

Attaque Man In The Middle (MITM) – ARP Poisoning



IRATNI Hocine

Nom de l'enseignant :

Bernard FERNANDEZ

Date de soumission : 25 mai 2025



I. Table des matières

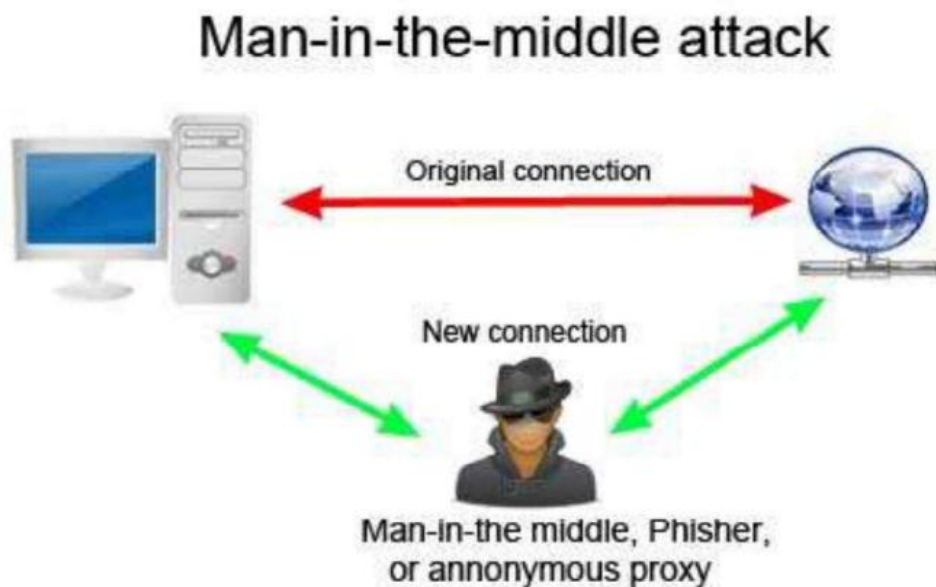
Table des matières

I.	Table des matières	2
II.	Introduction.....	3
III.	Prérequis et environnement.....	4
IV.	Méthodologie	5
V.	Conclusion.....	8

II. Introduction

Dans le monde moderne de l'informatique et des réseaux, la **sécurité des données** est devenue un enjeu majeur. Les attaques visant à intercepter, manipuler ou détourner les données transmises au sein des réseaux sont de plus en plus fréquentes. L'une des attaques les plus courantes est l'**attaque Man-in-the-Middle (MITM)**. Cette attaque consiste à intercepter les communications entre deux parties sans que celles-ci en aient conscience, permettant ainsi à l'attaquant de lire, modifier, ou injecter des informations.

L'objectif de ce travail pratique est d'illustrer comment une **attaque MITM** peut être réalisée à l'aide de la technique **ARP Spoofing**. L'ARP Spoofing consiste à envoyer de fausses informations ARP (Address Resolution Protocol) dans un réseau local afin de rediriger le trafic entre une victime et un routeur vers l'attaquant



Dans ce TP, nous allons utiliser **Kali Linux** comme environnement de test et plusieurs outils comme **Ettercap** pour réaliser l'attaque ARP Spoofing et **Wireshark** pour capturer et analyser le trafic HTTP en clair. L'attaque sera suivie d'une analyse détaillée des paquets HTTP, dans le but d'illustrer l'exposition potentielle des données sensibles, telles que les informations de connexion (nom d'utilisateur et mot de passe), transmises sans chiffrement.

Ce TP nous permettra de démontrer la vulnérabilité des connexions non sécurisées et de souligner l'importance des bonnes pratiques en matière de sécurité réseau, telles que l'utilisation de **HTTPS** et l'activation de **HSTS (HTTP Strict Transport Security)**.

III. Prérequis et environnement

3.1. Environnement de test

Pour ce TP, nous avons utilisé une machine virtuelle Kali Linux exécutée sur **Hyper-V**. Cette machine virtuelle est connectée à un **commutateur virtuel** qui, à son tour, est relié à la carte **Ethernet** de mon **laptop**. Ce réseau local permet d'étudier les attaques MITM et l'analyse du trafic dans un environnement contrôlé.

3.2. Configuration du réseau local

Le réseau local est composé des éléments suivants :

- **Routeur** : **Sagemcom F@st5688**, avec l'adresse IP **192.168.1.254**. Ce routeur sert de passerelle entre la victime et le reste du réseau.
- **Victime** : La machine cible à l'adresse IP **192.168.1.25**. Elle sera utilisée pour générer du trafic HTTP, qui sera ensuite intercepté.

3.3. Vérification de la connectivité

Avant de lancer l'attaque, il est essentiel de s'assurer que toutes les machines du réseau peuvent se communiquer. Nous avons utilisé la commande **ping** pour tester la connectivité entre la machine Kali Linux (l'attaquant), la victime et le routeur.

```
C:\Users\hocin>ping 192.168.1.25

Envoi d'une requête 'Ping' 192.168.1.25 avec 32 octets de données :
Réponse de 192.168.1.25 : octets=32 temps=20 ms TTL=64
Réponse de 192.168.1.25 : octets=32 temps=6 ms TTL=64
Réponse de 192.168.1.25 : octets=32 temps=58 ms TTL=64
Réponse de 192.168.1.25 : octets=32 temps=76 ms TTL=64

Statistiques Ping pour 192.168.1.25:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 6ms, Maximum = 76ms, Moyenne = 40ms
```

IV. Méthodologie

L'attaque ARP Spoofing avec Ettercap

1. Lancement d'Ettercap :

La première étape a consisté à lancer **Ettercap** en mode graphique à l'aide de la commande suivante :

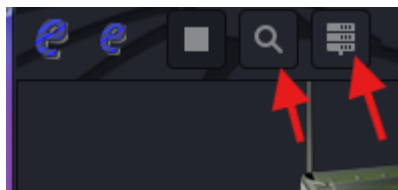
« sudo ettercap -G »

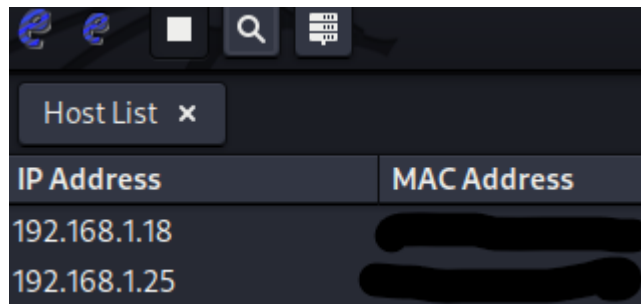
Nous devons Ensuite sélectionner notre Interface réseaux, dans notre exemple c'est le « eth0 »



2. Scanner le réseau :

Nous avons utilisé la fonction "**Scan for hosts**" d'Ettercap pour détecter les appareils sur le réseau local. Après avoir scanné, nous avons identifié la **victim** (IP : 192.168.1.25) et le **routeur** (IP : 192.168.1.254).





IP Address	MAC Address
192.168.1.18	[REDACTED]
192.168.1.25	[REDACTED]

3. Sélectionner les cibles :

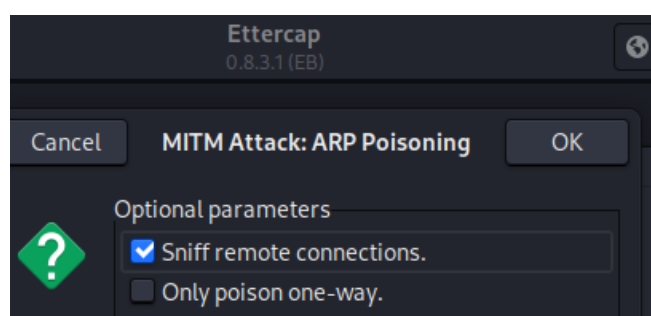
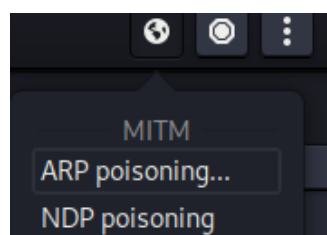
Une fois le réseau scanné, nous avons sélectionné la **victime** et le **routeur** comme cibles dans Ettercap. La victime était l'hôte dont nous souhaitons intercepter le trafic, tandis que le routeur agissait comme la passerelle vers Internet.

Nous allons renseigner comme « Target 1 » la **Victime** et mettre le **Routeur** comme « Target 2 »

4. Lancer l'attaque ARP Spoofing :

Nous avons lancé l'attaque **ARP Spoofing** en utilisant l'option "**ARP poisoning**" d'Ettercap. Cette option nous permet de rediriger tout le trafic entre la victime et le routeur via la machine Kali Linux. Les étapes suivantes ont été effectuées :

- Sélection de l'option "**Sniff remote connections**" pour intercepter le trafic réseau.



5. Vérification de l'attaque :

Une fois l'attaque lancée, nous avons vérifié dans Ettercap que le trafic entre la victime et le routeur était bien redirigé par notre machine Kali. En utilisant des outils comme **Wireshark**, nous avons pu observer que le trafic de la victime était effectivement intercepté.

192.168.1.18	239.255.255.250	UDP/XML	694 54539 → 3702 Len=652
192.168.1.25	192.168.1.254	ICMP	60 Echo (ping) reply id=0x7ee7, seq=32
192.168.1.25	192.168.1.254	ICMP	42 Echo (ping) reply id=0x7ee7, seq=32
192.168.1.71	192.168.1.255	UDP	210 8998 → 8998 Len=168
SagemcomBroa_ec:c7:95	Broadcast	ARP	60 Who has 192.168.1.25? Tell 192.168.1.2
00:ad:5d:01:12:00	SagemcomBroa_ec:c7:...	ARP	42 192.168.1.25 is at 00:ad:5d:01:12:00
00:ad:5d:01:12:00	b6:9c:3c:e9:8a:50	ARP	42 192.168.1.254 is at 00:ad:5d:01:12:00
00:ad:5d:01:12:00	SagemcomBroa_ec:c7:...	ARP	42 192.168.1.25 is at 00:ad:5d:01:12:00
00:ad:5d:01:12:00	SagemcomBroa_ec:c7:...	ARP	42 192.168.1.25 is at 00:ad:5d:01:12:00
00:ad:5d:01:12:00	b6:9c:3c:e9:8a:50	ARP	42 192.168.1.254 is at 00:ad:5d:01:12:00

6. Capture et analyse du trafic HTTP avec Wireshark

Analyser les paquets capturés :

En analysant les paquets capturés dans Wireshark, nous avons pu identifier des informations sensibles telles que des mots de passe en texte clair et d'autres données de formulaire envoyées par la victime. Ces informations ont été capturées grâce à l'attaque MITM, qui nous a permis de lire tout le trafic HTTP entre la victime et le serveur.

Nous avons choisi le site web de test <http://testphp.vulnweb.com/login.php>, qui accepte les requêtes en HTTP.

```
User-Agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
Referer: http://testphp.vulnweb.com/login.php\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: fr-FR,fr;q=0.9\r\n
\r\n
[Full request URI: http://testphp.vulnweb.com/userinfo.php]
File Data: 28 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
  Form item: "uname" = "TP-Kali"
    Key: uname
    Value: TP-Kali
  Form item: "pass" = "Azerty13."
```

V. Conclusion

Ce TP a démontré l'efficacité de l'attaque **Man-in-the-Middle (MITM)** via **ARP Spoofing**, qui permet d'intercepter le trafic réseau et de capturer des données sensibles telles que des **mots de passe** en texte clair. L'utilisation de **Wireshark** a révélé que les communications non sécurisées (HTTP) sont vulnérables aux interceptions.

Ce TP souligne l'importance d'utiliser des protocoles sécurisés comme **HTTPS** et de mettre en place des protections telles que **HSTS** pour éviter ce type d'attaque.

En conclusion, une gestion appropriée de la sécurité des communications est essentielle pour protéger les données sensibles contre les attaques MITM.