LAB 2 Cyber

U7 CYBER

SPINELLI Dylan
BTS SIO SISR | PARIS YNOV CAMPUS

Table des matières

1-Introduction

Attaque Man in the middle

Un serveur et un client communiquent grâce à un gateway

L'attaquant va se faire passer pour le gateway et recevoir toutes les informations du client et du serveur

Usurpation ARP : une requête ARP sera envoyée pour chercher l'adresse IP du gateway, et l'attaquant va répondre pour se faire identifier comme étant le gateway

Le switch va enregistrer dans sa table l'adresse MAC de l'attaquant et lui envoyer toutes les communications

2-Empoisonnement du cache ARP avec ARPspoof

Voici les machines utilisées pour ce TP :

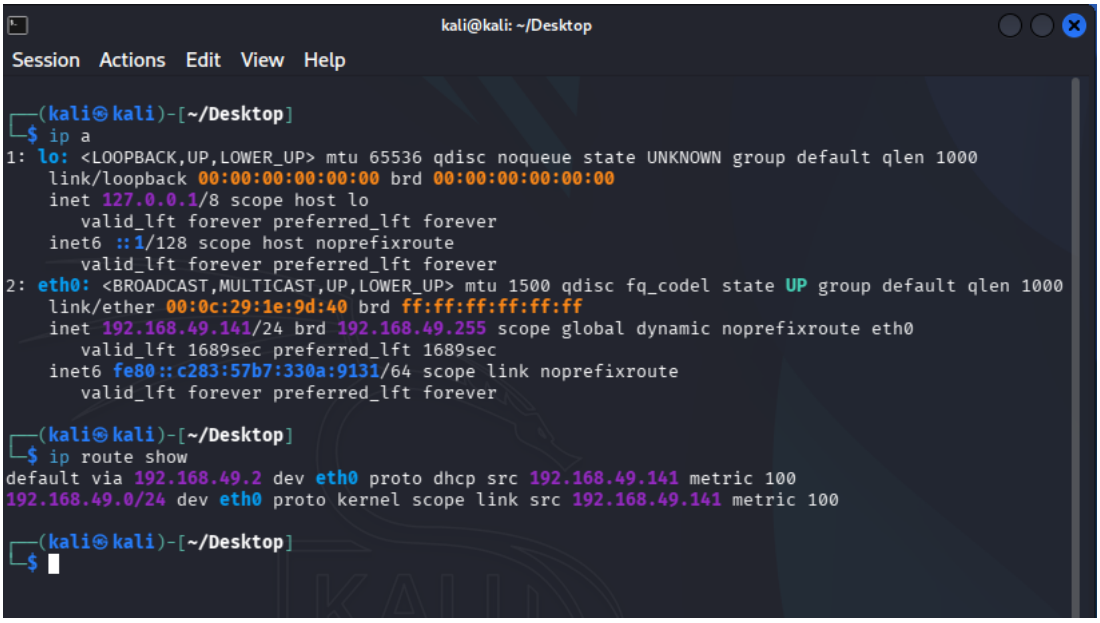
Machine	Adresse IP	Gateway
Kali	192.168.49.141/24	192.168.49.2
Client Linux	192.168.49.135/24	192.168.49.2
Serveur Linux	192.168.49.142/24	192.168.49.2

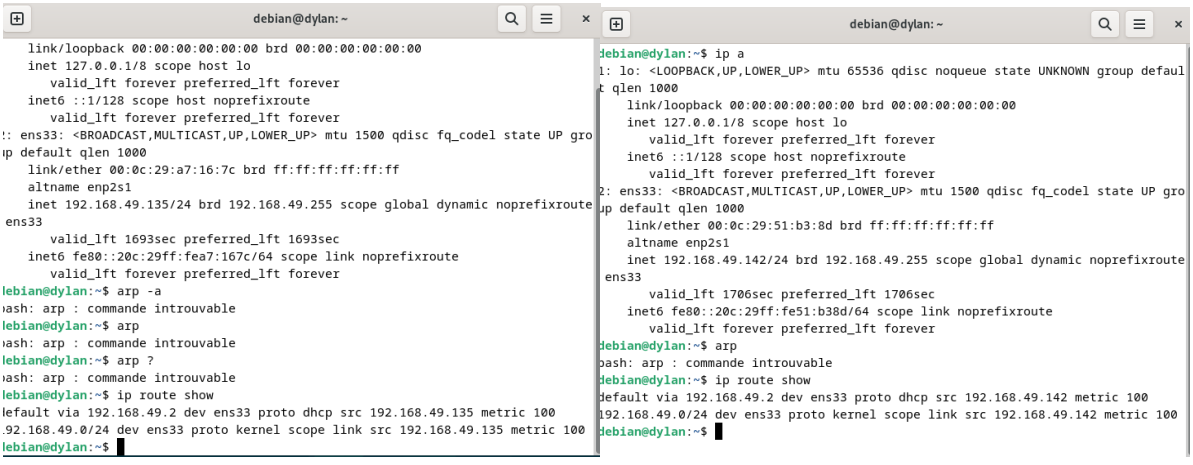
Dans le sujet :

.10 client

.20 kali

.254 Gateway





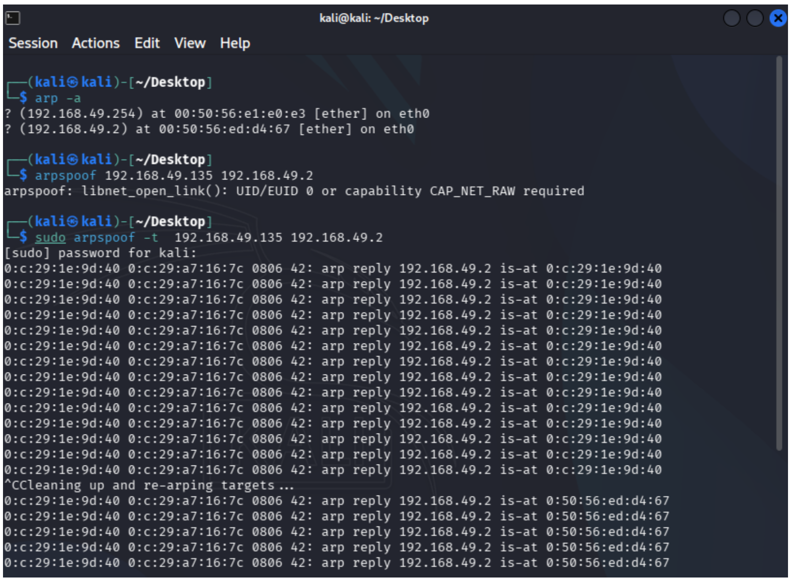
On vérifie l’état du cache ARP :

On reconnait notamment l’adresse IP du gateway (192.168.49.2) ainsi que son adresse MAC

00:50:56:ed:d4:67

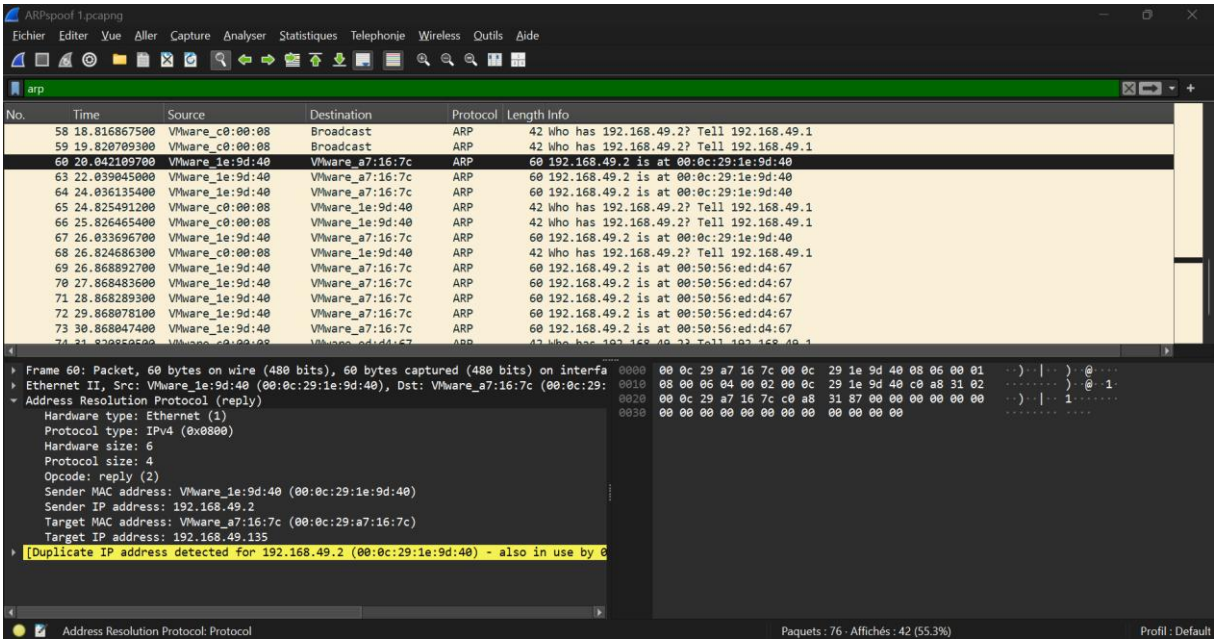
On utilise la commande Arpspoof afin de modifier l’adresse MAC du Gateway

On dit au client que c’est kali le Gateway :

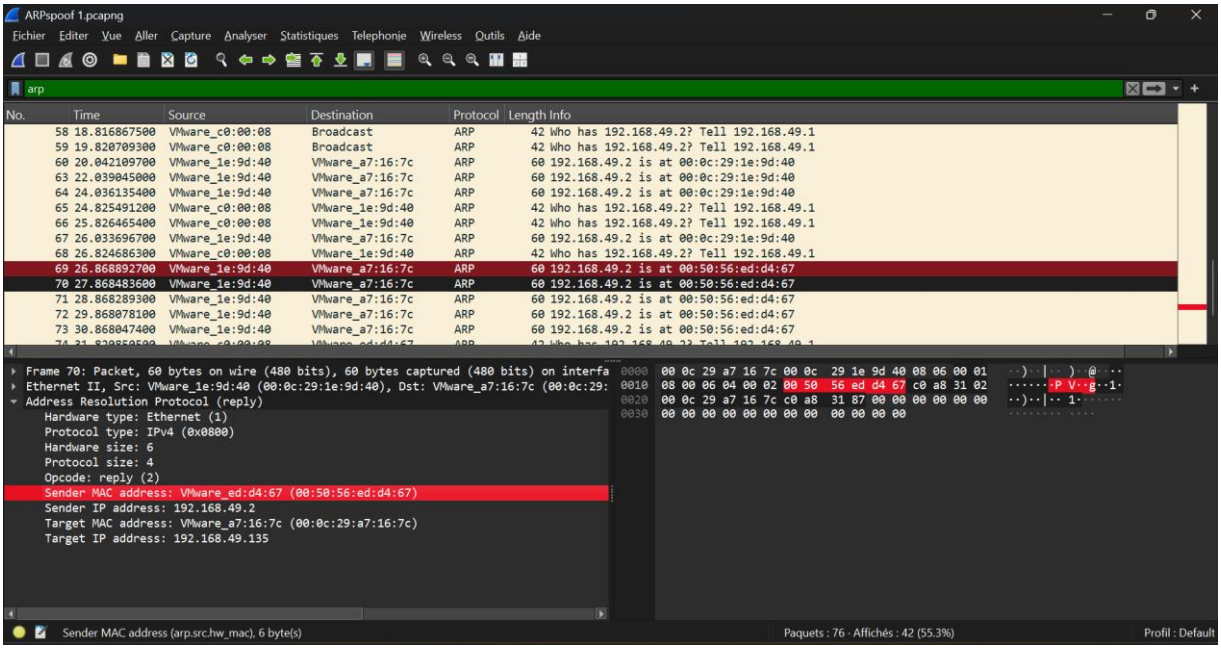


Analysons le trafic sur wireshark

On voit que lors des premiers échanges, l'adresse MAC du gateway 192.168.49.2 est 00:0c:29:1e:9d:40



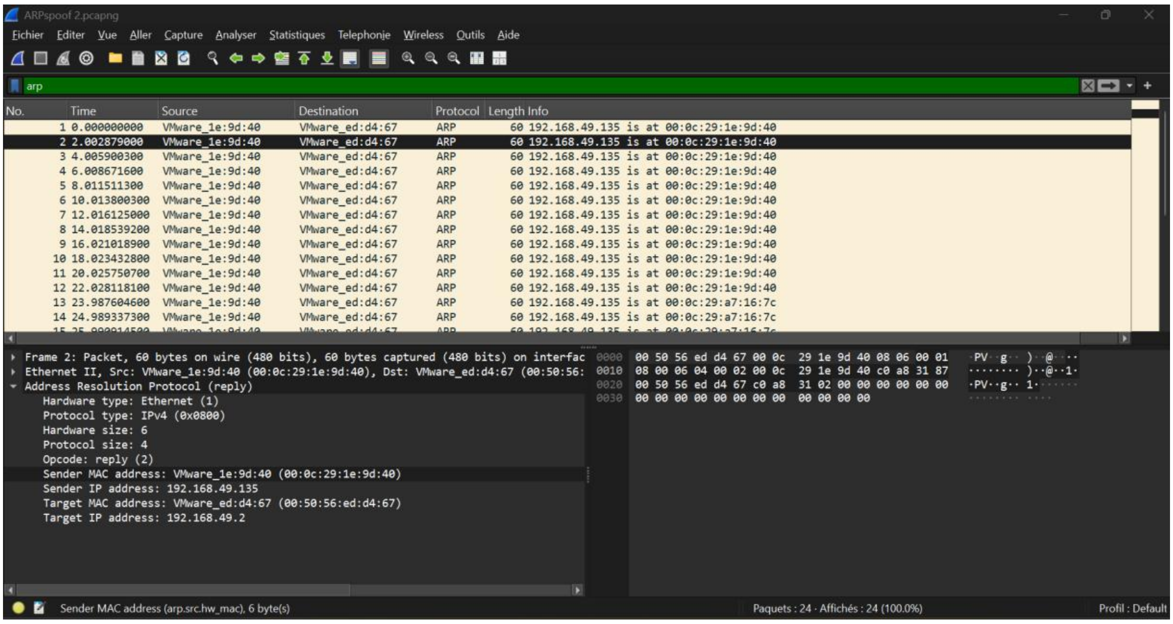
Puis ensuite, une fois l'usurpation ARP effectuée, l'adresse MAC correspondant au gateway est désormais 00:50:56:ed:d4:67



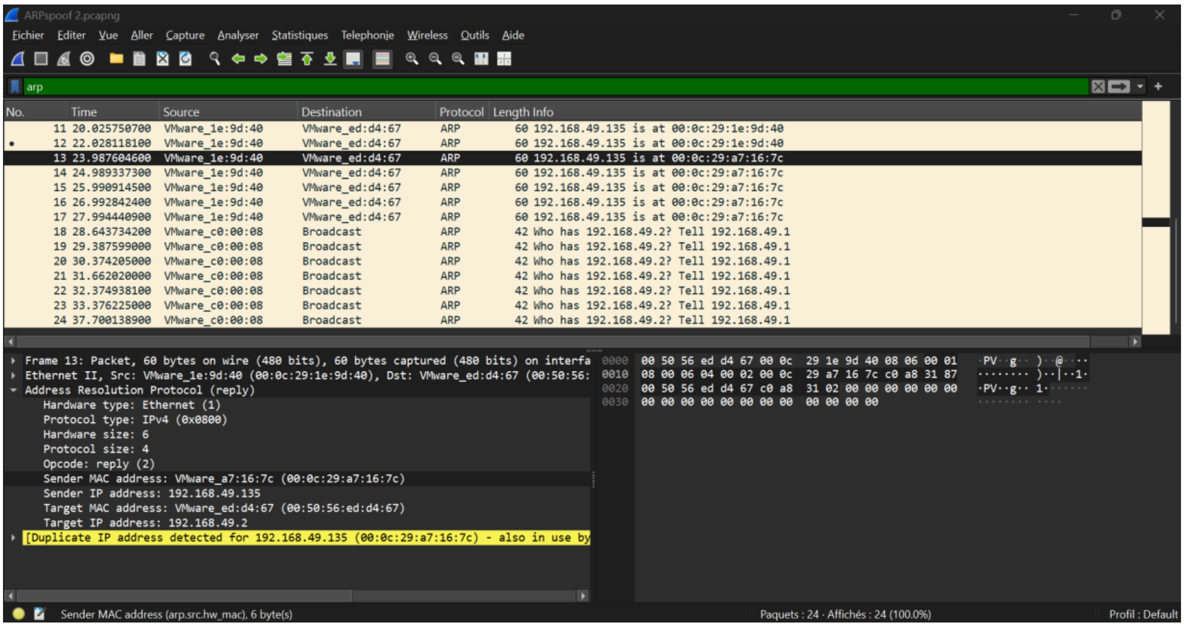
Maintenant nous allons dire au Gateway que c'est kali le client :

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo arpspoof -t  192.168.49.2 192.168.49.135
0:c:29:1e:9d:40 0:50:56:ed:d4:67 0806 42: arp reply 192.168.49.135 is-at 0:c:29:1e:9d:40
0:c:29:1e:9d:40 0:50:56:ed:d4:67 0806 42: arp reply 192.168.49.135 is-at 0:c:29:1e:9d:40
0:c:29:1e:9d:40 0:50:56:ed:d4:67 0806 42: arp reply 192.168.49.135 is-at 0:c:29:1e:9d:40
0:c:29:1e:9d:40 0:50:56:ed:d4:67 0806 42: arp reply 192.168.49.135 is-at 0:c:29:1e:9d:40
0:c:29:1e:9d:40 0:50:56:ed:d4:67 0806 42: arp reply 192.168.49.135 is-at 0:c:29:1e:9d:40
0:c:29:1e:9d:40 0:50:56:ed:d4:67 0806 42: arp reply 192.168.49.135 is-at 0:c:29:1e:9d:40
0:c:29:1e:9d:40 0:50:56:ed:d4:67 0806 42: arp reply 192.168.49.135 is-at 0:c:29:1e:9d:40
0:c:29:1e:9d:40 0:50:56:ed:d4:67 0806 42: arp reply 192.168.49.135 is-at 0:c:29:1e:9d:40
0:c:29:1e:9d:40 0:50:56:ed:d4:67 0806 42: arp reply 192.168.49.135 is-at 0:c:29:1e:9d:40
0:c:29:1e:9d:40 0:50:56:ed:d4:67 0806 42: arp reply 192.168.49.135 is-at 0:c:29:1e:9d:40
^CCleaning up and re-arping targets...
0:c:29:1e:9d:40 0:50:56:ed:d4:67 0806 42: arp reply 192.168.49.135 is-at 0:c:29:a7:16:7c
0:c:29:1e:9d:40 0:50:56:ed:d4:67 0806 42: arp reply 192.168.49.135 is-at 0:c:29:a7:16:7c
0:c:29:1e:9d:40 0:50:56:ed:d4:67 0806 42: arp reply 192.168.49.135 is-at 0:c:29:a7:16:7c
0:c:29:1e:9d:40 0:50:56:ed:d4:67 0806 42: arp reply 192.168.49.135 is-at 0:c:29:a7:16:7c
0:c:29:1e:9d:40 0:50:56:ed:d4:67 0806 42: arp reply 192.168.49.135 is-at 0:c:29:a7:16:7c
```

Dans Wireshark, on voit au début que l'adresse MAC du client 192.168.49.135 est 00:0c:29:1e:9d:40



Ensuite, on voit le changement d'adresse MAC qui devient 00:0c:29:a7:16:7c



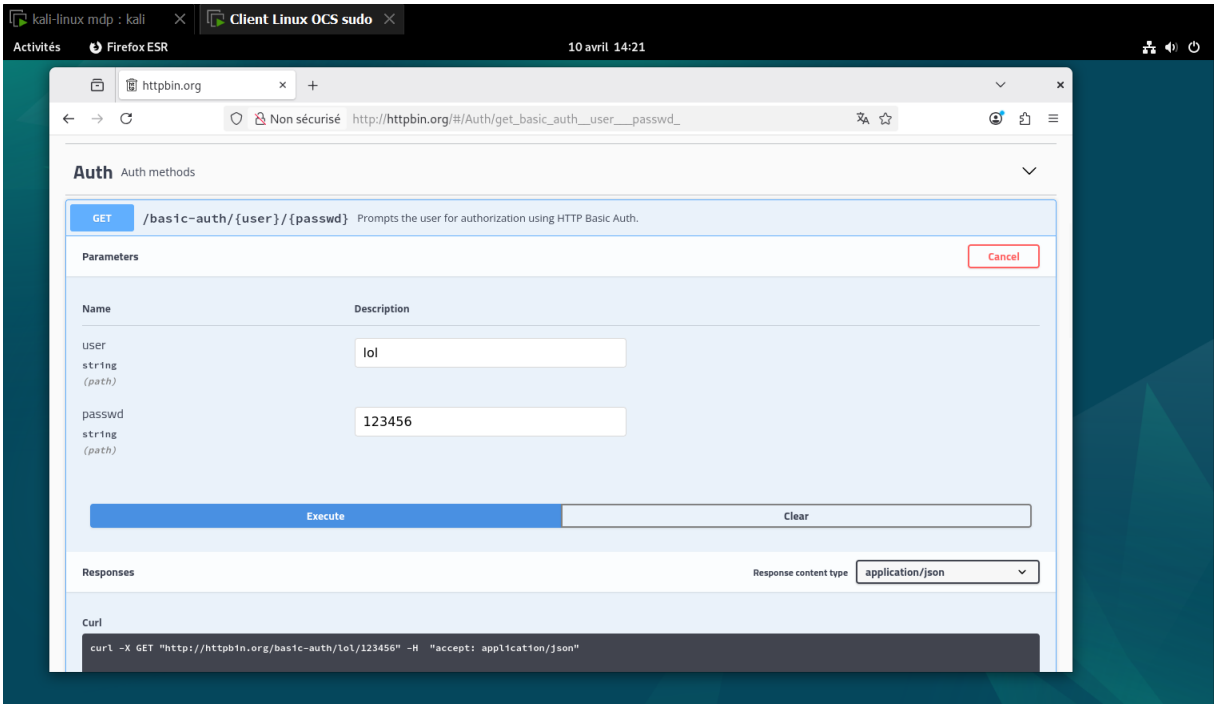
Dans ce TP, les adresses MAC sont renseignées de manière aléatoire. Dans un cas concret, c'est l'adresse MAC de l'attaquant qui serait renseignée à la place de l'adresse MAC de départ. De plus, chaque adresse MAC est unique et il est impossible d'avoir 2 adresses MAC identique dans un réseau. L'attaquant devra donc d'abord modifier l'adresse MAC du client puis remonter ensuite au serveur pour finir par le Gateway.

Le Gateway est la cible finale car tout le trafic sur le réseau passe par le Gateway.

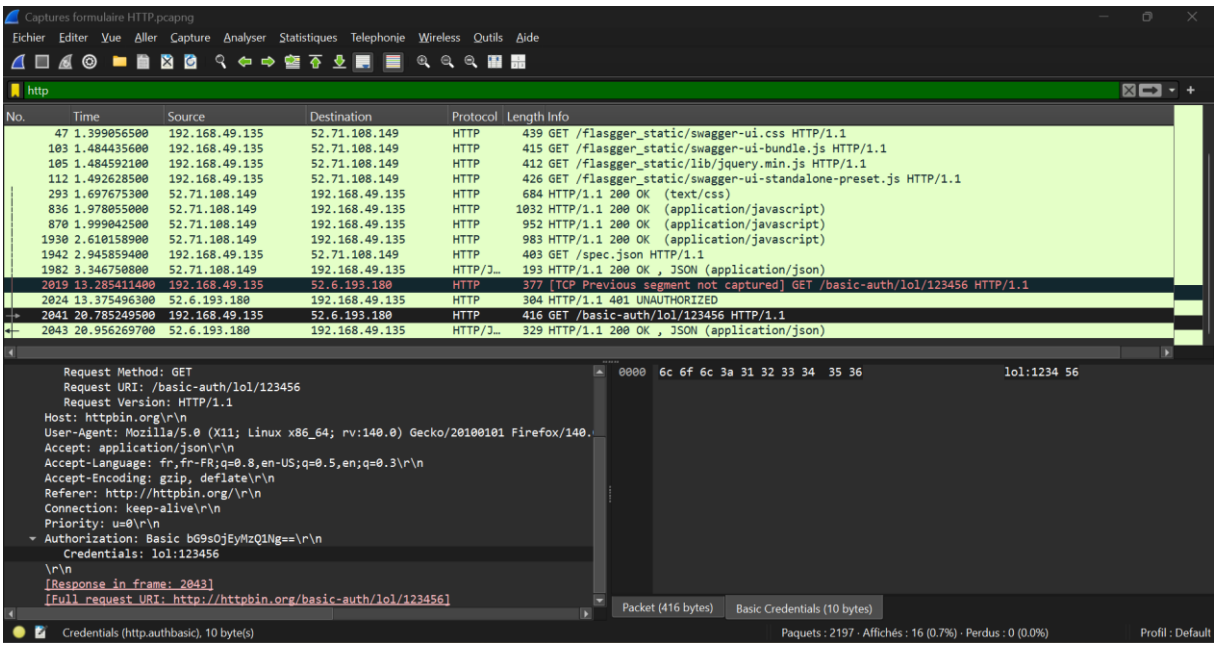
3-Capture de trafic http

On cherche à trouver les informations de connexion d'un formulaire http

Pour cela nous allons nous connecter à un site web vulnérable http://httpbin.org/



Analysons ensuite le trafic http pour voir si on retrouve bien nos logins :

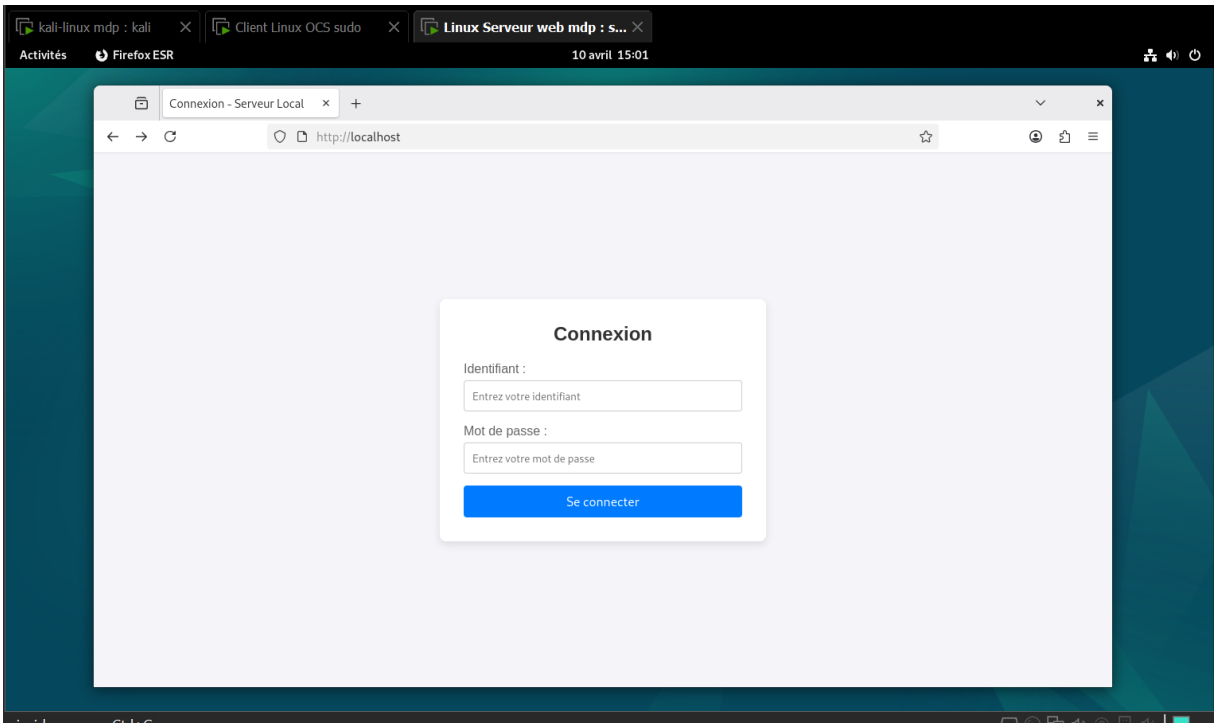


Les logins apparaissent bien en clair dans le trafic. Le protocole http n'est pas sécurisé. Il faut utiliser HTTPS afin que ces informations soient chiffrées.

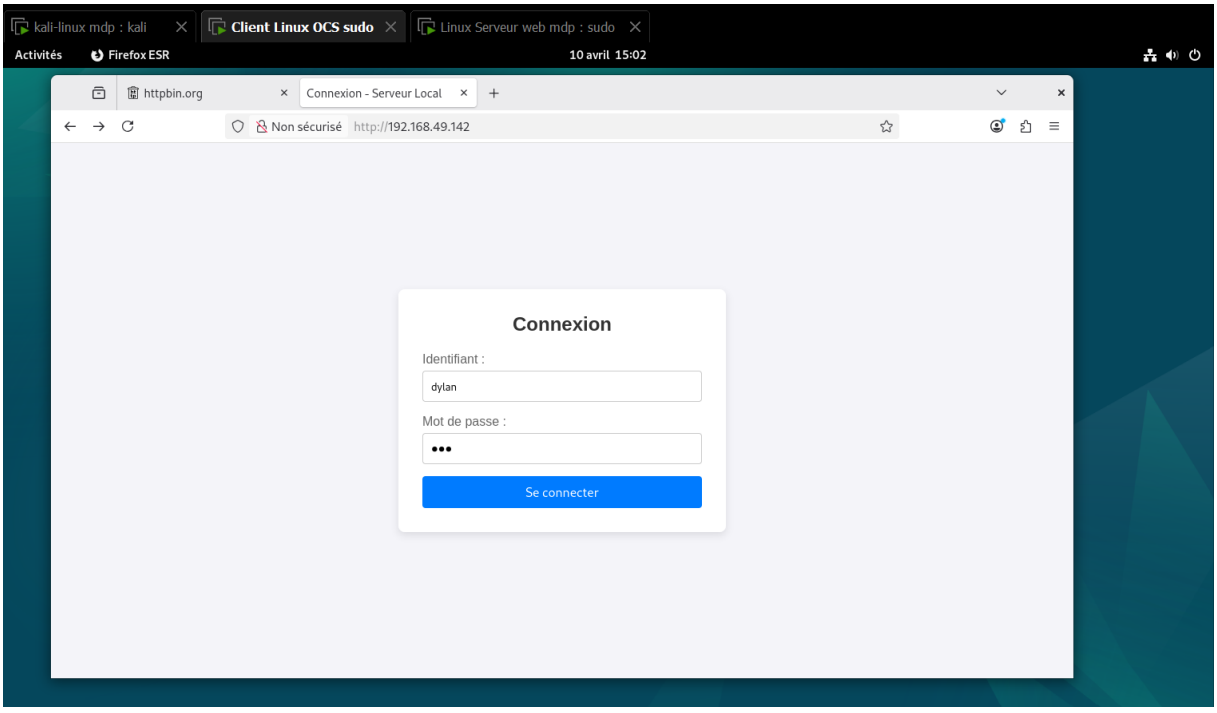
Un attaquant pourra toujours récupérer ces données, mais elles seront chiffrées et illisibles.

4-Serveur web local http

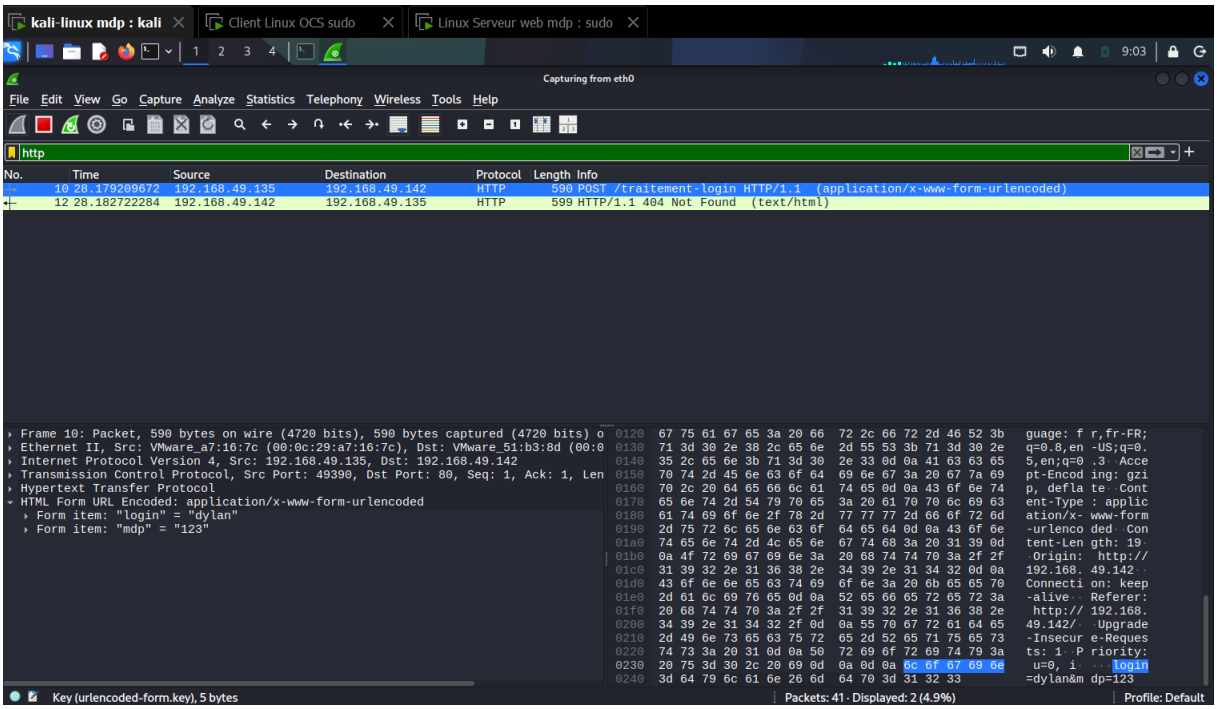
On crée un formulaire http avec un serveur web local apache sur une machine virtuelle :



Connectons-nous maintenant depuis notre client qui a été attaqué :



L’attaquant peut intercepter les informations envoyées par le client au serveur :

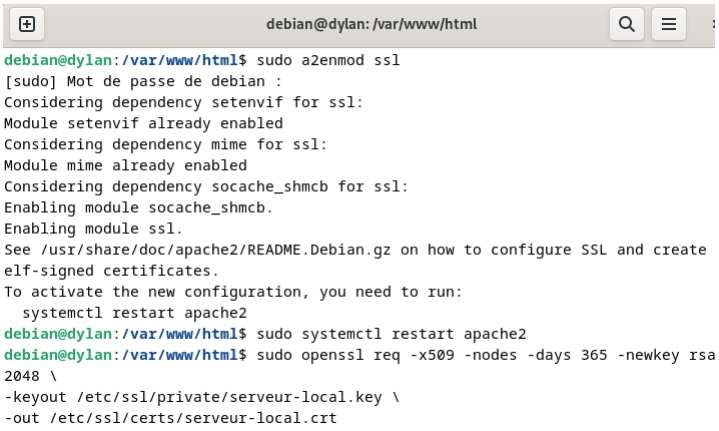


On retrouve bien le login et le mdp dans le trafic

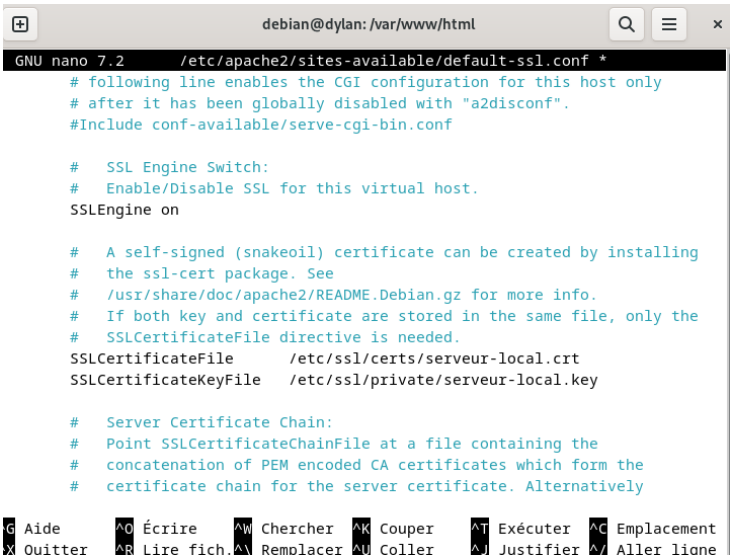
5-Serveur web local en HTTPS

Nous allons maintenant sécuriser le serveur web en HTTPS

Pour cela, on installe SSL sur notre serveur et on crée les clés de sécurité ainsi qu'un certificat auto-signé :



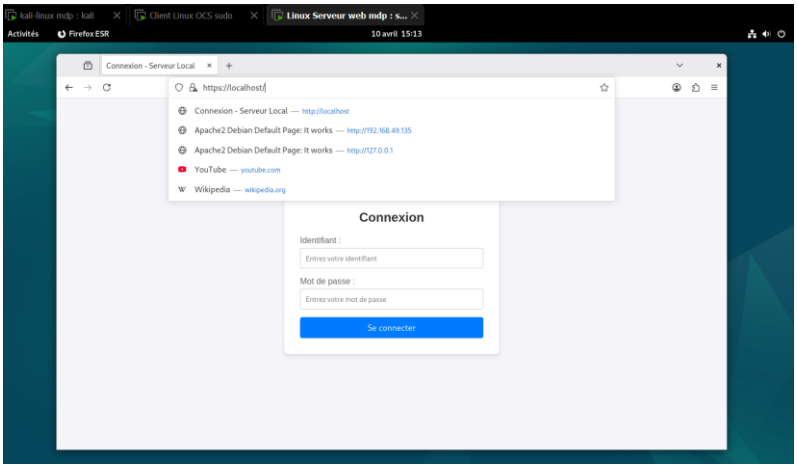
On renseigne les nouvelles clés de sécurité dans la configuration SSL :



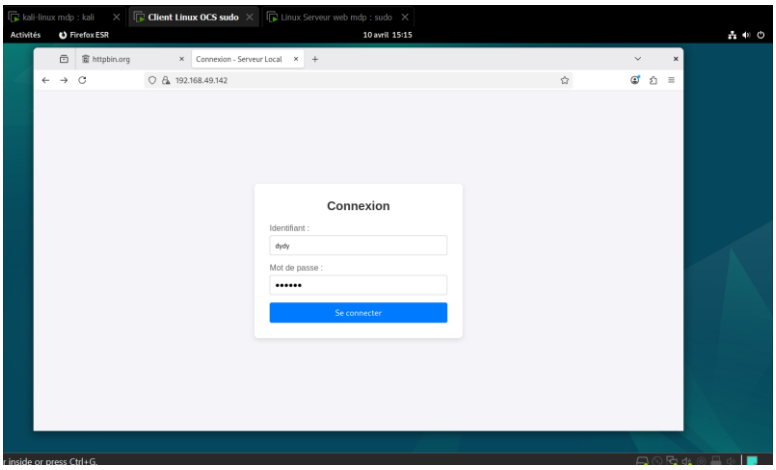
On termine en activant le site HTTPS et on relance apache :

```
debian@dylan: /var/www/html
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:FR
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:
debian@dylan:/var/www/html$
debian@dylan:/var/www/html$ sudo nano /etc/apache2/sites-available/default-ssl.c
onf
debian@dylan:/var/www/html$ sudo a2ensite default-ssl.conf
Enabling site default-ssl.
To activate the new configuration, you need to run:
  systemctl reload apache2
debian@dylan:/var/www/html$ sudo systemctl reload apache2
debian@dylan:/var/www/html$
```

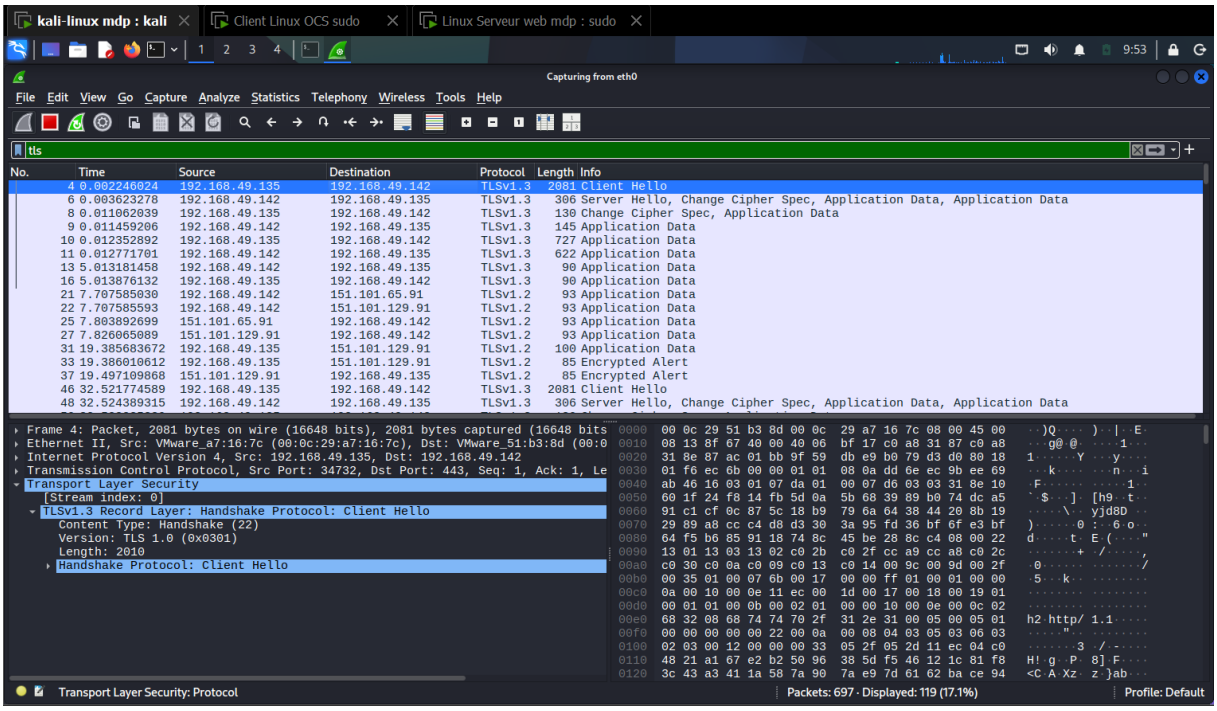
Notre serveur est maintenant en HTTPS :



Connectons-nous depuis le client et analysons le trafic depuis notre attaquant :



Le trafic sur wireshark est désormais en TLS :



Les communications sont désormais cryptées. L'attaquant pourra toujours les intercepter mais il ne pourra pas les utiliser car elles seront illisibles.