VOIP – Sécurisation d'une infrastructure de téléphonie IP avec Asterisk

Contexte

L'attaque de type eavesdropping réalisée précédemment a mis en lumière le manque de sécurité de la solution proposée initialement.
Vous êtes dorénavant chargé de proposer des contre-mesures avec chiffrement des échanges, évitant ainsi les attaques de type eavesdropping.

Préparation de la plateforme de test

Pour la réalisation de cette simulation d'attaque, vous utiliserez votre machine cliente « pirate » créée lors du TP14.

Vous aurez besoin de deux machines clientes équipées des softphones « Blink ».

Le reste de la plateforme reste inchangée.

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. Préparation des machines et installation de Blink

Dans cette première partie, vous devez commencer par installer et configurer le softphone Blink sur deux machines clientes. Vous devrez utiliser des postes clients sous Windows 10 ou sous Debian/Ubuntu avec environnement de bureau.

a) Installer le logiciel softphone sur chaque poste client.

b) **Ne pas créer de compte** sur ces softphones, vous effectuerez cette démarche dans un second temps.

2. Configuration du serveur Asterisk

Dans cette deuxième partie, vous devez configurer votre serveur Asterisk pour mettre en place le chiffrement avec TLS, ce chiffrement concerne l'intégralité de vos comptes utilisateurs présents sur votre plateforme.

a) Dans le fichier de configuration `sip.conf`, ajoutez les lignes « `transport` » et « `encryption` » pour chaque utilisateur, tel que décrit dans l'annexe.
b) A l'aide de l'annexe, créez sur votre serveur les certificats nécessaires (CA, serveur, et pour les deux softphones).
c) Installez le paquet `srtp-utils` sur votre serveur. Rechargez la configuration d'Asterisk puis vérifiez que le module `res_srtp.so` est chargé en utilisant la commande `module show like srtp` dans la console Asterisk.
d) Modifiez le fichier `sip.conf` afin de configurer le chiffrement avec TLS sur le serveur. Pour cela, considérez l'exemple de configuration fourni dans l'annexe. Rechargez la configuration d'Asterisk afin de prendre en considération les modifications apportées.

3. Configuration des comptes TLS sur les softphones Blink

a) A l'aide de l'annexe, configurez vos comptes Blink associés aux utilisateurs de votre plateforme. Ces comptes doivent permettre le chiffrement du flux de signalisation et du transport de la voix. Vérifiez leur enregistrement sur le serveur à l'aide de la commande `sip show peers` dans la console. Vous attendrez dans la console l'affichage du message confirmant l'acceptation des certificats (`SSL CERTIFICATE OK`).
   Remarque : pour transférer les certificats depuis le serveur vers les postes clients, vous pouvez utiliser un client SSH/SFTP sur un poste client, puis transférer les certificats aux machines virtuelles concernées.
b) Vérifiez que le mode de transport des comptes configurés est TLS à l'aide de la commande de console `sip show tcp`.

4. Premiers appels et capture de trames

a) Installez le logiciel `Wireshark` sur la machine associée au softphone du premier utilisateur.
b) Testez un appel entre les deux softphones et capturez les trames de signalisation associées aux échanges à l'aide du filtre Wireshark `tcp.port == 5061`.

5. Positionnement MITM (Man In The Middle)

Dans cette partie, vous devez configurer la machine pirate afin de tenter la capture d'un message déposé sur une boîte vocale.

a) Démarrez la machine pirate puis lancer Wireshark sans configurer de filtre.
b) Relevez les caches ARP du softphone du premier utilisateur et du serveur Asterisk.
c) Configurez un empoisonnement de cache ARP entre le softphone du premier du premier utilisateur et le serveur Asterisk.
d) Vérifiez le succès de l'empoisonnement en relevant à nouveau le contenu des caches ARP.
e) Utilisez le softphone du premier utilisateur afin de déposer un message sur la boîte vocale du second utilisateur.
f) Sur le Wireshark de la machine pirate, constatez l'échec de la capture du message vocal.