Commandes préalables:

openssl req -new -sha256 -nodes -newkey rsa:4096 -keyout lxle.key -out lxle.csr

openssl x509 -signkey lxle.key -in lxle.csr -req -days 365 -out lxle.crt

sudo ufw allow http

sudo ufw allow https

La page web est bien accessible depuis la machine hôte :

Une image contenant texte

Description générée automatiquement

En faisant une interception ARP-poisoning, il est possible d’intercepter le login et le mot de passe envoyés par le formulaire http simple :

Une image contenant texte

Description générée automatiquement

Pour empêcher la connexion non sécurisée de s’établir, il faut que le virtualhost qui écoute sur le port 80 n’ait pour seule utilité que de rediriger le navigateur vers la connexion HTTPS. On peut assi activer HSTS (HyperText Strict Transport Secure).

Client : 192.168.5.1, server : 192.168.5.128, pirate : 192.168.5.129.

Lorsque l’attaque MITM n’est pas active, la table ARP du client correspond bien aux adresses physiques des machines.

Une image contenant texte

Description générée automatiquement

Il est en de même pour le serveur :

Une image contenant texte

Description générée automatiquement

Lorsque l’attaque MITM est active, le client croit que l’adresse MAC du serveur est celle du pirate

Une image contenant texte

Description générée automatiquement

Et le serveur croit que l’adresse MAC du client est celle du pirate :



Afin de procéder à une attaque MITM sur une connexion SSL, il est nécessaire d’activer les redirections iptables dans le fichier */etc/ettercap/etter.conf*.

Cette configuration faisant planter l’interface graphique d’ettercap, il est nécessaire d’utiliser la version en ligne de commande :

*sudo ettercap -T -q -M arp:remote /192.168.5.1// /192.168.5.128// -w result*

Il est nécessaire d’accepter le nouveau certificat dans le navigateur, puisque ce dernier a changé. C’est le certificat d’ettercap (les empreintes sont différentes) :

|  |  |
| --- | --- |
| Certificat avant l’attaque | Certificat pendant l’attaque |
|  | Une image contenant texte  Description générée automatiquement |

Les identifiants sont bien interceptés.

