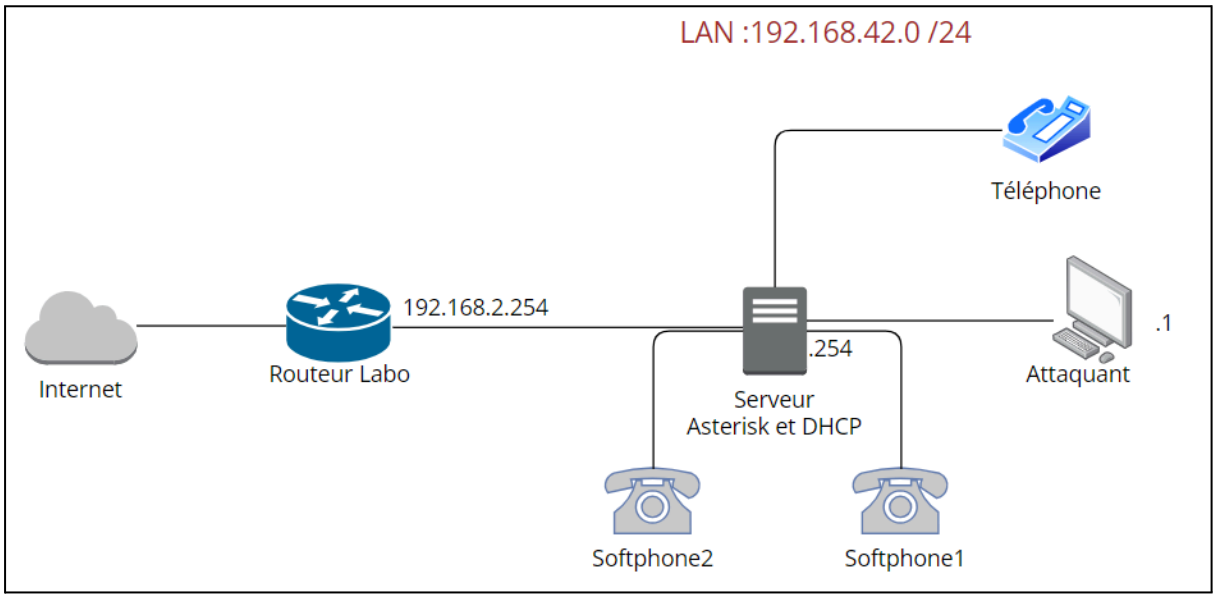
MITM VoIP

L'attaque Man In The Middle (MITM) sur une infrastructure VoIP consiste à intercepter les communications entre deux parties en manipulant les caches ARP pour rediriger le trafic à travers une machine attaquante. Voici les étapes et le fonctionnement détaillés dans le contexte des exercices liés à la téléphonie IP avec Asterisk.

Infrastructure réseau :

Schéma réseau :



Configuration :

Appareil	*Adresse IP*
Routeur Labo	192.168.2.254 /24
Serveur Asterisk et DHCP	192.168.42.254 /24
Attaquant	192.168.42.10 /24
Softphone1	Attribué par le DHCP
Softphone2	Attribué par le DHCP
Téléphone	Attribué par le DHCP

Mise en place du Serveur Asterisk:

Le serveur Asterisk joue un rôle central dans une infrastructure de téléphonie IP. Il agit comme un PBX IP (Private Branch Exchange), permettant aux téléphones connectés sur le même réseau IP de communiquer entre eux de manière audio et d'accéder à des fonctionnalités avancées.

Configuration du Serveur Asterisk :

La configuration du Serveur, se fait en partie grâce a 3 fichiers de configurations, situés dans **/etc/asterisk/** après l'installation du paquet, qui sont **users.conf**, **voicemail.conf**, et **extensions.conf**

On commence par la configuration du fichier : **users.conf qui permet de configurer chaque utilisateur** en mettant, le nom complet, le pseudo, le mot de passe, et à quel contexte il appartient.
Pour notre cas nous avons mis en place 2 contextes différents : **finance** et **compta**, pour lesquelles nous avons configuré 2 utilisateurs à chaque fois.

Ensuite, nous avons modifié le fichier de configuration **voicemail.conf** qui nous **permet de configurer la boîte vocale** en attribuant un numéro de boîte vocale à chaque utilisateur ou contexte.

Enfin nous avons modifié le fichier **extensions.conf**, afin de **permettre les appels entre utilisateurs ou contextes**. C'est ce fichier qui permet aussi de rediriger vers la boîte vocale si l'utilisateur appelé était injoignable.

Tests :

Après toutes ces configurations nous nous sommes assurés que tous les utilisateurs partageant un même contexte, pouvaient communiquer, à l'aide de l'outil Ekiga nous permettant de créer les comptes SIP sur les softphones et donc de passer des appels.
Puis nous avons fait de même pour vérifier que les utilisateurs pouvaient communiquer entre eux depuis un contexte différent

Mise en place de l'attaque MITM :

Ajout d'un poste filaire :

Avant de procéder à l'attaque nous avons installé un poste téléphonique filaire sur le réseau afin tout d'abord de tester la communication entre softphones et poste filaire.

Une fois le poste sur le réseau, nous procédons à une réinitialisation usine sur celui-ci, qui récupère après s'être allumé, une adresse IP lui est attribuée par le DHCP du serveur asterisk..

Nous entamons la partie configuration de celui- ci afin de le mettre en lien avec le serveur Asterisk, depuis son interface graphique (connexion en temps qu'utilisateurs …).

Puis vient une phase de tests entre le Téléphone filaire et les Softphones, afin d'observer si la connexion a bien été prise en compte (appels téléphoniques).

Début de l'Attaque :

L'objectif principal est de faire transiter les flux entre le serveur Asterisk et les téléphones via le poste attaquant afin de capturer et lire les communications. Cela est réalisé en empoisonnant le cache ARP des cibles (le serveur et les téléphones) afin de rediriger les paquets réseau.

Nous activons pour commencer la fonction de routage sur le poste attaquant, puis nous **commençons l'empoisonnement grâce** à la **commande arpspoof -t** en **ciblant les postes softphone1 et le serveur**.

Une **différence** est **remarquée sur la table arp des deux postes ciblés**, qui lorsqu'ils affichent **voient une adresse MAC différente** (celle de l'attaquante) liée aux adresses IP respectives du Serveur et du Softphone1.

Avec l'outil Wireshark, nous avons pu capturer les trames SIP et RTP provenant de l'appel effectué entre le Téléphone filaire et le Softphone1, afin de lire (écouter) la communication passée. Pour cela on se rend dans le menu Téléphonie puis appels VOIP.

Problèmes rencontrés :

Le signal audio capturé par le logiciel reste muet malgré plusieurs tests.