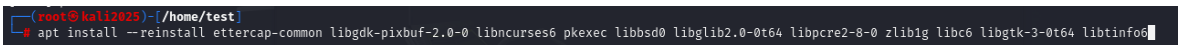
On démarre ces 5 machines :



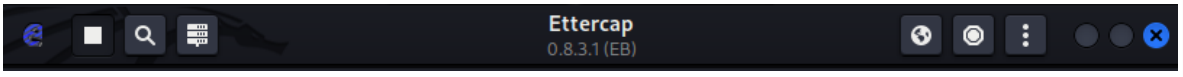
ensuite, on va démarrer le logiciel sur la machine kali ettercap après avoir réinstallé t tous les packages nécessaires grâce à la commande ci dessous :



Une fois ceci fait , on va lancer le logiciel :



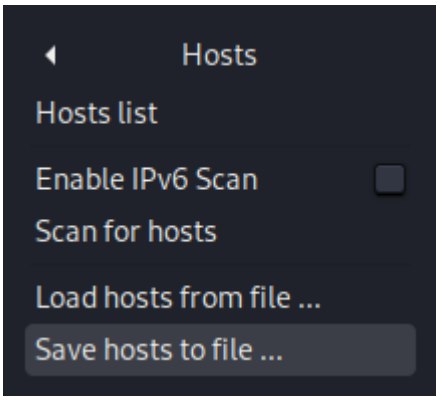
On va cliquer sur les trois petits point en haut à gauche :



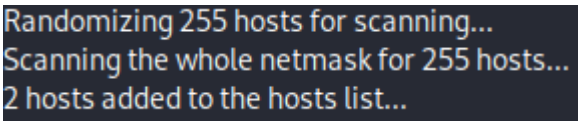
Puis on va dans hosts :



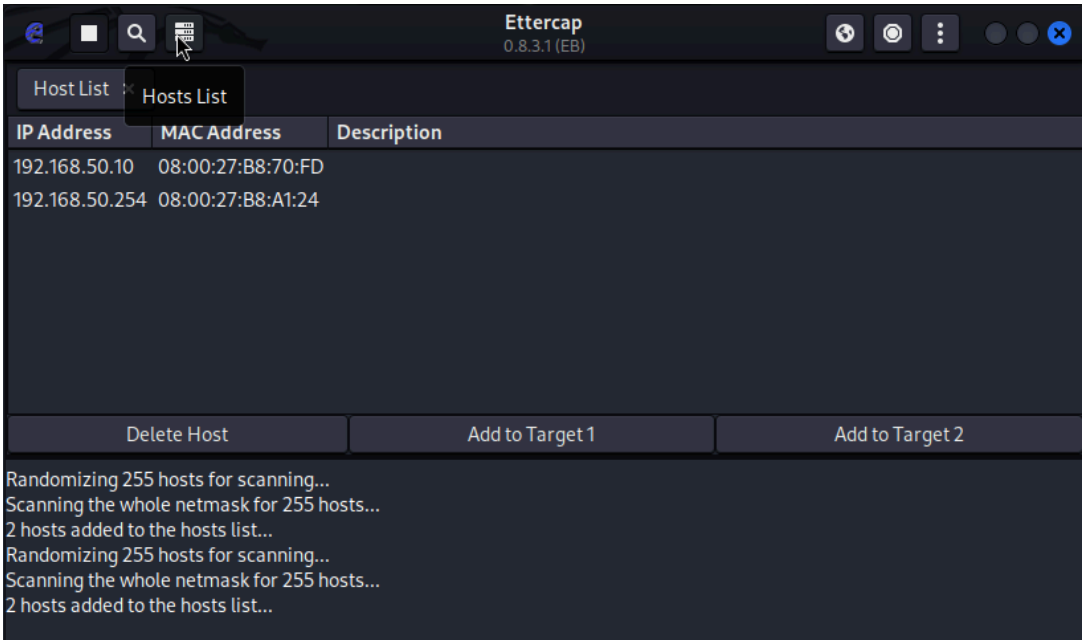
Et enfin :



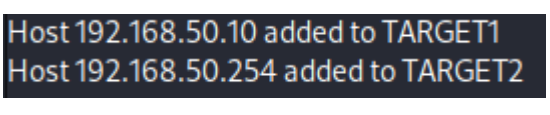
On va mettre scan for host



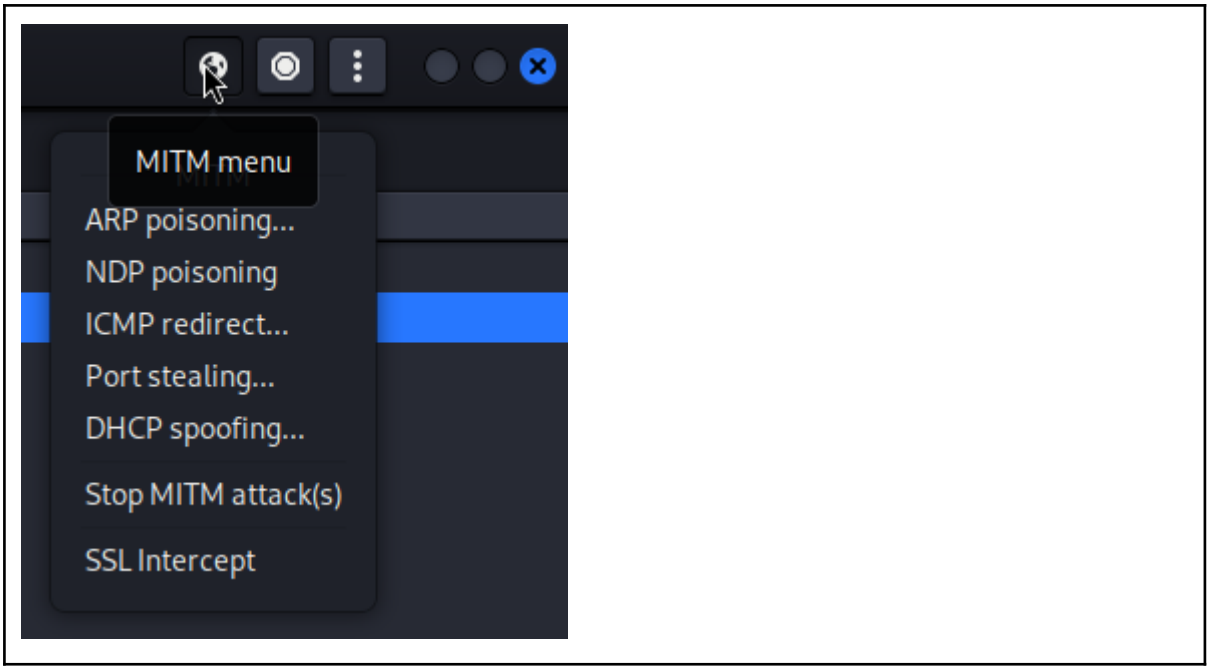
Et on voit que 2 hosts sont ajouté à la liste de hosts
On va donc sur la liste :



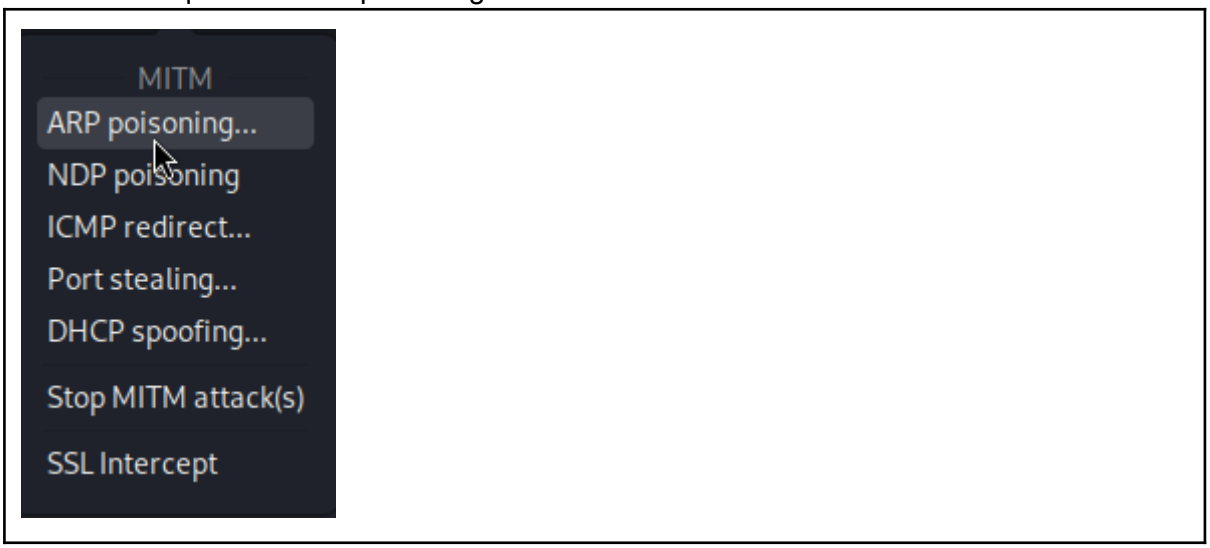
On va ajouter les cibles, 192.168.50.10 à la cible 1 et 192.168.50.254 à la cible 2 :



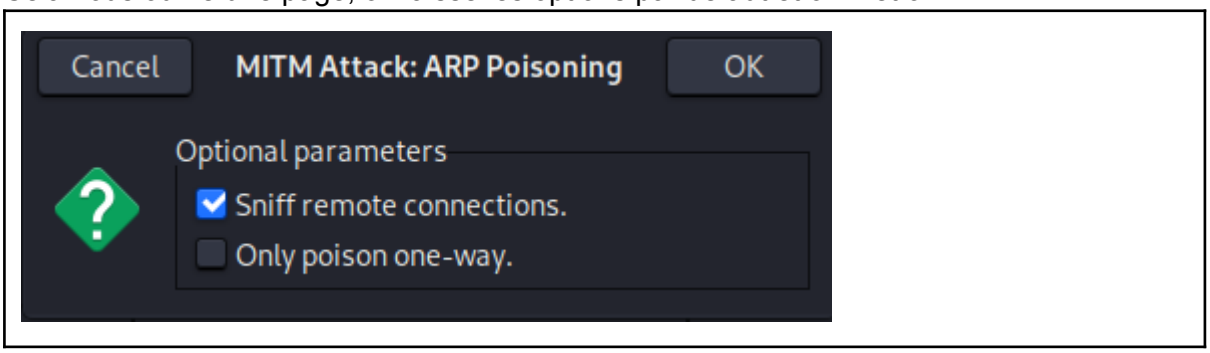
Ensuite on clique sur MITM MENU :

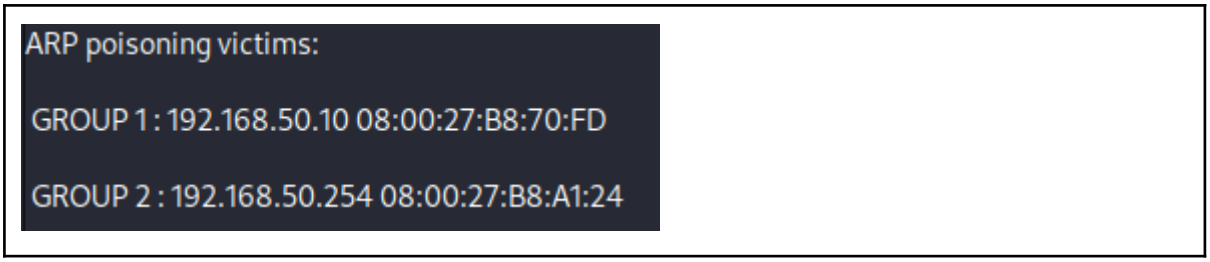


Puis on va cliquer sur ARP poisoning :

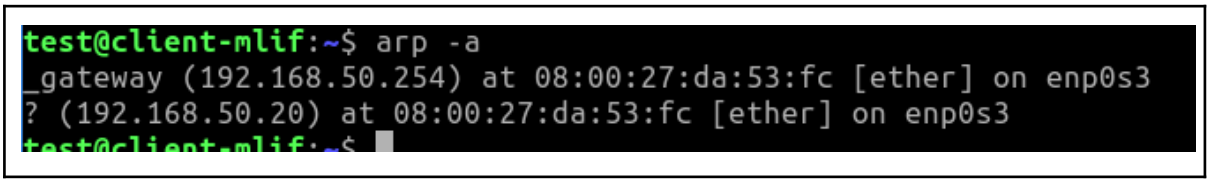


Cela nous ouvre une page, on laisse les options par défaut et on met ok :





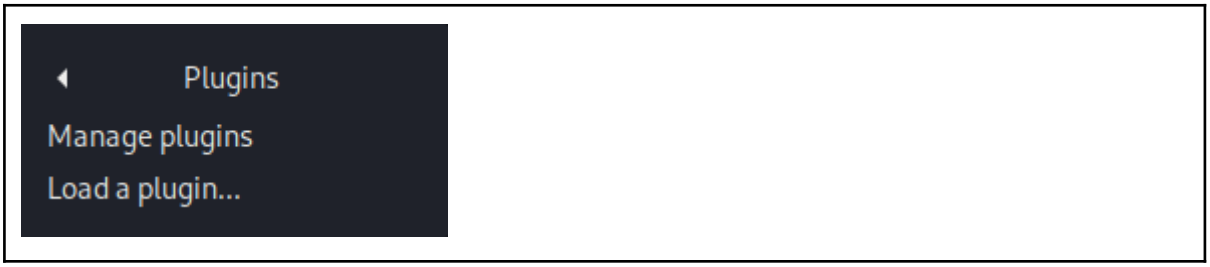
On va vérifier le cache arp sur la machine LUBUNTU training client :



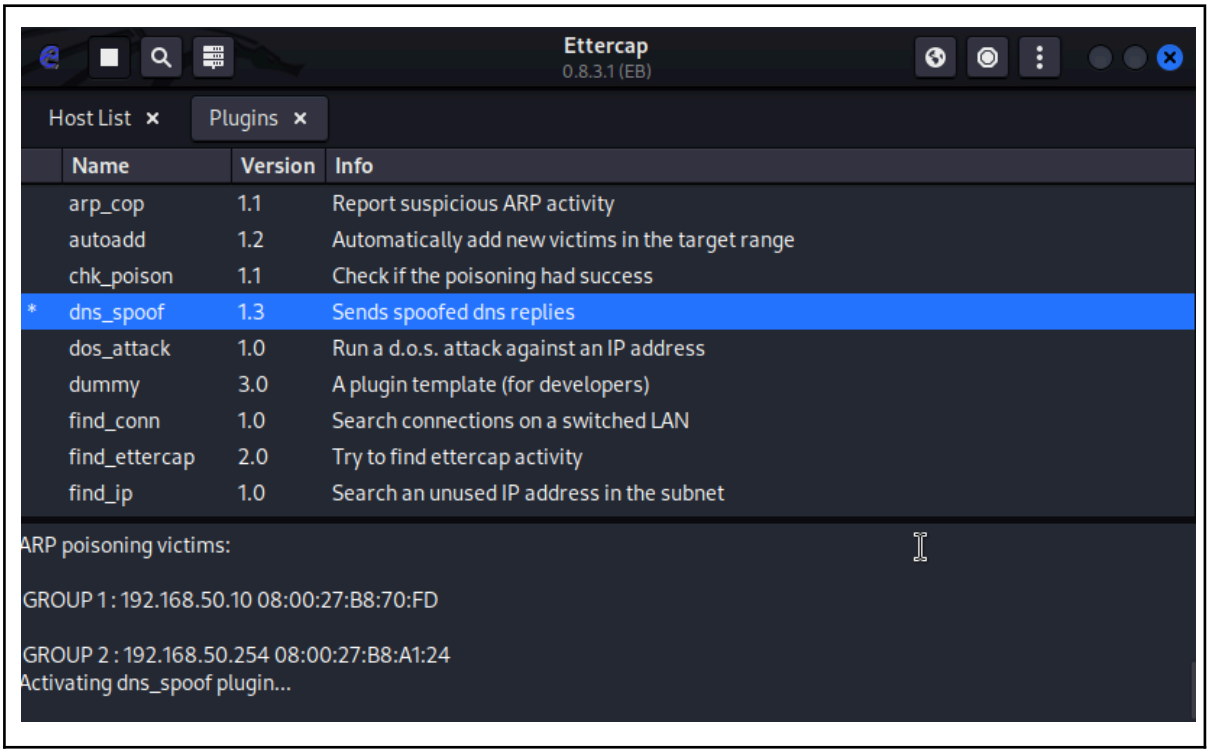
On va cliquer sur plugins :



Puis manage plugin :



Cela nous amène sur une page comme ça :
On va double cliquer sur dns spoof



On voit bien dans la boîte de dialogue en bas que le plugin à bien été activé

NE PAS OUBLIER DE DÉMARRER APACHE2 SUR LA KALI :



Sur la machine victime on voit bien qu'on atterrit sur le site pirate

Et sur la kali :

```
dns_spoof: A [www.mlif.local] spoofed to [192.168.50.20] TTL [3600 s]
dns_spoof: A [mail.mlif.local] spoofed to [192.168.50.20] TTL [3600 s]
dns_spoof: A [backup.mlif.local] spoofed to [192.168.50.20] TTL [3600 s]
dns_spoof: A [www.mlif.local] spoofed to [192.168.50.20] TTL [3600 s]
dns_spoof: A [mail.mlif.local] spoofed to [192.168.50.20] TTL [3600 s]
dns_spoof: A [backup.mlif.local] spoofed to [192.168.50.20] TTL [3600 s]
```

On voit donc que on a attaqué