ARP Poisoning Attack

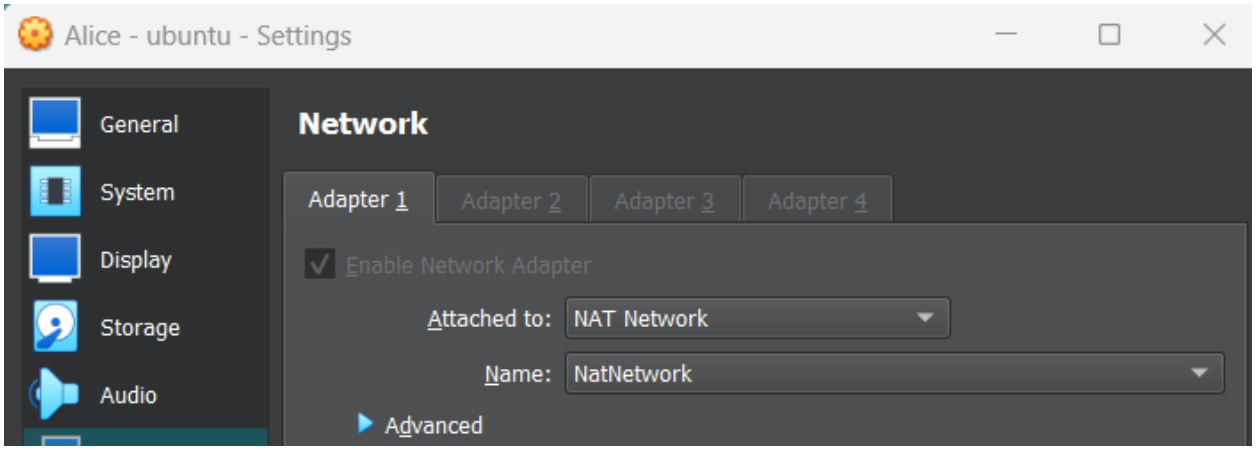
Aim: To implement a system in virtual box where an attacker machine does ARP Poisoning attack on a victim.

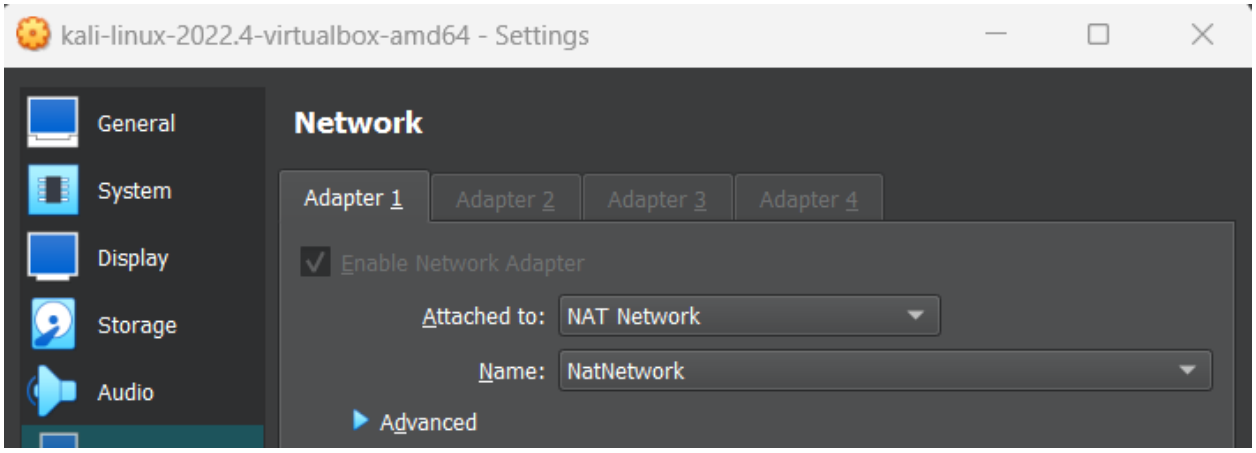
Requirements:

- Virtualbox
- Ubuntu
- Kali Linux

Procedure:

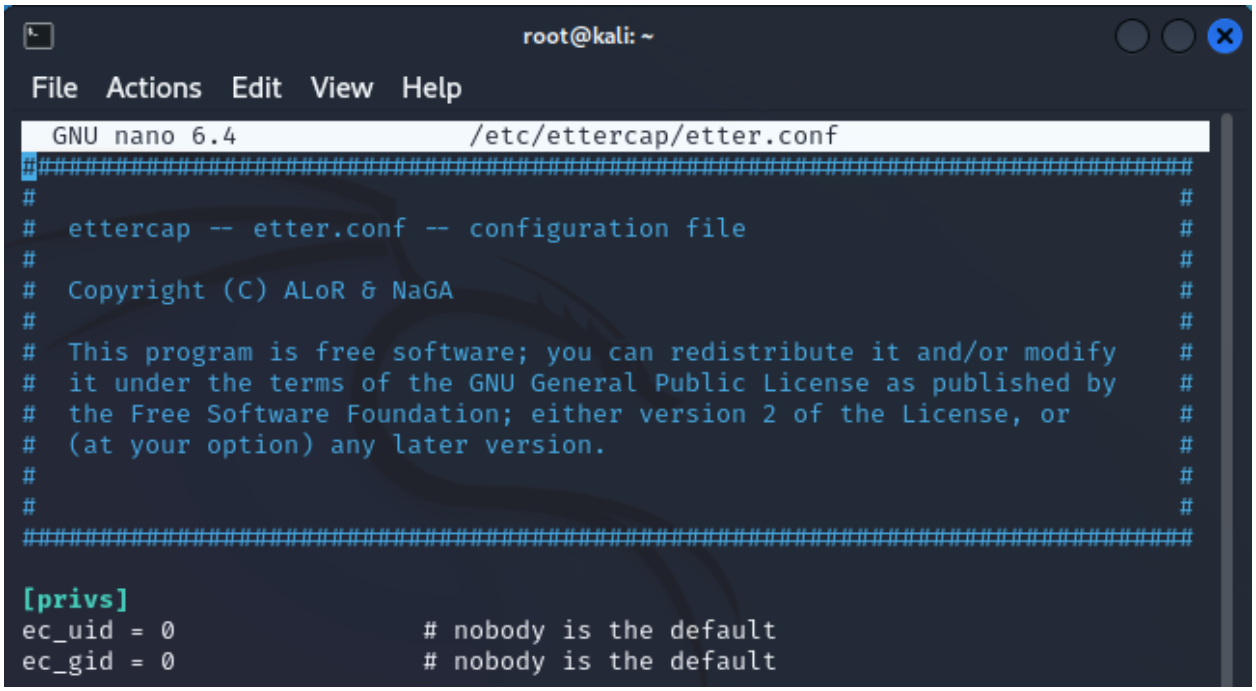
We need to install a Hypervisor, I used Virtual box. First we need to install Ubuntu and Kali Linux in the Virtualbox. Then we need to configure such that both Ubuntu and Kali Linux machines are present on same network. Both are set to 'NatNetwork' as shown below.



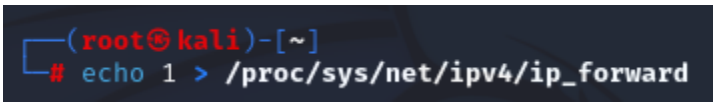


Now what the attacker does is change the MAC address of the victim to MAC address of his own victim.

We will be using ettercap tool to implement ARP poisoning. For that we need to make some changes in the configuration file as shown below.

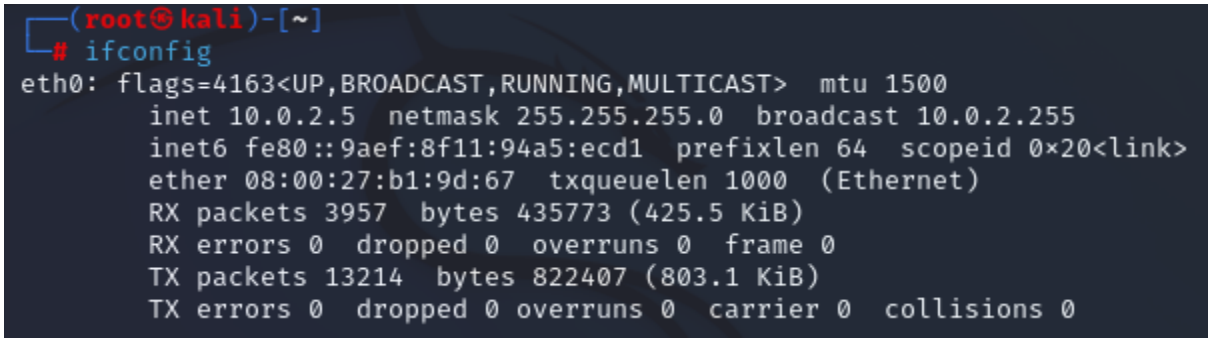


We need to set both ec_uid and ec_gid to 0. Now we need to enable ip forwarding.



IP address of KALI(attacker): 10.0.2.5

MAC address of KALI(attacker): 08:00:27:b1:9d:67



IP address of Alice(victim): 10.0.2.4

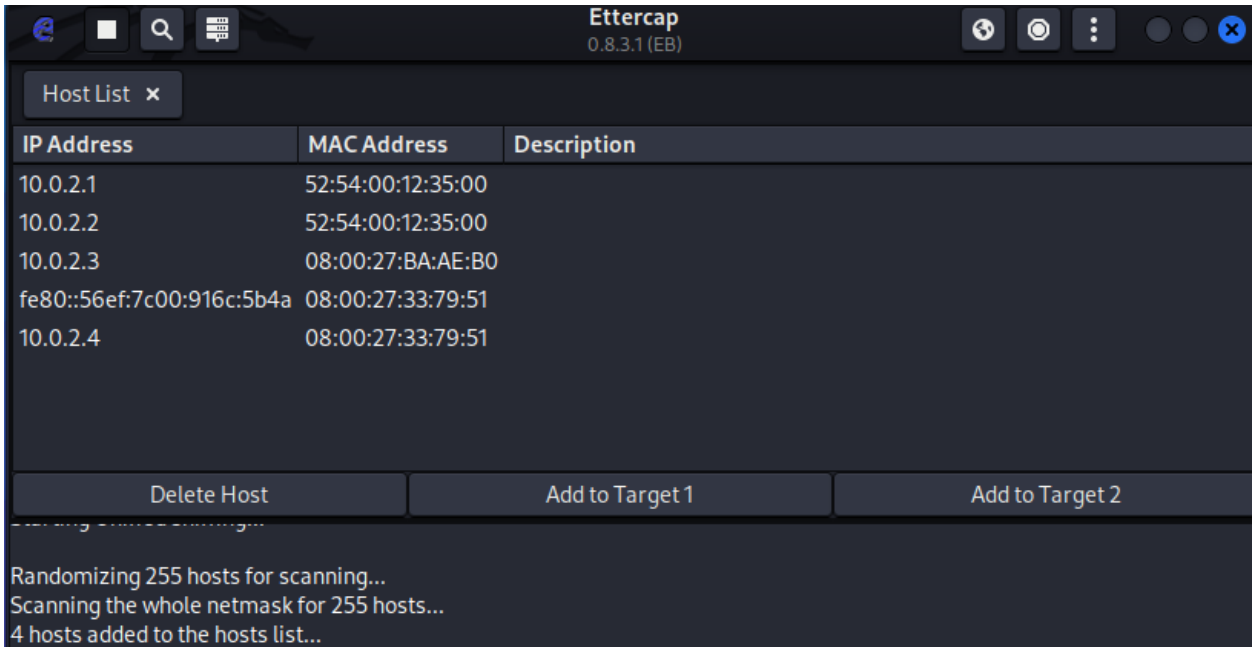
MAC address of Alice(victim): 08:00:27:33:79:51

```
alice@alice-VirtualBox:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.4  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::56ef:7c00:916c:5b4a  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:33:79:51  txqueuelen 1000  (Ethernet)
        RX packets 253719  bytes 378370393 (378.3 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 23575  bytes 1483949 (1.4 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

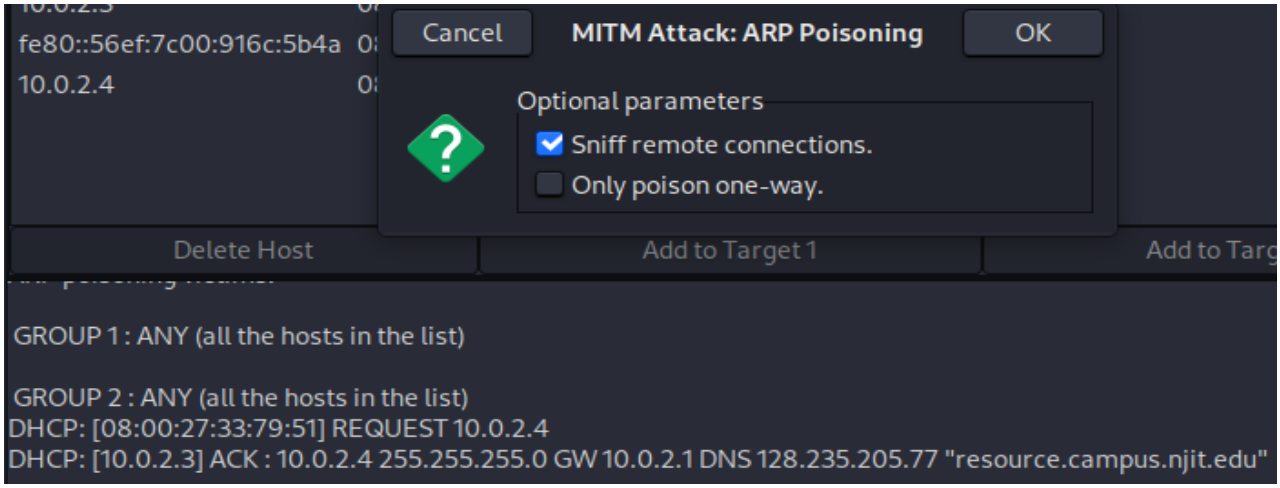
We can check the ARP cache of the victim machine by using arp -a command.

```
alice@alice-VirtualBox:~$ arp -a
? (10.0.2.2) at 52:54:00:12:35:00 [ether] on enp0s3
_gateway (10.0.2.1) at 52:54:00:12:35:00 [ether] on enp0s3
? (10.0.2.3) at 08:00:27:27:eb:74 [ether] on enp0s3
? (10.0.2.5) at 08:00:27:b1:9d:67 [ether] on enp0s3
alice@alice-VirtualBox:~$
```

Now, we open ettercap in Kali machine. First we need to scan for the hosts so add the target IP that we want to perform ARP spoofing on. We can check all the hosts from options as shown below.



In the above screenshot, we can see that the Alice machine (10.0.2.4) is in the host list. We add it to target list and switch ARP poisoning on from the by clicking globe option.

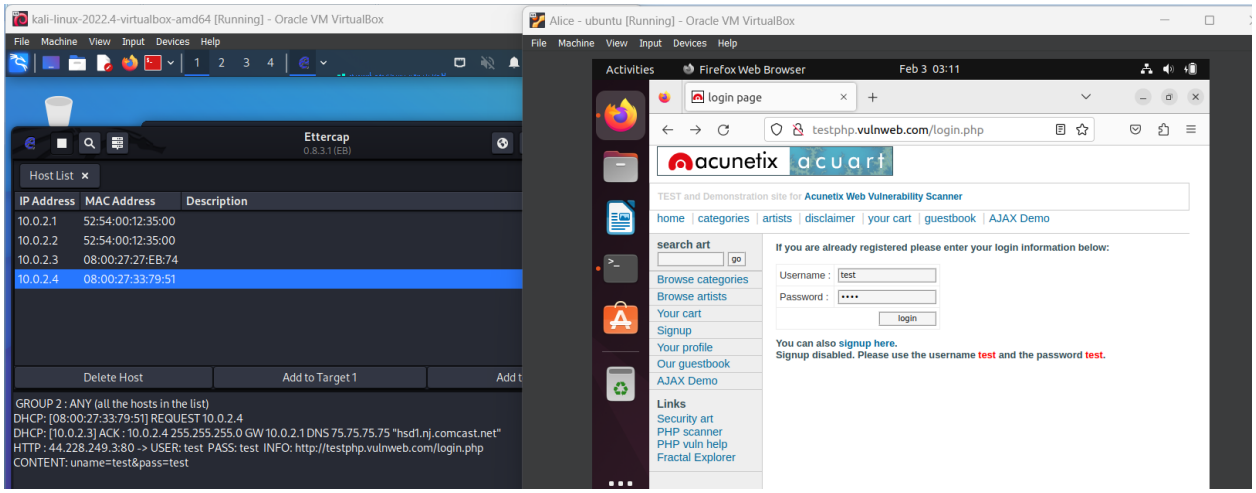


Now the ARP poisoning attack has been started. To Verify this we can check the arp cache of victim machine using arp –a.

```
alice@alice-VirtualBox:~$ arp -a
? (10.0.2.2) at 08:00:27:b1:9d:67 [ether] on enp0s3
_gateway (10.0.2.1) at 08:00:27:b1:9d:67 [ether] on enp0s3
? (10.0.2.3) at 08:00:27:b1:9d:67 [ether] on enp0s3
? (10.0.2.5) at 08:00:27:b1:9d:67 [ether] on enp0s3
```

We can see from the above picture that MAC addresses have been replaced with MAC address of KALI.

Now we can verify in browser as well. We will be using testphp.vulnweb.com which is a http site which can be used for demonstration purpose.



From the above picture, we can see that when I entered username and password in the right. It shows both login and password that were used in the logs in ettercap.