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 **30 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 : 5
- 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

PENTEST ET ANALYSES D'APPLICATIONS ANDROID ET IOS

Catégories : Pentest, Solution SaaS

Description

Cogiceo réalise régulièrement des missions d'audit d'applications mobiles Android et iOS. La société souhaite aujourd'hui renforcer son expertise en travaillant sur les contournements de protections présentes, développer ses méthodologies Android et iOS et détecter les comportements d'applications malveillantes. De plus, Cogiceo met à disposition de ses clients un service d'analyse de la sécurité des extensions chromes et des applications mobiles Android. Les travaux du stagiaire seront donc amenés à être intégrés à cette solution.

Objectifs

1. Le stagiaire se familiarisera dans un premier temps avec les différents systèmes Mobile et leurs vulnérabilités respectives (Android et iOS),
2. Recherche et analyse de vulnérabilité pouvant affecter des extensions chromes et des applications mobiles Android,
3. Développer des méthodologies d'audit sur iOS et maintenir la documentation,
4. Mise en place d'un environnement permettant l'analyse dynamique des extensions et applications mobiles,
5. Ajout du support des applications mobiles iOS sur notre plateforme d'analyse (établissement de point de contrôle, analyse statique).

COMPROMISSION AZURE AD ET REBONDS VERS AD ON PREMISES

Catégories : Pentest, Red Team

Description

Pour répondre à une demande de plus en plus forte, Cogiceo souhaite accompagner un stagiaire sur des travaux relatifs à la compromission d'un environnement Azure AD. L'état de l'art de cette recherche permettra d'identifier les moyens d'exploiter ces environnements, et surtout d'identifier comment pivoter sur de la compromission d'un AD on-premise, et inversement. Les points de contrôle résultants seront ensuite à intégrer dans la solution SaaS AD Analyzer.

Objectifs

1. Réaliser un état de l'art et une montée en compétence sur l'environnement Azure AD,
2. Identifier les méthodes d'exploitation des environnements Azure AD (accès initial, élévation de privilèges, persistance, exfiltration, …),
3. Mettre en place une infrastructure de tests alliant une infrastructure AD traditionnelle et un Azure AD,
4. Identifier les techniques permettant de pivoter d'un Azure AD vers un environnement On-premise et inversement,
5. Intégration des points de vérifications (vulnérabilités) Azure AD à ADA.

ARSENAL D'EXPLOITATION WI-FI

Catégories : Pentest, Red Team

Description

Cogiceo souhaite faire évoluer son arsenal Wi-Fi pour opérer efficacement lors d'exercices Red Team et Pentests. Cet équipement devra implémenter la majorité des attaques connues sur les réseaux sans-fils, que ce soit dans un contexte d'intrusion sur ces réseaux en exploitant des faiblesses des protocoles, ou dans le cadre de Phishing. Le matériel devra ensuite être testé en conditions réelles.

Objectifs

1. Établir un état de l'art des vulnérabilités sur les réseaux Wi-Fi et compléter les méthodologies existantes,
2. Construire un laboratoire Wi-Fi vulnérable pour les tests et la formation,
3. Configurer une Wireless Pwnbox (Wi-Fi Pineapple ou autre) pour automatiser les attaques sur les protocoles Wi-Fi lors des Red Team et campagnes de Phishing,
4. Mettre en places les méthodes et outils nécessaires à la réalisation des différentes attaques Wi-Fi,

MÉTHODES DE PHISHING ET ACCÈS INITIAL

Catégories : Pentest, Red Team

Description

Cogiceo a réalisé de nombreuses missions de Phishing pour sensibiliser ses clients. Désormais, l'équipe souhaite orienter ses campagnes de Phishing vers de l'obtention d'une exécution de commande distante, dans le but de réutiliser ce travail dans des exercices Red Team. Le stagiaire sera donc amené à recenser les méthodes existantes pour obtenir un accès initial, les tester dans des environnements dédiés, et les interconnecté à nos solutions de contournements AV / EDR. Une dimension relative à l'OSINT humaine et la psychologie viendra compléter ces recherches.

Objectifs

1. Développer de nouveaux scénarios de Phishing pour récolter des statistiques,
2. Tester et documenter les différentes méthodes de Phishing pour obtenir un accès initial (exécution de commande) sur un poste client ou un serveur,
3. Documenter les sources publiques (OSINT) permettant de concevoir au mieux une campagne de Phishing,
4. Agrémenter une base de prétextes utiles pour augmenter les chances de succès de ces attaques,
5. Faire des recherches et des tests sur la mise en place des infrastructures jetables.

CRÉATION D'UN ENVIRONNEMENT DE TESTS D'EXPLOIT AVEC SUPERVISION

Catégories : 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 de tester des exploitations de vulnérabilités récemment publiées en source ouverte et de contrôler la proportion de traces laissées par les outils utilisés et développés par COGICEO ou disponible publiquement.

Objectifs

1. Déploiement de système à l'état de l'art (Windows 10/11, GNU/Linux Rocky 9.0 ...etc) et obsolète ;
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 d'implants C2 et des différents outils utilisés par Cogiceo ;
5. Tests de détonations de charges exploitants des vulnérabilités récentes ;
6. Configuration d'un retour arrière (basé sur des snapshots) sur chaque système de test afin de le faire retourner à son état initial.

AMÉLIORATION DE L'IMPLANT PHYSIQUE POUR REDTEAM

Catégories : Red Team

Description

Pour la réalisation des exercices RedTeam, Cogiceo a créé un implant déposable lors d'une intrusion physique permettant d'attaquer le réseau interne sans avoir à rester dans les locaux de la cible. Cet outil est également prévu pour contourner les protections Network Access Control (NAC) 802.1x. Des fonctionnalités offensives doivent être ajoutées à l'implant afin de pouvoir notamment attaquer du WiFi, récupérer des creds via l'authentification du NAC, implémenter des scénarios d'attaque sur le 802.1AE etc.

Objectifs

1. Comprendre les différents protocoles de contrôle d'accès réseau ;
2. Comprendre l'architecture de l'implant et son fonctionnement (problématique d'architecture MIPS, taille allouée au système, etc.) ;
3. Identifier et implémenter les attaques WiFi ;
4. Déployer de nouvelles fonctionnalités pour l'implant, y compris des fonctionnalités offensives ;
5. Tests des fonctionnalités en environnement réel ;

AMÉLIORATION DE L'ANALYSE ET CASSAGE DES HASH

Catégories : Cryptographie

Description

Afin de fournir un service efficace de cassage de mot de passe dans le cadre des pentests mais également des outils d'analyse, Cogiceo a développé une plateforme de cassage de mots de passe centralisée. L'objectif de ce sujet et d'analyser les méthodes existantes et les stratégies possibles de cassage afin d'améliorer les performances de l'outil.

Objectifs

1. Recherche de l'état de l'état de l'art sur le cassage de mot de passe et des différentes stratégies existantes ;
2. Compréhension de l'architecture et des stratégie de cassage mises en place chez Cogiceo ;
3. Développement de nouvelles stratégies de cassage ;
4. Benchmark des stratégies de cassages et analyses des performances ;

CRÉATION DE MÉTHODOLOGIE D'AUDIT DES CI/CD / DEVOPS

Catégories : DFIR, Red Team

Description

La mise en place d'un CI/CD est aujourd'hui commune chez nombre de nos clients. L'automatisation des taches de déploiement et de test du code rend cette architecture un asset particulièrement sensible et parfois même central dans l'entreprise. L'objectif est d'identifier les différents outils pouvant intervenir dans ce processus, les vulnérabilités pouvant les impacter ainsi que les défauts de configuration permettant de les compromettre.

Objectifs

1. Identification des outils pouvant composer un CI/CD (Kubernetes, Jenkins, AzureDevOps, Ansible, Puppet, Docker, etc. ;
2. Analyse des chemins de compromission via vulnérabilité ou défauts de configuration ;
3. Mise en place d'environnements de tests ;
4. Recensement et tests des outils et techniques de compromission ;
5. Rédaction de la méthodologie d'attaque dans les cogi-playbooks ;