

## RAPPORT DE PROJET DE FIN D'ETUDE

Présenté en vue de l'obtention de  
LICENCE EN INFORMATIQUE, RÉSEAUX ET TÉLÉCOMMUNICATIONS

Spécialité : Télécommunication

---

Par ACHOUR MALEK ET LANDOULSI GHASSEN

Réalisé au sein de l'Agence Nationale de Sécurité Informatique



Encadrant Professionel : Mohamed Ali Ben Mabrouk

Période De Stage : 25/01/2022 - 15/05/2022

Année Universitaire : 2021 - 2022

## RAPPORT DE PROJET DE FIN D'ETUDES

Présenté en vue de l'obtention de la  
LICENCE EN INFORMATIQUE, RÉSEAUX ET TÉLÉCOMMUNICATIONS

Spécialité : Télécommunication

---

Par ACHOUR MALEK ET LANDOULSI GHASSEN

Réalisé au sein de l'Agence Nationale de Sécurité Informatique



### Autorisation de dépôt du rapport de Projet de Fin d'Etudes :

Encadrant Professionnel :  
Mohamed Ali Ben Mabrouk

Le :  
Signature :

Encadrant Académique :

Le :  
Signature :

# Dédicaces

c'est avec grand plaisir que je dédie ce modest travail à

A mes très chères mères

Quoi que je fasse ou que je dise, je ne saurai point te remercier comme il se doit. Tes affections me couvrent, tes bienveillances me guident et tes présences à mes côtés ont toujours été ma source de force pour affronter les différents obstacles.

A mon très cher père

Tu as toujours été à mes côtés pour me soutenir et m'encourager. Que ce travail traduit ma gratitude et mon affection.

A mes frères

je vous suis très reconnaissante de vos encouragements. J'espère toujours vous rendre heureux et fiers de moi.

A mon binôme

Pour son soutien moral, sa patience et sa compréhension tout au long de ce projet.

Sans oublier mes amies qui m'ont soutenu durant les moments de faiblesse et qui m'ont donné du courage et de la force pour continuer mon parcours.

**Achour Malek**

# Dédicaces

Je dédie ce projet à...

**Landoulsi Ghassen**

# Remerciements

start writing here...

# Table des matières

<b>Introduction Générale</b>	<b>1</b>
<b>1 Cadre du projet</b>	<b>2</b>
I Présentation Générale de l'Organisme d'Accueil . . . . .	2
I.1 Présentation de la Société ANSI . . . . .	2
I.2 Missions de L'ANSI . . . . .	2
II Présentation générale du projet . . . . .	3
II.1 Cadre de projet . . . . .	3
II.2 Problématique . . . . .	3
II.3 Etude de l'existant . . . . .	4
II.4 Solution proposée . . . . .	4
III Présentation de la sécurité informatique . . . . .	4
III.1 Objectifs de la sécurité informatique . . . . .	5
III.2 Les causes de l'insécurité . . . . .	5
III.3 Statistiques sur le cyberspace Tunisien . . . . .	5
IV Etude des attaques informatiques . . . . .	7
IV.1 DOS ou DDOS (Denial Of Service / Distributed Denial Of Service) . . . . .	8
IV.2 Phishing . . . . .	8
IV.3 Man in the middle (MITM) . . . . .	9
IV.4 Ransomware . . . . .	9
IV.5 Force Brute . . . . .	10
IV.6 Injection SQL . . . . .	10
<b>2 Gestion de la politique de sécurité</b>	<b>12</b>
I Étude de l'architecture réseau . . . . .	12
I.1 Implémentation de l'architecture réseau . . . . .	12
II Étude des vulnérabilités . . . . .	13
II.1 Déni de service (DOS) . . . . .	13
II.2 Phishing . . . . .	13
II.3 Man in the middle . . . . .	20
II.4 SSH brute force . . . . .	23
II.5 Injection SQL . . . . .	26
<b>3 Modélisation</b>	<b>27</b>
I Introduction . . . . .	27
II Exemples des systèmes de sécurité informatique . . . . .	28
II.1 Firewall . . . . .	28
II.2 Antivirus . . . . .	28
III Les cyberattaques . . . . .	28

III.1	Anatomie d'une cyberattaque . . . . .	29
III.2	Impacts des cyberattaques . . . . .	29
III.3	Les types de cyberattaques . . . . .	29
IV	Security operation center (SOC) . . . . .	29
IV.1	Composition du SOC [3] . . . . .	30
IV.2	Ressources Humaines . . . . .	30
IV.3	Les Processus . . . . .	31
IV.4	Avantages du SOC . . . . .	32
V	Security Event Information Management (SIEM) . . . . .	32
V.1	Fonctionnement de SIEM . . . . .	34
V.2	Rôles du SIEM dans un SOC . . . . .	35
V.3	Les SIEMs open source les plus connues . . . . .	36
VI	Security Onion Solutions (SOS) . . . . .	36
VI.1	Fonctionnement de SOS . . . . .	37
VI.2	Etude comparative des solutions étudiées . . . . .	37
VII	Conclusion . . . . .	37
VIII	Introduction . . . . .	38
IX	Diagramme de classes . . . . .	38
X	Diagramme de séquences du système . . . . .	38
X.1	Diagramme de séquence du client : . . . . .	38
X.2	Diagramme de séquence de l'admin : . . . . .	38
XI	Conclusion . . . . .	39
<b>4</b>	<b>Réalisation</b>	<b>41</b>
I	Introduction . . . . .	41
II	Environnement de travail . . . . .	41
II.1	Environnement matériel . . . . .	41
II.2	Environnement logiciel . . . . .	41
III	Technologies utilisées : . . . . .	41
III.1	HTML5 : . . . . .	41
III.2	CSS3 : . . . . .	41
III.3	ReactJS : . . . . .	42
IV	Tâches Réalisées . . . . .	42
V	Conclusion . . . . .	42
<b>Conclusion Générale</b>		<b>43</b>
<b>Bibliographie</b>		<b>44</b>

# Liste de figures

1.1	L'Agence Nationale de Sécurité Informatique . . . . .	2
1.2	Objectifs de la sécurité informatique . . . . .	5
1.3	Évolution du nombre des événements détectés au cours de l'année 2020 . . . . .	6
1.4	Nombre des incidents traités au cours de l'année 2020 . . . . .	6
1.5	Attaques DDoS en Tunisie au cours de 2020 . . . . .	7
1.6	Évolution du nombre des événements détectés au cours de l'année 2019 vs 2020 . . . . .	7
1.7	Phishing attack . . . . .	8
1.8	Phishing attack . . . . .	9
1.9	Man in the middle attack . . . . .	9
1.10	Ransomware attack . . . . .	10
1.11	bruteforce attack . . . . .	10
1.12	Injection SQL attack . . . . .	11
2.13	Scénario de phishing . . . . .	13
2.14	. . . . .	14
2.15	. . . . .	15
2.16	. . . . .	15
2.17	. . . . .	16
2.18	. . . . .	16
2.19	. . . . .	16
2.20	Liste des URL . . . . .	17
2.21	. . . . .	17
2.22	. . . . .	17
2.23	. . . . .	18
2.24	. . . . .	18
2.25	Mail envoyé sur la machine de victime . . . . .	18
2.26	Contenu du mail envoyé . . . . .	19
2.27	Page login d'un compte Gmail . . . . .	19
2.28	Les informations d'identification du victime . . . . .	19
2.29	Scénario de Man in the middle . . . . .	20
2.30	Lancement de Ettercap . . . . .	21
2.31	Lancement de Ettercap . . . . .	21
2.32	Résultats du scan . . . . .	22
2.33	Chargement de wireshark . . . . .	22
2.34	Capture de wireshark . . . . .	23
2.35	Résultat . . . . .	23
2.36	Résultat du scan . . . . .	24
2.37	Création des dictionnaires . . . . .	25
2.38	Attaque et résultat . . . . .	25

2.39 Accéder au serveur . . . . .	26
3.40 Firewall . . . . .	28
3.41 Antivirus . . . . .	29
3.42 Composition du SOC . . . . .	30
3.43 Ressources Humaines . . . . .	30
3.44 Security Event Information Management . . . . .	33
3.45 Fonctionnalités du SIEM . . . . .	34
3.46 Schéma explicatif de SIEM . . . . .	35
3.47 Security Onion . . . . .	36
3.48 Security Onion . . . . .	36
3.49 Security Onion . . . . .	37
3.50 Diagramme de classe général . . . . .	38
3.51 Diagramme de séquence du client . . . . .	39
3.52 Diagramme de séquence de l'admin . . . . .	40

# Liste des tableaux

# Introduction Générale

L'utilisation des réseaux informatiques est devenue très importante pour toutes les entreprises modernes. Durant ces deux dernières années, la pandémie (Covid-19) que nous vivons cause une grave perturbation aux organisations de travail et suscite une certaine inquiétude chez les entreprises.

Pour cela de nombreuses entreprises ont élaboré des plans d'urgence pour la continuité des activités et obligent leurs employés à travailler à domicile pour limiter le risque de virus. Cependant, le télétravail s'est révélé un aspect crucial de la poursuite des activités des entreprises, mais il peut aussi comporter des risques.

En effet, cette pandémie a fait augmenter les activités de diverses cyber menaces : le phishing, le spam, l'attaque par rançongiciel, les attaques DDoS, etc ... De ce fait, les entreprises cherchent à adapter les défenses existantes à un nouveau paradigme l'infrastructure, en essayant de minimiser l'exposition à une variété de nouvelles attaques ainsi que de savoir les motivations des attaquants et de profiter des solutions efficaces et avancées pour simplifier la gestion et la traçabilité des incidents.

Afin de faire face à ces menaces informatiques, les entreprises doivent pouvoir espionner leurs réseaux et systèmes informatiques , afin d'identifier les actions malveillantes qui les menacent et de se prémunir de potentielles attaques avant qu'elles ne causent de graves dommages.

La mise en place des pare-feux, des antivirus, des systèmes de détection n'est pas suffisante pour sécuriser les données de l'entreprise. Nous avons besoin de collecter les logs, d'avoir une visibilité globale sur l'environnement de travail et de supervision.

Les attaques cybernétiques sont de plus en plus évolutives, nous migrons vers une sécurité plutôt dynamique incarnée aujourd'hui par le centre d'opération de sécurité (SOC).

Ce rapport, qui expose notre projet de fin d'étude, est composé de ..... chapitres structurés comme suit :

- Le premier chapitre sera consacré à la fois de présenter l'Organisme d'Accueil et de présenter le cadre de projet.
- Le deuxième chapitre intitulé « Etat de l'art » met l'accent sur la présentation des fondements de base de la sécurité des systèmes d'information ainsi que les technologies et solutions utilisées dans notre projet.
- Dans le troisième chapitre, on va présenter l'analyse et la spécification des besoins, ainsi que la conception de la solution.

# Chapitre 1

## Présentation du cadre du projet

### Introduction

Ce chapitre est consacré pour décrire l'environnement dans lequel s'est déroulé notre travail à travers une présentation de l'Agence Nationale de la Sécurité Informatique (ANSI) et par la suite, on va analyser l'existant en spécifiant les besoins ainsi que les solutions proposées.

### I Présentation Générale de l'Organisme d'Accueil

Cette partie est dédiée pour introduire notre société d'accueil qui est "Agence Nationale de Sécurité Informatique", dans lequel notre stage a été effectué.

#### I.1 Présentation de la Société ANSI

L'ANSI en tant que coordinateur national, œuvre à développer un climat de confiance des technologies de l'information pour rassurer les utilisateurs, l'état et les investisseurs et protéger les citoyens et les biens publics et privés contre toute menace cybernétique [1].



FIGURE 1.1 – L'Agence Nationale de Sécurité Informatique

#### I.2 Missions de L'ANSI

L'Agence Nationale de Sécurité Informatique effectue un contrôle général des systèmes informatiques et des réseaux relevant des divers organismes publics et privés. Elle est chargée essentiellement des missions suivantes :

- Veiller à l'exécution des orientations nationales et de la stratégie générale en systèmes de sécurité des systèmes informatiques et des réseaux.
- Suivre l'exécution des plans et des programmes relatifs à la sécurité informatique dans le secteur public à l'exception des applications particulières à la défense et à la connexion sécurité nationale et assurer la coordination entre les intervenants dans ce domaine.
- Assurer la veille technologique dans le domaine de la sécurité informatique.
- Établir des normes spécifiques à la sécurité informatique et élaborer des guides techniques en l'objet et procéder à leur publication.
- Oeuvrer pour encourager le développement de solutions nationales dans le domaine de la sécurité informatique et à les promouvoir conformément aux priorités et aux programmes qui seront fixés par l'agence.
- Participer à la consolidation de la formation et du recyclage dans le domaine de la sécurité informatique.
- Veiller à l'exécution des réglementations relatives à l'obligation de l'audit périodique de la sécurité des systèmes informatiques et des réseaux [2].

## II Présentation générale du projet

Ce projet, intitulé « Mise en place d'une plateforme SOC à base d'outils Open Source», s'inscrit dans le cadre du projet de fin d'études pour la gestion des incidents et de renseignement sur les menaces cybernétiques .

### II.1 Cadre de projet

Après une étude minutieuse et pragmatique de l'existant au sein de l'entreprise qui met l'accent sur la manière de minimiser l'exposition à une variété de nouvelles attaques, le projet consiste à implémenter une plateforme SOC Open source qui permettant la supervision et l'administration de la sécurité du système d'information à travers d'outils de collecte, de corrélation d'événements et d'intervention à distance. pour identifier, préparer et protéger les infrastructures des entreprises contre les cybermenaces.

### II.2 Problématique

Actuellement, Dans tous les domaines professionnels, c'est à dire gestion, organisation, production et communication, l'informatique i est l' outil dont nous ne pouvons plus nous passer.

Les informations qui circulent entre les réseaux, peuvent contenir des données personnelles ainsi que des bases de données des sociétés, des renseignements importants sur des personnes et qui sont susceptibles d'être menacées et exposées à toute sorte de malveillances.

Afin de sécuriser les systèmes informatiques ,l'organisation a mis en place des équipements de sécurité , tels que des pares-feux, des systèmes de détection d'intrusion (IDS) et des systèmes de prévention des intrusions (IPS) qui sont pris en compte comme des solutions efficaces contre les cybermenaces internes et externes. Pourtant, les attaques

informatiques sont devenues de plus en plus complexes, et la sécurité statique n'est plus suffisante. Aussi, les problèmes liés à la sécurité traditionnelle ci-dessous listés ont été constatés :

- Le manque de gestion de la conformité.
- La difficulté de détecter la source et la nature de l'attaque.
- Manque de gestion et de centralisation des journaux.
- L'absence de création d'alerte et de rapport.

Par conséquent, il est absolument important de trouver un moyen adéquat afin de bien protéger ces informations, pour bénéficier d'une visibilité globale sur la sécurité des SI.

## II.3 Etude de l'existant

Lors de la récente pandémie de covid, nous avons été témoins de la propagation de nombreuses cyberattaques. Lors de l'analyse de ces attaques, nous avons constaté que quelques-unes ont gagné en popularité parmi les pirates en raison de leur facilité d'exécution sur plusieurs nouveaux utilisateurs de l'internet .

## II.4 Solution proposée

La solution proposée consiste à mettre en place une plateforme « Open Source » avancée pour la gestion des incidents et de renseigner sur les menaces cybérénétiques (Cyber Threat Intelligence) : pour identifier, préparer et protéger les infrastructures des entreprises contre les cybermenaces. En effet, la plateforme a pour objectif de permettre les deux types de réponse aux incidents suivants :

### - Réponse préventive :

- Renseigner sur les menaces cybérénétiques : Détecter et prévenir les cybermenaces contre les infrastructures des entreprises.
- Repérer les menaces contre les infrastructures et recueillir, analyser et diffuser l'information connexe, et ce, d'une façon systématique.
- Rendre les données du renseignement disponibles sur une base de données afin de les diffuser entre les différents partenaires des milieux de la sécurité.

### - Réponse réactive :

- Simplifier la gestion des incidents afin de permettre une réaction rapide et leurs impacts, de prévenir toute aggravation et de tirer des leçons dans le but de mettre en place des pratiques exemplaires.

## III Présentation de la sécurité informatique

La sécurité informatique est une discipline qui consiste à protéger les ressources informatiques ; les équipements, les logiciels, les informations, les systèmes de communication. De manière générale, il consiste à s'assurer que les ressources matérielles ou logicielles d'une organisation sont utilisées uniquement dans le cadre prévu.

### III.1 Objectifs de la sécurité informatique

La sécurité informatique doit garantir fondamentalement cinq objectifs :

- **Authentification** : Il s'agit de s'assurer de l'identité de l'utilisateur, c'est à dire d'assurer à chaque correspondant que son partenaire est bien celui qu'il pense .
- **Confidentialité** : Cela inclut de s'assurer que seules les personnes autorisées peuvent accéder en lecture aux ressources échangées.
- **Intégrité** : C'est-à-dire garantir que les données n'ont pas été modifiées pendant la communication.
- **Disponibilité** : Le but de la disponibilité est d'assurer l'accès aux services ou aux ressources.
- **Non-répudiation** : C'est la garantie qu'aucun des correspondants ne pourra nier la transaction à l'émission et à la réception.

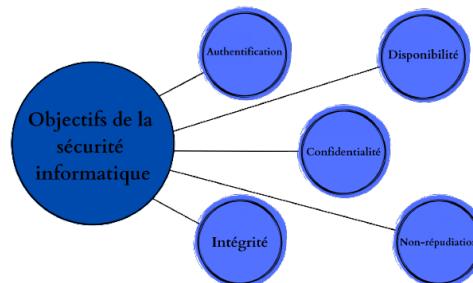


FIGURE 1.2 – Objectifs de la sécurité informatique

### III.2 Les causes de l'insécurité

On constate généralement deux types d'insécurité :

- **L'état actif** : C'est-à-dire la non-connaissance par l'utilisateur des fonctionnalités du système, dont certaines pouvant lui être nuisibles.
- **L'état passif** : C'est-à-dire la méconnaissance des moyens de sécurité mis en place, par exemple lorsque l'administrateur d'un système ne connaît pas les dispositifs de sécurité dont il dispose.

### III.3 Statistiques sur le cyberspace Tunisien

L'augmentation des cyberattaques s'explique par le recours massif aux solutions technologiques, notamment le télétravail à distance de plus en plus utilisé, surtout dans le cadre de la lutte contre la diffusion du virus durant l'épidémie du COVID 19 pour faire face aux défis imposés par la augmentation de la surface d'attaque.

En 2020, le nombre des cyberattaques a connu une hausse sans précédent. Selon Karim Mgannem, responsable veille à l'Agence nationale de la sécurité informatique (Ansi), plus de 20.000 incidents ont été détectés et déclarés par l'agence. Près de 330 ont été traités par l'équipe de traitement des incidents.

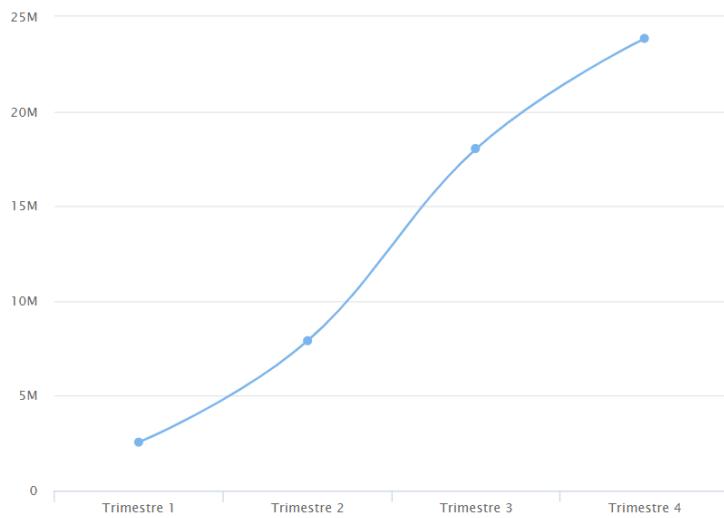


FIGURE 1.3 – Évolution du nombre des événements détectés au cours de l'année 2020

Le graphique de la figure 1.4 illustre les types d'attaque récurrents et les plus répandus dans la pandémie : les attaques DDos ; 45 incidents, le Fishing dont 95 cas ont été traiter, les attaques ransomware plus de 120 et d'extorsion 70 incidents.

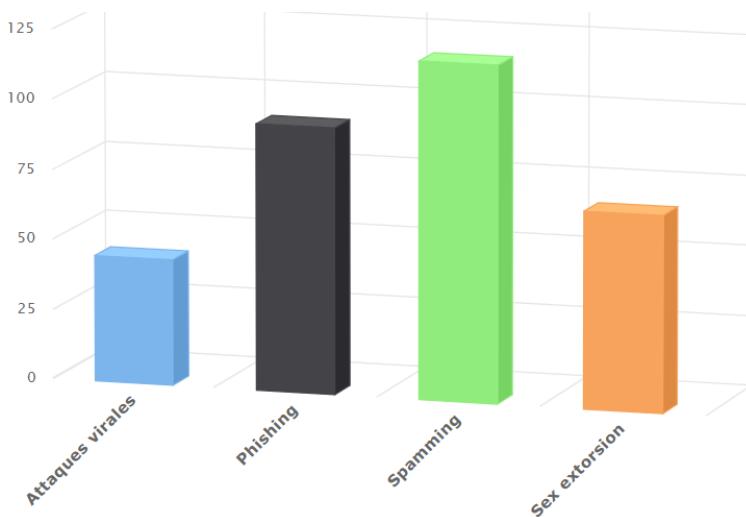


FIGURE 1.4 – Nombre des incidents traités au cours de l'année 2020

Durant cette période de crise, la flambée des attaques DDos était remarquable. Cette attaque est considérée, aujourd’hui, comme étant l’attaque la plus perturbante et redoutable de l’internet moderne. En effet, l’ANSI a détecté 994 attaques DDos en Tunisie au cours de l’année 2020.

Les attaques ont été multipliées par trois par rapport au nombre enregistré en 2019. Pour l’analyste, la hausse des cyberattaques, enregistrée en 2020, était prévue compte tenu de l’utilisation intensive de solutions technologiques pour faire face aux défis imposés par la propagation du virus. “L’année 2020 était caractérisée par de longues périodes de confinement. Il y a eu un recours très important au travail à distance”.

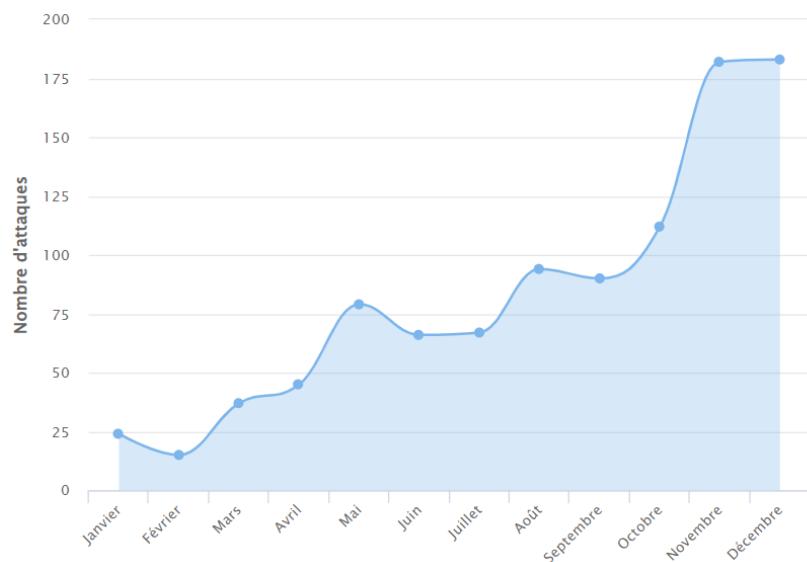


FIGURE 1.5 – Attaques DDoS en Tunisie au cours de 2020

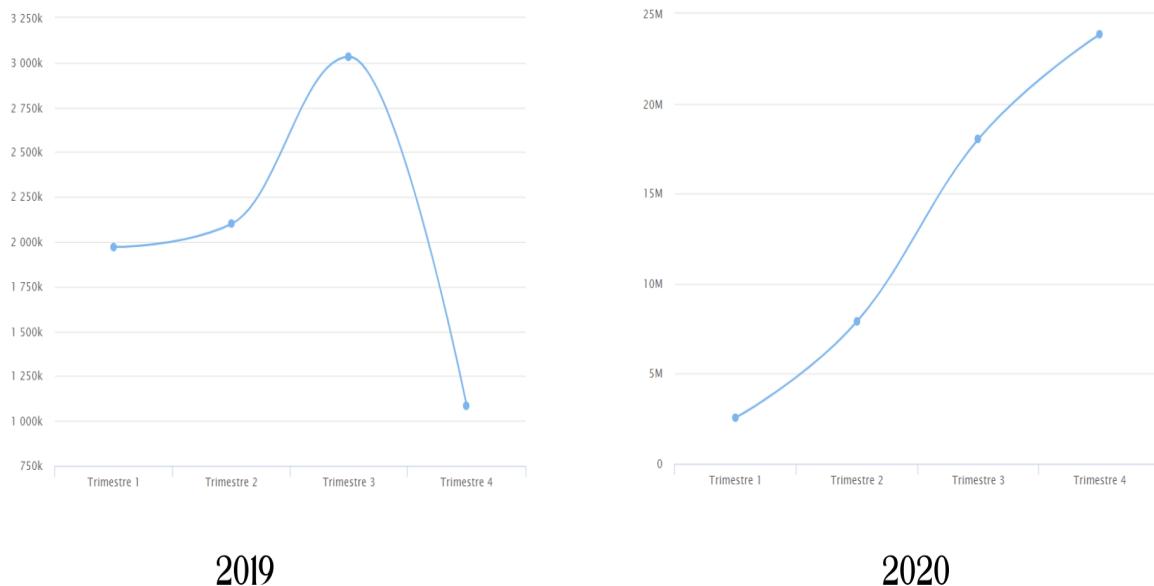


FIGURE 1.6 – Évolution du nombre des événements détectés au cours de l'année 2019 vs 2020

La figure 1.6 illustre que depuis le début de covid en 2019, le nombre d'attaques détectées a augmenté au cours des trois premiers trimestres, passant de 2 000 à plus de 3 000 attaques et au quatrième trimestre, il a chuté en raison des vacances et du fait que les travailleurs retournent à leurs bureaux et n'ont plus de travail à distance.

## IV Etude des attaques informatique

La cybersécurité fait référence à la protection des systèmes connectés à Internet contre les menaces présentes dans le cyberspace. Cette approche implique la protection des

logiciels, des données et du matériel et aide à empêcher les cybercriminels d'accéder aux appareils ou aux réseaux. Pour ce faire, il est d'abord nécessaire de connaître le mécanisme de fonctionnement de ces attaques afin de comprendre et de préciser clairement les actions qui peuvent être menées contre ces attaques, nous présentons les principales parmi celles pouvant être détectées par les systèmes de monitoring du cyberspace.

## IV.1 DOS ou DDOS (Denial Of Service / Distributed Denial Of Service)

Avec la croissance exponentielle du volume des données sur le Web, les attaques par déni de service distribuées sont de plus en plus fréquentes. Une attaque DDoS vise à rendre un serveur, un service ou une infrastructure indisponible. En effet, ce type d'attaque peut prendre différentes formes : une saturation de la bande passante du serveur pour le rendre inreachable, un épuisement des ressources système de la machine, l'empêchant ainsi de répondre au trafic légitime.

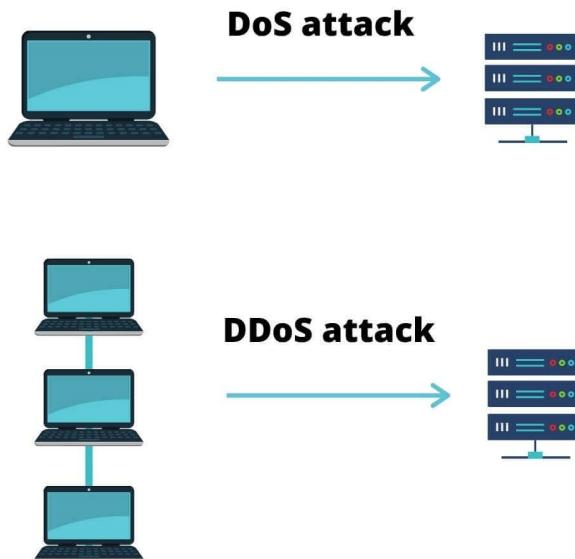


FIGURE 1.7 – Phishing attack

## IV.2 Phishing

Cette attaque combine l'ingénierie sociale et les compétences techniques, elle commence par un e-mail ou une autre communication destiné à tromper une victime. Le message semble provenir d'une personne de confiance. Si la victime tombe dans le piège, on lui demande de fournir des informations confidentielles, souvent sur un site web frauduleux. Parfois, des programmes malveillants sont également téléchargés sur l'ordinateur de la cible.



FIGURE 1.8 – Phishing attack

### IV.3 Man in the middle (MITM)

L'attaque de man-in-the-middle (MITM) ou l'homme du milieu attack est une technique d'attaque informatique qui a pour but d'intercepter les communications entre deux parties dans un même réseau. Toutes les formes de communications en ligne, telles que les réseaux sociaux, les e-mails, la navigation internet, sont susceptibles d'être corrompues par un cybercriminel. En effet, l'attaquant est capable d'observer l'échange et récupérer des données et par la suite il peut les utiliser, alterer ou les supprimer.

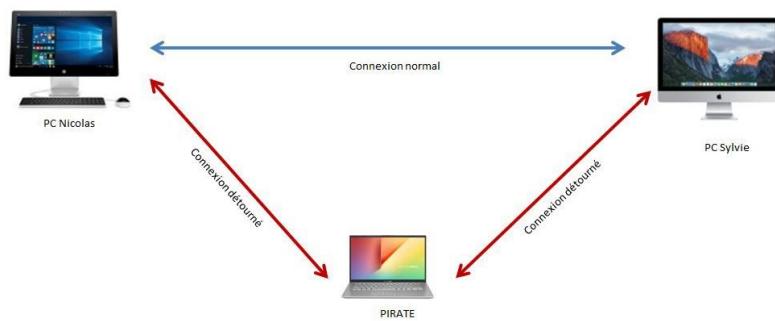


FIGURE 1.9 – Man in the middle attack

### IV.4 Ransomware

C'est un programme malveillant conçu pour pirater les ordinateurs ou des appareils mobiles et forcer les victimes à payer une rançon pour que leurs fichiers soient déchiffrés. Les pirates informatiques infectent votre ordinateur/mobile en vous demandant de télécharger la pièce jointe malveillante attachée à un e-mail ou de vous rendre sur un site contenant un code, qui chiffre par la suite vos fichiers critiques ou vous refuse l'accès à votre ordinateur.



FIGURE 1.10 – Ransomware attack

## IV.5 Force Brute

C'est une technique qui consiste à tester, l'une après l'autre, chaque combinaison possible d'un mot de passe ou d'une clé pour un identifiant donné afin de se connecter au service ciblé. Il s'agit d'une méthode ancienne et répandue chez les pirates. Le temps nécessaire à celle-ci dépend du nombre de possibilités, de la vitesse que met l'attaquant pour tester chaque combinaison et des défenses qui lui sont opposées.



FIGURE 1.11 – bruteforce attack

## IV.6 Injection SQL

C'est une technique d'injection d'un morceau de code utilisée pour modifier ou extraire des données de bases de données SQL. En insérant des instructions SQL spécialisées dans un champ de saisie, un attaquant est capable d'exécuter des commandes non autorisées sur la base de données SQL d'une victime et de détruire des données sensibles ou d'autres comportements de manipulation.

Avec l'exécution correcte des commandes SQL, le hacker peut usurper l'identité d'un utilisateur plus privilégié, se faire passer pour lui-même ou pour d'autres

administrateurs de base de données, altérer les données existantes, modifier les transactions et les soldes, et récupérer et/ou détruire toutes les données du serveur.

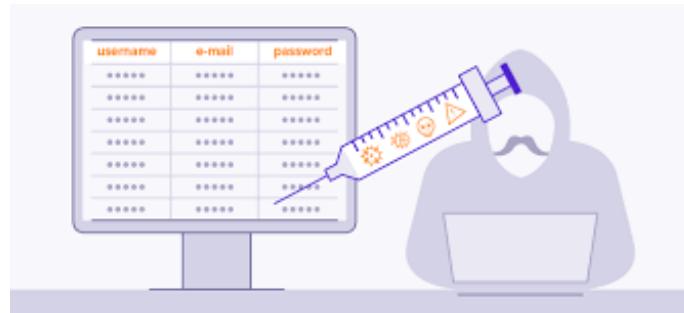


FIGURE 1.12 – Injection SQL attack

## Conclusion

Dans ce premier chapitre on a présenté l'organisation d'accueil de notre projet ainsi que le cadre général du projet. Dans ce qui suit, nous trouvons la phase d'études de sécurité dans laquelle nous présenterons des nombreux types d'attaques qui peuvent affecter la sécurité de notre réseau. Le chapitre suivant portera sur

# **Chapitre 2**

## **Gestion de la politique de sécurité**

### **Introduction**

L'objectif de ce chapitre est de donner un aperçu global sur l'architecture réseau. Par la suite nous allons exposer dans la deuxième partie les majeurs vulnérabilités par l'application des attaques les plus fréquentes.

### **I Étude de l'architecture réseau**

#### **I.1 Implémentation de l'architecture réseau**

## II Étude des vulnérabilités

### II.1 Déni de service (DOS)

- 1) Généralités
- 2) Scénario
- 3) Outils
- 4) Réalisation

### II.2 Phishing

- 1) Généralités

Le phishing est le principal le plus utilisé par les cybercriminels pour voler des informations personnelles et/ou bancaires. Par message électronique, SMS ou encore par téléphone, il vise à usurper l'identité d'un tiers de confiance pour tromper la victime et l'inciter à communiquer ses données personnelles sensibles , ses identifiants et mots de passe, ses numéros de carte bancaire ou bien sa carte d'identité numérisée.

- 2) Scénario

Le pirate envoie un e-mail de phishing contenant ce qui semble être une faille de sécurité sur l'un des comptes de réseaux sociaux de la victime (instagram/facebook/twitter...). Ce dernier ouvre le courrier avec manque de conscience et clique sur le lien dont il essaie de se connecter avec ses données personnelles.

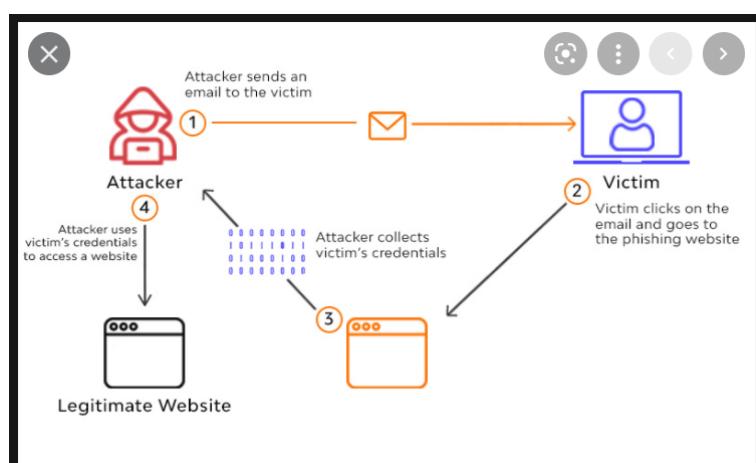


FIGURE 2.13 – Scénario de phishing

- 3) Outils

Les outils utilisés lors de cette attaque :

**- Pc exécutant le système d'exploitation « Parrot Os »**

Parrot OS est une distribution GNU/Linux gratuite et open source, orientée sécurité informatique basée sur une Debian et avec un environnement de bureau MATE. Il est

conçu pour les experts en sécurité, les développeurs et les personnes soucieuses de la confidentialité.

L'objectif de Parrot Security OS est de fournir une distribution regroupant l'ensemble des outils nécessaires aux tests de sécurité informatique. Elle contient également tout ce dont vous avez besoin pour développer vos propres programmes ou protéger votre vie privée et des outils nécessaires pour être un parfait hacker.

#### - Le framework «PhishMailer»

PhishMailer est un outil de phishing, open source et codé en python. Il est utilisé pour effectuer des attaques de phishing sur Target. En effet, il contient des modèles des pages Web de phishing tels que Facebook, Instagram, Google ... etc ou bien des modèles personnalisés. Cet outil permet d'effectuer facilement cette attaque dont il fait preuve de beaucoup de créativité pour rendre l'e-mail aussi légitime que possible.

#### - Le framework «Zphisher»

Zphisher est un outil de phishing avancé, développé par hr-tech. Il permet aux pirates d'effectuer des attaques de phishing des informations d'identification des réseaux sociaux. Cet outil dispose de 30 modèles pour différentes plateformes de médias sociaux. Il offre non seulement la possibilité de créer n'importe quel modèle mais aussi son lien URL .

#### - Le framework «MaskPhish»

Maskphisher est un outil gratuit, open source et qui est écrit en langage bash. Cet outil peut effectuer des attaques d'ingénierie sociale sur les victimes. En effet, il est utilisé pour masquer tous types de liens de phishing ou URL derrière le lien d'origine. Maskphish vous donne la flexibilité de l'utiliser selon les besoins.

## 4) Réalisation

Après avoir téléchargé "PhishMailer" sur notre machine parrotos, maintenant on exécute l'outil avec la commande suivante.

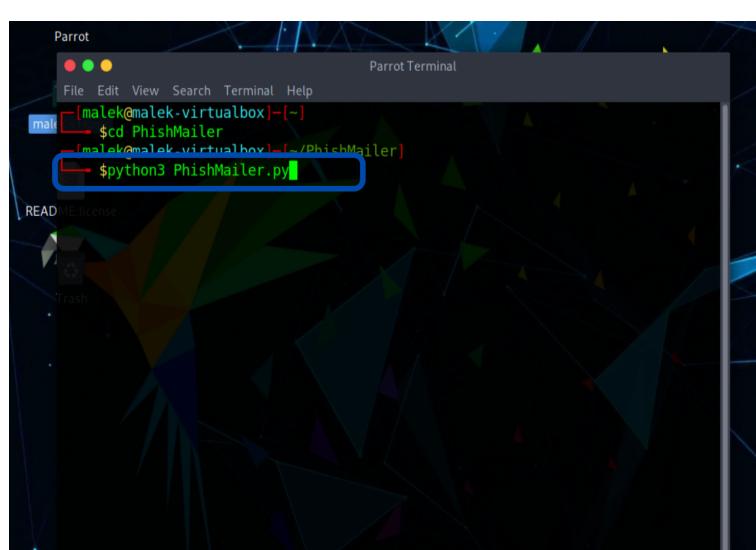


FIGURE 2.14 –

Tout d'abord il faut créer le mail de phishing on générant un modèle pour des sites populaires tels que Facebook, Instagram, Google, Snapchat, GitHub, Yahoo, Proton mail, Spotify, Netflix, LinkedIn, WordPress, Origin, Steam, Microsoft, ...etc.

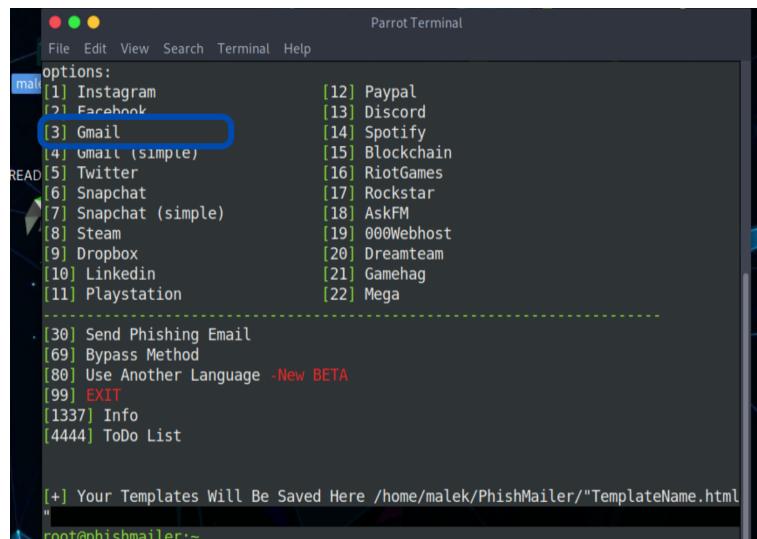


FIGURE 2.15 –

La figure 2.14 montre de nombreuses options ici, qu'on peut les utiliser pour créer des e-mails de phishing. En effet, on souhaite créer une page de phishing sur Gmail donc on utilise l'option 3. Par la suite, on remplit les champs souhaités (Target name/victim name ; Target Email ; Day ; Time ...) comme ils sont montrés dans la figure suivante :

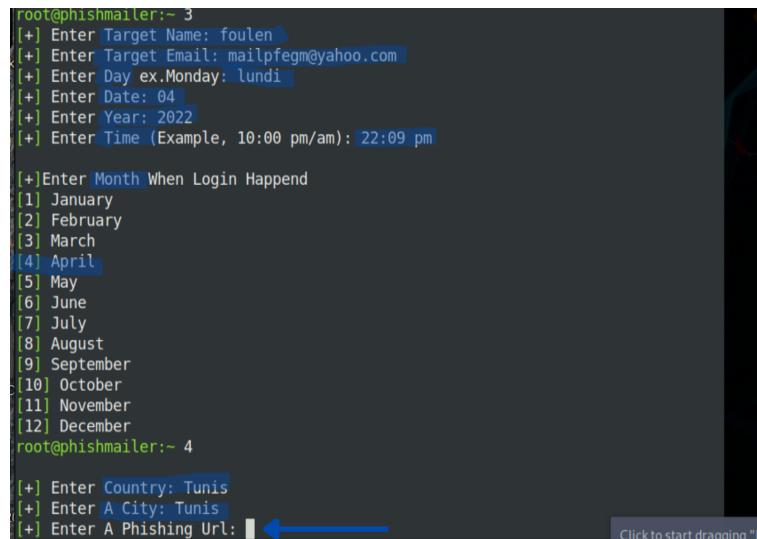


FIGURE 2.16 –

Pour le champs du URL on va utiliser le "Zphisher" pour créer un lien de phishing qui ressemble à un lien d'une page de Gmail. Pour cela, on exécute tout d'abord l'outil pour trouver toutes une liste des options de pages de phishing et puisque notre attaque se base sur le Gmail donc on va choisir l'option numéro 3.

Maintenant on passe pour créer le template d'une page "login" de Gmail tout en choisissant les options suivantes :

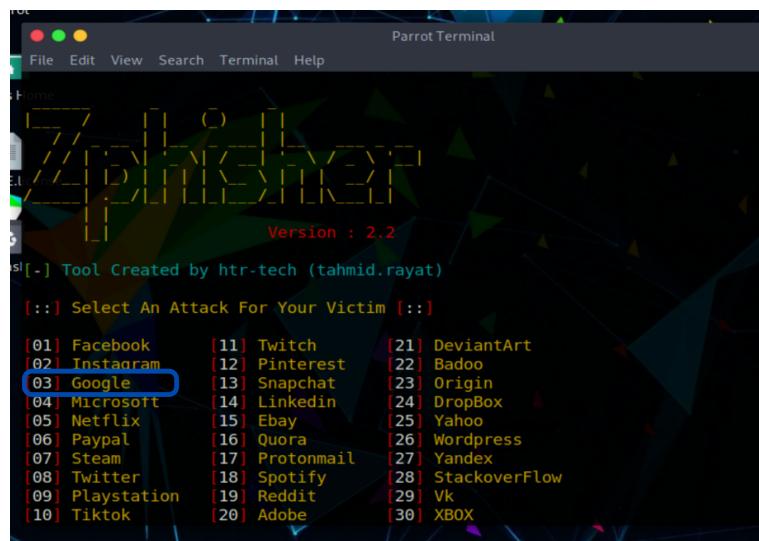


FIGURE 2.17 –

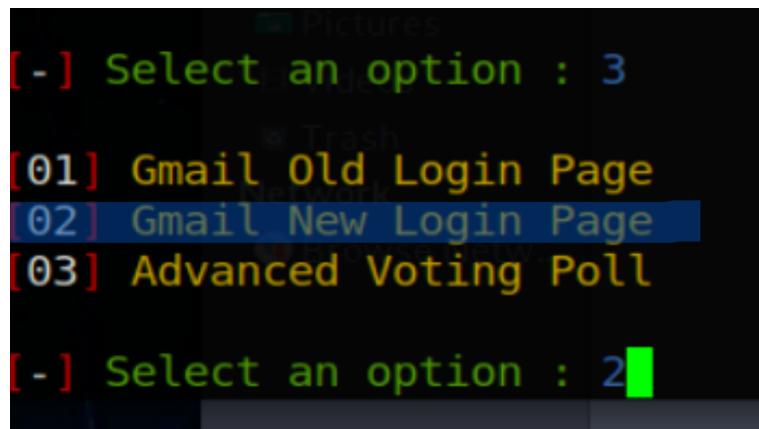


FIGURE 2.18 –

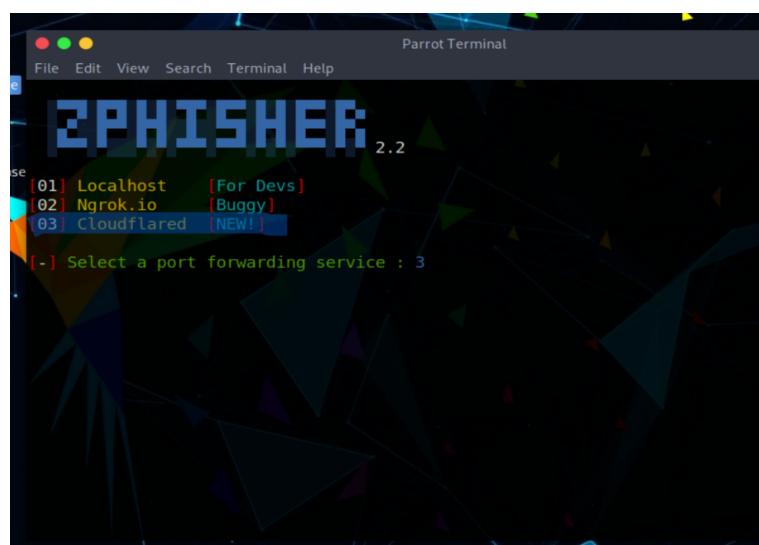
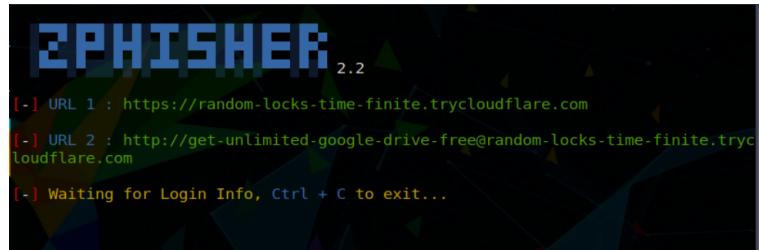


FIGURE 2.19 –

Enfin notre "Zphisher" non seulement va créer une page de "login" de Gmail mais aussi

des différents URL pour l'envoyer au victime. On va choisir le premier lien, mais on voit que le lien semble non-professionnel donc il faut le modifier.



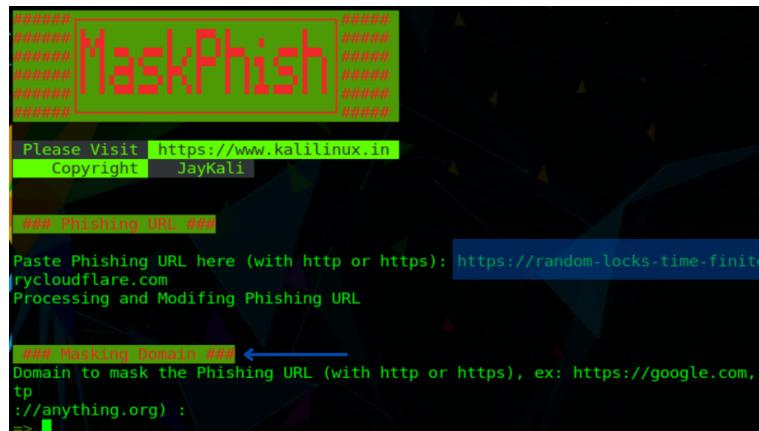
```

[+] URL 1 : https://random-locks-time-finite.cloudflare.com
[+] URL 2 : http://get-unlimited-google-drive-free@random-locks-time-finite.cloudflare.com
[+] Waiting for Login Info, Ctrl + C to exit...

```

FIGURE 2.20 – Liste des URL

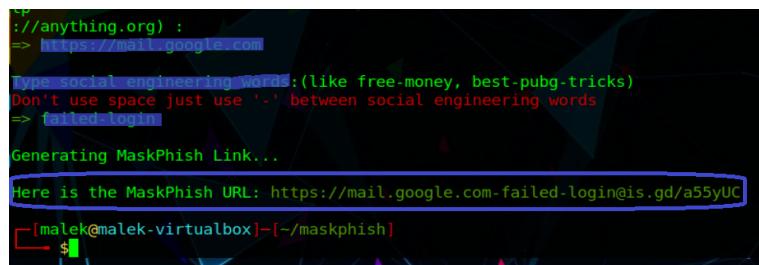
Dans cette étape on va essayer avec l'outil "MaskPhish" de masquer le lien de phishing ou l'URL derrière le lien d'origine. Après avoir lancer l'outil, on copie le lien qui a été généré par "Zphisher".



The screenshot shows the MaskPhish tool's user interface. It has a red title bar with "MaskPhish" in white. Below it, there's a green status bar with "Please Visit https://www.kalilinux.in" and "Copyright JayKali". The main area has a blue background with white text. It says "Paste Phishing URL here (with http or https): https://random-locks-time-finite.cloudflare.com" and "Processing and Modifying Phishing URL". At the bottom, there's a red input field labeled "Masking Domain" with "Domain to mask the Phishing URL (with http or https), ex: https://google.com, tp://anything.org) :" followed by a blue arrow pointing to the input field. A small green arrow points to the "Masking Domain" label.

FIGURE 2.21 –

Maintenant dans le “Masking Domain” on va effectuer quelques modifications pour le lien souhaité afficher à la victime, on suivant les étapes suivantes :



```

:tp://anything.org) :
=> https://mail.google.com
Type social engineering words:(like free-money, best-pubg-tricks)
Don't use space just use '-' between social engineering words
=> failed login
Generating MaskPhish Link...
Here is the MaskPhish URL: https://mail.google.com-failed-login@is.gd/a55yUC
[malek@malek-virtualbox] -[-maskphish]
$ 

```

FIGURE 2.22 –

Finalement on a créé le lien de phishing qui a été en plus masqué il suffit maintenant mettre ce dernier dans le champs ” Phishing URL” de ” PhishMailer” pour qu'il soit intégré dans notre template.

Dans la dernière étape on envoie le mail à notre victime dont on remplit les champs suivantes :

```
[+] Enter Country: Tunis
[+] Enter A City: Tunis
[+] Enter A Phishing Url: https://mail.google.com-failed-login@is.qd/a55yUc
[+] Enter Name On HTML File To Save: gmail
[!] HTML File Created
[malek@malek-virtualbox]-(~/PhishMailer)
```

FIGURE 2.23 –

```
Parrot Terminal
File Edit View Search Terminal Help
[+] Saved Emails
Options:
[1]: mailpfegm@gmail.com

[99] Use Another Email Once
[666] Save Another Email
[+] ----> 1
[+] Set Name You Want The Target To See (ex: Instagram Account Security)Gma
count_Security
[+] Enter Email Address To Send To: mailpfegm@yahoo.com
[+] Enter Subject: Gmail Account Security
[+] Enter Path To Html File: /home/malek/PhishMailer/gmail.html
gmail
[!]Email Sent[!]
```

FIGURE 2.24 –

## 5) Résultats

Après avoir envoyé le mail à notre victime ( machine Windows 10) voici ce qui se passe après l'ouverture de mail.

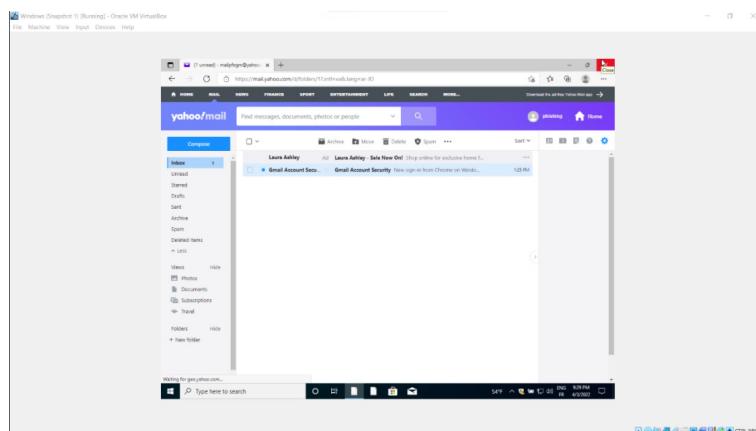


FIGURE 2.25 – Mail envoyé sur la machine de victime

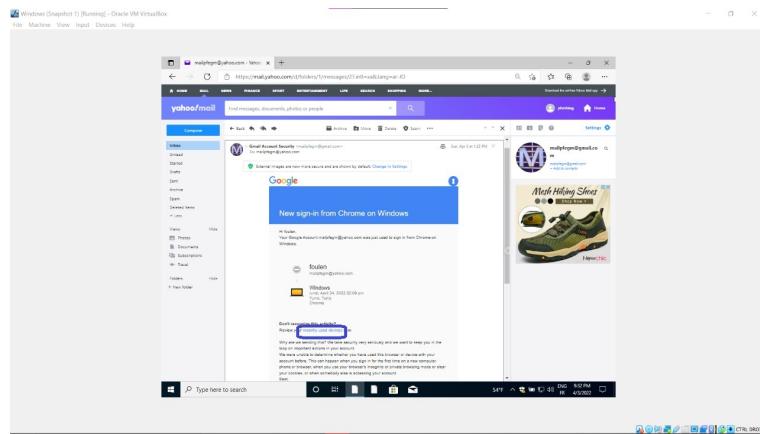


FIGURE 2.26 – Contenu du mail envoyé

Une fois que la victime clique sur ce lien , ce dernier se trouve dans une page qui ressemble bien à une page de login d'un compte Gmail et par manque de confiance il va remplir les champs avec ses données personnelles.

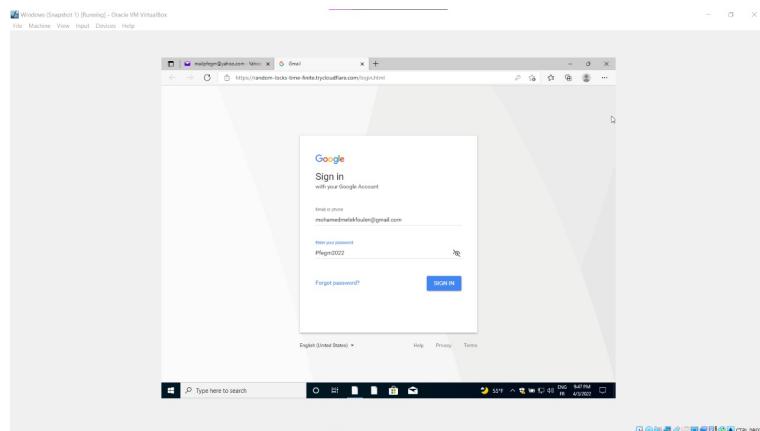


FIGURE 2.27 – Page login d'un compte Gmail

Finalement ces données seront envoyées vers la machine du pirate et seront aussi afficher dans l'outil “Zphisher” comme suit :

```
(-) Login info Found !!
(-) Account : mohamedmelekfoulen@gmail.com
(-) Password : Pfegm2022
(-) Saved in : usernames.dat
(-) Waiting for Next Login Info, Ctrl + C to exit.
```

FIGURE 2.28 – Les informations d'identification du victime

## II.3 Man in the middle

### 1) Généralités

Cette attribution de l'adresse MAC à l'adresse IP locale est stockée sous forme de tableau dans le cache ARP de l'ordinateur demandeur. C'est ici que l'empoisonnement du cache ARP est effectué. Le but de ce modèle d'attaque est de pouvoir manipuler les tableaux ARP de différents ordinateurs du réseau par le biais de fausses réponses ARP. En effet, cette attaque peut espionner les messages et également les modifier. L'attaque de MITM est basée donc sur l'empoisonnement du cache ARP.

### 2) Scénario

Sur le même réseau, le pirate essaie tout d'abord d'usurper l'adresse MAC du serveur auprès d'utilisateur pour que les paquets envoyés soient dans un premier temps envoyés vers le pirate. Ensuite, ce dernier va intercepter les paquets envoyés par l'utilisateur au serveur.

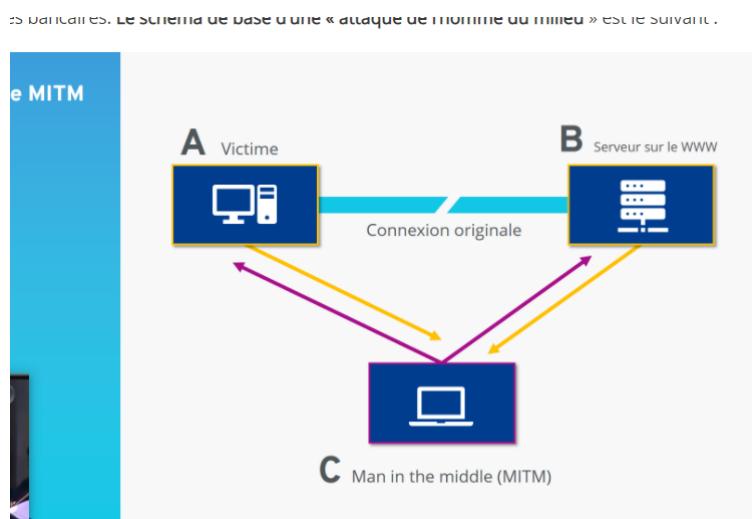


FIGURE 2.29 – Scénario de Man in the middle

### 3) Outils

Les outils utilisés lors de cette attaque :

- **Pc exécutant le système d'exploitation « Parrot Os »**

- **Le framework «Ettercap»**

Ettercap est un logiciel gratuit et open source, d'analyse du réseau informatique pour les attaques de sniffing sur le réseau local. Il est capable d'intercepter le trafic sur un segment réseau, de capturer les mots de passe, et de réaliser des attaques de Man In The Middle contre un certain nombre de protocoles de communication usuels tels que HTTP, FTP et certains protocoles chiffrés.

- **Le framework «WireShark»**

Wireshark est un logiciel d'analyse réseau (sniffer) qui permettant de visualiser l'ensemble des données transitant sur la machine qui l'exécute, et d'obtenir des

informations sur les protocoles applicatifs utilisés. Les octets sont capturés en utilisant la librairie réseau PCAP, puis regroupés en blocs d'informations et analysés par le logiciel. (<http://www.machaon.fr/isn/reseaux/Fiche-Wireshark.pdf>)

#### 4) Réalisation

Tout d'abord on ouvre notre interface graphique "Ettercap" qui est déjà installée par défaut sur la machine Parrot Os. Par la suite on choisit l'option "Sniffing at startup" on spécifiant l'interface sur laquelle on va écouter le trafic.

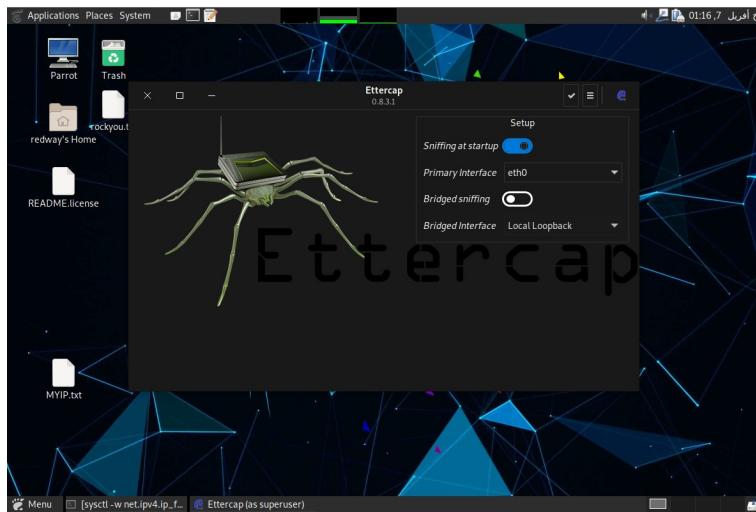


FIGURE 2.30 – Lancement de Ettercap

Maintenant on lance un scan pour rechercher les machines connectées sur le même réseau, donc il suffit d'aller dans le **menu hosts -> scan for hosts**, puis **hosts list** pour retrouver les résultats de notre scan.

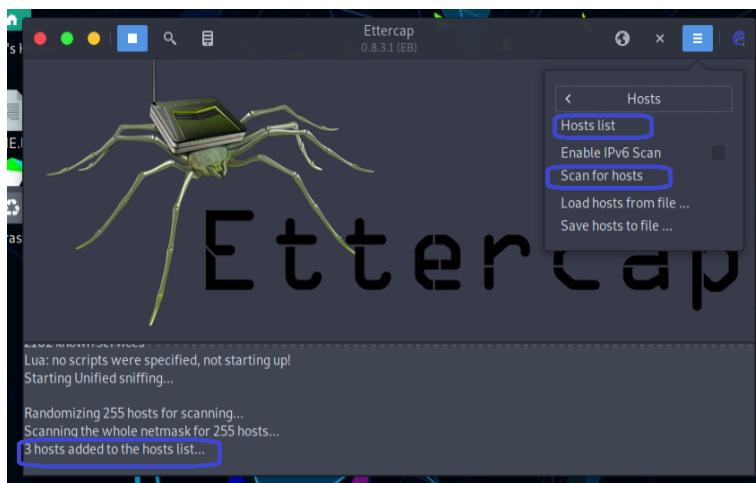


FIGURE 2.31 – Lancement de Ettercap

Dans cette étape le pirate va spécifier les cibles qu'il veut attaquer, donc il suffit de choisir pour chaque target les @ IP respectivement "Add To Target 1" pour la machine cible et "Add To Target 2" pour le serveur web. Après il lance lancer l'attaque via le menu **MITM -> ARP Poisoning**.

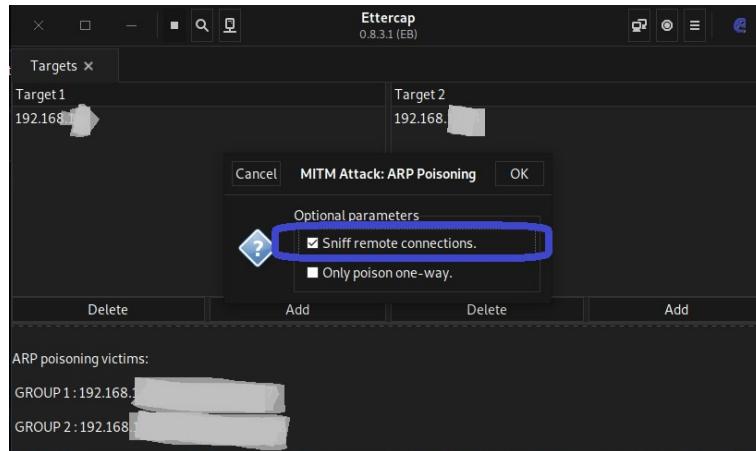


FIGURE 2.32 – Résultats du scan

Allons maintenant sur Wireshark pour visualiser le déroulement de cette attaque et son efficacité. Le pirate choisit son interface réseau, mais avant cela il faut activer le routage des paquets. De plus, il effectue un filtrage paquet par @ IP de serveur.

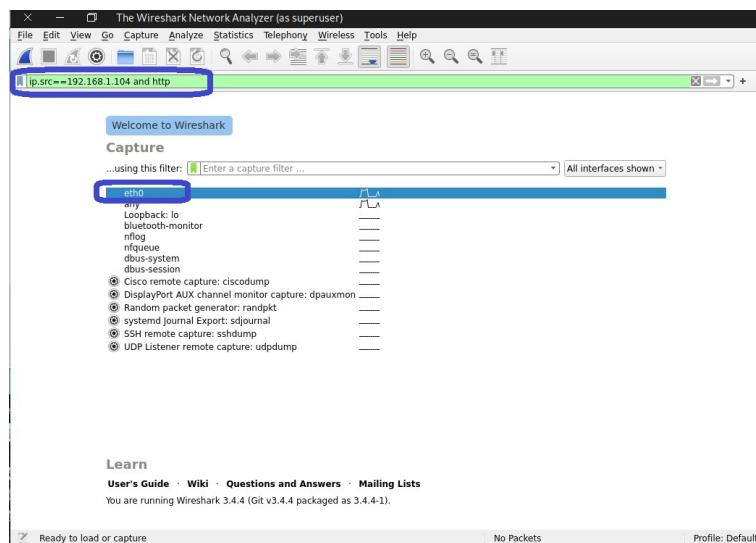


FIGURE 2.33 – Chargement de wireshark

Après avoir lancé l'attaque, dans ce qui suit une capture sur wireshark pendant l'attaque après que la victime se connecte sur le serveur :

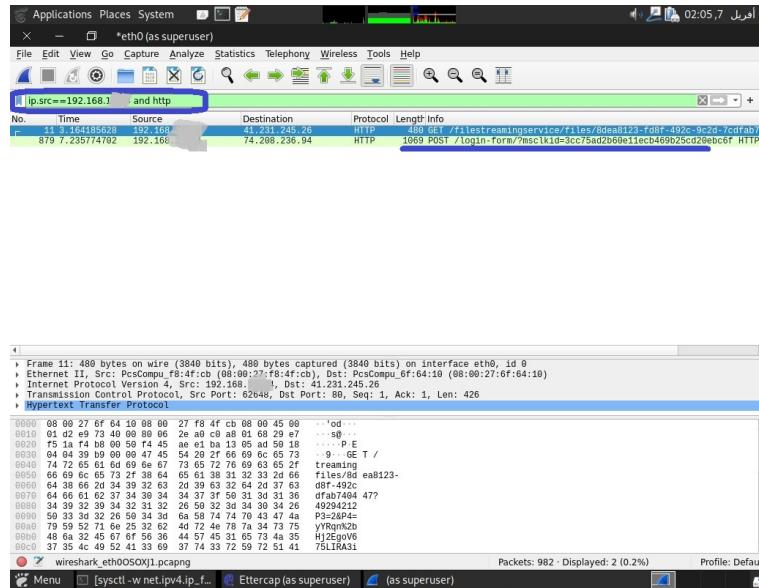


FIGURE 2.34 – Capture de wireshark

Une fois la victime authentifiée sur le serveur web, nous recevons le login et le mot de passe en clair comme le montre la figure suivante :

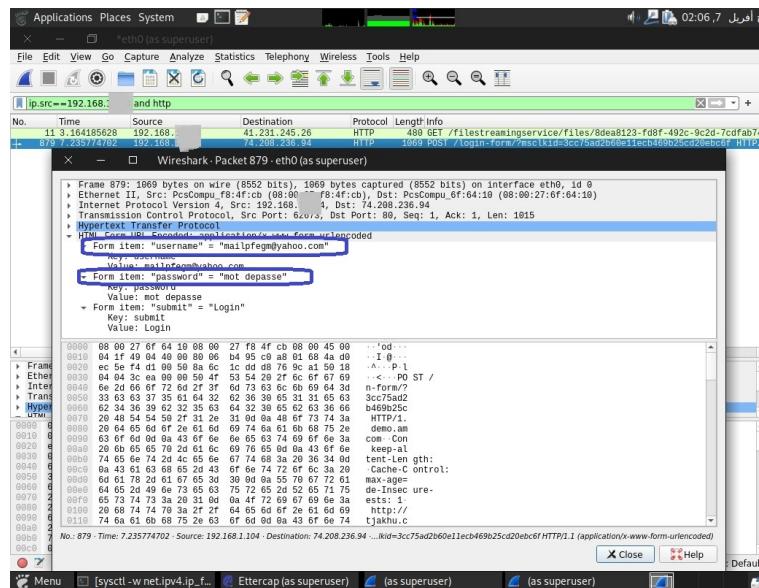


FIGURE 2.35 – Résultat

## II.4 SSH brute force

### 1) Généralités

L’attaque brute force SSH est une attaque très répandue. Il s’agit d’une tentative de connexions SSH effectuant une succession d’essais pour découvrir un couple utilisateur/mot de passe valide afin de prendre le contrôle de la machine.

## 2) Scénario

Un pirate talentueux essaye de trouver un port SSH ouvert et essaie de faire une combinaison d'informations d'identification valides pour effectuer des actions de vol à distance. Pour ce faire, il utilise deux listes contenant l'une des noms d'utilisateur et l'autre une liste de mots de passe probables.

## 3) Outils

Les outils utilisés lors de cette attaque :

- **Pc exécutant le système d'exploitation « Parrot Os »**

- **L'outil de scan «Nmap»**

Nmap ("Network Mapper") est un outil open source d'exploration réseau et d'audit de sécurité. Il est conçu pour détecter les ports ouverts, les services hébergés et les informations sur le système d'exploitation d'un ordinateur distant. Ce logiciel est devenu une référence puisqu'il utilise des paquets IP bruts pour déterminer quels sont les hôtes actifs sur le réseau, quels services ces hôtes offrent, quels systèmes d'exploitation ils utilisent, quels types de dispositifs de filtrage/pare-feux sont utilisés, ainsi que des douzaines d'autres caractéristiques.

- **Le framework «Hydra»**

Hydra est un outil open source et cracker de connexion parallélisé qui prend en charge de nombreux protocoles d'attaque. Il est très rapide et flexible qui permet de réaliser des brutes force en ligne c'est-à-dire d'essayer toutes les combinaisons possibles de login et de mot de passe. Il supporte plusieurs protocoles d'authentification tels que ssh2, imap, ftp, etc.. Cet outil permet aux chercheurs et consultants en sécurité de montrer à quel point il serait facile d'obtenir un accès non autorisé à un système à distance.

## 4) Réalisation

Pour commencer notre attaque, il faut d'abord scanner le réseau et trouver les ports ouverts de la machine linux. Pour ce faire, on utilise l'outil nmap comme suite :

**-p** : Spécifier un port pour scanner.

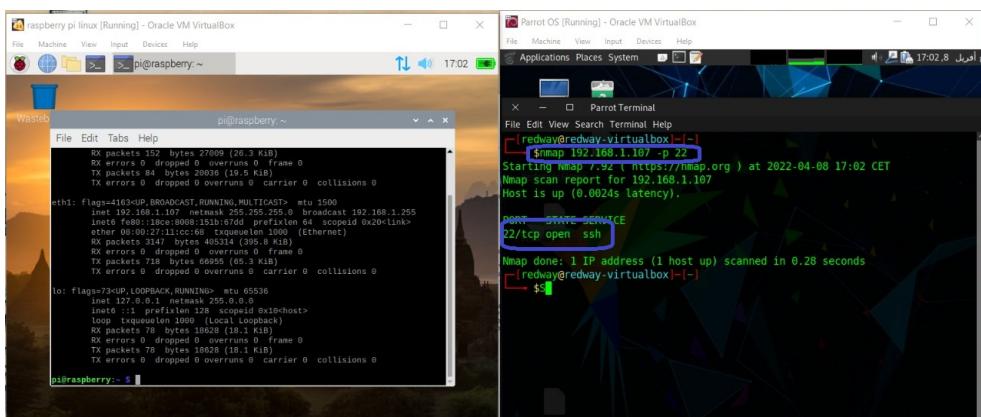


FIGURE 2.36 – Résultat du scan

Par la suite on crée deux dictionnaires, un avec une liste de noms d'utilisateurs probables et un autre avec une liste de mots de passe probables. Les dictionnaires sont nommés users.txt et passwords.txt.

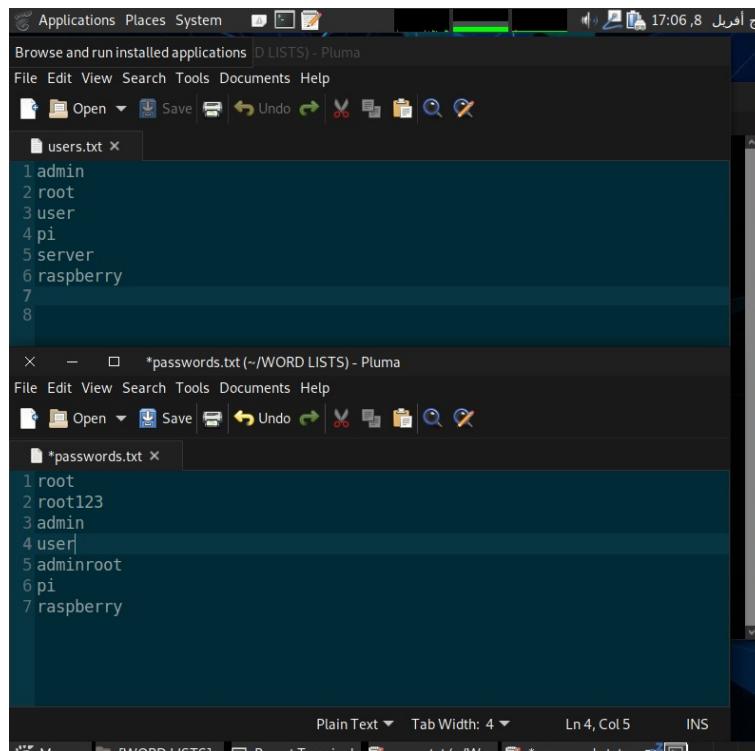


FIGURE 2.37 – Creation des dictionnaires

Maintenant on lance l'outil "hydra" qui est installé par défaut sur parrot os et on effectue l'attaque avec cette commande : **hydra -L users.txt -P passwords.txt ssh :// @ serveur victime -t 4** .

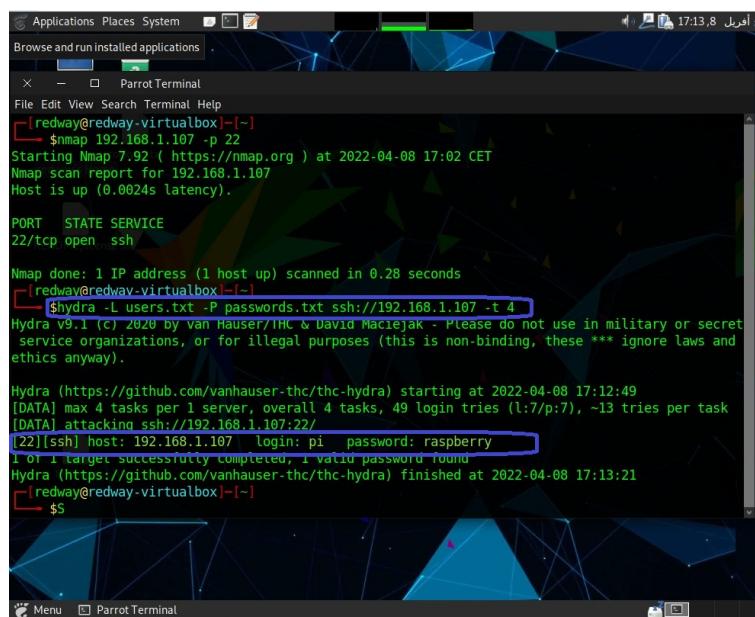


FIGURE 2.38 – Attaque et résultat

Nous voyons que l'outil a récupéré la paire d'informations d'identification du victime. Ensuite on teste les ces informations pour accéder au serveur avec l'utilisation de cette commande :

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-04-08 17:12:49
[DATA] max 4 tasks per 1 server, overall 4 tasks, 49 login tries (l:7/p:7), ~13 tries per task
[DATA] attacking ssh://192.168.1.107:22/
[22][ssh] host: 192.168.1.107 login: pi password: raspberry
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-04-08 17:13:21
pi@192.168.1.107:~$ ssh pi@192.168.1.107
pi@192.168.1.107's password:
Linux raspberry 4.19.0-13-amd64 #1 SMP Debian 4.19.160-2 (2020-11-28) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Apr  8 16:30:21 2022 from 192.168.1.106

SSH is enabled and the default password for the 'pi' user has not been changed.
This is a security risk - please login as the 'pi' user and type 'passwd' to set a new password.

pi@raspberry:~ $
```

FIGURE 2.39 – Accéder au serveur

## II.5 Injection SQL

- 1) Généralités
- 2) Scénario
- 3) Outils
- 4) Réalisation

## Conclusion

# **chapitre 3**

## **Modélisation**

### **I Introduction**

Après avoir présenté le cadre du projet dans le chapitre précédent, nous examinerons dans ce chapitre certains concepts de base nécessaires et liés à la sécurité informatique, les principales menaces et cyberattaques, les études comparatives des solutions disponibles et nous présentons les technologies et les solutions adoptées dans notre projet.

## II Exemples des systèmes de sécurité informatique

### II.1 Firewall

#### 1) Présentation de firewall et son rôle dans la sécurité informatique

Un firewall est un équipement de sécurité qui surveille le trafic réseau entrant et sortant et autorise/bloque les paquets de données en se basant sur un ensemble des règles . Il est chargé de dresser une barrière entre le réseau interne et le trafic entrant provenant de sources externes afin de bloquer le trafic malveillant des virus et des pirates.

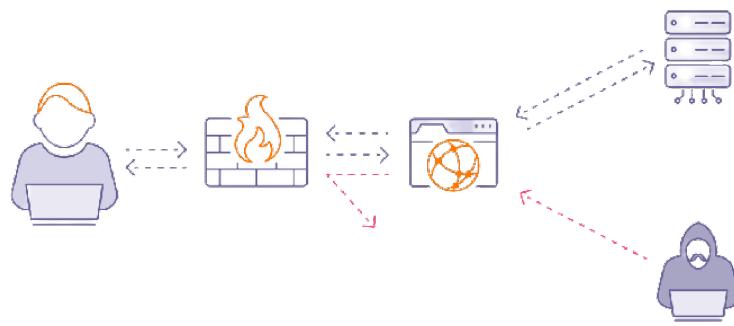


FIGURE 3.40 – Firewall

#### 2) Principe de fonctionnement d'un pare-feu

Un système pare-feu est basé sur 3 règles prédéfinies qui permet de mettre en œuvre une méthode de filtrage permettant :

- Autoriser (allow) : Cette règle est dédiée pour autoriser les connexions.
- Bloquer (deny) : Cette règle nous aide à bloquer les connexions.
- Rejeter (drop) : Cette règle nous offre l'opportunité de rejeter la demande de connexion sans avertir l'expéditeur.

### II.2 Antivirus

Les antivirus sont des logiciels conçus pour identifier, neutraliser et éliminer des logiciels malveillants.

## III Les cyberattaques

Une cyberattaque est tout type d'action offensive qui vise des systèmes, des infrastructures ou des réseaux informatiques. Les cyberattaques utilisent des codes malveillants pour voler, détruire ou modifier le code informatique, les données ou des systèmes informatiques ce qui entraîne des conséquences perturbatrices qui peuvent compromettre les données et mener à des cybercrimes, comme le vol d'informations et d'identité.



FIGURE 3.41 – Antivirus

### III.1 Anatomie d'une cyberattaque

L'anatomie d'une cyber attaque passe par quelques étapes :

Le hacker commence par "cyber scanner" ou il fait la reconnaissance du réseau et récolte des renseignements sur la cible puis Il teste toutes les vulnérabilités découvertes pour trouver les points faibles d'intrusion. Après avoir trouvé le point d'intrusion le hacker essaie de pénétrer le système ou dans quelque cas comme le dos il le rend inutilisable. Une fois dans le système, le hacker obtient un niveau d'autorisation élevé "administrateur" pour pouvoir effectuer des tâches malveillantes- sans l'intervention des antivirus - pour déployer des logiciels malveillants ou planter des portes dérobées pour l'accès ultérieur. Une fois son travail est fini il efface tous ses traces en détruisant toutes preuves potentiellement incriminantes.

### III.2 Impacts des cyberattaques

Les cyberattaques déclenchent toujours des crises majeures dans plusieurs domaines qui peuvent remettre en cause la pérennité même de l'entreprise . En effet, les conséquences sont toujours néfastes, et peuvent causer :

- Perte financière (frais de réparation et de protection).
- Arrêt de l'activité de la production.
- Perte de confiance.
- Vol ou extorsion de données.
- Usurpation d'identité.

### III.3 Les types de cyberattaques

**Selon notre cible**

## IV Security operation center (SOC)

Le SOC est une plateforme permettant la supervision et l'administration de la sécurité du système d'information au travers d'outils de collecte, de corrélation d'événements et d'intervention à distance. L'objectif d'un SOC est de détecter, analyser et remédier aux

incidents de cybersécurité. Pour cela, il utilise une combinaison de dispositifs technologiques ainsi qu'un ensemble de processus pour détecter et remonter le moindre incident afin que les équipes puissent réagir rapidement.

## IV.1 Composition du SOC [3]

Le SOC peut être représenté par les trois composants suivants :

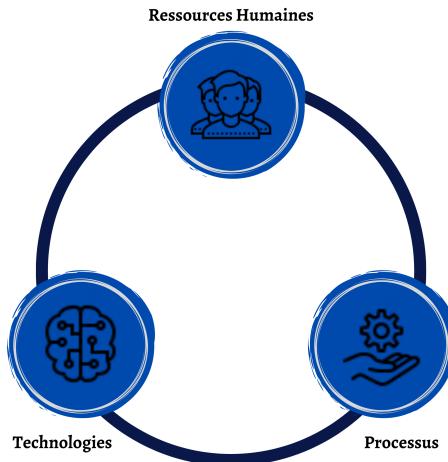


FIGURE 3.42 – Composition du SOC

## IV.2 Ressources Humaines

Les Ressources Humaines représentent les différents acteurs nécessaires au bon fonctionnement du SOC. Ils sont découpés en trois tiers, chaque tiers ayant un rôle spécifique :

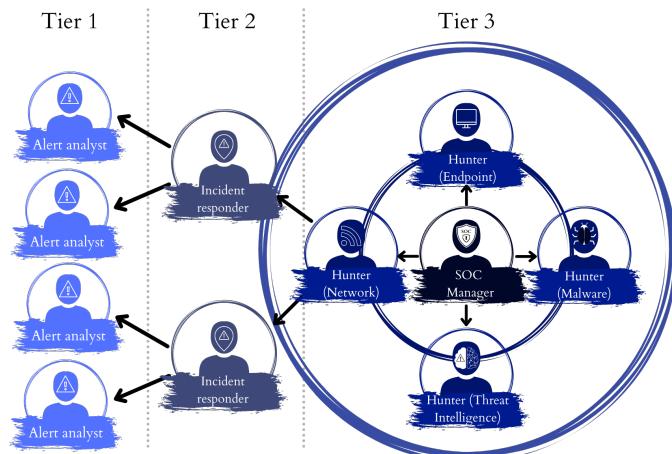


FIGURE 3.43 – Ressources Humaines

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 qualifier les événements avant de faire remonter au Tiers 2 ceux nécessitant une plus grande attention. En effet, le Tiers 1 effectue une analyse des événements en temps réel, celle-ci doit être brève et basée sur des scénarios prédéfinis afin de faire une première évaluation. La politique de sécurité mise en place dicte la durée maximum de l'analyse (moins d'un quart d'heure généralement). Tout événement dont l'étude n'est pas finie à ce moment-là est remonté vers le Tiers 2.

**- Le Tiers 2 (ou niveau 2) :** Cette équipe reçoit les alertes du niveau 1 et lance une analyse plus approfondie afin de déterminer avec plus de précision l'origine et les conséquences liées à l'évènement en cours. Contrairement au Tiers 1, ces équipes ne sont pas tenues de travailler en temps réel : elles peuvent ainsi allouer plus de temps pour étudier les alertes et déterminer si un incident a eu lieu. Elles rédigent aussi les procédures de traitement des événements pour le niveau 1 et participent à l'amélioration des règles de corrélation permettant au Tiers 1 de lever des alertes pertinentes.

**- Le Tiers 3 (ou niveau 3) :** Ce Tiers est légèrement différent des autres : premièrement il n'est pas présent dans tous les SOC. Son objectif étant plutôt d'éviter les incidents avant qu'ils ne se produisent, son rôle se rapproche du CSIRT. D'ailleurs dans certaines entreprises, c'est le CSIRT qui s'occupe de cette partie. Il s'agit donc ici d'une expertise plus poussée que pour les niveaux 1 et 2. Au sein du Tiers 3 peuvent être réalisés des activités de forensic ou de reverse-engineering afin d'analyser au maximum un incident et d'anticiper de futurs événements. En cas d'attaque non connue, les niveaux 1 et 2 ne sont pas alertés, c'est au niveau trois de faire une veille sur les menaces.

**- 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).

Afin d'avoir un meilleur taux de détection d'incidents, le soutien des utilisateurs des systèmes d'informations au sein de l'entreprise est par ailleurs nécessaire. En effet, ceux-ci sont invités à remonter toute irrégularité dans l'utilisation de leur système. C'est grâce à ces informations que les équipes du SOC ont la possibilité d'améliorer la protection des terminaux.

### IV.3 Les Processus

Les processus représentent les différentes actions courantes du SOC. Ils respectent souvent deux méthodes afin d'évoluer sur deux échelles de temps :

- Une échelle de temps à vision systémique : la méthode qui nous intéresse alors est une adaptation du PDCA (Plan Do Check Act) pour la cyber sécurité.

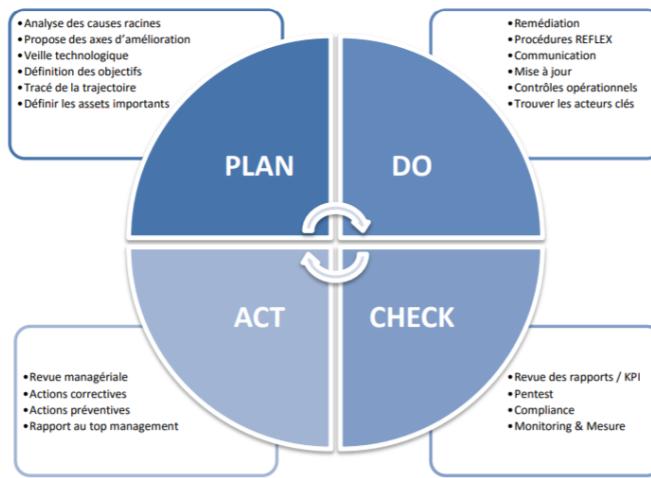
- Une échelle de temps de mouvement rapide : on adapte alors la méthode OODA (Observe Orient Decide Act).

Si l'on « traduit » la méthodologie par les actions classiques d'un SOC, on obtient :

On voit donc que cela correspond bien aux différentes étapes et actions réalisées par les membres des équipes du SOC

#### 1) Les Technologies du SOC

Le SOC implique une combinaison d'outils technologiques afin de se protéger des cybers attaques et d'assurer une sécurité informatique maximale. Parmi les principaux



outils constituant le SOC nous présentons le système de gestion des informations et des événements de sécurité (SIEM), une plate-forme de renseignement sur les menaces Cti (Cyber Threat Intelligence) et une plate-forme de réponse aux incidents de sécurité.

#### IV.4 Avantages du SOC

- La surveillance et l'analyse ininterrompues des activités suspectes.
- L'amélioration des temps de réponse aux incidents et des pratiques de gestion des incidents.
- La diminution de l'écart entre le moment de la compromission et celui de la détection.
- Des actifs logiciels et matériels centralisés pour permettre la mise en œuvre d'une approche plus holistique de la sécurité.
- Une communication et une collaboration efficaces pour détecter et classer les tactiques et techniques adverses.
- La réduction des coûts associés aux incidents de sécurité.
- Plus de transparence et de contrôle sur les opérations de sécurité.
- Une traçabilité fiable concernant les données utilisées dans les activités de cybersécurité post-mortem.

## V Security Event Information Management (SIEM)

SIEM est l'acronyme de “Security Incident and Event Management”. Il s'agit d'un système de sécurité qui combine les fonctions SIM (Security information management) et SEM (Security évent management) dans un seul système de gestion de sécurité.

- **SIM (Security Information Management) :** c'est la première génération, construite sur les systèmes traditionnels de collecte et de gestion des journaux. Il a introduit le stockage à long terme, l'analyse et la création des rapports sur les données des journaux, et a combiné les journaux avec les renseignements sur les menaces.

- **SEM (Security Event Management)** : c'est la deuxième génération, adressant les événements de sécurité - agrégation, corrélation et notification des événements des systèmes de sécurité tels que les antivirus, les pare-feux et les systèmes de détection d'intrusion (IDS), ainsi que les événements signalés directement par l'authentification, les traps SNMP, serveurs, bases de données, ... etc.

L'outil SIEM analyse en temps réel les alertes de sécurité créées par l'application et le réseau. Donc il peut-être défini comme un outil qui assure la collecte d'événements en temps réel, la surveillance, la corrélation et l'analyse des événements à travers des sources disparates [5]



FIGURE 3.44 – Security Event Information Management

## V.1 Fonctionnement de SIEM

La solution S.I.E.M. permet de surveiller des applications, des comportements utilisateurs et des accès aux données. A travers les fonctionnalités fournies par cette solution, il est donc possible de collecter les logs et données générés par les applications, les équipements de sécurité et les systèmes hôtes des entreprises pour les consolider au sein d'une plateforme centralisée. Il rassemble les données des antivirus, des logs des pare-feu, ... pour les classer en différentes catégories . Lorsque les outils SIEM identifient une menace sur le réseau, ils génèrent une alerte et lui attribuent un niveau de gravité en fonction de règles prédéfinies.

le SIEM peut fournir de nombreuses fonctionnalités, comme le montre la figure ci-dessous :

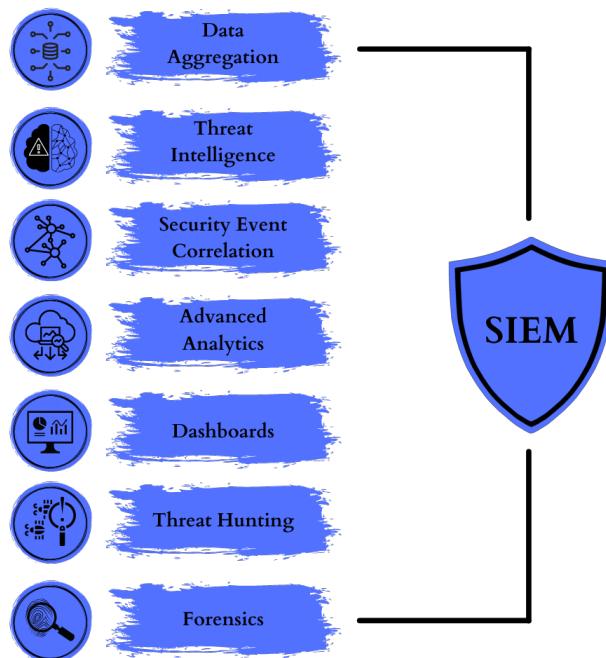


FIGURE 3.45 – Fonctionnalités du SIEM

- **Data Aggregation** : Le SIEM récupère des données telles que les journaux du système à partir de différentes sources en utilisant les éléments suivants :
  - Data Collectors (Collecteurs de données).
  - Data Forwarders (Transporteurs de données).
- **Threat Intelligence** : Dans le domaine de la cybersécurité, le renseignement sur les menaces consiste à recueillir des informations sur les cybermenaces passées, actuelles et potentielles, puis les analyser pour voir si elles sont pertinentes et comment elles pourraient avoir un impact sur l'organisation. Le SIEM utilise le renseignement sur les menaces pour vérifier que les données qu'il recueille ne contiennent pas de menaces.
- **Security Event Correlation** : Cette fonction comprend des algorithmes, une corrélation statistique ou basée sur des règles et d'autres méthodes, telles que la

corrélation de différents événements entre eux ou la corrélation d'événements avec des données contextuelles. La corrélation peut se produire en temps réel, mais tous les outils ne prennent pas en charge cette fonctionnalité. En effet, certains outils se concentrent sur l'association de données historiques dans leurs bases de données. De plus, d'autres méthodes d'analyse de log sont parfois incluses dans cette catégorie.

- **Advanced Analytics** : Cette opération permet de rechercher tous types de changements de comportements, même les comportements typiques qui pourraient indiquer des compromis.
- **Dashboards** : Cette fonction comprend des tableaux de bord de monitoring de la sécurité et affiche des opérations à l'usage du personnel. Ainsi, les analystes peuvent voir les informations collectées mais aussi les résultats des corrélations pratiquement en temps réel. Les données historiques et archivées peuvent également être présentées de cette manière.
- **Threat Hunting** : Cette fonction permet d'utiliser les nouvelles données sur les menaces pour examiner les données SIEM existantes à la recherche d'anomalies potentielles que les anciennes données sur les menaces n'ont pas détectées.
- **Forensics** : C'est une analyse des données SIEM existantes pour obtenir des indices en vue d'une enquête médico-légale. En effet les données sont conservées pendant une période minimale, par exemple un an.

## V.2 Rôles du SIEM dans un SOC

Le rôle du SIEM est de fournir aux analystes du Security Operations Center une intelligence complète issue de l'analyse de données événementielles trop diverses et volumineuses pour être étudiées manuellement. L'analyse SIEM des données machine et des fichiers journaux peut détecter les activités malveillantes et déclencher des réponses automatisées, réduisant considérablement le temps de réponse aux attaques.

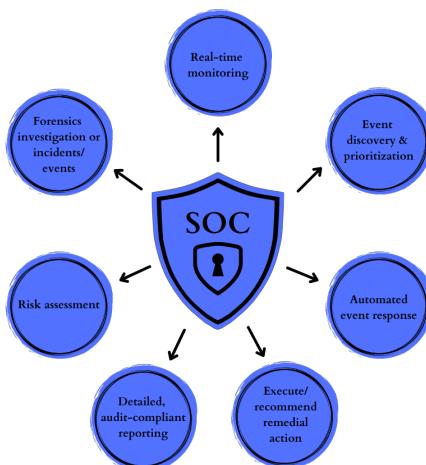


FIGURE 3.46 – Schéma explicatif de SIEM

### V.3 Les SIEMs open source les plus connues

SIEM est en fait le logiciel le plus important dans notre projet. Nous devons d'abord mener une étude comparative pour choisir un bon logiciel, puis l'implémenter dans notre architecture. Après une recherche ciblée, nous avons trouvé plusieurs logiciels open sources concurrents :

## VI Security Onion Solutions (SOS)

Les chances d'une cyberattaque augmentent de façon exponentielle, et non seulement les grandes organisations sont ciblées par les cybercriminels, mais aussi les petites et moyennes entreprises. Par conséquent, nous devons disposer des outils nécessaires pour assurer la sécurité de notre infrastructure. La security onion est un système de sécurité, elle s'agit d'une distribution linux orientée vers la détection d'intrusions, la supervision de la sécurité et la gestion des logs. cette distribution intègre des outils inclus par défaut pour les Alerts, Hunt, PCAP, et des outils de sécurité issus de communautés open source par exemple : Playbook, FleetDM, osquery, CyberChef, Elasticsearch, Logstash, Kibana, Suricata, Zeek, and Wazuh.



FIGURE 3.47 – Security Onion

La raison pour laquelle ce système de sécurité est appelé security onion est la gestion de sécurité par couche. La figure suivante montre les différentes couches sécurisées.

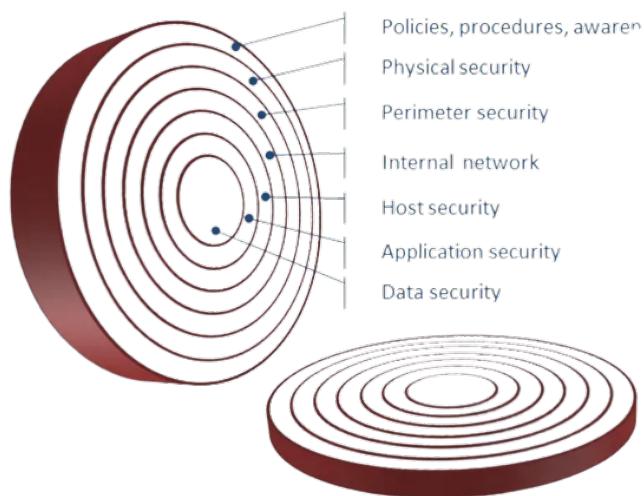


FIGURE 3.48 – Security Onion

## VI.1 Fonctionnement de SOS

La security onion peut fournir de nombreuses fonctionnalités comme :

- Capture et sauvegarde de trafic.
- Journalisation d'événements.
- Architecture distribuée (client/serveur).
- Outils d'analyse et rapports.
- NIDS (signature et comportemental).
- HIDS.

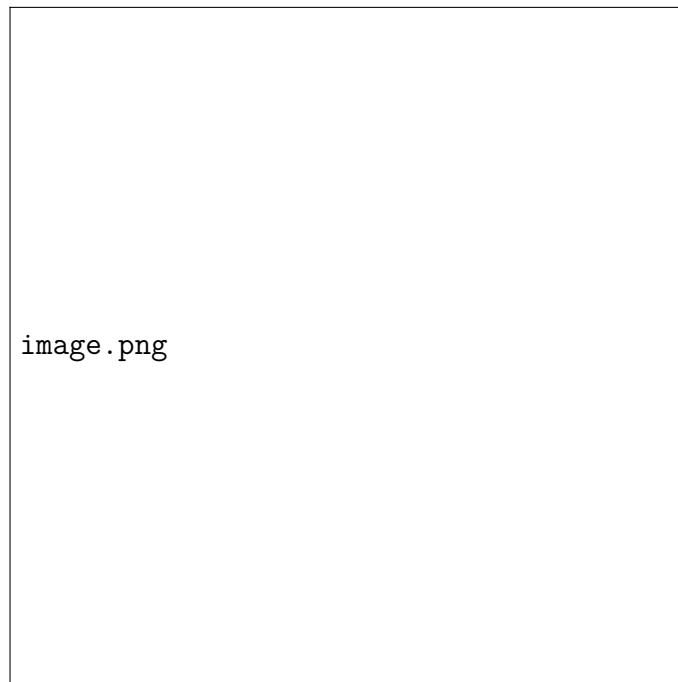


FIGURE 3.49 – Security Onion

En revanche, S.O est une grande distribution qui facilite la mise en relation et l'intégration de plusieurs éléments.

## VI.2 Etude comparative des solutions étudiées

## VII Conclusion

Dans ce chapitre, nous avons présenté les concepts de base de la cybersécurité, les composants principaux de notre centre d'opération de sécurité SOC ainsi que la solution adoptée. Le prochain chapitre sera réservé à l'analyse des besoins, et la conception de notre solution.

## VIII Introduction

### IX Diagramme de classes



FIGURE 3.50 – Diagramme de classe général

## X Diagramme de séquences du système

### X.1 Diagramme de séquence du client :

### X.2 Diagramme de séquence de l'admin :



FIGURE 3.51 – Diagramme de séquence du client

## XI Conclusion

conclusion



FIGURE 3.52 – Diagramme de séquence de l'admin

# **chapitre 4**

## **Réalisation**

### **I Introduction**

intro

### **II Environnement de travail**

#### **II.1 Environnement matériel**

...

#### **II.2 Environnement logiciel**

Dans notre projet, nous avons utilisé les logiciels suivants :

- 1) Visual Studio Code :**
- 2) Github :**
- 3) Creately :**

Creately est un outil de collaboration visuelle qui permet la création de diagrammes et de conception.

L'application est principalement connue pour créer des chartes, des graphes, des diagrammes UML,...etc.

### **III Technologies utilisées :**

#### **III.1 HTML5 :**

..

#### **III.2 CSS3 :**

..

### III.3 ReactJS :

ReactJS [2] est une bibliothèque JavaScript déclarative, efficace et flexible pour la création d'interfaces utilisateur (UI).

Cette framework nous permet de composer des interfaces utilisateur complexes à partir de petits morceaux de code isolés appelés «composants».

#### Pourquoi ReactJS

...

## IV Tâches Réalisées

tahki aali 5demthom w t7ot des captures d'écran

## V Conclusion

# **Conclusion Générale**

# Bibliographie

[2] <https://reactjs.org>. ReactJS.