VOIP - MISE EN PLACE D'UNE ATTAQUE DE TYPE EAVESDROPPING

Contexte

La solution proposée au directeur commercial par l'équipe des services d'information de SCIS convient parfaitement aux besoins de l'équipe commerciale. Cependant, la direction commerciale s'interroge sur la sécurité d'une telle solution. Votre responsable vous charge de simuler une attaque de type eavesdropping sur la solution IPBX Asterisk mise en place précédemment.
Le but d'une telle simulation est de mettre en lumière les problèmes de sécurité liés à l'utilisation d'une plateforme IPBX.

Préparation de la plateforme de test

Pour la réalisation de cette simulation d'attaque, vous utiliserez une nouvelle machine cliente « pirate » fournie : « `CLT-Debian.ova` »

Cette machine s'ajoutera à votre maquette existante de la solution Asterisk.

Les identifiants de cette machine : `root:1234 / test:1234`

Travail à faire

À l'aide de l'annexe fournie, vous devez réaliser l'ensemble des travaux. Vous prendrez note au fur et à mesure de votre avancement. Lors de chaque étape, vous devez indiquer les commandes utilisées vous permettant de tester vos configurations.

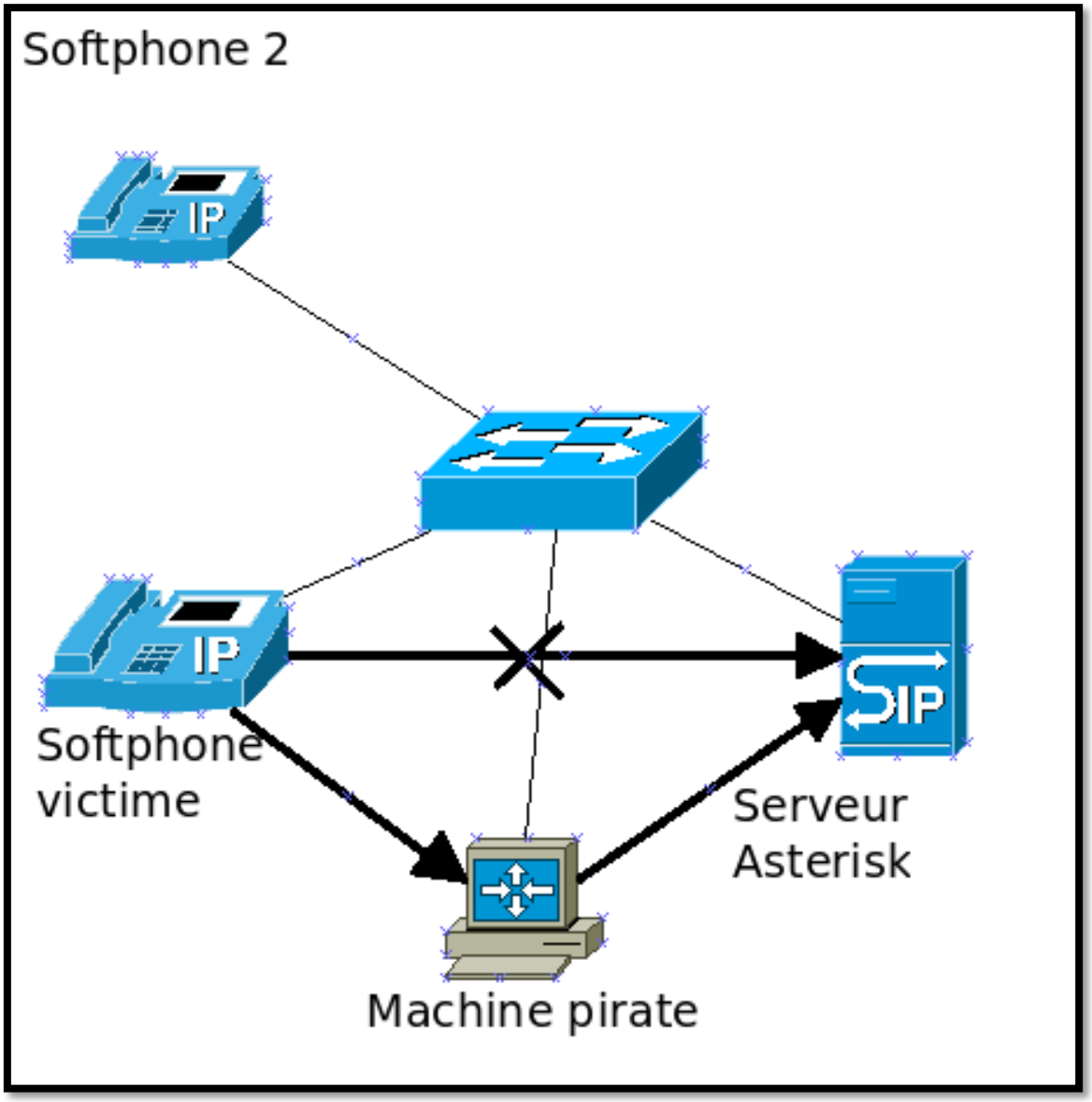
1. Pré-requis

a) Vérifiez le bon fonctionnement de votre solution Asterisk, Mike, John et Fred peuvent t'ils se contacter et laisser des messages vocaux ?

b) Préparez la machine attaquante en installant les paquets `wireshark` et `dsniff`. Configurez ensuite l'interface réseau et testez la connectivité avec le serveur Asterisk (ping).

2. Ecoute clandestine

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 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.



Dans les pages suivantes, les machines ont pour IP :

- Machine pirate : 192.168.0.100
- Softphone victime : 192.168.0.201
- Softphone 2 : 192.168.0.202
- Serveur Asterisk : 192.168.0.1

Vous adapterez l'adressage en fonction de votre maquette.

Q2.1. Commencez par reporter sur votre documentation les caches ARP de la machine victime et du serveur Asterisk. Utilisez les tableaux suivants.

Machine pirate :

CONFIGURATION DE LA CARTE RÉSEAU DE LA MACHINE PIRATE	
ADRESSE IP	**ADRESSE MAC**
192.168.0.100	

Victime (softphone d'adresse 192.168.0.201) :

CACHE ARP DE LA VICTIME	
ADRESSE IP	**ADRESSE MAC**
192.168.0.1	

Serveur Asterisk (192.168.0.1) :

CACHE ARP DU SERVEUR	
ADRESSE IP	**ADRESSE MAC**
192.168.0.201	

Q2.2. Utilisez l'outil **arpspoof** afin de positionner la machine attaquante entre le softphone d'adresse 192.168.0.201 et le serveur Asterisk.

Q2.3. Reportez les caches ARP de la machine victime (192.168.0.201) et du serveur Asterisk. Utiliser les deux tableaux suivants.

Victime (softphone d'adresse 192.168.0.201) :

CACHE ARP DE LA VICTIME	
ADRESSE IP	**ADRESSE MAC**
192.168.0.1	

Serveur Asterisk (192.168.0.1) :

CACHE ARP DU SERVEUR	
ADRESSE IP	**ADRESSE MAC**
192.168.0.201	

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

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

Q2.5. Utilisez le softphone de la victime afin de déposer un message vocal à destination du softphone d'adresse IP 192.168.0.202

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

Mettez fin à l'attaque et relevez les caches ARP de la victime et du serveur. Expliquez les changements observés.