

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]

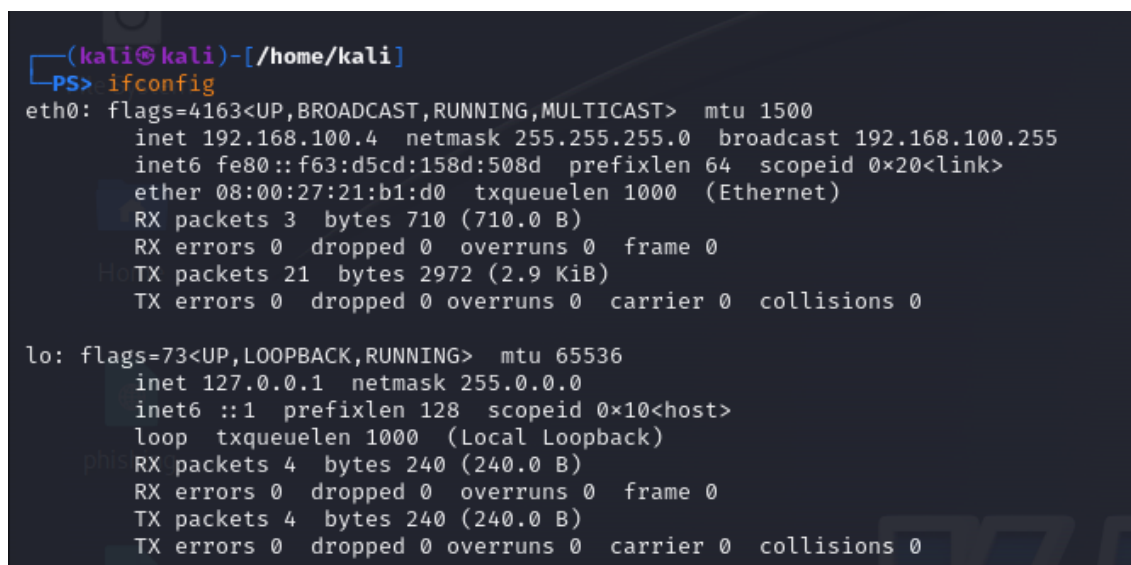
Try to execute following commands on linux terminal or Windows command prompt.

- Ipconfig / ifconfig
- ping
- Tracert/Traceroute/Tracepath
- Finger
- NSlookup
- Netstat
- Hostname
- Port Scan / nmap
- Arp Route
- 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 0x20<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 0x10<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

```
(kali㉿kali)-[/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>

```
(kali㉿kali)-[/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:

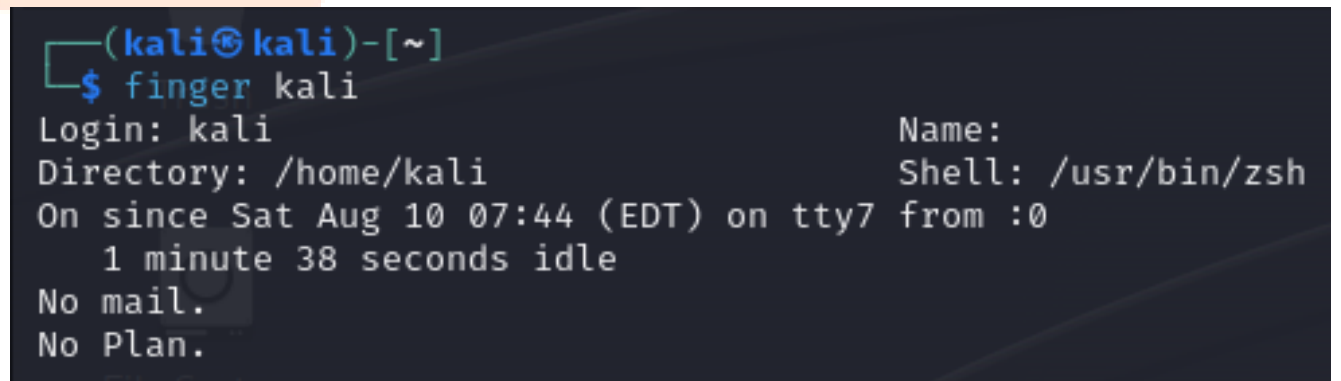
- Traces the path to a network host discovering the MTU along this path.
- Usage : tracepath <destination>



```
(kali㉿kali)-[/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:

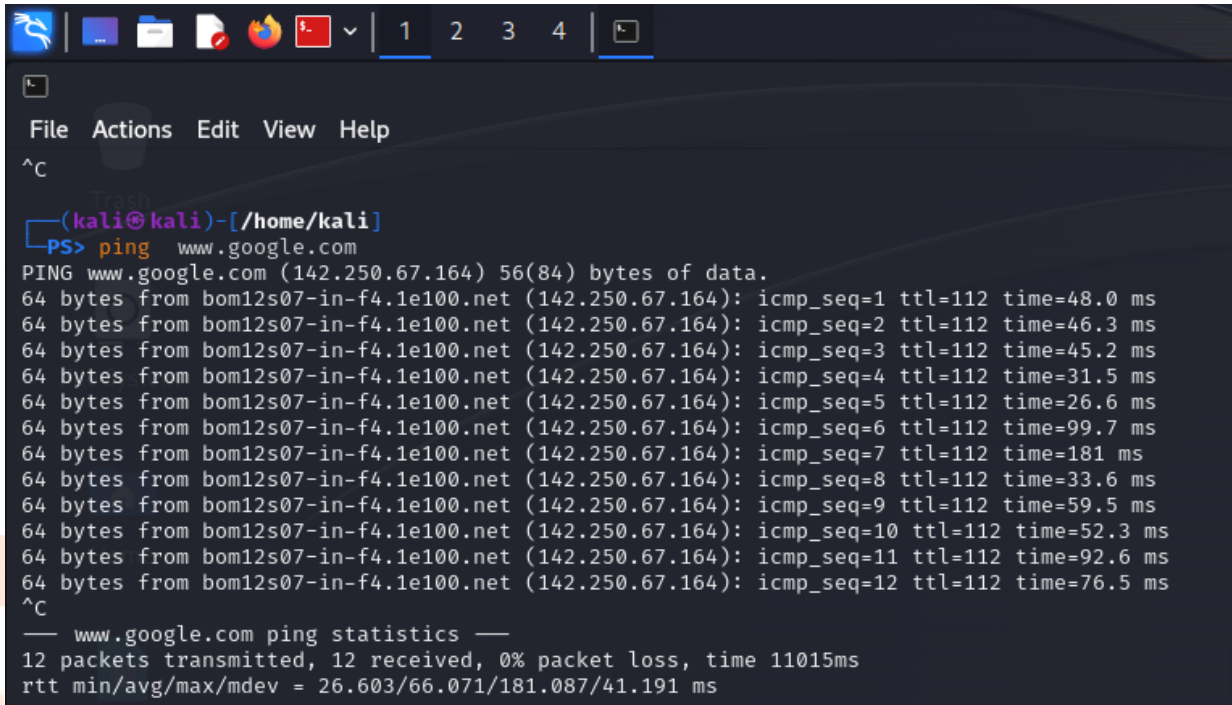
- Provides information about users on the system or network. (Note: finger may not be installed by default on some systems.)
- Usage : finger username



```
(kali㉿kali)-[~]
$ 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>



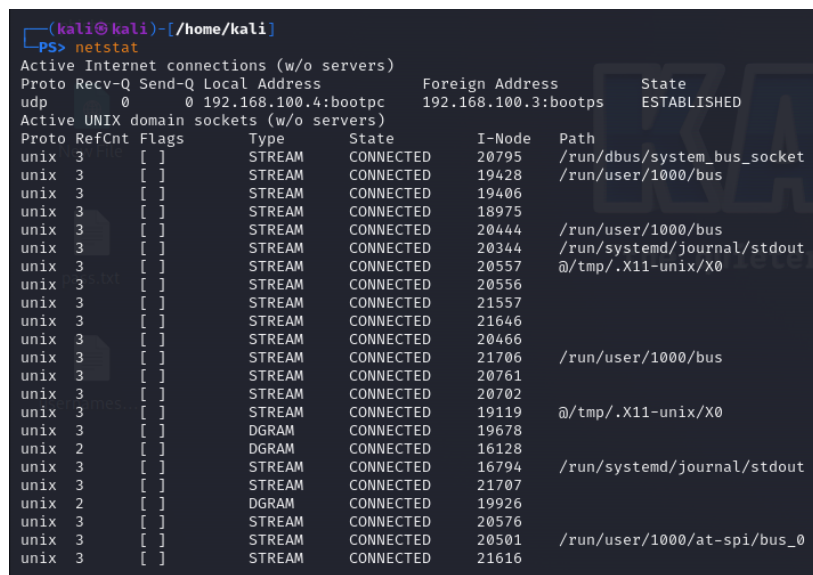
```

(kali@kali)-[/home/kali]
PS> ping www.google.com
PING www.google.com (142.250.67.164) 56(84) bytes of data.
64 bytes from bom12s07-in-f4.1e100.net (142.250.67.164): icmp_seq=1 ttl=112 time=48.0 ms
64 bytes from bom12s07-in-f4.1e100.net (142.250.67.164): icmp_seq=2 ttl=112 time=46.3 ms
64 bytes from bom12s07-in-f4.1e100.net (142.250.67.164): icmp_seq=3 ttl=112 time=45.2 ms
64 bytes from bom12s07-in-f4.1e100.net (142.250.67.164): icmp_seq=4 ttl=112 time=31.5 ms
64 bytes from bom12s07-in-f4.1e100.net (142.250.67.164): icmp_seq=5 ttl=112 time=26.6 ms
64 bytes from bom12s07-in-f4.1e100.net (142.250.67.164): icmp_seq=6 ttl=112 time=99.7 ms
64 bytes from bom12s07-in-f4.1e100.net (142.250.67.164): icmp_seq=7 ttl=112 time=181 ms
64 bytes from bom12s07-in-f4.1e100.net (142.250.67.164): icmp_seq=8 ttl=112 time=33.6 ms
64 bytes from bom12s07-in-f4.1e100.net (142.250.67.164): icmp_seq=9 ttl=112 time=59.5 ms
64 bytes from bom12s07-in-f4.1e100.net (142.250.67.164): icmp_seq=10 ttl=112 time=52.3 ms
64 bytes from bom12s07-in-f4.1e100.net (142.250.67.164): icmp_seq=11 ttl=112 time=92.6 ms
64 bytes from bom12s07-in-f4.1e100.net (142.250.67.164): icmp_seq=12 ttl=112 time=76.5 ms
^C
--- www.google.com ping statistics ---
12 packets transmitted, 12 received, 0% packet loss, time 11015ms
rtt min/avg/max/mdev = 26.603/66.071/181.087/41.191 ms

```

6.netstat:

- Displays network connections, routing tables, interface statistics, masquerade connections, and multicast memberships.
- Usage : netstat -a, netstat -r, netstat -l



```

(kali@kali)-[/home/kali]
PS> netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 192.168.100.4:bootpc    192.168.100.3:bootps    ESTABLISHED

Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags   Type       State           I-Node    Path
unix    3      [ ]     STREAM    CONNECTED      20795      /run/dbus/system_bus_socket
unix    3      [ ]     STREAM    CONNECTED      19428      /run/user/1000/bus
unix    3      [ ]     STREAM    CONNECTED      19406
unix    3      [ ]     STREAM    CONNECTED      18975
unix    3      [ ]     STREAM    CONNECTED      20444      /run/user/1000/bus
unix    3      [ ]     STREAM    CONNECTED      20344      /run/systemd/journal/stdout
unix    3      [ ]     STREAM    CONNECTED      20557      @/tmp/.X11-unix/X0
unix    3      [ ]     STREAM    CONNECTED      20556
unix    3      [ ]     STREAM    CONNECTED      21557
unix    3      [ ]     STREAM    CONNECTED      21646
unix    3      [ ]     STREAM    CONNECTED      20466
unix    3      [ ]     STREAM    CONNECTED      21706      /run/user/1000/bus
unix    3      [ ]     STREAM    CONNECTED      20761
unix    3      [ ]     STREAM    CONNECTED      20702
unix    3      [ ]     STREAM    CONNECTED      19119      @/tmp/.X11-unix/X0
unix    3      [ ]     DGRAM     CONNECTED      19678
unix    2      [ ]     DGRAM     CONNECTED      16128
unix    3      [ ]     STREAM    CONNECTED      16794      /run/systemd/journal/stdout
unix    3      [ ]     STREAM    CONNECTED      21707
unix    2      [ ]     DGRAM     CONNECTED      19926
unix    3      [ ]     STREAM    CONNECTED      20576
unix    3      [ ]     STREAM    CONNECTED      20501      /run/user/1000/at-spi/bus_0
unix    3      [ ]     STREAM    CONNECTED      21616

```

```

File Actions Edit View Help
unix 3 [ ] STREAM CONNECTED 20119 @621f89544b5c9add/bus/systemd/bus-api-user

PS: netstat -a
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address State
udp 0 0 192.168.100.4:bootpc 192.168.100.3:bootps ESTABLISHED
raw6 0 0 [::]:ipv6-icmp [::]:* 7

Active UNIX domain sockets (servers and established)
Proto RefCnt Flags Type State I-Node Path
unix 3 [ ] STREAM CONNECTED 20795 /run/dbus/system_bus_socket
unix 3 [ ] STREAM CONNECTED 19428 /run/user/1000/bus
unix 3 [ ] STREAM CONNECTED 19406
unix 3 [ ] STREAM CONNECTED 18975
unix 3 [ ] STREAM CONNECTED 20444 /run/user/1000/bus
unix 3 [ ] STREAM CONNECTED 20344 /run/systemd/journal/stdout
unix 3 [ ] STREAM CONNECTED 20557 @/tmp/.X11-unix/X0
unix 3 [ ] STREAM CONNECTED 20556
unix 3 [ ] STREAM CONNECTED 21557
unix 3 [ ] STREAM CONNECTED 21646
unix 3 [ ] STREAM CONNECTED 20466
unix 3 [ ] STREAM CONNECTED 21706 /run/user/1000/bus
unix 3 [ ] STREAM CONNECTED 20761
unix 3 [ ] STREAM CONNECTED 20702
unix 3 [ ] STREAM CONNECTED 19119 @/tmp/.X11-unix/X0
unix 3 [ ] DGRAM CONNECTED 19678
unix 2 [ ] STREAM LISTENING 18552 /tmp/.X11-unix/X0
unix 2 [ ] DGRAM CONNECTED 16128
unix 3 [ ] STREAM CONNECTED 16794 /run/systemd/journal/stdout
unix 3 [ ] STREAM CONNECTED 21707
unix 2 [ ] DGRAM CONNECTED 19926
unix 3 [ ] STREAM CONNECTED 20576
unix 3 [ ] STREAM CONNECTED 20501 /run/user/1000/at-spi/bus_0
unix 3 [ ] STREAM CONNECTED 21616
unix 3 [ ] STREAM CONNECTED 19263 /run/user/1000/bus
unix 3 [ ] STREAM CONNECTED 21746
unix 2 [ ] STREAM LISTENING 20300 /tmp/ssh-TbvLRb1z3qW5/agent.857
unix 3 [ ] STREAM CONNECTED 19407 @/tmp/.ICE-unix/857
unix 3 [ ] STREAM CONNECTED 19325 /run/user/1000/bus
unix 3 [ ] STREAM CONNECTED 20793 /run/user/1000/bus
unix 3 [ ] STREAM CONNECTED 20079 /run/systemd/journal/stdout
unix 2 [ ] STREAM LISTENING 21318 /tmp/dbus-wqab7Cdqpf
unix 3 [ ] STREAM CONNECTED 19363
unix 3 [ ] STREAM CONNECTED 20520 @/tmp/.X11-unix/X0
unix 2 [ ] STREAM LISTENING 20377 /tmp/.ICE-unix/857
unix 3 [ ] STREAM CONNECTED 20873 /run/user/1000/gvfsd/socket-gy6olTcc
unix 3 [ ] STREAM CONNECTED 20474 /run/systemd/journal/stdout
unix 3 [ ] DGRAM CONNECTED 15805
unix 3 [ ] STREAM CONNECTED 20720 /run/user/1000/bus
unix 3 [ ] STREAM CONNECTED 16164 /run/dbus/system_bus_socket
unix 3 [ ] DGRAM CONNECTED 15916
unix 2 [ ] STREAM LISTENING 21092 /tmp/dotnet-diagnostic-1446-3342-socket

```

7.ss:

- Utility to investigate sockets.
- Usage : ss -tuln, ss -s

```

File Actions Edit View Help
PS: ss
Netid State Recv-Q Send-Q Local Address:Port Peer Address:Port Process
u_str ESTAB 0 0 /run/dbus/system_bus_socket 20795 * 20794
u_str ESTAB 0 0 /run/user/1000/bus 19428 * 20628
u_str ESTAB 0 0 * 19406 * 19407
u_str ESTAB 0 0 * 18975 * 18976
u_str ESTAB 0 0 /run/user/1000/bus 20444 * 20443
u_str ESTAB 0 0 /run/systemd/journal/stdout 20344 * 20343
u_str ESTAB 0 0 @/tmp/.X11-unix/X0 20557 * 19369
u_str ESTAB 0 0 * 20556 * 19367
u_str ESTAB 0 0 * 21557 * 21558
u_str ESTAB 0 0 * 21646 * 20673
u_str ESTAB 0 0 * 20466 * 19294
u_str ESTAB 0 0 /run/user/1000/bus 21706 * 20954
u_str ESTAB 0 0 * 20761 * 20762
u_str ESTAB 0 0 * 20702 * 20783
u_str ESTAB 0 0 @/tmp/.X11-unix/X0 19119 * 19118
u_dgr ESTAB 0 0 * 19678 * 19677
u_dgr ESTAB 0 0 * 16128 * 15451
u_str ESTAB 0 0 /run/systemd/journal/stdout 16794 * 15066
u_str ESTAB 0 0 * 21707 * 20955
u_dgr ESTAB 0 0 * 19926 * 15451
u_str ESTAB 0 0 * 20576 * 19372
u_str ESTAB 0 0 /run/user/1000/at-spi/bus_0 20501 * 19341
u_str ESTAB 0 0 /run/user/1000/bus 21616 * 20810
u_str ESTAB 0 0 * 19263 * 19262
u_str ESTAB 0 0 * 21746 * 21747
u_str ESTAB 0 0 @/tmp/.ICE-unix/857 19407 * 19406
u_str ESTAB 0 0 /run/user/1000/bus 19325 * 19324
u_str ESTAB 0 0 /run/user/1000/bus 20793 * 20792
u_str ESTAB 0 0 /run/systemd/journal/stdout 20079 * 10945
u_str ESTAB 0 0 * 19363 * 19364
u_str ESTAB 0 0 @/tmp/.X11-unix/X0 20520 * 20519
u_str ESTAB 0 0 /run/user/1000/gvfsd/socket-gy6olTcc 20873 * 21846
u_str ESTAB 0 0 /run/systemd/journal/stdout 20474 * 20473
u_str ESTAB 0 0 /run/user/1000/bus 20720 * 20719
u_dgr ESTAB 0 0 /run/dbus/system_bus_socket 16164 * 16163
u_str ESTAB 0 0 * 15916 * 15917
u_dgr ESTAB 0 0 * 15908 * 15451
u_str ESTAB 0 0 /run/systemd/journal/stdout 15805 * 18397
u_str ESTAB 0 0 @/tmp/.X11-unix/X0 21092 * 21095
u_str ESTAB 0 0 * 21573 * 20738
u_str ESTAB 0 0 * 19341 * 20581
u_str ESTAB 0 0 * 20324 * 18995
u_str ESTAB 0 0 * 19397 * 20588
u_str ESTAB 0 0 /run/dbus/system_bus_socket 16400 * 18520
u_str ESTAB 0 0 * 21898 * 21891
u_str ESTAB 0 0 * 20322 * 20323
u_str ESTAB 0 0 * 20371 * 19368
u_str ESTAB 0 0 /run/systemd/journal/stdout 16102 * 16222

```

8.dig:

- Queries DNS servers for information about host addresses, mail exchanges, name servers, and related information.
- Usage: dig <domain>

```

kali@kali: /home/kali
PS> dig
;; global options: cmd
;; Got answer:
;; HEADER= opcode: QUERY, status: NOERROR, id: 41548
;; flags: qr rd ra; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 27

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 1280
;; QUESTION SECTION:
;
IN NS

;; ANSWER SECTION:
. 31745 IN NS h.root-servers.net.
. 31745 IN NS g.root-servers.net.
. 31745 IN NS f.root-servers.net.
. 31745 IN NS a.root-servers.net.
. 31745 IN NS b.root-servers.net.
. 31745 IN NS e.root-servers.net.
. 31745 IN NS d.root-servers.net.
. 31745 IN NS c.root-servers.net.
. 31745 IN NS i.root-servers.net.
. 31745 IN NS j.root-servers.net.
. 31745 IN NS m.root-servers.net.
. 31745 IN NS k.root-servers.net.

;; ADDITIONAL SECTION:
m.root-servers.net. 204544 IN AAAA 2001:dc3::35
l.root-servers.net. 204544 IN AAAA 2001:500:9f::42
k.root-servers.net. 438865 IN AAAA 2001:7fd::1
j.root-servers.net. 438864 IN AAAA 2001:503:c27::2:30
i.root-servers.net. 438864 IN AAAA 2001:7fe::53
h.root-servers.net. 438864 IN AAAA 2001:500:1::53
g.root-servers.net. 438864 IN AAAA 2001:500:12::b0d
f.root-servers.net. 544984 IN AAAA 2001:500:2f::f
e.root-servers.net. 161279 IN AAAA 2001:500:a8::e
d.root-servers.net. 161282 IN AAAA 2001:500:12d::d
c.root-servers.net. 588918 IN AAAA 2001:500:12::c
b.root-servers.net. 588908 IN AAAA 2001:130:18::b
a.root-servers.net. 204543 IN AAAA 2001:503:b30::2:30
w.root-servers.net. 204544 IN AAAA 64:ff9b::c4c:1021
l.root-servers.net. 204544 IN AAAA 64:ff9b::c787:532a
k.root-servers.net. 588932 IN AAAA 64:ff9b::c180:c81
j.root-servers.net. 588916 IN AAAA 64:ff9b::c03a:8816
i.root-servers.net. 588906 IN AAAA 64:ff9b::c024:9411
h.root-servers.net. 588912 IN AAAA 64:ff9b::c011:b035
g.root-servers.net. 588914 IN AAAA 64:ff9b::c070:2a04

```

9.nslookup:

- Queries the DNS to obtain domain name or IP address mapping.
- Usage: nslookup <domain>

```

kali@kali: /home/kali
PS> nslookup
> www.google.com
Server:          192.168.59.147
Address:         192.168.59.147#53

Non-authoritative answer:
Name:   www.google.com
Address: 142.250.67.164
Name:   www.google.com
Address: 2404:6800:4009:820::2004
>

```

10.nmap:

- Network exploration tool and security/port scanner.
- Usage: nmap <options> <target>

```
(kali㉿kali)-[/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>

```
(kali㉿kali)-[/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>

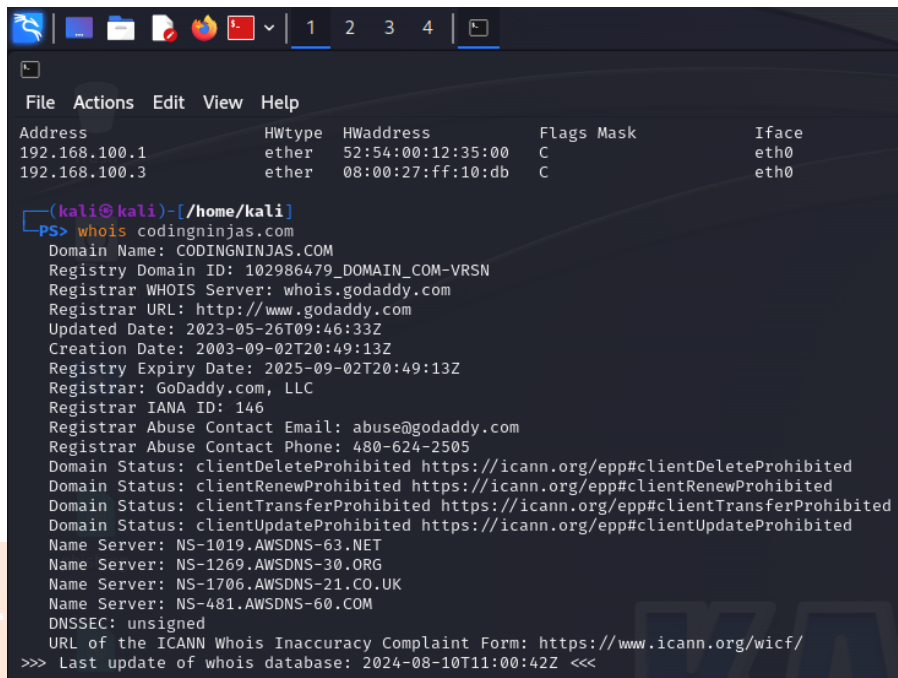
```
(kali㉿kali)-[/home/kali]
PS> arp

```

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>



```
(kali@kali)-[/home/kali]
PS> whois codingninjas.com
Domain Name: CODINGNINJAS.COM
Registry Domain ID: 102986479_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Updated Date: 2023-05-26T09:46:33Z
Creation Date: 2003-09-02T20:49:13Z
Registry Expiry Date: 2025-09-02T20:49:13Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: 480-624-2505
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Name Server: NS-1019.AWSDNS-63.NET
Name Server: NS-1269.AWSDNS-30.ORG
Name Server: NS-1706.AWSDNS-21.CO.UK
Name Server: NS-481.AWSDNS-60.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2024-08-10T11:00:42Z <<<
```

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.