MITMATTACKWITHETTERCAP

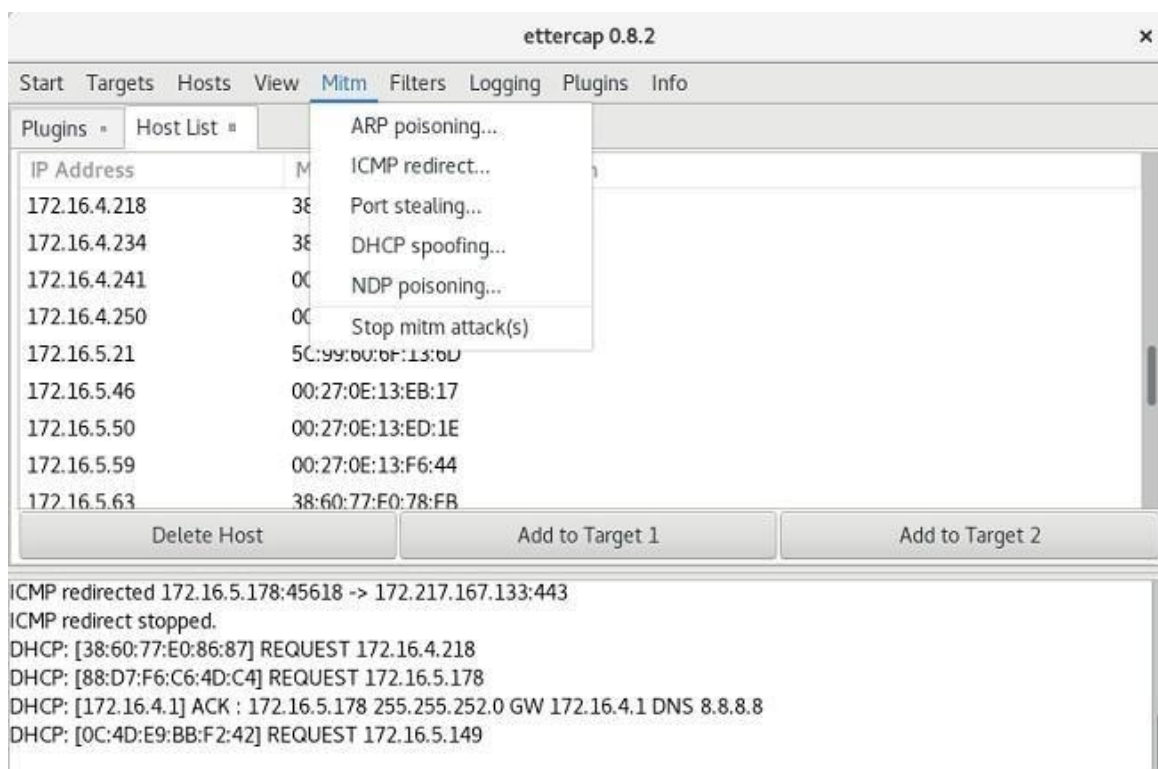## AIM:
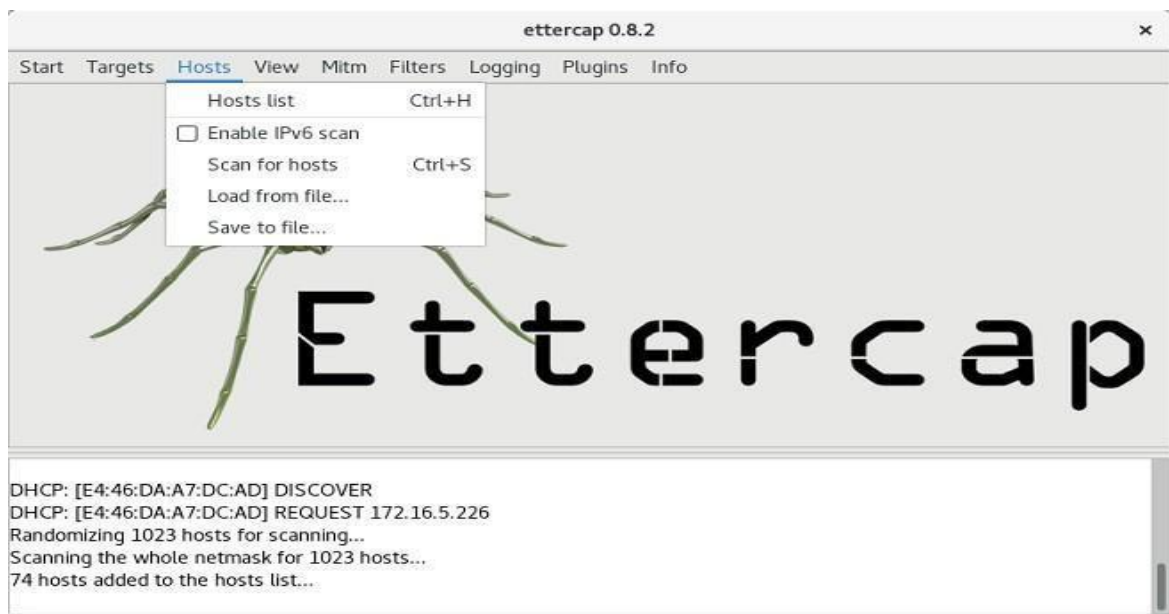
ToinitiateaMITMattackusingICMPredirectwithEttercaptool.

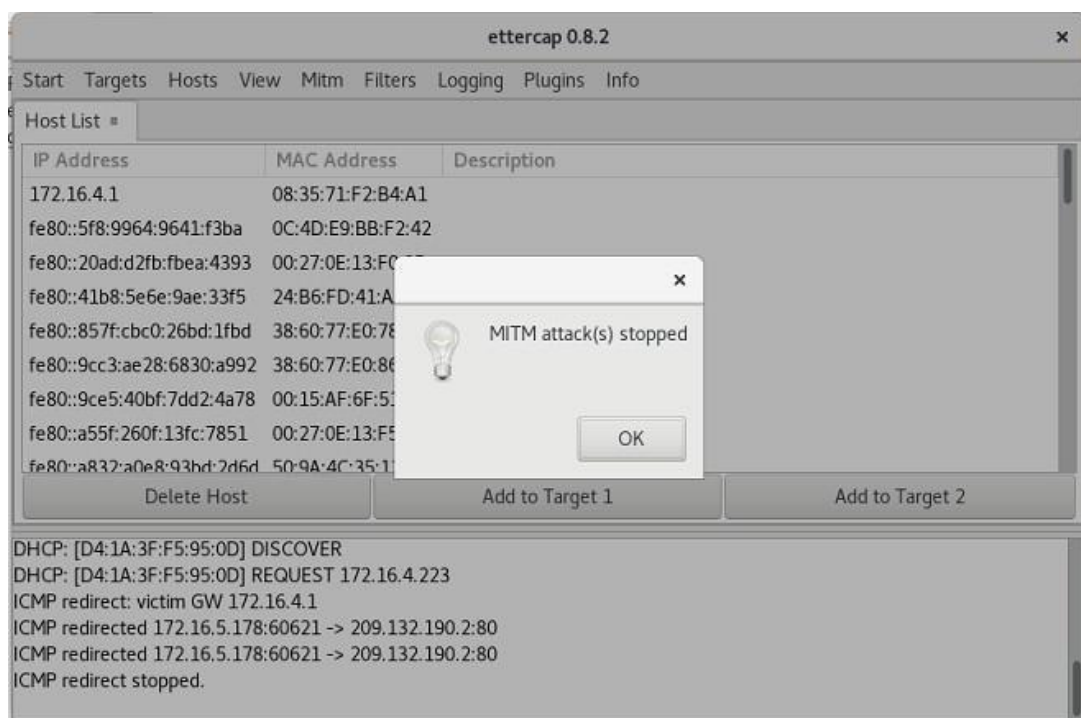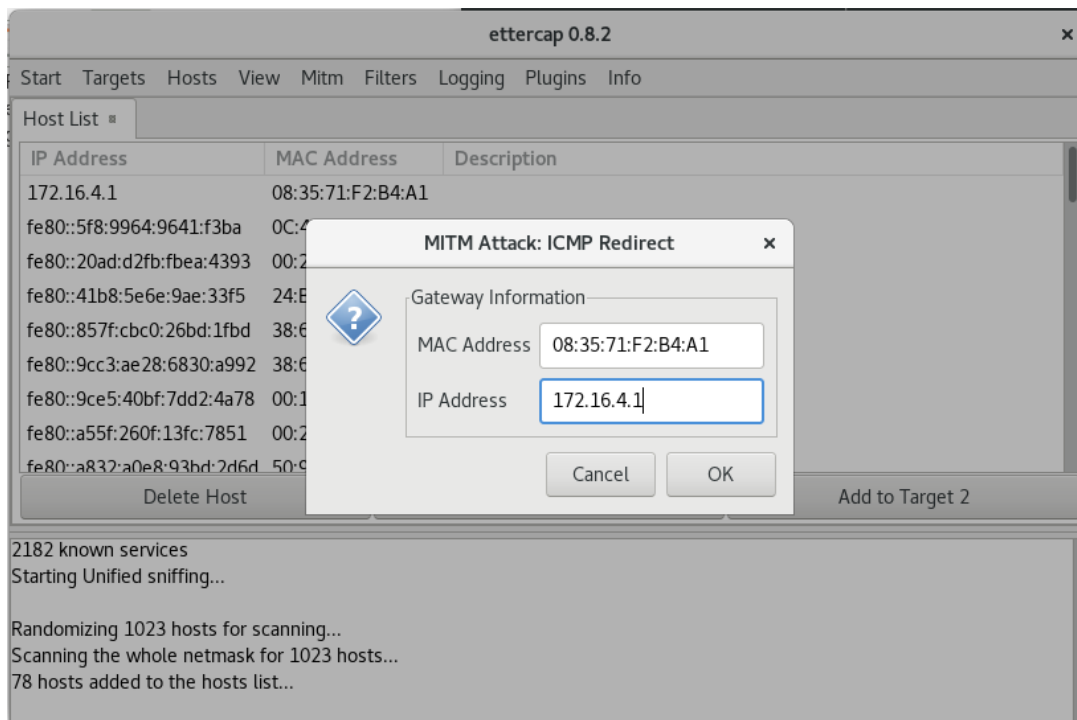## ALGORITHM:

1. Installettercapifnotdonealreadyusing the command- dnf install ettercap
2. Openetter.conffileandchangethevaluesofec_uidandec_gidtozero from default. vi /etc/ettercap/etter.conf
3. Next start ettercap in GTKettercap -G
4. Clicksniff,followedbyunifiedsniffing.
5. Selecttheinterface connectedtothenetwork.
6. NextettercapshouldloadintoattackmodebyclickingHostsfollowedbyScanfor Hosts
7. ClickHostListandchoosethe IPaddressfor ICMPredirect
8. NowalltraffictothatparticularIPaddressisredirectedtosomeotherIPaddress.
9. ClickMITMandfollowed byStopto closetheattack.

OUTPUT:

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

ettercap 0.8.2   ✕

Start   Targets   **Hosts**   View   Mitm   Filters   Logging   Plugins   Info

Hosts list	Ctrl+H
☐ Enable IPv6 scan	
Scan for hosts	Ctrl+S
Load from file…	
Save to file…	

DHCP: [E4:46:DA:A7:DC:AD] DISCOVER
DHCP: [E4:46:DA:A7:DC:AD] REQUEST 172.16.5.226
Randomizing 1023 hosts for scanning…
Scanning the whole netmask for 1023 hosts…
74 hosts added to the hosts list…

ettercap 0.8.2   ✕

Start   Targets   Hosts   View   **Mitm**   Filters   Logging   Plugins   Info

Plugins ▪   Host List ▪

| ARP poisoning… |
| ICMP redirect… |
| Port stealing… |
| DHCP spoofing… |
| NDP poisoning… |
| Stop mitm attack(s) |

IP Address	M
172.16.4.218	38
172.16.4.234	38
172.16.4.241	00
172.16.4.250	00
172.16.5.21	5C:99:60:6F:13:6D
172.16.5.46	00:27:0E:13:EB:17
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

RESULT:

TheexperimenttoinitiateaMITMattackusingICMPredirectwithEttercap tool is executed successfully.