

Practical No.3

Aim: Linux Network Analysis and ARP Poisoning

1. Linux Network Analysis:

- Execute the ifconfig command to retrieve network interface information.
- Use the ping command to test network connectivity and analyze the output.
- Analyze the netstat command output to view active network connections.
- Perform a traceroute to trace the route packets take to reach a target host.

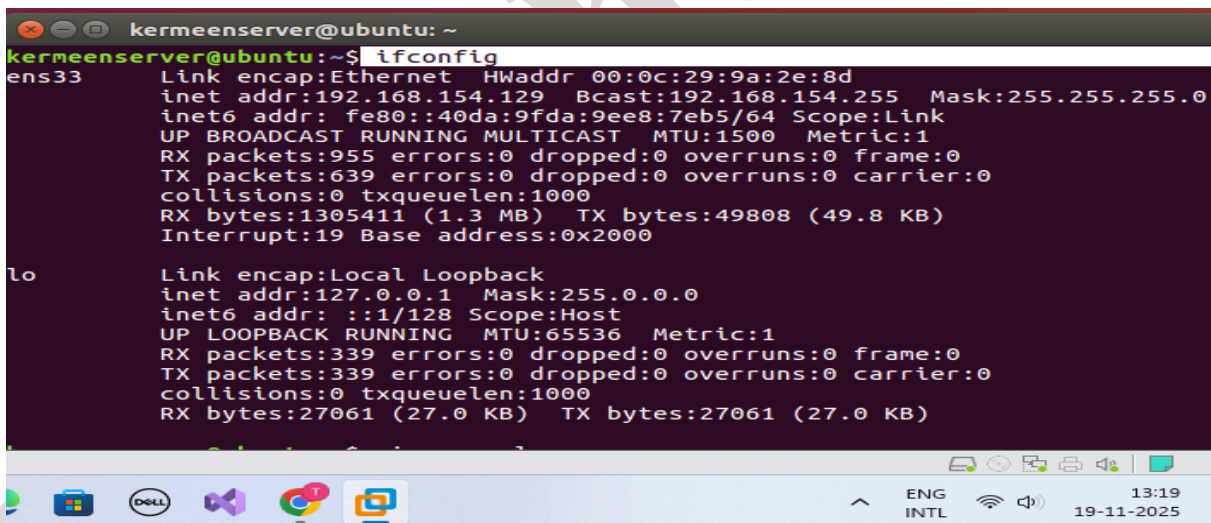
2. ARP Poisoning:

- Use ARP poisoning techniques to redirect network traffic on a Windows system.
- Analyze the effects of ARP poisoning on network communication and security.

A Linux Network Analysis:

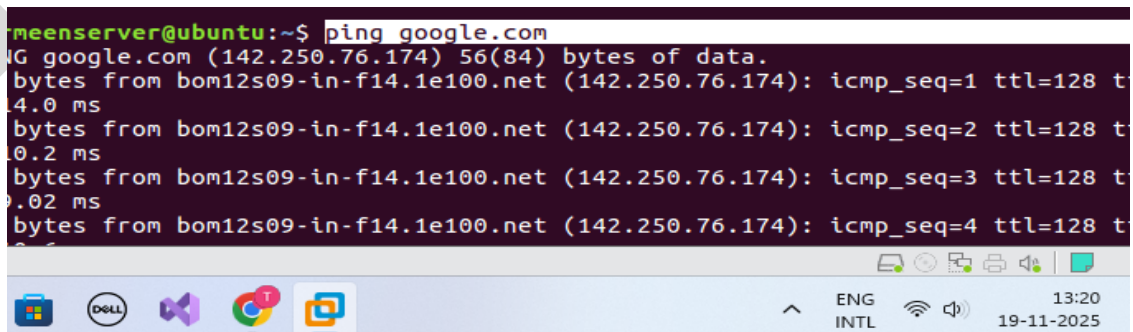
Linux:

1) ifconfig



```
kermeenserver@ubuntu: ~  
kermeenserver@ubuntu:~$ ifconfig  
ens33      Link encap:Ethernet  HWaddr 00:0c:29:9a:2e:8d  
            inet addr:192.168.154.129  Bcast:192.168.154.255  Mask:255.255.255.0  
            inet6 addr: fe80::40da:9fda:9ee8:7eb5/64 Scope:Link  
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
            RX packets:955 errors:0 dropped:0 overruns:0 frame:0  
            TX packets:639 errors:0 dropped:0 overruns:0 carrier:0  
            collisions:0 txqueuelen:1000  
            RX bytes:1305411 (1.3 MB)  TX bytes:49808 (49.8 KB)  
            Interrupt:19 Base address:0x2000  
  
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:65536  Metric:1  
            RX packets:339 errors:0 dropped:0 overruns:0 frame:0  
            TX packets:339 errors:0 dropped:0 overruns:0 carrier:0  
            collisions:0 txqueuelen:1000  
            RX bytes:27061 (27.0 KB)  TX bytes:27061 (27.0 KB)
```

2) ping google.com



```
meenserver@ubuntu:~$ ping google.com  
PING google.com (142.250.76.174) 56(84) bytes of data:  
bytes from bom12s09-in-f14.1e100.net (142.250.76.174): icmp_seq=1 ttl=128 t  
4.0 ms  
bytes from bom12s09-in-f14.1e100.net (142.250.76.174): icmp_seq=2 ttl=128 t  
0.2 ms  
bytes from bom12s09-in-f14.1e100.net (142.250.76.174): icmp_seq=3 ttl=128 t  
0.02 ms  
bytes from bom12s09-in-f14.1e100.net (142.250.76.174): icmp_seq=4 ttl=128 t
```

3) netstat

```
kermeenserver@ubuntu:~$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags               Type                   State                  I-Node   Path
unix    2      [ ]                 DGRAM                  25434          /run/user/1000/systemd/notify
unix    2      [ ]                 DGRAM                  14649          /run/systemd/cgroups-agent
unix   19      [ ]                 DGRAM                  14654          /run/systemd/journal/dev-log
unix    2      [ ]                 DGRAM                  22263          /var/lib/samba/private/msg.sock/1487
```

4) traceroute [google.com](https://www.google.com)

```
kermeenserver@ubuntu:~$ sudo apt install traceroute
[sudo] password for kermeenserver:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  php-ldap php7.0-ldap snapd-login-service
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  traceroute
0 upgraded, 1 newly installed, 0 to remove and 101 not upgraded.
```

```
kermeenserver@ubuntu:~$ traceroute google.com
traceroute to google.com (142.250.70.46), 30 hops max, 60 byte packets
 1  192.168.154.2 (192.168.154.2)  0.271 ms  0.221 ms  0.192 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
```

Windows:

1) ipconfig

```
Command Prompt
C:\Users\itlab>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 3:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 4:
```

2) ping

```
C:\Users\itlab>ping

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
           [-r count] [-s count] [[-j host-list] | [-k host-list]]
           [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
           [-4] [-6] target_name

Options:
    -t             Ping the specified host until stopped.
                   To see statistics and continue - type Control-Break;
                   To stop - type Control-C.
    -a             Resolve addresses to hostnames.
    -n count       Number of echo requests to send.
    -l size        Send buffer size.
    -f             Set Don't Fragment flag in packet (IPv4-only).
    -i TTL         Time To Live.
    -v TOS         Type Of Service (IPv4-only. This setting has been deprecated)
```

3) netstat

```
C:\Users\itlab>netstat

Active Connections

Proto Local Address           Foreign Address         State
TCP    127.0.0.1:49285          IT:49286                ESTABLISHED
TCP    127.0.0.1:49286          IT:49285                ESTABLISHED
TCP    127.0.0.1:49287          IT:49288                ESTABLISHED
TCP    127.0.0.1:49288          IT:49287                ESTABLISHED
TCP    127.0.0.1:53064          IT:53065                ESTABLISHED
TCP    127.0.0.1:53065          IT:53064                ESTABLISHED
TCP    127.0.0.1:57085          IT:57086                ESTABLISHED
TCP    127.0.0.1:57086          IT:57085                ESTABLISHED
TCP    127.0.0.1:62704          IT:62705                ESTABLISHED
TCP    127.0.0.1:62705          IT:62704                ESTABLISHED
TCP    192.168.29.211:49688     4.213.25.242:https      ESTABLISHED
TCP    192.168.29.211:51380     20.190.145.140:https    TIME_WAIT
```

4) tracert www.google.com

```
C:\Users\itlab>tracert www.google.com

Tracing route to www.google.com [2404:6800:4009:812::2004]
over a maximum of 30 hops:

 1      2 ms      2 ms      2 ms  2405:201:5:8868:aada:cff:fe04:cf52
 2      *        *        *      Request timed out.
 3     10 ms     10 ms     11 ms  2405:203:400:100:172:31:2:24
 4      8 ms      7 ms      7 ms  2405:200:801:c00::1244
 5      6 ms      5 ms      7 ms  2405:200:803:3168:61::7
 6      *        *        *      Request timed out.
 7     14 ms      6 ms     10 ms  2405:200:801:c00::1232
 8      *

Taskbar icons: [Icons for various applications including Edge, File Explorer, and others]
System tray: ENG INTL, 13:32, 19-11-2025
```