Lab. ARP Spoofing (MITM)

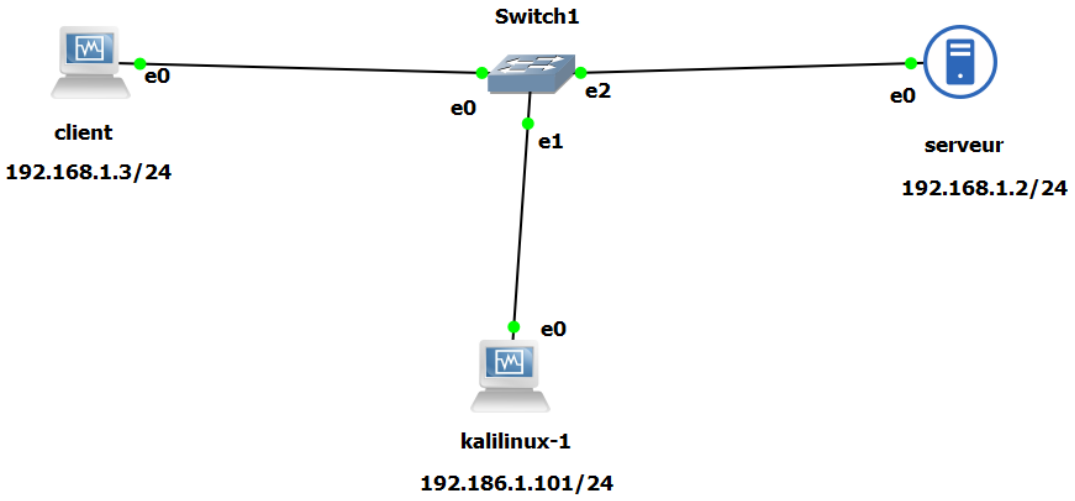
1. But

- Intercepter la communication entre 2 appareils dans un réseau commuté

2. Logiciels utilisés

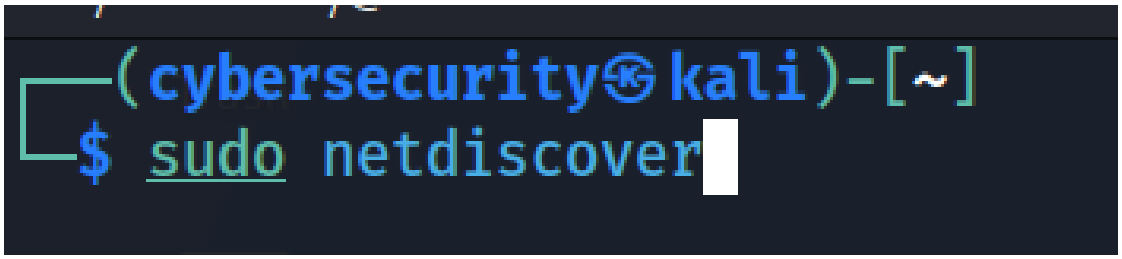
- Kali Linux
- 2 appareils
- Wireshark

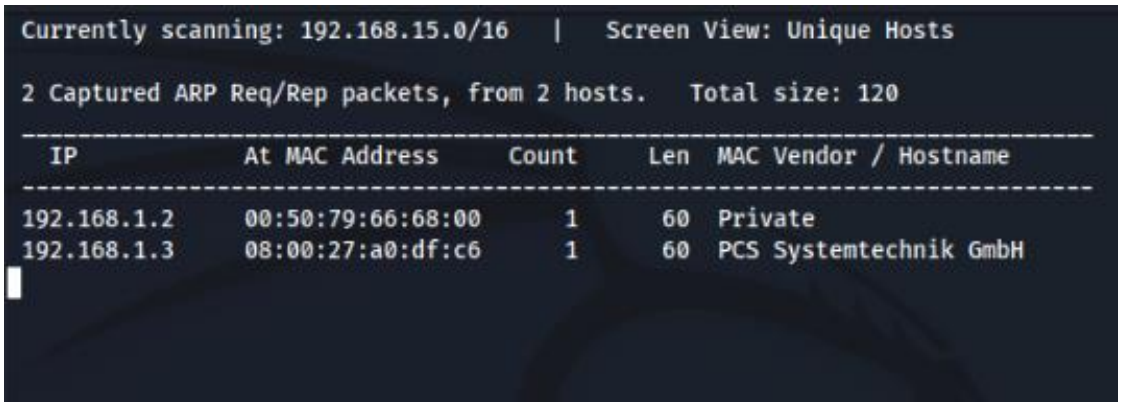
3. Installation



4. Commencer

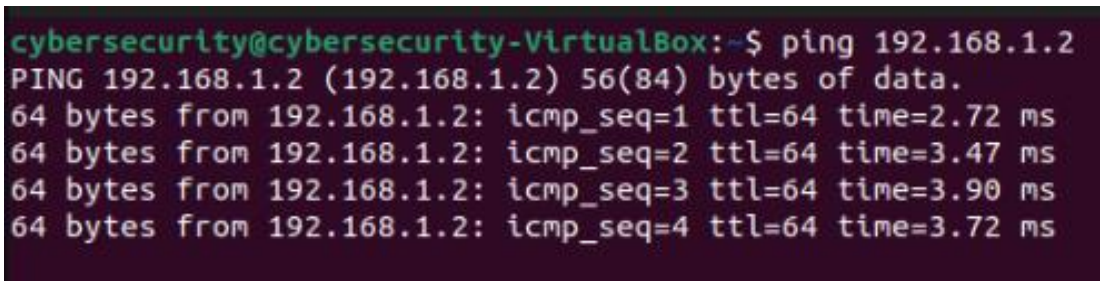
i. Obtenez un aperçu de votre réseau. (Kali Linux)



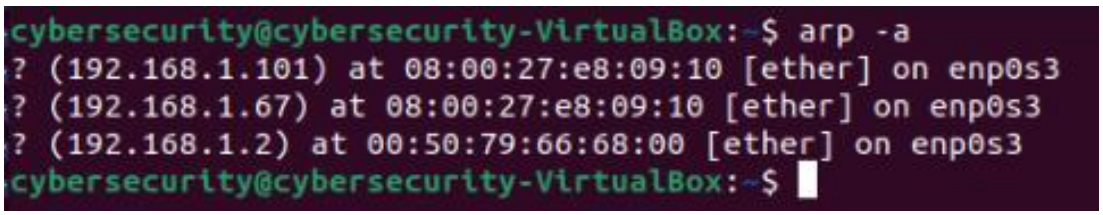


Le résultat nous montre le client (192.168.1.3) et le serveur (192.168.1.2).

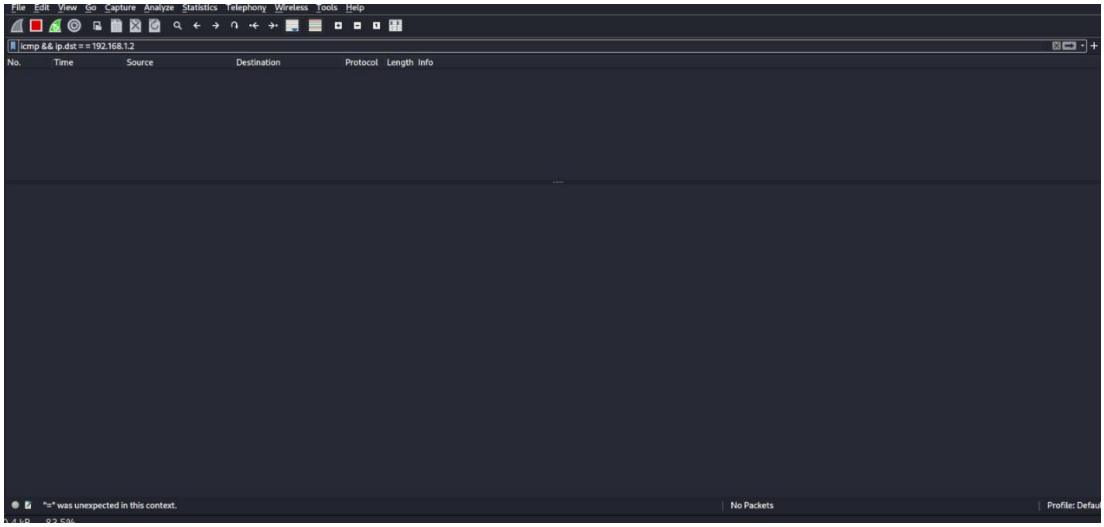
ii. Démarrez la communication entre le client et le serveur.



iii. Regardez la table d'adresses MAC du client.



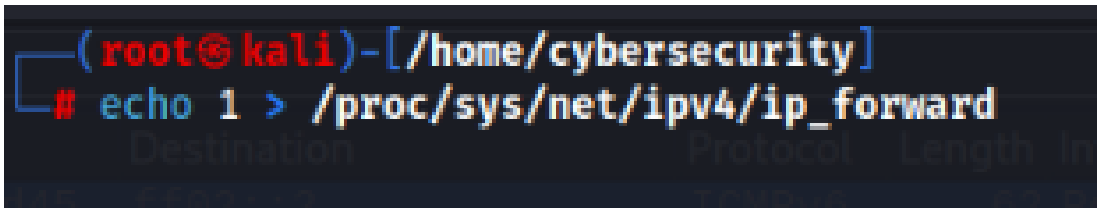
iv. Démarrer Wireshark (Kali Linux)



Le résultat nous montre aucun trafic ICMP destiné au serveur (192.168.1.2).

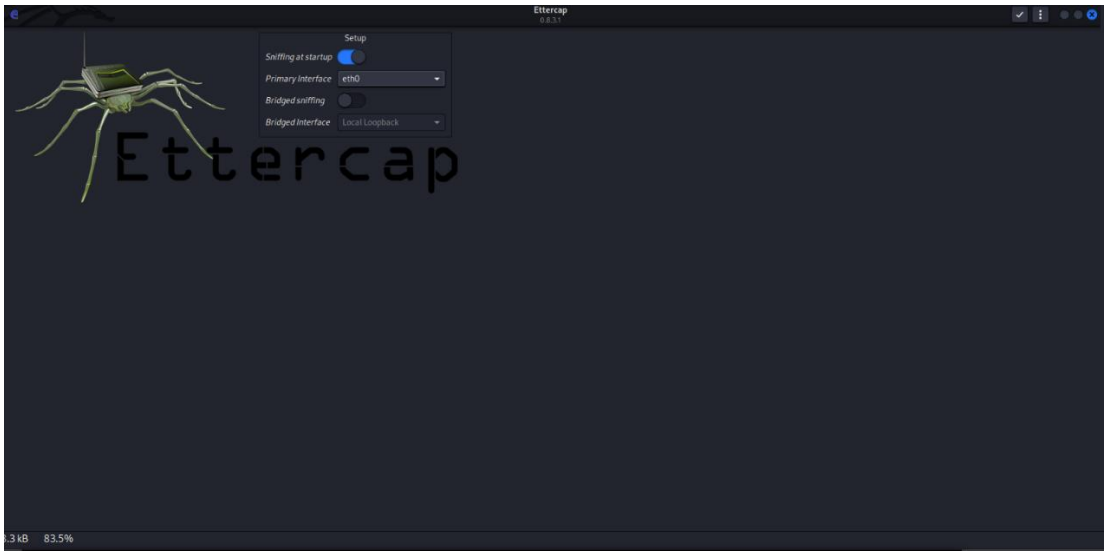
v. Définissez le transfert IP. (Kali Linux)

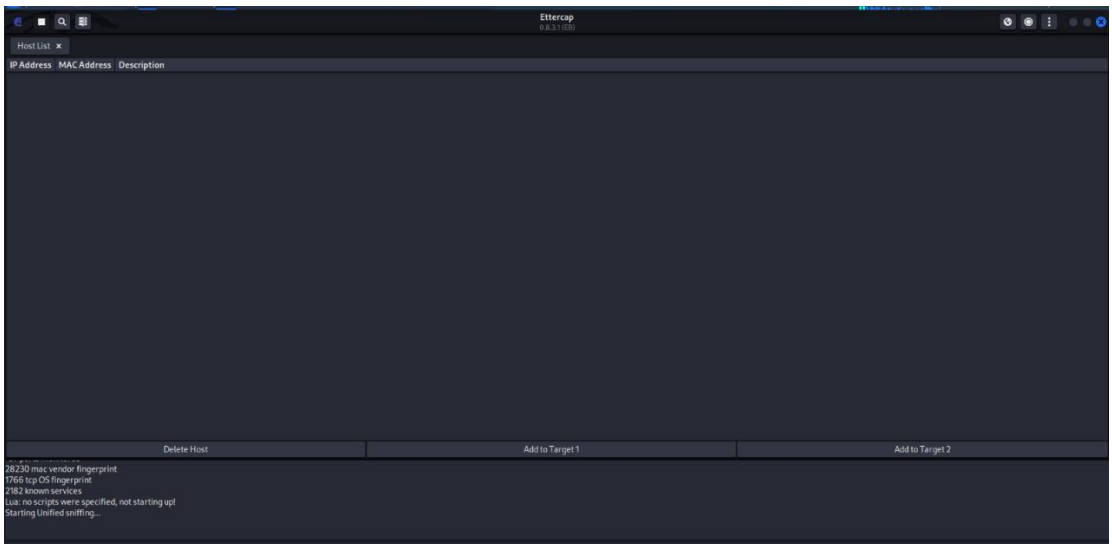
Le transfert IP permet à un système d'exploitation de transférer des paquets comme le fait un routeur ou plus généralement de les acheminer via d'autres réseaux.



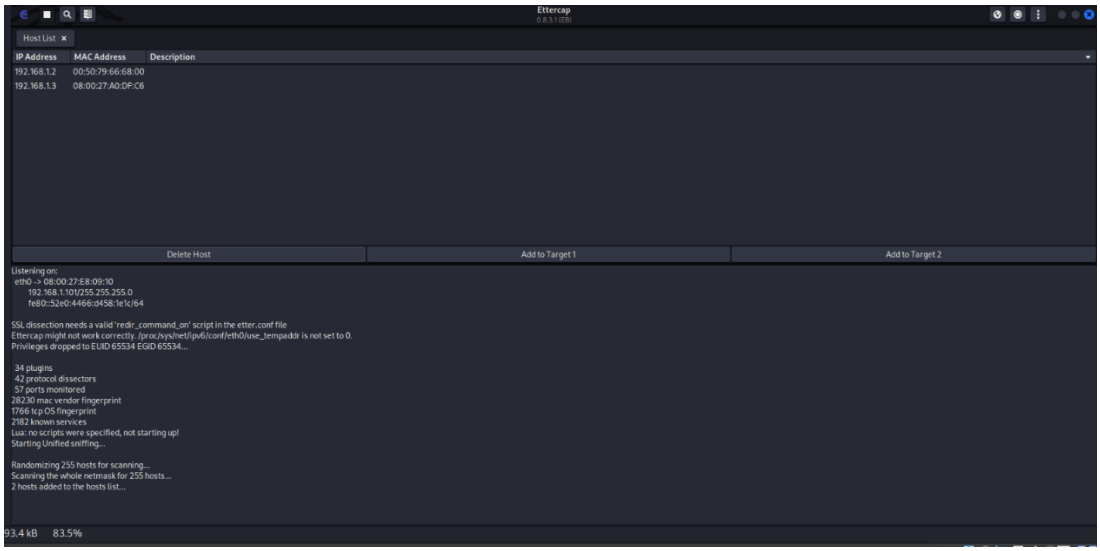
vi. Lancez l'attaque MITM. (Kali Linux)

vii. Démarrer Ettercap et Sélectionnez la méthode et l'interface de sniffing correctes.

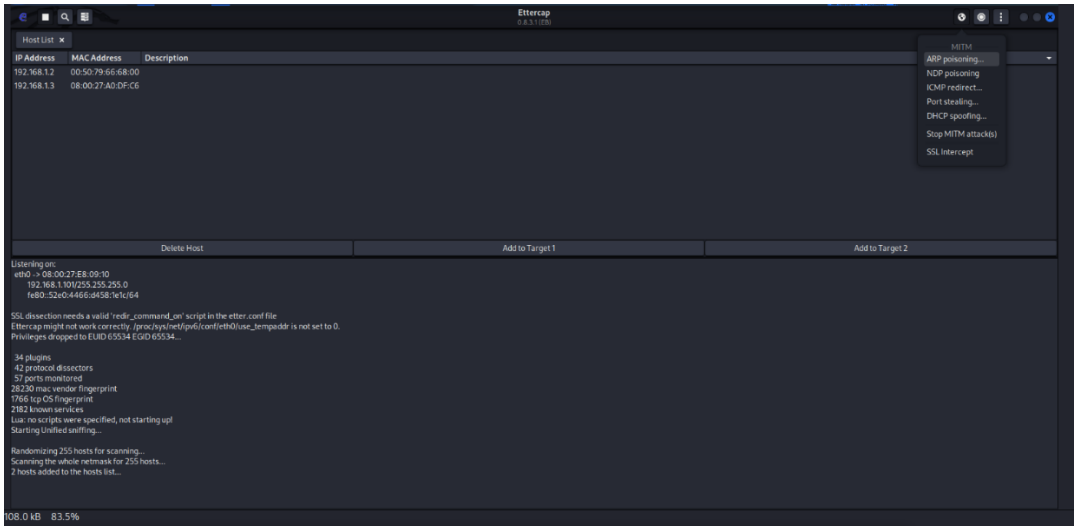


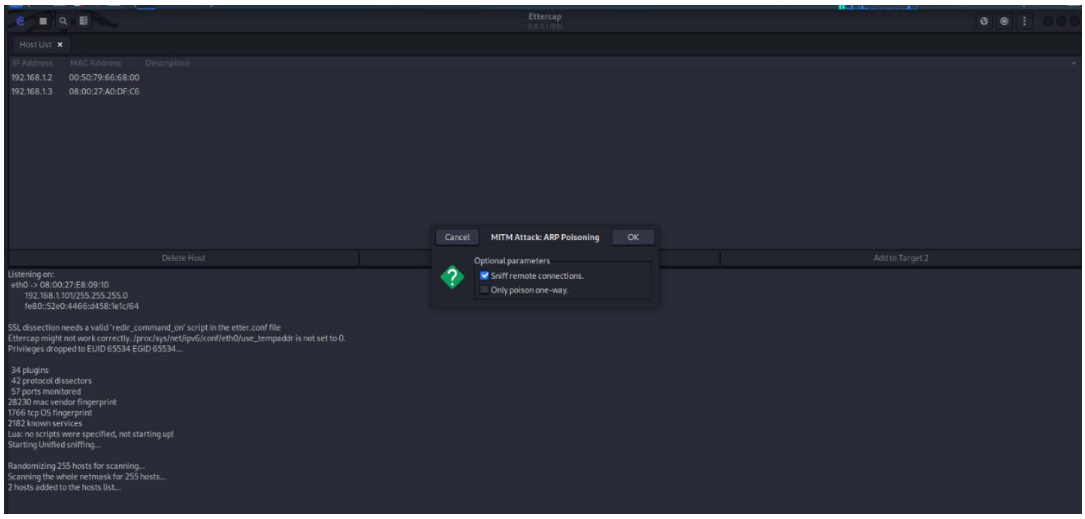


viii. Sélectionnez les hôtes (via un scan (Ctrl+S) ou manuellement (Add to target 1/2))



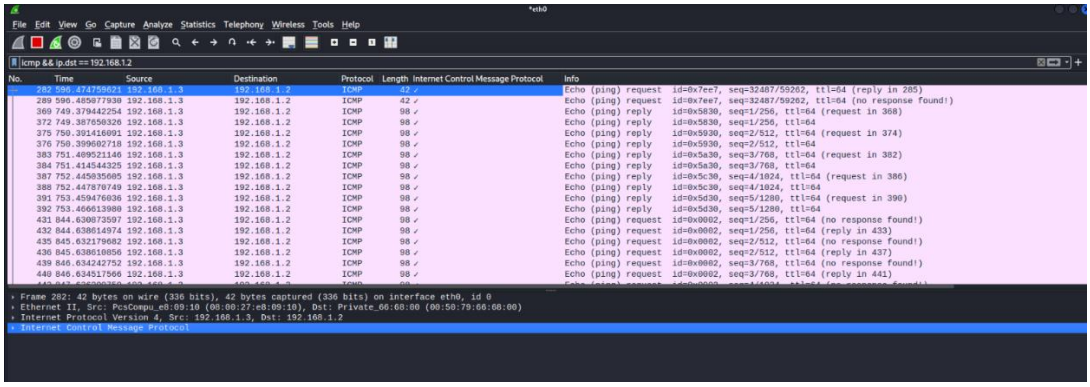
ix. Lancez l'attaque



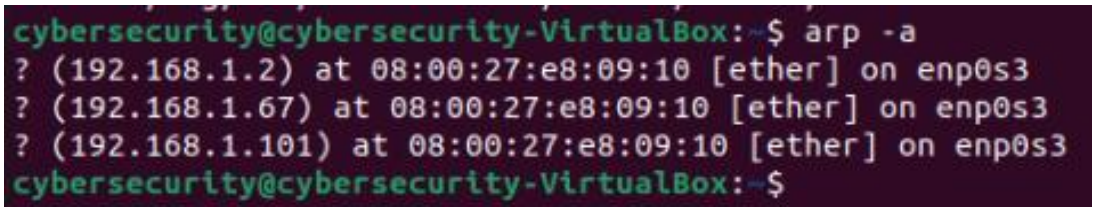


x. Vérifiez si l'attaque a réussi

Nous capturons maintenant le trafic entre le client et le serveur.



La table d'adresses MAC du client est poisonend. (192.168.1.101 est notre Kali)



xi. Conclusion

Une attaque de l'homme du milieu (MITM) est facile à établir et difficile à détecter