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

STAGE ASSISTANT RSSI

Enzo Collot

Aix-Marseille Université

Responsable entreprise : Julien Valiente

Responsable académique : Tin Nguyen

2023

Table des matières

1 Introduction

Dans le cadre de mon stage de fin d'année, j'ai été amené à passer dix semaines au sein de la cellule SSI-RGPD d'AMU, Aix-Marseille Université aux côtés de Julien Valiente et Hervé Isar qui sont à la tête de cette cellule, ainsi que Jérémy Fournier, Bastien Mallet, Alicia Hassan et Yann Simoni également stagiaires et alternants dans cette même section.

L'objectif de ce stage, était de porter assistance au RSSI, Responsable de la Sécurité des Système d'Information dans ses missions pour ce faire, diverses tâches m'ont été attribué à savoir aider l'équipe RGPD, Réglementation Général de la Protection des Données et faire ce qui nous était donné par Mr Valiente au fil des semaines.

Dans la suite de ce rapport, je commencerai par présenter le service dans sa globalité, poursuivrai en détaillant l'ensemble de mon travail ainsi qu'une brève explication des outils utilisés et je finirai par une conclusion récapitulant l'ensemble du rapport et mon ressenti sur ce stage.

2 Présentation de l'entreprise

2.1 La cellule SSI-RGPD

La Dirnum, Direction du Numérique précédemment DOSI est le service d'AMU, Université d'Aix-Marseille permettant la mise en œuvre de la politique de sécurité de l'établissement concernant les systèmes d'information qui fournit aux étudiants ainsi qu'au personnel un service informatique opérationnel, constant et sécurisé.

Le service est structuré en différents pôles, le pôle réseau, le pôle système, infrastructures et de nombreux autre comme on peut le voir sur le document ci-dessous, dont celui où j'ai été affecté qui contient la cellule SSI-RGPD.

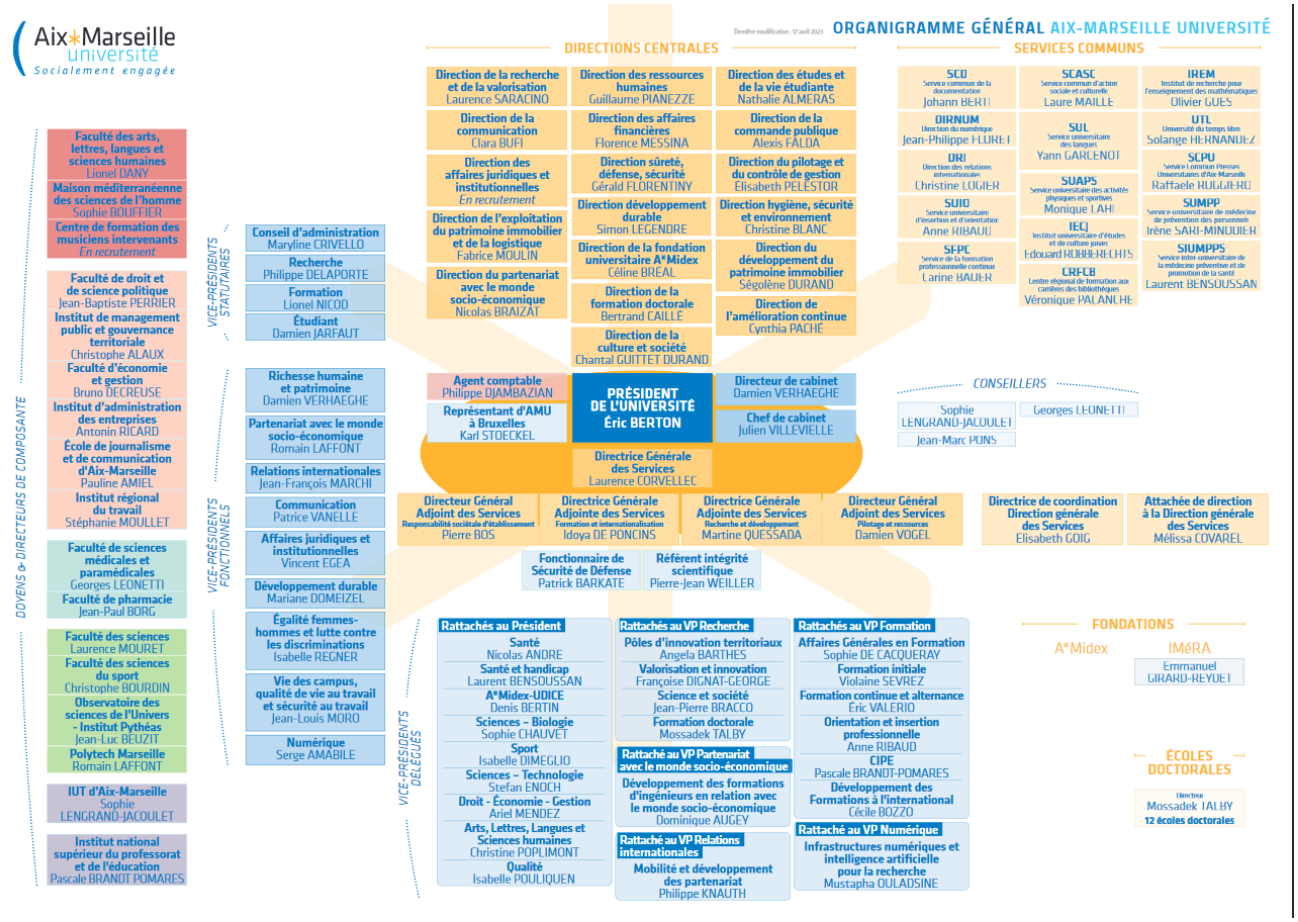

Figure 1 : Organigramme Amu

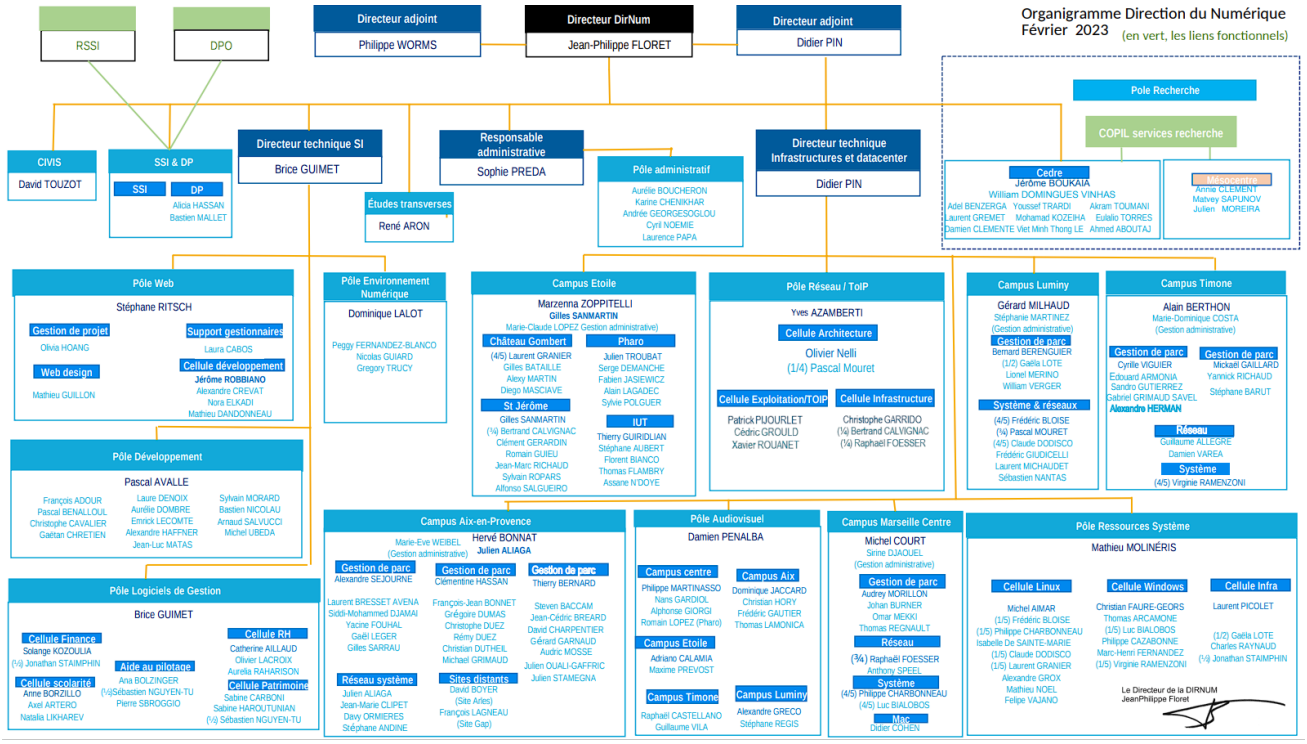

Figure 2 : Organigramme Dirnum

Comme on peut le voir sur cet organigramme, la cellule à laquelle j'ai été affecté est sous la direction de Julien Valiente le RSSI et Hervé Isar le DPO, le délégué à la protection des données.

Cette cellule a pour objectif, de s'assurer de la conformité de la protection des données personnelles et des systèmes d'information au sein d'AMU pour éviter de se faire saisir par un organisme créé pour s'en assurer tel que la CNIL, Commission nationale de l'informatique et des libertés.

Au terme organisationnel, cette cellule est assez spéciale, car même si elle est représentée sous le DSI, Directeur des Système d'Information au terme fonctionnel, elle est directement rattachée au président comme le RSSI.

2.2 Localisation

AMU dispose de plusieurs sites où différentes équipes travaillent, mais aussi de labos, cependant, n'étant pas allé sur chacun des sites, je vais parler uniquement de ceux sur lesquels j'ai pu travailler, à savoir celui du Jardin du Pharo, 58 Boulevard Charles Livon, 13007 Marseille pour travailler sur le côté SSI.

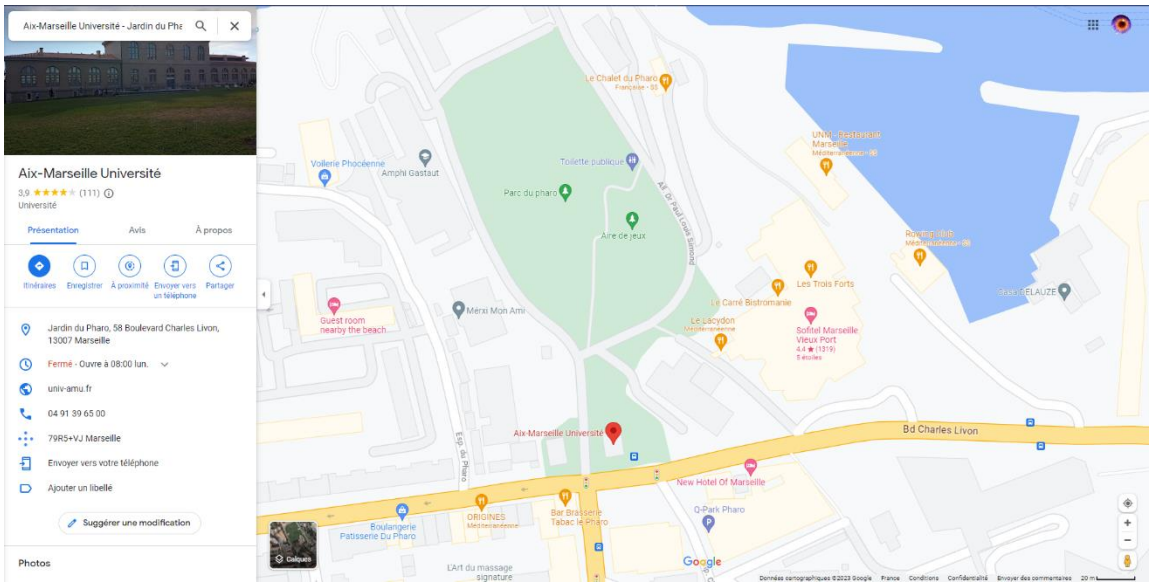

Figure 3 : site du Pharo

Et celui d'Aix dans les locaux de LID2MS, l'Équipe du Laboratoire Interdisciplinaire de Droit des Médias et des Mutations Sociales, pour travailler sur le côté RGPD.

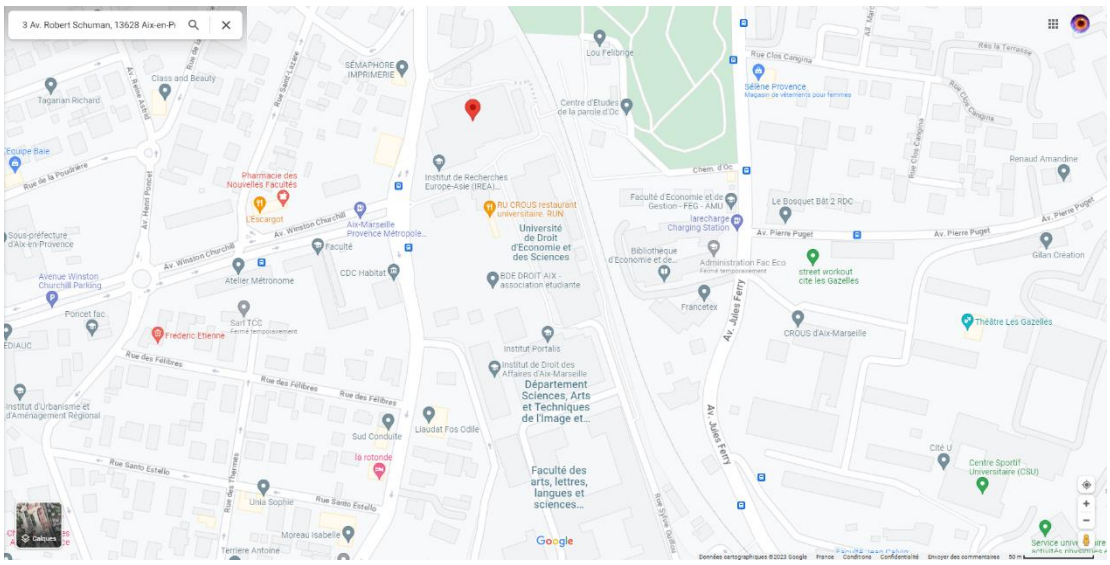

Figure 4 : site d'Aix

3 Travaux effectués

Au cours de ce stage, 3 missions principales m'ont été affectées au fil des semaines par Mr Valiente pour le coté SSI et 1 mission générale pour le coté RGPD.

Ces missions, sont les suivantes en premier le durcissement des postes de travails nous ayant été affecté au début de notre stage par la Dirnum, en second la Cartographie du réseau d'AMU pour permettre plus tard l'Homologation des SI qui est la dernière tâche nous ayant été confiées.

Une tâche annexe nous a aussi été confié à savoir la mise en place d'une procédure contre l'hameçonnage qui a été rapidement fait.

Concernant le côté RGPD, la mission qui nous a été confiée était de participer aux réunions et d'apporter notre assistance lorsque des connaissances sur les SI sont nécessaires, nous avons également été placés sur dossier concernant les contrôles des accès.

Nous rentrerons plus en détails sur toutes ces missions plus tard, mais pour résumer les tâches qui nous ont été données hormis la dernière du côté SSI et celle dans l'équipe RGPD, consistait à se mettre dans la peau d'un virus pour voir ce qu'il voyait une fois le réseau d'AMU et quelles actions il pouvait effectuer.

3.1 Durcissement

Durant ma première semaine de stage au sein de la l'unité, j'ai reçu un poste de travail personnel portable distribué par la Dirnum.

Il nous a également été donné un compte administrateur local afin de pouvoir installer des logiciels ou juste utiliser le poste à notre guise si nécessaire, pour lancer wireshark en tant qu'administrateur par exemple.

Pour donner suite à cela, la première tâche qui m'a été confiée fut de durcir ce poste dans le sens où je devais essayer de trouver s'il comportait des éléments potentiellement sensibles pouvant être utilisé par une entité tierce en l'état une fois donné.

Ce qui était entendu ici par élément sensible, signifiait tout aussi être la présence d'un fichier contenant un port ouvert, une communication ou encore une application n'ayant pas lieu d'être sur un poste neuf qu'une paire d'utilisateurs - mots de passe.

Je devais aussi voir si le pc était suffisamment sécurisé en me basant sur ce qui était donné par les bonnes pratiques de certains organismes reconnus tels que l'ANSSI, Agence Nationale de la Sécurité des Systèmes d'Information ou le NIST, National Institute of Standards and Technology.

Une autre idée, était de tester certains logiciels pour voir comment pouvait réagir l'antivirus ainsi que l'équipe si un logiciel malveillant est détecté et analyser les flux sur le pc.

Pour ce faire, j'ai eu carte blanche, mon tuteur m'a donné quelques pistes pour progresser tels que de copier la RAM, Random Access Memory ou d'utiliser des logiciels de forensique comme récuva que je ne connaissais pas, ce que j'ai fait après avoir regardé un tutoriel.

Une fois le pc en main, ainsi qu'un compte administrateur local sur la machine, j'ai téléchargé récuva et je l'ai utilisé.

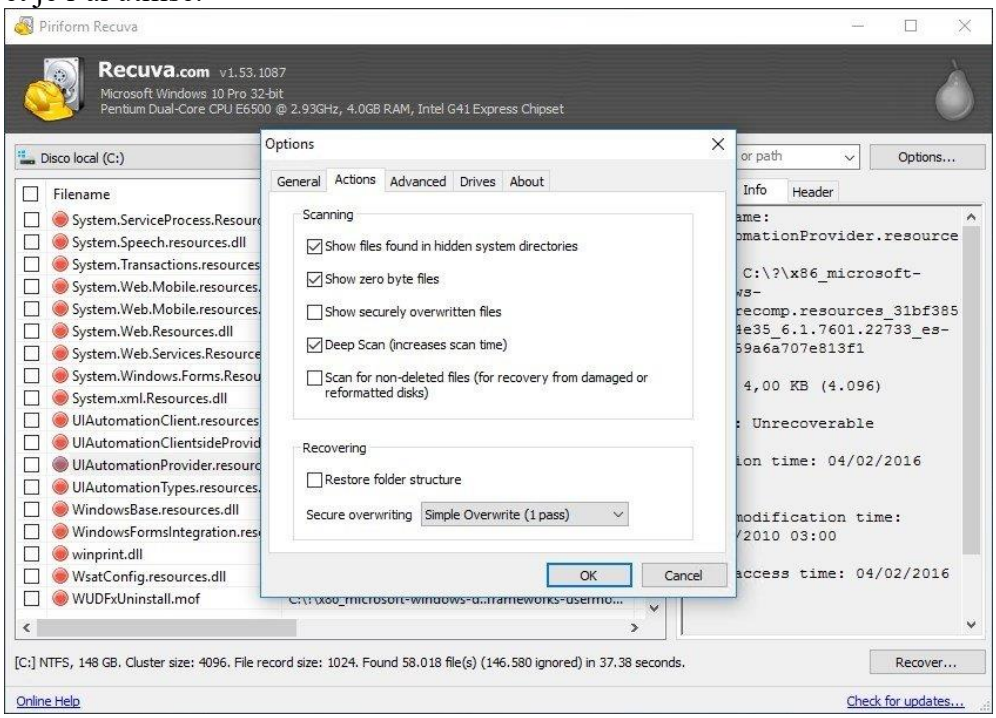

Figure 5 : logiciel récuva

Récuva est une application permettant de restaurer des fichiers effacés par l'utilisateur ou par erreur de la machine, allant de fichier textes aux fichiers audio et vidéo en scannant le disque dur.

Afin d'expliquer rapidement le fonctionnement de récuva, ce qu'il fait, consiste simplement à récupérer les données présentes sur les partitions du disque où quelque chose est déjà écrit, mais n'est plus forcément affecté.

Pour illustrer la chose, lorsque l'on télécharge un fichier, notre ordinateur écrit sur le disque les données de ce fichier et empêche la réécriture par-dessus celles-ci.

Cependant, lorsque l'on le supprime, il ne retire pas ces données, il se contente de signaler que l'on peut réécrire dessus, car elles ne sont plus affectées en tant que données du fichier au vu du fait que celui-ci est supprimé.

Après avoir lancé mon scan récuva, pendant que celui-ci se faisait en arrière-plan, j'ai commencé à regarder un peu dans la machine quelle sécurité était mise en place par défaut, j'ai pu constater que BitLocker était mis en place par défaut sur l'image de la machine, j'ai donc annulé mon scan pour retirer BitLocker et ai ensuite relancé récuva.

La raison pour laquelle j'ai annulé mon scan et retiré BitLocker est parce que ce logiciel permet de chiffrer le disque dur et donc d'empêcher des logiciels tels que récuva de fonctionner correctement, le scan se fera, mais ne trouvera rien de vraiment intéressant généralement si BitLocker est activé.

Ce point étant intéressant, je l'ai noté pour un compte-rendu de la tâche, car c'est une bonne chose pour la sécurité si jamais la machine est volée cela permettrait d'éviter que les données soient facilement accessibles.

Par la suite, j'ai continué en regardant dans les fichiers intéressants de Windows, en télécharger des logiciels comme mimikatz pour accéder au SAM, Security Account Manager cependant l'antivirus l'a détecté et supprimé ce qui m'a empêché de l'utiliser.

La raison pour laquelle j'ai essayé d'accéder au SAM, est parce qu'il s'agit de l'endroit où sont stockés les utilisateurs locaux de la machine ainsi que leurs mots de passes dans un registre.

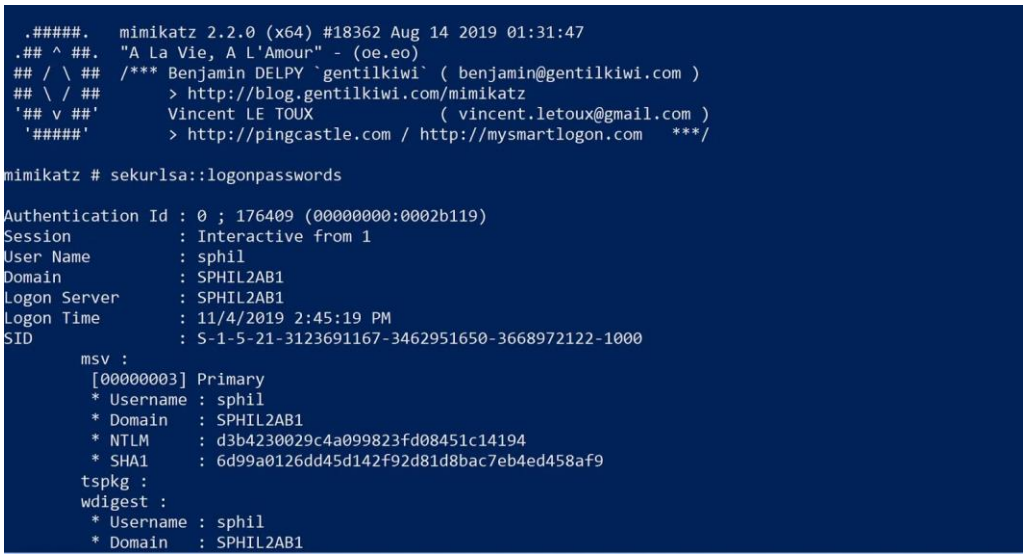

Figure 6 : exemple résultat mimikatz

Mimikatz une application en accès libre qui permet aux utilisateurs de voir et enregistrer des informations d'authentification, elle est couramment utilisée pour voler des données d'identification et augmenter les droits, mais dispose aussi d'autre module que je n'aborderai pas.

Grâce à cela, j'ai pu assez rapidement constater que l'équipe système a reçu une notification de Windows defenders et a vite réagi en m'envoyant un message me signalant un potentiel virus et surtout,

j’ai pu remarquer que l’antivirus n’autorise pas le logiciel à se lancer, il va même jusqu’à le supprimer de lui-même.

J’ai donc ensuite cherché une solution alternative et ai utilisé les outils .NET de Microsoft qui ont fonctionné, mais je n’ai rien pu trouver.

Une fois le scan récuva fini, j’ai regardé les résultats et me suis rendu compte que je n’avais également rien trouvé même en ayant retiré BitLocker.

Ensuite, j’ai essayé un autre outil FTK imager, Forensic Toolkit imager que je n’avais jamais utilisé auparavant, FTK imager ayant nécessité quasiment une journée pour fonctionner, en parallèle, j’ai lancé une capture de trafics des flux de ma machine avec wireshark.

Wireshark, est un logiciel d’analyse de protocole réseau essentiel pour investiguer du trafic, c’est un logiciel OpenSource pouvant permettre de déboguer les performances sur le réseau local en analysant si du trafic suspect est effectué en direction ou depuis le poste où il lançait.

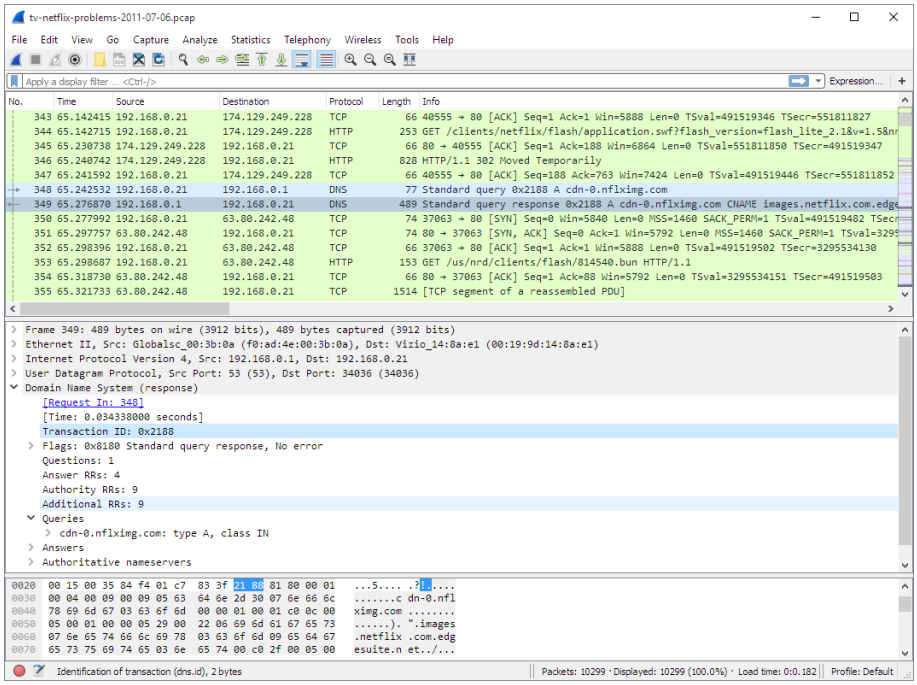

Figure 7 : Exemple de capture wireshark tiré de google

Une fois ma capture wireshark terminé, je l’ai analysé pour voir si du trafic étrange transiter dans ces flux tels qu’un DNS, Domain Name System en .ru ou autre, mais encore une fois, je n’ai rien trouvé.

Par la suite, j’ai continué de chercher d’autres informations à la main le temps que FTK Imager se termine, mais je n’ai trouvé qu’un LDAP, Lightweight Directory Access Protocol et l’adresse électronique de la personne ayant configuré mon pc avant de le donné, je suis donc passée à un logiciel qui pouvait me récupérer des informations utiles en cherchant dans les fichiers sensibles de la machine, mais il m’a uniquement redonné le même résultat, un LDAP et une adresse électronique.

Une fois que FTK Imager avait fini, j’ai tenté d’autres manœuvres telles que de mettre un nouvel OS, mais étant bloqué, on ne peut pas localement le modifier, j’ai donc aussi voulu tester la suite WinPEAS, Windows Privilege Escalation, mais elle est détectée par l’antivirus ce qui est aussi une bonne chose.

Figure 8 : logo WinPEAS

WinPEAS est un est script similaire à mimikatz dans le sens où il va chercher toutes les façons possibles pour élever ses privilèges sous un système Windows et donc pouvoir prendre le contrôle de la machine.

Ensuite, j'ai étudié le fonctionnement d'autopsy pour le lancer ensuite qui est lui aussi un autre logiciel de forensique plus complet.

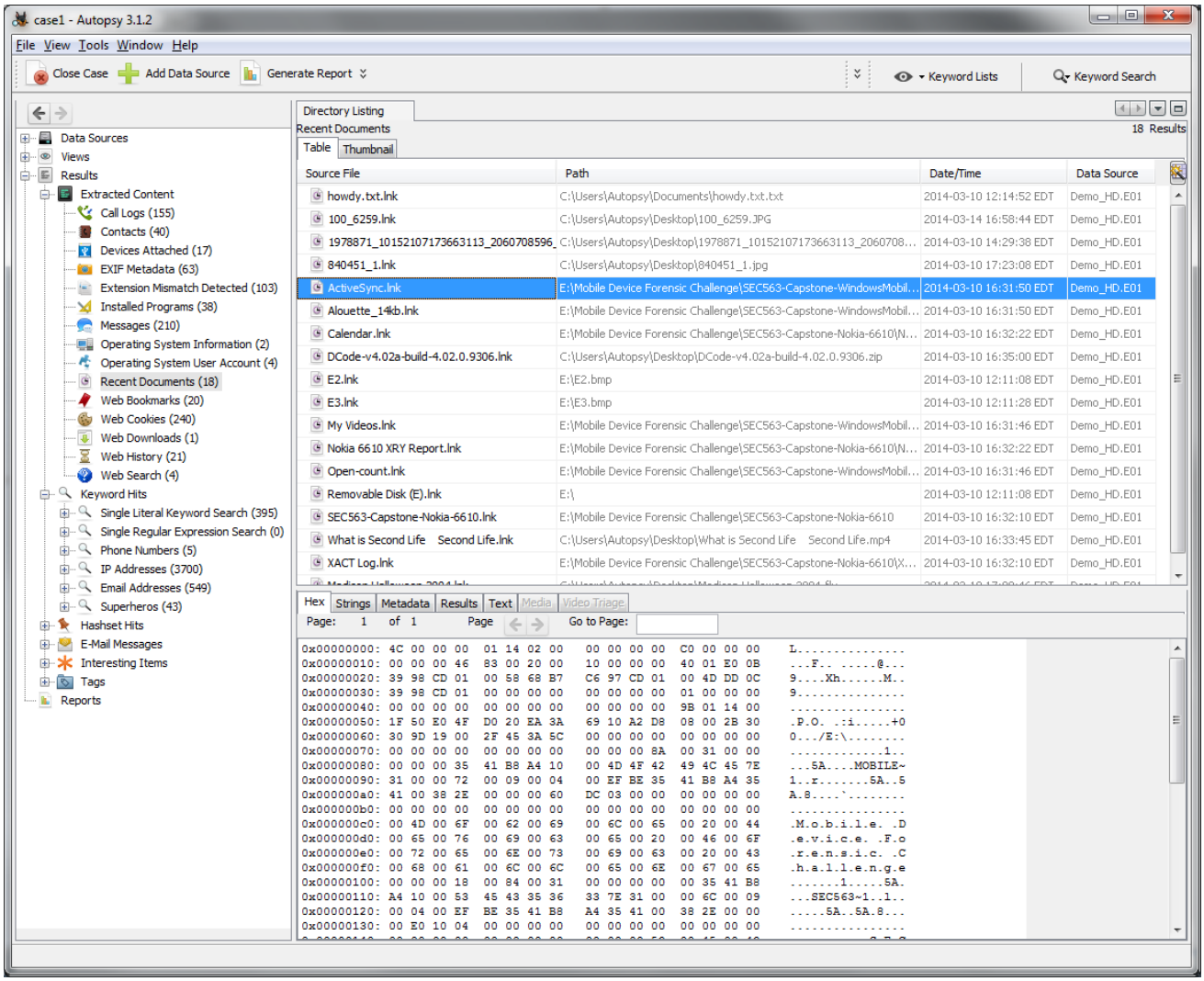

Figure 9 : Exemple de résultat autopsy

Une fois son étude finit, j'ai lancé autopsy qui lui, a pris 3 jours pour se finir durant la 2nd semaine, ensuite créée un rapport avec mon résultat et je l'ai envoyé à mon tuteur, mais il n'y avait rien d'intéressant.

Pour finir sur cette partie, je me suis rendue sur MITRE D3F3ND afin de voir si je pouvais trouver quelque chose d'intéressant pour durcir un SI et j'ai pu trouver STIG, Security Technical Implementation Guide qui donnait des bonnes pratiques en termes de sécurité des SI, Système d'information j'ai donc testé tout ce qui était en HIGH avec Jérémy et on a pu trouver quelques parties intéressantes également noté dans le compte-rendu.

3.2 Cartographie

Cette tâche consistait à faire une carte du réseau d'AMU à partir de ce qu'on avait trouvé auparavant répertoriant les machines, leurs noms, le responsable du serveur et les applications liées à cette machine.

Je me suis rendu dans mes scan wireshark précèdent, car j'ai pu voir qu'il y avait du DNS sur des serveurs terminant par univ-amu.fr, j'ai ensuite filtré sur le logiciel ce qui m'intéressait soit le 'univ-amu.fr' et j'ai récupéré ces adresses IP, Internet Protocol j'ai aussi interrogé le DNS d'AMU.

J'ai ensuite scanné les réseaux de chaque adresse AMU que j'ai pu trouver avec un ping sweep soit 7 réseaux au total et grâce à l'option '- -traceroute' je suis remonté jusqu'à scanner la totalité du réseau encore en ping sweep avec une résolution de nom grâce à la suite graphique du logiciel nmap appelé ZenMap.

Figure 10 : Logo Nmap

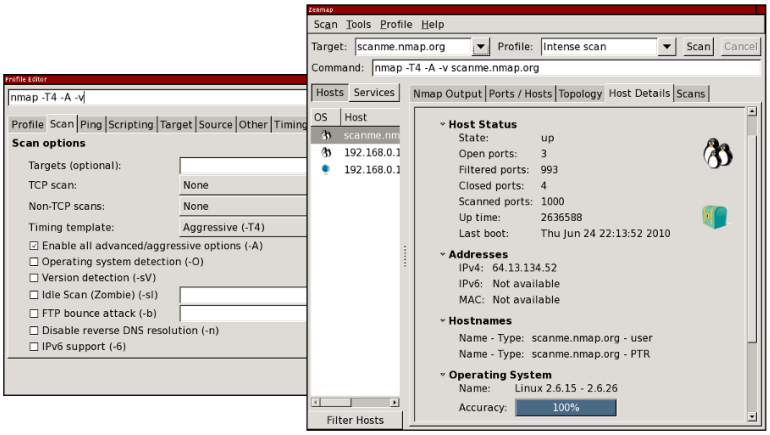

Figure 11 : interface de zenmap prit du guide utilisateur en ligne

Nmap est un scanner de ports conçus pour détecter les ports ouverts, identifier les services hébergés et obtenir des informations sur le système d'exploitation d'un ordinateur distant.

Il est aussi équipé de son engin de scripting appelé NSE, Nmap Scripting Engine qui permet de tenter d'exploiter des ports ouverts afin de vérifier s'ils sont vulnérables ou non tels que le port 21 de FTP, File Transfer Protocol avec le login anonymous qui permet de se connecter sans mots de passe sur un partage de fichier FTP.

Grâce à ce scan, plus de trois milles machines ont été trouvé et pour confirmer qu'il ne s'agissant pas juste d'un Firewall filtrant les paquets en les droppant, mais me renvoyant un UP, j'ai ensuite observé le résultat et chercher des résolutions de nom en univ-amu.fr et tout était bien résolu.

Une des fonctions pratiques de la version graphique de Nmap est le fait qu'elle peut nous donner un plan logique des scans que l'on a fait comme celui ci-dessous qui montre le chemin parcouru pour atteindre chaque hôte grâce à l'option cité précédemment.

Figure 12 : Scan logique réseau AMU via nmap

Le schéma ci-dessus est une des fonctions de zenmap, il permet de se représenter logiquement ce à quoi correspond notre réseau où le point noir est mon pc, de plus comme on peut le voir sur cette image chacun des hôtes est effectivement résolu ce qui montre que c'est un scan valide et qu'il n'y a potentiellement pas de Firewall sur le réseau interne.

Ensuite, j'ai dû attendre la confirmation de Mr Valiente pour savoir si je pouvais lancer de vrais scans sur les ports UDP, User Datagram Protocol et TCP, Transmission Control Protocol sur chacun des hôtes et potentiellement essayer des scripts sur des services sensibles tel qu'un partage.

Une fois la permission accordée j'ai donc lancé mes scans puis utilisé le NSE pour voir ce qui pouvait être exploitable et visible par un virus ou une APT, Advanced Persistant Threat qui se serait infiltré sur réseau interne.

Cependant, avant de faire ceci, j'ai testé en wifi et en filaire sur les 2 sites où j'ai travaillé si la route prise par les paquets est la même ou non, j'ai pu constater qu'elle changeait, mais uniquement dans la plage d'adresse publique autrement tout le chemin reste le même pour accéder aux serveurs et plus globalement au réseau d'AMU.

Ce scan a parmi de répertorier quels services sont ouverts sur quels hôtes, j'ai donc ensuite utilisé le compte pro qui m'a été fourni un peu plus tard pour voir à quelle application appartenait à quel serveur et j'ai rentré tout ceci dans un fichier XML,Extensible Markup Language commun avec Jérémy.

Grâce à cette carte, j'ai surtout pu constater qu'en réalité je n'avais qu'environ 400 serveurs à tester avec des scripts, car le reste d'entre eux consistait à servir uniquement de serveur d'équilibrage des charges.

Lorsque j'avais fini de rentrer toutes ces données, j'ai finalement commencé en tester un peu plus en détails les services notamment les serveur SNMP, Simple Network Managing Protocol que j'ai trouvé, pour ceux en v2 et v3 j'ai commencé par un Brute-Force avec la permission de mon tuteur, mais n'ayant rien trouvé, j'ai ensuite simplement énuméré les informations de ceux en version 1 ne nécessitant pas de mots de passe.

SNMP, est un protocole permettant de surveiller ses équipements réseau pour les gérer en obtenant leur état actuel sans avoir besoin d'y accéder physiquement ou de se connecter dessus à distance grâce à un agent préinstallé sur la machine.

Pour ce faire, j'ai utilisé les scripts de netmap et j'ai ensuite essayé à la main en utilisant ManageEngine MibBrowser.

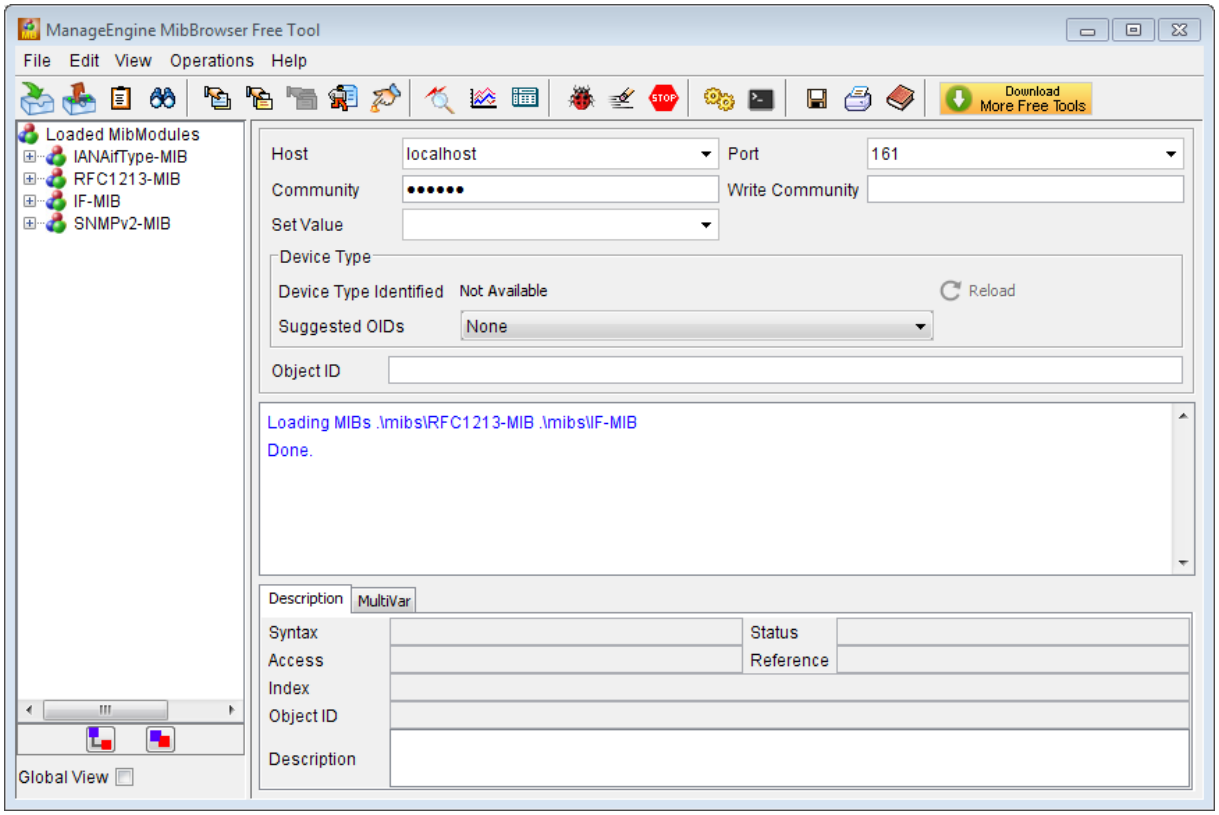

Figure 13 : ManageEngine MibBrowser

ManageEngine MibBrowser est un logiciel permettant de parcourir une base MIB, management information base hébergé sur un serveur SNMP et de recueillir des informations sur cette machine et les autres machines du réseau.

Après avoir testé, rien de vraiment intéressant n'est ressorti de cette exploration, je suis donc passé à la suite principalement les ayant un partage et ceux ayant un site web.

Pour ceux ayant un partage, j'ai essayé d'énumérer ce qu'il était possible, mais encore rien d'intéressant n'en est sorti, j'ai donc ensuite essayé de passer sur les serveurs web, mais encore une fois, je n'ai rien trouvé.

3.3 Homologation de SI

À la suite d'une réunion avec tous les RSSI du réseau RENATER, Réseau National de Télécommunications pour la Technologie, l'Enseignement et la Recherche qui est là où est hébergé une partie du réseau d'AMU, notre tuteur nous a informé que nous devions nous préparer pour l'homologation du réseau AMU en accord avec NIS2.

NIS2, Network and Information Security 2 est la directive européenne, adoptée en janvier 2023, qui obligera des milliers d'entreprises à renforcer leurs normes en matière de sécurité.

Elle vise à atteindre une maturité cyber commune dans l'ensemble de l'Union européenne qui entrera en vigueur le deuxième semestre de 2024 au plus tard, il reste donc encore un à deux ans à AMU pour se mettre à jour concernant cette norme.

Pour effectuer ceci, le travail nous ayant été confié consistait à rassembler des informations sur les SI au sein d'AMU ou plus globalement les serveurs d'applications, afin de pouvoir observer quel niveau de sécurité est mis en place sur ces serveurs, allant de l'accès physique à la sauvegarde ou encore s'il disposait d'un système de journalisation pour les accès et les modifications.

Dès le début de ce travail, l'objectif pour nous était de commencer en priorité par les applications jugées comme étant sensible, à savoir les serveurs d'application de messagerie et de ticketing.

Nous avons commencé par les serveurs de messagerie, car c'est par là que passe la majeure partie des communications au sein d'AMU, de plus, c'est par ici que les APT peuvent tenter de passer en utilisant des campagnes de phishing, nous pouvons aussi parler des spams qui sont une gêne, mais seront abordés plus tard.

Ensuite, nous sommes allés vers les serveurs de ticketing au vu du fait que les informations concernant des problèmes sont centralisées sur ce serveur, c'est donc une sorte de centre de commande étant nécessaire pour pouvoir évaluer la source du problème.

Pour ce faire nous avons donc organisé des rendez-vous avec les équipes techniques et fonctionnelles responsables des applications en question, afin de savoir qui contacter, nous nous en sommes référé à une application interne d'AMU appeler SIAMU qui rassemble les informations sur ces responsables et nous donnent également les serveurs sur lesquels sont hébergés ces applications ainsi que les responsables des dits serveurs.

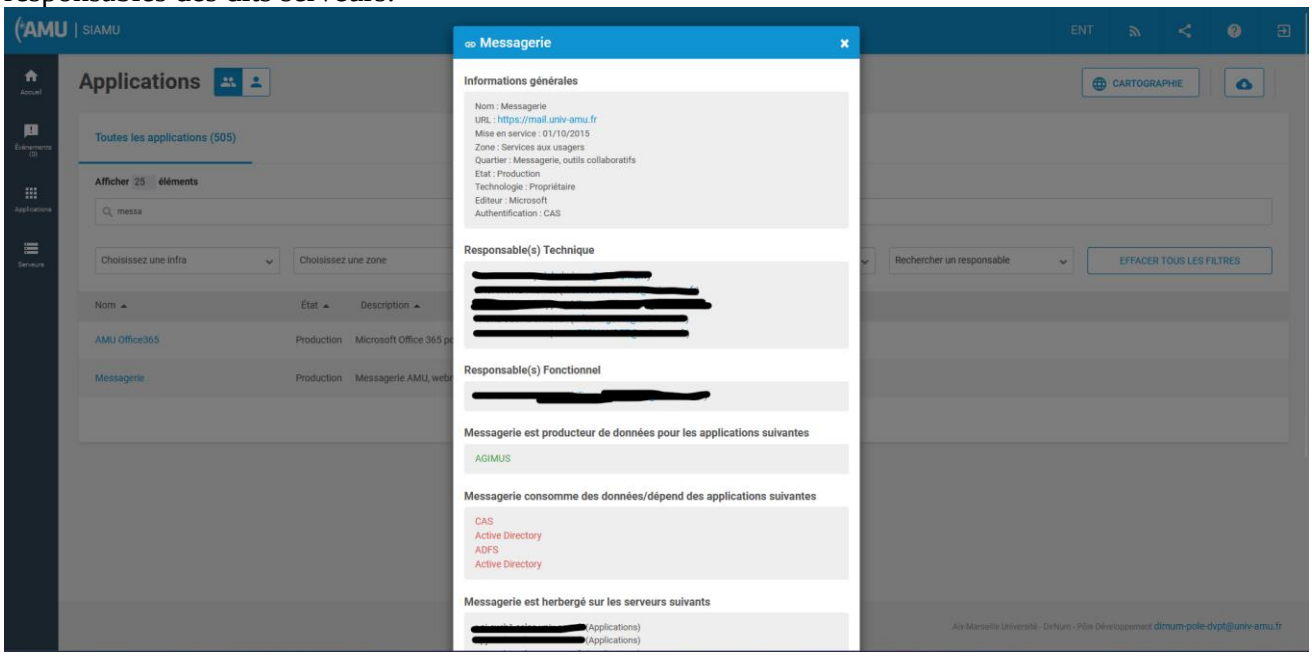

Figure 14 : SIAMU

Après avoir récolté les contacts des responsables, nous avons rassemblé des informations pour mettre en place un questionnaire qui sera utilisé durant ces réunions afin de nous donner un fil rouge à suivre pour nous organiser du au fait que non seulement, il y avait l'équipe SSI, Sécurité des Système d'Information mais aussi l'équipe RGPD qui devait assister à ces réunions et donc poser leurs questions.

Concernant le côté SSI le questionnaire s'est basé sur ce que l'on peut trouver dans la norme ISO, Organisation International de Normalisation 27002 datant de 2013.

La raison pour laquelle nous avons choisi ISO, car Mr Valiente nous l'avait recommandé, à la vue du fait qu'il s'agit d'une référence dans le domaine nous donnant ce qui est conseillé pour la sécurité des SI.

Pour communiquer ces informations entre nous, nous avons utilisé une autre application interne à AMU appelé AMUBox nous ayant servi de diverses façons, notamment pour savoir avec quelles applications planifier nos rendez-vous avec l'onglet appelé decks et pour y stocker nos notes durant ces réunions sur des fichiers partagées dans l'onglet fichier.

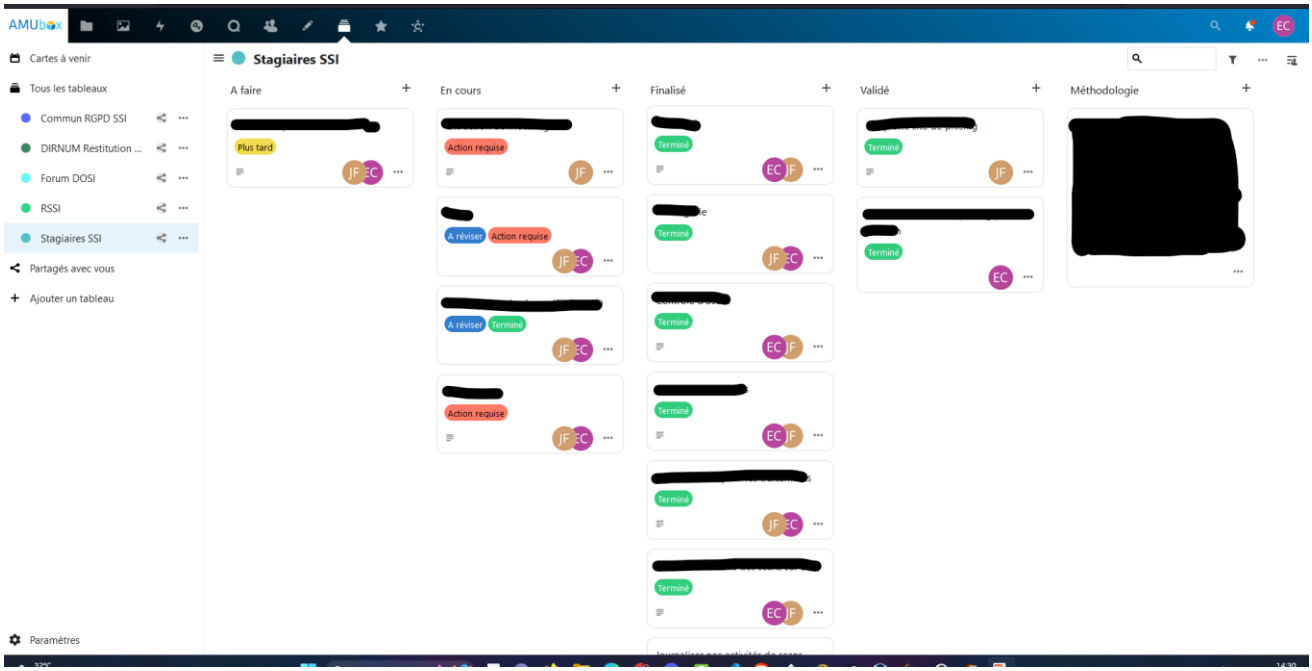

Figure 15 : Deck d'AMUBox

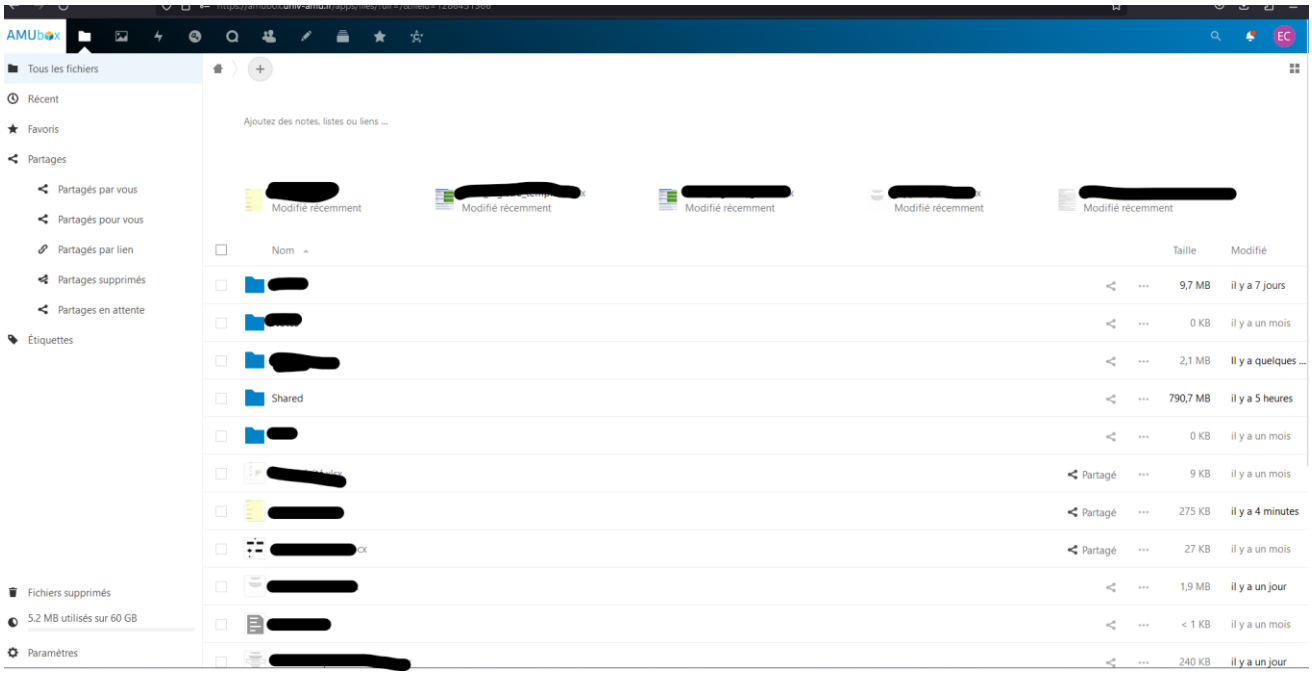

Figure 16 : fichier d'AMUBox

Après que nous ayons rassemblé ces informations, nous les avons plus tard retransmises à notre tuteur et elles seront replacées sous forme d'une carte logique pour savoir où se situe le ou les serveurs de chaque application, comment transite les données liées à l'application et pour finir où sont stocké ces données, en utilisant comme base la cartographie faite dans notre tâche précédente.

Nous avons aussi eu une autre tâche à faire en parallèle de la prise de rendez-vous, qui consistait à mettre une place une procédure pour contrer le phising précédemment mentionner, car la plupart du temps tous ces mails de phishing sont directement rediriger vers le RSSI qui doit donc les gérer un à un chacun de ces cas, nous devions donc imaginer une procédure pour régler ce problème avec deux versions.

La première version en attendant que la seconde puisse être mise en place consiste à copier le lien vers une application externe qui rentrera le lien dans les sites non autorisés par le pare-feu d'AMU puis à stocker ce lien dans une base de données en attendant que le lien soit supprimé.

La seconde version, quant à elle, consiste à cliquer sur le bouton signaler le spam pour rediriger le mail vers une adresse spécifique derrière laquelle tourne un serveur SMTP, Simple Mail Transfert Protocol et un script pour effectuer le processus de la première version sur ledit serveur en automatique dès lors qu'il reçoit un mail redirigé vers l'adresse électronique du serveur.

SMTP, est un protocole de communication utilisé pour transférer le courrier électronique (courriel) vers les serveurs de messagerie électronique

Ce travail était donc divisé en deux parties, la première consistait à expliquer le processus aux membres du personnels pour qu'ils puissent être mis en place et la seconde partie consistait à modéliser l'interface de la version un, pour ma part je me suis occupé de la première partie.

3.4 Assistance à l'équipe RGPD

De nos jours, la protection des données personnelle est une problématique ainsi qu'une obligation à laquelle font face les institutions traitant des données dans ce cadre et un manquement à cette obligation peut être sanctionnée par un organisme connu sous le nom de CNIL.

Cet organisme a été créé pour que l'évolution de l'informatique respecte les droits à la vie privée des citoyens, elle s'en assure en saisissant les institutions par des contrôles si une plainte est reçue pour confirmer la protection des données personnelles des usagers**.**

La cellule SSI-RGPD traite donc dans le domaine de la protection des données à partir de registre et notre travail ici, consistait à assister aux réunions de l'équipe RGPD, afin d'y apporter nos connaissances pour aider à finaliser un questionnaire permettant de connaître comment sont traitées les données sur chacun des SI au sein du réseau d'AMU que ce soit pour les applications ou les laboratoires.

Nous avons également participé sur des sujets divers tels que le traitement des données relatives du dit questionnaire en extrayant les données pour les rentrer dans un fichier XML et tout ceci de façon automatisée.

Nous avons également discuté de la possibilité d'ajouter un QR-code pouvant être scanné avec un téléphone qui redirige vers les registres de l'université, dans le cas où la CNIL ou une autre personne demande à consulter ces registres.

Plus tard durant le stage, une autre mission nous a été affectée en lien avec l'homologation des SI demander par le NIS 2 où nous avons été placés sur un dossier déjà abordé par les membres de l'équipe RGPD concernant les systèmes de contrôles d'accès du à une plainte que la CNIL a reçu de la part d'un membre du personnel sur des caméras sur un des sites de l'université.

Notre travail dans cette mission, consistait à vérifier le comportement des SI concernant le contrôle des accès au sein du réseau en interviewant les responsables de ces services pour comprendre son fonctionnement.

4 Conclusion

Durant mon stage au sein de la cellule SSI-RGPD, j'ai pu aborder beaucoup d'aspects fonctionnels de l'informatique, mais aussi bénéficier d'une introduction à la RGPD que je ne connaissais pas avant le début de ce stage.

J'ai rapidement pu me rendre compte qu'en réalité au sein d'une cellule SOC, Security Operation Center le travail ne consiste pas uniquement dans les aspects techniques, mais aussi à communiquer et à planifier des réunions avec différents services pour pouvoir fonctionner correctement.

En conclusion, ce stage m'a été bénéfique, il m'a permis de comprendre le fonctionnement du milieu d'entreprise et de voir ce à quoi ressemble la partie défenseur dans le milieu de la cybersécurité.

5 Remerciements

Tout d’abord, j’adresse mes remerciements à mon professeur Monsieur Tin Nguyen qui m’a orienté pour obtenir ce stage en proposant ma candidature.

Je tiens à remercier mon tuteur en entreprise, Monsieur Julien Valiente, son expertise m’a permis de comprendre plus en profondeur la façon de se positionner pour défendre efficacement son SI contre des attaques.

De manière plus générale, je remercie toutes les personnes qui ont contribué à ce que ce stage soit une expérience enrichissante.

6 Glossaire

BUT, Bachelor Universitaire de Technologie

RSSI, Responsable de la Sécurité des Système d'Information

RGPD, Réglementation Général de la Protection des Données

AMU, Université d'Aix-Marseille

DPO, Data Protection Officer, délégué à la protection des données

CNIL, Commission nationale de l'informatique et des libertés

DSI, Directeur des Système d'Information

ANSSI, Agence Nationale de la Sécurité des Systèmes d'Information

NIST, National Institute of Standards and Technology

RAM, Random Access Memory

SAM, Security Account Manager

FTK imager, Forensic Toolkit imager

DNS, Domain Name System

LDAP, Lightweight Directory Access Protocol, service d'annuaire

WinPEAS, Windows Privilege Escalation

STIG, Security Technical Implementation Guide

SI, Système d'information

Ping sweep, envoi d'une requête qui consiste à vérifier si un ordinateur distant est allumé sans aller interroger ses ports

NSE, Nmap Scripting Engine

UDP, User Datagram Protocol

TCP, Transmission Control Protocol

APT, Advanced Persistant Threat

XML, Extensible Markup Language

SNMP, Simple Network Managing Protocol

RENATER, Réseau national de télécommunications pour la technologie, l'enseignement et la recherche

NIS2, Network and Information Security 2

SSI, Sécurité des Système d'Information

ISO, International Organization for Standardization, en français Organisation internationale de normalisation

SMTP, Simple Network Transfert Protocol

SOC, Security Operation Center

7 Bibliographie