| Student Name | Shreya Dhameja |
|---|---|
| SRN No | 202202178 |
| Roll No | 40 |
| Program | Computer Engg. |
| Year | Third Year |
| Division | F |
| Subject | Computer Network Laboratory (BTECCE22506) |
| Assignment No | 2 |

## Assignment Number - 02

**Title :** Study of Linux and Windows Network commands

**Problem Statement** Studying Linux and Windows network commands. [ ping, pathping, ipconfig/ifconfig, arp, netstat, nbtstat, nslookup, route, traceroute/tracert, nmap, etc]

**Try to execute following commands on linux terminal or Windows command prompt.**

- o **Ipconfig / ifconfig**
- o **ping**
- o **Tracert/Traceroute/Tracepath**
- o **Finger**
- o **NSlookup**
- o **Netstat**
- o **Hostname**
- o **Port Scan / nmap**
- o **Arp  Route**
- o **Whois**

**Theory :**

1. **ifconfig**:

● Displays or configures a network interface.

● Usage : ifconfig

```
┌──(kali㉿kali)-[/home/kali]
└─PS> ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.100.4  netmask 255.255.255.0  broadcast 192.168.100.255
        inet6 fe80::f63:d5cd:158d:508d  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:21:b1:d0  txqueuelen 1000  (Ethernet)
        RX packets 3  bytes 710 (710.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 21  bytes 2972 (2.9 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 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

**2.ip**:

- Shows/manipulates routing, devices, policy routing, and tunnels.

- Usage : ip addr, ip route, ip link

```
┌──(kali㊉kali)-[/home/kali]
└─PS> ip
Usage: ip [ OPTIONS ] OBJECT { COMMAND | help }
       ip [ -force ] -batch filename
where  OBJECT := { address | addrlabel | amt | fou | help | ila | ioam | l2tp |
                   link | macsec | maddress | monitor | mptcp | mroute | mrule |
                   neighbor | neighbour | netconf | netns | nexthop | ntable |
                   ntbl | route | rule | sr | tap | tcpmetrics |
                   token | tunnel | tuntap | vrf | xfrm }
       OPTIONS := { -V[ersion] | -s[tatistics] | -d[etails] | -r[esolve] |
                    -h[uman-readable] | -iec | -j[son] | -p[retty] |
                    -f[amily] { inet | inet6 | mpls | bridge | link } |
                    -4 | -6 | -M | -B | -0 |
                    -l[oops] { maximum-addr-flush-attempts } | -br[ief] |
                    -o[neline] | -t[imestamp] | -ts[hort] | -b[atch] [filename] |
                    -rc[vbuf] [size] | -n[etns] name | -N[umeric] | -a[ll] |
                    -c[olor]}
```

**3.traceroute**:

- Prints the route packets take to the network host.

- Usage : traceroute <destination>

```
┌──(kali㊉kali)-[/home/kali]
└─PS> traceroute kali -4
traceroute to kali (127.0.1.1), 30 hops max, 60 byte packets
 1  kali (127.0.1.1)  0.025 ms  0.004 ms  0.004 ms
```

**4.tracepath**:
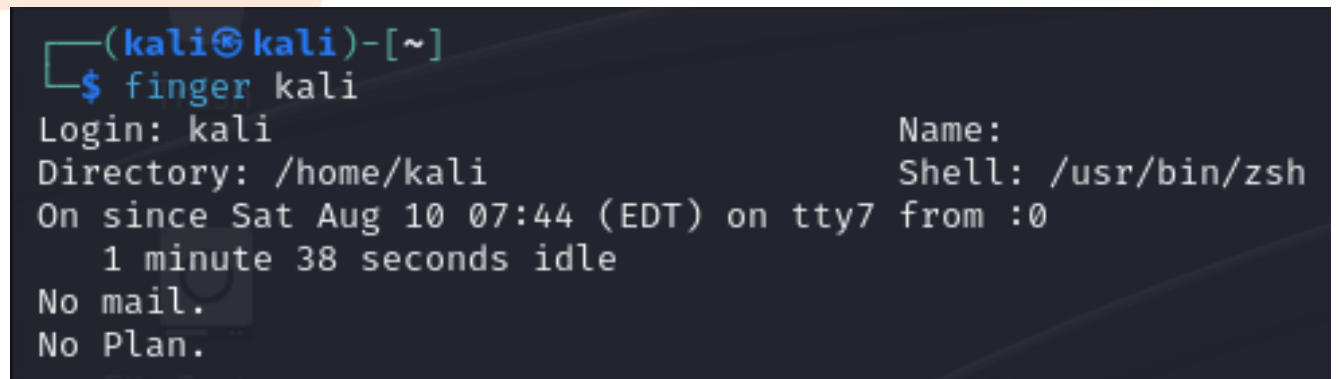
● Traces the path to a network host discovering the MTU along this path.

● Usage : tracepath <destination>

```
File  Actions  Edit  View  Help

┌──(kali㊉kali)-[/home/kali]
└─PS> tracepath -b www.google.com
1?: [LOCALHOST]                        pmtu 1500
1:  192.168.100.1 (192.168.100.1)                        0.659ms
1:  192.168.100.1 (192.168.100.1)                        0.644ms
2:  no reply
3:  no reply
```

**5. Finger:**

● Provides information about users on the system or network. (Note: finger may not be installed by default on some systems.)

● Usage : finger username

```
┌──(kali㊉kali)-[~]
└─$ finger kali
Login: kali                        Name:
Directory: /home/kali              Shell: /usr/bin/zsh
On since Sat Aug 10 07:44 (EDT) on tty7 from :0
   1 minute 38 seconds idle
No mail.
No Plan.
```

**5.ping**:

- Sends ICMP ECHO_REQUEST to network hosts to check their reachability.

- Usage : ping <hostname or IP>



**6.netstat**:

- Displays network connections, routing tables, interface statistics, masquerade connections, and multicast memberships.

- Usage : netstat -a, netstat -r, netstat -I

**7.ss:**

- Utility to investigate sockets.

- Usage : ss -tuln, ss -s

**8.dig**:

- Queries DNS servers for information about host addresses, mail exchanges, name servers, and related information.

- Usage: dig <domain>



**9.nslookup**:

- Queries the DNS to obtain domain name or IP address mapping.

- Usage: nslookup <domain>

**10.nmap**:

- Network exploration tool and security/port scanner.

- Usage: nmap <options> <target>

```
┌──(kali㊉kali)-[/home/kali]
└─PS> nmap -v -sn 192.168.0.0
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-10 06:59 EDT
Initiating Ping Scan at 06:59
Scanning 192.168.0.0 [2 ports]
Completed Ping Scan at 06:59, 3.01s elapsed (1 total hosts)
Nmap scan report for 192.168.0.0 [host down]
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.02 seconds
```

**11.host**:

- Simple utility for performing DNS lookups.

- Usage: host <domain>

```
┌──(kali㊉kali)-[/home/kali]
└─PS> host www.google.com
www.google.com has address 142.250.67.164
www.google.com has IPv6 address 2404:6800:4009:820::2004
```

**12.arp**:

- Displays and modifies the ARP (Address Resolution Protocol) cache.
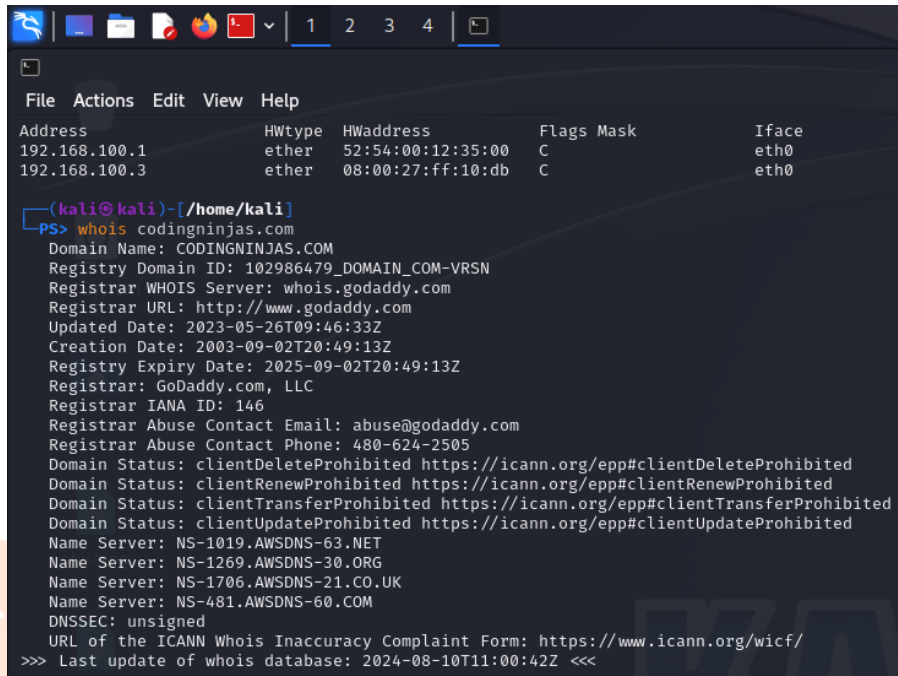
- Usage: arp -a, arp -d <IP>

```
┌──(kali㊉kali)-[/home/kali]
└─PS> arp
Address                 HWtype  HWaddress           Flags Mask            Iface
192.168.100.1           ether   52:54:00:12:35:00   C                     eth0
192.168.100.3           ether   08:00:27:ff:10:db   C                     eth0
```

**13.whois**:

- Queries the WHOIS database for information about domain names and IP address blocks.

- Usage: whois <domain>



**Conclusion :** In this assignment, we explored a variety of network commands used in both Linux and Windows environments to manage and troubleshoot network configurations. Each command provides unique functionality and is crucial for different aspects of network administration and diagnostic processes.