



FARINEL Sacha |
L'attaque « Man In
The Middle »
(L'Homme du milieu)

Dans cette documentation, nous allons voir ce que l'on appelle une attaque « MITM », comment cela se passe concrètement et comment s'en prémunir.

GRETA de Vannes, BTS SIO option SLAM.



I. Table des matières

I.	Qu'appelle-t-on une attaque « MITM » ?	2
A.	Définition :	2
B.	Quel est son but ?	2
C.	Comment cela fonctionne-t-il concrètement ?	3
a.	L'écoute des réseaux WI-FI	3
b.	DNS cache poisoning	3
c.	HTTPS spoofing.....	3
d.	Détournement de session	3
e.	L'Empoisonnement ARP.....	3
II.	La méthode MITM « ARP Poisoning »	4
A.	Qu'est-ce que l'ARP ?	4
B.	Qu'est-ce que l'empoisonnement ARP ?	4
C.	Les phases d'un empoisonnement ARP	5
a.	L'attaquant choisit une ou plusieurs machines victimes	5
b.	L'attaquant lance des outils et commence l'attaque	5
c.	L'attaquant utilise le trafic qu'il a détourné	5
D.	Les différents types d'empoisonnements ARP.....	5
E.	Quel est le but d'un empoisonnement ARP ?	6
F.	Quels sont les effets d'un empoisonnement ARP ?	7
G.	Comment détecter un empoisonnement du cache ARP.....	7
H.	Comment empêcher l'empoisonnement ARP	7
a.	Tables ARP statiques.....	7
b.	Sécurité du commutateur.....	8
c.	Sécurité physique.....	8
d.	Isolation du réseau.....	8
e.	Chiffrement	8
I.	Le mot de la fin	9
III.	Cas pratique	10
A.	Mise en service et installation	10
B.	Paramétrage de l'attaque avec Ettercap.....	10
C.	Initialisation de l'attaque avec WireShark.....	12
D.	Démarrage de l'attaque ARP Poisoning.....	13
E.	Première attaque : FTP	13
F.	Deuxième attaque : HTTP.....	14
G.	Jeux de rôle	15

L'attaque «Man in the Middle» (L'Homme du milieu)

I. Qu'appelle-t-on une attaque «MITM» ?

A. Définition :

Une attaque de l'homme du milieu désigne un modèle de cyberattaque dans lequel un cybercriminel installe, physiquement ou logiquement, un système contrôlé entre le système de la victime et une ressource Internet qu'elle utilise. L'objectif de l'attaquant est d'intercepter, de lire ou de manipuler toute communication entre la victime et sa ressource sans se faire remarquer.

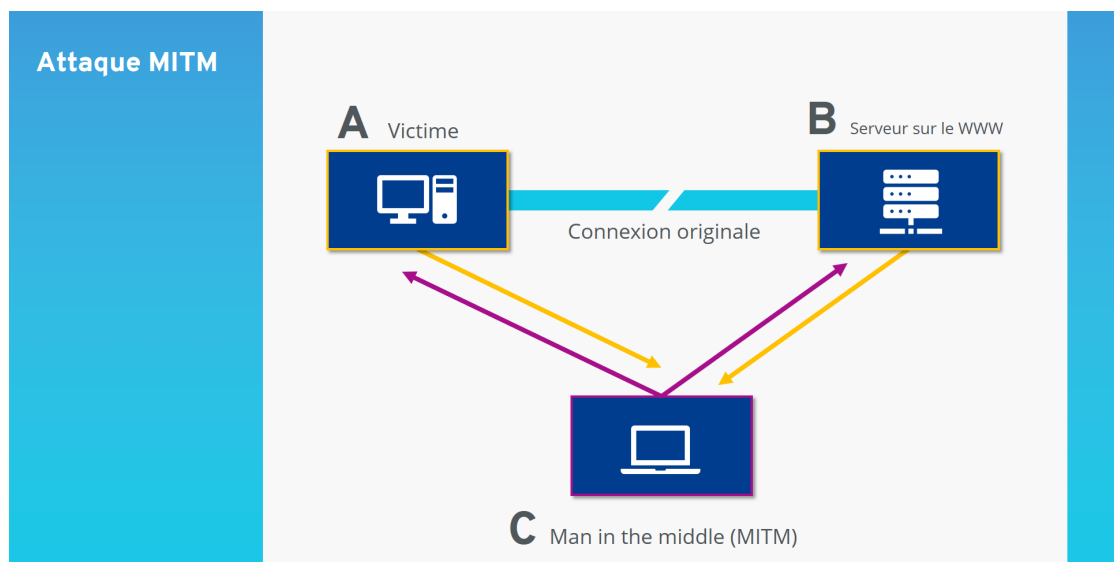


Figure 1 : Le fonctionnement d'une attaque MITM.

B. Quel est son but ?

La méthode de l'attaque MITM repose sur le fait que le hacker intercepte le trafic des données entre deux partenaires d'une communication, tout en laissant les deux parties penser qu'elles communiquent seules. Les attaques « man in the middle » sur les réseaux informatiques s'appliquent principalement pour contourner le cryptage SSL/TLS et accéder ainsi à des informations privées et secrètes, comme les noms d'utilisateurs, les mots de passe ou encore les coordonnées bancaires.

C. Comment cela fonctionne-t-il concrètement ?

Auparavant, ces attaques ont été menées en manipulant le canal de communication physique. En temps de partage des communications sur les réseaux publics, des tiers non autorisés peuvent logiquement interférer entre deux ou plusieurs partenaires de communication. De nos jours, il existe plusieurs types d'attaques MITM :

a. L'écoute des réseaux WI-FI

Un attaquant peut « écouter » le trafic d'un réseau Wi-Fi public, voire créer un faux réseau Wi-Fi auquel des personnes vont se connecter. C'est une attaque dangereuse et facile à mettre en place.

b. DNS cache poisoning

DNS veut dire *Domain Name System*, soit système de noms de domaine en français. Un type d'attaque *man-in-the-middle* est l'empoisonnement du cache DNS. L'attaquant donne une fausse entrée DNS qui renvoie vers un faux site web. L'utilisateur croit être sur le bon site web et va naturellement entrer ses données, celles d'un compte mail par exemple. L'attaquant peut aussi faire transiter le réseau de l'utilisateur à son ordinateur, puis de son ordinateur vers le vrai site web.

c. HTTPS spoofing

Une attaque consiste à utiliser la confiance d'un utilisateur envers les URL en HTTPS. L'attaquant crée un faux site web avec un certificat d'authentification valide et une URL à peine différente du vrai site web, par exemple en changeant la valeur Unicode d'un caractère (sans changer le caractère). Le phishing est un bon moyen de faire en sorte que l'utilisateur aille sur le site en question. Une fois que le certificat d'authentification est stocké sur l'ordinateur de la victime, l'attaquant relaie le trafic vers le vrai site *via* son ordinateur.

d. Détournement de session

Lors d'un détournement de session, l'attaquant attend que la victime se connecte à une page web, par exemple le site de sa banque. Il vole ensuite le cookie de session pour se connecter à ce même compte depuis son navigateur. Il peut ainsi utiliser le compte de la victime.

e. L'Empoisonnement ARP

L'ARP poisoning ou empoisonnement ARP est un type de cyberattaque qui exploite les faiblesses du protocole ARP (Address Resolution Protocol) très largement utilisé, pour interrompre, rediriger ou espionner le trafic réseau.

C'est cette attaque que nous allons essayer de comprendre aujourd'hui.

II. La méthode MITM « ARP Poisoning »

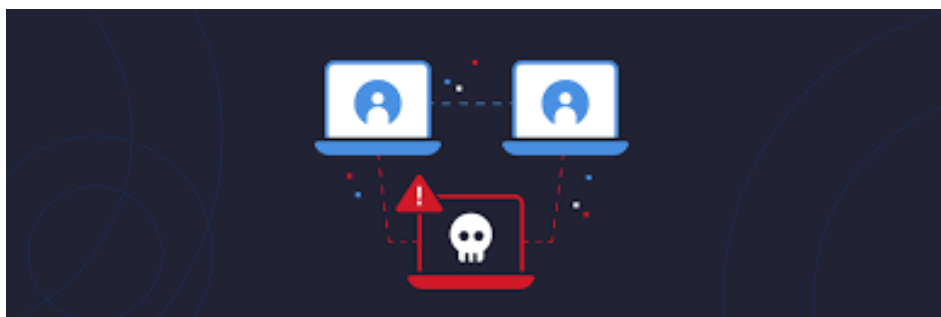
A. Qu'est-ce que l'ARP ?

Le protocole ARP a été conçu pour soutenir l'approche en couches utilisée depuis le tout début des réseaux informatiques. Chaque couche, des signaux électriques qui voyagent le long d'un câble Ethernet au code HTML utilisé pour afficher une page Web, fonctionne en grande partie indépendamment des autres. C'est pour cela que nous pouvons aujourd'hui utiliser l'IPv4, une technologie de couche réseau qui remonte au début des années 1980, en même temps que des technologies récentes comme le Wi-Fi et le Bluetooth. Les couches plus basses, physiques et de liaison de données, s'occupent de transférer les données via un canal spécifique comme les ondes radio.

Le but de l'ARP est de faire en sorte que les adresses de la couche liaison de données – appelées adresses MAC – et les adresses de la couche réseau, typiquement les adresses IP, puissent dialoguer entre elles. Il permet aux appareils sur le réseau de « demander » quel appareil correspond à une adresse IP donnée. Les appareils peuvent également annoncer ce mappage au reste du réseau, sans qu'on le leur demande. Pour être plus efficaces, les appareils mettent généralement en cache ces réponses et enregistrent une liste actualisée de correspondances « adresses IP-adresses MAC ».

B. Qu'est-ce que l'empoisonnement ARP ?

L'empoisonnement ARP ou ARP poisoning consiste à exploiter les faiblesses de l'ARP pour corrompre les correspondances adresses IP-adresses MAC des autres appareils sur le réseau. Quand l'ARP a fait ses débuts en 1982, la sécurité ne faisait pas partie des préoccupations premières et les créateurs de ce protocole n'ont pas inclus de mécanismes d'authentification pour valider les messages ARP. Tout appareil sur le réseau peut répondre à une requête ARP, que le message d'origine lui soit destiné ou non. Par exemple, si l'ordinateur A « demande » l'adresse MAC de l'ordinateur B, un attaquant sur l'ordinateur C peut répondre et l'ordinateur A traitera cette réponse comme une réponse authentique. Cet oubli a ouvert la voie à une variété d'attaques. Grâce à des outils facilement accessibles, un acteur malveillant peut « empoisonner » le cache ARP des autres hôtes sur un réseau local, en remplissant le cache ARP d'entrées inexactes.



C. Les phases d'un empoisonnement ARP

a. L'attaquant choisit une ou plusieurs machines victimes

La première étape dans la planification et l'exécution d'un empoisonnement ARP est de choisir sa cible. Il peut s'agir d'un terminal spécifique sur le réseau, d'un groupe de terminaux ou d'un appareil réseau comme un routeur. Les routeurs sont des cibles prisées car une attaque réussie sur l'ARP contre un routeur peut interrompre le trafic d'un sous-réseau tout entier.

b. L'attaquant lance des outils et commence l'attaque

Une grande variété d'outils sont facilement accessibles à quiconque cherche à exécuter un empoisonnement ARP. Après avoir lancé l'outil de son choix et configuré les paramètres applicables, l'attaquant passe à l'attaque. Il commencera peut-être immédiatement à diffuser des messages ARP ou attendra de recevoir une requête de l'un des appareils.

c. L'attaquant utilise le trafic qu'il a détourné

Une fois le cache ARP corrompu sur une ou plusieurs machines victimes, l'attaquant agira d'une manière ou d'une autre sur le trafic détourné. Il peut alors l'inspecter, le modifier ou le faire disparaître dans un « blackhole » (trou noir) pour qu'il n'atteigne jamais la destination prévue. L'action entreprise par l'attaquant dépend de ses motivations.

D. Les différents types d'empoisonnements ARP

Un empoisonnement ARP survient généralement de deux façons : soit l'attaquant attend de voir une requête ARP qui vise une cible en particulier et émet une réponse à sa place, soit il envoie un message non sollicité à tout le réseau, qu'on appelle aussi « gratuitous ARP ». La première approche est moins détectable sur le réseau et son impact moins grave également. Un « gratuitous ARP » en revanche, est plus immédiat et peut affecter davantage de machines, mais il a l'inconvénient de générer beaucoup d'activité sur le réseau. Quelle que soit l'approche, le ou les caches ARP corrompus sur les machines victimes peuvent être davantage exploités par la suite :

a. L'attaque MITM

Les attaques de l'homme du milieu sont probablement le but le plus courant, et potentiellement le plus dangereux, d'un empoisonnement ARP. L'attaquant envoie des réponses ARP falsifiées pour une adresse IP donnée, en général la passerelle par défaut d'un subnet. Suite à cela, les machines victimes remplissent leur cache ARP avec l'adresse MAC de la machine de l'attaquant, au lieu de l'adresse MAC du routeur local. Les machines victimes redirigeront alors leur trafic réseau vers l'attaquant, sans le savoir. Des outils comme Ettercap permettent à l'attaquant d'agir comme proxy et de voir ou de modifier les informations avant d'envoyer le trafic vers sa destination voulue. Pour la victime, tout paraît normal.

Conjuguer l'empoisonnement ARP et l'empoisonnement DNS peut radicalement augmenter l'efficacité d'une attaque de l'homme du milieu. Dans ce scénario, l'utilisateur victime peut saisir le nom d'un vrai site comme google.com et recevoir l'adresse IP de la machine de l'attaquant, au lieu de la bonne adresse.

b. L'attaque DDOS

Une attaque DoS vise à refuser à une ou plusieurs victimes l'accès à des ressources réseau. Dans le cas de l'ARP, l'attaquant enverra peut-être des messages de réponse ARP qui mappent incorrectement des centaines voire des milliers d'adresses IP à une seule adresse MAC, surchargeant potentiellement la machine ciblée. Ce type d'attaque, parfois appelée « ARP flooding » ou inondation ARP, peut également viser les commutateurs, pour affecter la performance du réseau dans son ensemble.

c. Le piratage de session

Le piratage de session est similaire par sa nature aux attaques de l'homme du milieu, à l'exception du fait que l'attaquant ne redirige pas dans ce cas le trafic de la machine victime vers sa destination voulue. Au lieu de cela, l'attaquant capture une séquence TCP authentique ou un cookie Web de la victime et l'utilise pour se faire passer pour elle. Cette tactique peut servir par exemple à accéder aux comptes de réseaux sociaux d'un utilisateur s'il y est connecté.

E. Quel est le but d'un empoisonnement ARP ?

Les pirates ne manquent pas de motivations et l'empoisonnement ARP ne fait pas exception. Un attaquant peut lancer ce genre d'attaque pour de nombreuses raisons, qui vont de l'espionnage de haut vol à l'exaltation d'avoir perturbé un réseau. Dans un scénario potentiel, un attaquant utilise des messages ARP falsifiés pour remplacer la passerelle par défaut d'un sous-réseau donné et réussira à rediriger l'ensemble du trafic sur sa machine, au lieu du routeur local. Il pourra alors espionner, modifier ou éliminer le trafic. Ces attaques génèrent du « bruit » car elles laissent des traces mais elles n'interfèrent pas avec le fonctionnement du réseau. Si le but ultime est l'espionnage, la machine de l'attaquant transfèrera simplement le trafic vers sa destination d'origine et l'utilisateur final ne saura jamais que quelque chose s'est passé.

En revanche, une attaque DoS peut chercher à créer des perturbations suffisamment visibles dans le fonctionnement du réseau. Bien que les motivations ici pourraient être d'empêcher simplement une entreprise de fonctionner à la normale, les attaques DoS sont souvent exécutées par des attaquants moins compétents qui prennent du plaisir à créer des problèmes.

Les attaques en interne sont particulièrement inquiétantes quand il s'agit d'un empoisonnement ARP. Les messages ARP piratés n'iront pas au-delà des limites du réseau local, l'attaque doit donc être lancée à partir d'un appareil connecté au réseau local. Il n'est pas impossible pour quelqu'un d'externe de lancer une attaque sur l'ARP, mais il devra d'abord compromettre à distance un système local via d'autres moyens. Une personne interne, en revanche, aura seulement besoin d'un accès au réseau et de quelques outils facilement disponibles

F. Quels sont les effets d'un empoisonnement ARP ?

L'impact le plus direct d'un empoisonnement ARP est que le trafic destiné à un ou plusieurs hôtes sur le réseau local sera redirigé vers la destination choisie par l'attaquant. Les effets précis de cette redirection dépendent des paramètres spécifiques de l'attaque. Le trafic pourrait être redirigé sur la machine de l'attaquant ou envoyé vers un lieu qui n'existe pas. Dans le premier cas, on ne remarquerait rien du tout, tandis que le second cas pourrait interdire l'accès au réseau.

L'empoisonnement du cache ARP lui-même ne dure pas dans le temps. Les entrées ARP sont mises en cache pendant quelques minutes pour les appareils finaux ou quelques heures pour les commutateurs. Dès qu'un attaquant met fin à l'empoisonnement des tables, les entrées corrompues deviennent obsolètes et le flux correct du trafic reprend. L'empoisonnement ARP seul ne laisse pas de traces permanentes d'infection ni de présence sur les machines victimes. Cependant, les pirates combinent souvent plusieurs types d'attaques et l'empoisonnement ARP peut être une partie seulement d'une campagne plus vaste.

G. Comment détecter un empoisonnement du cache ARP

De nombreux logiciels commerciaux et open source existent pour détecter un empoisonnement du cache ARP, mais vous pouvez facilement vérifier les tables ARP sur votre ordinateur sans installer quoi que ce soit. Sur la plupart des systèmes Windows, Mac et Linux, la commande « arp-a » sur un terminal ou dans l'invite de commande affichera les mappages actuels IP-MAC de la machine.

Les outils comme arpwatch et X-ARP sont utiles pour surveiller le réseau en continu et peuvent alerter un admin si des signes d'empoisonnement du cache ARP sont détectés. Toutefois, attention aux faux positifs qui peuvent créer beaucoup d'alertes indésirables.

H. Comment empêcher l'empoisonnement ARP

Il existe différentes approches pour empêcher une attaque par empoisonnement ARP :

a. Tables ARP statiques

Il est possible de mapper de manière statique toutes les adresses MAC d'un réseau à leur adresse IP correcte. Cette méthode est très efficace dans la prévention de ce type d'attaque, mais elle ajoute une charge importante de travail aux admin. Tout changement effectué sur le réseau devra être répercuté manuellement dans les tables ARP sur tous les hôtes. Cette technique n'est donc pas réalisable pour la plupart des grandes entreprises. Pourtant, dans les situations où la sécurité est cruciale, élaborer un segment réseau séparé, dans lequel seront utilisées des tables ARP statiques, est un bon moyen de protéger les informations critiques.

b. Sécurité du commutateur

La plupart des commutateurs Ethernet gérés sont dotés de fonctionnalités conçues pour atténuer les attaques d'empoisonnement ARP. Généralement connues sous le nom de Dynamic ARP Inspection (DAI) ou inspection dynamique de l'ARP, ces fonctionnalités évaluent la validité de chaque message ARP et éliminent les paquets qui ont l'air suspects ou malveillants. La DAI peut aussi être configurée pour limiter le débit de transfert des messages ARP via le commutateur et ainsi empêcher efficacement les attaques DoS.

La DAI et autres fonctionnalités similaires étaient auparavant l'apanage des équipements réseau haut de gamme, mais elles sont aujourd'hui fournies de série sur quasiment tous les commutateurs professionnels, même ceux des petites entreprises. Une bonne pratique consiste à activer la DAI sur tous les ports excepté ceux connectés à d'autres commutateurs. Cette fonctionnalité n'a pas beaucoup d'impact sur les performances mais devra possiblement être activée avec d'autres fonctionnalités comme le DHCP Snooping.

Appliquer une sécurité au niveau du port sur un commutateur peut également atténuer les attaques d'empoisonnement du cache ARP. La sécurité des ports peut être configurée pour n'autoriser qu'une seule adresse MAC sur un port du commutateur, empêchant les attaquants potentiels de prendre plusieurs identités sur le réseau.

c. Sécurité physique

Pour atténuer les attaques d'empoisonnement ARP, vous pouvez aussi contrôler l'accès physique des personnes aux locaux de votre entreprise. Les messages ARP ne sont pas redirigés hors du réseau local, les attaquants potentiels doivent donc se trouver à proximité du réseau ciblé ou avoir déjà accès à l'une des machines du réseau. Notez que dans le cas des réseaux sans fil, la proximité ne signifie pas forcément que l'attaquant doit se trouver physiquement dans les locaux, un signal qui capterait jusqu'à la rue ou sur le parking peut être suffisant. Que le réseau soit filaire ou sans fil, l'utilisation d'une technologie de type 802.1x peut garantir que seuls les appareils autorisés et/ou gérés puissent se connecter au réseau.

d. Isolation du réseau

Comme nous l'avons déjà dit, les messages ARP ne voyagent pas au-delà du subnet local. Cela signifie qu'un réseau bien segmenté est potentiellement moins vulnérable à un empoisonnement du cache ARP. En effet, une attaque sur l'un des subnets ne pourrait pas se propager aux autres appareils. Concentrer les ressources importantes dans un segment dédié du réseau derrière une sécurité renforcée peut considérablement diminuer l'impact potentiel d'un empoisonnement ARP.

e. Chiffrement

Bien que le chiffrement ne soit pas capable d'empêcher les attaques ARP, il peut atténuer les dégâts potentiels qu'elles causeraient. Les attaques de l'homme du milieu étaient souvent utilisées pour capturer des identifiants de connexion, qui étaient auparavant transmis en texte brut. Avec l'utilisation plus répandue du chiffrement SSL/TLS sur Internet, ce type d'attaque est devenu plus difficile à exécuter. L'acteur malveillant peut encore intercepter le trafic, mais il ne peut rien en faire sous sa forme chiffrée.

I. Le mot de la fin

Bien qu'il soit pratiqué depuis plus longtemps que les menaces modernes comme les ransomwares, l'empoisonnement ARP reste un danger pour les entreprises. Comme toutes les cybermenaces, la meilleure solution consiste à mettre en place un programme complet de sécurité de l'information. Les solutions Varonis de détection et de réponse peuvent vous aider à déterminer où se situe votre entreprise en matière de sécurité. Varonis Edge peut vous permettre de détecter les signes d'exfiltration de données pouvant survenir après un empoisonnement ARP.

III. Cas pratique

Dans cette partie, nous allons tenter de reproduire sur nos machines une attaque MITM avec pour méthode l'ARP poisoning. Pour ce faire, nous allons avoir besoin de :

- Wireshark, logiciel d'analyse de paquets.
- Ettercap, logiciel d'analyse du réseau informatique. Il va être capable d'intercepter le trafic sur un segment de notre réseau.
- Un serveur LAMP accessible via SSH. Il sera la cible de nos attaques.
- Un Client GNU/Linux. Il sera le « sniffer », celui qui va analyser les paquets envoyés.

Nos deux machines seront virtualisées à l'aide de VirtualBox et toutes les deux en accès par ponts.

A. Mise en service et installation

Sur notre machine « client » Ubuntu, en mode graphique, il faut :

Mettre à jour les paquets systèmes :

```
sio@sio-VirtualBox:~$ sudo apt-get update
```

Installer WireShark :

```
sio@sio-VirtualBox:~$ sudo apt-get install wireshark
```

Installer Ettercap :

```
sio@sio-VirtualBox:~$ sudo apt-get install ettercap-graphical
```

Il faut ensuite activer la redirection des IP : (Il faut se mettre en super admin → sudo su)

```
root@sio-VirtualBox:/home/sio# sudo echo 1 > /proc/sys/net/ipv4/ip_forward
```

Pour vérifier si cela à bien été pris en compte, il faut taper la commande suivante :

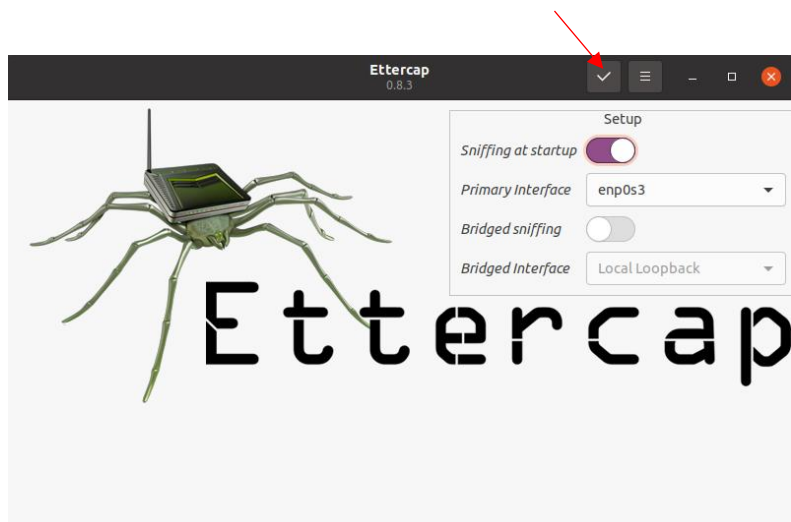
```
root@sio-VirtualBox:/home/sio# cat /proc/sys/net/ipv4/ip_forward
1
```

B. Paramétrage de l'attaque avec Ettercap

On lance Ettercap en mode graphique afin de préparer l'attaque :


```
root@sio-VirtualBox:/home/sio# sudo ettercap -G
```

La fenêtre Ettercap apparaît (ainsi qu'un onglet dans le menu déroulant à gauche).



Il faut ensuite cliquer sur l'icône : 



Trois nouveaux icône apparaissent, cliquer sur l'icône  afin de scanner votre réseau. Dans mon cas, il a découvert 4 hôtes sur mon réseau.

```
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
4 hosts added to the hosts list...
```

Grâce à Ettercap, je vois mon hôte Windows :

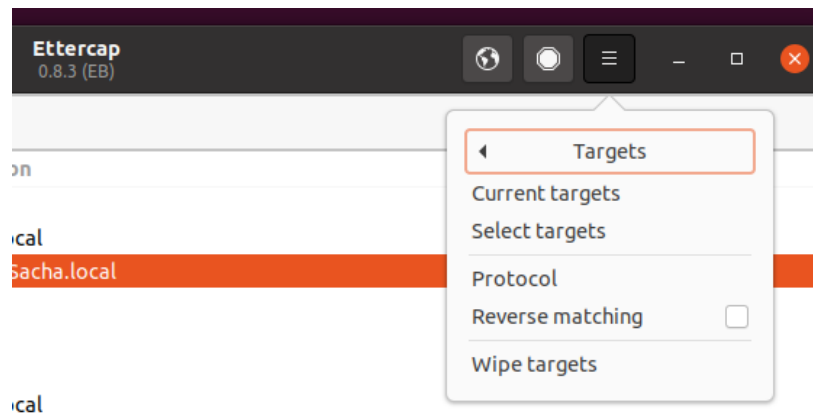
192.168.1.13 **1C:BF:CE:64:21:B1** **DESKTOP-Sacha.local**


Ainsi que mon serveur LAMP :

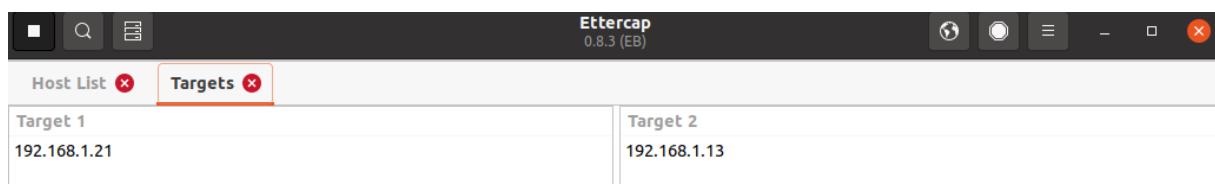
192.168.1.21 **08:00:27:BD:96:35**

Je peux maintenant les ajouter en tant que cible (*target*).

J'ajoute mon serveur LAMP en tant que « target 1 » et mon hôte Windows en tant que « target 2 ».



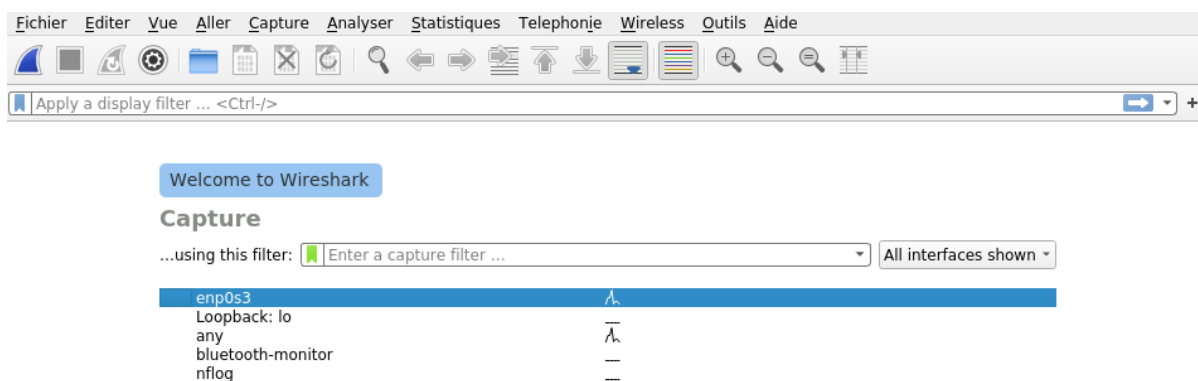
Je peux maintenant les retrouver en cliquant sur l'icône , puis sur « targets » et enfin sur « current target ».



C. Initialisation de l'attaque avec Wireshark

Sur notre hôte « sniffer », celui qui pratique l'attaque, lancer Wireshark :

```
sio@sio-VirtualBox:~$ sudo wireshark
```




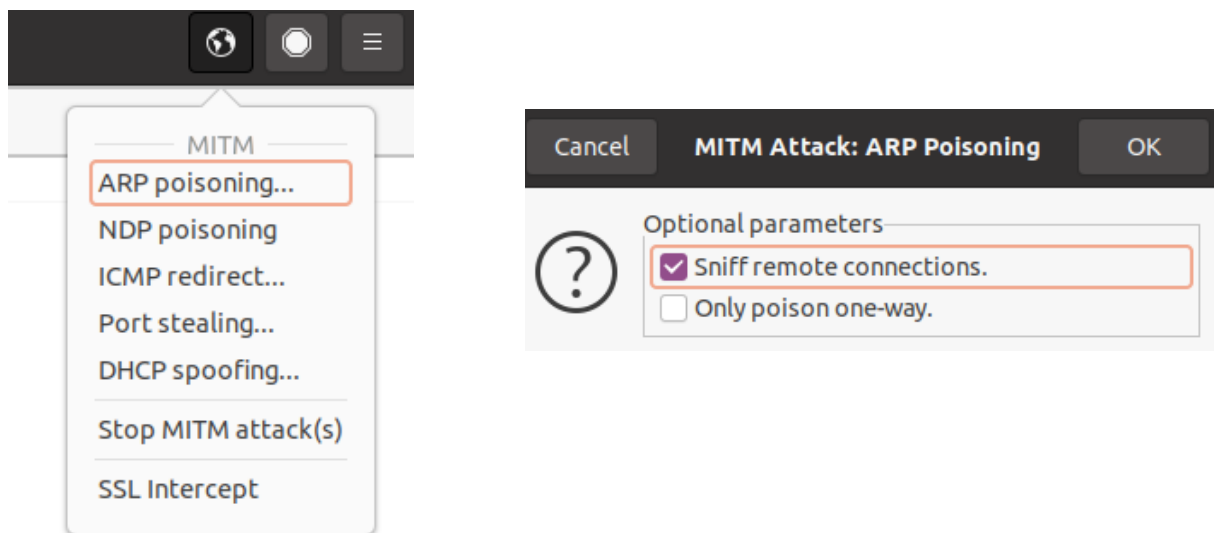
Grâce à Wireshark, nous pouvons voir l'envoi et la réception des paquets de données sur notre réseau.

```
128 99.728531046 192.168.1.1
129 99.831671406 192.168.1.13
130 101.647387051 192.168.1.11
131 101.981047341 IngramMi_ee:09:
132 102.446721774 192.168.1.23
```

D. Démarrage de l'attaque ARP Poisoning



Retourner sur Ettercap et cliquer sur l'icône  afin d'accéder au menu MITM, puis sur ARP Poisoning (N'oubliez pas d'activer le sniffing) :



E. Première attaque : FTP

Dans cette partie, nous allons voir les failles que contient le FTP (*File Transfer Protocol*). De nos jours, il a été remplacé par un protocole bien plus sécurisé, le FTPS (*File Transfer Protocol Secure*) ou SFTP (*Secure File Transfer Protocol*) connu sous le nom de protocole de transfert de fichiers SSH.

Pour ce faire, nous devons ouvrir un gestionnaire de FTP, comme FileZilla.



Puis, cliquer sur l'icône , afin d'entrer dans le gestionnaire de site.

Il faudra rentrer les informations suivantes (en remplaçant bien évidemment l'IP de votre serveur) :

Nous voyons bien que même FileZilla nous avertit que la connexion en FTP simple est **non sécurisée**.

Si nous retournons sur notre machine qui effectue une attaque MITM, nous pouvons nous apercevoir qu'elle a eu accès à notre identifiant ainsi qu'à notre mot de passe.

```
GROUP 1 : 192.168.1.21 08:00:27:BD:96:35
GROUP 2 : 192.168.1.13 1C:BF:CE:64:21:B1
FTP : 192.168.1.21:21 -> USER: sio PASS: sio
```

F. Deuxième attaque : HTTP

Nous allons maintenant voir un deuxième type d'attaque. La récupération d'information d'un formulaire, transmise au travers de PHP grâce à la méthode POST, possible sur les sites non sécurisés, en HTTP. Cette attaque n'est pas à négliger, car même si le protocole HTTP a été remplacé depuis par le protocole HTTPS, il s'avère néanmoins qu'il reste plus de 15% des sites mondiales qui n'ont pas encore passé le cap.

Pour tester cette attaque, j'ai à disposition un petit document PHP, contenant deux inputs gérés par une méthode POST afin de comparer la validité du mot de passe.



POST String :

```
Array
(
    [user] => bob
    [password] => abc123
    [rank] => superadmin
    [validate] => Validate
)
```

Welcome Bob !

- password=abc123
- rank=superadmin

Si par exemple notre utilisateur rentre son identifiant et son mot de passe, voilà se que notre hacker pourra apercevoir sur Ettercap (*Les informations sensibles sont ici divulguées !*)

```
HTTP : 192.168.1.21:80 -> USER: bob+ PASS: abc123 INFO: http://192.168.1.21/php_post.php
CONTENT: user=bob+&password=abc123&rank=superadmin&validate=Validate
```

G. Jeux de rôle

Nous allons effectuer une petite mise en situation. Ici le but est de reproduire ce que nous venons de voir, mais ce n'est pas tout. En effet, l'enjeu n'est pas de savoir effectuer des attaques MITM, mais bien de les empêcher !

Pour ce faire, je vais simuler une attaque MITM avec 3 participant :



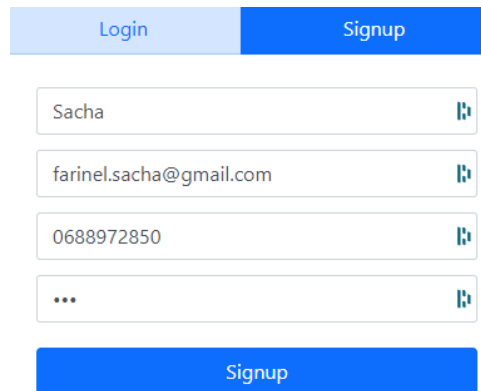
- **Un utilisateur « lambda »**, qui créera un compte, sur notre hôte Windows.
- **La personne du milieu**, qui essayera de détourner les identifiants de l'utilisateur afin de lui subtiliser son compte.
- **L'administrateur du serveur**, qui lui devra contrer cette attaque.

Mise en route :

- Avec son navigateur, l'utilisateur doit se connecter sur l'interface ci-dessus avec l'IP du serveur géré par le dev/admin.
- Le dev/admin doit avoir mis en route son serveur LAMP et commencer l'analyse du code source (cf. *interface ci-dessus*).
- Le hacker doit connaître l'IP du serveur géré par le dev/admin et celle de sa cible (user). Ettercap et Wireshark doivent être actifs pour les 2 cibles !

L'action :

1 - L'**utilisateur** va s'inscrire (*Signup*), puis va se connecter (*Login*).

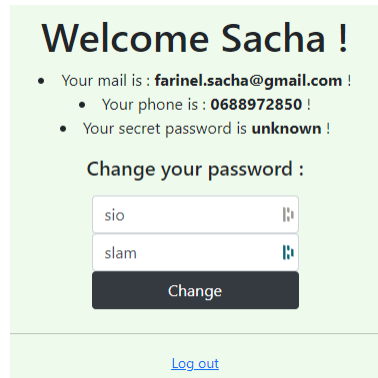


The image shows a web form for user registration. At the top, there are two tabs: 'Login' (light blue) and 'Signup' (dark blue). Below the tabs are four input fields, each with a blue eye icon on the right: the first contains 'Sacha', the second 'farinel.sacha@gmail.com', the third '0688972850', and the fourth contains three dots '...'. At the bottom of the form is a large blue button labeled 'Signup'.

2 - À ce moment le **hacker** a intercepté avec *Ettercap* les identifiants de user qu'il a su analyser (*user/password*).

```
HTTP : 192.168.1.21:80 -> USER: Sacha PASS: INFO: http://192.168.1.21/mitm/
CONTENT: user_name=Sacha&user_mail=farinel.sacha%40gmail.com&user_phone=0688972850&user_pswd=sio
```

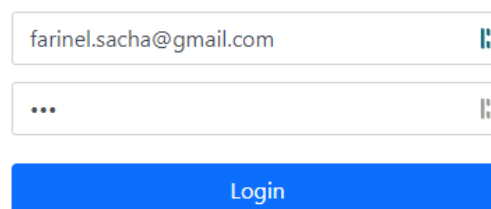
3 - Le hacker connaît maintenant l'identifiant et le mot de passe de l'utilisateur ! Avec son navigateur le hacker va se connecter sur le compte de l'utilisateur. Le hacker change le mot de passe, connu par lui seul maintenant.



The image shows a green-themed 'Welcome' page for a user named 'Sacha'. The title is 'Welcome Sacha !'. Below it, there is a list of user details: 'Your mail is : farinel.sacha@gmail.com !', 'Your phone is : 0688972850 !', and 'Your secret password is unknown !'. A section titled 'Change your password :' contains two input fields with blue eye icons; the first is labeled 'sio' and the second 'slam'. Below these fields is a dark grey button labeled 'Change'. At the bottom of the page is a blue link labeled 'Log out'.

4 - L'**utilisateur** va à nouveau se reconnecter (*Login*). Évidemment, la connexion sera refusée.

Il avertit (« *par email* ») l'administrateur (*dev/admin*) au sujet de cette anomalie.



The image shows a login form. It has two input fields with blue eye icons: the first contains the email 'farinel.sacha@gmail.com' and the second contains three dots '...'. Below the fields is a large blue button labeled 'Login'.

Accès non reconnu !

5 - L'**administrateur** « *très inquiet* » va analyser les logs Apache de son serveur afin d'identifier l'IP du hacker. Probablement, l'IP sera identifiée sur les dernières lignes de son fichier *access.log*.

Pour ce faire, l'administrateur doit taper la commande suivante :

```
root@ubuntu:~# tail -f /var/log/apache2/access.log
```

Il voit apparaître le journal des connexion sur son serveur :

```
192.168.1.24 - - [09/Jan/2022:18:26:35 +0000] "GET /mitm/asset/js/welcome.js HT1
192.168.1.24 - - [09/Jan/2022:18:26:35 +0000] "GET /mitm/asset/js/jquery.min.js
192.168.1.24 - - [09/Jan/2022:18:26:42 +0000] "POST /mitm/index.php?ajax=change
```

Une activité suspecte, ce n'est pas l'adresse IP de l'utilisateur qui vient de le contacter par mail. Il vient de mettre la main sur l'IP du hacker.

6 - Le **dev/admin** va appliquer cette règle à la racine de son serveur *Apache* afin de bloquer l'accès du hacker :

```
root@ubuntu:/etc# cd /var/www/html
root@ubuntu:/var/www/html# nano .htaccess
```

Et de taper :

```
GNU nano 4.8
deny from 192.168.1.24
```

7 - Le **dev/admin** va devoir trouver une solution afin de rétablir les données de l'utilisateur.

Dans ce cas, un mot de passe temporaire sera transmis discrètement à l'utilisateur.

Une solution simple, mais pas très pratique, est que l'amin créer un nouveau compte. Cela générera son mot de passe avec le hashage MD5 ainsi que le salage de celui-ci. Il se trouvera chiffré dans le document : *users.json*

```
{
  "mot_de_passe_provisoire": {
    "name": "mdp_provisoire",
    "phone": "0000000000",
    "password": "5bca4e763a9ce3927bb7ad5bf4265d00",
    "salt": "b9b096ab698d55b4fe6e7ff2ddd1d288"
  }
}
```

Il n'aura plus qu'à remplacer le mot de passe de l'utilisateur (qui est inconnu) ainsi que le sel par ceux qu'il vient de générer.

```
{
  "farinel.sacha@gmail.com": {
    "name": "Sacha",
    "phone": "0688972850",
    "password": "5bca4e763a9ce3927bb7ad5bf4265d00",
    "salt": "b9b096ab698d55b4fe6e7ff2ddd1d288"
  },
  "mot_de_passe_provisoire": {
    "name": "mdp_provisoire",
    "phone": "0000000000",
    "password": "5bca4e763a9ce3927bb7ad5bf4265d00",
    "salt": "b9b096ab698d55b4fe6e7ff2ddd1d288"
  }
}
```

L'administrateur n'aura plus qu'à lui communiquer le mot de passe en clair via une plateforme sécurisée.

Welcome Sacha !

- Your mail is : **farinel.sacha@gmail.com** !
 - Your phone is : **0688972850** !
 - Your secret password is **unknown** !

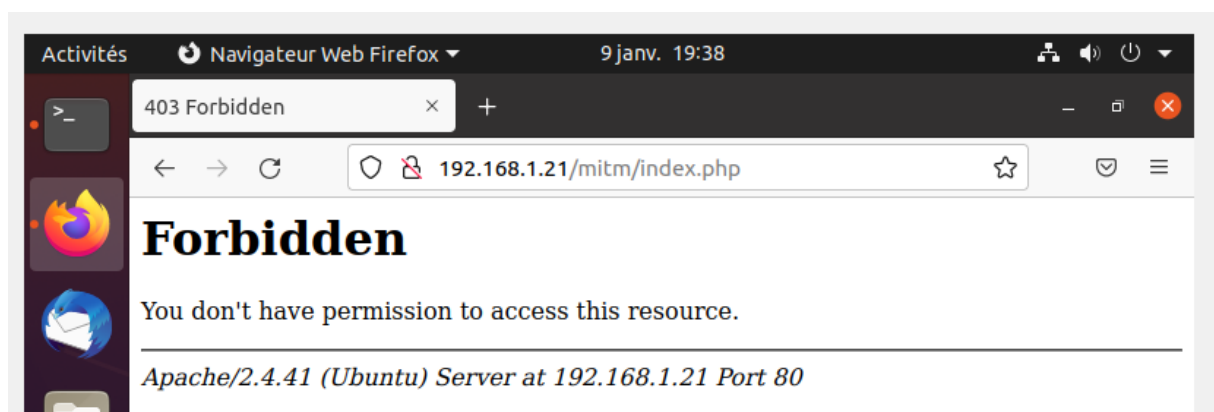
Change your password :

Old password
 New password

Change

[Log out](#)

8 - Avec son navigateur, **Le hacker** ne pourra plus se connecter sur le serveur du dev/admin.



9 - **L'utilisateur** va devoir se connecter (*Login*) avec le protocole **HTTPS** et changer son mot de passe !

Pour que notre utilisateur puisse utiliser le protocole HTTPS, il va falloir configurer notre serveur. Pour ce faire, nous allons avoir besoin d'installer OpenSSL :

Il faut mettre à jour notre système :

```
root@ubuntu:/home/sio# sudo apt-get update
```

Installer OpenSSL :

```
root@ubuntu:/home/sio# apt-get install openssl
```

Activer le module Apache :

```
root@ubuntu:/home/sio# sudo a2enmod ssl
```

```
root@ubuntu:/home/sio# sudo a2enmod rewrite
```

A présent, nous pouvons créer le dossier de notre certificat et y placé notre clé privé ainsi que notre certificat :

```
root@ubuntu:/home/sio# sudo mkdir /etc/apache2/certificate
```

```
root@ubuntu:/home/sio# cd /etc/apache2/certificate
```

```
sudo openssl req -new -newkey rsa:4096 -x509 -sha256 -days 365 -nodes -out  
apache-certificate.crt -keyout apache.key
```

Nous devons maintenant remplir les informations contenus dans le certificat : Pays, région, organisme, nom, email, etc.

A présent, nous devons éditer le fichier configuration d'Apache2 :

```
root@ubuntu:/etc/apache2/certificate# sudo nano /etc/apache2/sites-enabled/000-default.conf
```

Et remplacer :

```
<VirtualHost *:80>  
    ServerAdmin webmaster@localhost  
    DocumentRoot /var/www/html  
    ErrorLog ${APACHE_LOG_DIR}/error.log  
    CustomLog ${APACHE_LOG_DIR}/access.log combined  
</VirtualHost>
```

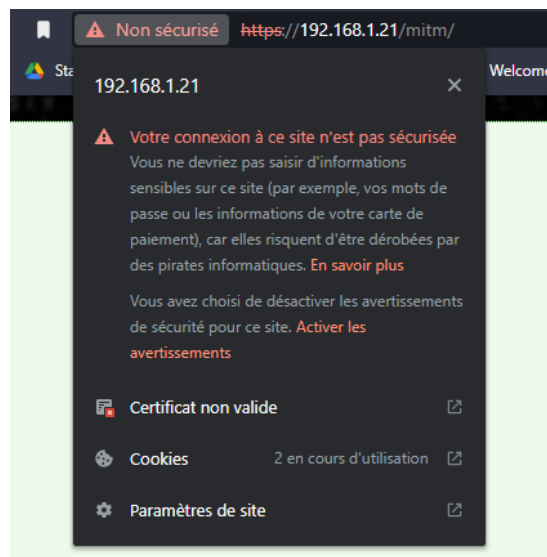
Par :

```
<VirtualHost *:443>
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
    SSLEngine on
    SSLCertificateFile /etc/apache2/certificate/apache-certificate.crt
    SSLCertificateKeyFile /etc/apache2/certificate/apache.key
</VirtualHost>
```

Il ne reste plus qu'à redémarrer notre serveur :

```
root@ubuntu:/etc/apache2/certificate# sudo service apache2 restart
```

Maintenant, si nous rentrons : <https://192.168.1.21/mitm/> , nous avons notre page en https !



10 - À ce moment, le hacker n'aura aucune information avec *Ettercap*.

