Offres de stages 2020

12 SUJETS DE STAGE À CHOISIR
(PRÉ-EMBAUCHE EN CDI)

Envoyez vos CV à : apply@synacktiv.com

Table des matières

1. SYNACKTIV

1.1. Prêt pour l'aventure ?

Rejoindre **Synacktiv**, c'est faire partie d'une équipe de passionnés où l'exigence et l'expertise sont de rigueur. Le tout saupoudré d'une bonne dose de fun ! Voici quelques-unes de nos valeurs qui ont fait grandir et vibrer Synacktiv depuis ses débuts :

- **Expertise :** nous recrutons et permettons aux meilleurs experts techniques de continuer à développer leur savoir-faire en sécurité informatique. Nous sommes capables de répondre aux besoins des clients les plus exigeants.
- **Innovation :** nous améliorons constamment nos méthodologies et nos outils pour être plus pertinents et plus efficaces dans notre approche. Nous trouvons des solutions innovantes aux problèmes uniques de nos clients.
- **Pertinence :** nous travaillons à répondre précisément aux demandes de nos clients et à mettre l'accent sur les points qu'ils jugent importants. Nos méthodologies s'adaptent aux besoins spécifiques de chaque client.
- **Transparence :** nous sommes transparents sur nos compétences et nos propres limites. Nous n'hésitons pas à orienter nos clients vers un autre prestataire si nous ne sommes pas les plus à même de traiter une demande.

Pour en savoir plus, rendez-vous sur : https://www.synacktiv.com/blog.htmlblog.html

1.2. Pour la petite histoire

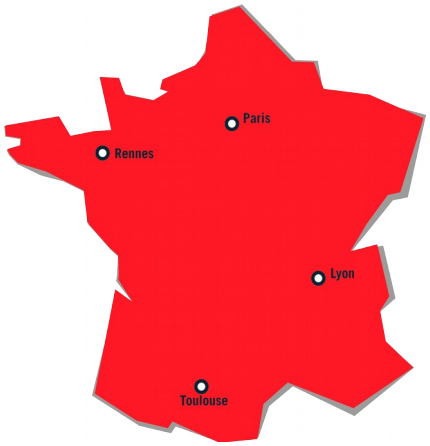
Fondée en 2012 par deux consultants passionnés par la sécurité des systèmes d'information, Synacktiv a su attirer et rassembler les meilleurs experts francophones dans ce domaine. **La société compte plus de 50 experts de la sécurité offensive** à même d'épauler ses clients sur des projets de **test d'intrusion**, d'**audit de sécurité** et de **rétro-ingénierie** dans des environnements techniques de plus en plus complexes.

Une partie de ces **travaux de R&D est également partagée avec la communauté sécurité**. Une liste des publications et d'outils développés par Synacktiv est disponible sur le site web de la société à l'adresse suivante : *https://www.synacktiv.com/fr/ressources.html*. Celle-ci est régulièrement mise à jour avec les dernières vulnérabilités découvertes par l'équipe Synacktiv et le développement de nouveaux outils.

1.3. Implantation géographique

Notre implantation dans plusieurs villes de France permet aux meilleurs profils de travailler avec Synacktiv, quel que soit le lieu !

Nos stages sont majoritairement à pourvoir à Paris. Mais nous développons des dispositifs innovants afin de promouvoir la mobilité professionnelle.



2. Ils ont choisi Synacktiv !

2.1. Lena David – ninja chez Synacktiv

Experte sécurité chez Synacktiv, diplômée de l'ENSEEIHT, recrutée en tant que stagiaire au pôle dev en 2018.

- **Pourquoi choisir un stage chez Synacktiv ?**

« J'ai fait ma dernière année d'études dans une formation spécialisée en sécurité, d'où ma recherche d'un stage dans le domaine. Parmi les offres portant sur l'amélioration d'outils internes, deux m'ont particulièrement intéressée. Les échos positifs sur Synacktiv que j'avais eus par d'anciens étudiants qui travaillent dans la sécurité ont aussi contribué à ma décision de postuler à ces offres. Je ne regrette pas du tout ce choix : faire un stage chez Synacktiv, c'est s'entourer d'une équipe d'un très bon niveau technique, et travailler dans un environnement agréable où l'entraide et le partage de connaissances sont encouragés, ce qui aide beaucoup à progresser. »

- **Quel a été ton parcours ?**

« J'ai fait une prépa (MPSI/MP), puis je suis entrée à l'ENSEEIHT à Toulouse, dans le département Informatique/Maths appliquées. En dernière année, au lieu de suivre la fin de cursus classique, j'ai opté pour une formation spécialisée en sécurité accessible aux étudiants de plusieurs écoles d'ingénieurs de Toulouse, TLS-SEC. J'ai rejoint Synacktiv lors de mon stage de fin d'études et y suis restée par la suite.»

- **Quel a été ton sujet de stage ?**

« J'ai travaillé sur deux de nos outils internes, utilisés au quotidien dans le cadre de tests d'intrusion : Kraqozorus, notre plateforme de cassage de mots de passe - et Oursin, notre plateforme de spear-phishing. Dans les deux cas, le but était d'améliorer des features existantes et d'en développer de nouvelles en fonction notamment de besoins identifiés ou de difficultés rencontrées pendant des missions. »

2.2. Corentin Bayet – ninja chez Synacktiv

Expert sécurité chez Synacktiv, école 42, recruté en tant que stagiaire dans le pôle reverse en 2017.

- **Pourquoi choisir un stage chez Synacktiv ?**

« J'avais déjà entendu parler de Synacktiv lors de mon précédent stage et lors de conférences. La procédure de recrutement a confirmé positivement tout ce que j'avais pu entendre. Le stage proposé avait l'air intéressant et a été conforme à mes attentes. La gratification me convenait aussi, car Synacktiv s'est basé davantage sur mes compétences que mon niveau d'étude. »

- **Quel a été ton parcours ?**

« Après avoir obtenu mon bac S en 2014, je suis rentré directement à l'école 42. Je suis monté en compétences tout seul avec des plateformes en ligne comme root-me. Par ailleurs, j'ai fait des rencontres dans la communauté cyber-sécurité et à faire des CTF. J'ai ensuite fait un premier stage dans une entreprise qui a découlé sur une conférence à la Nuit du Hack en 2017, avant d'intégrer Synacktiv. »

- **Quel a été ton sujet de stage ?**

« J'ai travaillé à améliorer et démocratiser le framework de fuzzing interne de l'entreprise. J'ai pu intervenir sur beaucoup de sujets, de technologies différentes, et surtout approfondir énormément de connaissances. Je suis, aujourd'hui, le référent de ce projet et une partie de mon temps de travail y est alloué. »

3. Stage pôle test d'intrusion – Red Team arsenal

3.1. The king of escape

Description du poste

Synacktiv recherche un stagiaire (H/F) en sécurité informatique capable de participer à l'extension de l'arsenal **Red Team** de Synacktiv. Vous intégrerez notamment l'équipe en charge du projet **Houdini** (https://synacktiv.com/ressources/synacktiv_houdini_plaquette.pdf). L'objectif de ce projet est de réduire à son maximum le temps de présence sur site des équipes lors d'une **intrusion physique**, en proposant un implant physique capable d'automatiser toutes les actions nécessaires pour joindre un ***Command and Control*** (C&C) distant. Cela implique une **automatisation** complète du processus de **reconnaissance** au sein d'un réseau d'entreprise inconnu afin de trouver un chemin permettant d'atteindre le C&C. Les enjeux de ce projet sont d'une importance capitale, car il doit garantir le **maintien des accès** de l'équipe après une intrusion physique réussie. Les maîtres mots de ce projet sont : efficacité, polyvalence et fiabilité.

En intégrant le projet Houdini au sein du pôle pentest de Synacktiv, votre rôle sera de :

- prendre en main l'existant ;
- recueillir les besoins opérationnels de l'équipe (nouvelles fonctionnalités, furtivité, etc.) ;
- prioriser les fonctionnalités attendues et les implémenter ;
- les tester avec un haut niveau d'exigence au sein d'environnements représentatifs afin d'identifier l'ensemble des *corner cases* et ainsi accroître l'efficacité et la fiabilité du projet sur le long terme ;
- apporter le support nécessaire aux équipes sur place lors des intrusions physiques.

Dans un second temps, vous pourrez être amenés à participer à l'**extension de l'arsenal** par l'intégration de nouveaux implants, la **formation de l'équipe** à leur utilisation et au support de l'équipe opérationnelle.

Vous serez également amenés tout au long du stage à intervenir sur des missions de type ***Red Team*** afin de mieux comprendre le métier et ainsi proposer un projet au plus proche du besoin.

Il est attendu que le stage débouche sur un CDI d'expert sécurité chez Synacktiv.

Profil & compétences

- Forte volonté d'apprendre, de se perfectionner et d'innover sur les techniques d'évasion réseau et de furtivité.
- Programmation **Python**. Notre suite d'outils internes est principalement programmée dans ce langage, vous devez avoir une expérience minimale en Python pour contribuer à son développement.
- Bonnes connaissances en réseau. Les problématiques traitées par le projet Houdini sont étroitement liées au réseau (filaire, Wi-Fi, mobile, Bluetooth, etc.).
- Anglais et français indispensables.
- Stage basé à Paris dans le 2ème arrondissement (Grands Boulevards).
- Rémunération 1500€ brut / mois.

À VOS CV !apply@synacktiv.com

3.2. Invisible man

Description du poste

Synacktiv recherche un stagiaire (F/H) en sécurité informatique capable de participer à l'extension de l'arsenal **Red Team** de Synacktiv. Vous intégrerez notamment l'équipe en charge du projet **Oursin** (https://www.synacktiv.com/ressources/synacktiv_oursin_plaquette.pdf). Oursin est une plate-forme de ***spear-phishing*** permettant de mettre en place des **attaques ciblées** de postes clients. Création de scénario, distribution de charge, **contournement d'antivirus** et **prise de contrôle à distance** font partie de ses fonctionnalités.

Les attaques ciblées sont parmi les clés de la réussite des intrusions en **Red Team**. Un e-mail, une clé USB malveillante sont souvent synonymes de la compromission d'un utilisateur inattentif. La porte est alors ouverte à la **persistance**, au **rebond** et à la **compromission** de masse.

Pour garder une longueur d'avance vis-à-vis des méthodes de défense de plus en plus avancées, les méthodes d'attaque doivent être en constante évolution. En intégrant l'équipe en charge du projet Oursin, votre rôle sera de concevoir, améliorer, suggérer de nouveaux composants sur l'outil Oursin**.** À ce titre, vous devrez :

- Imaginer et mettre en œuvre des mécanismes de **détection de sandboxes** voulant analyser les charges utiles et implémenter des solutions de **contournement** afin de duper les analyses dynamiques de plus en plus courantes et performantes ;
- Imaginer et mettre en œuvre des solutions de **rebonds** et de **domain fronting** pour protéger le C&C ;
- Imaginer et mettre en œuvre des méthodes de **contournement des principaux EDR du marché** ;

Pour intégrer notre équipe, vous devrez également :

- Avoir des bases en développement Python et le recul vous permettant de prendre en main un projet existant ;
- Travailler en collaboration avec des experts en intrusion expérimentés qui utilisent le projet quotidiennement.

Vous serez également amenés tout au long du stage à intervenir sur des missions de type **Red Team** afin de mieux comprendre le métier et ainsi proposer un projet au plus proche du besoin.

Il est attendu que le stage débouche sur un CDI d'expert sécurité chez Synacktiv.

Profil & compétences

- Forte volonté d'apprendre, de se perfectionner et d'innover sur les techniques d'évasion réseau et de furtivité.
- Programmation **Python**. Notre suite d'outils internes est principalement programmée dans ce langage, vous devez avoir une expérience minimale en Python pour contribuer à son développement.
- Anglais et français indispensables.
- Stage basé à Paris dans le 2ème arrondissement (Grands Boulevards).
- Rémunération 1500€ brut / mois.

À VOS CV ! apply@synacktiv.com

3.3. Mastermind

Description du poste

Synacktiv recherche un expert en sécurité informatique capable de participer au développement du projet existant **Disconet** (http://www.synacktiv.ninja/ressources/synacktiv_disconet_plaquette.pdf).

Disconet est utilisé à la fois comme automate et comme plate-forme collaborative pour la réalisation des **opérations d'intrusion**. Il agrège un large volume d'informations concernant des réseaux, des systèmes, des applications, et des groupes d'utilisateurs. Ces informations sont ensuite traitées par une intelligente artificielle (IA) capable de prendre ou suggérer des décisions aux équipes opérationnelles.

Le projet est déployé en production, mais nécessite des évolutions constantes notamment sur l'évolution de l'IA du projet qui doit à terme pouvoir être considérée comme un véritable assistant pour les équipes. À ce titre, vous devrez :

- travailler en collaboration avec l'équipe de développement du projet ;
- faire évoluer les capacités de l'automate (développement de nouveaux plugins automatisant certaines attaques, la collecte d'information, etc.) avec un focus prioritaire sur les chaînes automatisant les phases de reconnaissances pré-authentification (aussi bien **web** que **Windows**, **Linux**, etc.) ;
- interfacer le projet Disconet avec des projets Synacktiv déjà existants.

Dans les faits, il s'agira de :

- savoir s'intégrer dans une équipe de développement et prendre en main un projet existant ;
- être capable de développer et résoudre des problématiques de façon transverse sur une application 3-tiers : des requêtes SQL à l'interface graphique JS/CSS, en passant par la logique Python ;
- De travailler en collaboration avec des consultants sécurité expérimentés qui utilisent le projet quotidiennement.

Au cours de ce stage vous serez également amenés à participer à des tests d'intrusion de manière régulière afin de recueillir les besoins de l'équipe opérationnelle et monter en compétence sur le sujet.

Il est attendu que le stage débouche sur un CDI d'expert sécurité chez Synacktiv.

Profil & compétences

- Forte volonté d'apprendre et de se perfectionner sur les aspects techniques liés aux tests d'intrusion et au développement d'outils de sécurité.
- Programmation **Python**. Notre suite d'outils internes est principalement programmée dans ce langage, vous devrez connaître ou être prêt à apprendre rapidement Python pour contribuer à son développement. Maîtrise de SQL et JavaScript, notions de CSS.
- Anglais et français indispensables.
- Stage basé à Paris dans le 2ème arrondissement (Grands Boulevards).
- Rémunération 1500€ brut / mois.

À VOS CV ! apply@synacktiv.com

4. Stage pôle reverse engineering

4.1. 0day hunting / reverse-me if you can

Description du poste

Dans le cadre de différentes missions d'intrusion, les experts sécurité Synacktiv font face à des technologies n'ayant pas fait l'objet de recherches suffisantes. Les outils pour manipuler certains protocoles manquent et les vulnérabilités diffusées publiquement sont souvent de type « unspecified vectors / unspecified impact ».

Synacktiv recherche un expert sécurité pour travailler sur la **rétro-ingénierie**, le **matériel** et la conception d'**outils d'attaques**.

Les technologies ciblées seront discutées avant le début du stage. À titre d'exemple, voici une liste de technologies et produits susceptibles d'être étudiés : Citrix, Windows (kernel & userland), technologies mobiles du marché, Linux, Cisco IOS, virtualisation, RDP, et d'autres. Il s'agit de :

- Étudier des technologies et des **logiciels propriétaires**.
- **Développer des outils** permettant de tester la sécurité de ces technologies : canaux de communication, chiffrement, interception, etc.
- Chercher des **vulnérabilités** et de développer les codes d'exploitation associés.

Il ne s'agit pas de :

- Rédiger un guide de bonnes pratiques ou de faire une compilation des recherches existantes, même s'il sera attendu une bonne maîtrise des attaques existantes.
- Chercher des vulnérabilités théoriques sans scénarios opérationnels plausibles.

Il est attendu que le stage débouche sur un CDI d'expert sécurité dans le pôle rétro-ingénierie de Synacktiv.

Profil & compétences

- Forte volonté d'apprendre et de se perfectionner sur les aspects techniques liés à la rétro-ingénierie, l'audit sécurité de code source et la recherche de vulnérabilités.
- Programmation **Python**. Notre suite d'outils internes est principalement programmée dans ce langage, vous devrez connaître ou être prêt à apprendre rapidement Python pour contribuer à son développement.
- Maîtrise des outils de rétro-ingénierie comme **IDA** sur différentes architectures et de l'analyse sécurité de protocoles.
- Anglais et français indispensables.
- Stage basé à Paris dans le 2ème arrondissement (Grands Boulevards).
- Rémunération 1500€ brut / mois.

À VOS CV ! apply@synacktiv.com

4.2. One fuzzer to rule them all

Description du poste

Synacktiv recherche un expert en sécurité informatique capable de participer au développement de son **framework de fuzzing**.

Le fuzzing est un outil indispensable dans la recherche de vulnérabilités. Il existe aujourd'hui dans l'état de l'art de nombreux moyens pour rendre un fuzzer plus efficace : génération et/ou mutation de *test-case* intelligente, couverture de code, exécution symbolique, etc. Cependant, la diversité des cibles et la complexité des logiciels font que les outils existants se révèlent souvent limités et le fuzzing reste aujourd'hui un sujet de recherche ouvert.

Le framework développé par Synacktiv est déjà opérationnel et largement utilisé en interne. Néanmoins plusieurs axes d'améliorations demeurent :

- Amélioration et optimisation des différents composants du framework.
- Développement de grammaires.
- Support d'architectures et d'environnements supplémentaires.
- Développement d'outils afin de faciliter la mise en place de campagnes avancées.
- Implémentation de **techniques de fuzzing innovantes**.
- Fuzzer le monde en vue de sa conquête.

Il s'agit de :

- Intégrer de nouvelles fonctionnalités à un outil existant.
- Travailler sur des cas concrets et bloquants rencontrés par les experts Synacktiv.
- Utiliser la rétro-ingénierie afin d'étudier des **logiciels *closed-source***.

Il est attendu que le stage débouche sur un CDI d'expert sécurité dans le pôle rétro-ingénierie de Synacktiv.

Profil & compétences

- Forte volonté d'apprendre et se perfectionner en développement bas niveau et en rétro-ingénierie.
- Programmation en **C**, la quasi-totalité des composants du framework étant développés en C.
- Programmation **Python**. Notre suite d'outils internes est principalement programmée dans ce langage, vous devrez connaître ou être prêt à apprendre rapidement Python pour contribuer à son développement.
- Anglais et français indispensables.
- Stage basé à Paris dans le 2ème arrondissement.
- Rémunération 1500€ brut / mois.

À VOS CV ! apply@synacktiv.com

4.3. Gotta glitch ’em all!

Description du poste

Synacktiv recherche un expert en sécurité informatique capable de participer au développement d’attaques par injection de fautes sur des **microcontrôleurs couramment utilisés dans le monde IoT**.

Ces microcontrôleurs embarquent des protections pour empêcher la lecture de leur firmware, l’utilisation de leurs **interfaces de débogage** ou le **chargement d’un firmware illégitime**. Les implémentations de ces mécanismes ne sont généralement pas résistantes aux attaques matérielles telles que les « **glitch** » en courant. Ces protections peuvent être un point bloquant pour les missions de pentest et de rétro-ingénierie.

Il existe depuis peu des frameworks open source basés sur du matériel peu coûteux pour construire des bancs d’attaque pour ce type de microcontrôleur.

Afin d’améliorer l’efficacité et la qualité des audits de composants IoT, Synacktiv souhaite développer un ensemble d’outils pour réaliser rapidement ce type d’attaque. Il s’agit de :

- Mettre en place un banc d’attaque.
- Réaliser les modifications sur les cartes permettant de réaliser les attaques.
- Paramétrer les attaques pour différents microcontrôleurs dans différentes configurations.
- Outiller l’exploitation des fautes (dump de **firmware**, **JTAG**, **bypass secure boot**, etc.).
- Utiliser la **rétro-ingénierie** afin d’étudier les bootrom des microcontrôleurs.
- Travailler sur des cas concrets et bloquants rencontrés par les experts Synacktiv.

Il est attendu que le stage débouche sur un CDI d'expert sécurité dans le pôle rétro-ingénierie de Synacktiv.

Profil & compétences

- Forte volonté d'apprendre et se perfectionner en développement bas niveau et en rétro-ingénierie.
- Programmation sur **FPGA**.
- Programmation **Python**.
- Anglais et français indispensables.
- **Stage basé à Toulouse.**
- Rémunération 1500€ brut / mois.

À VOS CV ! apply@synacktiv.com

4.4. SIMsploit

Description du poste

Synacktiv recherche un stagiaire (H/F) en sécurité informatique capable d'étudier des cartes **SIM**, leurs applications et d'entreprendre des attaques sur les différentes interfaces exposées par ces applications.

Les cartes SIM sont des *smartcards* dotées d'un système d'exploitation, de fonctions, permettant d'identifier et d'authentifier un abonné, d'un système de fichiers et d'applets permettant d'autres actions comme le NFC-SIM pour le paiement, le *tracking*, *roaming management*, etc. Normalement, chaque application est correctement isolée dans une *sandbox* Java et peut-être managée à distance, par exemple avec un SMS de type OTA (Over-The-Air). Chaque application a un niveau de sécurité appelé le MSL (Minimum Security Level), permettant de protéger une commande en intégrité et confidentialité. Cependant, ce niveau de sécurité peut-être très hétérogène entre les différentes applications. Il est donc rare, mais pas impossible de retrouver des applications non sécurisées avec un niveau MSL=0. De plus, en 2014, des attaques ont montré que des clés OTA étaient faibles et qu'un attaquant capable de casser ces clés pouvait ainsi compromettre l'application ciblée.

Dernièrement, des attaques ont été publiées sur S@T (SIM Application Toolkit) et WIB (Wireless Internet Browser) permettant à un attaquant d'envoyer des messages arbitraires et d'effectuer d'autres actions malveillantes, augmentant ainsi notre fort intérêt dans l'étude des cartes SIM.

Il existe aujourd'hui des outils comme SIMtester[1] permettant de tester différentes vulnérabilités, mais ces outils sont encore peu exhaustifs et nous ne connaissons que trop peu les autres fonctionnalités et applications exposées, ainsi que les applications spécifiques à l'opérateur.

Le stage consistera donc à renforcer les connaissances de l'équipe au sujet des cartes SIM en :

- effectuant un état de l'art sur la sécurité des cartes SIM.
- mettant en place un **environnement de test de cartes SIM** sur des attaques connues.
- trouvant de **nouvelles vulnérabilités sur des cartes SIM** d'opérateurs variés.
- développant des techniques d'**attaques à distance en mobile et en NFC** pour exploiter les applications exposées.
- enrichissant l'environnement de test avec les nouvelles attaques mises au point.

Il est attendu que le stage débouche sur un CDI d'expert sécurité dans le pôle rétro-ingénierie de Synacktiv.

Profil & compétences

- Forte volonté d'apprendre et se perfectionner en mobile et carte à puce.
- Programmation **Python, Java, ou C/C++**.
- Anglais et français indispensables.
- Stage basé à Paris dans le 2ème arrondissement.
- Rémunération 1500€ brut / mois.

À VOS CV ! apply@synacktiv.com

1 https://srlabs.de/bites/sim_attacks_demystified/

5. Stage pôle étude et développement

5.1. Crack me if you can !

Description du poste

Synacktiv recherche un stagiaire (H/F) en sécurité informatique capable de participer au développement de deux projets existants : **Kraqozorus** et **Leakozorus**, deux projets en relation avec le **cassage de mots de passe**. Le premier est une plateforme de calcul distribué à base de CPU et GPU permettant de retrouver les mots de passes à partir de leurs empreintes. Le second est une plateforme d'archivage, d'indexation et de recherche des mots de passes récupérés dans des fuites publiques. Ces outils sont utilisés par nos équipes de test d'intrusion pour la réalisation de *red-teams* et d'audits de sécurité.

Les mots de passes faibles ou laissés par défaut sont un des vecteurs d'intrusion les plus efficaces et cette offre de stage vise à améliorer l'état de l'art de **Kraqozorus** sur plusieurs aspects :

- Améliorer les performances de cracking via **l'optimisation** et la **parallélisation** de l'effort,
- Améliorer les règles de **génération** de mots de passes candidats,
- Générer dynamiquement des **dictionnaires** adaptés à une cible et à un format de hachage donné,
- Consolider les résultats de plusieurs années de cracking afin d'optimiser et affiner les stratégies d'attaques,
- Utiliser du ***machine-learning*** pour générer des mots de passes candidats.

En ce qui concerne **Leakozorus**, les challenges sont différents et touchent plus au monde du « big data » :

- **Indexer** efficacement plusieurs milliards d'entrées,
- Améliorer les performances de recherche,
- Améliorer la **scalabilité horizontale** de la solution,
- Analyse, statistiques et représentations graphiques de très gros volume de données.

Il est attendu que le stage **débouche sur un CDI** d'expert sécurité chez Synacktiv.

Profil & compétences

- Programmation **Python**.
- Expérience avec **JohnTheRipper** et **Hashcat**.
- Expérience en développement en environnement **Linux**.
- Avoir des bases en **sécurité** des systèmes d'information ainsi qu'en **réseaux, cryptographie et systèmes UNIX.**
- Expérience en SQL requise, et si possible ElasticSearch.
- Forte volonté d'**apprendre**, de **progresser** et d'**innover** sur les techniques d'intrusion et la sécurité offensive.
- Bonnes compétences rédactionnelles et de communication. **Anglais et français indispensables.**
- Stage basé à Paris dans le 2ème arrondissement (Grands Boulevards).
- Rémunération 1500€ brut / mois.

A VOS CV ! apply@synacktiv.com

5.2. Offensive Tooling

Description du poste

Synacktiv recherche un stagiaire (H/F) en sécurité informatique capable de rejoindre son **pôle développement**. En plus de créer et maintenir des outils internes au profit des autres départements, le pôle réalise des missions de développement **d'outils d'intrusion** et de sécurité dite offensive. L'expert peut donc être amené à travailler sur des projets de R&D de type : implants et C&C, packer, fuzzer, cassage de mots de passes, spear-phishing, systèmes embarqués, ou autres.

Voici quelques exemples de réalisations précédentes :

- **Kraqozorus** : plateforme de cassage de mots de passes (https://synacktiv.com/ressources/synacktiv_kraqozorus_plaquette.pdf)
- **Oursin** : une plateforme de spear-phishing (https://synacktiv.com/ressources/synacktiv_oursin_plaquette.pdf)
- **Disconet** : un automate collaboratif pour les tests d'intrusions (https://synacktiv.com/ressources/synacktiv_disconet_plaquette.pdf)
- **Houdini** : un système embarqué pour les intrusions physiques (https://synacktiv.com/ressources/synacktiv_houdini_plaquette.pdf)

Ce poste permet de faire **avancer l'état de l'art** de la sécurité offensive tout en ayant la **satisfaction** d'équiper des experts du domaine avec de nouveaux outils d'intrusion !

Il est attendu que le stage débouche sur un CDI d'expert sécurité chez Synacktiv.

Profil & compétences

- Programmation **Python et C**. Notre suite d'outils internes est principalement programmée en Python, et le C reste incontournable pour la programmation système et bas niveau qui en font donc un pré-requis essentiel.
- Expérience en développement en environnement Linux.
- Avoir des bases en **sécurité** des systèmes d'information ainsi qu'en **réseaux, cryptographie et systèmes UNIX.**
- Forte volonté d'**apprendre**, de **progresser** et d'**innover** sur les techniques d'intrusion et la sécurité offensive.
- Bonnes compétences rédactionnelles et de communication. **Anglais et français indispensables.**
- Stage basé à Paris dans le 2ème arrondissement (Grands Boulevards).
- Rémunération 1500€ brut / mois.

A VOS CV ! apply@synacktiv.com

6. Stages pôle administration systèmes & réseau

6.1. Audit As a Service

Description du poste

Synacktiv recherche un stagiaire (H/F) pour participer à la conception d'une solution d'audit continu de ses infrastructures sensibles. Afin d'avoir une vision plus claire au quotidien nous souhaitons avoir la possibilité de fournir des outils pour orchestrer l'audit permanent de la sécurité de nos systèmes.

Synacktiv possède déjà des outils permettant la collecte d'informations et l'audit des données collectées afin d'identifier des vulnérabilités classiques. Cependant ces briques de base ne sont pas intégrées dans un outil plus global permettant la supervision du système d'information et l'identification des vulnérabilités est générique, et parfois inadaptée aux problématiques sécurité du système d'information de Synacktiv.

L'objectif de ce stage est la réalisation d'une maquette orchestrant l'audit continu d'une infrastructure hétérogène (serveur, poste utilisateur, équipement réseau) en se basant sur des outils internes déjà développés et des solutions existantes du marché. La plateforme devra réaliser de façon automatique et régulière la collecte d'informations, l'analyse et la synthèse des données.

Les axes de travail suivants sont à considérer :

- Identification et collecte d'indicateurs ;
- Stockage et journalisation de ses derniers ;
- Analyse régulière et comparaison de l'évolution ;
- Remonté d'alertes en fonction de l'analyse des résultats ;
- Proposition d'amélioration de l'existant ;

Le stagiaire peut donc espérer trouver des tâches de **développement** (Shell, Python...), d'administration système ainsi que du **durcissement** de système Linux.

Il est attendu que le stage débouche sur un CDI d'administrateur réseau et systèmes chez Synacktiv.

Profil & compétences

- Intérêt pour les systèmes **Linux** et la **sécurité** des SI.
- Programmation **Python et Shell**.
- Forte volonté d'**apprendre**, de **progresser** et d'**innover** sur les techniques de défense des systèmes d'information.
- Stage basé à Paris dans le 2ème arrondissement.
- Rémunération 1500€ brut / mois.

A VOS CV ! apply@synacktiv.com

6.2. Pimp my HIPS

Description du poste

Dans le cadre de l'implémentation de défenses en profondeur, Synacktiv souhaite **améliorer ses capacités en termes de détection d'intrusion au niveau de ces serveurs sensibles.** Dans ce cadre, Synacktiv recherche un stagiaire (H/F) pour participer à ce projet. Ce stage concerne la détection d'intrusion au niveau « hôte » (HIPS), c'est-à-dire sans réaliser de capture réseau (NIDS).

Les systèmes sensibles dont il est question sont des serveurs Linux classiques hébergeant des applicatifs divers. La détection d'intrusion est à considérer au niveau noyau (ex : auditd, LSM, pare-feu local), au niveau système (ex : PAM) et au niveau applicatif (ex : journaux applicatifs).

Ce projet est découpé 3 phases :

- identification des **marqueurs d'intrusion** spécifiques au système d'information Synacktiv ;
- modification de la configuration des services et systèmes afin de générer de nouveaux marqueurs si nécessaire ;
- consolidation du système de remontée et d'agrégation d'**évènements sécurité** ;

Afin d'assister le stagiaire dans son travail, des experts Synacktiv réaliseront des attaques sur des systèmes de pré-production afin de générer. Un ensemble de marqueurs qui pourront ensuite être utilisés comme jeu de test. Les marqueurs de bases spécifiques au système d'information Synacktiv seront fournis mais il est attendu que le stagiaire identifie de nouveaux marqueurs d'intrusion.

Il est attendu que le stage débouche sur un CDI administrateur réseau et systèmes chez Synacktiv.

Profil & compétences

- Intérêt pour les systèmes **Linux** et la **sécurité** des SI.
- Programmation **Python et Shell**.
- Forte volonté d'**apprendre**, de **progresser** et d'**innover** sur les techniques de défense.
- Stage basé à Paris dans le 2ème arrondissement.
- Rémunération 1500€ brut / mois.

A VOS CV ! apply@synacktiv.com

6.3. KerneSec

Description du poste

Dans le cadre de l'implémentation de défenses en profondeur sur son système d'information, Synacktiv recherche un stagiaire (H/F) pour renforcer la sécurité noyau des systèmes sensibles. Il s'agit dans un premier temps d'étudier la possibilité d'appliquer des modifications au noyau Linux. Et dans un second temps il s'agit d'améliorer des politiques de sécurité AppArmor. **L'objectif est de réduire la probabilité d'exploitation d'une vulnérabilité applicative ou système.**

La première partie du stage concerne la réalisation d'une maquette permettant de patcher, compiler et tester des noyaux Linux personnalisés. Les patchs seront publics ou internes avec comme objectif de fournir une meilleure protection du noyau. Les étapes suivantes seront nécessaires à la réalisation de la maquette :

- État de l'art des différents mesure de **sécurité du noyau Linux** (ex : KSPP, grsecurity, lockdown…) ;
- **Automatisation** de l'application et de la compilation d'un ensemble de patch pour un type de profil ;
- **Tests et validation** de non régression ;

La deuxième partie du stage concerne l'audit et l'amélioration des politiques de sécurité **AppArmor** déjà déployées chez Synacktiv.

Il est attendu que le stage débouche sur un CDI administrateur réseau et systèmes chez Synacktiv.

Profil & compétences

- Intérêt pour les systèmes **Linux** et la **sécurité** des systèmes d'information.
- Programmation **Python et Shell**.
- Forte volonté d'**apprendre**, de **progresser** et d'**innover** sur les techniques de défense.
- Stage basé à Paris dans le 2ème arrondissement.
- Rémunération 1500€ brut / mois.

A VOS CV ! apply@synacktiv.com