



MEMOIRE

Présenté à

**L’Institut Supérieur des Sciences Appliquées et de
Technologie de Gafsa**

(Département Informatique)

En vue de l’obtention du

MASTERE PROFESSIONNEL

Expert en Cyber Sécurité

Par

AOUN Souha

LA MISE EN PLACE D’UN SOC

Soutenu le 00 / 00 /0000, devant le jury composé de

M.

Président

M.

Rapporteur

Mme.

AL YAOUI Nouha

Encadreur

A.U : 2022 – 2023

Dédicace

Du plus profond de mon cœur et avec le plus grand plaisir de ce monde, je dédie ce modeste travail à

Mes chers parents « **Lotfi** » et « **Bouthaina** », que nulle dédicace ne puisse exprimer mes sincères sentiments, pour leur encouragement contenu, leur aide en témoignage de mon profondeur amour et respect pour leurs grands sacrifices.

Mes grands-parents, qui ont toujours attendu ma réussite depuis mon enfance

Mes chers frères et ma sœur « **Sahar** », « **Mohamed** » et « **Ahmed** » pour leur tendresse, leur complicité et leur présence.

Mes chères « **Aida Belgacem** », « **Dalila Belgacem** », « **Wiem Aoun** » et « **Imen Aoun** » pour leur grand amour et leur soutien, J'étais toujours entouré de votre soutien et vos encouragements.

Ma meilleure amie « **Dina** » la plus grande source de mon bonheur, et toute sa famille « **Ammar** » qui je souhaite bonne chance dans la vie. Merci d'être toujours là pour moi.

Mr « **Souhail Dhouibi** » merci de m'avoir donné du courage.

Tous mes enseignants, de la maternelle au mastère, sans lesquels je n'aurais jamais pu arriver à achever mon rêve spécialement Mme « **ALYAOUI Nouha** » et Mr « **FAKHET Walid** » pour la qualité de renseignements qu'ils m'ont prodigué au cours de ces deux années de mastères.

A mes chers amis sans que la liste ne puisse être exhaustive J'étais toujours entouré de votre soutien et vos encouragements

A la mémoire de mon cher cousin « **Nidhal Omri** » J'aurais tant aimé que vous soyez présents. Que Dieu ait vos âmes dans sa sainte miséricorde

Hommage à mon cousin Nidhal Omri
AOUN Souha

Remerciements

Je remercie dieu le tout puissant de m'avoir donné la santé et la volonté d'entamer et de terminer de mémoire.

Tout d'abord, ce travail ne serait pas aussi riche et n'aurait pas pu avoir le jour sans l'aide et l'encadrement de Madame « ***ALYAOUI Nouha*** »

Maître Assistant en Télécommunications, a l'institut « ISSAT Gafsa » Pour son encadrement et son aide précieux dans la réalisation de ce travail.

Je la remercie pour la qualité de son encadrement exceptionnel, pour sa patience, sa rigueur, ses conseils précieux et sa disponibilité durant la préparation de ce mémoire.

Mes vifs respects et mes forts remerciements vont aux membres de jury pour avoir accepté de juger mon travail

Monsieur le président de Jury Monsieur « »,

Maitre-assistant à l'ISSAT Gafsa qui a bien voulu me faire l'honneur d'évaluer ce travail.

Monsieur le Rapporteur Monsieur « »

Maitre-assistant à l'ISSAT Gafsa qui a bien voulu me faire l'honneur d'évaluer ce travail.

J'adresse mes sincères remerciements à tous les professeurs, intervenants et l'équipe d'administration à l'ISSAT Gafsa spécialement le chef de notre département « **HRIZI FATMA** » qui par leurs paroles, leurs écrits, leurs conseils et leurs critiques ont guidé nos réflexions et ont accepté de nous rencontrer et de répondre à nos questions durant notre recherche

AOUN Souha

Sommaire

Liste des abréviations	vii
Liste des figures	viii
<i>INTRODUCTION GENERALE</i>	1
Chapitre 1 : Présentation du CPG	2
1. Introduction.....	3
2. Présentation de la CPG	3
2.1. Présentation générale	3
2.2. Organigramme de la Société	4
2.3. Les différents services.....	4
2.3.1. Section administrative	4
2.3.2. Section sociale.....	5
2.3.3. Section paie	5
3. Le département informatique de la société	5
3.1. Présentation générale	5
3.2. Le réseau local de Gafsa	7
3.3. Ressources matérielles	8
3.3.1. Armoire Principale	8
3.3.2. Armoire 1	8
3.3.3. Armoire 2	8
3.4. Ressources logicielles	8
3.5. 5 Les diverses utilisations des réseaux.....	9
Chapitre 2 : Présentation du SOC et Blue Teaming	10
1. Introduction.....	11

2. Présentation du Pentest.....	11
2.1. Définition de pentest.....	11
2.2. Objectif de pentest	11
2.3. Les avantages du pentest.....	12
2.4. Les types de Pentest	12
2.5. Outils.....	13
2.6. La méthodologie ou les étapes de Pentest.....	13
3. Présentation du Red Teaming	14
4. Présentation du Blue Teaming	15
5. Comparaison entre Blue Teaming, Red Teaming et Pentest	17
7. Présentation du SOC [5]	20
8. Les niveaux de SOC :.....	25
9. Workflow de la data dans un SOC	26
9.1. Surveillance	26
9.2. Corrélation.....	27
9.3. Détection	28
9.4. Priorisation	29
10. Conclusion.....	29
Chapitre 3 :.....	30
Mise en place du SOC	30
1. Introduction.....	31
2. Mise en place du Système.....	31
3. VMware Workstation	32
4. Ubuntu	32
5. Mitre ATT&CK	32
5.1. Présentation	32

5.2.	Composants et principe de fonctionnement	33
5.3.	Apport	36
6.	Mitre DeTECT	36
6.1.	Présentation	36
6.2.	Composants et principe de fonctionnement	37
7.	Mitre D 3FEND.....	40
7.1.	Présentation	40
7.2.	Composants et principe de fonctionnement	41
8.	Have I Been Pwnd.....	43
8.1.	Présentation	43
8.2.	Composants et principe de fonctionnement	44
9.	DeHashed.....	44
10.	URLscan.....	45
11.	VirusTotal.....	46
12.	PyPhish.....	46
13.	Conclusion.....	47
	Chapitre 4 : Application du SOC	48
1.	Introduction.....	49
2.	Les outils appliqués	49
3.	MITRE DeTECT	49
4.	Have I Been Pwned ?	58
5.	DeHashed.....	61
6.	URLscan :	63
7.	VIRUSTOTAL.....	64
8.	Attaque phishing	64
8.1.	Attaque sur Facebook	66

8.2. Attaque sur Instagram	67
8.3. Attaque sur Gmail	69
9. Bloquer une attaque de phishing	72
9.1. SPF	72
9.2. DKIM	72
10. Anti SPAM	73
11. Conclusion	74
Conclusion Générale	75
Références Bibliographiques	76
Résumé	77
Abstract	77

Liste des abréviations

APT : Advanced persistent threat

CSIRT : Computer Security Incident Response Team ATT&CK

DKIM : DomainKeys Identified Mail

DeTT&CK : Detection, Denial and Disruption Framework Empowering Network Defense

DMARC : Domain-based Message Authentication, Reporting & Conformance

D3FEND : Detection Denial and Disruption Framework Empowering Network

IA : Intelligence Artificielle

IDS : Intrusion detection System

IPS : Intrusion Prevention System

ISAPI : Internet Server Application Programming Interface

SOC : Security Operation Center

NSA : National Security Agency

NOC : Network Operation Center

PTES : Penetration Testing Execution Standard

SIEM : Security Information and Event Management

SPF : Sender Policy Framework

TTP : tactics, techniques, and procedures

URL : Uniform Resource Locator

VMware : virtuel machine ware

.

Liste des figures

Figure 1: La Compagnie de Phosphates de Gafsa	3
Figure 2: Organigramme de la Société.....	4
Figure 3: Le réseau local de Gafsa.....	7
Figure 4 : Outils de pentest	13
Figure 5:les étapes de Pentest.....	13
Figure 6: Méthodologie pour développer un programme de sécurité	16
Figure 7: Catégories de phishing	20
Figure 8:Les composants d'un SOC	25
Figure 9: Les niveaux de SOC.....	26
Figure 10: Workflow de la data dans un SOC.....	29
Figure 11: Le système a appliqué	31
Figure 12 : Logo VMware Workstation.....	32
Figure 13: Logo Ubuntu.....	32
Figure 14: LA matrice ATT&CK pour le système d'entreprise	34
Figure 15: La tactique Accès initial aves ces techniques	35
Figure 16: les sous-techniques de la tactiques Accès initial.....	35
Figure 17: Cartographie par inférence grâce à l'ontologie des artefacts numériques.....	41
Figure 18: Cartographie des techniques offensives et défensives via les artefacts numériques	41
Figure 19 : Matrice MITRE D3FEND	43
Figure 20 : Exemple 1	44
Figure 21 : Exemple 1	44
Figure 22: URLScan.iso.....	45
Figure 23 : VIRUSTOTAL	46
Figure 24: PYPHISHER	46
Figure 25: Installation Git	49
Figure 26: Installation de DeTT&CT.....	50
Figure 27: Installation des packages	50
Figure 28: Installation python3-pip	51
Figure 29: Installer tous les modules	51
Figure 30: Lancement editeur DeTT&CT	52
Figure 31: Interface de l'éditeur DeTT&CT	52
Figure 32: Configuration du fichier d'administration de la source de données	53
Figure 33: Configuration des sources de données	53
Figure 34: Afficher les data sources	54
Figure 35:Afficher le contenu de fichier YAML	54
Figure 36: Convertir le fichiey YAML en JSON	55
Figure 37:Mitre navigator	55
Figure 38: Notre fichier json	56
Figure 39: Couverture des sources de données.....	56
Figure 40: Génération de la couverture de visibilité.....	57
Figure 41: Couche de couverture de visibilité.....	57
Figure 42: Notre fichier json de couverture de visibilité.....	57
Figure 43: Matrice de visibilité ATT&CK.....	57
Figure 44: Exemple 1 Have I Been Pwned ?	58
Figure 45: Exemple 2 Have I Been Pwned ?	59

Figure 46: Exemple 3 Have I Been Pwned ?	60
Figure 47: Exemple 1 DeHashed	61
Figure 48: Exemple 2 DeHashed	62
Figure 49: Exemple 3 DeHashed	62
Figure 50 : Analyse URL par URLscan	63
Figure 51 : Analyse URL par VIRUSTOTAL	64
Figure 52: Cloner le dépôt Installer PyPhisher	64
Figure 53:Entrer dans le répertoire et installer tous les modules	65
Figure 54: exécution pyphisher.py.....	65
Figure 55: Sélectionnez l'option Facebook.....	66
Figure 56: URL Facebook malicieux.....	67
Figure 57: La page malicieuse Facebook	67
Figure 58: Sélectionnez l'option Instagram	68
Figure 59: URL Instagrem malicieux	68
Figure 60: La page malicieuse d'Instagram.....	68
Figure 61: Sélectionnez l'option Gmail	69
Figure 62: URL Gmail malicieux	69
Figure 63: La page malicieuse de gmail.....	70
Figure 64: les données d'une victime	70
Figure 65: PyPhisher Data.....	71
Figure 66 : Analyse d'un URL malicieux	71
Figure 67: Fonctionnement de SPF	72
Figure 68: Fonctionnement de DKIM.....	73
Figure 69: Fonctionnement de DMARC.....	73

INTRODUCTION GENERALE

Durant ces dernières années, le monde numérique se progresse par les technologies de l'information et des télécommunications qui témoigne une évolution considérable. En conséquence, cette évolution entraîne l'augmentation du taux de risques d'attaque pour cela la sécurité des systèmes d'informations est devenue l'objectif principale des entreprises.

En effet, les entreprises tentent à développer les solutions et les technologies pour protéger leurs architectures réseaux du piratage et de la perte des données confidentielles. Ils sont toujours à la recherche des meilleures solutions pour mieux surveiller les systèmes d'information et détecter les intrusions et les attaques en utilisant des outils d'analyse des alertes et des journaux, des firewalls ainsi que des IDS/IPS.

C'est dans ce contexte que s'inscrit notre projet intitulé « la mise en place d'une solution SOC » réalisé au sein de CPG. Les différentes étapes de réalisation de notre projet sont décrites dans le rapport courant, qui s'articule autour de trois chapitres.

Nous présenterons au sein de premier chapitre, le pentest, le Red Teaming, le Blue Teaming avec leurs tâches et normes, une comparaison entre eux, une présentation du SOC et le Workflow de la Data. Ensuite, un deuxième chapitre est consacré pour la mise en place du SOC et les outils que nous utilisons tout long de notre travail. Le troisième chapitre présente et traite l'application du SOC. Les résultats seront par la suite analysés et des contre-mesures seront également proposés dans l'objectif d'améliorer le niveau de sécurité du système proposé. Nous clôturons notre travail par une conclusion générale.

Chapitre 1 : Présentation du CPG

1. Introduction [19]

J'ai eu la chance d'effectuer mon stage PFE, du 01/02/2023 au 15/05/2023, au sein de la compagnie des phosphates de Gafsa (CPG) qui a comme domaine d'activité l'extraction, le traitement et l'exportation des gisements de phosphate en Tunisie.

Ce chapitre comportera une présentation de cette société d'une façon générale (Historique, les différents divisions)

2. Présentation de la CPG

2.1. Présentation générale

La Compagnie des phosphates de Gafsa ou CPG est une entreprise tunisienne d'exploitation des phosphates basée à Gafsa. Elle est rattachée en 1994 au Groupe chimique Tunisien.

La CPG figure parmi les plus importants producteurs de phosphates, occupant la cinquième place mondiale avec une production de presque huit millions de tonnes en 2009. En 2014, la production a chuté à cinq millions de tonnes et la Tunisie est le huitième producteur mondial, avec 2,27 %.

En 2010, la CPG exploite huit mines à ciel ouvert, situées dans les délégations de Redeyef, Moulares, Metlaoui, Mdhila et onze laveries destinées au traitement du minerai. Cette activité nécessite près de dix millions de m³ d'eau pompée dans les nappes fossiles et engendre le déversement d'eaux de lavage dans la nature, causant la colère des agriculteurs et des écologistes.



Figure 1: La Compagnie de Phosphates de Gafsa

2.2.Organigramme de la Société

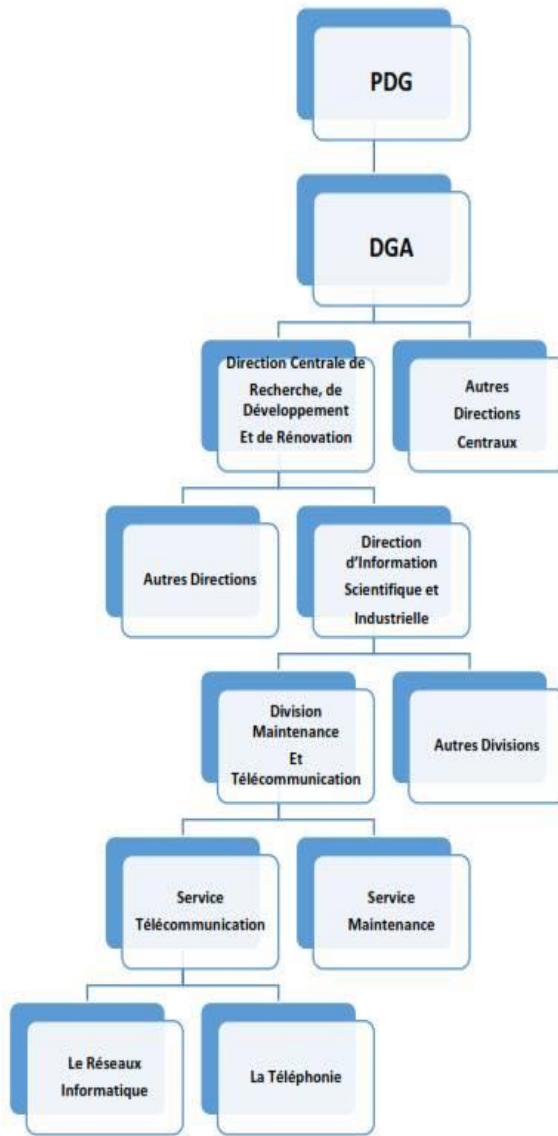


Figure 2: Organigramme de la Société

2.3.Les différents services

2.3.1. Section administrative

Pour cette section, elle a pour mission principale le suivi de l'activité de personnel (cadres, employés et ouvriers). Les responsables dans cette section établissement des

fichiers, des documents ainsi que des dossiers qui comportent tous les renseignements possibles concernant les maladies, accidents de travail, la retraite, les congés et la mutation.

2.3.2. Section sociale

La section sociale s'intéresse à tout ce qui concerne la vie sociale de l'agent telle que :

- La mutuelle
- Capitale de décès
- Les permis de circulation
- Les allocations familiales
- Le logement
- Les congés légaux

2.3.3. Section paie

C'est la section qui assure la paie des agents, en effet elle communique le pointage et les différents primes liées de travaux au centre de traitement informatique à Gafsa pour édition des bulletins de paie. Comme pour chaque section on trouve qu'elle est rédigée par un chef section principale et un chef section.

- ❖ C5 congé de mariage
- ❖ P1 permission UGTT
- ❖ P8 permission sans solde
- ❖ M1 maladie de courte durée
- ❖ M2 maladie de longue durée

3. Le département informatique de la société

3.1. Présentation générale

La CPG dispose de trois centres de traitements informatiques :

- Centre de traitement informatique de Gafsa.
- Centre de traitement informatique de Metlaoui.
- Centre de traitement informatique de Tunis.

Et quatre mini-centres informatiques implantés à M'dhilla, Redeyef, Sfax et Moulaires. Le centre de Gafsa s'occupe de la gestion des systèmes suivants :

- ◆ Système pièces de caisse.
- ◆ Gestion administrative

Le centre de Tunis s'occupe de la gestion des systèmes trésoriers et financiers. Le centre de Metlaoui s'occupe de la gestion des systèmes suivants :

- ◆ L'application productive GMAO.
- ◆ L'application des suivis des engins.
- ◆ L'application des inventaires.

Les tâches d'installation d'administration et de maintenance des réseaux informatiques locaux (LAN) et étendus (WAN) est accordée au service de télécommunication qui s'intéresse, aussi, à la connexion à l'Internet.

Pour les mini-centres, ils ne représentent que des points de liaisons entre les utilisateurs distants situés aux différents sites de la CPG et les applications qui se tournent dans les trois centres de traitement des informations. Ils renferment les équipements réseaux nécessaires pour garantir cette liaison tel que les routeurs, les Switch, les modems, les lignes de communication ...

Le réseau informatique de la CPG est implanté sur 7 sites géographiquement éloignés : Metlaoui, Gafsa, Tunis, Redeyef, M'dhilla, Moulaires et Sfax. A chaque site, il existe un réseau (LAN ou MAN). Le but de ce réseau est de connecter tous les utilisateurs aux différents services des ressources applicatives installés aux centres informatiques.

L'interconnexion inter sites est faite à travers deux types de liaisons de transmission des données :

- ❖ Liaison MPLS
- ❖ Liaison par satellites (VSAT)

La CPG dispose de 7 ports MPLS, dont 4 port en cuivre ayant un débit de 2Mbit/s et 3 ports en fibre ayant un débit de 10Mbit/s. Ce type de liaison est utilisé pour relier les directions des secteurs et aussi pour lier la CPG aux entreprises externes, telles que la douane, TTN Les liaisons satellitaires sont utilisées pour relier les sites de production à la DMM (Metlaoui), avec un débit de 256Kb/s chaque une.

La liaison à l'Internet est établie à l'aide d'une liaison ADSL de débit 20Mbit/s.

3.2. Le réseau local de Gafsa

Au siège social à Gafsa, on trouve des liaisons câblées : cuivre (UTP/FTP Cat. 5e ou 6) ou Fibre optique avec un débit de 1 Gb/s; et des liaisons sans fils (Wifi) avec un débit théorique entre 150 Mb/s et 200 Mb/s pour une surface de 460 mètres carrés pour chaque radio. Il existe 6 points d'accès.

Le réseau de Gafsa est segmenté à des sous-réseaux de petites tailles. Les serveurs d'applications et les imprimantes réseaux sont installés dans une zone autre que le réseau local. La segmentation est assurée par un pare-feu Juniper. En effet, il existe 5 zones : Serveurs, LAN, Wifi, Internet et MPLS pour les sites distants.

La liaison MPLS avec les sites distants est assurée par un routeur de types Cisco.

La liaison à l'Internet est assurée par un filtrage simple sur le pare-feu et un filtrage applicatif sur le serveur proxy.

Pour les liaisons locales, il existe deux switchs de type HP Procurve respectivement de 140 et 240 ports et un switch Dlink de 48 ports.

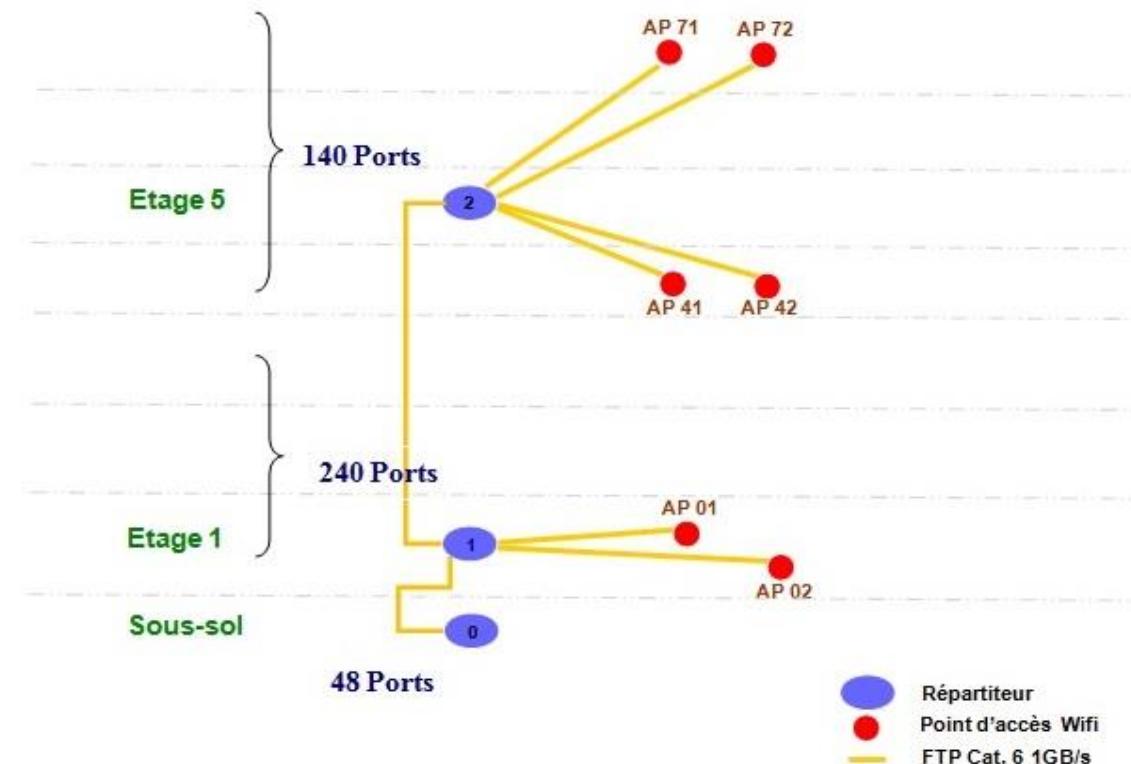


Figure 3: Le réseau local de Gafsa

3.3.Ressources matérielles

3.3.1. Armoire Principale

- Un Routeur ADSL 20Mbit/s pour la connexion Internet (ligne spécialisé haut débit).
- Un Routeur fibre optique.
- Un Routeur CISCO 1700 pour MPLS.
- Un Switch DLink (48 ports RJ45(1Gbit/s)) pour le LAN.
- Deux Firewalls Juniper SSG 550.
- Un contrôleur wifi Ruckus 1100.
- Deux serveurs Proxy OLFEAO R7000.

3.3.2. Armoire 1

- Switch HP 5412 ZL(240 ports de 1Gbit/s).
- Ventilateur.
- Bloc d'alimentation.

3.3.3. Armoire 2

- Switch HP 5412 ZL(140 ports de 1Gbit/s).
- Ventilateur.
- Bloc d'alimentation

3.4.Ressources logicielles

- Active directory : cet outil permet de gérer les ordinateurs du domaine de tous les utilisateurs du secteur sont inscrits sous Active Directory avec des droits différents.
- DNS : pour la résolution du nom du domaine il contient les indicateurs de la racine et les adresses du domaine parent.
- DHCP : est un protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres IP d'une station, notamment en lui affectant automatiquement une adresse IP et un masque de sous-réseau.
- ISA Server : Appelé précédemment Microsoft Proxy Server, ISA est un produit de

sécurité de type pare-feu basé sur Microsoft Windows conçu initialement pour présenter (publier) sur Internet des serveurs Web et d'autres systèmes serveur de manière sécurisée. Il fournit un système pare-feu au niveau de la couche « application » gérant l'état des sessions et l'accès Internet pour les ordinateurs clients dans un réseau d'entreprise.

- Symantec Antivirus Server : Symantec antivirus version serveur installée sur le serveur version client et sur les autres utilisateurs, il a pour rôle la détection des virus dans tout le réseau.

3.5.5 Les diverses utilisations des réseaux

- Le partage des ressources réseaux tels que les fichiers, les documents, l'imprimante
- La mise à jour des données concernant la production et l'extraction
- La saisie des pièces de caisse pour la section
- La connexion à INTERNET.

Ces applications, possèdent chacune une base de données installée sur le serveur à la direction générale de Gafsa pouvant être accessible pour saisir des données de n'importe quel Point du réseau.

Le logiciel GMAO utilisé à 90% pour la gestion du matériel, est accessible partout les utilisateurs du réseau à travers le protocole Telnet Encore la gestion du personnel, activités, métiers, planning de charge, prévisionnel, pointage des heures, etc.

Pour assurer l'automatisation de sa communication interne le CPG a opté pour l'outil **LOTUSNOTES**, Cet outil assure une bonne circulation d'informations fiable, il est utilisé à un Pourcentage limité à 90 % pour le transfert des fichiers.

Chapitre 2 : Présentation du SOC et Blue Teaming

1. Introduction

Au cours des prochaines années, la **cyberprotection** jouera un rôle important dans la protection des données, des systèmes et des programmes, car les agressions se produisent à un rythme toujours croissant. Les sociétés qui investissent dans le domaine de la protection informatique seront donc plus efficaces dans la prévention des cyberattaques. Pour faire face efficacement aux risques de sécurité informatique, l'équipe rouge, l'équipe bleue semblent être des solutions simples, pratiques et performantes.

2. Présentation du Pentest

2.1. Définition de pentest

Le test d'intrusion est une technique de piratage éthique de cybersécurité consistant à identifier et détecter la sensibilité des réseaux ou des systèmes informatiques, mettre en évidence les vulnérabilités de leur posture de sécurité et mieux évaluer les risques potentiels.

Le pentest effectue un enregistrement de mesures mises en œuvre, un rapport détaillé sur les vulnérabilités et aussi les solutions pour améliorer les niveaux de sécurité informatique mais la correction des faiblesses qu'elles surviennent et l'exécution de mesure de renforcement informatique ne font pas partie du test d'intrusion. Le pentest peut être effectué de manière automatisée à l'aide des applications logicielles ou manuellement par des pentesters qui sont des experts en informatique connus sous le nom de pirates éthiques en utilisant différentes méthodologies, outils et approches identiques à celles utilisées par les vrais attaquants ou pirate informatiques pour pénétrer dans un système sans autorisation.

2.2. Objectif de pentest

L'objectif principal du pentest est de détecter les vulnérabilités du système, de réseaux ou du logiciel cible en effectuant des tests de sécurité des systèmes et des logiciels appartenant aux actifs informatiques et de les documenter dans un rapport détaillé. Il effectue des simulations d'attaques d'ingénierie sociale sur des organisations en concevant des attaques d'ingénierie sociale. Tout en effectuant des tests de sécurité, il suit constamment les technologies les plus récentes et crée de nouvelles méthodes d'attaque en s'informant sur la sécurité. Cela inclut les méthodes d'attaque dans le cadre des tests de sécurité. En plus des tests de sécurité, il détecte les failles de sécurité dans le code source des applications en effectuant une analyse du code source.

Après avoir effectué des tests de sécurité des applications, des dispositifs de réseau et des infrastructures informatiques, il crée des rapports contenant des informations détaillées sur les résultats à fournir au client. Il informe l'organisation des vulnérabilités qui existent dans la pratique et qui doivent être éliminées grâce à son point de vue et ses capacités offensives

2.3. Les avantages du pentest

Le testeur d'intrusion travaille toujours dans un environnement où il peut appliquer les techniques d'attaque les plus récentes tout en effectuant des tests de sécurité. Il peut utiliser ses propres outils d'attaque tout en détectant les vulnérabilités du système cible. Il rencontre de nouvelles technologies dans la pratique, car il a l'occasion d'effectuer des tests de sécurité d'une grande variété de technologies

2.4. Les types de Pentest

Il existe trois niveaux généraux de réalisation d'un test d'intrusion : le pentest en boite blanche, le pentest en boite grise (gray box), le pentest en boite noire (black box).

- Le pentest en boite blanche**

Sont les plus avancés. Les testeurs possèdent une connaissance détaillée d'information technique et de sécurité d'une organisation. Ces testeurs peuvent améliorer la sécurité d'une organisation donc ils sont chargés de découvrir les moindres failles de l'infrastructure de sécurité

- Le pentest en boite grise (gray box)**

Le pentest en grey box ou boite grise : les testeurs généralement ne possèdent qu'une quantité limite d'informations, ils ont une certaine connaissance des systèmes et des mesures de sécurité de la cible. Cela va ouvrir d'autres portes sans pour autant donner toutes les informations. Cet audit permettra d'aller un peu loin dans le test et de parcourir d'autre domaine. L'objectif d'un test de boîte grise est d'apprendre des détails sur les vulnérabilités qui peuvent être exploitées à un niveau supérieur à celui des évaluations de boîte noire.

- Le pentest en boite noire**

Le pentest en Black box ou boite noire : c'est la méthode la plus réaliste. Dans ce cas, l'hacker commence de tester le système sans aucune connaissance ou compréhension de l'infrastructure technologique et des dispositions de sécurité de la cible. Il va s'agir comme le ferait un attaquant, en testant tour à tour les différentes portes à la recherche d'une vulnérabilité à exploiter. Ces tests à l'aveugle ont pour principaux avantages d'identifier rapidement des

vulnérabilités faciles à exploiter. Cependant, ils sont moins exhaustifs et ne testent pas la qualité de la configuration du système.

2.5. Outils

Plusieurs outils peuvent être utiles lors de l'application du pentest. Parmi lesquels nous pouvons citer Nmap, Metasploit, OWASP ZAP, Searchsploit, Burp Suite, Wireshark, Mimikatz, Netcat, Nikto, pwncat, SET, ...



Figure 4 : Outils de pentest

2.6. La méthodologie ou les étapes de Pentest

Pour la réalisation d'un pentest, le pentester doit suivre une méthodologie référencée. Les phases de test de pénétration sont basées sur PTES (Penetration Testing Execution Standard) un standard de version V1.0 créé afin de proposer aux entreprises et aux équipes de sécurité une trame commune et un cadre pour l'exécution d'un pentest.

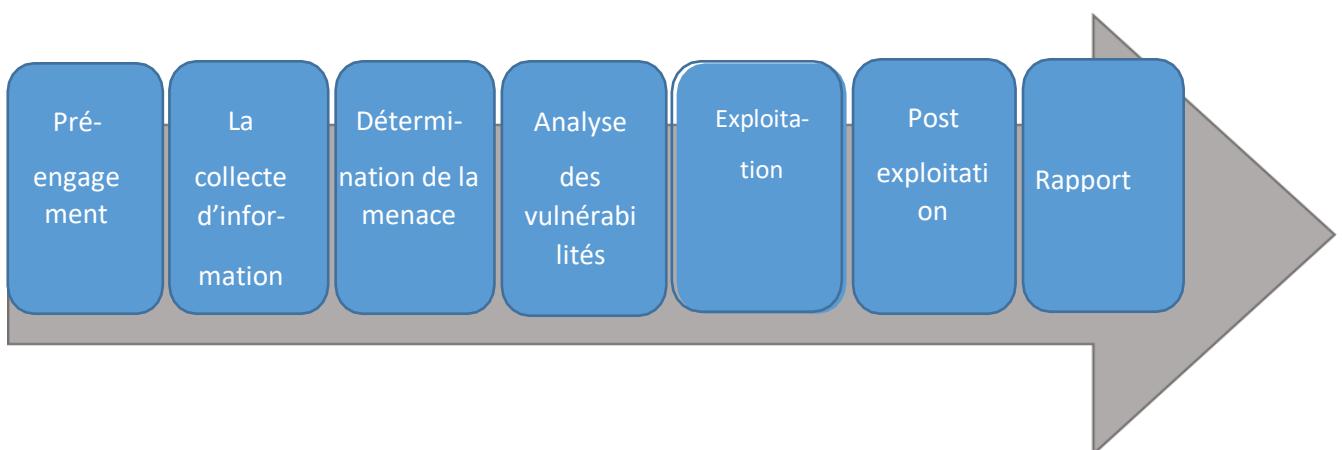


Figure 5:les étapes de Pentest

- **Pre-engagement** : chaque test d'intrusion commence par une négociation, une compréhension des besoins clients, la détermination de type de pentest, la limitation de l'attaquant et finalement la création du contrat ou accord de priorité.
- **La collecte d'information** : L'organisation testée fournira au pentester des renseignements/d'informations générales sur les cibles.
- **Détermination de la menace** : Dans celle étape et en se basant sur les informations recueillies on va chercher à dresser une liste des menaces pour l'entreprise tels que les sous- domaines, disponibles pour les applications Web ou les ports et les services qui étaient disponibles pour les hôtes ciblés.
- **Analyse des vulnérabilités** : La troisième phase de test d'intrusion est l'évaluation de la vulnérabilité dans laquelle le testeur serve toutes les informations collectées précédemment lors des phases de reconnaissance afin d'acquérir des connaissances initiales analyser les systèmes, le personnel et les processus et d'identifier de vulnérabilités exploitables et les éventuelles failles de sécurité qui pourraient permettre à un attaquant extérieur d'accéder à l'environnement ou à la technologie testée
- **Exploitation** : Après avoir identifié les vulnérabilités obtenues dans la phase précédente, il est temps de les exploiter et à avancer dans l'intrusion, Les pentest tente d'accéder au système cible et d'exploiter les vulnérabilités identifiées, généralement en utilisant un outil comme Metasploit pour simuler des attaques réelles.
- **Post exploitation** : Cette phase comporte plusieurs phases importantes, comme un vrai hacker, le testeur de pénétration va devoir effacer ses traces pour que ces agissements soient les plus discrets possible.
- **Rapport** : Le testeur prépare un rapport documentant le déroulement du test d'intrusion et d'exposer à l'entreprise. Ce rapport peut être utilisé pour corriger les vulnérabilités trouvées dans le système et améliorer la posture de sécurité de l'organisation

3. Présentation du Red Teaming[8]

3.1. Définition Red teaming

Le Red teaming est un groupe qui prétend être un ennemi. C'est un groupe qui travail pour l'organisation ou embauché par l'organisation son travail est légal il tente une intrusion physique ou numérique, simule le comportement et le mode de pensée des adversaires et concurrents afin d'identifier les faiblesses, les problèmes et les vulnérabilités des systèmes, des

processus et des stratégies de l'organisation puis fait rapport à l'organisation afin que celle puisse améliorer ses défenses.

Les activités de Red teaming sont généralement menées dans le cadre d'un processus d'évaluation ou de test plus large et peuvent inclure une série d'activités telles que les tests de pénétration, l'ingénierie sociale et les exercices basés sur des scénarios.

Le Red Teaming est utilisé dans plusieurs domaines notamment la cyber sécurité, les forces de l'ordre, les agences de renseignement, l'armée et la sécurité des aéroports.

Les Red Team représentent des entités interne au sein de l'organisation ou comprendre des consultants et des experts externes dédiées à tester l'efficacité d'une politique de sécurité en émulant au maximum les outils et techniques d'attaque potentielles de la manière la plus réaliste possible.

3.2. L'objectif du red teaming

L'objectif du red teaming est de :

- Identifier et d'exposer les faiblesses et les vulnérabilités qui ne sont pas évidentes pour l'organisation et de faire des recommandations pour améliorer les défenses de l'organisation contre des adversaires ou des concurrents potentiels.
- Améliorer la sécurité et la résilience de l'organisation, car elles donnent une image plus réaliste et plus complète de la situation.
- Identifier les menaces potentielles et à y répondre. Il peut également aider les organisations à identifier les menaces potentielles et à y répondre.
- Identifier et de hiérarchiser les domaines à améliorer, ainsi que d'élaborer et de mettre en œuvre des contre-mesures et des stratégies plus efficaces.
- Des mesures et des stratégies plus efficaces peuvent être développées.
- Les équipes rouges sont généralement dirigées par une équipe d'experts possédant les connaissances et les compétences nécessaires pour simuler les tactiques, les techniques et les procédures des adversaires et des concurrents.

4. Présentation du Blue Teaming

4.1. Définition Blue teaming

Le Blue Team est composé de professionnels de la sécurité qui ont une vue d'ensemble de l'organisation leur tâche consiste à protéger les actifs critiques de l'organisation contre tout type de menace et exécuter toutes les fonctions SOC .Généralement , le Blue Team est chargé

de la gestion des informations et des événements de sécurité, de la surveillance des événements, de la collecte de données sur les menaces, de la collecte et de l'analyse des paquets de données et de l'automatisation de la sécurité. En outre, le Blue Team identifie les installations critiques et effectuent des évaluations régulières des risques sous la forme d'analyses des vulnérabilités et de tests d'intrusion afin de surveiller en permanence leur exposition. Le graphique ci-dessous illustre le chemin parcouru et le cadre ou la méthodologie que nous utilisons pour aider nos clients à développer leur programme de sécurité.

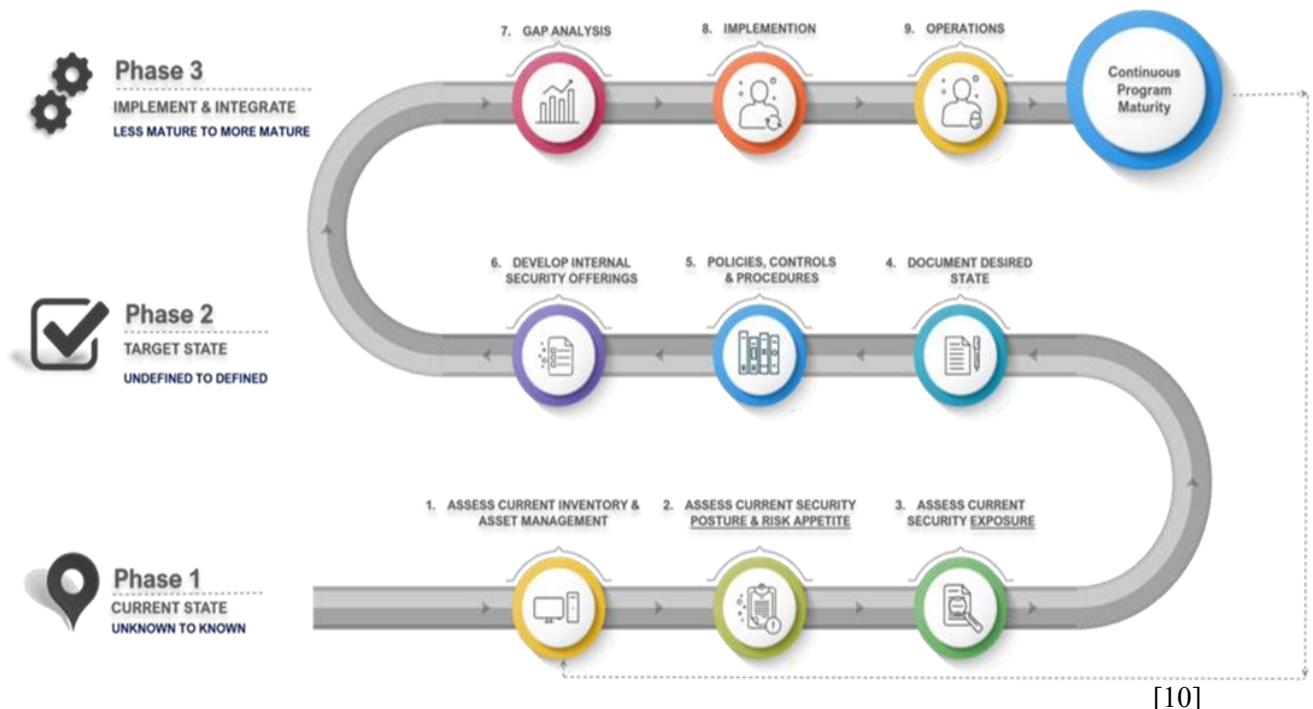


Figure 6: Méthodologie pour développer un programme de sécurité

4.2. Objectif de Blue Team :

- Équipes de sécurité défensive
- Améliorer la posture de sécurité de l'organisation
- Identifier les intrusions
- Réponse aux incidents
- Analyse des logiciels malveillants

4.3. Les tâches d'une Blue Teaming

- La réalisation d'une analyse de l'empreinte numérique de l'organisme.
- La mise en oeuvre et le maintien de solution SIEM afin de pouvoir enregistrer et logger toute activité sur le réseau et le système.

- Surveiller la partie sécurité sur l'hôte et réseau.
- Analyse les risques par rapport à un autre infrastructure, un autre contexte technique et organisationnel.
- Threat Hunting.
- Durcissement réseaux et systèmes.
- Sensibilisation.

5. Comparaison entre Blue Teaming, Red Teaming et Pentest

Le test d'intrusion s'agit d'une attaque simulée d'un système informatique qui cherche des faiblesses de sécurité et peut potentiellement accéder aux fonctions et aux données de l'ordinateur. Il peut aider à déterminer si un système est vulnérable à une attaque, si les différences sont suffisantes et quelles défenses le test a mise en échec. Il existe plusieurs approches pour réaliser un pentest, parmi ces approches on trouve les approches Red Team sont des professionnels de la sécurité offensive c'est-à-dire les experts qui tentent d'attaquer les défenses de cybersécurité d'une organisation et Bleu Team sont les professionnels de la sécurité défensive c'est-à-dire des experts chargés de maintenir les défenses du réseau interne contre toutes les cyberattaques et menaces. Ces approches consistent effectivement à pouvoir effectuer un test d'intrusion approfondie qu'un test d'intrusion classique et traditionnelle avec un durée du temps beaucoup plus lent. Mais cela ne va pas forcément être toujours une équipe contre une équipe on puisse avoir les deux équipes travaillent en parfaite harmonie pour pouvoir mieux sécuriser le système d'information. Le Red Teaming simule des attaques contre les Blue Teaming pour tester l'efficacité de la sécurité du réseau et cette approche collaborative fournit une solution de sécurité holistique garantissant des défenses solides.[17]

6. L'analyse des Leaks [4]

Le manque de sensibilisation et de connaissances sur les concepts de sécurité constitue une plus grande menace pour le public. Le piratage, la fuite et la violation des données sont redoutables. Les cybercriminels parviennent à récupérer des données sensibles (identifiants, e-mail et mot de passe) par une attaque contre un site internet qui possède une vaste base de données.

Les Leaks représentent des fuites de données accessibles sur internet en public ou en vente libre. Un des plus importants pour une Blue Team est de faire une veille continue sur les Leaks des organismes.

6.1.Les causes de la fuite de données

La fuite de données revêt différentes formes. On retrouve d'ailleurs deux terminologies distinctes pour illustrer cette diversité :

- **Le Data Breach** : la violation (cyberattaque par exemple). L'attaquant met en place des mécanismes pour sciemment dérober les data de l'entreprise.
- **Le Data Leak** : La compromission des données est fait suite à un comportement à risque de la part d'un collaborateur ou encore une vulnérabilité déjà présente dans le système

6.2. Attaque de Phishing

a. Définition

Le phishing ou hameçonnage (le vol des données sensibles) est un type d'attaque d'ingénierie sociale dans laquelle les cybercriminels tentent d'inciter les utilisateurs à fournir des informations sensibles et des renseignements personnels telles que leurs noms d'utilisateur et leurs mots de passe sur un faux site Web, dont l'apparence est identique à celle du site légitime. Cette technique frauduleuse est généralement effectuée par usurpation d'adresse électronique ou par messagerie instantanée qui semblent provenir d'une source légitime, comme une plateforme de médias sociaux ou une banque. En utilisant des courriels, l'attaquant distribue des liens malveillants ou des pièces jointes qui peuvent exécuter une variété de fonctions, y compris l'extraction d'informations d'ouverture de session ou d'information sur les comptes des victimes. Ils peuvent vous demander de cliquer sur un lien ou de saisir vos identifiants de connexion pour vérifier votre compte. L'information est ensuite utilisée pour accéder à des comptes importants et peut entraîner un vol d'identité et des pertes financières. Pour protéger contre les attaques de phishing, il est important d'être prudent lorsque vous cliquez sur des liens ou entrez vos identifiants de connexion sur les plateformes de médias sociaux. Vérifiez toujours la source ou la publication du message pour vous assurer qu'il est légitime. Si vous avez besoin d'éclaircissements, contactez l'équipe d'assistance de la plateforme de médias sociaux pour vérifier l'authenticité du message.

Les messages d'hameçonnage réussis, habituellement présentés comme provenant d'une entreprise bien connue, sont difficiles à distinguer des messages authentiques. Un courriel de phishing peut comprendre des logos d'entreprise et d'autres graphiques et données d'identification recueillis auprès de l'entreprise qui fait l'objet d'une fausse représentation. Les liens malveillants dans les messages de phishing sont généralement conçus pour donner

l'impression qu'ils vont à l'organisation usurpée. L'utilisation de sous-domaines et d'URL mal orthographiés (typosquatting) sont des astuces courantes, tout comme l'utilisation d'autres techniques de manipulation de liens.

Le phishing exploite les faiblesses de la sécurité Web actuelle. Les tentatives pour faire face au nombre croissant d'incidents d'hameçonnage comprennent la législation, la formation des utilisateurs, la sensibilisation du public et les mesures techniques de sécurité.

b. Types de phishing

- **Le spear phishing** : est dirigé vers des individus ou des entreprises spécifiques. Les courriels envoyés semblent authentiques car ils utilisent des informations précises. Les messages peuvent comprendre des références à des collègues ou à des cadres de l'organisation de la victime, ainsi que l'utilisation du nom, de l'emplacement ou d'autres renseignements personnels de la victime.
- **Les attaques de whaling** ciblent spécifiquement les cadres supérieurs au sein d'une entreprise, souvent dans le but de voler de grosses sommes d'argent. Les cybercriminels font des recherches détaillées sur leurs victimes pour créer un message authentique. Souvent, la victime est un employé ayant la capacité d'autoriser des paiements. Le message d'hameçonnage semble être un ordre d'un cadre supérieur en vue d'autoriser un paiement important à un fournisseur. La victime, dupée, paye en fait les cybercriminels.
- **Le pharming** est un type d'hameçonnage qui redirige les utilisateurs d'un site légitime vers un site frauduleux et les amène à utiliser leurs identifiants de connexion pour tenter de se connecter au site frauduleux.
- **Le clone phishing** consiste à faire une copie - ou clone - du courriel légitime en remplaçant un ou plusieurs liens ou fichiers joints par des liens malveillants ou des pièces jointes malveillantes. Comme le message semble être une copie du courriel légitime d'origine, les victimes peuvent souvent être amenées à cliquer sur le lien malveillant ou à ouvrir la pièce jointe malveillante. Cette technique est souvent utilisée par les attaquants qui ont pris le contrôle du système d'une autre victime.
- **Le phishing de type evil twin Wi-Fi** est une attaque qui crée un point d'accès Wi-Fi qui ressemble à un point d'accès légitime. Lorsque les victimes se connectent au réseau Wi-Fi jumeau, les attaquants ont accès à toutes les transmissions envoyées vers ou depuis les dispositifs de la victime, y compris les ID utilisateur et les mots de passe.

- **Le vishing (voice phishing)**, est une forme d'hameçonnage qui utilise un logiciel de synthèse vocale. Cette technique consiste à laisser des messages vocaux censés informer la victime d'une activité suspecte sur un compte bancaire ou de crédit. La victime est alors sollicitée pour composer un numéro et confirmer son identité. En réalité, elle la compromet en donnant des informations personnelles à une source malveillante.
- **Le phishing par SMS, ou SMShing**, utilise les textos pour convaincre les victimes de divulguer les informations d'identification de compte ou d'installer des logiciels malveillants.



[20]

Figure 7: Catégories de phishing

Il peut donc être intéressant de savoir si des cybercriminels sont parvenus à dérober les données et de protéger contre la violation des données, c'est le but de plusieurs site Web

7. Présentation du SOC [7]

7.1. Définition de Security Operations Center (SOC)

Security Operations Center (SOC), désigne dans une entreprise l'équipe en charge d'assurer la sécurité de l'information. Il se compose des personnes et des équipements techniques. Le SOC est une plateforme chargée de surveiller et d'analyser les réseaux et les systèmes d'une organisation. C'est un centre de supervision et d'administration de la sécurité du système d'information pour détecter les menaces, les comportements anormaux et les vulnérabilités de sécurité en utilisant une variété d'outils de collecte, de corrélation d'événements et d'intervention à distance, tels que les systèmes de gestion des informations et des événements de sécurité (SIEM) qui est l'outil principal du SOC qui tente à collecter et analyser les données provenant de diverses sources, telles que les journaux, le trafic réseau et d'autres sources.

7.2. Objectif d'un SOC

L'objectif de SOC est de détecter, analyser et remédier aux menaces et incidents de cyber sécurité par la surveillance continue à l'aide de solutions technologiques et d'un ensemble de démarches. Il surveille et analyse l'activité sur les réseaux, les serveurs, les terminaux, les bases de données, les applications, les sites Web et d'autres systèmes.

7.3. Fonctionnement d'un SOC

Le SOC surveille les données de sécurité générées dans l'ensemble de l'infrastructure informatique de l'organisation, des systèmes et applications hôtes au réseau et aux dispositifs de sécurité, tels que les pare-feux et les solutions antivirus.

En combinant une série d'outils avancés (Le SIEM (Security Information and Event Management), La technologie de machine Learning, le scanner de vulnérabilité, la Threat Intelligence ainsi que les outils de visualisation et d'alerte et les compétences d'experts en cyber sécurité notamment de spécialistes qui installent, intègrent les outils et paramètrent les différents systèmes de supervision de la sécurité, le SOC remplit les fonctions essentielles suivantes :

- Surveillance, détection, enquête et traitement des alertes de sécurité.
- Gestion de la réponse aux incidents de sécurité, y compris l'analyse des logiciels malveillants et les enquêtes médico-légales.
- Gestion des données sur les menaces (enregistrement, création, traitement et diffusion).
- Gestion des vulnérabilités basée sur les risques (y compris la priorisation des correctifs).
- Suivi des menaces.
- Gestion et maintenance des équipements de sécurité.
- Développement de données et d'indicateurs pour le reporting /la gestion de la conformité.

7.4. Les avantages de Security Operations Center (SOC)

L'intégration d'un système de surveillance tel que le SOC offre aux entreprises de nombreux avantages puisque le principal avantage du SOC est d'améliorer la détection des incidents de sécurité grâce à une surveillance et une analyse continue de l'activité du réseau tout en tirant parti des données de renseignement électronique. L'analyse permanente d'activité sur les réseaux d'entreprise permet l'identification rapide des attaques et d'une capacité à les faire échouer avant la survenue de dommages graves. Cette capacité est importante, car le temps est

l'un des éléments les plus critiques lorsqu'il s'agit de répondre efficacement aux incidents de cyber sécurité.

Les principaux avantages d'un SOC sont les suivants :

- Surveillance et analyse permanentes des activités suspectes.
- Amélioration des délais de réponse aux incidents et des procédures de gestion des incidents.
- Réduction du temps entre le point d'intrusion et la détection.
- Des ressources logicielles et matérielles centralisées pour permettre une approche holistique de la sécurité.
- Communication et collaboration efficaces pour identifier et classer les tactiques et techniques de l'adversaire, par exemple en utilisant le cadre ATT&CK de MITRE.
- Réduire les coûts liés aux incidents de sécurité.
- Visibilité et contrôle accrus des opérations de sécurité.
- Traçabilité fiable des données utilisées dans les activités de cyber sécurité post-mortem.

7.5. Les défis d'un Security Operations Center (SOC) [11]

Le rôle du SOC devient de plus en plus complexe car il gère tous les aspects de la sécurité numérique d'une organisation. Pour de nombreuses organisations, la création et le maintien d'un SOC pleinement fonctionnel peuvent s'avérer difficiles.

Les défis classiques sont :

- **Le volume :** Le plus grand défi pour les organisations est le volume des alertes de sécurité, dont beaucoup nécessitent à la fois des systèmes avancés et des ressources humaines pour classer correctement les menaces, les hiérarchiser et y répondre. Avec un grand nombre d'alertes, certaines menaces peuvent être mal classées ou ne pas être détectées du tout. Ce risque met en évidence la nécessité de disposer d'outils de surveillance avancés et de capacités d'automatisation, ainsi que d'une équipe dédiée d'experts en cyber sécurité.
- **La complexité :** La nature des affaires, la flexibilité du lieu de travail, l'utilisation croissante de la technologie du cloud et d'autres questions ont rendu plus complexe la protection d'une entreprise et la réponse aux menaces. Aujourd'hui, des solutions relativement simples telles que les pare-feux ne suffisent plus, en tant que mesure autonome, à protéger l'entreprise contre ses adversaires numériques. Une sécurité plus efficace nécessite une solution combinant

technologie, personnel et processus, ce qui peut être difficile à organiser, à mettre en œuvre et à exploiter.

- **Le coût :** La mise en place d'un SOC demande beaucoup de temps et de ressources. Le maintenir peut-être encore plus difficile, car le paysage des menaces est en constante évolution et nécessite des mises à jour et des mises à niveau fréquentes, ainsi qu'une formation continue pour le personnel de cyber sécurité. En outre, peu d'entreprises disposent en interne des compétences nécessaires pour comprendre suffisamment bien le paysage actuel des menaces. De nombreuses entreprises s'associent à des fournisseurs de sécurité externes pour obtenir des résultats fiables sans nécessiter d'importants investissements internes en technologie ou en ressources humaines.

7.6. Modèles du SOC

- **SOC virtuel :** Ce type de SOC ne dispose pas d'installations spécifiques et les membres de l'équipe sont activés en cas d'alarme ou d'incident critique, un peu comme les pompiers.
- **SOC dédié :** comme son nom l'indique, nécessite une installation en interne et une équipe entièrement dédiée.
- **SOC distribué ou cogéré :** Le SOC est cogéré lorsqu'il est géré avec un MSSP (Managed Security Service Provider)
- **SOC de commande :** il coordonne les autres SOC, fournit les renseignements sur les menaces.
- **Fusion ou orienté Threat Intelligence :** Il combine des fonctions traditionnelles avec le cyber intelligence, l'apprentissage automatique et l'intelligence artificielle (IA) pour établir le profil des agresseurs potentiels.
- **Hybride :** certaines opérations sont gérées par des équipes externes (analyses suite à un incident, cyber veille, etc.) et des collaborateurs en interne se chargent du support de niveau 3 comme la gestion des incidents graves ou critiques
- **Inclus dans un NOC (Network Operation Center) :** le NOC prend en charge les tâches du Security Operation Center et d'autres tâches critiques en se chargeant de maintenir le réseau, stocker, virtualiser et sauvegarder ces données...

7.7. Les composants d'un SOC

- **Ressources Humaines :** Un SOC requiert des professionnels de la sécurité qualifiés pour enquêter sur les incidents de sécurité, intervenir dans les incidents et les analyses médico-légales, et aider à maintenir une organisation à flot en cas de violation des données. Ces experts en sécurité sont chargés de fournir des informations précises à la direction afin

que l'organisation puisse prendre des décisions prudentes, par exemple s'il faut fermer des systèmes critiques pour les analyser ou arrêter les fuites de données et protéger l'organisation contre les cyberattaques.

- **Les processus et les procédures :** Les processus et procédures au sein d'un SOC définissent clairement les rôles et les responsabilités ainsi que les procédures de surveillance. Ces procédures comprennent des processus opérationnels, technologiques et analytiques. Ils décrivent les mesures à prendre en cas d'alarme ou de violation de la sécurité, y compris les procédures d'escalade, les procédures de notification et les procédures de réponse à une violation de la sécurité. En général, les SOC devraient s'efforcer de mettre en place les procédures de sécurité suivantes avant de commencer :

- Procédures de surveillance
- Procédure de notification
- Procédure d'escalade
- Procédures de journalisation
- Procédures de journalisation des événements
- Contrôle de la conformité
- Procédure de notification

Le plus important est le processus qui relie les différentes étapes entre elles et qui garantit que la transition des différentes tâches est clairement définie d'un jour à l'autre et d'une personne à l'autre. En cas d'attaque réelle, chacun au sein du SOC connaît donc ses responsabilités et sait comment s'insérer dans le processus de bout en bout.

- **La technologie :** Un SOC doit être équipé d'un ensemble d'outils technologiques qui fournissent une image correcte de l'environnement de sécurité de l'organisation. Le SOC est généralement basé sur un système de gestion des informations et des incidents de sécurité ou "Security Incident and Event Management (SIEM)", qui collecte et corrèle les données et les événements liés à la sécurité.

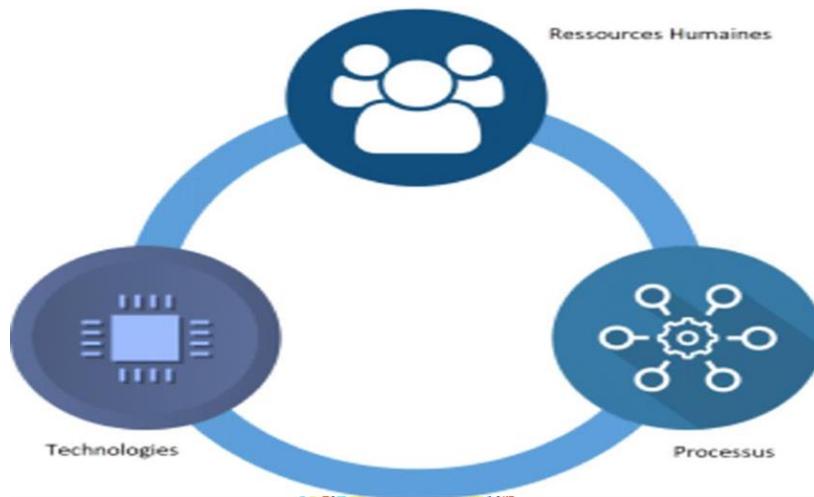


Figure 8:Les composants d'un SOC [14]

8. Les niveaux de SOC

Les équipes sont donc divisées en trois parties :

- **Le Tiers 1 (ou niveau 1) :** Il s'agit d'une équipe d'analystes dont la mission est de trier et de qualifier les événements avant de transmettre ceux qui nécessitent une plus grande attention au niveau 2. En fait, le niveau 1 effectue une analyse des événements en temps réel, qui doit être brève et basée sur des scénarios prédéfinis afin d'effectuer une première évaluation. La politique de sécurité en place dicte la durée maximale de l'analyse (généralement moins d'un quart d'heure). Tout événement dont l'étude n'est pas terminée à ce moment-là est envoyé au Tiers.
- **Le Tiers 2 (ou niveau 2) :** Cette équipe reçoit les alertes de niveau 1 et entame une analyse plus approfondie afin de déterminer plus précisément l'origine et les conséquences de l'événement en cours. Contrairement au niveau 1, ces équipes ne doivent pas travailler en temps réel. Elles peuvent donc consacrer plus de temps à l'examen des alertes et à la détermination de l'existence d'un incident. Ils rédigent également les procédures de traitement des incidents pour le niveau 1 et contribuent à améliorer les règles d'association qui permettent au niveau 1 de déclencher des alertes pertinentes.
- **Le Tiers 3 (ou niveau 3) :** Ce tiers diffère légèrement des autres : Premièrement, il n'existe pas dans tous les SOC. Comme son objectif est plutôt de prévenir les incidents avant qu'ils ne se produisent, son rôle est similaire à celui du CSIRT. Dans certaines entreprises, le CSIRT est responsable de ce domaine. Il s'agit donc d'un niveau d'expertise plus profond que celui des niveaux 1 et 2. Au niveau 3, des activités médico- légales ou de rétro-ingénierie

peuvent être menées afin d'analyser un incident autant que possible et de prédire les événements futurs. En cas d'attaque inconnue, les niveaux 1 et 2 ne sont pas alertés, mais la surveillance de la menace incombe au niveau 3.

- **le SOC Manager :** Il est responsable de l'ensemble des trois niveaux du SOC et reporte directement au RSSI ou au DSI (en fonction de l'organisation de l'entreprise).

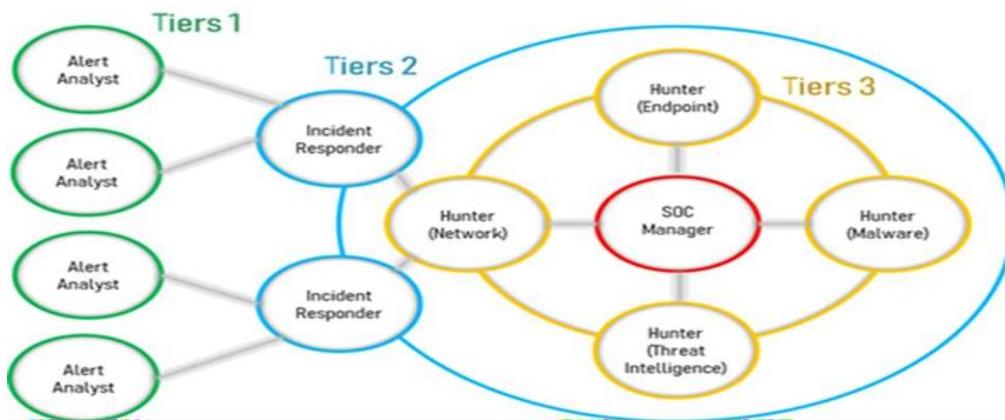


Figure 9: Les niveaux de SOC [18]

9. Workflow de la data dans un SOC

Un soc efficace est une cible ambitieuse et une trajectoire qu'il faut construire étape par étape. Le Workflow montre comment traiter un événement ou les contrôler, des plausibilités sont effectuées, quand contacter le superviseur du SOC et quand faire la documentation nécessaire, l'escalade ou le transfert à un autre département ou division.

9.1. Surveillance

Un SOC s'appuie en première lieu sur la surveillance des systèmes opérationnels, une analyse des journaux du trafic, des actions des utilisateurs et le tri des informations selon des critères de pertinence de l'événement afin de donner une synthétique et exploitables aux analystes. Toutes ces informations vont pouvoir récoltés à travers toutes les différentes sources c'est-à-dire l'activité réseau, les services, les analyses de vulnérabilité. Le SOC collecte les logs pour rééditer chaque composant du système d'information, il analyse les flux pour avoir une meilleure vision des interactions point à point entre applications et entre utilisateurs pour identifier les vulnérabilités existantes qui pourrait être exploitée par un attaquant. Cette activité est à la charge d'un analyste dit de niveau 1. Il s'agit d'une équipe d'analystes (1 ou 2 agents de niveau 1) ce sont généralement les nouveaux dont la mission est d'effectuer une analyse des événements en temps réel (rapide) avant de faire remonter au tier 2 en apprenant par la pratique

et avec l'aide de la base de connaissances et de leurs collègues. Celle-ci doit être brève et basée sur des scénarios prédéfinis.

Lors de processus de traitement des événements de niveau 1, l'analyste doit suivre les étapes suivantes.

- S'il est un événement commun elle le résoudre comme d'habitude et passe au traitement des événements processus de dotation.
- S'il est un événement connu mais rare elle cherche dans les connaissances base de connaissance pour la solution ou la remédiation et agir en conséquence puis elle passe au traitement des événements processus de dotation.
- S'il est un événement nouveau ou inconnu il le remonte au niveau 2.
- Si non elle contact le chef d'équipe de SOC.

9.2. Corrélation

Si l'analyste niveau 1 ne peut effectuer un tri et communiquer de manière exploitable l'alerte au processus de gestion des incidents, une analyse complémentaire s'avère nécessaire les événements complexes et les comportements suspects peuvent être transmis à une d'experts qui peut mener une enquête poussée sur la réalité d'une attaque et comprendre son mode opératoire donc il doit faire appel à un niveau 2 (1 agent de niveau 2) qui peuvent traiter la plupart des événements par expérience , connaissent bien les flux de travail et autres procédures et dans une certaine mesure analysent les événements en profondeur. Cette même équipe peut aussi faire une analyse proactive de système pour traquer les incidents c'est le fameux street hunting ou l'analyste se met dans la peau du chasseur à la recherche des attaques les experts peuvent s'appuyer sur une quantité d'information externes, les échanges avec d'autres équipes de sécurité, l'analyse de Dark Web et nombreuses sources ouvertes. Une nouvelle vulnérabilité sur un protocole de communication. Selon l'événement l'agent doit effectuer quelques tâches :

- S'il est un événement courant il le résoudre comme d'habitude et fini par traitement des événements processus de dotation.
- S'il est un événement connu mais rare il cherche dans la base de connaissances la solution ou la remédiation et agir en conséquence et passa au traitement des événements processus de dotation.
- Si non il analyse l'événement en termes de cause, d'impact, de gravité, de mise à jour du ticket et de la KB. Puis il créer une idée et une stratégie de résolution de problème

- S'il est nécessaire d'impliquer des autres départements, l'agent doit créer un ticket dans le système de tickets des autres départements.
- Si le problème est résolu, il demande des informations détaillées sur la manière dont le problème a été résolu puis il va créer, mettre à jour, réviser ou documenter les tickets, KB etc..., et la dernière étape c'est le traitement des événements processus de doture.
- Si le problème n'est pas résolu l'agent doit suivre et pousser et refait la résolution.
- Si non l'agent résolve le problème seul ou avec ses collègues de SOC.
- Si le problème est résolu l'agent doit créer, mettre à jour, réviser ou documenter les tickets et KB etc. Enfin, le traitement des événements processus de doture.
- Sinon, si le système est nouveau ou il est inconnu, il faut le remonter au niveau 3. Sinon, il contact le chef d'équipe et le superviseur du SOC.

9.3. Détection

Les informations sont corrélées et bien sûr grâce à différents indicateurs de compromission à des règles de détection réduite de la création de l'apprentissage des modèles comportementaux on peut arriver à identifier les comportements inhabituels mais caché à ce moment –là une fois qu'on est passé par la corrélation de la détection on va pouvoir identifier les vraies menaces, des comportements suspects. C'est un niveau d'escalade ou de complexité d'un événement nécessaire le soutien d'un expert en la matière (SME).

Les tâches de l'analyste niveau 3 sont :

- S'il est un événement courant il le résoudre comme d'habitude et fini par traitement des événements processus de doture.
- S'il est un événement connu mais rare il cherche dans la base de connaissances la solution ou la remédiation et agir en conséquence et passa au traitement des événements processus de doture.
- Si non il analyse l'événement en termes de cause, d'impact, de gravité, de mise à jour du ticket et de la KB. Puis il doit impliquer les experts en la matière (PME) et créer une idée et une stratégie de résolution des problèmes. Informer / discuter avec les départements.
- S'il est nécessaire d'impliquer des autres départements, l'agent doit créer un ticket dans le système de tickets des autres départements.
- Si le problème est résolu, il demande des informations détaillées sur la manière dont le problème a été résolu puis il va créer, mettre à jour, réviser ou documenter les tickets, KB etc..., et la dernière étape c'est le traitement des événements processus de doture.

- Si le problème n'est pas résolu l'agent doit suivre et pousser et refait la résolution.
- Si non l'agent résolve le problème seul ou avec ses collègues de SOC PME, département.
- Si le problème est résolu l'agent doit créer, mettre à jour, réviser ou documenter les tickets et KB etc. Enfin, le traitement des événements processus de dotation.
- Si non si le système est nouveau ou inconnu il faut contacter le CSIRT externe processus. Si non il contact le chef d'équipe et le superviseur du SOC.

9.4. Priorisation

Là en fait c'est le travail le plus du c'est de pouvoir retrouver vraiment et identifier les menaces de manière édile de pouvoir les prioriser selon leur sévérité et selon leur pertinence parce que derrière on peut retrouver beaucoup de faux positifs mais aussi des faux négatifs et ça c'est le pire cauchemar au niveau d'un SOC il y a toute une stratégie pour le faire.

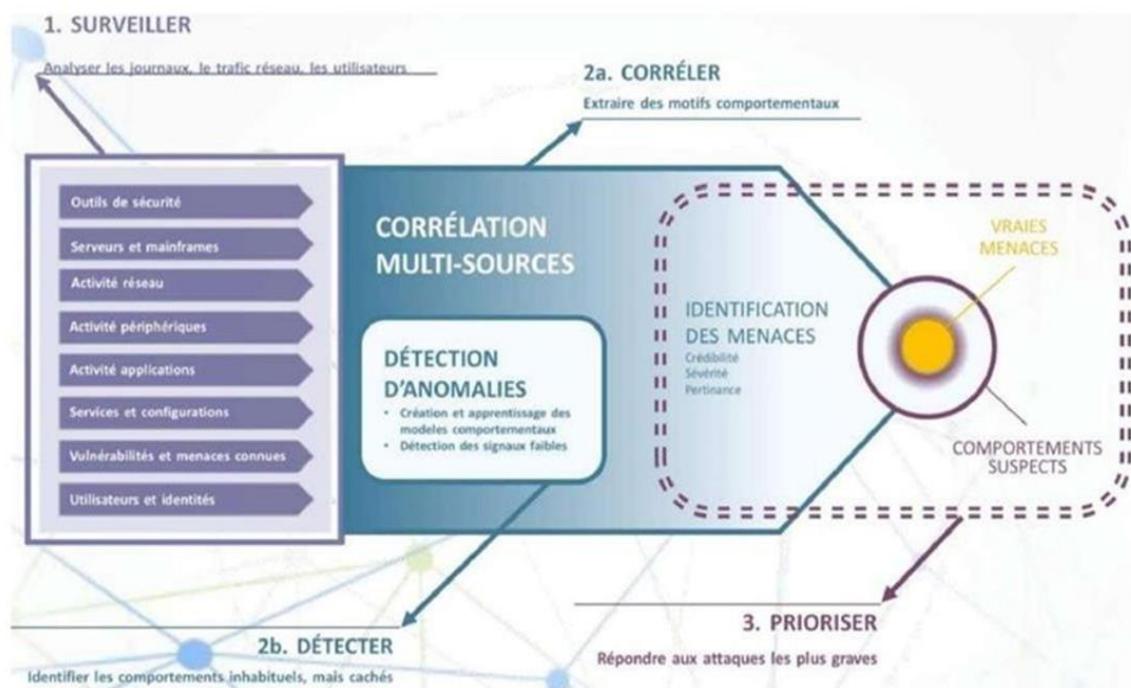


Figure 10: Workflow de la data dans un SOC [3]

10. Conclusion

L'objectif principale de cet état d'art est de donner un aperçu sur le SOC et le Workflow de la data. Nous avons présenté également le Pentest, Blue Teams, Red Teams et la comparaison entre eux. Une dernière partie a été réservé pour la fuite des données et l'attaque de phishing.

Chapitre 3 :

Mise en place du SOC

1. Introduction

Après avoir présenté l'importance de la mise en place d'un SOC au sein de l'entreprise moderne, et après avoir étudié les différences entre Blue Teaming, Red Teaming et Pentest, nous allons passer à présenter le cadre dans lequel, notre projet sera mis en place.

2. Mise en place du Système

Pour la mise en place du système, nous aurons besoins des outils matériels et des outils logiciels.

✓ Partie matérielle :

- PC victime
- PC attaquant dispose
 - RAM: 20 Go
 - Disque Dur: 512 GB SSD
 - Processeur: i7
 - OS: Windows 11

✓ Partie logicielle

- Nous avons téléchargé et installé VMware Workstation 16 pro sur notre machine réelle
- Nous avons téléchargé l'image de Ubuntu de version 64 et l'installé sur VMware
- Nous avons installé DeTECT et PyPhisher sur notre machine virtuelle Ubuntu

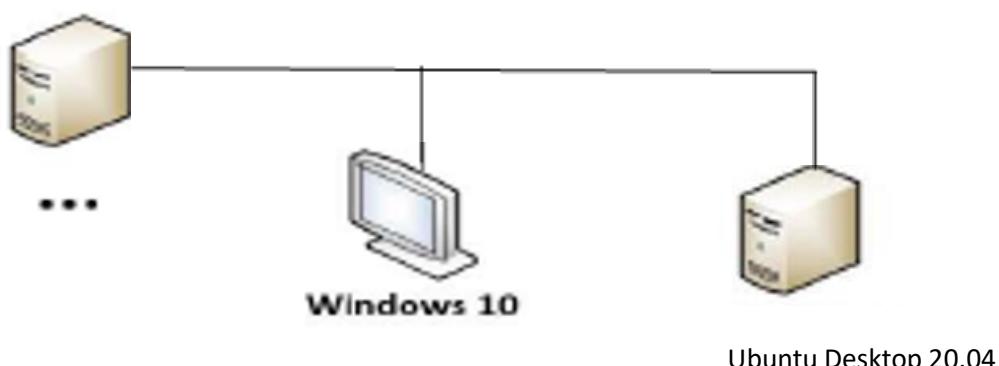


Figure 11: Le système proposé

3. VMware Workstation

VMware Workstation est un outil de virtualisation de poste de travail créé par la société VMware, il peut être utilisé pour mettre en place un environnement de test pour développer de nouveaux logiciels, ou pour tester l'architecture complexe d'un système d'exploitation avant de l'installer réellement sur une machine physique.



Figure 12 : Logo VMware Workstation

4. Ubuntu

C'est un système d'exploitation libre et open-source. Son nom trouve son origine en Afrique du Sud et est issu du mot bantou « Ubuntu » qui pourrait être traduit par « je suis ce que je suis grâce à ce que nous sommes tous ».



Figure 13: Logo Ubuntu

5. Mitre ATT&CK

5.1. Présentation

Le MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) est un des frameworks (Matrice) le plus connus du MITRE c'est en fait une base de documentation

comme base de données des différentes tactiques, techniques des adversaires et les procédures contradictoires qui vont être utilisés par les groupes des menaces autrement appelé les menaces persistantes avancées (APT).

MITRE ATT&CK est une base de connaissance accessibles à l'échelle mondiale sur TTPs et un modèle de comportement des cyber-adversaires. Cette base de connaissance est utilisée comme fondement pour le diagnostic d'attaque (la criminalistique) et l'atténuation (la réponse à l'intrusion) en reflètent les différentes phases de cycle de vie des attaques d'un adversaire et les plateformes qu'il est connu pour cibler elle est utilisée pour le développement de modèles de menaces de méthodologies spécifiques dans le secteur privé, au sein de gouvernement, et dans la communauté des produits et services de cyber sécurité.

ATT&CK fournit une taxonomie commune pour la défense et l'attaque et devenu un outil conceptuel utile dans de nombreuses disciplines de la cyber sécurité pour transmettre des renseignements sur les menaces.

Le MITRE ATT&CK est un point de départ pour effectuer de la threat intelligence pour voir l'image en grand pour ceux qui vont pouvoir essayer l'analyse. Mais c'est aussi un des points les plus importants à connaître pour bâtir une ligne défensive efficace il permettre aussi de pouvoir déterminer ou d'effectuer des analystes financiers de manière plus précise et conc de pouvoir cibler les indicateurs de compromission non pas traditionnellement parlant mais orienté TTP orienté scénario et donc orienté événement.[1]

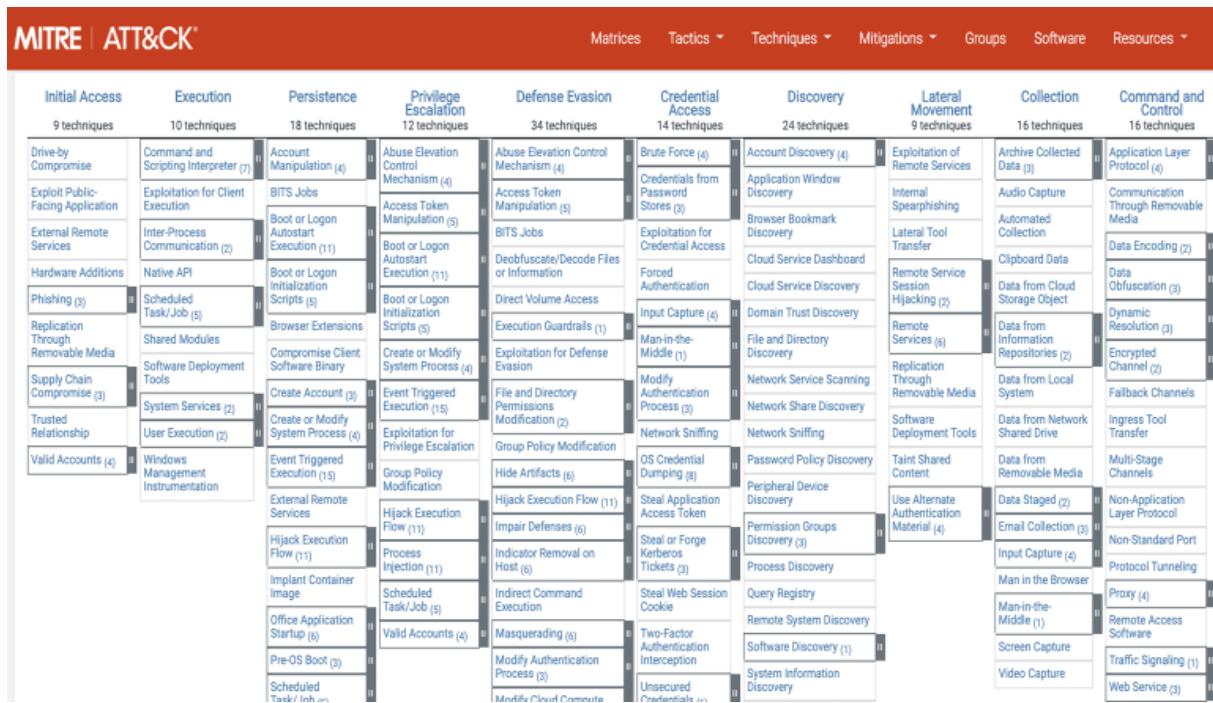
Le site officiel de MITRE ATT&CK est : <https://attack.mitre.org/>

5.2. Composants et principe de fonctionnement [12]

Le MITRE ATT&CK est un modèle comportemental qui se compose des éléments de base suivants :

- **Tactique** : Désigne les objectifs tactiques d'un adversaire pendant une attaque, dont le code est TAXXXX où XXXX est une série de chiffre
- **Technique** : Les moyens utilisées par les adversaires pour atteindre ses objectifs tactiques. Le code est TXXXX.
- **Sous-technique** : Les moyens les plus spécifiques utilisées pour atteindre les objectifs tactiques avec un code TXXXX.YYY
- **Procédure** : Utilisation documentés de procédures par l'adversaire de technique.

La matrice ATT&CK permet de représenter la relation entre ces éléments. En effet, Le MITRE ATT&CK pour un système d'entreprise décompose une attaque informatique à un ensemble des tactiques (14 tactiques : 12 dans la matrice classique et 2 complémentaires issues de la matrice pré-attaque PRE) qui forment les 14 colonnes. Chaque tactique ou colonne contient une série des techniques dont l'adversaire peut utiliser une technique unique pour atteindre son objectif. En outre, certaines techniques peuvent être décomposées en sous-techniques pour détailler la réalisation de ces comportements.



[2]

Figure 14: LA matrice ATT&CK pour le système d'entreprise

Accès initial

9 techniques

Compromis au volant	
Exploiter l'application publique	
Services à distance externes	
Ajouts matériels	
Hameçonnage (3)	
RéPLICATION via des supports amovibles	
Compromis de la chaîne d'approvisionnement (3)	
Relation de confiance	
Comptes valides (4)	

Figure 15: La tactique Accès initial avec ces techniques

Accès initial

9 techniques

Compromis au volant	
Exploiter l'application publique	
Services à distance externes	
Ajouts matériels	
Hameçonnage (3)	<ul style="list-style-type: none"> Pièce jointe de harponnage Lien de harponnage Spearphishing via le service
RéPLICATION via des supports amovibles	
Compromis de la chaîne d'approvisionnement (3)	<ul style="list-style-type: none"> Compromettre les dépendances logicielles et les outils de développement Compromettre la chaîne d'approvisionnement des logiciels Compromettre la chaîne d'approvisionnement du matériel
Relation de confiance	
Comptes valides (4)	<ul style="list-style-type: none"> Comptes par défaut Comptes de domaine Comptes locaux Comptes infonuagiques

Figure 16: les sous-techniques de la tactiques Accès initial

5.3. Apport

Sachant que les attaquants peuvent différer mais les modes opératoires vont rester stables à travers le temps.

- Le framework du MITRE nous permet de pouvoir analyser et suivre l'évolution des TTP c'est-à-dire que fur et à mesure de l'avancement de ces différentes techniques, tactiques et procédures il faut savoir aussi que le framework va aussi avoir évoluer grâce à un travail communautaire extrêmement pointus alors du coup pour suivre un petit peu les tendances en matière de ttp il faudra suivre ce framework.
- Il va aussi nous permettre de pouvoir comparer les ttps des différents attaquants, différents acteurs de menaces afin de trouver des points communs ou encore tout simplement pouvoir différencier des groupes ou des quelques groupes.
- Il va aussi nous permettre d'hiérarchiser la détection et l'analyse des incidents en ciblant les approches les plus critiques pour notre organisme.
- Pour les Red Team il va leur permettre aussi d'effectuer ce qu'on appelle de l'Adversary Emulation ou de l'émulation des menaces vu qu'on va avoir des modes opératoires tout près il nous faudra juste à ce moment-là les concrétiser grâce à différents outils.
- Il nous permet aussi de créer un espace de partage ses acquis les collaboratif où le renseignement sur les menaces nous y pouvons partager plus que des incidents de compromission mais également des ttp modéliser. Les indicateurs de compromission sont transmis et se repositionnent dans un contexte et une succession d'actions informant sur les décisions prises par l'attaquant une fois qu'il a compromis les systèmes d'information.

6. Mitre DeTTECT

6.1. Présentation

DeTT&CT signifie Detect Tactics, Techniques & Combat Threats. Ce cadre a été créé au Cyber Defense Center de Rabobank et est développé et au moment de la rédaction maintenu par Marcus Bakker et Ruben Bouman. L'outil DeTTECT fait partie des outils les plus intéressants. Il permet de pouvoir analyser la qualité des data sources qu'on récolte pour pouvoir les mapper avec la matrice de Mitre ATT&CK, ça permet de détecter ce qu'on arrive à surveiller comme TTP.

Le but de DeTT&CT est d'aider les équipes SOC autrement dit les Blu Teaming à comparer la qualité de leurs data sources aux matrices Mitre ATT&CK pour noter et comparer la qualité de la source de journalisation des données, la couverture de visibilité et la couverture de détection. En utilisant ce cadre, les équipes bleues peuvent rapidement détecter les lacunes dans la couverture de détection ou de visibilité et hiérarchiser l'ingestion de nouvelles sources de journaux.

6.2. Composants et principe de fonctionnement

Les différents composants de DeTT&CT :

- un outil Python (DeTT&CT CLI)
- Fichiers d'administration YAML
- l'éditeur DeTT&CT (pour pouvoir gérer les différents fichiers YAML qu'on va pouvoir analyser)
- tableaux de scorping pour aider à évaluer l'environnement : les détections, les sources de données et la visibilité

DeTT&CT CLI est un script python (dettect.py) qui fonctionne avec six modes différents :

éditeur : démarrer l'interface Web de l'éditeur DeTT&CT

datasource (ds) : mappage et qualité des sources de données

visibilité (v) : cartographie de la couverture de visibilité basée sur des techniques et des sources de données

détection (d) : cartographie de la couverture de détection basée sur des techniques

groupe (g) : mappage des groupes d'acteurs menaçants

générique (ge): inclut:statistiques sur la source de données ATT&CK et mises à jour sur les techniques, les groupes et les logiciels [14]

Le Framework DeTT&CT utilise des fichiers YAML (langage de sérialisation de données lisible par l'homme) pour administrer les sources de données, la visibilité, les techniques et les groupes et pour créer et gérer ces différents fichiers d'administration YAML. Nous pouvons soit utiliser l'interface de ligne de commande, soit lancer l'éditeur.

Les types de fichiers suivants peuvent être identifiés :

- Gestion des sources de données
- Administration technique (visibilité et couverture de détection)
- Gestion des groupes

✓ **Data-sources**

Les data-sources sont les journaux bruts ou les événements générés par les systèmes. Pour les Bleu Team il est important de savoir quelles sources des journaux des données, quelle est la qualité et si elles sont exploitables pour effectuer les analyses des données.

Nous pouvons administrer plusieurs aspects tels que la qualité des données et cette administration des data-sources est stockée dans un fichier Yaml.

✓ **La visibilité**

La visibilité est utilisée dans DeTT&CT pour indiquer si nous disposons de suffisamment de sources de données avec une qualité suffisante.

La visibilité est nécessaire pour :

- Répondre aux incidents
- Exécuter des enquêtes de chasse
- Créer des détections

Pour installer DeTT&CT, nous exécutons les commandes suivantes :[6]

```
git clone https://github.com/rabobank-cdc/DeTTECT.git
```

```
cd DeTTECT
```

```
pip install -r requirements.txt
```

Une fois installé, nous pouvons soit utiliser l'interface de ligne de commande, soit lancer l'éditeur DeTT&CT.

Pour lancer DeTT&CT Editor, nous saisissons la commande suivante :

```
python3 dettect.py editor
```

Puis nous exécutons DeTTECT sur l'adresse <http://localhost:8080/>

Nous pouvons afficher les data sources et les plateformes de manière plus détailler avec la commande suivante :

```
Python3 dettect.py generic -ds
```

Nous allons maintenant convertir ce fichier YAML en un fichier JSON à l'aide de l'outil DeTT&CT CLI et charger ce fichier JSON en tant que couche ATT&CK dans ATT&CK Navigator .

```
python3 dettect.py ds -fd ..//Téléchargements/data-sources-new.yaml -l --health
```

Les drapeaux pertinents pour cette commande sont

-ds: sélectionnez le mode de source de données

-fd: chemin d'accès au fichier YAML d'administration de la source de données-l: générer une couche de source de données pour le navigateur ATT&CK

-l: générer une couche de source de données pour le navigateur ATT&CK

--health : permet de récupérer le fichier et de corriger les différentes erreurs

Nous pouvons générer un fichier YAML d'administration technique basé sur notre fichier d'administration de source de données, ce qui nous donnera des scores de visibilité approximatifs.

```
python3 dettect.py ds -fd ..//Téléchargements/data-sources-new.yaml --yaml
```

-ds: sélectionnez le mode de source de données

-fd: chemin d'accès au fichier YAML d'administration de la source de données

--yaml: générer un fichier YAML d'administration technique avec des scores de visibilité basés sur le nombre de sources de données disponibles

Pour visualiser les scores de visibilité dans une couche ATT&CK Navigator, nous exécutons la commande suivante et chargez le fichier résultant dans ATT&CK Navigator.

```
python3 dettect.py v -ft ..//Téléchargements/techniques-administration-example-all.yaml -l
```

Les paramètres et drapeaux pertinents pour cette commande sont

v: cartographie de couverture de visibilité basée sur des techniques et des sources de données

-ft: chemin du fichier YAML d'administration de la technique

-l: générer une couche de source de données pour le navigateur ATT&CK

7. Mitre D 3FEND

7.1. Présentation

L'agence du renseignement Américaine NSA (La National Security Agency) vient de rendre disponible un nouveau Framework D3FEND « Detection, Denial and Disruption Framework Empowering Network Defense » via le MITRE. Ce dernier établit une terminologie des techniques de défense des réseaux informatiques afin d'éclaircir les relations précédemment non spécifiées entre les méthodes défensives et les méthodes offensives.

Le Framework MITRE D3FEND est un projet complémentaire aux framework de MITRE ATT&CK. Mais, ces deux projets restent très différents. Puisque le framework ATT&CK tente à classer les outils, techniques et les méthodes utilisées par les adversaires pour pénétrer dans les réseaux. Alors que, Le Framework D3FEND est une matrice de connaissances permettant de fournir des informations sur les analyses à effectuer mais aussi les méthodologies défensives face à ces différentes TTP. D3FEND constitue une base de connaissance technique, des contres mesures défensives pour les techniques offensives courant.

Comme l'a expliqué le créateur et cyberingénieur principal chez Mitre Peter Kaloroumakis, qui travaille sur le schéma depuis plusieurs années, « D3FEND combine les langages et les techniques de la bioinformatique et établit une terminologie des techniques de défense des réseaux informatiques afin d'éclaircir les relations précédemment non spécifiées entre les méthodes défensives et offensives ». Comme mentionné dans le communiqué de presse, « D3FEND permet aux professionnels de la cybersécurité de personnaliser les défenses contre des cybermenaces spécifiques, réduisant ainsi la surface d'attaque potentielle d'un système ».[9]

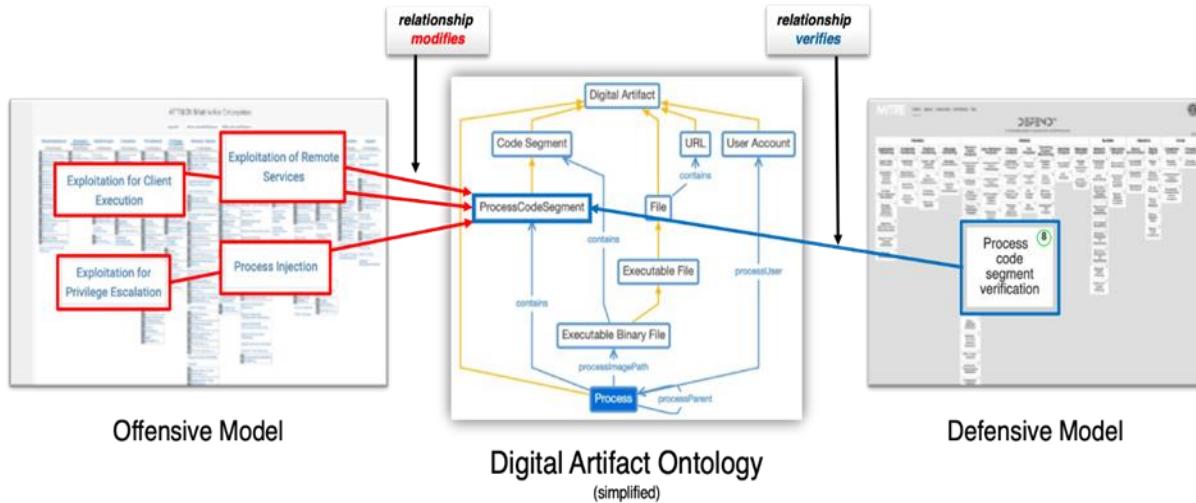


Figure 17: Cartographie par inférence grâce à l'ontologie des artefacts numériques

7.2. Composants et principe de fonctionnement

D3FEND est composé de 3 éléments essentiels.

- Un graphe de connaissances qui résume les méthodes défensives.
- Une série d'interfaces utilisateur pour accéder à ces données.
- Une façon de mettre en correspondance ces mesures avec le modèle d'ATT&CK.

Il existe un point commun entre les méthodologies de défense et les méthodologies d'attaque qui sont les artefacts digitaux c'est-à-dire les traces qu'ils vont être laissés une attaque va pouvoir produire un artefact c'est-à-dire un indicateur de compromission ou un indicateur d'attaque.



Figure 18: Cartographie des techniques offensives et défensives via les artefacts numériques

Le cadre MITRE ATT&CK est divisé en trois matrices (Enterprise, Mobile et ICS), mais pour MITRE D3FEND il n'existe qu'une seule matrice. Les informations de contre-mesures de D3FEND sont organisées de la même manière que la hiérarchie des TTP adverses d'ATT&CK.

La matrice de MITRE D3FEND présente :

- **Les tactiques** : la classification de plus haut niveau et correspondent aux objectifs spécifiques c'est la manœuvre défensive contre un adversaire. Il s'agit de Durcir, Déetecter, Isoler, Tromper et Expulser.
 - **Durcir** : rendre l'exploitation du réseau plus difficile et plus coûteuse.
 - **Déetecter** : identifier l'accès ou l'activité de l'adversaire, la détection de menaces.
 - **Isoler** : créer des barrières logiques ou physiques pour limiter l'accès de l'adversaire.
 - **Tromper** : attirer les attaquants potentiels et leur permettre d'accéder à un environnement observé ou contrôlé autrement dit piéger l'attaquant.
 - **Expulser** : supprimer l'adversaire du réseau.

La page de chaque tactique affiche une définition et une liste des techniques de cette catégorie.

- **Les techniques de base** : les techniques de haut niveau appelées aussi catégories.

La page de chaque technique de base affiche les détails suivants :

- Définition
- Aperçu technique
- Relations avec les artefacts numériques : comment la technique est liée aux artefacts

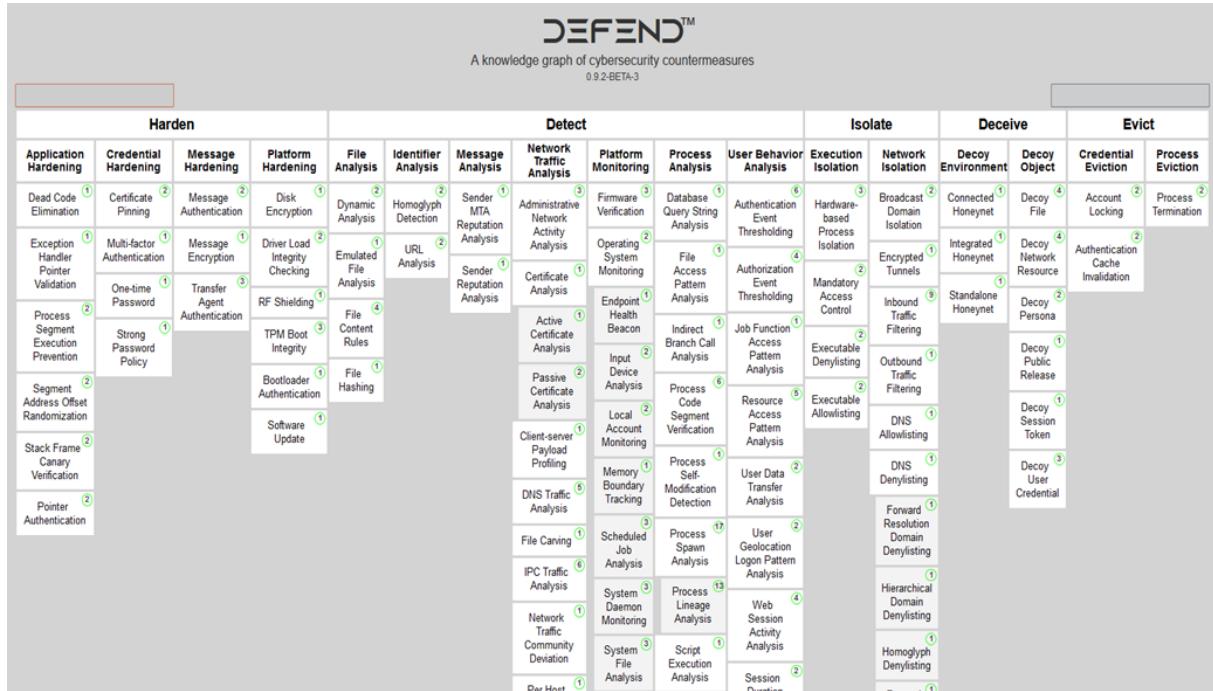


Figure 19 : Matrice MITRE D3FEND

8. Have I Been Pwned

8.1. Présentation

Have i been pwned est un excellent site géré par Troy Hunt en Australie c'est service gratuit qui va te permettre de savoir si ton adresse e-mail ou ton numéro de téléphone est concerné par une attaque informatique donc le but de have i been pwned est de savoir si des cybercriminels sont parvenus à dérobés ces données. Chaque fois qu'il y a une brèche qui existe sur des données qui ont été publiées il en récupère une copie, supprime les mots de passe puis prend les adresses e-mail et les attribue les attaches à une certaine brèche.

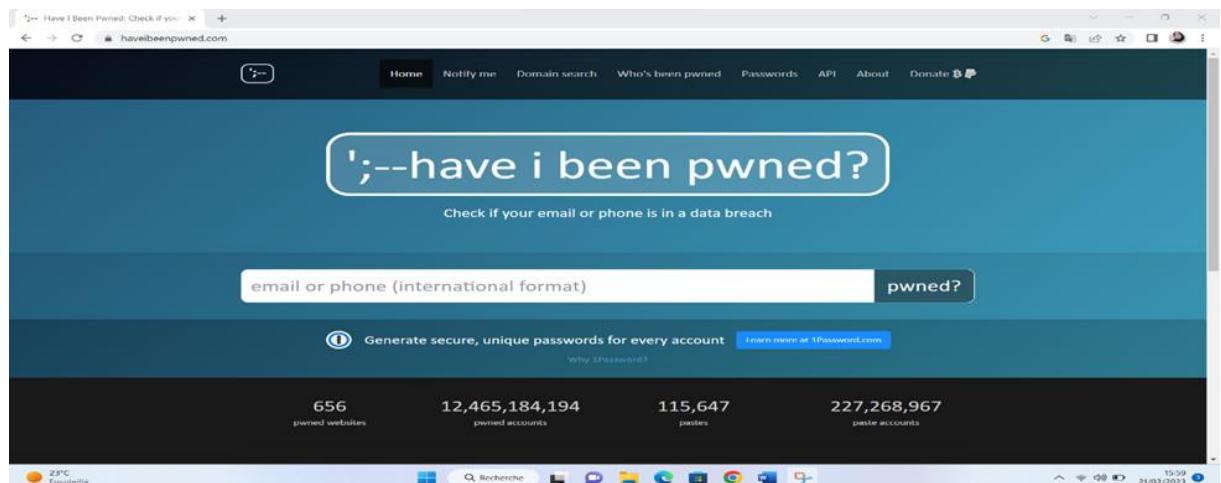


Figure 20 : Exemple 1

8.2. Composants et principe de fonctionnement

Le principe de have i been pwned.

- Il faut se rendre sur le site <https://haveibeenpwned.com>
- On saisit l'adresse e-mail du compte que l'on souhaite vérifier.
- Le site vous indique si le compte a été piraté ou non.
 - Si le compte n'est pas présent dans aucune base de données de sites piratés. Le site passe en vert et affiche le message « Good news – no pwnage found ! ».
 - Si le compte présent dans une base de données de sites piratés. Le site passe en rouge et affiche le message « Oh no – pwned ! ».

9. DeHashed

DeHashed est un exemple de site anti-Fraude et outil de sécurité avancé. C'est un moteur de recherche de base de données piratés ou de violation de données les plus importantes et les plus rapides disponibles en ligne. Cette solution permet aux particuliers, aux organisations et aux entreprises de vérifier si leurs informations confidentielles apparaît sur les listes piratées en ligne.

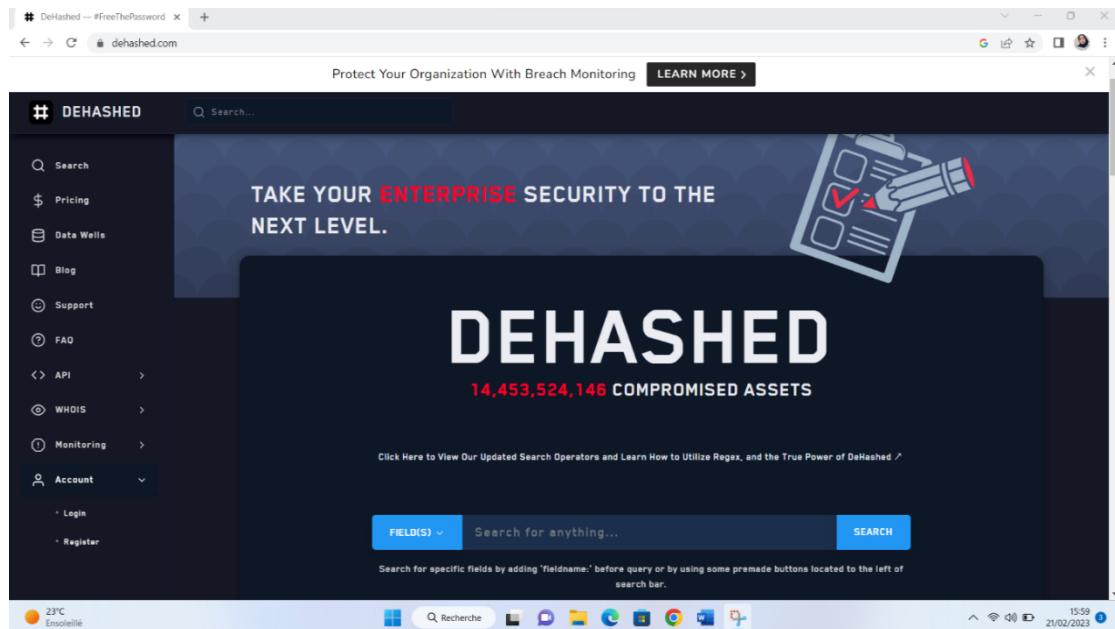


Figure 21 : Exemple 1

Il existe plusieurs méthodes de recherche il ne s'arrête pas qu'à la recherche d'adresse e-mail :

- Nom d'utilisateur
- Adresses IP
- E-mail
- Numéro de téléphone
- Les adresses VIN
- Adresses

10.URLscan

URL Scan est un filtre ISAPI (Internet Server API). C'est un service gratuit pour scanner et analyser des sites web. C'est un outil de sécurité qui affiche toutes les requêtes entrantes sur le serveur en filtrant les requêtes en fonction des règles définies par l'administrateur.

urlscan.io sert à détecter les URL. Si vous obtenez un lien suspect, vous pouvez le télécharger sur ce site Web et il vous fournira des informations sur ce lien. Ce site Web donne des informations sur le domaine telles que les détails IP, les liens sur le site Web, les redirections, les certificats et d'autres détails utiles.

URL Scan va pouvoir nous fournir une interface c'est à dire une Sandbox afin de pouvoir analyser des domaines de manière très détaillée et déterminer certains indicateurs qui nous permettent de déterminer si on est devant du phishing ou pas mais aussi de pouvoir effectuer d'autres recherches plus avancées. En arrivant sur la première page nous remarquons les scans en live qui sont en train d'être effectué. Site Web Urlscan io : <https://urlscan.io/> [16] [15]

The screenshot shows the urlscan.io homepage. At the top, there's a navigation bar with links for Home, Search, Live, API, Blog, Docs, Pricing, and Login. A banner for SecurityTrails is visible. Below the header, the main content area has a title 'urlscan.io' with the subtitle 'A sandbox for the web'. There are two buttons: 'Public Scan' and 'Options'. Underneath, a section titled 'Recent scans' shows a table of 10 recent scans. The columns in the table are: URL, Age, Size, IPs, and Flags. The data from the table is as follows:

URL	Age	Size	IPs	Flags
galaxy	12 seconds	842 KB	41	9 1
www.pudg-masterga/	15 seconds	72 KB	5	1 1
sunbeamfarm.com/privateShipments/www.usps.com/tracking/private-parcellocat...	15 seconds	481 KB	17	4 1
backofficemanagercharles.com/login	17 seconds	1 MB	27	7 3
admininfo.com/vgl/sys/suspendedpage.ngl	17 seconds	69 KB	6	4 1
www.sms-magic.com/subscription-preferences-center/	17 seconds	3 MB	155	32 5
nextopdelivery.com/	23 seconds	850 KB	45	5 2
outlooksoft.dkr.maildir@urlscan.com/html/e766f6_0d639d7024f5209eaab6609ccfe160...	25 seconds	47 KB	5	1 1
www.lse.or.jp/	25 seconds	846 KB	39	6 2
tracking.semilarpedia-mail.com/tracking/unsubscribe?ds=WD-FFrOwR5IEAnC6WV12hgk...	29 seconds	21 KB	6	4 2

Figure 22: URLScan.iso

11.VirusTotal

VirusTotal est une application Web simple et accessible qui est idéale pour analyser les fichiers suspects, les adresses IP, les URL, les domaines et les valeurs de hachage. Il est largement utilisé dans le renseignement sur les menaces. Il est facile à utiliser tout simplement il faut glisser et déposer le fichier et il affichera les résultats. Virustotal utilise une base de données prédefinie et l'analyse du fournisseur de sécurité pour vérifier si l'exemple de fichier ou l'URL est malveillant ou non.

Si quelqu'un nous envoie un fichier et que vous ne savez pas s'il est malveillant ou non, téléchargez-le et laissez Virustotal le détecter.

Si quelqu'un vous envoie une URL suspecte, copiez-la soigneusement (ne cliquez pas sur l'URL) et collez-la dans la section "URL" du site Web et effectuez une recherche.

Si vous trouvez une adresse IP, un domaine ou un hachage suspect, vous pouvez également utiliser virustotal pour le trouver. [16]

Site Internet de VirusTotal : www.virustotal.com



Figure 23 : VIRUSTOTAL

12.PyPhish



Figure 24: PYPHISHER

PyPhish est un outil de phishing en python, c'est un Framework qui permet la simulation des compagnes de phishing pour tester la cyber-sensibilisation et la résilience des cibles. Il inclut des sites web populaires comme facebook, Instagram, Twitter, github, gmail...Les caractéristiques d'un tel outil sont :

- Multi plate-forme (prend en charge la plupart des Linux)
- Facile à utiliser
- Diagnostiqueur d'erreur possible
- 77 modèles de sites Web
- Tunneling 3 simultané (Cloudflared, Loclx et LocalHostRun)
- Jusqu'à 6 liens pour le phishing
- Prise en charge d'OTP
- Prise en charge des arguments
- Envoi de justificatifs
- Masquage d'URL intégré
- Masquage personnalisé de l'URL
- Ombrage d'URL
- Paramètres d'URL de redirection
- Fichier portable (peut être exécuté à partir de n'importe quel répertoire)
- Obtenez l'adresse IP et de nombreux autres détails ainsi que les identifiants de connexion [13]

13. Conclusion

Au cours de ce second chapitre, nous avons commencé par présenter notre architecture de travail proposé. En deuxième lieu, nous avons cité les outils nécessaires pour réaliser ce travail qui sera l'objectif du chapitre suivant.

Chapitre 4 : Application du SOC

1. Introduction

Après avoir installé et configuré les outils indispensables nous passerons à la suite de travail. Ce chapitre est consacré à la récolte des data sources pour les analyser, collecter des données compromises et les informations personnelles, scanner et analyser des site web et effectuer une usurpation du site web par phishing.

2. Les outils appliqués

Au cours de ce chapitre nous utiliserons :

- le Framework de Mitre ATT&CK et le Framework de Mitre DeTT&CT
- Have I Been Pwned et DeHashed
- URLscan et VIRUSTOTAL
- PyPhisher

3. MITRE DeTECT

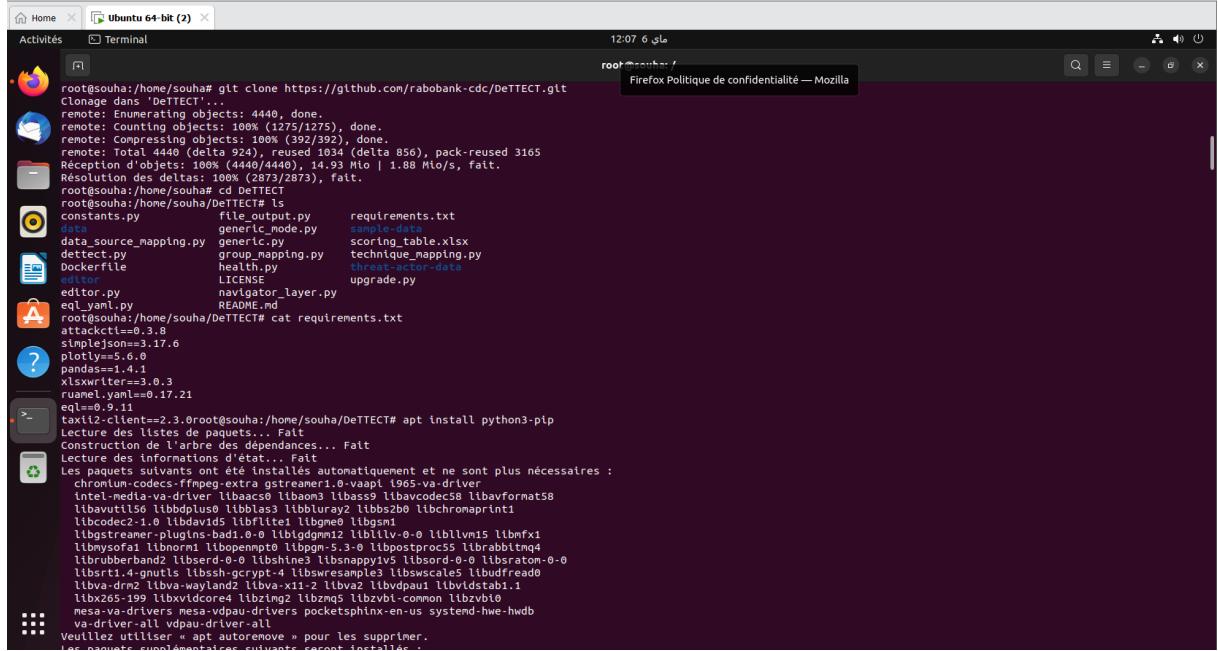
Sur ma machine Ubuntu nous avons entré en mode « sudo » puis nous avons commencé par « apt update » pour mettre à jour la liste des package en suite « apt install git » pour installer les outils de Git sur Ubuntu

```
root@souha:/home/souha# apt install git
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets suivants ont été installés automatiquement et ne sont plus nécessaires :
  chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi i965-va-driver
  intel-media-va-driver libaacso libaom3 libass9 libavcodec58 libavformat58
  libavutil56 libbdplus0 libblas3 libbluray2 libbsz2b0 libchromaprint1
  libcodec2-1.0 libdavids5 libflite1 libgme0 libgsml1
  libgstreamer-plugins-bad1.0-0 libigdmm12 liblilv-0-0 libllvm15 libmfx1
  libmysqld1 libnorm1 libopenmp10 libpgm-5.3-0 libpostproc55 librabbitmq4
  librubberband2 libserd-0-0 libshine3 libsnappy1v5 libsord-0-0 libratom-0-0
  libsr1t.4-gnutls libssh-gcrypt-4 libswresample3 libwscale5 libudfread0
  libva-drm2 libva-wayland2 libva-x11-2 libv2a libvpau1 libvidstab1.1
  libz65-199 libxvidcore4 libzimg2 libzmq5 libzvbi-common libzvbi0
  mesa-va-drivers mesa-vdpau-drivers pocketsphinx-en-us systemd-hwe-hwdb
  va-driver-all vdpau-driver-all
Veuillez utiliser « apt autoremove » pour les supprimer.
Les paquets supplémentaires suivants seront installés :
  git-man liberror-perl
Paquets suggérés :
  git-daemon-run | git-daemon-sysvinit git-doc git-email git-gui gitk gitweb
  git-cvs git-mediawiki git-svn
Les NOUVEAUX paquets suivants seront installés :
  git git-man liberror-perl
0 mis à jour, 3 nouvellement installés, 0 à enlever et 323 non mis à jour.
Il est nécessaire de prendre 4,147 ko dans les archives.
Après cette opération, 21.0 Mo d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] o
Réception de :1 http://tn.archive.ubuntu.com/ubuntu jammy/main amd64 liberror-perl all 0.17029-1 [26.5 kB]
Réception de :2 http://tn.archive.ubuntu.com/ubuntu jammy-updates/main amd64 git-man all 1:2.34.1-1ubuntu1.9 [954 kB]
Réception de :3 http://tn.archive.ubuntu.com/ubuntu jammy-updates/main amd64 git amd64 1:2.34.1-1ubuntu1.9 [3,166 kB]
4,147 ko réceptionnés en 3s (1,206 ko/s)
Sélection du paquet liberror-perl précédemment désélectionné.
(Lecture de la base de données... 201989 fichiers et répertoires déjà installés.
)
Préparation du dépaquetage de .../liberror-perl_0.17029-1_all.deb ...
Dépaquetage de liberror-perl (0.17029-1) ...
Sélection du paquet git-man précédemment désélectionné.
Préparation du dépaquetage de .../git-man_1%3a2.34.1-1ubuntu1.9_all.deb ...
Dépaquetage de git-man (1:2.34.1-1ubuntu1.9) ...
```

Figure 25: Installation Git

Une fois l'installation de git est effectuée nous passerons à effectuer un git clone afin de pouvoir récupérer le repetary de DeTT&CT en utilisant la commande suivante :

« git clone https://github.com/rabobank-cdc/DeTTECT.git »



```
root@souha:/home/souha# git clone https://github.com/rabobank-cdc/DeTTECT.git
Clonage dans 'DeTTECT'...
remote: Enumerating objects: 4440, done.
remote: Counting objects: 100% (1275/1275), done.
remote: Compressing objects: 100% (392/392), done.
remote: Total 4440 (delta 924), reused 1034 (delta 856), pack-reused 3165
Reçus d'objets: 100% (4440/4440), 14.93 Mo | 1.88 Mo/s, fait.
Delta compressées: 100% (392/392), 0.00 (0.073/2873), fait.
root@souha:/home/souha# cd DeTTECT
root@souha:/home/souha/DeTTECT# ls
constants.py          file_output.py      requirements.txt
data                 generic_mode.py    sample-data
data_source_mapping.py generic.py       scoring_table.xlsx
detetect.py           group_mapping.py technique_mapping.py
Dockerfile            health.py        threat-actor-data
editor               LICENSE         upgrade.py
editor.py             navigator_layer.py README.md
eql                  eql_output.py
eql@souha:/home/souha/DeTTECT# cat requirements.txt
attackcti==0.3.8
simplejson==3.17.6
plotly==5.6.0
pandas==1.4.1
xlsxwriter==3.0.3
ruamel.yaml==0.17.21
eql==0.9.11
taxi2-client==2.3.0
root@souha:/home/souha/DeTTECT# apt install python3-pip
Lecture des listes de paquets... Fait
Constructeur d'index des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets suivants ont été installés automatiquement et ne sont plus nécessaires :
  chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi_1.965-va-driver
  intel-media-va-driver libaacso0 libao0 libass9 libavcodec58 libavformat58
  libavutil56 libbdplus0 libblas3 libbluray2 libbs2b0 libchromaprint1
  libcodec2-1.0 libdavids0 libfflate1 libgme0 libgsml1
  libgstreamer-plugins-bad1.0-0 liblbind0 liblomm1 liblommw1 liblomfx1
  libmysqfa0 libnorn1 libopenmp10 libppm-5.3-0 libpostproc5 librabitmq4
  librubberband0 libserd-0.0 libshme3 libsnappy1v5 libssord-0.0 libsratom-0.0
  libstl-4-grnltis libssh-gcrypt-4 libswresample3 libswscale0 libvdpau1 libvdpauabi1
  libx265-pp libx265dec0 libx265_1 libzmq4 libzvbi-common libzvbi0
  mesa-va-drivers mesa-vdpau-drivers pocketphinx-en-us systemd-hwe-hwdb
  va-driver-all vdpau-driver-all
Veuillez utiliser « apt autoremove » pour les supprimer.
Les paquets supplémentaires suivants seront installés :
```

Figure 26: Installation de DeTT&CT

Maintenant nous venons à installer les différents requirements c'est-à-dire les package nécessaire pour l'utilisation de python nous utilisons la commande «cat requirements.txt »

```
root@souha:/home/souha/DeTTECT# cat requirements.txt
attackcti==0.3.8
simplejson==3.17.6
plotly==5.6.0
pandas==1.4.1
xlsxwriter==3.0.3
ruamel.yaml==0.17.21
eql==0.9.11
```

Figure 27: Installation des packages

Sur Ubuntu, python3 est installé par défaut donc il doit installer python3-pip en utilisant « apt install python3-pip »

```

taxii2-client==2.3.0root@souha:/home/souha/DeTECT# apt install python3-pip
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets suivants ont été installés automatiquement et ne sont plus nécessaires :
  chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi i965-va-driver
  intel-media-va-driver libaacs0 libaom3 libass9 libavcodec58 libavformat58
  libavutil56 libbdplus0 libblas3 libbluray2 libbs2b0 libchromaprint1
  libcodec2-1.0 libdavids5 libflite1 libgme0 libgsm1
  libgstreamer-plugins-bad1.0-0 libigdmm12 liblilv-0-0 libllvm15 libmfx1
  libmysofa1 libnorm1 libopenmp10 libpgm-5.3-0 libpostproc5 librabbitmq4
  librubberband2 libserd-0-0 libshine3 libsappiyiv5 libsord-0-0 libsratom-0-0
  libsrt1.4-gnutls libssh-gcrypt-4 libswresample3 libswscale5 libudfread0
  libva-drm2 libva-wayland2 libva-x11-2 libva2 libvdpau1 libvidstab1.1
  libx265-199 libxvidcore4 libzimg2 libzmq5 libzvbi-common libzvbi0
  mesa-va-drivers mesa-vdpau-drivers pocketsphinx-en-us systemd-hwe-hwdb
  va-driver-all vdpau-driver-all
Veuillez utiliser « apt autoremove » pour les supprimer.
Les paquets supplémentaires suivants seront installés :
  binutils binutils-common binutils-x86-64-linux-gnu build-essential cpp-11
  dpkg-dev fakeroot g++ g++-11 gcc gcc-11 gcc-11-base gcc-12-base
  javascript-common libalgorithm-diff-perl libalgorithm-diff-xs-perl
  libalgorithm-merge-perl libasan6 libatomic1 libbinutils libc-dev-bin
  libc-devtools libc6-dev libgcc1-0 libcrypt-dev libctf-nobfd0 libctf0
  libdpkg-perl libexpat1 libexpat1-dev libfakeroot libfile-fcntllock-perl
  libgcc-11-dev libgcc-s1 libgomp1 libitm1 libjs-jquery libjs-sphinxdoc
  libjs-underscore liblsan0 libnsl-dev libpython3-dev libpython3-stdlib
  libpython3.10 libpython3.10-dev libpython3.10-minimal libpython3.10-stdlib
  libquadmath0 libstdc++-11-dev libstdc++6 libtirpc-dev libtsan0 libubsan1
  linux-libc-dev lto-disabled-list make manpages-dev python3 python3-dev
  python3-distutils python3-lib2to3 python3-minimal python3-pkg-resources
  python3-setuptools python3-wheel python3.10 python3.10-dev
  python3.10-minimal rpcsvc-proto zlib1g zlib1g-dev
Paquets suggérés :
  binutils-doc gcc-11-locales debian-keyring g++-multilib g++-11-multilib
  gcc-11-doc gcc-multilib autoconf automake libtool flex bison gcc-doc
  gcc-11-multilib apache2 | lighttpd | httpd glibc-doc bzr libstdc++-11-doc
  make-doc python3-doc python3-tk python3-venv python-setuptools-doc
  python3.10-venv python3.10-doc binfmt-support
Les NOUVEAUX paquets suivants seront installés :
  binutils binutils-common binutils-x86-64-linux-gnu build-essential dpkg-dev
  fakeroot g++ g++-11 gcc gcc-11 javascript-common libalgorithm-diff-perl

```

Figure 28: Installation python3-pip

```

root@souha:/home/souha/DeTECT# pip install -r requirements.txt
Collecting attackctl==0.3.8
  Downloading attackctl-0.3.8-py3-none-any.whl (14 kB)
Collecting simplejson==3.17.6
  Downloading simplejson-3.17.6-cp310-cp310-manylinux_2_5_x86_64.manylinux1_x86_64.manylinux_2_12_x86_64.manylinux2010_x86_64.whl (137 kB)
    137.1/137.1 KB 1.7 MB/s eta 0:00:00
Collecting plotly==5.6.0
  Downloading plotly-5.6.0-py3-none-any.whl (27.7 MB)
    27.7/27.7 MB 2.1 MB/s eta 0:00:00
Collecting pandas==1.4.1
  Downloading pandas-1.4.1-cp310-cp310-manylinux_2_17_x86_64.manylinux2014_x86_64.whl (11.7 MB)
    11.7/11.7 MB 2.2 MB/s eta 0:00:00
Collecting xlsxwriter==3.0.3
  Downloading XlsxWriter-3.0.3-py3-none-any.whl (149 kB)
    150.0/150.0 KB 1.6 MB/s eta 0:00:00
Collecting ruamel.yaml==0.17.21
  Downloading ruamel.yaml-0.17.21-py3-none-any.whl (109 kB)
    109.5/109.5 KB 2.3 MB/s eta 0:00:00
Collecting eql==0.9.11
  Downloading eql-0.9.11-py2.py3-none-any.whl (104 kB)
    104.7/104.7 KB 1.7 MB/s eta 0:00:00
Collecting taxii2-client==2.3.0
  Downloading taxii2_client-2.3.0-py2.py3-none-any.whl (24 kB)
Collecting stix2
  Downloading stix2-3.0.1-py2.py3-none-any.whl (177 kB)
    177.8/177.8 KB 2.2 MB/s eta 0:00:00
Requirement already satisfied: six in /usr/lib/python3/dist-packages (from plotly==5.6.0->-r requirements.txt (line 3)) (1.16.0)
Collecting tenacity==6.2.0
  Downloading tenacity-8.2.2-py3-none-any.whl (24 kB)
Collecting numpy>=1.21.0
  Downloading numpy-1.24.3-cp310-cp310-manylinux_2_17_x86_64.manylinux2014_x86_64.whl (17.3 MB)
    17.3/17.3 MB 2.0 MB/s eta 0:00:00
Requirement already satisfied: python-dateutil>=2.8.1 in /usr/lib/python3/dist-packages (from pandas==1.4.1->-r requirements.txt (line 4)) (2.8)
Requirement already satisfied: pytz>=2020.1 in /usr/lib/python3/dist-packages (from pandas==1.4.1->-r requirements.txt (line 4)) (2022.1)
Collecting ruamel.yaml.libc==0.2.6
  Downloading ruamel.yaml.libc-0.2.7-cp310-cp310-manylinux_2_17_x86_64.manylinux2014_x86_64.manylinux_2_24_x86_64.whl (485 kB)
    485.6/485.6 KB 2.4 MB/s eta 0:00:00
Collecting lark-parser==0.11.1

```

Figure 29: Installer tous les modules

Une fois installé, nous pouvons soit utiliser l'interface de ligne de commande, soit lancer l'éditeur DeTT&CT.

Pour lancer DeTT&CT Editor, nous saisissons la commande suivante « python3 dettect.py » en spécifiant le paramètre editor pour démarrer l'éditeur DeTT&CT localement.

```
root@souha:/home/souha/DeTTECT# python3 dettect.py editor
Editor started at port 8080
Opening webbrowser: http://localhost:8080/
```

Figure 30: Lancement editeur DeTT&CT

Cela lancera automatiquement un navigateur web dans l'interface DeTT&CT. Nous sélectionnons « data sources » et nous choisissons « new file ».

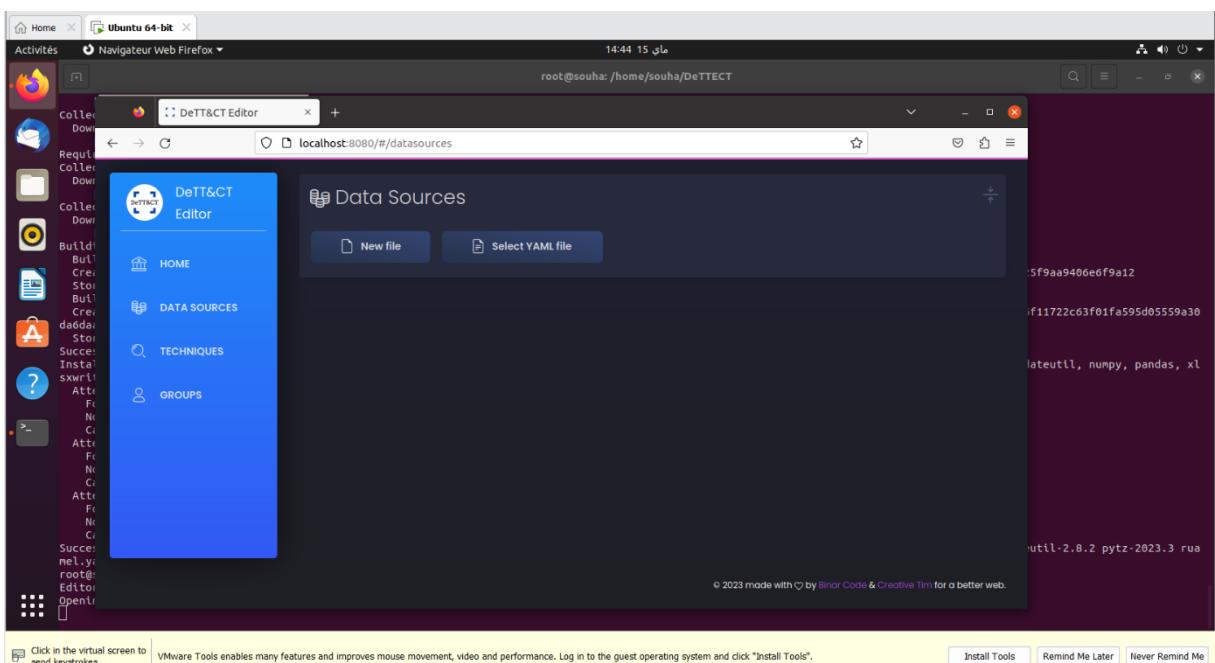


Figure 31: Interface de l'éditeur DeTT&CT

Ensuite nous avons ajouté des sources de données en fonction des sources de données dont nous disposons déjà sur notre réseau.

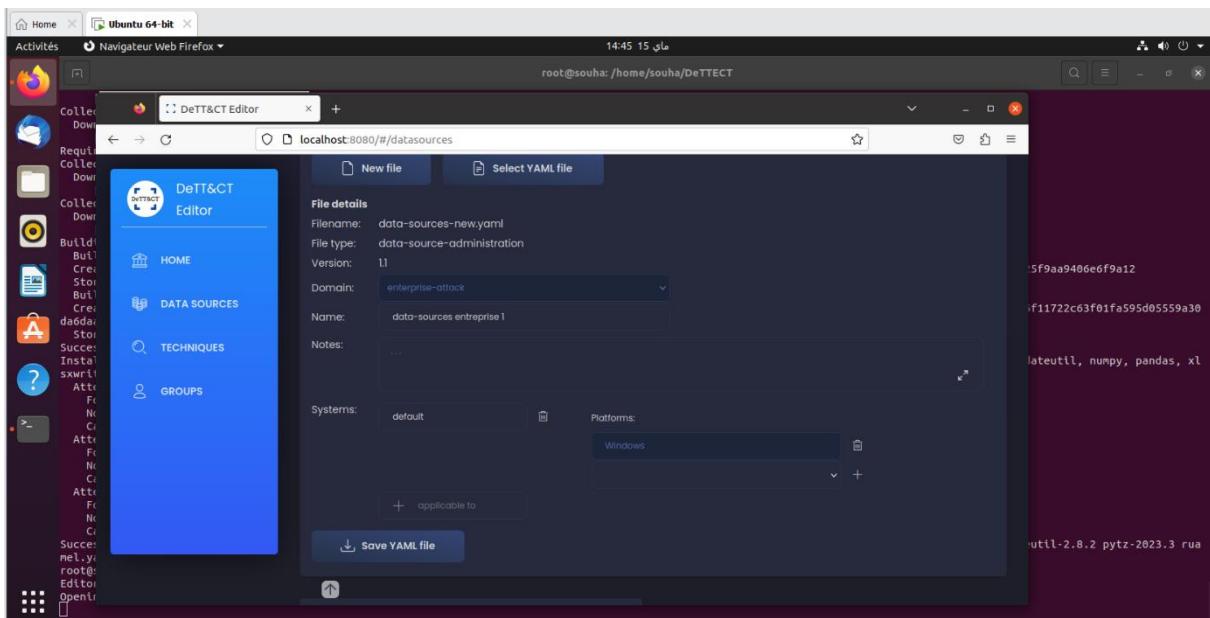


Figure 32: Configuration du fichier d'administration de la source de données

Maintenant, nous cliquons à gauche sur « Add data sources » et une nouvelle fenêtre apparaît à droite où nous pouvons commencer à ajouter nos sources de données.

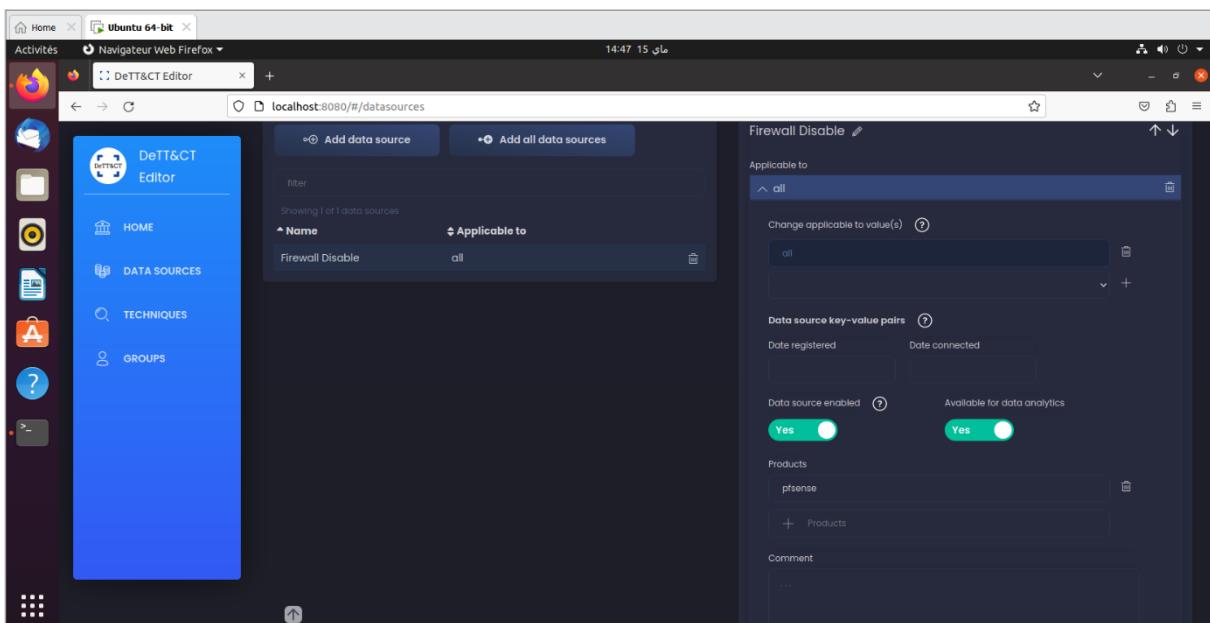


Figure 33: Configuration des sources de données

Maintenant sur le terminal nous pouvons visualiser l'ensemble des data sources avec l'approche suivante :

`python3 dettect.py generic -ds` donc là nous pouvons voir la liste des data sources et les plateformes qui les associés de manière plus détaillée.

```
souha@souha:~$ cd DeTTECT
souha@souha:~/DeTTECT$ ls
LS : commande introuvable
souha@souha:~/DeTTECT$ ls
cache      data_source_mapping.py  editor      file_output.py  group_mapping.py  navigator_layer.py  README.md    scoring_table.xlsx  upgrade.py
constants.py  detetect.py        editor.py    generic_mode.py  health.py       output      requirements.txt  technique_mapping.py
data        Dockerfile          eq_yaml.py  generic.py     LICENSE        __pycache__  sample-data   threat-actor-data
souha@souha:~/DeTTECT$ sudo python3 detetect.py generic -ds
[sudo] Mot de passe de souha :
Count Data Source          Platform(s)
----- -----
268 Command Execution      Android, Containers, Linux, Network, Windows, iOS, macOS
226 Process Creation      Android, Linux, Windows, iOS, macOS
104 File Modification     Linux, Network, Windows, macOS
94 OS API Execution       Android, Linux, Windows, iOS, macOS
91 File Creation          Linux, Network, Windows, macOS
86 Network Traffic Flow   Android, IaaS, Linux, Windows, iOS, macOS
82 Network Traffic Content Android, IaaS, Linux, Windows, iOS, macOS
72 Application Log Content Google Workspace, IaaS, Linux, Office 365, SaaS, Windows, macOS
65 Window Registry Key Modification Windows
61 Network Connection Creation Android, IaaS, Linux, Windows, iOS, macOS
54 Module Load             Linux, Windows, macOS
47 File Access             Linux, Network, Windows, macOS
47 Web [DeTTECT data source] Windows, macOS, Linux, IaaS, Office 365, Google Workspace, SaaS, Network, Containers
44 File Metadata           Linux, Network, Windows, macOS
37 Logon Session Creation Azure AD, Google Workspace, IaaS, Linux, Office 365, SaaS, Windows, macOS
38 Script Execution        Windows
26 Response Content        Windows
26 User Account Authentication Azure AD, Containers, Google Workspace, IaaS, Linux, Office 365, SaaS, Windows, macOS
22 Windows Registry Key Creation Windows
21 Process Access          Android, Linux, Windows, iOS, macOS
21 Internal DNS [DeTTECT data source] Windows, macOS, Linux, IaaS, Network, Containers
18 Host Status              Android, Linux, Windows, iOS, macOS
18 Email [DeTTECT data source] Windows, macOS, Linux, Office 365, Google Workspace, SaaS
16 Active Directory Object Modification Azure AD, Windows
15 Process Metadata         Android, Linux, Windows, iOS, macOS
14 Driver Load              Linux, Windows, macOS
14 Service Creation        Linux, Windows, macOS
13 File Deletion            Linux, Network, Windows, macOS
```

Figure 34: Afficher les data sources

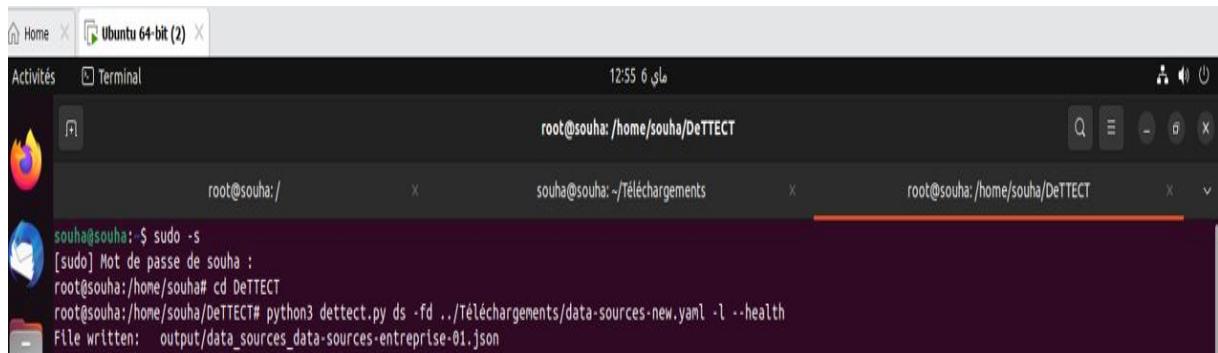
Maintenant une fois que nous gérons notre fichier qui est dans téléchargements, nous avons les différents data-sources et les paramètres qui les assimilés

```
souha@souha:~$ cat data-sources-new.yaml
data-sources-new.yaml
souha@souha:~/Téléchargements$ cat data-sources-new.yaml
version: 1.1
file_type: data-source-administration
name: data sources enterprise 01
domain: enterprise-attack
systems:
- applicable_to: default
  platform:
  - Windows
data_sources:
- data_source_name: Active Directory Credential Request
  data_source:
  - applicable_to:
    - all
    date_registered: null
    date_connected: null
    products: []
    available_for_data_analytics: false
    comment: ''
    data_quality:
      device_completeness: 0
      data_field_completeness: 0
      timeliness: 0
      consistency: 0
      retention: 0
- data_source_name: Active Directory Object Access
  data_source:
  - applicable_to:
    date_registered: null
    date_connected: null
    products: []
    available_for_data_analytics: false
    comment: ''
    data_quality:
      device_completeness: 0
      data_field_completeness: 0
      timeliness: 0
      consistency: 0
      retention: 0
- data_source_name: Active Directory Object Creation
```

Figure 35:Afficher le contenu de fichier YAML

Nous allons maintenant convertir ce fichier YAML en un fichier JSON à l'aide de la commande `python3 detetect.py ds -fd ..//Téléchargements/data-sources-new.yaml -l --health`.

Et là nous avons notre fichier json que nous avons récupéré et nous le mettons dans le bureau par la commande suivante « cp output/data_sources_data-sources-entreprise-01.json »



```
souha@souha: ~$ sudo -s
[sudo] Mot de passe de souha :
root@souha:/home/souha# cd DeTTECT
root@souha:/home/souha/DeTTECT# python3 dettect.py ds -fd ..//Téléchargements/data-sources-new.yaml -l --health
File written: output/data_sources_data-sources-entreprise-01.json
```

Figure 36: Convertir le fichiey YAML en JSON

Maintenant nous revenons à mitre Navigator et nous allons utiliser l'option « Open Existing Layer ». Nous choisissons l'option locale

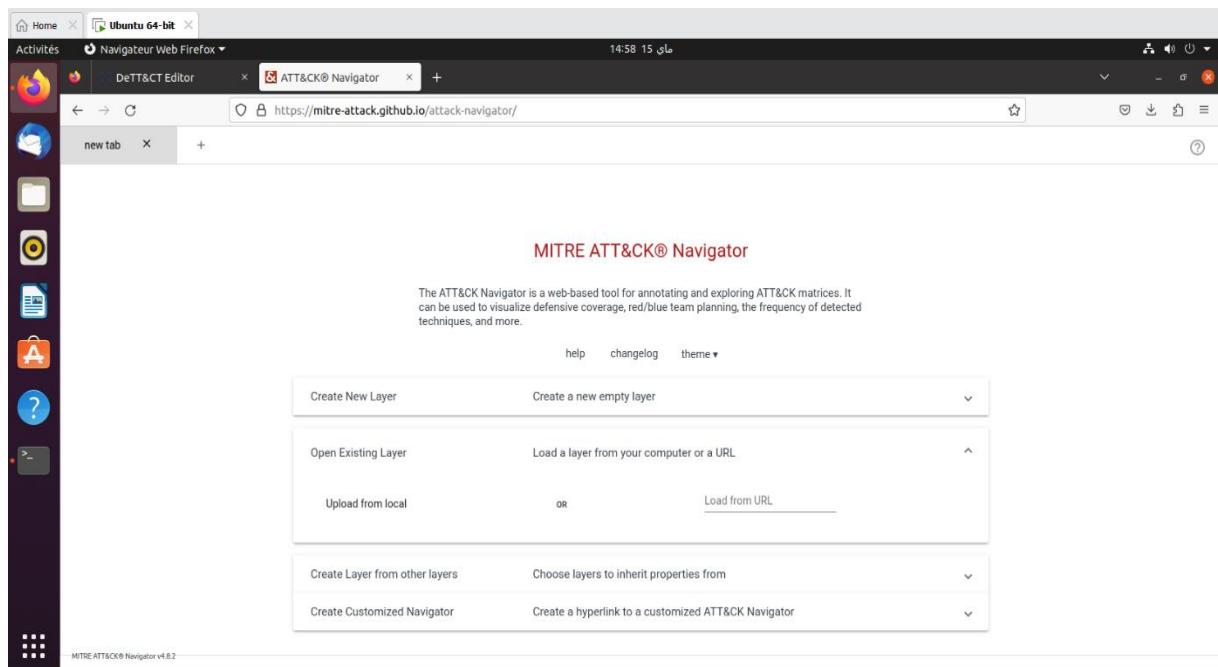


Figure 37:Mitre navigator

Donc là nous avons notre fichier json qui nous essayons de l'ouvrir

LA MISE EN PLACE D'UN SOC

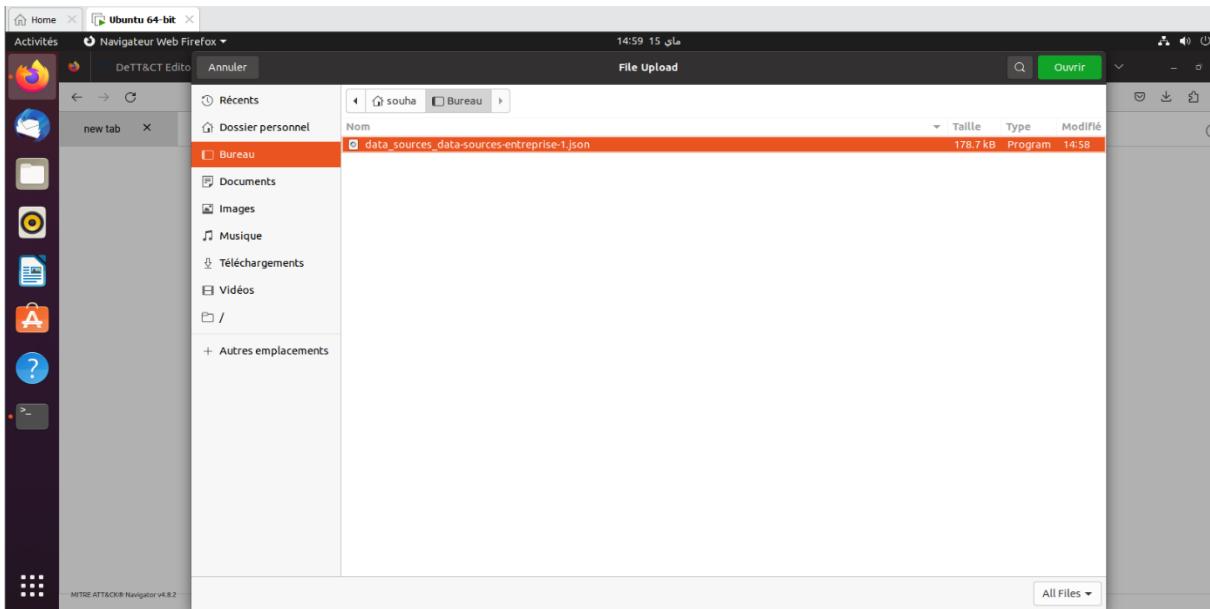


Figure 38: Notre fichier json

Cette matrice représente le mappage MITRE ATT&CK basé sur les sources de données que nous avons spécifié dans notre fichier d'administration des sources de données.

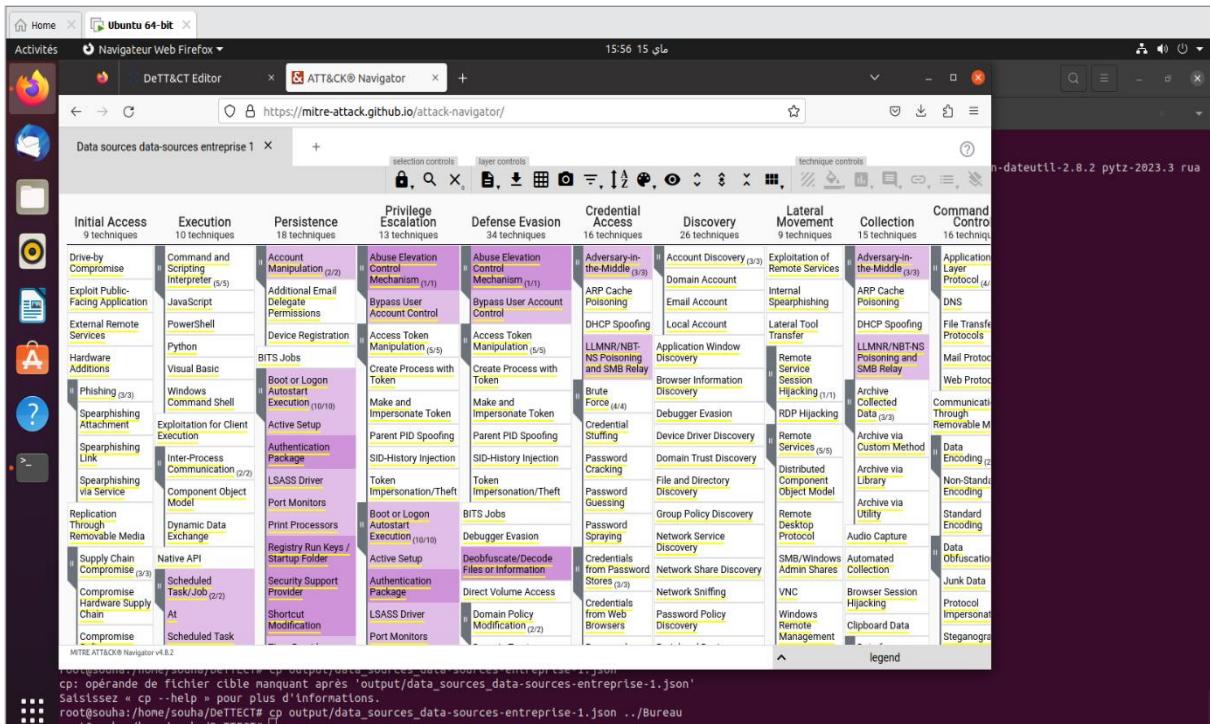


Figure 39: Couverture des sources de données

Nous pouvons générer un fichier YAML d'administration technique basé sur notre fichier d'administration de source de données

```
root@souha:/home/souha/DeTTECT# python3 dettect.py v -ft output/techniques-administration-data-sources-entreprise-1.yaml -l
File written:  output/visibility_data-sources-entreprise-1.json
root@souha:/home/souha/DeTTECT# cp output/visibility_data-sources-entreprise-1.json ..../Bureau
```

Figure 40: Génération de la couverture de visibilité

Maintenant nous allons visualiser le score de visualisation

```
root@souha:/home/souha/DeTTECT# python3 dettect.py ds -fd ..//Téléchargements/data-sources-new.yaml --yaml
File written:  output/techniques-administration-data-sources-entreprise-1.yaml
```

Figure 41: Couche de couverture de visibilité

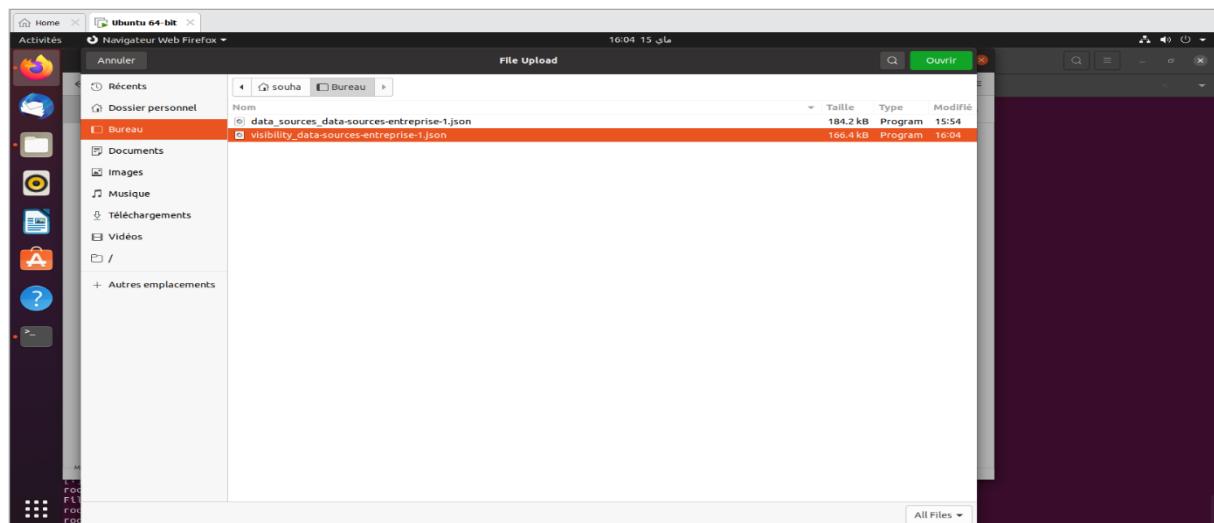


Figure 42: Notre fichier json de couverture de visibilité

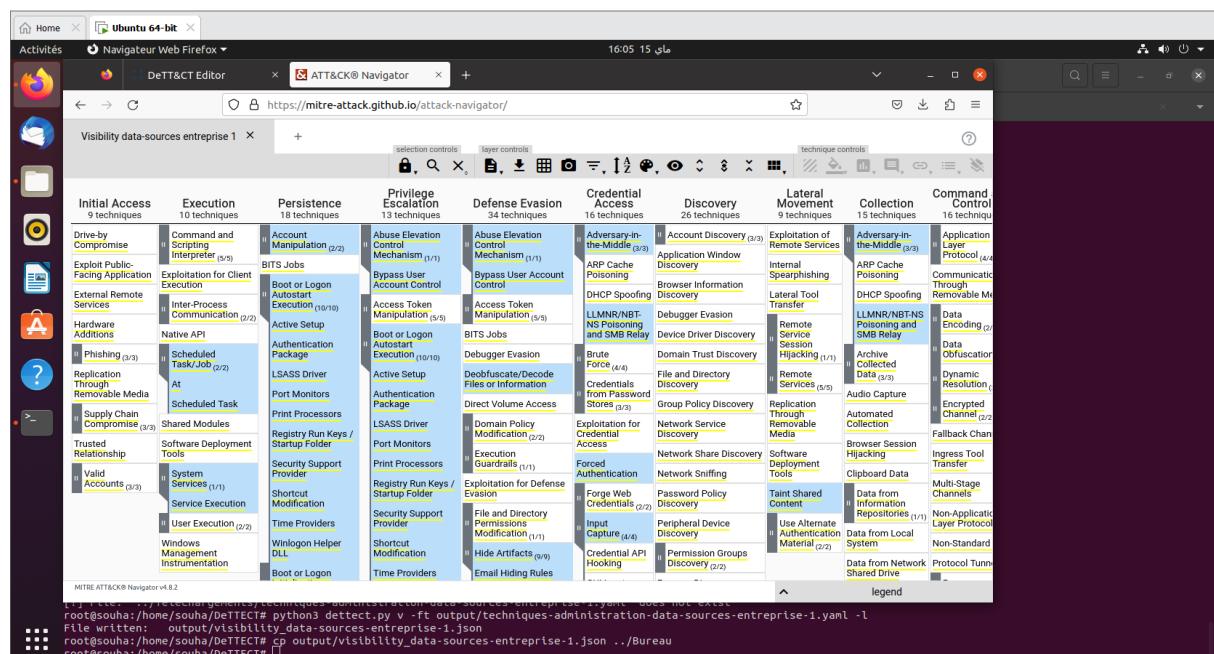


Figure 43: Matrice de visibilité ATT&CK

4. Have I Been Pwned ?

Nous vérifierions 3 exemples d'adresse e-mail de CPG :

- abderraouf.hidri@cpg.com.tn
- semah.raddaoui@cpg.com.tn
- ghassen.rdhounia@cpg.com.tn

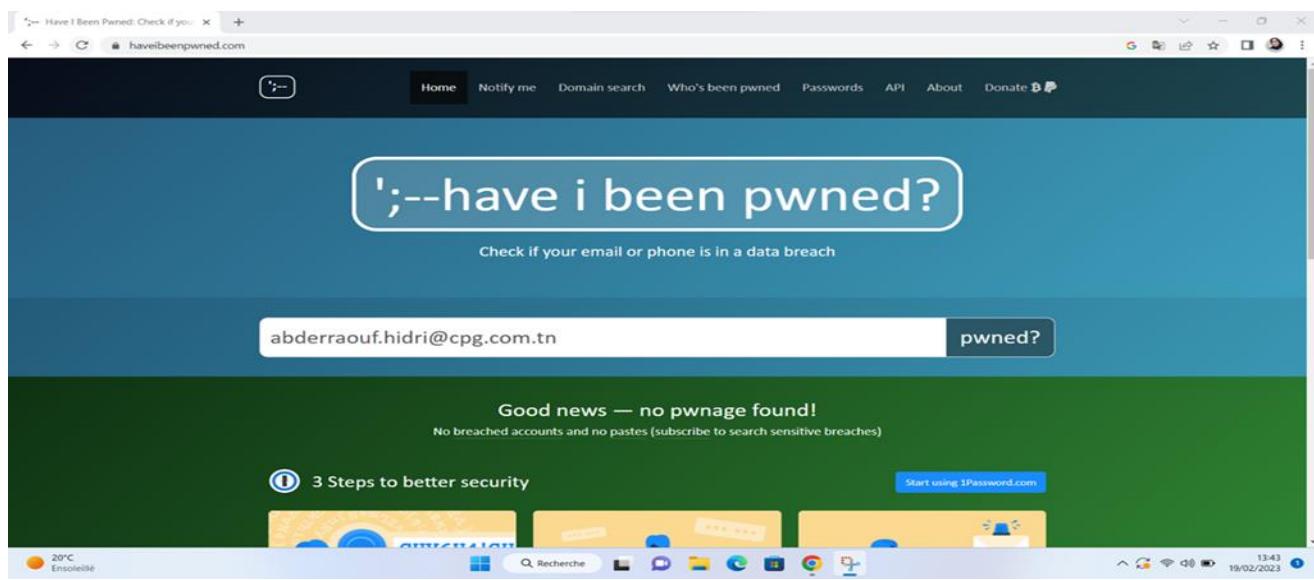


Figure 44: Exemple 1 Have I Been Pwned ?

Pour le premier exemple le site est en vert et affiche le message suivant « Good news – no pwnage found ! » Ça veut dire que l'adresse e-mail saisie ne se trouve dans aucune base de données de sites piratés.

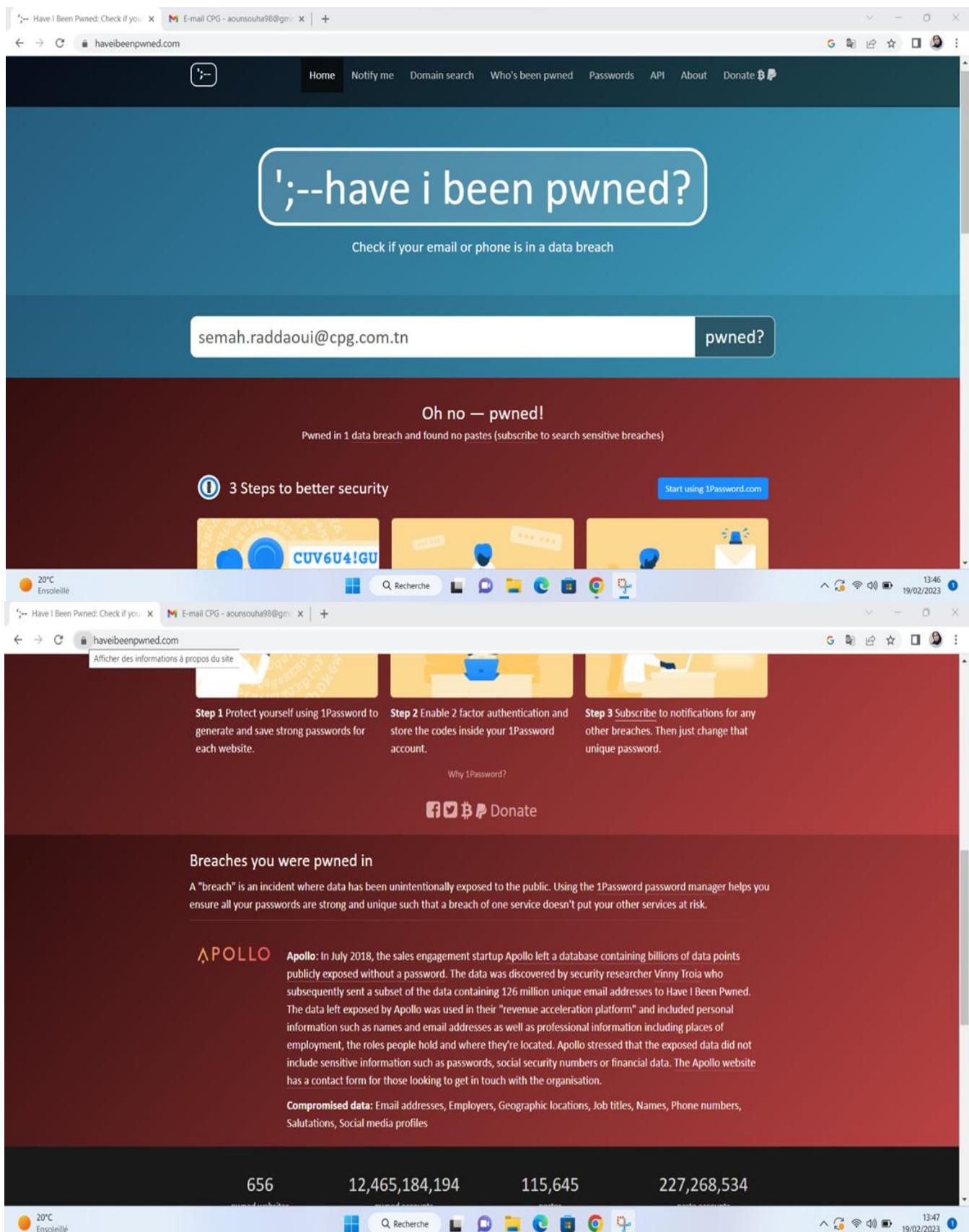


Figure 45: Exemple 2 Have I Been Pwned ?

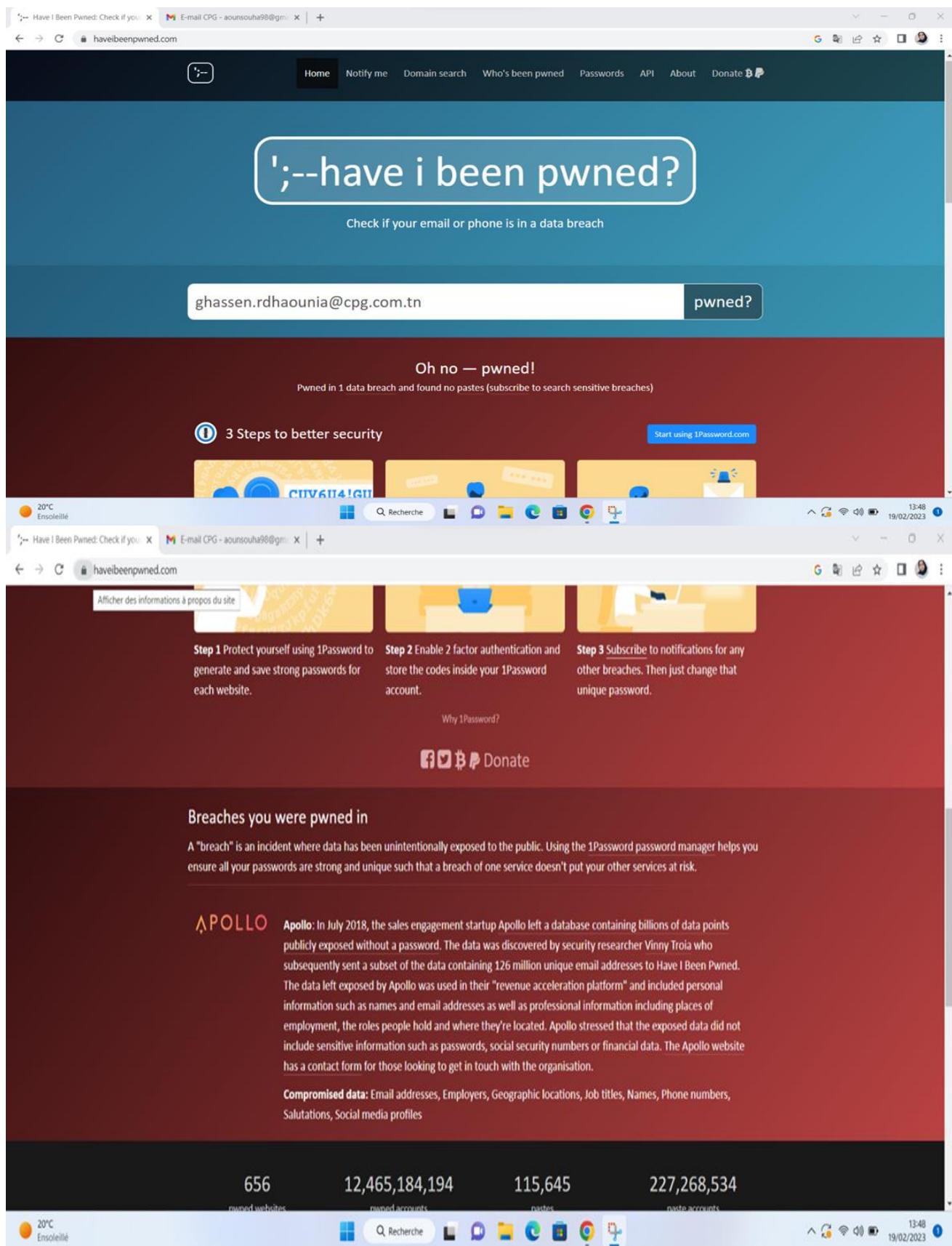


Figure 46: Exemple 3 Have I Been Pwned ?

Pour les deux exemples 2 et 3 le résultat obtenu sera marqué comme site rouge et message « Oh no – pwned » : C'est mal il affiche le pwnage dont les données ont été violées Cette plateforme précise

le site attaqué : Apollo

La date de la fuite : juillet 2018

La nature des données compromises : adresse e-mail, employeurs, emplacements géographiques, titres d'emploi, nom, numéros de téléphone, salutations, profils de médias sociaux. Donc c'est urgent de vérifier le compte saisi et améliorer la sécurité.

5. DeHashed

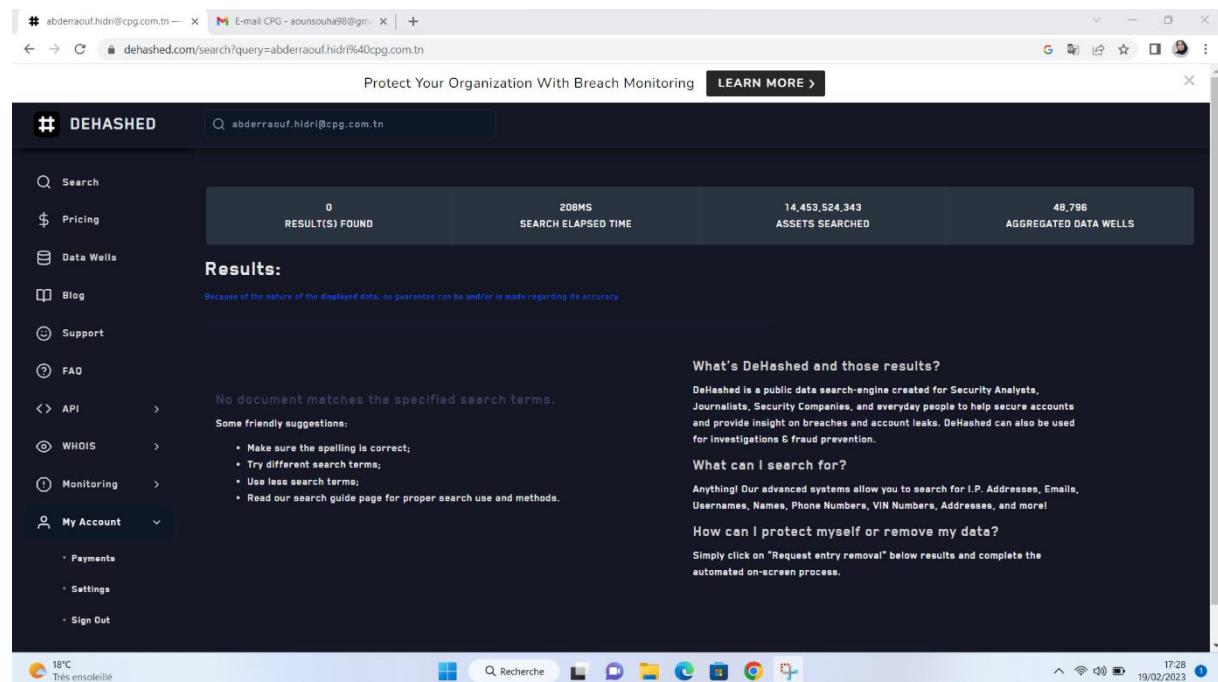


Figure 47: Exemple 1 DeHashed

LA MISE EN PLACE D'UN SOC

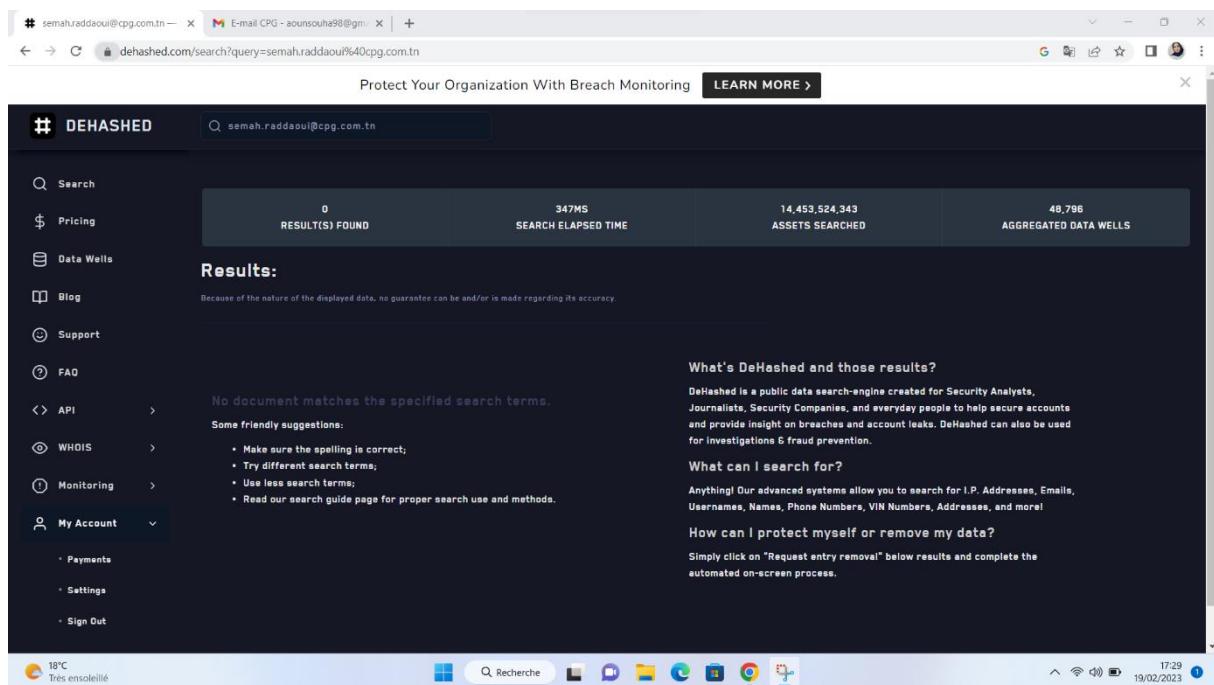


Figure 48: Exemple 2 DeHashed

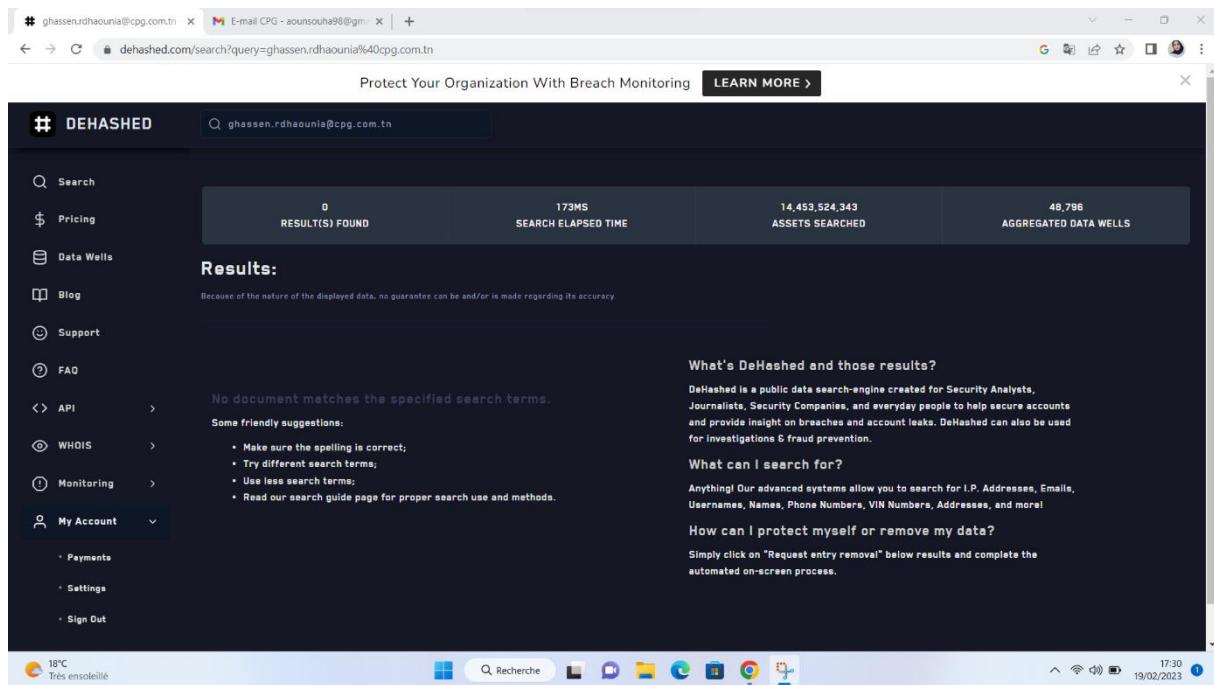


Figure 49: Exemple 3 DeHashed

Pour les trois exemples qui correspondent aux trois e-mails : il n'existe aucune violation de données et les trois ne présentent dans aucune base de données de site piraté.

6. URLscan :

Après la récolte de notre URL il paraît qu'il est malicieux et au niveau de cette plateforme nous pouvons voir :

- L'adresse IP
- Le pays
- Le serveur
- Le certificat de sécurité
- La durée de validité
- Les Scan qui ont déjà été effectués sur ce domaine
- Verdict le brand de l'entreprise qui est ciblé par cette attaque
- Les résultats du Google Safe Browsing qui le détecte comme malicieux
- Le serveur DNS

Figure 50 : Analyse URL par URLscan

7. VIRUSTOTAL

Dans cette partie nous avons utilisé VIRUSTOTAL pour analyser un URL. Nous avons recollé notre URL et là nous pouvons voir certains retours de certains éditeurs qui le répertorier comme malicieux.

Security vendor	Result	Security vendor	Result
Trustwave	Phishing	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
AICC (MONITORAPP)	Clean	AlienVault	Clean
alphaMountain ai	Clean	Antiy-AVL	Clean
Artists Against 419	Clean	Avira	Clean
benikow cc	Clean	Bfore Ai PreCrime	Clean
BitDefender	Clean	BlockList	Clean

Figure 51 : Analyse URL par VIRUSTOTAL

8. Attaque phishing

Sur le terminal et en mode sudo nous tapons la commande

git clone://github.com/kasoudra/PyPhisher.git afin de pouvoir récupérer le repertory de PyPhisher

```
souha@souha:~$ sudo -s
[sudo] Mot de passe de souha :
root@souha:/home/souha# git clone https://github.com/KasRoudra/PyPhisher.git
Clonage dans 'PyPhisher'...
remote: Enumerating objects: 237, done.
remote: Counting objects: 100% (237/237), done.
remote: Compressing objects: 100% (113/113), done.
remote: Total 237 (delta 124), reused 214 (delta 108), pack-reused 0
Réception d'objets: 100% (237/237), 2.42 Mio | 2.08 Mio/s, fait.
Résolution des deltas: 100% (124/124), fait.
root@souha:/home/souha#
```

Figure 52: Cloner le dépôt Installer PyPhisher

En entrant au répertoire PyPhisher par cd PyPhisher nous installons tous les modules en utilisant l'approche suivante : pip install -r files/requirements.txt

```
root@souha:/home/souha# cd PyPhisher
root@souha:/home/souha/PyPhisher# pip3 install -r files/requirements.txt
Requirement already satisfied: requests in /usr/lib/python3/dist-packages (from -r files/requirements.txt (line 1)) (2.25.1)
Collecting bs4
  Downloading bs4-0.0.1.tar.gz (1.1 kB)
    Preparing metadata (setup.py) ... done
Collecting rich
  Downloading rich-13.3.5-py3-none-any.whl (238 kB)
    238.7/238.7 KB 1.9 MB/s eta 0:00:00
Collecting beautifulsoup4
  Downloading beautifulsoup4-4.12.2-py3-none-any.whl (142 kB)
    143.0/143.0 KB 2.5 MB/s eta 0:00:00
Collecting pygments<3.0.0,>=2.13.0
  Downloading Pygments-2.15.1-py3-none-any.whl (1.1 MB)
    1.1/1.1 MB 2.2 MB/s eta 0:00:00
Collecting markdown-it-py<3.0.0,>=2.2.0
  Downloading markdown_it_py-2.2.0-py3-none-any.whl (84 kB)
    84.5/84.5 KB 2.4 MB/s eta 0:00:00
Collecting mdurl==0.1
  Downloading mdurl-0.1.2-py3-none-any.whl (10.0 kB)
Collecting soupsieve<1.2
  Downloading soupsieve-2.4.1-py3-none-any.whl (36 kB)
Building wheels for collected packages: bs4
  Building wheel for bs4 (setup.py) ... done
    Created wheel for bs4: filename=bs4-0.1-py3-none-any.whl size=1272 sha256=dd2fee704058eef9c6717a00a7cf628c41825f9a4908c850ca43d4364138bb2c
    Stored in directory: /root/.cache/pip/wheels/25/42/45/b773edc52acb16cd2db4cf1a0b4717e2f69bb4eb300ed0e70
Successfully built bs4
Installing collected packages: soupsieve, pygments, mdurl, markdown-it-py, beautifulsoup4, rich, bs4
Successfully installed beautifulsoup4-4.12.2 bs4-0.0.1 markdown-it-py-2.2.0 mdurl-0.1.2 pygments-2.15.1 rich-13.3.5 soupsieve-2.4.1
```

Figure 53:Entrer dans le répertoire et installer tous les modules

Nous avons exécuté le fichier pyphisher.py pour vérifier l'installation par python3 pyphisher.py

```
root@souha:/home/souha/PyPhisher# python3 pyphisher.py
[+] Please wait!
[+] Installing php
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets suivants ont été installés automatiquement et ne sont plus nécessaires :
  chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi i965-va-driver intel-media-va-driver libaaacs0 libao3 libass9 libavcodec58 libavformat58 libavutil56 libbdplus0 libblas3
  libbluray2 libbsz2b0 libchromaprint1 libcodecs2-1.0 libdavids5 libflite1 libgme0 libgsm1 libgstreamer-plugins-bad1.0-0 libigdgmm12 liblilly-0-0 liblilv15 libmfx1 libmysqfa1
  libnorm libopenmp10 libppm-5.3.0 libpostproc55 librabitmq4 librubberband2 libred5-0-0 libshnne15 libssord-0-0 librato-0-0 libsr1t1.4-gnutls libssh-gcrypt-4
  libswresample3 libswscale5 libudfread0 libva-wayland2 libva-x11-2 libvba2 libvdpa1 libvidstab1.1 libvpx2 libzmq5 libzvbi-common
  libzvbt0 mesa-va-drivers mesa-vdpau-drivers pocketsphinx-en-us systemd-hw-hwdb va-driver-all vdpau-driver-all
Veuillez utiliser « sudo apt autoremove » pour les supprimer.
Les paquets supplémentaires suivants seront installés :
  apache2 apache2-bin apache2-data apache2-utils libapache2-mod-php8.1 libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap php-common php8.1 php8.1-cli
  php8.1-common php8.1-opcache php8.1-readline
Paquets suggérés :
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom www-browser php-pear
Les NOUVEAUX paquets suivants seront installés :
  apache2 apache2-bin apache2-data apache2-utils libapache2-mod-php8.1 libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap php php-common php8.1 php8.1-cli
  php8.1-common php8.1-opcache php8.1-readline
0 mis à jour, 16 nouvellement installés, 0 à enlever et 303 non mis à jour.
Il est nécessaire de prendre 7,045 Ko dans les archives.
Après cette opération, 29,0 Mo d'espace disque supplémentaires seront utilisés.
Réception de :1 http://tn.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libapr1 amd64 1.7.0-8ubuntu0.22.04.1 [108 kB]
Réception de :2 http://tn.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libaprutil1 amd64 1.6.1-5ubuntu4.22.04.1 [92.6 kB]
Réception de :3 http://tn.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libaprutil1-dbd-sqlite3 amd64 1.6.1-Subuntu4.22.04.1 [11.3 kB]
Réception de :4 http://tn.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libaprutil1-ldap amd64 1.6.1-Subuntu4.22.04.1 [9,168 B]
Réception de :5 http://tn.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libapache2-bin amd64 2.4.52-Subuntu4.5 [534.5 kB]
Réception de :6 http://tn.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libapache2-data amd64 2.4.52-Subuntu4.5 [165 kB]
Réception de :7 http://tn.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libapache2-utils amd64 2.4.52-Subuntu4.5 [89.1 kB]
Réception de :8 http://tn.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libapache2-mod-php8.1 amd64 2.4.52-Subuntu4.5 [97.8 kB]
Réception de :9 http://tn.archive.ubuntu.com/ubuntu jammy/main amd64 php-common all 2.92+ubuntu1 [12.1 kB]
Réception de :10 http://tn.archive.ubuntu.com/ubuntu jammy-updates/main amd64 php8.1-common amd64 8.1.2-ubuntu2.11 [1,126 kB]
Réception de :11 http://tn.archive.ubuntu.com/ubuntu jammy-updates/main amd64 php8.1-opcache amd64 8.1.2-ubuntu2.11 [365 kB]
Réception de :12 http://tn.archive.ubuntu.com/ubuntu jammy-updates/main amd64 php8.1-readline amd64 8.1.2-ubuntu2.11 [13.5 kB]
Réception de :13 http://tn.archive.ubuntu.com/ubuntu jammy-updates/main amd64 php8.1-cli amd64 8.1.2-ubuntu2.11 [1,833 kB]
Réception de :14 http://tn.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libapache2-mod-php8.1 amd64 8.1.2-ubuntu2.11 [1,765 kB]
Réception de :15 http://tn.archive.ubuntu.com/ubuntu jammy-updates/main amd64 php8.1-all 8.1.2-ubuntu2.11 [9,150 B]
Réception de :16 http://tn.archive.ubuntu.com/ubuntu jammy/main amd64 php all 2.8.1-92ubuntu1 [2,756 B]
7 outre la réception de 16 (1,057 Ko)
```

Figure 54: exécution pyphisher.py

Maintenant et après l'exécution de PyPhisher nous allons utiliser l'outil PyPhisher pour trouver les identifiants d'un utilisateur. Nous allons exécuter 3 cas : Facebook, Instagram et Gmail.

Au niveau de chaque cas une liste des options qui s'affiche. Nous sélectionnons l'option qui correspond à notre situation. Sur le terminal Ubuntu, 4 URL malveillantes s'affichent. Ces URL nous seront utiles pour effectuer l'attaque de phishing.

8.1. Attaque sur Facebook

Dans un premier cas, nous choisissons l'option 1 qui correspond au facebook

```

root@souha: /home/souha/PyPhisher
[By KasRoudra]

01 Facebook Traditional [27] Reddit [53] Gitlab
02 Facebook Voting [28] Adobe [54] Github
03 Facebook Security [29] DebianArt [55] LinkedIn
04 Facebook Messenger [30] Admodo [56] iCloud
05 Instagram Traditional [31] Clash Of Clans [57] VLmeo
06 Insta Auto Followers [32] Ajio [58] MySpace
07 Insta 1000 Followers [33] JIorouter [59] Venmo
08 Insta Blue Verify [34] FreeFire [60] Cryptocurrency
09 Gmail Old [35] Pubg [61] SnapChat2
10 Gmail New [36] Telegram [62] Verizon
11 Gmail Poll [37] YouTube [63] Wi-Fi
12 Microsoft [38] Airtel [64] Discord
13 Netflix [39] ClubAtClub [65] Roblox
14 PayPal [40] Ola [66] GameEats
15 Steam [41] Outlook [67] Zomato
16 Twitter [42] Amazon [68] WhatsApp
17 PlayStation [43] Origin [69] PayTM
18 TikTok [44] DropBox [70] PhonePay
19 Twitch [45] Yahoo [71] MobiKwik
20 Pinterest [46] WordPress [72] Hotstar
21 SnapChat [47] Yandex [73] FlipCart
22 LinkedIn [48] StackOverflow [74] Teachable
23 Ebay [49] VK [75] Mail
24 Quora [50] Poll [76] CryptoAir
25 Protonmail [51] Xbox [77] Anino
26 Spotify [52] Mediafire [78] Custom

[a] About [m] Main Menu [o] Exit

?] Select one of the options > 1

```

Figure 55: Sélectionnez l'option Facebook

Et voilà une série de 4 URL malveillantes qui apparaît.

```

root@souha: /home/souha/PyPhisher
[By KasRoudra]

[•] Initializing PHP server at localhost:8080....
[+] PHP Server has started successfully!

souha@souha:~$ sudo -s
[sudo] Mot de passe de souha :
root@souha:/home/souha# git clone https://github.com/KasRoudra/PyPhisher.git
Clonage dans 'PyPhisher'...
remote: Enumerating objects: 237, done.
remote: Counting objects: 100% (237/237), done.
remote: Compressing objects: 100% (113/113), done.
remote: Total 237 (delta 124), reused 214 (delta 108), pack-reused 0
Réception d'objets: 100% (237/237), 2.42 Mio | 2.08 Mio/s, fait.
Résolution des deltas: 100% (124/124), fait.
root@souha:/home/souha#

```

Figure 56: URL Facebook malicieux

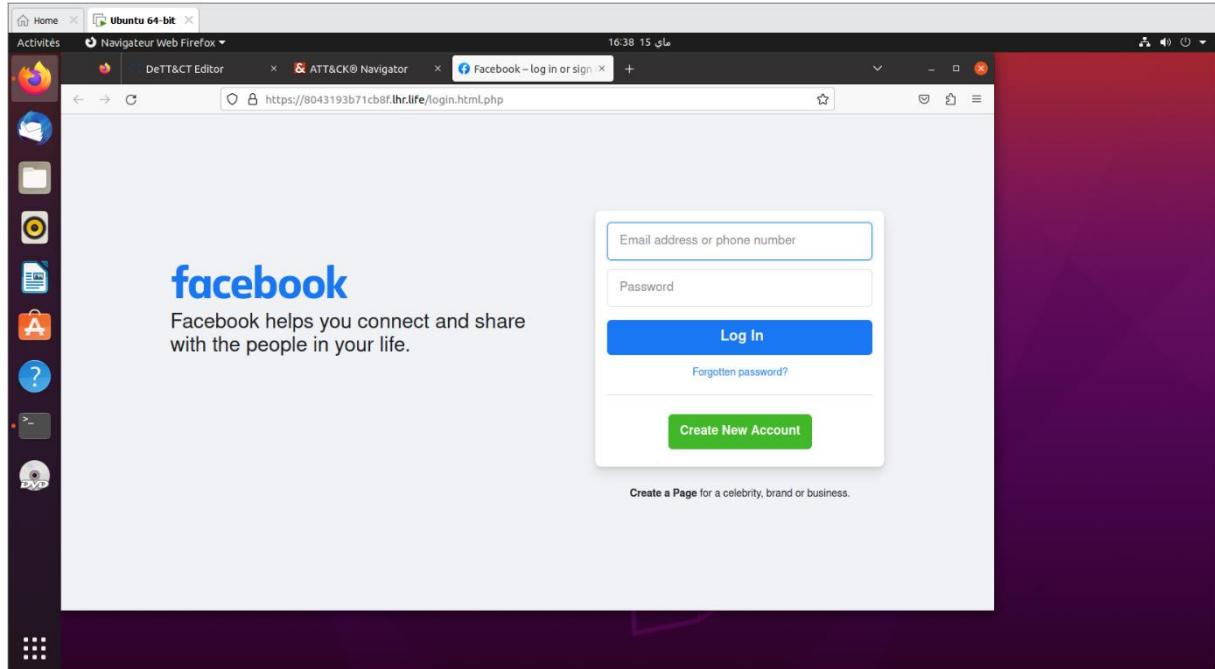


Figure 57: La page malicieuse Facebook

Si nous ouvrons l'URL, une page Facebook s'affichera et il paraît comme une page officielle.

8.2. Attaque sur Instagram

Le deuxième cas est l'Instagram. Nous tapons 5.

```

Activités Terminal 18:47 11 آی
root@souha: /home/souha/PyPhisher

[01] Facebook Traditional [27] Reddit [53] Gitlab
[02] Facebook Voting [28] Adobe [54] Github
[03] Facebook Security [29] DevianArt [55] Apple
[04] Messenger [30] Badoo [56] iCloud
[05] Instagram Traditional [31] Clash OF Clans [57] Vimeo
[06] Insta Auto Followers [32] Ajio [58] MySpace
[07] Insta 1000 Followers [33] JioRouter [59] Venmo
[08] Insta Blue Verify [34] FreeFire [60] Cryptocurrency
[09] Gmail Old [35] Pubg [61] SnapChat2
[10] Gmail New [36] Telegram [62] Verizon
[11] Gmail Poll [37] Youtube [63] Wi-Fi
[12] Microsoft [38] Airtel [64] Discord
[13] Netflix [39] Socialclub [65] Roblox
[14] Paypal [40] Olx [66] UberEats
[15] Steam [41] Outlook [67] Zomato
[16] Twitter [42] Amazon [68] WhatsApp
[17] PlayStation [43] Origin [69] PayTM
[18] TikTok [44] DropBox [70] PhonePay
[19] Twitch [45] Yahoo [71] Mobikwik
[20] Pinterest [46] WordPress [72] Hotstar
[21] SnapChat [47] Yandex [73] FlipCart
[22] LinkedIn [48] StackOverflow [74] Teachable
[23] Ebay [49] VK [75] Mail
[24] Quora [50] VK Poll [76] CryptoAtr
[25] Protonmail [51] Xbox [77] Amino
[26] Spotify [52] Mediafire [78] Custom

[a] About [m] Main Menu [0] Exit

[?] Select one of the options > 5
[?] Do you want OTP Page? [y/n] > n
[?] Enter shadow url (for social media preview)[press enter to skip] :

```

Figure 58: Sélectionnez l'option Instagram

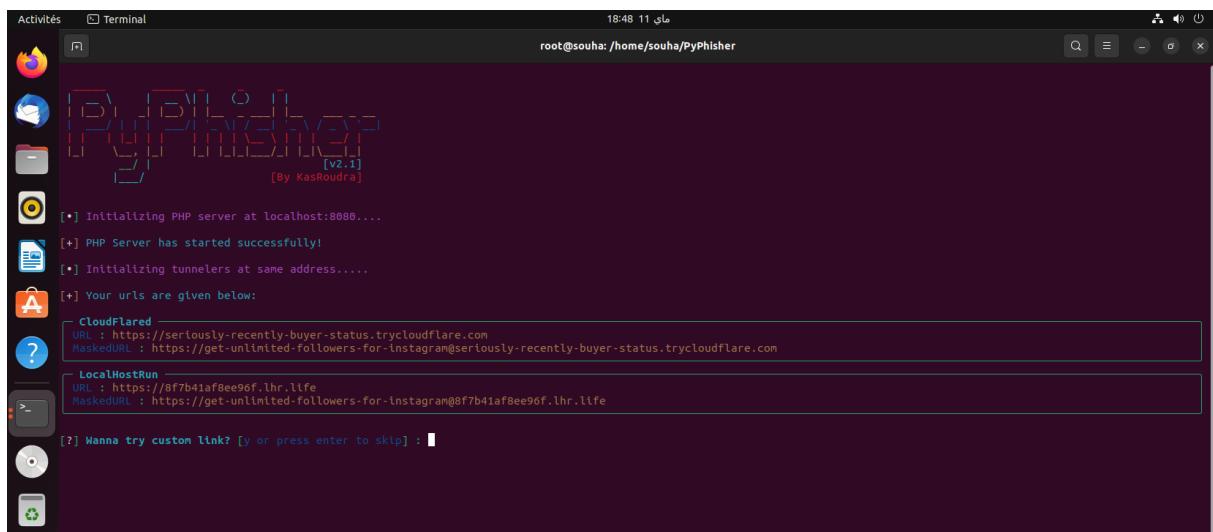


Figure 59: URL Instagram malicieux

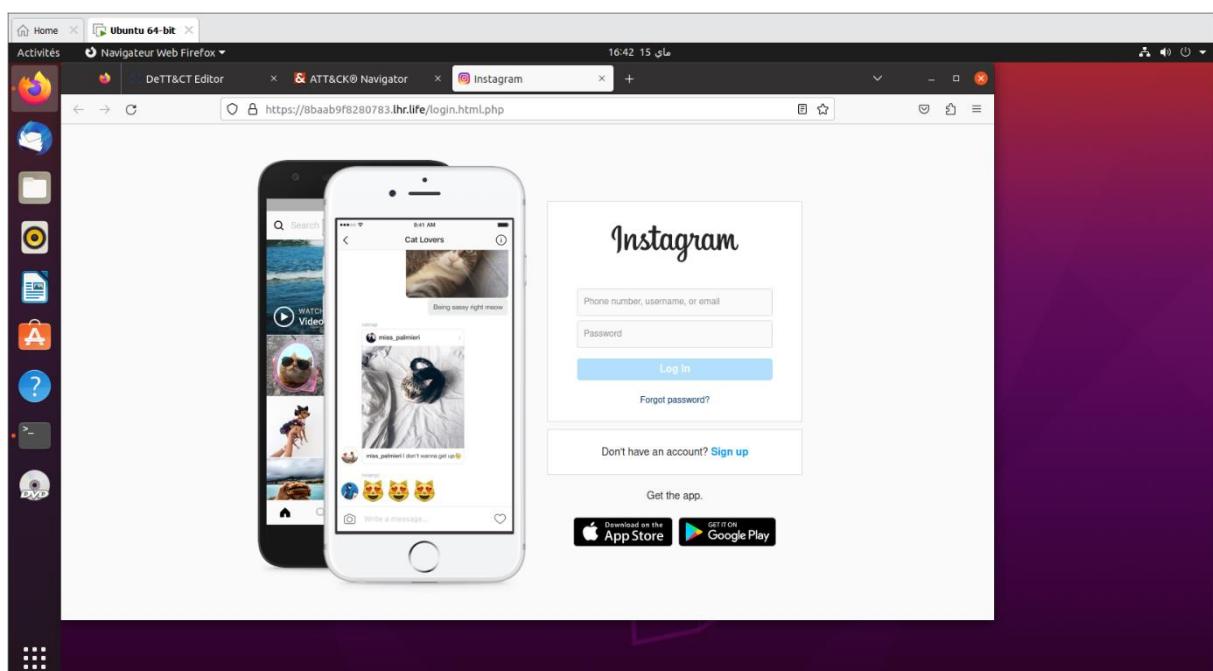


Figure 60: La page malicieuse d'Instagram

8.3. Attaque sur Gmail

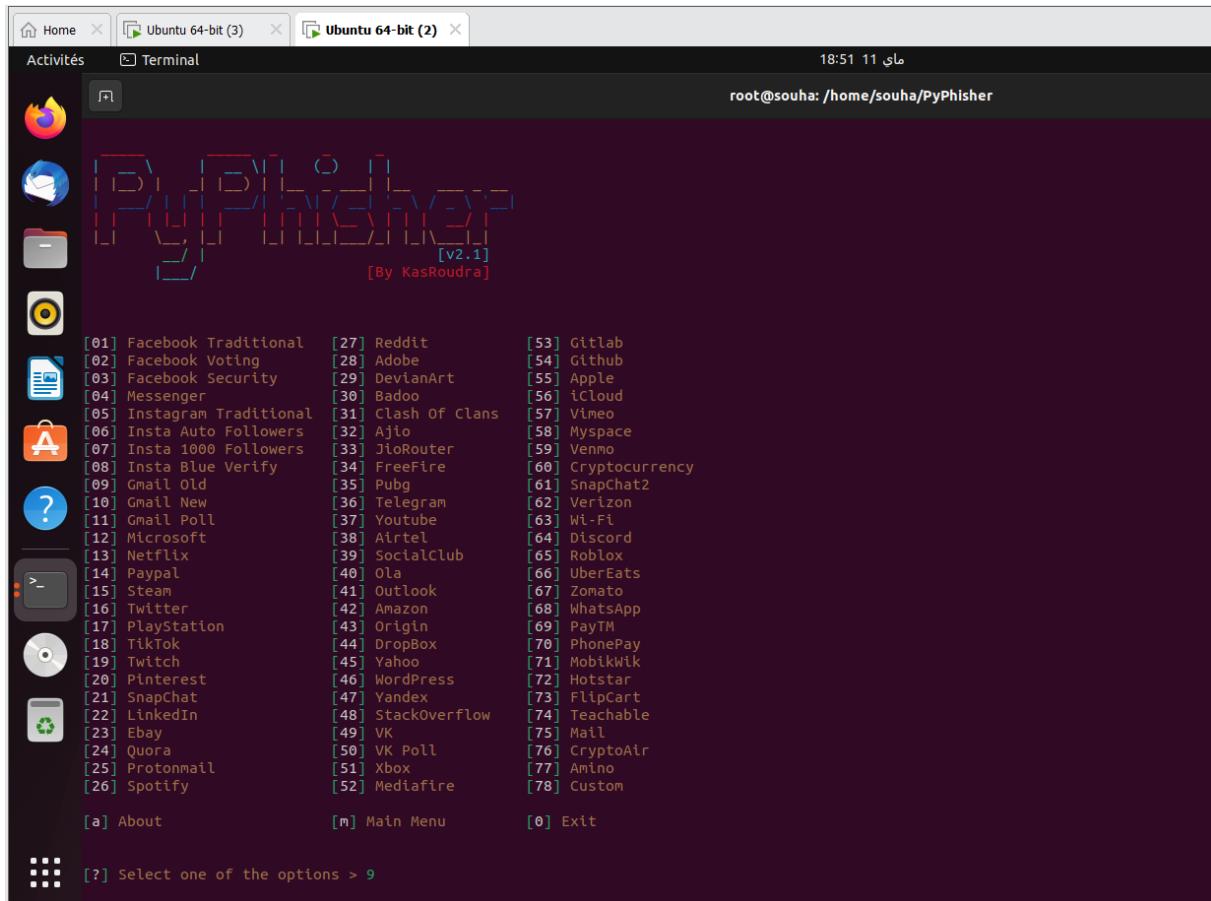


Figure 61: Sélectionnez l'option Gmail

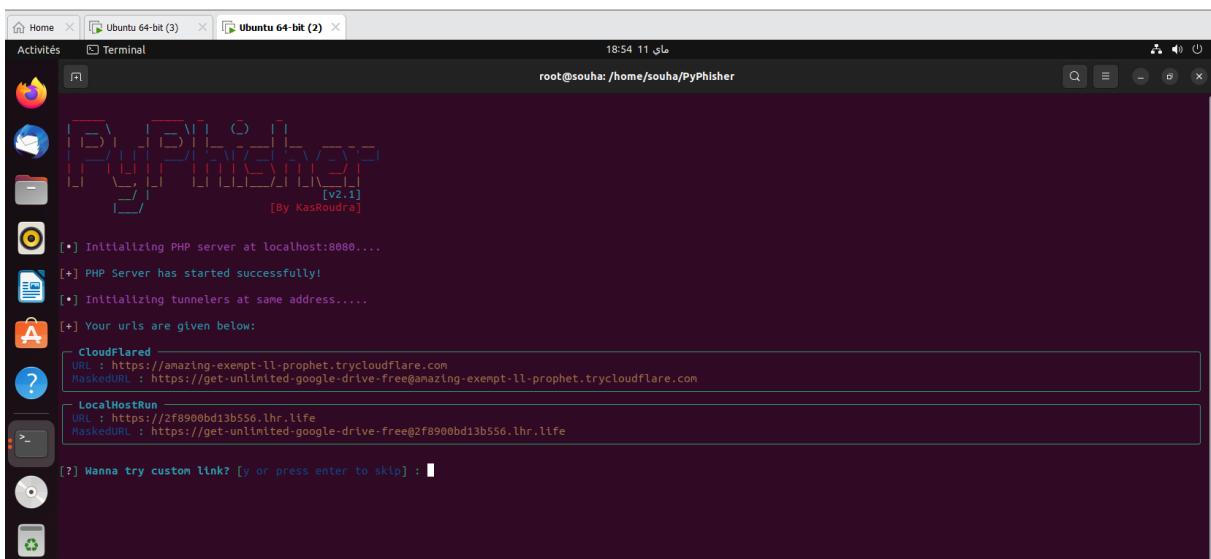


Figure 62: URL Gmail malicieux

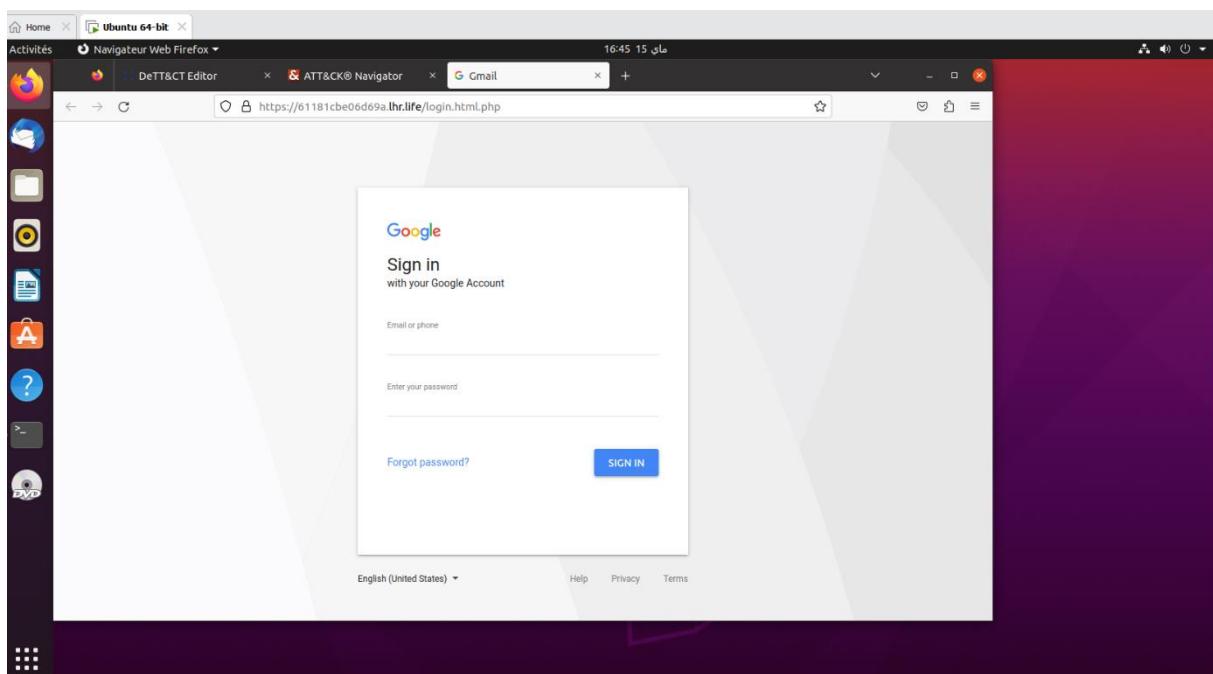


Figure 63: La page malicieuse de gmail

Et voilà un victime qui accède à cette page malicieuse et saisie ses coordonnées (l'adresse email et le mot de passe)

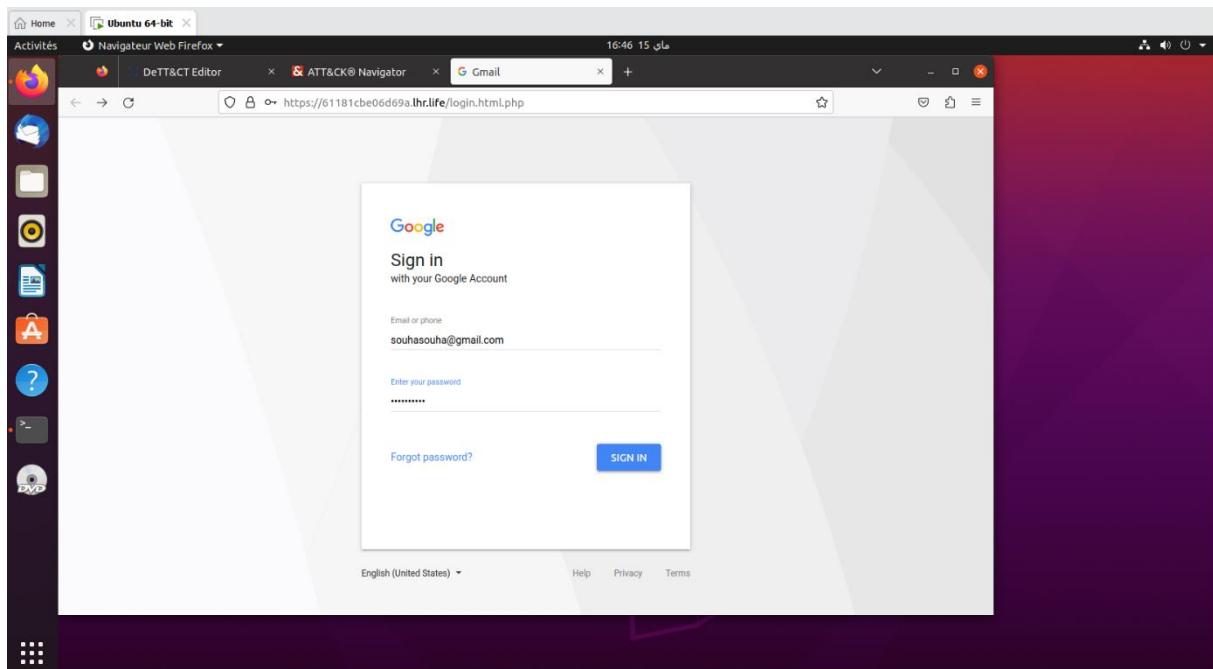


Figure 64: les données d'une victime

Les informations d'identification saisies sont capturées par l'outil PyPhisher

```

root@souha:/home/souha/PyPhisher
[*] User OS      : Ubuntu
[*] User Agent   : Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/111.0
[*] Version       : Linux
[*] Browser       : Firefox
[*] Location      : Manouba, Tunisia, Africa
[*] Geolocation(lat, lon): 36.8110561, 10.0909495
[*] Currency      : Tunisian Dinar

[*] Saved in ip.txt
[+] Waiting for next.....Press Ctrl+C to exit

[V] Victim IP found!

pyPhisher Data
[*] IP           : 102.158.236.151
[*] IP Type      : IPv4
[*] User OS      : Ubuntu
[*] User Agent   : Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/111.0
[*] Version       : Linux
[*] Browser       : Firefox
[*] Location      : Manouba, Tunisia, Africa
[*] Geolocation(lat, lon): 36.8110561, 10.0909495
[*] Currency      : Tunisian Dinar

[*] Saved in ip.txt
[+] Waiting for next.....Press Ctrl+C to exit

[V] Victim login info found!

pyPhisher Data
[*] Gmail Username: souhasouha@gmail.com
[*] Password: lssatgafsa

[*] Saved in creds.txt
[+] Waiting for next.....Press Ctrl+C to exit

```

Figure 65: PyPhisher Data

Nous avons choisi un des URL précédentes et nous l'analyserons par VIRUSTOTAL et voilà le résultat c'est un url malicieux.

Security vendor	Result	Notes
Anti-AVL	Malicious	
Emsisoft	Phishing	
Fortinet	Phishing	
Seclookup	Malicious	
Webroot	Malicious	
Acronis	Clean	
AICC (MONITORAPP)	Clean	
Avira	Phishing	
ESET	Phishing	
Netcraft	Malicious	
Sophos	Phishing	
Abusix	Clean	
ADMINUSLabs	Clean	
AlienVault	Clean	

Figure 66 : Analyse d'un URL malicieux

9. Bloquer une attaque de phishing [5]

Une bonne politique de sécurisation du système de messagerie consiste à utiliser plusieurs niveaux de protection. Les trois technologies qui sont les plus utilisées aujourd’hui, SPF, DKIM et DMARC, elles permettent d’authentifier et légitimer un email et son expéditeur.

9.1. SPF

SPF (Sender Policy Framework) : Implémentation de la partie IP

C'est un protocole de validation de courrier électronique conçu pour détecter et bloquer l’usurpation de courrier électronique qui permet aux échangeurs de courriers de vérifier que le courrier entrant d'un domaine provient d'une adresse IP autorisée par l'administrateurs de ce domaine.

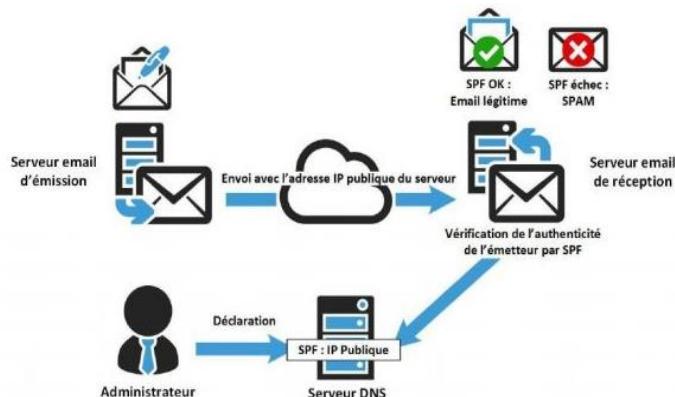


Figure 67: Fonctionnement de SPF

9.2.DKIM

DKIM (Domains Keys Identified Mail) : Implémentant une signature des mails.

Permet d’assurer le transit du mail fait partie de type de solution de la méthode d’authentification des mails qui va rajouter une signature numérique au niveau du message sortant.

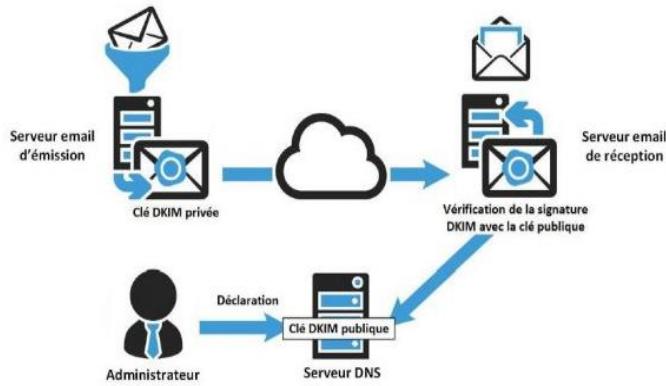


Figure 68: Fonctionnement de DKIM

8.1 DMARC :

DMARC (Domaine-base Message Authentication, Reporting et Conformance) fait partie de courrier de mail qui permet d'assurer un canal sécurisé il permet à toute administrateur d'authentifier, détecter et empêcher les attaquants du circuit d'identité de l'organisme et les techniques d'usurpation de courrier son approche se base principalement sur le SPF et le DKIM.



Figure 69: Fonctionnement de DMARC

10.Anti SPAM

L'anti spam a pour but de filtrer les logiciels malveillants, les messages publicitaires et les ransomwares sur un compte de messagerie électronique en vue de supprimer les courriers indésirables. Il permet de

- Analyser des mails.
- Bloquer des adresses URL malveillantes.
- Protéger contre le phishing et les fuites données.
- Identifier les menaces avant qu'elles soient déployées.

On ne peut pas forcément être capable de pouvoir se protéger contrairement des mails de phishing et encore en plus de tous ces différents éléments qui vont pouvoir être mis en place il faut avoir des mesures préventives

- Mettre en place des mesures de sensibilisation des compagnies de phishing.
- Sécurisation des serveurs mails avec DKIM, SPF et DMARC.
- Mesures réactives.
- Effectuer une sauvegarde et exploitation du Mail.
- Effectuer une analyse du Mail.
- La mise en place de stratégies de blocage de Mail (Application des contre-mesures).

11. Conclusion

Ce chapitre présente la partie conception et la réalisation pratique : collecte des data-sources, collecte des données personnelles fuitées, analyse et scan des sites Web et enfin la réalisation d'une attaque de phishing avec usurpation de site Facebook, Instagram et Gmail. Une dernière partie est réservée pour la présentation de quelques contre-mesures pour éviter l'attaque phishing.

Conclusion Générale

Aujourd'hui, la sécurité informatique est quasiment indispensable au bon fonctionnement d'un réseau filaire ou sans fil. Aucune entreprise ne peut se targuer d'avoir mis en place une infrastructure réseau, quelle que soit sa taille, sans envisager une politique de sécurité et sans chercher en permanence à améliorer le niveau de sécurité.

L'objectif principal de ce travail était de mettre en place un SOC qui s'agit d'une solution de sécurité qui tente à faire la collecte, l'analyse et la corrélation de gros trafic en temps réel afin d'éviter les attaques et de gagner le temps. Pour se faire, nous avons utilisé divers logiciels et outils, à savoir, les Framework de Mitre ATT&CK, DeTT&CT et D3FEND. Nous avons appliqué également les deux plateformes Have I Been Pwned et Dehashed pour analyser les Leaks afin de voir les données personnelles fuitées.

Le présent travail traite aussi l'analyse des URL ainsi que les pièces jointes des mails de phishing suite à l'application des deux outils URLscan et VIRUSTOTAL. Comme résultat, nous avons pu implémenter des moyens qui permettent d'éviter les attaques de phishing.

Références Bibliographiques

- [1] <https://attack.mitre.org/>
- [2] <https://attack.mitre.org/matrices/enterprise/>
- [3] Alphorm.com
- [4] <https://www.appvizer.fr/magazine/services-informatiques/protection-donnees/fuite-de-donnees>
- [5] <https://blog.devensys.com/2020/06/07/spf-dkim-dmrc-securite-mail/>
- [6] <https://cloudyhappypeople.com/2021/04/17/using-detect-and-the-mitre-attack-framework-to-assess-your-security-posture/>
- [7] https://clusif.fr/wp-content/uploads/2017/03/clusif-2017-deploiement-soc_vf.pdf CLUB DE LA SECURITE DE L'INFORMATION FRANÇAIS : Comment réussir le déploiement d'un SOC
- [8] <https://www.comptia.org/blog/cybersecurity-red-team-or-blue-team>
- [9] <https://d3fend.mitre.org/>
- [10] <https://www.emagged.com/blog/penetration-testing-methodology>
- [11] <https://www.ibm.com/fr-fr/topics/security-operations-center>
- [12] <https://mitre-attack.github.io/attack-navigator/>
- [13] <https://github.com/KasRoudra/PyPhisher>
- [14] <https://github.com/rabobank-cdc/DeTECT>
- [15] <https://learn.microsoft.com/fr-fr/iis/extensions/working-with-urlscan/urlscan-faq>
- [16] <https://medium.com/@haircutfish/tryhackme-threat-intelligence-tools-task-1-room-outline-task-2-threat-intelligence-and-task-3-24bbfe94b9f3>
- [17] <https://purplesec.us/red-team-vs-blue-team-cyber-security/>
- [18] Richea Perry on linkedIn : Cybersecurity & GRC Professional | TRECCERT Certified Trainer| Content Creator (Udemy Courses) | Active Directory Security | Podcaster(CyberJA) | OCEG-GRCP,GRCA,IPMP I Aspiring CISO | Best Practices Guru
- [19] Sabri Boubaker , Majdi Hassen et Imen Berouiche :Guide de bonne gouvernance de la compagnie des phosphates de gafsa avec l'assistance technique et le soutien financier du Natural Ressource Governance Institut
- [20] <https://securityboulevard.com/2022/09/the-major-types-of-phishing-attacks-how-to-identify-them-the-definitive-guide/>

Résumé

La cybersécurité est un élément essentiel de la protection contre les cybermenaces et le maintien de la sécurité et de l'intégrité des systèmes d'information. En comprenant et en suivant les meilleures pratiques en matière de cybersécurité, les individus et les organisations peuvent réduire considérablement le risque de cyberattaques.

L'objectif de notre travail est la mise en place d'un centre opérationnel de sécurité (SOC) qui est un élément essentiel de l'infrastructure de sécurité d'une organisation. Cet élément est responsable de la surveillance, de la détection et de la réponse aux menaces et aux problèmes de sécurité afin de mettre l'accent sur les causes de fuites des données et éviter les URL, les pièces jointes malicieux et l'attaque de phishing.

Mot Clés : Sécurité, SOC, Blue Teams, Leaks, Phishing, Framework de Mitre

Abstract

Cybersecurity is an essential part of protecting against cyber threats and maintaining the security and integrity of information systems. By understanding and following cybersecurity best practices, individuals and organizations can significantly reduce the risk of cyber attacks. The objective of our work is to establish a Security Operations Centre (SOC) which is an essential part of any organization's security infrastructure, responsible for monitoring, detecting and responding to security threats and issues in order to focus on the causes of data leakage and how to avoid malicious URLs, attachments and also avoid phishing attacks.

Keywords : Security, SOC, Blue Teams, Leaks , Phishing , Mitre Framework

