Institut Universitaire de Technologie,
Aix-Marseille Université

RAPPORT DE STAGE de fin de deuxième année
Bachelor Universitaire de Technologie
Spécialité Réseaux et Télécommunications
parcours cybersécurité

Assistant Responsable de la sécurité des systèmes d'information

Jérémy FOURNIER

Université d'Aix-Marseille

Responsable entreprise : Julien Valiente

Responsable académique : NGUYEN Cong tin

2023

Table des matières

1. Introduction

J'ai effectué un stage au sein du service de la sécurité des systèmes d'information de la Direction du numérique de l'université d'Aix-Marseille . Pendant cette période, mon objectif principal était d'assister le responsable sécurité des systèmes d'information de l'université dans diverses missions liées à la cartographie du réseau et à l'analyse des mesures de sécurité en place.

Dans ce rapport, je vais commencer par présenter brièvement l' Université d'Aix-Marseille, en mettant l'accent sur son organisation interne. Par la suite, je détaillerai les missions qui m'ont été confiées, en mettant en évidence les objectifs que j'ai poursuivi tout au long de mon stage.

Ensuite, j'expliquerai l'environnement technique dans lequel j'ai évolué, en mettant l'accent sur le lien entre mes missions et le respect du Règlement général sur la protection des données (RGPD). En effet, l'université doit se conformer à cette réglementation en matière de protection des données, ce qui a eu un impact significatif sur mes activités.

Par la suite, je décrirai en détail les différents travaux que j'ai réalisé pendant mon stage, en mettant l'accent sur la cartographie du réseau et l'analyse des mesures de sécurité existantes. Je mettrai également en avant ma collaboration avec d'autres membres de la Direction du numérique, notamment l'équipe en charge du respect du RGPD pour les applications et services proposés par l'université.

En conclusion, je dresserai un bilan de mon expérience de stage, en analysant les réussites et les défis auxquels j'ai été confronté. Je mettrai également en évidence les compétences que j'ai pu acquérir et développer au cours de cette expérience.

2. Présentation de l'Université Aix-Marseille

2.1 L'université et ses composantes

Aix-Marseille Université (AMU), créée le 1er janvier 2012, est la fusion des trois universités de la région (Université de la méditerranée, Université de Provence et l' Université Paul Cezane). Fortement orientée vers la recherche, elle est en partenariat avec des organismes majeurs comme le CNRS, Inserm, IRD et CEA, et structure ses activités autour de cinq pôles de recherche interdisciplinaires (PR2I).

Elle est organisée autour de cinq secteurs disciplinaires et répartie sur 54 sites totalisant plus de 830 000 m², s'étendant sur quatre départements et neuf villes.

AMU possède une organisation interne très vaste et complexe avec de nombreux services communs, composantes, directions centrales, fondations et instituts. Chaque service et direction possède leur propre organisation et équipes.

AMU accueille près de 80 000 étudiants, dont 10 000 internationaux, et propose 1 100 diplômes. Elle comprend 12 écoles doctorales, 120 associations étudiantes, 8 000 personnels, 17 facultés et écoles, 18 instituts interdisciplinaires, et 5 grands campus. Elle abrite également 122 structures de recherche, dont 113 unités de recherche et 9 structures fédératives.

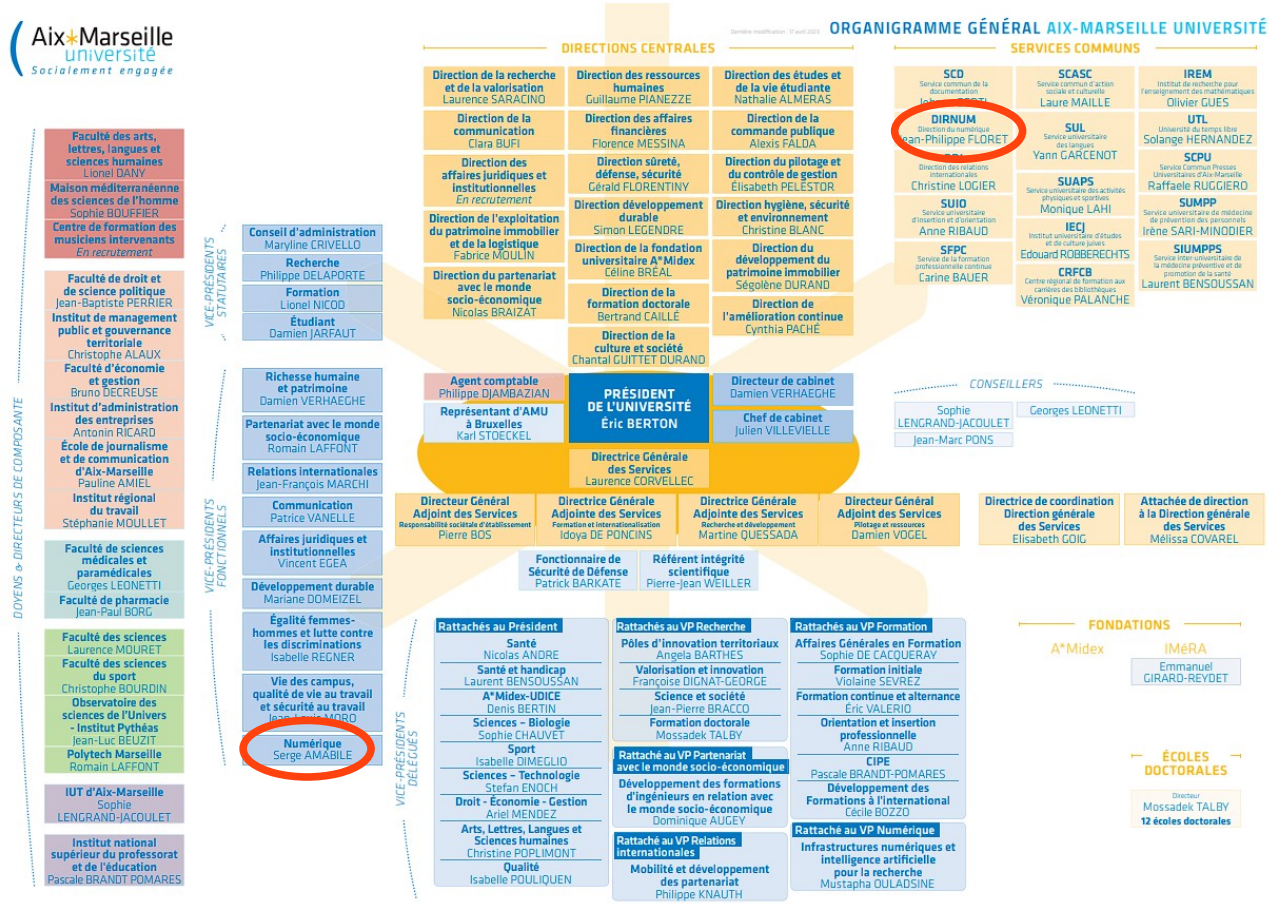


Figure 1 : Organigramme général d'AMU

2.2 Rôle du responsable de la sécurisation des systèmes d'informations

Le responsable de la Sécurité des Systèmes d'Information (RSSI) est un poste clé au sein d'une université, ayant pour responsabilité la supervision de tous les aspects de sécurité relatifs à l'informatique et à l'information en général. Son rôle s'étend à la garantie de la sécurité du Système d'Information (SI) de l'institution, laquelle repose sur quatre critères essentiels concernant les données : leur confidentialité, leur intégrité, leur disponibilité et leur traçabilité.

Le RSSI exerce une fonction de conseil, en participant à l'évaluation de nouveaux dossiers tels que les applications, les modes de stockage d'informations, l'utilisation du réseau et les problématiques liées à l'usage d'appareils personnels.

Outre ces responsabilités, le RSSI se charge de la formation et de la diffusion d'informations relatives à l'usage du SI. Son rôle inclut également la sensibilisation des utilisateurs quant aux aspects de sécurité. En outre, il guide l'élaboration de la Politique de Sécurité des Systèmes d'Information (PSSI) propre à l'établissement.

La sécurité du SI implique une chaîne d'acteurs en interaction ascendante et descendante, chargée du relais d'informations, de la veille technologique et juridique, ainsi que de l'émission d'alertes. Cette chaîne interagit fréquemment avec divers services de l'État, tels que l'UCLAT (unité de coordination de la luttre antiterrorisme) , le Procureur de la République, les services de police et de gendarmerie, ainsi que plusieurs CERT (Computer Emergency Response Team), qui jouent un rôle crucial dans la surveillance constante du réseau et du système.

Au sein d'AMU, les acteurs de la sécurité du SI incluent le Président, le FSD (fonctionnaire sécurité défense) , le RSSI, la DirNum et les correspondants SSI par structure. Cette chaîne de la SSI se compose de trois réseaux, notamment une chaîne fonctionnelle pour la transmission et la réception d'informations, une chaîne opérationnelle composée d'agents techniques pour la mise en œuvre active, et une chaîne d'alerte pour gérer les crises.

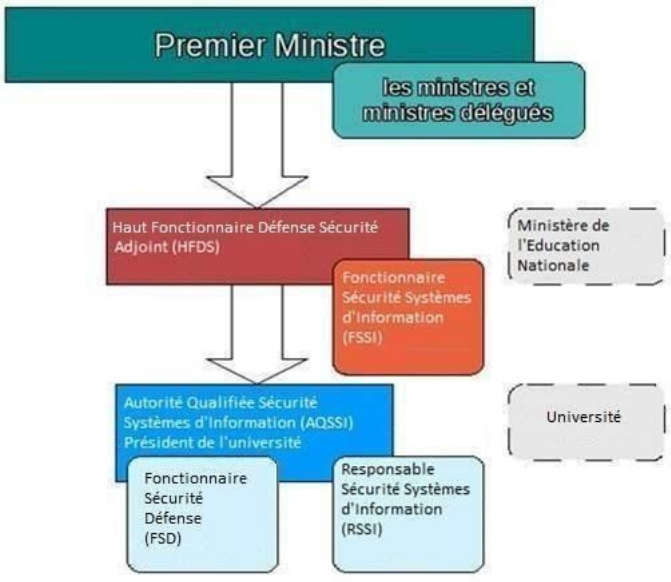


Figure 2 : Acteurs de la chaîne SSI

2.3 La Direction du Numérique

La Direction du Numérique (DirNum) de l'université d'Aix-Marseille est une entité organisée en différents pôles et équipes chargés de la gestion et du développement des services informatiques au sein de l'université. Au cours de mon stage, j'ai eu l'opportunité d'intégrer le pôle Sécurité des Systèmes d'Information (SSI) & Délégué à la Protection des Données (DPO), qui a été récemment créé et qui est externe à la DirNum mais qui travaille avec elle dans le but de garantir la sécurité des services existants et futurs, tout en respectant les obligations réglementaires de la législation générale sur la protection des données.

Ce pôle a pour mission principale d'assurer la protection des systèmes d'information de l'université et de veiller à la conformité de ses activités en matière de protection des données. Il travaille en étroite collaboration avec les autres départements de la DirNum ainsi qu'avec les différents acteurs de l'université pour mettre en place des mesures de sécurité efficaces et garantir la confidentialité, l'intégrité et la disponibilité des données.

En plus de sécuriser les services déjà déployés, le pôle SSI & DPO joue également un rôle clé dans la mise en œuvre de nouvelles solutions et services, en veillant à ce qu'ils respectent les normes et réglementations en matière de protection des données et de sécurité. Il contribue ainsi à renforcer la confiance des utilisateurs et à assurer une gestion rigoureuse des informations sensibles de l'université.

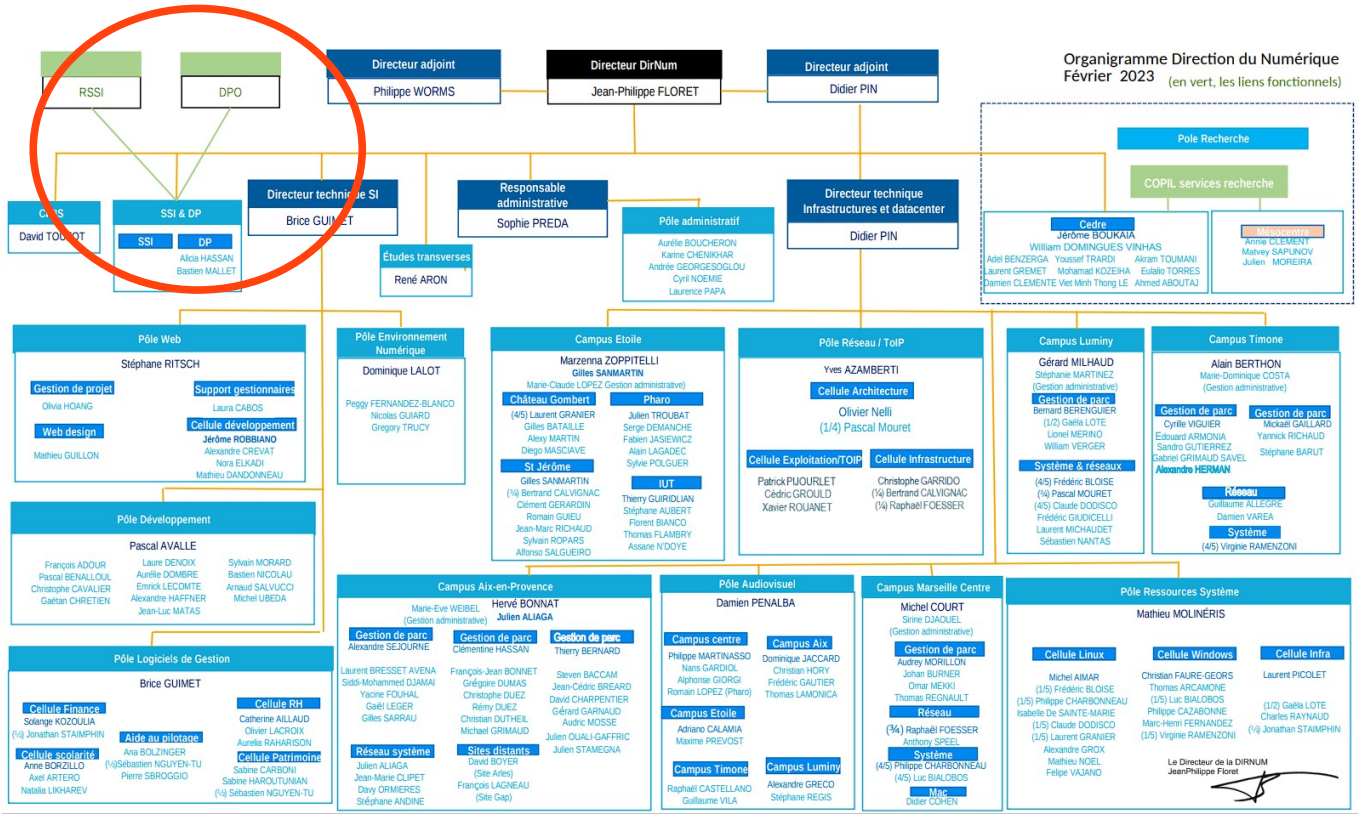


Figure 3 : Organigramme de la DirNum

3. Contextualisation

3.1 Missions et objectif du stage

L'objectif de mon stage était de mettre en pratique les compétences acquises lors de ma formation dans le domaine de la cybersécurité, tout en développant de nouvelles connaissances. J'ai été chargé de nombreuses missions qui seront détaillées ultérieurement. Voici une description générale de ces missions :

- Sécurisation et enquêtes sur les postes : Recherche des bonnes pratiques de sécurité pour les postes Windows utilisés par le personnel de l'université. J'ai vérifié la mise en place de ces bonnes pratiques et j'ai également été initié à la discipline du forensic.

- Cartographie du réseau : Phase de reconnaissance active et passive sur le réseau de l'université en se mettant dans la peau d'un attaquant ayant un accès au réseau depuis l'intérieur, afin de découvrir ce qu'il pourrait voir et observer.

- Schématisation des services à risques : J'ai eu l'opportunité de rencontrer les responsables des différents services pour obtenir des informations sur le fonctionnement des applications, les mesures de sécurité mises en place et les potentielles failles à corriger.

- Extraction automatique des fiches registres en lien avec le RGPD: Développement d'un programme python afin d'automatiser l'extraction des réponses des enquêtes réalisées via Limesurvey vers une fiche registre Excel à remplir.

- Application de la méthodologie de sécurisation des services et analyse des dangers : Recherches et application des méthodologies d'analyse des risques et les concepts de tests d'intrusion appliqués aux applications en production dans le but de sécuriser les services et évaluer les vulnérabilités potentielles.

3.2 Environnement et organisation

La Direction du Numérique (DirNum) possédant une structure vaste et composée de différents pôles, nous avons dû organiser des réunions pour nous présenter aux autres membres et commencer à planifier la collaboration en sollicitant leur aide et des informations confidentielles concernant le fonctionnement de l'université d'Aix-Marseille (AMU).

L'environnement de l'université est réputé pour être fermé et contrôlé, avec peu de documentation publique et de partage d'informations entre les différents pôles. Étant donné que nos missions visaient à sécuriser AMU de manière globale, ces informations étaient indispensables pour avancer rapidement.

Ainsi, une réunion a été organisée au Datacenter de Saint-Jérôme, permettant de mettre en place les relations futures entre le Pôle Réseau et le Pôle Sécurité des Systèmes d'Information & Délégué à la Protection des Données (SSI&DPO).

Lors de cette réunion, une présentation générale du fonctionnement du réseau, de la répartition des charges entre les différents secteurs et campus a été faite. Cela a permis d'établir des liens étroits et de favoriser la collaboration entre les équipes.

En ce qui concerne les locaux, j'étais situé sur le site du Pharo, dans le bâtiment B, où se trouvent les espaces de travail en open-space de la DirNum, récemment rénovés. Ces locaux offraient un cadre calme et propice au travail, favorisant ainsi l'organisation de réunions efficaces.

En ce qui concerne mon emploi du temps, j'étais basé sur le campus d'Aix-en-Provence le lundi, dans les locaux du LID2MS (Laboratoire Interdisciplinaire de Droit, Médias et Mutations Sociales), où l'équipe Délégué à la Protection des Données (DPO) discutait de nos missions et problématiques afin d'intégrer au mieux notre collaboration au sein de la DirNum.

Le reste de la semaine se déroulait au Pharo où chaque mardi, nous avions une réunion de bilan du côté SSI avec mon maître de stage, Julien Valiente, pour avancer et communiquer sur les missions en cours. Les jeudi et vendredi étaient réservés au télétravail, permettant une flexibilité dans l'organisation de mes tâches.

3.3 Équipe Déléguée à la Protection des Données & RGPD

Avant le début de mon stage, j'ai suivi une formation sur le Règlement général sur la protection des données (RGPD) à travers des ateliers proposés sur le site de la Commission nationale de l'informatique et des libertés (CNIL). Cette formation m'a permis de me familiariser avec les concepts liés à cette réglementation, qui n'avaient pas été abordés lors de ma formation initiale.

Le RGPD est une loi qui vise à garantir que la collecte et le traitement des données personnelles se fassent dans le respect des droits des utilisateurs. Il impose que les données soient sécurisées, minimisées, pseudonymisées, anonymisées, et que le traitement final soit légitime.

Étant donné que l'université d'Aix-Marseille compte plus de 300 applications en production utilisées par plus de 80 000 étudiants et 8 000 membres du personnel, nous sommes responsables d'une quantité importante de données personnelles, et il est donc crucial de s'assurer que tout est conforme aux normes en vigueur.

L'équipe Délégué à la Protection des Données (DPO), avec laquelle j'ai collaboré pendant mon stage, a pour mission de mettre en place un questionnaire relatif aux informations requises par le RGPD, afin de créer une fiche registre résumant et permettant un accès direct à ces informations.

Cette mission est complexe, car elle nécessite la création d'un formulaire précis, tout en restant accessible aux responsables concernés, sans utiliser un langage trop juridique. De plus, il est également nécessaire de mettre en place un système d'extraction automatique des informations collectées, afin de les rendre lisibles et modifiables à tout moment. Ainsi, si la CNIL procède à un contrôle pour vérifier la conformité des applications, nous serons en mesure de leur fournir les réponses nécessaires.

La mise en place de ces mesures conformes au RGPD est essentielle pour garantir la protection des données personnelles au sein de l'université et démontrer notre engagement envers le respect de la vie privée des utilisateurs.

4. Travaux réalisés

4.1 Sécurisation et enquêtes des postes AMU

Ma première mission, une fois que j'ai reçu mon PC portable de l'université d'Aix-Marseille (AMU), a été d'analyser les mesures de sécurité en place et de vérifier qu'aucune mauvaise configuration n'était présente afin de s'assurer de la sécurité des postes déployés sur le réseau. J'ai réalisé un travail approfondi d'analyse et de recherche pour comprendre comment sécuriser un poste Windows, en utilisant notamment les guides fournis par la **CNIL** et l'**ANSSI**, ainsi qu'en vérifiant les paramètres de configuration Windows afin de combler d'éventuelles failles.

Voici les critères de sécurité que j'ai étudiés :

- Anti-virus : Quelle solution est utilisée ? Est-elle la plus optimale pour assurer une protection efficace ?

- Pare-feu : Quelles sont les règles de filtrage en fonction des contextes ? Le PC est-il protégé contre les scans externes ?

- Politique de mise à jour des applications et du système : Comment sont gérées les mises à jour ? Sont-elles automatisées ? Si oui, de quelle manière ? Est-ce de manière centralisée sur les postes AMU ?

- Chiffrement du stockage : Le disque dur est-il chiffré ? Quel est le moyen utilisé pour cela ? Comment fonctionne concrètement le processus ?

- Sauvegarde des données : Quelles solutions de sauvegarde sont mises en place et sont-elles obligatoires ?

- Protection des ports : L'autorun est-il activé lors de l'insertion d'une clé USB ?

- Outils d'administration à distance : Par quels moyens un administrateur peut-il se connecter à distance sur le PC d'un personnel pour effectuer des dépannages ? Si oui cela se fait-il par des canaux sécurisés ?

- Gestion des droits d'exécution : Le compte utilisateur est-il réellement limité au strict minimum ? Est-il correctement cloisonné et peut-il exécuter n'importe quel programme ?

- Accès limité au BIOS : L'utilisateur peut-il accéder aux paramètres du BIOS et ainsi modifier certains paramètres de sécurité ?

Suite à l'établissement de ces critères, j'ai mené une série de recherches comparatives par rapport à l'état actuel du système. Pour des questions de confidentialité, je ne peux pas dévoiler les informations collectées, mais j'ai pu faire un état des lieux concernant l'état actuel de ces mesures et en discuter avec mon maître de stage mais aussi certains responsables réseau de AMU afin de bien comprendre et d'assimiler les politiques mise en place.

La dernière étape de cette analyse consistait à vérifier la conformité des configurations actuelles de Windows avec le **Guide Technique d'Implémentation de Sécurité pour Windows 10 (STIG)**. Ce

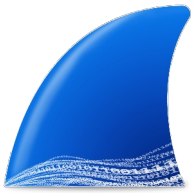
guide répertorie les erreurs les plus communes et les plus graves relatives aux configurations de Windows 10.

Il a été constaté que plus de sept failles majeures étaient présentes. Certaines d'entre elles étaient justifiables, étant le résultat de décisions délibérées et de contrôles spécifiques, tandis que d'autres semblaient être le fruit de simples oublis. L'ensemble de ces informations a été compilé et remonté aux responsables.

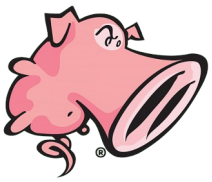
De plus, j'ai procédé à une analyse comportementale des postes afin de détecter d'éventuelles connexions suspectes, notamment celles vers des serveurs externes à l'université. Pour y parvenir, j'ai étudié les connexions TCP/UDP établies et, en associant le numéro d'identification de processus (PID) au service concerné, j'ai été en mesure d'identifier des connexions potentiellement problématiques.

Dans le cadre de cette analyse, j'ai utilisé des outils de surveillance et d'analyse réseau tel que **WireShark**. J'ai donc mis en marche mon poste pendant plusieurs heures, capturant chaque paquet de données entrant et sortant. J'ai ensuite analysé manuellement ces données et les ai sauvegardées sous forme de fichiers de capture PCAP. Cela m'a permis de procéder à une analyse détaillée et d'associer les informations observées, pour cela, j'ai notamment utilisé le logiciel **Network Miner** qui permet de bien visualiser les échanges et les hôtes à partir d'un enregistrement des trafics réseau.

Enfin, je me suis familiarisé avec le concept d'IDS/IPS (Intrusion Detection System/Intrusion Prevention System), qui est un élément clé dans le domaine de la défense en cybersécurité. Pour ce faire, j'ai utilisé l'outil open-source **Snort**. Cette expérience pratique m'a permis d'acquérir une compréhension approfondie du fonctionnement d'un système de détection et de prévention d'intrusions. L'utilisation de Snort m'a aidé à identifier et à comprendre comment ces systèmes peuvent surveiller efficacement le trafic réseau, détecter les activités suspectes.



Wireshark



Snort

Network Miner

L'analyse des connexions m'a permis de mieux comprendre le rôle essentiel que jouent les systèmes IDS/IPS. Ces outils, souvent utilisés en complément des pare-feu, sont cruciaux pour la détection des intrusions. En outre, cela m'a éclairé sur le concept d'un Centre Opérationnel de Sécurité (SOC), qui est la première ligne de défense en cybersécurité.

Une fois cette phase d'analyse terminée, j'ai pu passer à l'étape suivante, qui consistait à examiner les supports de stockage des ordinateurs d'AMU afin de vérifier s'il restait des informations compromettantes, même après une réinitialisation du support de stockage.

Pour cela, j'ai dû me familiariser avec la discipline du forensic qui consiste à extraire, analyser et interpréter des données sur des supports de stockage. J'ai donc acquis une compréhension approfondie du fonctionnement et des principes fondamentaux comme :
- **L'analyse logique,** avec examinant les fichiers, répertoires
- **La recherche de signatures spécifiques**
- **L'analyse d'artefacts** notamment dans les fichiers de journalisation du système, fichiers temporaires, caches etc.

Pour m'aider dans cette tache j'ai utilisé des outils spécialisés dans le domaine de l'analyse forensic, tels que :

Autopsy

Recuva

PhotoRec

Ces différents outils m'ont permis d'automatiser l'extraction et l'analyse d'artefacts ou données sensibles notamment **Autopsy** qui possède un certain nombre de modules qu'on peut ajouter pour rajouter de la précision dans l'interprétation des résultats et aussi de générer des rapports d'analyse de façon automatique.

À partir des résultats obtenus, j'ai pu établir un rapport indiquant si les ordinateurs laissaient des traces préoccupantes même après une réinitialisation complète.

Cette analyse des supports de stockage des postes de AMU était essentielle pour s'assurer que les données sensibles et potentiellement compromettantes étaient correctement effacées. Elle contribue à renforcer la confidentialité et la sécurité des informations, tout en garantissant le respect des exigences de protection des données et de la vie privée.

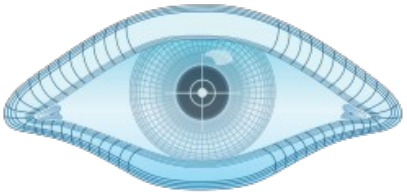
4.2 Cartographie réseau

Ma deuxième mission, après avoir sécurisé un poste, était de remonter dans le réseau afin de simuler une attaque et d'adopter le point de vue d'un véritable attaquant qui aurait un accès sur le réseau de l'université.

Pour cela, j'ai développé une méthodologie d'attaque : J'ai commencé par dresser une liste des plages d'adresses IP en utilisant les informations de configuration IP des postes d'AMU sur différents sites tels que le Pharo et le site d'Aix en Provence, afin d'observer les éventuelles différences.

J'ai ensuite identifié ma passerelle, mon masque de sous réseau, mes serveurs DNS et DHCP, puis j'ai effectué des scans avec l'option de traçage des routes (trace-route) pour suivre le chemin emprunté par les paquets pour transiter sur le réseau privé mais aussi à destination de l'extérieur afin de bien déterminer les routeurs en bord de zone et quadriller le réseau.

Pour réaliser ces opérations, j'ai utilisé des outils tels que :



Nmap

Masscan

J'ai principalement utilisé **Nmap** lors de mes scans et sa version graphique **Zenmap** qui offre une visualisation des scans, ce qui m'a été très pratique lors des premières réunions afin d'avoir une idée de la taille du réseau qui contenait plus de 3 000 hôtes actifs.

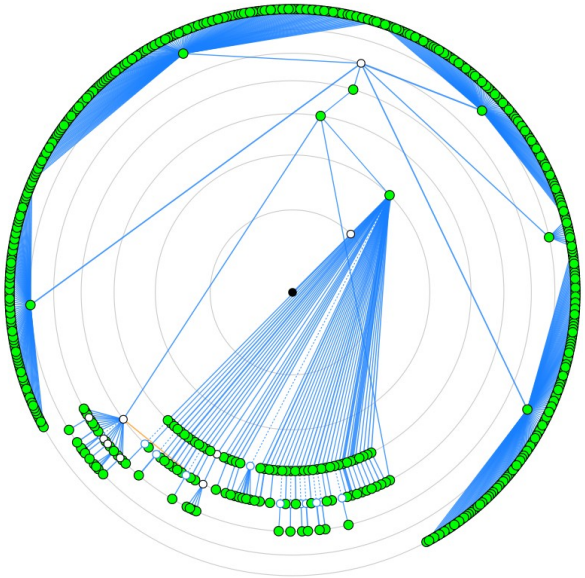


Figure 4 : Scan sur différents réseaux de AMU

Avec Nmap, j'ai procédé de manière progressive en identifiant les hôtes actifs à l'aide de requêtes ICMP ou ARP, permettant ainsi de contourner plus facilement les pare-feu. Une fois les noms d'hôtes et leurs adresses IP recueillis, j'ai effectué des scans de versions et de vulnérabilités sur chaque serveur. À la fin de cette phase, j'ai pu créer un tableau Excel regroupant toutes les informations accessibles à partir d'un ordinateur AMU connecté au réseau comme : les noms de domaine, les adresses IP, les ports ouverts, les services et leurs versions et le résultat des détections de failles potentielles

J'ai complété les informations obtenues en tant qu'attaquant avec la base de données des serveurs enregistrés dans **SIAMU**, l'application qui répertorie les serveurs avec leurs adresses IP et leurs noms ainsi que d'autres informations comme les noms des responsables techniques et fonctionnels des serveurs et applications. Cela m'a permis d'obtenir une cartographie plus précise des serveurs actifs et des informations que nous avons pu recueillir à leur sujet.

En complément de la reconnaissance active, j'ai également réalisé une phase de reconnaissance passive pour analyser les résultats obtenus depuis l'extérieur du réseau. Pour cela, j'ai dû me former et découvrir les différentes méthodes permettant de mener cette reconnaissance.

J'ai notamment utilisé des moteurs de recherche spécialisés tels que **Censys** et **Shodan** qui sont des moteurs de recherches qui permettent de trouver des informations sur les dispositifs connectés à Internet, tels que les serveurs, les routeurs, les caméras IP, etc. Il fournit des données précieuses pour évaluer la surface d'attaque potentielle.

Ces moteurs de recherche spécialisés m'ont permis d'obtenir des informations supplémentaires sur les dispositifs connectés et d'élargir ma compréhension de la surface d'attaque potentielle. Cela m'a également aidé à évaluer la visibilité des services et des configurations accessibles depuis l'extérieur du réseau, ce qui est essentiel pour renforcer la sécurité et prévenir les éventuelles vulnérabilités.

Cette étape de reconnaissance, à la fois passive et active, m'a permis d'identifier les actifs du réseau, de repérer d'éventuelles vulnérabilités et de mieux comprendre l'infrastructure de l'université. Ces informations ont été essentielles pour la suite de notre mission de sécurisation et pour renforcer la résilience du réseau face aux potentielles attaques.

4.3 Schématisation logique des services sensibles

Ma troisième mission consistait à réaliser une cartographie fonctionnelle des applications à risque au sein d'AMU. Nous avons commencé par analyser les risques et les dépendances des applications, en identifiant celles qui étaient les plus à risques et critiques sur le plan fonctionnel et celles qui manipulaient le plus d'informations personnelles.

Une fois cette liste établie, j'ai pris des rendez-vous avec les responsables techniques et fonctionnels de chaque application afin de leur poser de nombreuses questions pour comprendre le fonctionnement général de l'application. J'ai cherché à savoir avec quels serveurs elles communiquaient, comment les informations étaient transmises et sauvegardées.

A partir de la norme internationale **ISO/CEI 27002** qui est le code de bonne pratique pour le management de la sécurité de l'information et de la méthodologie **EBIOS Risk Manager** qui a pour but d'identifier, analyser et savoir comment traiter les risques de sécurité, j'ai créé un questionnaire comprenant une quarantaine de questions pour obtenir une vue d'ensemble des communications, des serveurs et des mesures de sécurité logicielles, réseaux et physiques.

Cette tâche a été longue et a demandé beaucoup de temps, car j'ai dû contacter les responsables individuellement, organiser les rendez-vous en fonction de leurs disponibilités et mener les réunions de manière à ne laisser aucune information essentielle de côté.

J'ai dû également préparer une fiche de bord en collaboration avec l'équipe RGPD afin de bien mener les entretiens et ne bien mettre en avant l'objectif des réunions et les étapes clefs à ne pas manquer si on veut obtenir le plus d'informations utiles.

Une fois toutes les informations recueillies, j'ai commencé à créer une cartographie logique des applications et des mesures de sécurité qui y étaient liées. L'objectif de cette cartographie était de vérifier, en cas de doute, quelles mesures de sécurité étaient réellement mises en place et de réaliser des audits par la suite pour identifier d'éventuelles failles ou vulnérabilités. Les résultats de ces audits seraient ensuite remontés afin de prendre les mesures nécessaires pour renforcer la sécurité des applications et des données qu'elles manipulent.

Cette mission a été à la fois complexe et enrichissante, me permettant de développer une nouvelle compétence : la communication et l'adaptation en fonction des interlocuteurs. En effet, j'ai eu l'occasion d'interagir avec des experts en programmation qui n'étaient pas nécessairement spécialistes en architecture réseau. J'ai dû ainsi ajuster mes questions et mon approche en fonction de leurs compétences et connaissances spécifiques.

4.4 Extraction automatique et ajustements des fiches registres

Ma quatrième mission consistait à créer un programme en Python pour aider l'équipe **DPO** (Délégué à la Protection des Données) dans l'extraction des réponses d'un questionnaire **LimeSurvey** utilisé par les responsables des applications pour remplir les informations légales relatives au respect des mesures de traitement conformément au **RGPD**.

Le fonctionnement de la fiche registre est simple :

1) Les responsables des applications se rendent sur le questionnaire en ligne LimeSurvey mis en place par l'équipe DPO.

2) On extrait les réponses du questionnaire au format XLS qui est illisible ou du moins pas très visuel (Figure 4).

3) Un programme prend en entrée les réponses du questionnaire au format XLS, il extrait les réponses et les trie de façon logique selon des critères spécifiques et injecte ces réponses dans une fiche registre pré-formatée elle aussi au format XLS.

L'objectif est d'avoir une fiche bien structurée, plus lisible et modifiable en cas de modifications futures comme ci-dessous (Figure 5) :

	A	B	C	D	E	F	G	H
1	id	submitdate	lastpage	startlanguage	seed	startdate	datestamp	Q1a
2	13	2023-06-13 1	4	fr	544562405	2023-06-13 1	2023-06-13 1	Un serv

Figure 5 : Réponses au questionnaire LimeSurvey

FICHE REGISTRE DES ACTIVITES DE TRAITEMENT		Nommer la fiche de cette mani
Description du traitement		
Date de création de la fiche registre	submitdate	
Date de mise en oeuvre du traitement	startdate	
Date de dernière mise à jour de la fiche registre	datestamp	
Nom du rédacteur de la fiche	Q1f[SQ001]	
Prénom du rédacteur de la fiche	Q1f[SQ002]	
Coordonnées du responsable du traitement (RT)		
Nom du responsable du traitement	Aix-Marseille Université (AMU)	
Adresse	Site du Pharo - 58 Boulevard Charles Livon	
Code Postal	13284	
Ville	Marseille Cedex 07	
Numéro de téléphone	0491396501	
Courriel		
Nom et coordonnées du Délégué à la Protection des Données		
Prénom et Nom	Hervé ISAR	
Adresse	Site du Pharo - 58 Boulevard Charles Livon	
Code Postal	13284	
Ville	Marseille Cedex 07	
Numéro de téléphone	0491396501	
Courriel	dpo@univ-amu.fr	
Nom et coordonnées de la structure en charge de l'activité de traitement		
Nom de la structure en charge du traitement		REP1
Nom du responsable de la structure en charge de l'activité de traitement		REP2
Prénom du responsable de la structure en charge de l'activité de traitement		REP3
Nom de la personne chargée de la mise en œuvre opérationnelle du traitement		REP4
Prénom de la personne chargée de la mise en oeuvre opérationnelle du traitement		REP5
Fonction de la personne chargée de la mise en oeuvre opérationnelle du traitement		REP6
Autres structures interne à AMU		Nom de la str
Structure 1		Q1e[SQ00
Structure 2		Q1e[SQ00
Structure 3		Q1e[SQ00
Structure 4		Q1e[SQ00
Structure 5		Q1e[SQ00

Figure 6 : Fiche registre pré-formatée

Pour résoudre ce problème, j'ai utilisé mes compétences en Python pour automatiser cette tâche et ainsi faciliter la conformité au RGPD au sein de AMU. J'ai utilisé des modules Python spécialisés dans le traitement des fichiers XLS, tels que **Pandas** et **Openpyxl**.

J'ai tenu de nombreuses réunions avec un ou plusieurs membres de l'équipe DPO pour clarifier les fonctionnalités et spécificités dont ils avaient besoin, telles que :

- La création automatique d'une arborescence de répertoires afin de trier les fiches registres.

- Le nommage des fichiers en fonction des réponses du questionnaire avec la date, le service écrit d'une façon spécifique et du rangement automatique dans les répertoires de l'arborescence.

Le développement de ce programme a pris plus de temps que prévu car certaines cases de la fiche registre pouvaient prendre la réponse de plein de questions différentes en fonction des réponses précédentes. J'ai dû donc creuser et bien comprendre le fonctionnement logique du formulaire, quelles questions dépendent de celles d'avant etc …

Cette tâche fut la plus complexe non pas par la difficulté à coder, mais à maintenir à jour mon programme afin de s'assurer qu'il puisse continuer de fonctionner malgré les modifications du formulaire et de la fiche registre qui a énormément changé entre le début et la fin.

En plus du développement du programme, j'ai également participé à la correction et à l'ajustement de certaines questions dans le questionnaire LimeSurvey, afin de respecter les exigences légales tout en rendant le questionnaire compréhensible pour les responsables et en évitant un jargon juridique trop complexe.

Grâce à ce programme Python, l'équipe DPO a pu automatiser le processus d'extraction des réponses du questionnaire LimeSurvey vers la fiche registre, ce qui a permis d'améliorer l'efficacité et l'exactitude de la collecte des informations liées à la conformité RGPD.

5. Retour d’expérience

5.1 Analyse des réussites et défis rencontrés

Lors de ce stage, j'ai été confronté à différents défis et j'ai réussi à les relever avec succès. La sécurisation des postes Windows a été une réussite, me permettant de mettre en pratique les connaissances acquises lors de ma formation et de renforcer les mesures de sécurité pour les utilisateurs d'AMU.

La phase de reconnaissance du réseau a également été un succès, me permettant d'explorer les infrastructures réseau, d'identifier les hôtes actifs et de comprendre les vulnérabilités potentielles. Cela m'a permis de développer mes compétences en matière de reconnaissance active et passive, ainsi que ma compréhension des principes fondamentaux de la sécurité des réseaux.

La cartographie des applications à risques a été un autre accomplissement. En travaillant en étroite collaboration avec les responsables techniques et fonctionnels, j'ai pu collecter des informations précieuses sur le fonctionnement des applications et les mesures de sécurité mises en place. Cela m'a permis de développer mes compétences en matière d'analyse des risques et de comprendre l'importance de prendre en compte les aspects fonctionnels et les données personnelles dans l'évaluation de la sécurité des applications.

La création d'un programme Python pour automatiser l'extraction des réponses du questionnaire LimeSurvey a été une autre réussite. J'ai pu développer un outil efficace qui a simplifié le processus pour l'équipe DP et a contribué à améliorer la conformité RGPD au sein d'AMU.

Cependant, j'ai également été confronté à des défis tout au long du stage. La gestion des rendez-vous avec les responsables techniques et fonctionnels a été un défi logistique, nécessitant une bonne planification et une coordination efficace. Cependant, grâce à une communication claire et à une organisation rigoureuse, j'ai réussi à surmonter ces obstacles et à obtenir toutes les informations nécessaires.

En résumé, ce stage m'a permis de relever différents défis et de connaître des réussites dans chaque mission. J'ai pu développer mes compétences techniques en cybersécurité, renforcer ma compréhension des enjeux de protection des données et acquérir une expérience précieuse en travaillant avec une équipe dynamique et motivée.

5.2 Compétences acquises et développées durant le stage

Ce stage m'a offert l'opportunité d'acquérir et de développer plusieurs compétences clés dans le domaine de la cybersécurité. Parmi les compétences acquises :

- La sécurisation des postes Windows : J'ai développé des compétences pratiques en matière de configuration et de gestion de la sécurité sur les postes de travail, en suivant les bonnes pratiques recommandées par les organismes de référence tels que la CNIL et l'ANSSI.

- La reconnaissance des réseaux: J'ai appris à utiliser des outils de reconnaissance active et passive, tels que Nmap, Zenmap et Masscan, pour cartographier les infrastructures réseau, identifier les hôtes actifs et évaluer les vulnérabilités potentielles.

- L'analyse des risques : J'ai développé des compétences en matière d'analyse des risques liés aux applications, en identifiant les dépendances, en évaluant les risques fonctionnels et en comprenant l'importance de prendre en compte les données personnelles dans l'évaluation de la sécurité.

- La programmation en Python : J'ai utilisé mes compétences en Python pour automatiser des tâches dans un environnement en évolution et où de nombreuses modifications ont été apportées.

- La gestion de projet : J'ai appris à planifier et à organiser les rendez-vous avec les responsables techniques et fonctionnels, à coordonner les échanges d'informations et à respecter les délais.

- Le forensic : J'ai eu l'occasion de me former et de mettre en pratique les techniques de forensic, notamment dans l'analyse des supports de stockage des ordinateurs d'AMU. J'ai utilisé des outils spécialisés tels que Autopsy, Recuva et PhotoRec pour examiner les traces numériques et identifier les informations compromettantes. Cette expérience m'a permis de comprendre les principes fondamentaux du forensic et d'acquérir des compétences pratiques dans l'analyse des supports de stockage.

- Réglementations informatiques : J'ai acquis une solide compréhension des réglementations informatiques clés, notamment les normes ISO, la directive NIS et le RGPD. J'ai appris à appliquer les principes de protection des données et à évaluer les risques liés à la confidentialité et à la sécurité des informations. Cette expérience m'a permis de développer des compétences pratiques en matière de conformité et de renforcer ma compréhension des enjeux liés à la sécurité de l'information.

- **L'adaptabilité et flexibilité**: En travaillant aux côtés de professionnels spécialisés dans divers domaines, j'ai dû m'adapter en fonction des compétences de chaque individu, qu'ils soient orientés vers la programmation ou l'infrastructure. J'ai acquis la capacité de synthétiser de manière claire et concise les objectifs de chacun et les moyens pour les atteindre. Cette flexibilité m'a permis de collaborer efficacement avec une équipe multidisciplinaire et de maximiser la productivité tout en favorisant une compréhension mutuelle des enjeux et des ressources disponibles.

J'ai acquis une expérience pratique qui complète mes connaissances théoriques et me permet d'être mieux préparé pour ma future carrière professionnelle.

6. Remerciements

Je souhaite exprimer ma sincère gratitude envers les membres de la Direction du numérique (DirNum) avec qui j'ai eu la chance de collaborer tout au long de mon stage. Leur bienveillance, expertise et leurs contributions ont enrichi mon expérience et m'ont permis d'acquérir de nouvelles compétences et connaissances.

Je tiens également à remercier mon maître de stage pour son suivi attentif et l'aide précieuse qu'il m'a apporté tout au long de mon parcours. Ses conseils et son expertise ont été d'une importance capitale dans la résolution des problématiques auxquelles j'ai été confronté.

Enfin, je voudrais adresser mes remerciements à l'université d'Aix-Marseille pour m'avoir offert cette opportunité de stage enrichissante et pour avoir créé un environnement propice à l'apprentissage et à la collaboration.

7. Glossaire

BUT, Bachelor Universitaire de Technologie

AMU, Aix-Marseille Université

DIRNUM, Direction du Numérique

SSI, Sécurité des systèmes d'information

RSSI, Responsable de la sécurité des systèmes d'information

RGPD, Règlement général sur la protection des données

DPO, Délégué à la protection des données

CNIL, Commission nationale de l'informatique et des libertés

ANSSI, Agence nationale de la sécurité des systèmes d'information

SOC, Security operations center

CNRS, Centre national de la recherche scientifique

IRD, Institut de recherche pour le développement

CEA, Commissariat à l'énergie atomique

ISO, Organisation internationale de normalisation

NIS, Network and Information Security

EBIOS RM, Expression des besoins et identification des objectifs de sécurité risk manager

LID2MS, Laboratoire Interdisciplinaire de Droit, Médias et Mutations Sociales

8. Annexes

8.1 Chronologie des taches effectuées

Semaine 1-3 :

- Découverte des locaux et des équipes de la DirNum

- Première réunion avec l'équipe DPO en charge de la RGPD pour nous présenter et mettre en avant nos objectifs communs

- Visite du data center de Saint-Jérome et réunion avec le pôle réseau afin de présenter l'équipe SSI&DPO et les futures collaborations

- Sécurisation et analyse des mesures de sécurités sur les postes AMU

- Initiation au forensic et à l'analyse des supports de stockage des postes AMU

Semaine 4-6 :

- Analyse comportementale des activités réseaux des postes AMU

- Reconnaissance active et passive du réseau

- Découverte des méthodologies d'analyse de risques

Semaine 7-10 :

- Rendez-vous avec les responsables techniques et fonctionnels des applications sensibles

- Création du programme d'extraction pour les fiches registres