EX NO: 12   **REGISTER NO:210701509**

DATE:

MITM ATTACK WITH ETTERCAP

AIM:

   To initiate a MITM Aattack using ICMP redirect with Ettercap tool
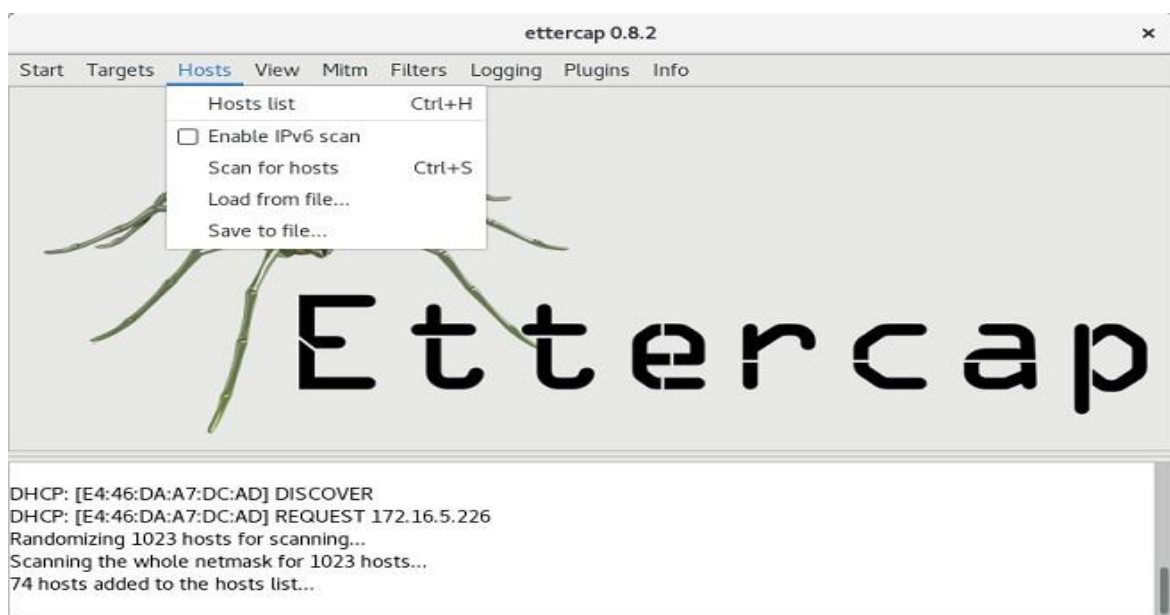
ALGORITHM:

- Install ettercap if not done already using the command-
     dnf install ettercap
- Open etter.conf file and change the values of ec_uid and ec_gid to zero from default.
     vi /etc/ettercap/etter.conf
- Next start ettercap in GTK
     ettercap -G
- Click sniff, followed by unified sniffing.
- Select the interface connected to the network.
- Next ettercap should load into attack mode by clicking Hosts followed by Scan for Hosts
- Click Host List and choose the IP address for ICMP redirect
- Now all traffic to that particular IP address is redirected to some other IP address.
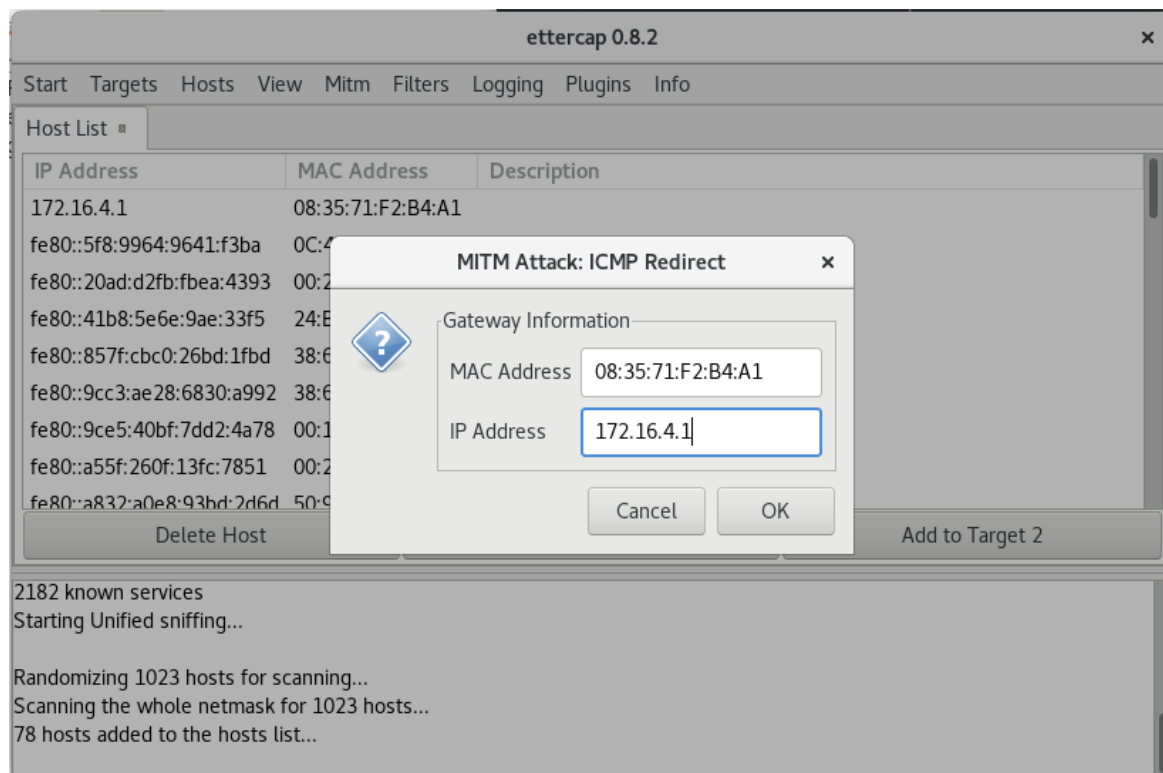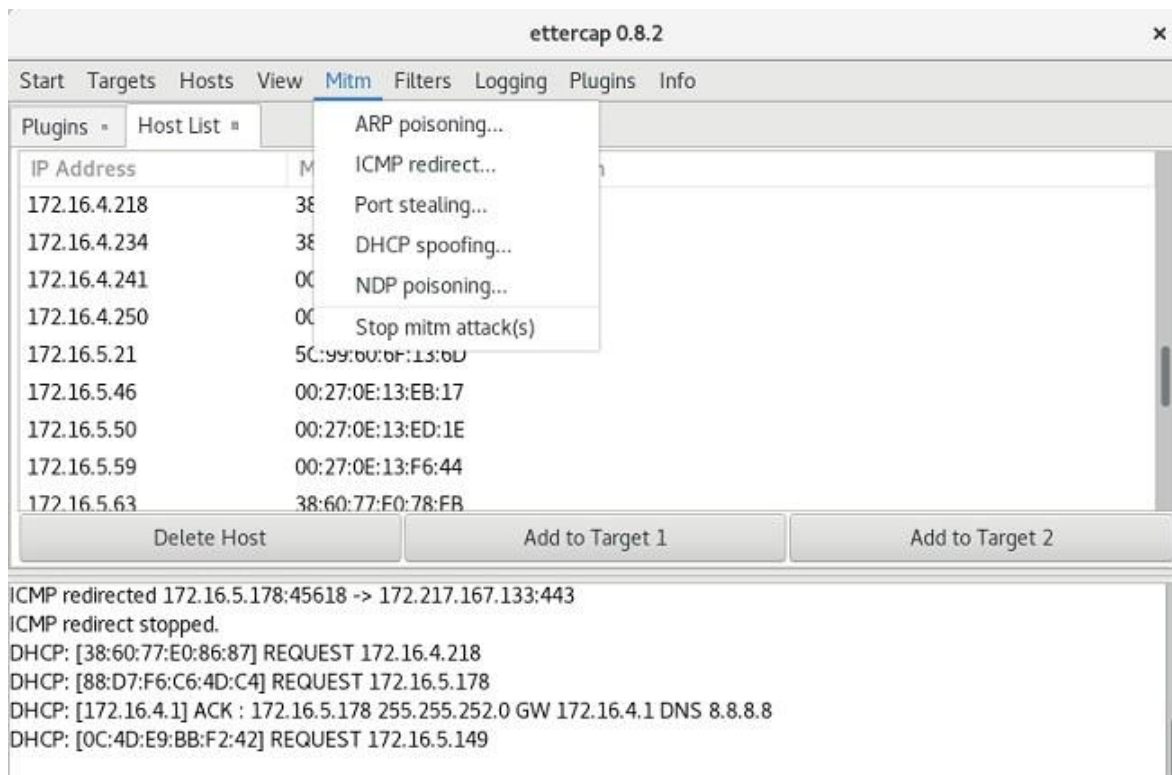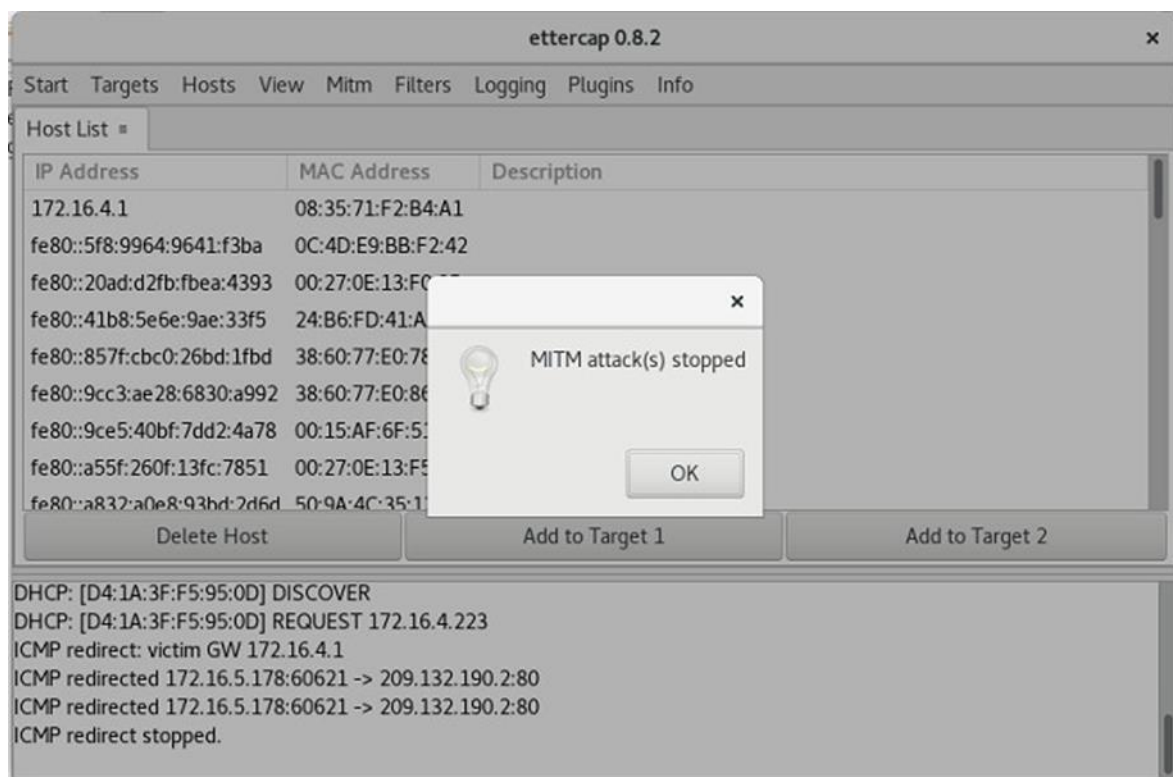- Click MITM and followed by Stop to close the attack.

Output:
[root@localhost security lab]# dnf install ettercap
[root@localhost security lab]# vi /etc/ettercap/etter.conf
[root@localhost security lab]# ettercap –G

ettercap 0.8.2

Start Targets Hosts View Mitm Filters Logging Plugins Info

Plugins ▫ Host List ▫

IP Address	M	
172.16.4.218	38	ARP poisoning...
172.16.4.234	38	ICMP redirect...
172.16.4.241	00	Port stealing...
172.16.4.250	00	DHCP spoofing...
172.16.5.21	5C:99:60:6F:13:6D	NDP poisoning...
172.16.5.46	00:27:0E:13:EB:17	Stop mitm attack(s)
172.16.5.50	00:27:0E:13:ED:1E	
172.16.5.59	00:27:0E:13:F6:44	
172.16.5.63	38:60:77:F0:78:FB	

Delete Host	Add to Target 1	Add to Target 2

ICMP redirected 172.16.5.178:45618 -> 172.217.167.133:443
ICMP redirect stopped.
DHCP: [38:60:77:E0:86:87] REQUEST 172.16.4.218
DHCP: [88:D7:F6:C6:4D:C4] REQUEST 172.16.5.178
DHCP: [172.16.4.1] ACK : 172.16.5.178 255.255.252.0 GW 172.16.4.1 DNS 8.8.8.8
DHCP: [0C:4D:E9:BB:F2:42] REQUEST 172.16.5.149

---

ettercap 0.8.2

Start Targets Hosts View Mitm Filters Logging Plugins Info

Host List ▫

IP Address	MAC Address	Description
172.16.4.1	08:35:71:F2:B4:A1	
fe80::5f8:9964:9641:f3ba	0C:4	
fe80::20ad:d2fb:fbea:4393	00:2	
fe80::41b8:5e6e:9ae:33f5	24:E	
fe80::857f:cbc0:26bd:1fbd	38:6	
fe80::9cc3:ae28:6830:a992	38:6	
fe80::9ce5:40bf:7dd2:4a78	00:1	
fe80::a55f:260f:13fc:7851	00:2	
fe80::a832:a0e8:93bd:2d6d	50:9	

MITM Attack: ICMP Redirect ✕

Gateway Information

MAC Address 08:35:71:F2:B4:A1

IP Address 172.16.4.1

Cancel   OK

Delete Host		Add to Target 2

2182 known services
Starting Unified sniffing...

Randomizing 1023 hosts for scanning...
Scanning the whole netmask for 1023 hosts...
78 hosts added to the hosts list...

RESULT: