



VIT[®]
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

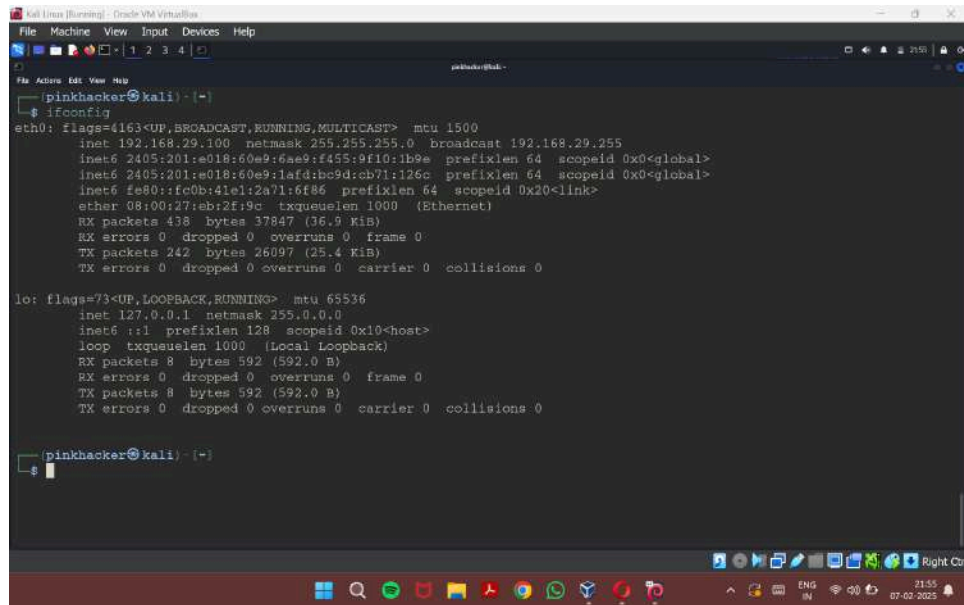
ARP Spoofing

NAME: DHEVATHA S P
REG NO.: 22BCE0826

NAME OF FACULTY: DR. Satish C.J
COURSE TITLE : Penetration Testing and Vulnerability
Analysis Lab
COURSE CODE: BCSE319P
LAB SLOT: L55+L56
SEMESTER: Winter Semester 2024-25
CLASS NO.: VL2024250505928

Dhevatha S P
22BCE0826

1. IP address of host machine (Kali Linux) and the victim machines (Ubuntu and Metasploitable2).

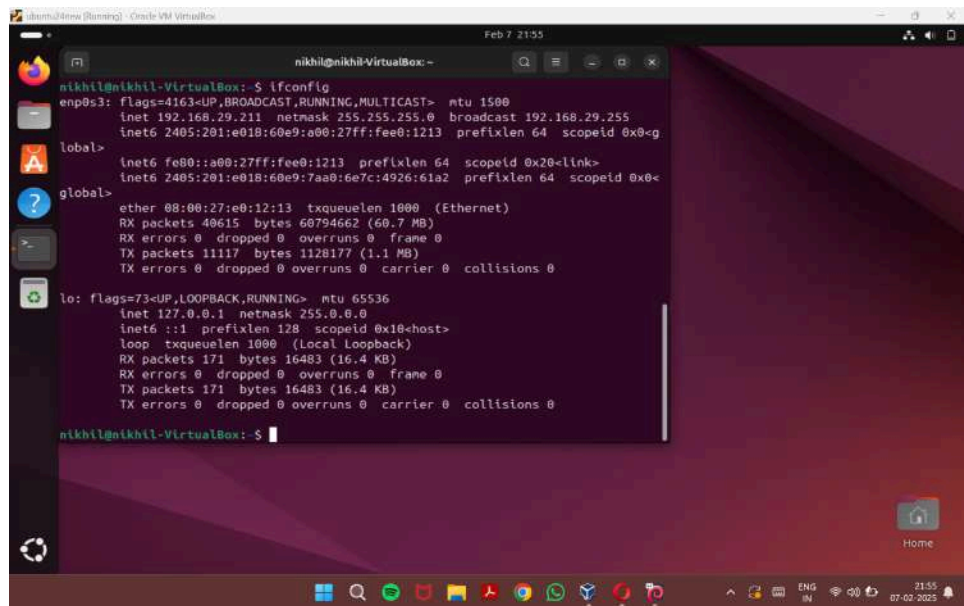


```

Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
pinkhacker@kali: ~
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.29.100 netmask 255.255.255.0 broadcast 192.168.29.255
    inet6 2405:201:e018:60e9:fae9:f455:9f10:1b9e prefixlen 64 scopeid 0x0<global>
    inet6 2405:201:e018:60e9:1af4:b9d:cb71:126c prefixlen 64 scopeid 0x0<global>
    inet6 fe80::fc0b:41e1:2a71:6f86 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:eb:2f:9c txqueuelen 1000 (Ethernet)
    RX packets 438 bytes 37847 (36.9 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 242 bytes 26097 (25.4 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

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 8 bytes 592 (592.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 592 (592.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

pinkhacker@kali: ~
$
  
```



```

Ubuntu [Running] - Oracle VM VirtualBox
Feb 7 21:55
nikhil@nikhil-VirtualBox: ~
$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.29.211 netmask 255.255.255.0 broadcast 192.168.29.255
    inet6 2405:201:e018:60e9:a00:27ff:fee0:1213 prefixlen 64 scopeid 0x0<global>
    inet6 fe80::a00:27ff:fee0:1213 prefixlen 64 scopeid 0x20<link>
    inet6 2405:201:e018:60e9:7aa0:6e7c:4926:61a2 prefixlen 64 scopeid 0x0<global>
    ether 08:00:27:e0:12:13 txqueuelen 1000 (Ethernet)
    RX packets 40615 bytes 60794662 (60.7 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 11117 bytes 1128177 (1.1 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

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 171 bytes 16483 (16.4 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 171 bytes 16483 (16.4 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

nikhil@nikhil-VirtualBox: ~
$
  
```

```

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:f7:56:85
          inet addr:192.168.29.93  Bcast:192.168.29.255  Mask:255.255.255.0
          inet6 addr: 2405:201:e018:60e9:a00:27ff:fef7:5685/64  Scope:Global
          inet6 addr: fe80::a00:27ff:fef7:5685/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:231 errors:0 dropped:0 overruns:0 frame:0
          TX packets:108 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:21081 (20.5 KB)  TX bytes:12673 (12.3 KB)
          Base address:0xd020  Memory:f0200000-f0220000

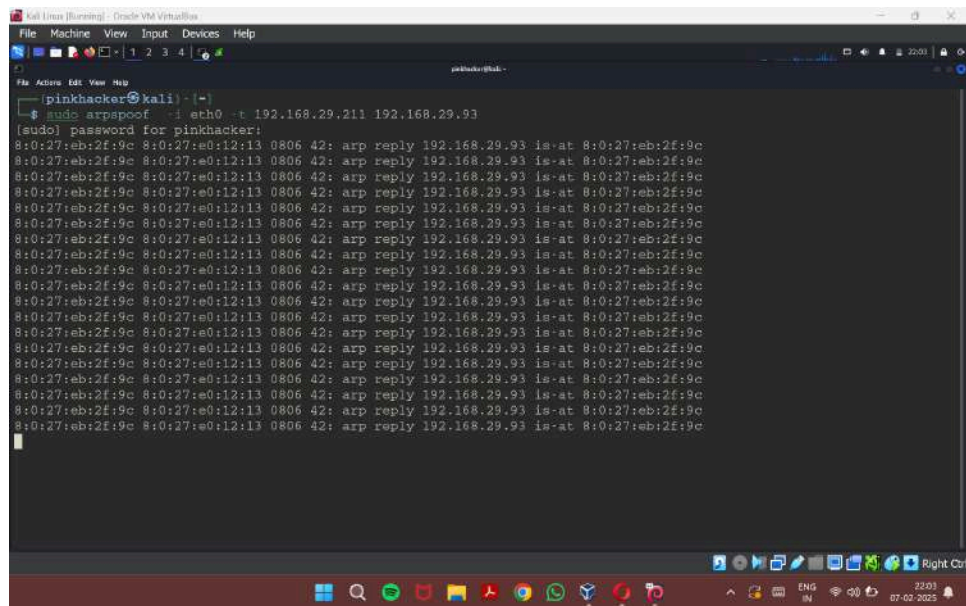
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128  Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:96 errors:0 dropped:0 overruns:0 frame:0
          TX packets:96 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:21437 (20.9 KB)  TX bytes:21437 (20.9 KB)

msfadmin@metasploitable:~$

```

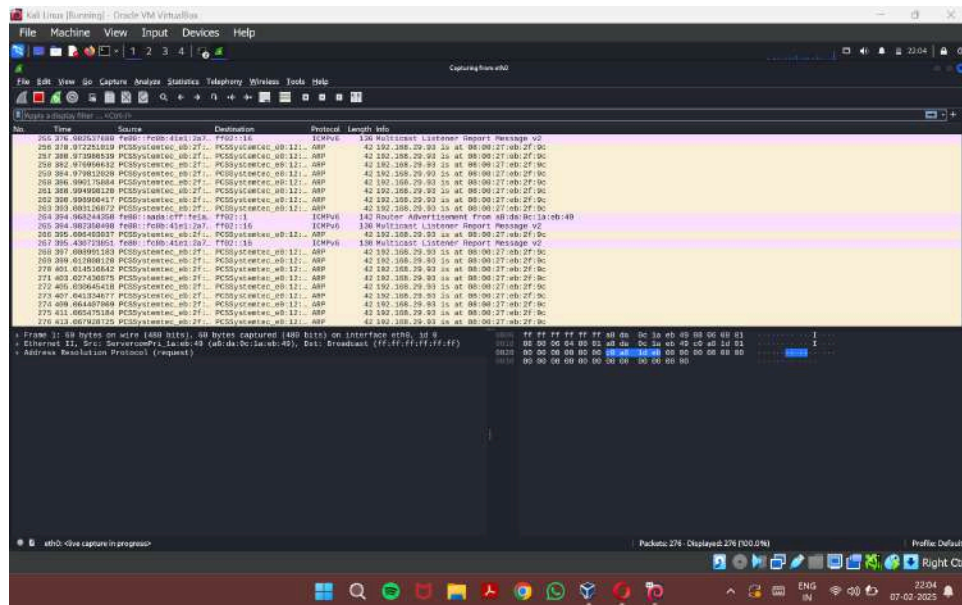
2. Start Wireshark in Kali Linux

The screenshot shows the Wireshark interface with a packet capture on the eth0 interface. The packet list shows a frame from 192.168.29.93 to 192.168.29.255. The packet details show Ethernet II, Internet Protocol Version 4, and Address Resolution Protocol (request). The packet bytes show the raw data in hexadecimal and ASCII.

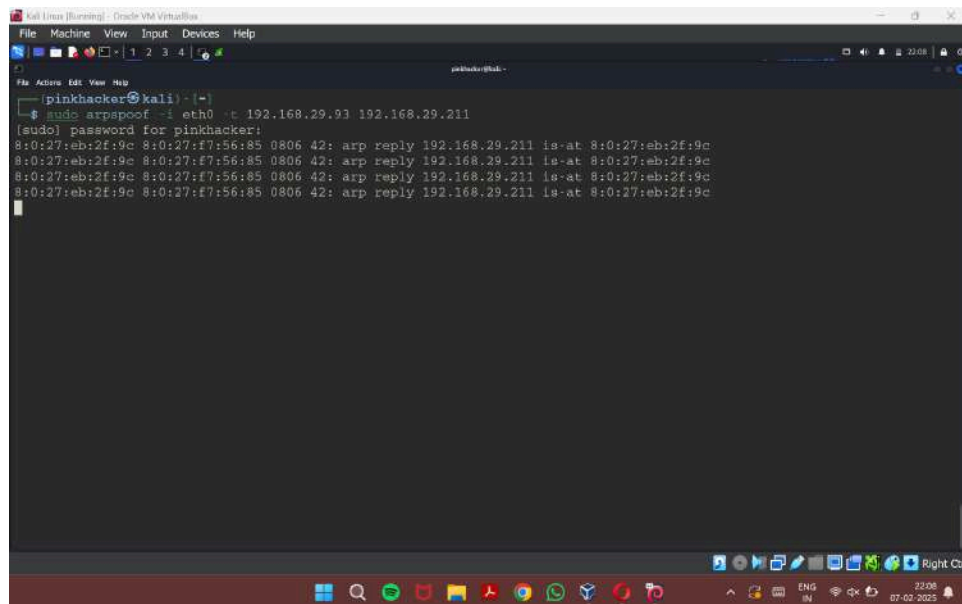


Dhevatha S P
22BCE0826

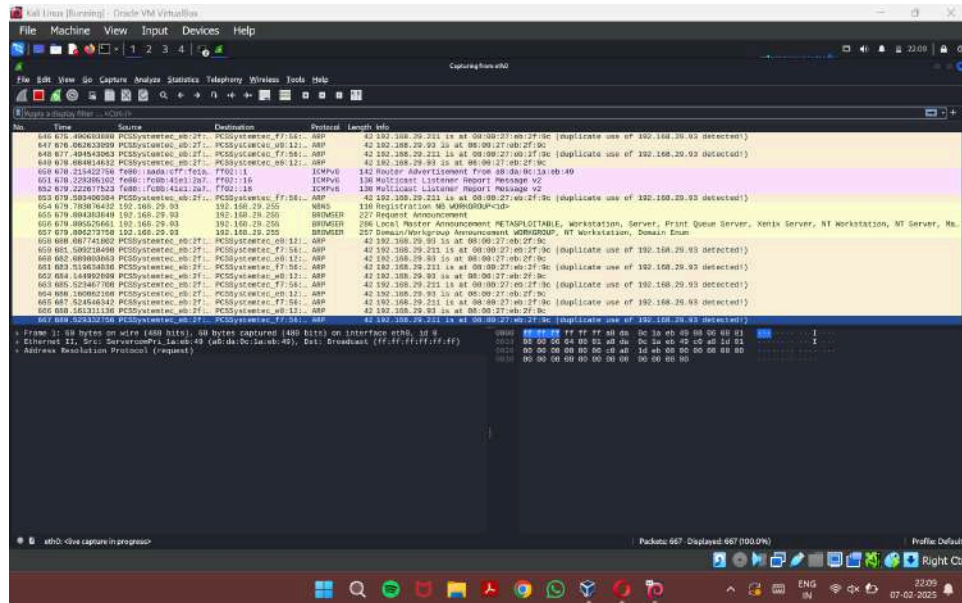
Wireshark in parallel



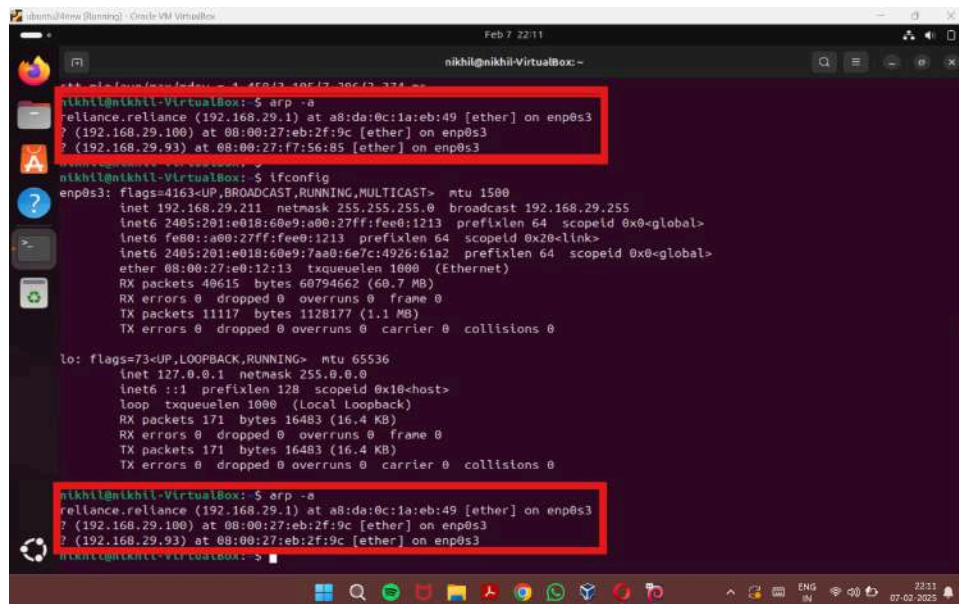
4. Repeating step 3 for the reverse communication



Wireshark in parallel



5. Result of spoofing in Ubuntu machine

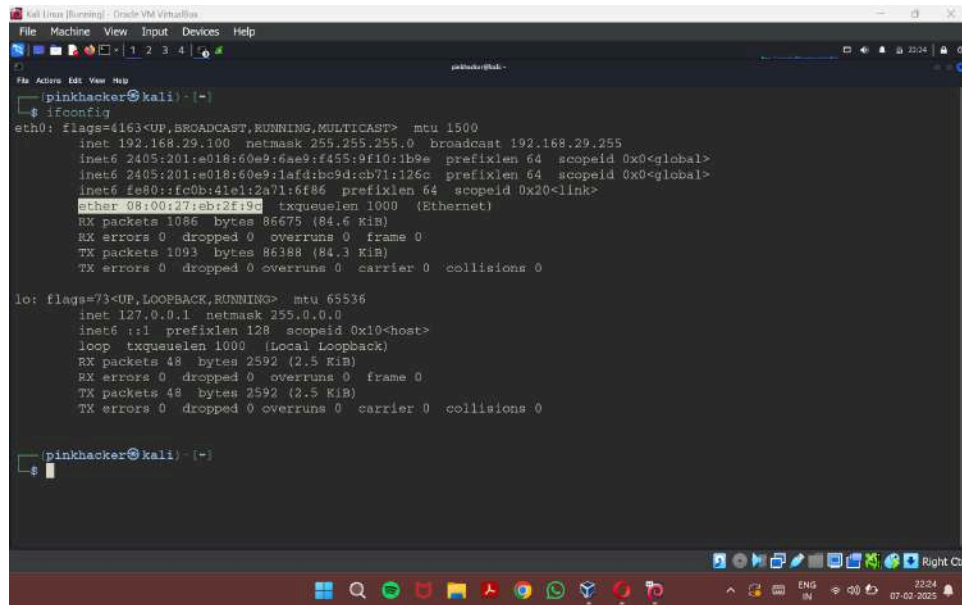


The change in the MAC Address before and after the spoofing, meaning all the pings or messages from the ubuntu machine is

Dhevatha S P
22BCE0826

forwarded to the Kali Linux machine and not the metasploitable2.

MAC address of Kali Linux machine.



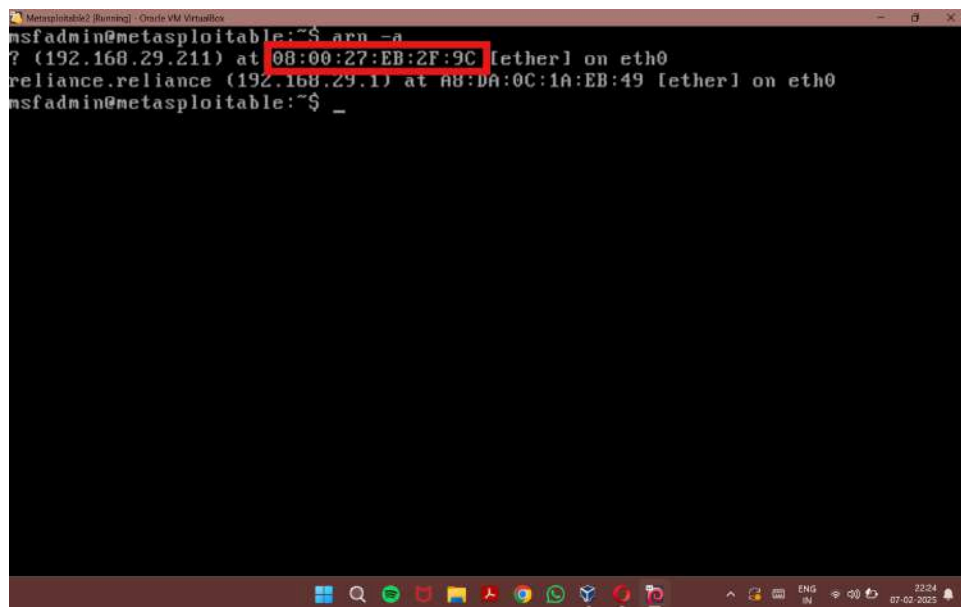
```

(pinkhacker@kali) ~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.29.100 netmask 255.255.255.0 broadcast 192.168.29.255
    inet6 2405:201:e018:60e9:6ae9:f455:9f10:1b9e prefixlen 64 scopeid 0x0<global>
    inet6 2405:201:e018:60e9:1afd:bc9d:cb71:126c prefixlen 64 scopeid 0x0<global>
    inet6 fe80::fc0b:41e1:2a71:6f86 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:EB:2F:9C txqueuelen 1000 (Ethernet)
    RX packets 1086 bytes 86675 (84.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1093 bytes 86388 (84.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

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 48 bytes 2592 (2.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 48 bytes 2592 (2.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(pinkhacker@kali) ~$
  
```

ARP configuration of the Metasploitable2.



```

msfadmin@metasploitable2:~$ arp -a
? (192.168.29.111) at 08:00:27:EB:2F:9C [ether] on eth0
reliance.reliance (192.168.29.1) at AB:DA:0C:1A:EB:49 [ether] on eth0
msfadmin@metasploitable2:~$ _
  
```