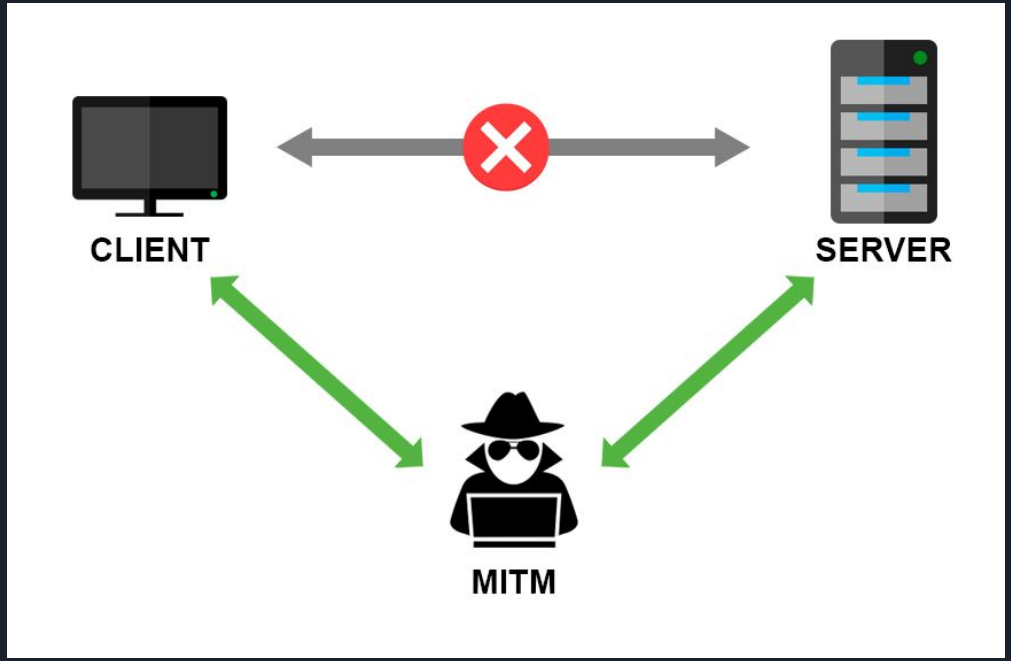
Sécurité réseau et MITM

MITM : Man In the Middle

Attaque de l'**homme du milieu** en français

MITM Passif : observe juste le trafic

MITM Actif : modifie le trafic

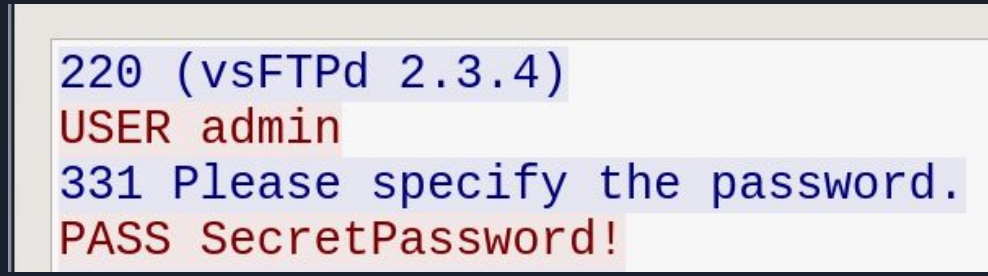


MITM : Man In the Middle

Un attaquant va pouvoir **récupérer des identifiants.**

Protocoles non chiffrés :

- FTP
- Telnet
- HTTP
- POP



Interception de trafic FTP avec Wireshark

ARP cache poisoning

ARP

La table ARP fait le lien entre :

- les adresses matérielles / Ethernet
- les adresses IP

Tout matériel relié à Internet possède sa propre adresse MAC.

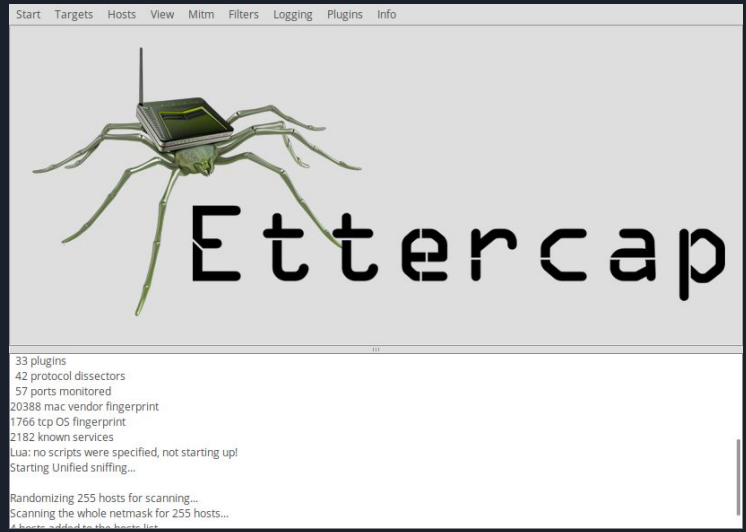
```
└─$ arp -n
Address                  HWtype  HWaddress
192.168.3.50             ether   00:0c:29:09:bf:86
192.168.3.171            ether   00:0c:29:20:7b:3a
192.168.3.17             ether   00:0c:29:d4:35:4b
192.168.3.62             ether   00:0c:29:6d:11:9d
192.168.3.12             ether   00:0c:29:69:bd:2f
192.168.3.164            ether   00:0c:29:7f:2d:48
192.168.3.55             ether   00:0c:29:89:40:b1
192.168.3.168            ether   00:0c:29:fa:f1:84
192.168.3.1              ether   00:0c:29:84:68:bb
192.168.3.172            ether   00:0c:29:c1:1f:e6
192.168.3.18             ether   00:0c:29:97:65:07
192.168.3.9              ether   00:0c:29:7f:2d:48
192.168.3.13             ether   00:0c:29:0c:00:7b
192.168.3.152            ether   00:0c:29:94:6d:b3
```

Table ARP

ARP cache Poisoning

Principe :

- Le protocole ARP ne vérifie pas la provenance d'une réponse.
- Un attaquant envoie une réponse ARP en usurpant l'IP d'une machine du réseau.
- La machine envoie les paquets IP à la mauvaise machine..



DHCP & DNS Spoofing

Une machine prend en compte la 1ère réponse DNS ou DHCP

Un attaquant peut répondre avant le serveur

- Usurper l'identité d'une machine avec le DNS
- Se faire passer pour la gateway avec une réponse DHCP

MAC flooding

MAC flooding

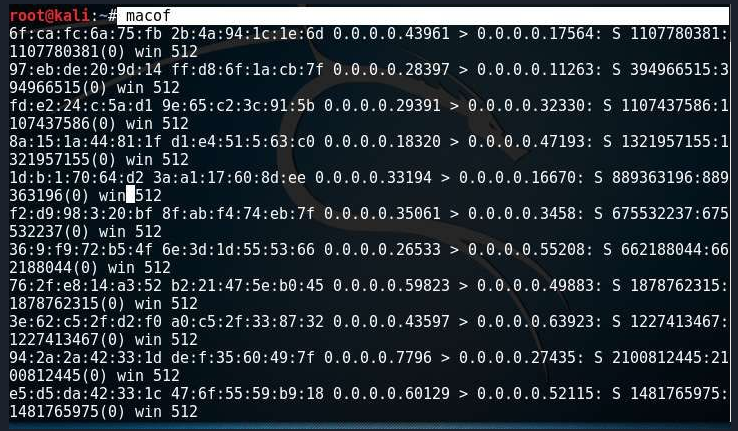
Envoyer un nombre important de réponses ARP à un Switch.

On sature le cache ARP du Switch.

Le Switch envoie alors le trafic sur tous les ports (mode Hub)

Outil d'attaque : `macof`

- remplit la table en moins de 1 minute



SSL Strip

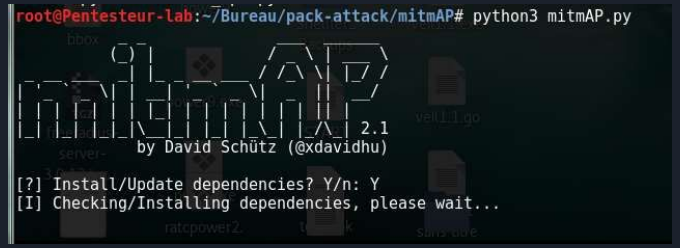
SSL Strip

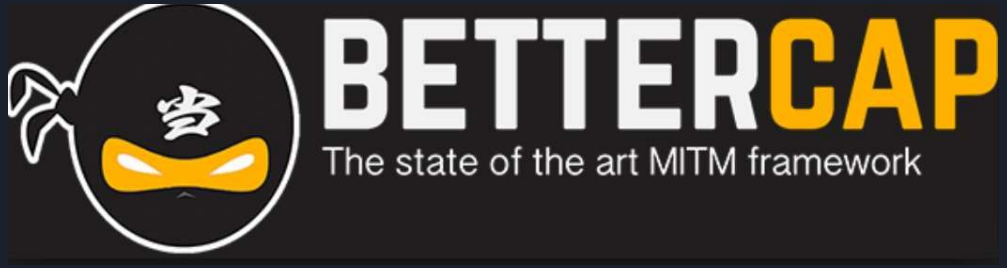
Les outils précédents permettent de capturer le trafic, mais pas lorsque celui-ci est chiffré

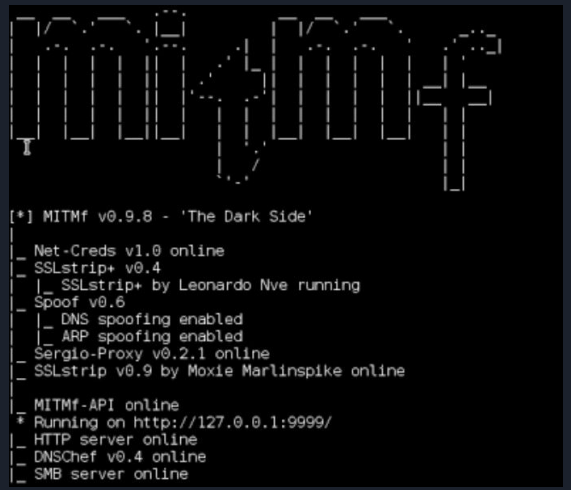
SSL strip permet de capturer le trafic HTTPS :

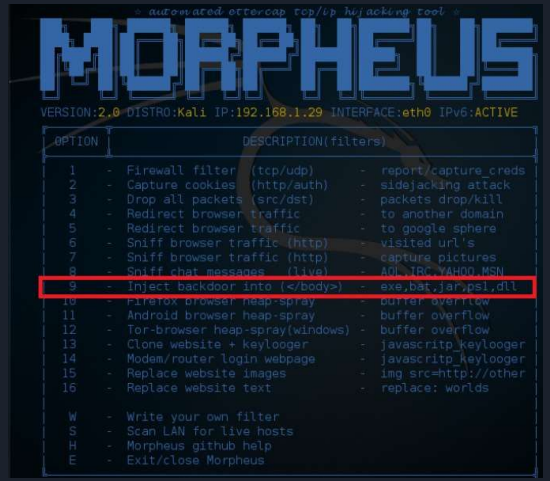
- Remplace tous les liens HTTPS par des liens HTTP
- Supprime tous cookie sécurisé qu'il voit dans le champ de la requête http
- Ajoute un icone cadenas

Automatisation MITM









Responder

LLMNR, NBT-NS, mDNS et WPAD poisoning

Si un nom DNS n'existe pas pas, Windows utilise les protocoles suivants :

- LLMNR
- NBT-NS
- mDNS

pour découvrir la machine sur le réseau local.

WPAD est utilisé pour découvrir des paramètres de proxy, sans configurer chaque navigateur.

Les messages sont envoyés en Broadcast. Responder va répondre à ces messages, et se faire passer pour le serveur distant.

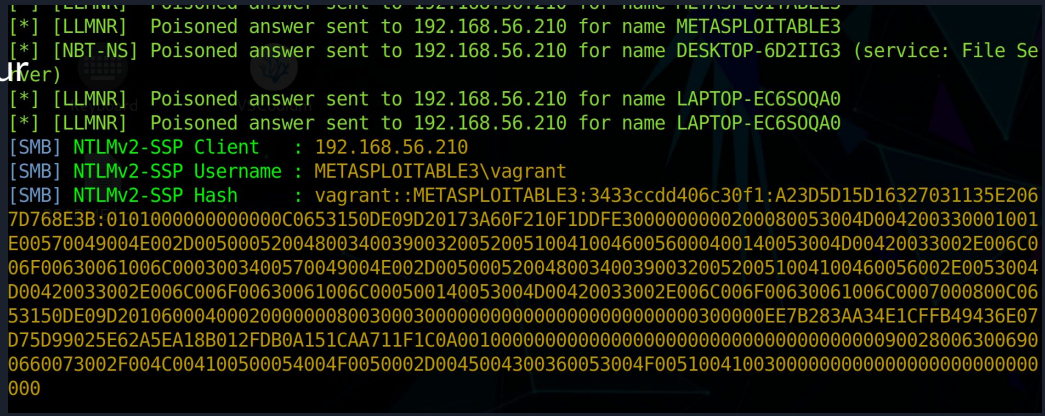
Responder

On récupère des hashs Net-NTLMv2 généralement. On peut

- Les cracker avec Hashcat
- Les utiliser pour s'authentifier sur d'autres machines (nécessite SMB signing désactivé)

Cette attaque nécessite soit :

- Une erreur de frappe d'un utilisateur
- Un script qui accède à un partage réseau inexistant
- Une erreur de configuration autorisant WPAD dans le navigateur.

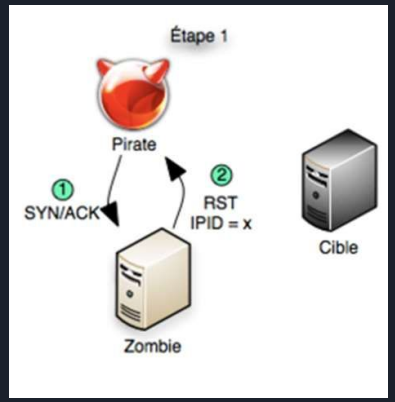


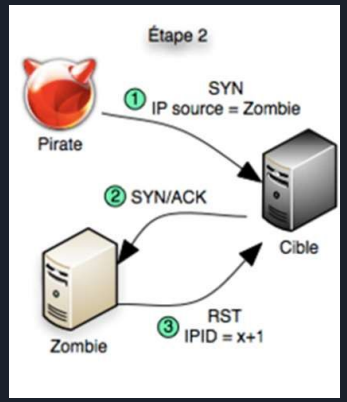
IDLE Scan

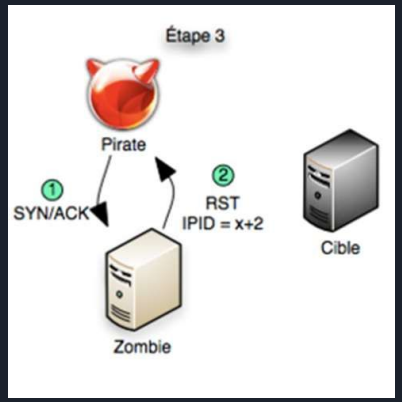
IDLE scan : Scan anonyme

Principe : créer un zombie pour scanner un autre hôte. La cible reçoit les paquets du zombie et pas de l'attaquant.

Se base sur des numéros d'identification IP prévisibles (IPID).







Trouver un zombie

Avec hping :

`hping3 -S -r <target IP>`

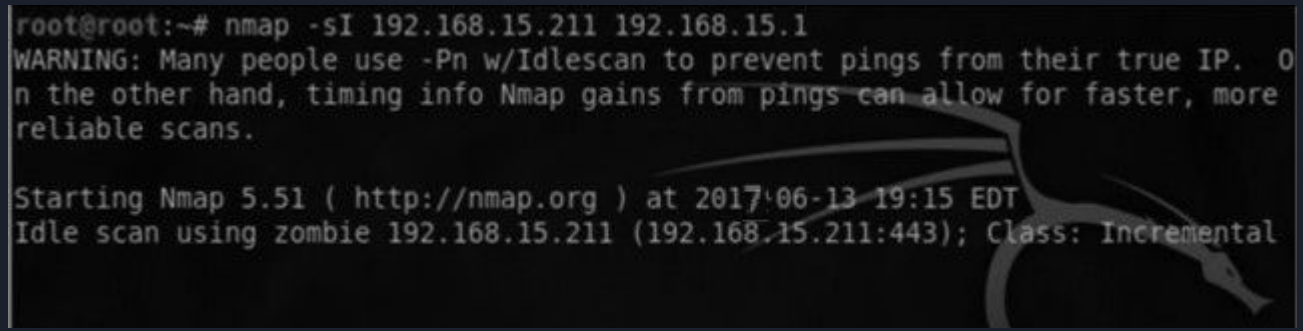
- S = envoi d'un drapeau SN
- r = id relatif

```
root@root:~# hping3 -S -r 192.168.15.211
HPING 192.168.15.211 (eth0 192.168.15.211): S set, 40 headers + 0 data bytes
len=46 ip=192.168.15.211 ttl=128 id=189 sport=0 flags=RA seq=0 win=0 rtt=0.8 ms
len=46 ip=192.168.15.211 ttl=128 id=+1 sport=0 flags=RA seq=1 win=0 rtt=0.9 ms
len=46 ip=192.168.15.211 ttl=128 id=+1 sport=0 flags=RA seq=2 win=0 rtt=0.8 ms
len=46 ip=192.168.15.211 ttl=128 id=+1 sport=0 flags=RA seq=3 win=0 rtt=0.6 ms
len=46 ip=192.168.15.211 ttl=128 id=+1 sport=0 flags=RA seq=4 win=0 rtt=0.6 ms
len=46 ip=192.168.15.211 ttl=128 id=+1 sport=0 flags=RA seq=5 win=0 rtt=0.7 ms
```

id incrémenté de 1 = bon candidat

Scan IDLE avec Nmap

```
$ nmap -sI <IP du zombie> <IP machine cible> -Pn
```



- `-sI` : machine cible
- `-Pn` : ne pas envoyer un paquet initial à la cible (ping)

Attaques Wifi

Monitor mode

La plupart des cartes ne supportent pas le mode monitor, et il est nécessaire d'utiliser un adaptateur.

Ce mode permet d’examiner tout le trafic, et pas seulement celui qui est destiné à notre machine.

802.11 désigne les normes Wifi

Vulnérabilités

- WEP : chiffrement faible, et facilement cassable (algorithme RC4)

PSK faible :

- Un attaquant peut capturer une session d'authentification, et casser le code wifi
- Fonctionne sur WPA et WPA2

WPS : génère un PIN pour se connecter au Wifi

- De nombreuses failles connues (Pixie Dust)
- Il est fortement recommandé de le désactiver.

Evil Twin

- Équivalent d’un Scam pour les réseaux Wifi
- Un attaquant créé un réseau se faisant passer pour le réseau Wifi légitime
- Il est alors en mesure d’effectuer un MITM

Mesure de sécurité à connaître

- Mac filtering : on accepte sur le réseau que les adresses MAC connues.
- Authentification RADIUS (802.1.X) : utiliser un serveur centralisé pour l'authentification
- Table ARP fixe : on attribue des IPs à certains MAC
- Créer une DMZ : les serveurs peuvent seulement recevoir des connexions, mais pas en initier.