

## STAGE DÉVELOPPEUR PYTHON

### MÉTIER

COGICEO est une société indépendante, spécialisée dans l'audit en sécurité informatique. Fondée par des consultants seniors de grandes entreprises françaises et forts de plus de 10 ans d'expérience, son cœur de métier repose sur leur expertise technique dans ce domaine et en particulier dans les tests d'intrusion. Nos services s'articulent autour de 2 axes majeurs :

#### Audit

*Analyser la robustesse d'un système face aux attaques réelles.*

- ⦿ Test d'intrusion
- ⦿ Audit de configuration
- ⦿ Audit d'architecture
- ⦿ Audit organisationnel et physique
- ⦿ Audit de code source

#### Formation

*Acquérir des compétences techniques en sécurité grâce à des ateliers.*

- ⦿ Sensibilisation COMEX/CODIR/DSI
- ⦿ Formation développement web sécurisé
- ⦿ Formation administration système et réseau sécurisée

### CADRE DU STAGE

- ⦿ Nombre de postes à pourvoir : 1
- ⦿ Contrat : convention de stage obligatoire
- ⦿ Durée du stage : de 5 à 6 mois
- ⦿ Rémunération : gratification de stage selon profil
- ⦿ Lieu principal : 28 bis boulevard de Sébastopol - 75004 Paris
- ⦿ Date d'entrée en poste : au plus tôt
- ⦿ Horaires : du lundi au vendredi de 9h30 à 18h30 (35h)

### PROFIL RECHERCHÉ

Nous recherchons une personne **appréciant les métiers du développement** et qui soit capable de s'intégrer dans une équipe jeune et dynamique sans pour autant en oublier de **réaliser ses tâches avec rigueur**. Afin de réussir à ce poste, une bonne maîtrise du langage **Python** et une **sensibilité accrue à la sécurisation de son code** sont absolument nécessaires. Vous serez par ailleurs épaulé par des membres de l'équipe dans la gestion de vos projets.

Des compétences en **exploitation ou administration de systèmes Linux** constitueraient un avantage.

### CANDIDATURE

Pour postuler à ce stage, veuillez **envoyer votre CV** à l'adresse suivante : **stages@cogiceo.com**

Dans votre mail, **vous préciserez le(s) sujet(s) académiques** le(s) plus en adéquation avec vos attentes et les raisons de ce choix. Vous serez recontacté pour un entretien téléphonique avant une éventuelle rencontre dans nos locaux à Paris.

### DÉBOUCHÉ

Le stage de fin d'études peut déboucher sur une proposition d'**embauche en CDI**.

## SUJETS ACADÉMIQUES

Votre rôle principal sera de participer au développement de nos outils internes et externes. Tous ces outils sont codés en Python et n'utilisent, autant que possible, que les bibliothèques standard (pas de django, requests, ...). Selon votre profil et vos aspirations, vous pourrez également être amené(e) à travailler à l'administration de systèmes. Voici quelques exemples de sujets que nous pouvons vous proposer :

### Implémentation Python d'une bibliothèque codée en C

Les domaines Active Directory sont omniprésents dans les réseaux d'entreprises. Difficiles à sécuriser, ces domaines représentent souvent la partie la plus vulnérable d'un système d'information. Pour accompagner ses clients, Cogiceo dispose d'un outil d'analyse du niveau de sécurité des domaines Microsoft. Une grande partie des informations d'un domaine Active Directory sont contenues dans un fichier de base de données nommé NTDS.DIT. Ce fichier est au format ESE, un format utilisé par de nombreuses technologies Microsoft. Le but du stage est d'écrire une bibliothèque de parsing de ce format en Python, sachant que nous disposons déjà d'une bibliothèque fonctionnelle écrite en C.

### Conception d'un tunneler réseau automatique

Le tunneling consiste à encapsuler un protocole réseau dans un autre (par exemple TCP sur HTTP ou TCP sur ICMP) dans le but de contourner des règles de filtrage existantes et ainsi d'accéder à une machine ou un réseau qui n'est normalement pas joignable. Après avoir recensé les technologies existantes, le but de ce sujet de stage est de développer un outil polyvalent permettant d'analyser automatiquement les règles de filtrage en place et de monter un tunnel adéquat en fonction des protocoles réseaux disponibles (DNS, ICMP, HTTP, etc). Des connaissances réseaux (modèle OSI, protocoles les plus courants) et en développement (python, C) seront nécessaires. Ce tunneler automatiquement sera exploité par les consultants de Cogiceo dans le cadre des exercices Redteam.

### Conception d'un serveur C&C et son agent

Le « C&C » ou « C2 », pour « Command & Control » est un outil que Cogiceo exploite dans le cadre de ses missions Redteam et qui se décompose en deux parties : un serveur et plusieurs agents. Les agents sont initiés sur des machines compromises et viennent régulièrement récupérer auprès du serveur des instructions à exécuter. Le but de ce stage sera d'améliorer et de compléter les outils déjà existant : développement de nouveaux agents dans différents langages (Powershell, bash, python, C), mise en place de techniques d'obfuscation réseau et logicielle et amélioration du serveur de contrôle . Un état de l'art sera au préalable nécessaire afin de recenser les technologies existantes.

### Conception physique et logique d'un mouchard réseau

Dans le cadre de l'amélioration des outils utilisés lors des missions Redteam, Cogiceo a développé un mouchard réseau. Après avoir réalisé un état de l'art des solutions existantes, le stagiaire devra concevoir et développer un mouchard réseau miniaturisé permettant le montage automatique de tunnel via une connexion mobile. Ce « Plug and Forget » devra également intégrer un panel d'outils utilisables lors des tests d'intrusion, une interface Wi-Fi, le support du PoE ainsi que la possibilité de stocker les différentes trames émises en broadcast. Une partie du stage sera également consacrée à la sécurisation du mouchard afin de rendre sa détection sur le réseau le plus complexe possible.