Expertise technique en sécurité informatique

LA SOCIÉTÉ

MÉTIER

Cogiceo est une société indépendante, spécialisée dans l'audit technique en sécurité informatique. Fondée en 2012 par 2 consultants seniors issus de grandes entreprises françaises, son cœur de métier repose sur l'expertise technique dans le domaine de la sécurité des systèmes d'informations et en particulier dans les **tests d'intrusion qui représente 80 % de son chiffre d'affaires.**

OFFRES

Audit

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

Red Team

- Campagne de Phishing
- Social Engineering
- Test d'intrusion physique
- Test d'intrusion de l'exposition Internet
- Test d'intrusion réseau interne

Forensic

- Gestion d'incident
- Digital forensic
- Analyse de malware
- Network tracking

Scan

- ADA : Active Directory Security Analyzer
- LINA : Linux Security Analyzer
- MOBAA : Mobile and Browser Application Audit
- Explorer : Internet Exposure Exploration

Formation

- Sensibilisation C-Level managers et end-users
- Formation sécurité administrateur système et réseaux
- Formation sécurité développeur
- Formation sécurité administrateur AD

ÉQUIPE

Cogiceo est une entreprise à taille humaine composée actuellement de **25 collaborateurs.** Une forte limitation dans la croissance de la structure est clairement affichée afin d'effectuer une formation optimale des collaborateurs et ainsi garantir une excellente qualité de prestation auprès des clients. **Notre équipe est dynamique** et nous souhaitons explicitement nous démarquer des nombreuses SSII sur le marché en prenant le temps de former nos consultants. Nos collaborateurs bénéficient donc d'**importants transferts de compétences et de temps de R&D notables**.

LE STAGE

OBJECTIF

L'objectif globale du stage de fin d'études est la formation au métier de consultant en sécurité des systèmes d'information. Dans cet esprit, vous accompagnerez, **50 % de votre temps**, nos équipes de consultants expérimentés sur certaines de leurs missions (principalement sur des **pentests** de systèmes exposés sur Internet puis, selon votre progression, sur des **pentests** de systèmes internes aux SI de nos clients). En parallèle, vous travaillerez **50% de votre temps sur un sujet de recherche académique** (à choisir dans notre catalogue, ou à proposer vous-même).

PROFIL RECHERCHÉ

Le stagiaire doit être en fin d'étude de **niveau BAC+5 (École d'Ingénieur ou Master en Sécurité)** et posséder des bases solides en informatique : réseau, système, développement, etc. De plus, il doit être **passionné par la sécurité informatique** et être capable d'**apprendre rapidement** au contact de consultants expérimentés. Des bases en **Python** seraient fortement appréciées. Les qualités humaines recherchées sont : probité, persévérance, curiosité et autonomie. Des compétences en **exploitation ou administration de systèmes Linux** constitueraient un avantage.

CADRE DU STAGE

- Nombre de postes à pourvoir : 3
- Contrat : convention de stage obligatoire
- Durée du stage : de 5 à 6 mois
- Rémunération : **1500€** par mois
- Avantages : 50 % de la carte de transport, tickets restaurant
- Lieu principal : 95 boulevard de Sébastopol - 75002 Paris
- Date d'entrée en poste : au plus tôt
- Horaires : du lundi au vendredi de 9h30 à 18h30 (35h)

DÉBOUCHÉ

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

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, dans l'ordre de préférence. Vous serez recontacté pour un entretien téléphonique avant une éventuelle rencontre dans nos locaux à Paris.

SUJETS DE STAGE

#1 - ANALYSE AUTOMATIQUE D'UN ENVIRONNEMENT ACTIVE DIRECTORY - ADA

Catégories : Produit SaaS, Pentest

Description

Les domaines Active Directory sont omniprésents dans les réseaux d'entreprises et difficiles à sécuriser. Ces domaines représentent souvent la partie la plus vulnérable d'un système d'information.
Cogiceo développe ADAnalyzer, un outil permettant d'analyser le niveau de sécurité d'un domaine et de remonter les vulnérabilités présentes sur celui-ci.
Après s'être familiarisé avec les fonctionnalités déjà implémentées dans l'outil ADAnalyzer, le stagiaire participera à la recherche et l'implémentation de nouvelles fonctionnalités.

Objectifs

1. Recherche et documentation des chemins de compromission via AD CS (Services de certificats Active Directory)
2. Recherche et documentation des chemins de compromission via des ACL mal configurées
3. Recherche et documentation des techniques récentes d'élévation de privilèges sur un système Windows
4. Participer à l'implémentation en Python du calcul des nouvelles vulnérabilités
5. Ajout de modules au script PowerShell permettant la récolte de nouvelles informations à analyser

#2 - ANALYSE DE SÉCURITÉ AUTOMATIQUE D'UN PARC DE SERVEURS LINUX - LINA

Catégories : Produit SaaS, Pentest

Description

Cogiceo propose à ses clients un produit d'analyse automatique de la sécurité d'un parc de serveurs Linux. Il permet d'identifier les vulnérabilités présentes sur chaque serveur, mais aussi de corréler les informations inter-serveurs. Après s'être familiarisé avec les fonctionnement de l'outil et le développement UNIX shell, le stagiaire travaillera sur la partie collecte des données en implémentant de nouvelles fonctionnalités techniques, le support de nouveaux OS et de serveurs LDAP. Une fois ces données collectées, il pourra passer à l'analyse et à la corrélation ces informations pour identifier des chemins de compromission au sein du réseau.

Objectifs

1. Réaliser la collecte des données d'un serveur OpenLDAP
2. Identifier et implémenter les vulnérabilités des serveurs OpenLDAP
3. Comprendre le fonctionnement des mécanismes sudoers et implémenter une analyse approfondies des vulnérabilités identifiables
4. Lister et implémenter les points de contrôles restants CIS sur Red Hat et Debian
5. Travailler à la méthode de calcul de la note du périmètre audité

#3 – ANALYSE ET PENTEST D'APPLICATIONS ANDROID, IOS ET CHROME

Catégories : Solution SaaS, Pentest

Description

Cogiceo réalise régulièrement des missions d'audit d'application mobile Android et iOS. De plus, Cogiceo met à disposition de ses clients un service d'analyse de la sécurité des extensions chromes et des applications mobiles Android. Dans un premier temps le stagiaire étudiera les vulnérabilités et méthodologies d'analyses des applications mobiles et des extensions chrome. Il participera par la suite à l'intégration de nouveaux points de contrôles sur le service d'analyse.

Objectifs

1. Recherche et analyse de vulnérabilité pouvant affecter des extensions chromes et des applications mobiles Android
2. Ajout de point de contrôle précis lié aux environnements Firebase
3. Mise en place d'un environnement permettant l'analyse dynamique des extensions et applications mobiles
4. Ajout du support des applications mobiles iOS sur notre plateforme d'analyse (établissement de point de contrôle, analyse statique)

#4 - DÉVELOPPEMENT D'UN FRAMEWORK D'ÉVASION DES SOLUTIONS AV ET EDR

Catégories : Red Team

Description

Lors des missions de Pentest ou de RedTeam, les auditeurs sont souvent amenés à contourner les dispositifs de détection (AV / EDR) afin d'exécuter du code ou de déposer des exécutables (implant C2, outils, ...) sur une machine compromise. Pour cela, des « Packer » existent et permettent d'injecter des modules de bypass (AMSI, ajout de Sycall, ...) mais aussi d'obfusquer, de chiffrer et de transformer un exécutable pour masquer son fonctionnement malveillant. A l'exécution, le binaire va se retransformer en mémoire pour exécuter le code original. En revanche, la signature de ces packers est très rapidement reconnus par les AV et les EDR après leur publication. Le but de ce stage est donc de créer un outil permettant de modifier un exécutable pour le rendre plus difficilement détectable par les solutions antivirale du marché et de le packer avec un module interne dont la signature n'est pas connue.

Objectifs

1. Réaliser un état de l'art sur les Packer de PE et les techniques d'évasion antivirale existants et les tester (Inceptor, …)
2. Sélectionner les techniques d'évasion les plus pertinentes à mettre en œuvre (Bypass AMSI, Direct Syscall, ...)
3. Mettre en place un outil interne (custom ou intégrant des features de différents outils) permettant de Packer des exécutables pour les rendre indétectable par les solutions antivirales
4. Tester la viabilité de cet outil face aux AV et EDR les plus fréquemment rencontrés en mission

#5 - DÉVELOPPEMENT D'OUTILS DE RECONNAISSANCE POUR LES RED TEAM

Catégories : Red Team, Pentest

Description

Cogiceo réalise régulièrement des missions de cartographie ou d'empreinte externe pour ses clients, que ce soit dans le cadre d'une surveillance régulière de l'exposition d'une entreprise ou dans le cadre de missions ponctuelles orientées « Red Team ». Le but de ce stage est dans un premier temps de se former aux méthodes passives et actives qui permettent de cartographier la surface d'attaque exposée par une entreprise. Ensuite, le stagiaire pourra développer des méthodologies opérationnelles et des outils permettant de faciliter la collecte d'informations pour les missions Red Team. Dans le cadre spécifique de ce stage, vous serez également amenés à travailler sur des missions de cartographie externe - reconnaissance - OSINT.

Objectifs

1. Se former aux techniques de recon / OSINT et recenser les sources Web d'intérêt
2. Analyser et comparer les workflow de recon issues du monde du Bug Bounty
3. Développer un arsenal d'outils de reconnaissance pour faciliter la réalisation de missions
4. Intégrer ces outils dans nos méthodologies
5. Réflechir à la conception d'un framework interne pour la reconnaissance

#6 - DÉVELOPPEMENT D'UN OUTIL DE PENTEST COLLABORATIF

Catégories : Pentest, Red Team

Description

Lors d'exercices Red Team ou lors des pentests sur de grands périmètres, la prise de note et la collaboration entre les consultants joue un rôle central dans la réussite de la mission. Cogiceo souhaite aujourd'hui développer un outil interne pour répondre à ce besoin et recherche donc un stagiaire pentester ayant de bonnes compétences en développement Python. L'interface développée permettra d'avoir une vision synthétique du périmètre et de l'avancement des tests. Des fonctionnalités indispensables comme des check-lists et un bloc note partagé devront être implémentées. Les missions d'audit auxquelles participera le stagiaire lui permettront de mettre à l'épreuve cet outil et de l'améliorer de façon continue.

Objectifs

1. Réaliser un benchmark des solutions existantes et de leurs fonctionnalités (LAIR, ReconMAP, Hive, IVRE, etc.)
2. Récupérer les besoins internes auprès des consultants et concevoir une première version de l'outil avec interface Web et CLI
3. Intégrer un système d'import des données de test d'intrusion (scans Nmap, Nessus, etc.)
4. Mettre en place un système de prise de note partagée sur les cibles identifiées
5. Mettre en place un système de check-lists par périmètre ou cibles identifiées

#7 - PLATEFORME ANTIVIRALE INTERNE

Catégories : DFIR

Description

Dans le cadre de ses activités de rétro-ingénierie, le CSIRT COGICEO a besoin d'un équivalent d'une plateforme VirusTotal hébergée en interne et coupée de tous réseaux. Cette plateforme sera raccordée à plusieurs solutions antivirales du marché (Symantec Endpoint Protection, Kaspersky Anti-Virus, ClamAV ...etc) afin d'effectuer les premiers scans rapides et à larges échelles de charges suspectes identifiées lors de nos investigations numériques.

Objectifs

1. La plateforme doit évaluer une charge via à minima 5 solutions antivirales d'éditeurs différents;
2. La mise à jour du système hébergeant ce service doit pouvoir se faire hors-connexion Internet;
3. La mise à jour des signatures des solutions antivirales doit se faire hors-connexion Internet;
4. La plateforme doit être développée via une version supérieure ou égale à Python 3.9;
5. La sortie des scans doit être récupérable via une API REST;
6. Les charges suspectes doivent pouvoir être téléversée sur la plateforme via un client Web;
7. L'authentification à cette plateforme doit être vérifiée via l'annuaire OpenLDAP de COGICEO;
8. L'interface Web devra afficher un logo stylé associé au service.

#8 - SYSTÈME D'INGESTION DE DONNÉES SÉCURISÉ

Catégories : DFIR

Description

Dans le cadre de ses activités d'investigation numérique, le CSIRT COGICEO a besoin d'un système physique d'ingestion de données (images de volumes, sorties de collectes d'artefacts, journaux bruts, disques physiques ...etc). Ce système sera constitué d'un ou plusieurs dock de disques, d'un bloqueur en écriture et d'un NAS. Il sera mis à disposition des analystes du CSIRT COGICEO dans une baie sécurisée.

Objectifs

Le système devra être en capacité de :

1. Détecter un branchement de support externe sur un dock;
   - Vérifier le contenu du disque et en déterminer la nature (collectes, images, journaux ...etc);
   - Vérifier la présence ou l'absence de ce contenu sur le NAS;
   - Créer automatiquement un répertoire associé à l'affaire lié à ces collectes sur le NAS;
   - Copier le contenu du ou des supports externes sur le NAS;
2. Le service associé à ce système devra dresser un inventaire du contenu du NAS;
3. Le service associé à ce système devra afficher les copies en cours sur le NAS et le temps restant avant leur finalisation;
4. L'accès à ce système sera restreint par un contrôle par badge afin de garantir une traçabilité totale des gestes effectuées sur le système.

#9 - CRÉATION D'UN ENVIRONNEMENT DE TESTS D'EXPLOIT AVEC SUPERVISION

Catégories : DFIR, Red Team

Description

Dans le cadre de ses activités de R&D, COGICEO a besoin pour ses équipes offensives (REDTEAM) et défensives (CSIRT) d'un service de supervision de systèmes Windows & GNU/Linux afin d'identifier des traces laissés par l'exécution de charges et d'exploitation de vulnérabilités. Ce service permettra aux équipes défensives de tester des exploitations de vulnérabilités récemment publiées en source ouverte et aux équipes offensives de contrôler la proportion de traces laissées par les outils utilisés et développés par COGICEO.

Objectifs

1. Déploiement de système à l'état de l'art (Windows 10/11, GNU/Linux Rocky 9.0 ...etc);
2. Déploiement et configuration d'outils de journalisation additionnels et/ou intégrés (ex : Sysmon, auditd ...etc);
3. Déploiement et configuration d'outils de collecte et de visualisation de journaux (Filebeat, Logstash, Opensearch et Opensearch Dashboards);
4. Tests de détonations des implants du C2 COGICEO avec les équipes offensives;
5. Tests de détonations de charges exploitants des vulnérabilités récentes avec les équipes défensives;
6. Configuration d'un retour arrière (basé sur des snapshots) sur chaque système de test afin de le faire retourner à son état initial.