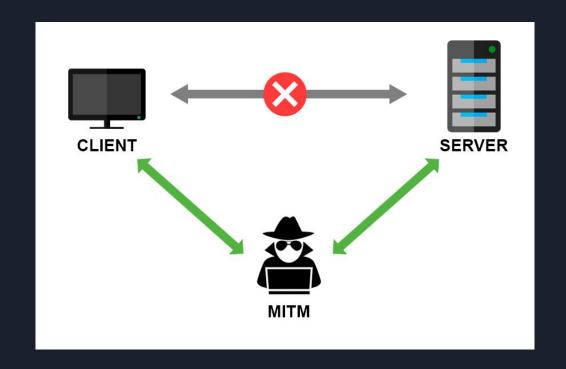
# Sécurité réseau et MITM

### 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

```
220 (vsFTPd 2.3.4)

USER admin

331 Please specify the password.

PASS SecretPassword!
```

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

```
Pootekali:~# macof

6f:ca:fc:6a:75:fb 2b:4a:94:lc:le:6d 0.0.0.0.43961 > 0.0.0.0.17564: S 1107780381:
1107780381(0) win 512

9f:eb:de:20:9d:14 ff:d8:6f:la:cb:7f 0.0.0.0.28397 > 0.0.0.0.11263: S 394966515:3

94966515(0) win 512

6d:e2:24:c:5a:d1 9e:65:c2:3c:91:5b 0.0.0.0.29391 > 0.0.0.0.32330: S 1107437586:1

107437586(0) win 512

8a:15:la:44:81:lf d1:e4:51:5:63:c0 0.0.0.0.18320 > 0.0.0.0.47193: S 1321957155:1

321957155(0) win 512

1d:b:1:764:d2 3a:al:17:60:8d:ee 0.0.0.33194 > 0.0.0.0.16670: S 889363196:889

363196(0) win 512

1d:b:1:760:4d:2 3a:al:47:66:8d:ee 0.0.0.35061 > 0.0.0.3458: S 675532237:675

532237(0) win 512

36:9:f9:72:b5:4f 6e:3d:ld:55:53:66 0.0.0.0.26533 > 0.0.0.0.55208: S 662188044:66

2188044(0) win 512

76:2f:e8:14:a3:52 b2:21:47:5e:b0:45 0.0.0.59823 > 0.0.0.0.49883: S 1878762315:

1878762315(0) win 512

3e:62:c5:2f:d2:f0 a0:c5:2f:33:87:32 0.0.0.0.43597 > 0.0.0.6.63923: S 1227413467:

1227413467(0) win 512

94:22:22:42:33:1d de:f:35:60:49:7f 0.0.0.0.7796 > 0.0.0.0.27435: S 2100812445:21

00812445(0) win 512

94:22:24:42:33:1c 47:6f:55:59:b9:18 0.0.0.60129 > 0.0.0.0.52115: S 1481765975:

1481765975(0) win 512
```

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.

```
$sudo responder -I eth1
           NBT-NS, LLMNR & MDNS Responder 3.0.2.0
 Author: Laurent Gaffie (laurent.gaffie@gmail.com)
 To kill this script hit CTRL-C
[+] Poisoners:
   LLMNR
   NBT-NS
                                 [ON]
                                 [ON]
   DNS/MDNS
[+] Servers:
   HTTP server
                                 [ON]
   HTTPS server
                                 [ON]
   WPAD proxy
   Auth proxy
   SMR server
                                 [ ON ]
                                 [ON]
   Kerberos server
                                 [ON]
   FTP server
                                 [ON]
                                 [ON]
   IMAP server
   POP3 server
                                 [ ON ]
                                 [ON]
   SMTP server
   DNS server
                                 [ ON ]
                                 [ON]
   LDAP server
   RDP server
                                 [ ON ]
```

### 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 :

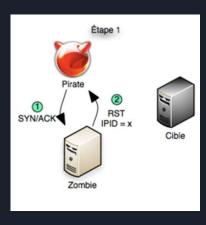
- Une erreur de frappe d'un utilisateurer
- Un script qui accède à un partage réseau inexistant
- Une erreur de configuration autorisant WPAD dans le navigateur.

# IDLE Scan

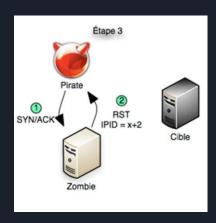
## IDLE scan: Scan anonyme

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

```
root@root:~# nmap -sI 192.168.15.211 192.168.15.1
WARNING: Many people use -Pn w/Idlescan to prevent pings from their true IP. O
n the other hand, timing info Nmap gains from pings can allow for faster, more
reliable scans.

Starting Nmap 5.51 ( http://nmap.org ) at 2017.06-13 19:15 EDT
Idle scan using zombie 192.168.15.211 (192.168.15.211:443); Class: Incremental
```

- -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.