester informé des dernières avancées en cybersécurité :

1. **Livres et Témoignages :**
    - **"Lève-toi et code : Confessions d'un hacker"** par Rabbin des Bois : Ce livre autobiographique explore les motivations, les défis et les dilemmes éthiques d'un hacker repenti. Il met en lumière des exploits techniques et les implications de la sécurité informatique de manière personnelle et philosophique.
    - **"Princesse Data"** : Dans ce livre, Rabbin des Bois discute des manipulations de données en ligne et des dangers de la surveillance numérique, illustrant comment les informations personnelles peuvent être utilisées à des fins de contrôle et de manipulation.
2. **Médias et Actualités :**
    - Interviews et vidéos sur YouTube, notamment des interventions de Rabbin des Bois sur des chaînes comme Le Grand JD et Konbini, où il discute des enjeux éthiques de la cybersécurité et des défis rencontrés dans le domaine du hacking.

Résumé des Livres et Témoignages

- **"Lève-toi et code"** offre un regard intime sur les motivations et les méthodes de Rabbin des Bois en tant que hacker, explorant les implications éthiques du hacking et les défis personnels rencontrés.

- **"Princesse Data"** met l'accent sur les dangers de la manipulation des données et de la vie privée en ligne, soulignant l'importance d'une vigilance accrue face à l'usage des informations personnelles sur internet.

Application Personnelle et Intérêt en tant que Futur Spécialiste

Ces ressources m'ont profondément intéressé en tant que futur spécialiste de la cybersécurité, particulièrement dans le rôle de pentester. Voici pourquoi :

- **Impact Éthique :** Les témoignages de Rabbin des Bois illustrent l'importance de l'éthique dans la cybersécurité. En tant que pentester, il est crucial d'adopter une approche responsable et éthique pour identifier et corriger les vulnérabilités des systèmes.
- **Prise de Conscience :** Les récits personnels et les exemples concrets m'ont sensibilisé aux dangers potentiels pour la vie privée et à l'importance de sécuriser les données personnelles dans un environnement numérique de plus en plus interconnecté.

Analyse Critique de la Veille Professionnelle

Ma veille professionnelle est structurée autour d'une diversité de sources et d'une routine régulière de consultation. Cela me permet de rester informé des nouvelles techniques d'attaques et des pratiques émergentes en cybersécurité. En analysant ces informations, je suis capable d'adapter mes compétences et de contribuer efficacement à la sécurité des systèmes d'information.

En conclusion, ma veille professionnelle sur la cybersécurité et le métier de pentester m'aide à approfondir mes connaissances et à développer une conscience critique des enjeux éthiques dans ce domaine crucial. Cela renforce ma motivation à devenir un professionnel compétent et éthique, prêt à relever les défis complexes de la sécurité informatique dans un monde numérique en constante évolution.

Bilan des compétence a partir de SAE

Liste de mes expériences (saé)

S1.03 - installation d’un poste pour le développement

Compétence

Les principaux compétence concernant par cette SAE sont principalement :

- Administrer

Apprentissage critique visées

- AC13.01 | Identifier les différents composants (matériels et logiciels) d’un système numérique-
- AC13.02 | Utiliser les fonctionnalités de base d’un système multitâches / multiutilisateurs
- AC13.03 | Installer et configurer un système d’exploitation et des outils de développement

degré de maîtrise

AC13.01 : Bien maitriser je pense que je maîtrise bien cette partie principalement de matériel , de différent compétence d'un système numérique

AC13.02 : Moyennement maitriser pour moi cette partie là , je la maîtrise bien mais sans plus , principalement dans le terminal que je trouve bien maîtriser , mais il a differents thème que je dois mieux maîtriser

AC13.03 : Bien maitriser cette partie me rappelle la SAE , que j'ai bien aimé et que j'ai trouvé cela assez simple meme si il y a quelque point que je dois améliorer

Preuve de mes compétence

AC13.01 : je pense que je maitrise bien cette partie principalement de matériel , de différent compétence d'un système numérique , il y a aussi le fait que j'ai deja monter un PC moi même car je suis propriétaire d'un PC fixe , j'ai aussi déterminer les différents composant à acheter pour que mon PC soit le plus optimisé

AC13.02 : pour moi cette partie là , je la maîtrise mais sans plus , principalement dans le terminal que je trouve bien maîtriser , mais il a differents thème que je dois mieux maîtrisé

AC13.03 : cette partie me rappelle la SAE , que j'ai bien aimé et que j'ai trouvé cela assez simple meme si il y a quelque point que je dois améliorer

Plan d'action pour développer mes compétences

AC13.01 : Pour m'améliorer et développer mes compétences je peux m'informer de comment les composants sont mis avec des vidéos internet , comment optimiser ces composants etc…

AC13.02 : Pour cette compétence la , je peux aller voir des vidéos aller sur des site internet qui pourrait m’aider à maîtriser davantage cette compétence ou aller dans le site de l'enseignant qui a different chapitre je peux les relire pour mieux les maîtriser

AC13.03 : pour cette partie là , je pourrais refaire la SAE par exemple qui m’a beaucoup plu , pour pouvoir voir les questions ou je me suis loupé et comprendre pourquoi je n’ai pas pu répondre a ces question

Liste de mes expériences (saé)

S2.03 - Installation de services réseau

Compétence

Les principaux compétence concernant par cette SAE sont principalement :

- Administrer

Apprentissage critique visées

- AC13.01 | Identifier les différents composants (matériels et logiciels) d’un système numérique
- AC13.02 | Utiliser les fonctionnalités de base d’un système multitâches / multiutilisateurs
- AC13.03 | Installer et configurer un système d’exploitation et des outils de développement
- AC13.04 | Configurer un poste de travail dans un réseau d’entreprise

degré de maîtrise

AC13.01 : Bien maîtrisé

- Je pense que je maîtrise bien cette compétence, notamment en ce qui concerne le matériel et les différents composants d'un système numérique.

AC13.02 : Moyennement maîtrisé

- J'ai une bonne maîtrise de cette compétence, surtout en ce qui concerne l'utilisation du terminal. Cependant, il y a plusieurs aspects que je dois encore approfondir.

AC13.03 : Bien maîtrisé

- Cette compétence me rappelle la SAE que j'ai appréciée et trouvée relativement simple, même s'il y a quelques points que je dois encore améliorer.

AC13.04 : Bien maîtrisé

- je pense bien maîtrisé cette compétence je suis ouvert d'esprit , je sais ce que je veux faire comme métier professionnel et ce que je dois faire pour y arriver

Preuve de mes compétence

AC13.01 : je pense que je maitrise bien cette partie principalement de matériel , de différent compétence d'un système numérique , il y a aussi le fait que j'ai deja monter un PC moi même car je suis propriétaire d'un PC fixe , j'ai aussi déterminer les différents composant à acheter pour que mon PC soit le plus optimisé

AC13.02 : pour moi cette partie là , je la maîtrise mais sans plus , principalement dans le terminal que je trouve bien maîtriser , mais il a differents thème que je dois mieux maîtrisé

AC13.03 : cette partie me rappelle la SAE , que j'ai bien aimé et que j'ai trouvé cela assez simple meme si il y a quelque point que je dois améliorer

AC13.04 : je trouve avoir une bonne communication avec les autres , droit dans ce que je veux faire c'est à dire que je sais que faire pour y arriver

Plan d'action pour développer mes compétences

AC13.01 : Pour m'améliorer et développer mes compétences je peux m'informer de comment les composants sont mis avec des vidéos internet , comment optimiser ces composants etc… . M'intéresser au nouveau technologie crée , leur architecture etc…

AC13.02 : Pour cette compétence la , je peux aller voir des vidéos aller sur des site internet qui pourrait m'aider à maîtriser davantage cette compétence ou aller dans le site de l'enseignant qui a different chapitre je peux les relire pour mieux les maîtriser

AC13.03 : pour cette partie là , je pourrais refaire la SAE par exemple qui m'a beaucoup plu , pour pouvoir voir les questions ou je me suis loupé et comprendre pourquoi je n'ai pas pu répondre a ces question et aussi refaire un autre projet de ce type avec d'autre aspects a voir

AC13.04 : pour développer cette compétence je compte m'informer sur les nouveautés de mon projet professionnel , m'ouvrir au autre pour etre de plus en plus a l'aise

Objectifs/Actualisation du Projet Professionnel

Objectifs à Long Terme

Dans 10 à 15 ans, je me vois en tant qu'expert reconnu en cybersécurité, spécialisé dans le pentesting et la protection des systèmes d'information contre les menaces cybernétiques. Mon objectif est de devenir un leader dans le domaine, capable de diriger des équipes de sécurité et de développer des stratégies innovantes pour défendre les infrastructures critiques contre les cyberattaques. En tant que consultant en sécurité, je souhaite également partager mes connaissances et mon expertise à travers des conférences, des ateliers de formation et la publication de travaux de recherche.

Objectifs à Moyen Terme

À moyen terme, après l'obtention de mon BUT Informatique, je prévois de poursuivre mes études en intégrant un programme de Master en cybersécurité. Ce cursus me permettra d'approfondir mes compétences techniques et de me spécialiser davantage dans le pentesting. Parallèlement, je compte obtenir des certifications reconnues dans le domaine, telles que le Certified Ethical Hacker (CEH) et le Offensive Security Certified Professional (OSCP), afin de renforcer mon profil professionnel et d'accroître ma crédibilité auprès des employeurs potentiels.

Mon objectif est d'obtenir mon premier emploi en tant qu'analyste en sécurité ou pentester junior dans une entreprise spécialisée en cybersécurité ou au sein du département informatique d'une grande entreprise. Cette expérience me permettra de mettre en pratique mes compétences et de continuer à apprendre en travaillant sur des projets réels.

Objectifs à Court Terme

Pour réaliser ces objectifs, je vais adopter les stratégies suivantes dès maintenant :

1. **Formation Continue :**
    - Poursuivre activement mes études en BUT Informatique, en mettant l'accent sur les cours et projets liés à la cybersécurité.
    - Participer à des cours en ligne et des ateliers pour acquérir des compétences spécifiques en hacking éthique et en pentesting.
    - Lire des ouvrages et des articles spécialisés, et suivre des blogs et des podcasts de référence dans le domaine de la cybersécurité.
2. **Certifications Professionnelles :**
    - Commencer à préparer les examens de certifications en cybersécurité, notamment CEH et OSCP, en utilisant des ressources en ligne et en suivant des formations spécialisées.
    - M'inscrire à des plateformes de formation telles que Cybrary, Udemy, et Offensive Security pour accéder à des cours et des exercices pratiques.
3. **Expérience Pratique :**

    - Participer à des compétitions de hacking et à des CTF (Capture The Flag) pour mettre en pratique mes compétences en pentesting dans un environnement contrôlé et compétitif.
    - Rechercher des stages ou des projets freelance en cybersécurité pour acquérir une expérience professionnelle concrète et enrichir mon CV.
4. **Réseautage et Engagement Communautaire :**
    - Rejoindre des communautés et des associations professionnelles en cybersécurité, telles que l'OWASP (Open Web Application Security Project) et l'ISSA (Information Systems Security Association).
    - Assister à des conférences et des événements de cybersécurité pour rencontrer des professionnels du secteur et élargir mon réseau.
5. **Veille Technologique :**
    - Maintenir une veille technologique rigoureuse en suivant des sources fiables et en restant informé des dernières tendances et des nouvelles menaces en cybersécurité.
    - Partager mes découvertes et mes analyses sur des forums et des blogs spécialisés pour contribuer à la communauté et démontrer mon expertise.

En mettant en œuvre ces stratégies, je suis convaincu que je pourrai progresser efficacement vers mes objectifs à long terme et devenir un expert en cybersécurité compétent et respecté.