

NAME : SOHAM DOMBALE

MIS NO : 142203005

1. IPCONFIG :

Used to to display the configuration of network interfaces on a local computer. It provides information about the computer's IP (Internet Protocol) address, subnet mask, default gateway, and more.

```
dumascus@dumascus-soham:~$ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
    ether 02:42:53:cb:d0:d5 txqueuelen 0 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    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 3227 bytes 334805 (334.8 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 3227 bytes 334805 (334.8 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlp1s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.43.191 netmask 255.255.255.0 broadcast 192.168.43.255
    inet6 fe80::a30c:27b6:762e:fc4f prefixlen 64 scopeid 0x20<link>
    inet6 2401:4900:5037:d4e6:55e7:47ce:359d:345 prefixlen 64 scopeid 0x0<global>
    inet6 2401:4900:5037:d4e6:8a8a:a960:544d:fedc prefixlen 64 scopeid 0x0<global>
    ether 00:45:e2:d2:e6:13 txqueuelen 1000 (Ethernet)
    RX packets 44749 bytes 32824966 (32.8 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 26766 bytes 5359783 (5.3 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

dumascus@dumascus-soham:~$
```

2. IP :

used to perform a wide range of network-related tasks. It allows you to interact with and configure various aspects of network interfaces, routing tables, and more.

```
dumascus@damascus-soham:~$ ip
Usage: ip [ OPTIONS ] OBJECT { COMMAND | help }
       ip [ -force ] -batch filename
where  OBJECT := { address | addrlabel | 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

Used to trace the route that packets take to reach a destination host on a network. It helps you identify the network hops (routers or intermediate devices) between your computer and the target host.

```
dumascus@damascus-soham:~$ traceroute
Usage:
  traceroute [ -4dFItnreAUDV ] [ -f first_ttl ] [ -g gate,... ] [ -l device ] [ -m max_ttl ] [ -N squerles ] [ -p port ] [ -t tos ] [ -l flow_label ] [ -w MAX,HERE,NEAR ] [ -q nqueries ] [ -s src_addr ]
  [ -z sendwait ] [ --fwmark=num ] host [ packetlen ]
Options:
  -4                      Use IPv4
  -6                      Use IPv6
  -d --debug              Enable socket level debugging
  -F --dont-fragment      Do not fragment packets
  -f first_ttl --first=first_ttl
                          Start from the first_ttl hop (instead from 1)
  -g gate,... --gateway=gate,...
                          Route packets through the specified gateway
                          (maximum 8 for IPv4 and 127 for IPv6)
  -I --icmp               Use ICMP Echo for tracerouting
  -T --tcp                Use TCP SYN for tracerouting (default port is 80)
  -l device --interface=device
                          Specify a network interface to operate with
  -m max_ttl --max-hops=max_ttl
                          Set the max number of hops (max TTL to be
                          reached). Default is 30
  -N squerles --sn=n-queries=squerles
                          Set the number of probes to be tried
                          simultaneously (default is 10)
  -n                      Do not resolve IP addresses to their domain names
  -p port --port=port     Set the destination port to use. It is either
                          initial udp port value for "default" method
                          (incremented by each probe, default is 33434), or
                          initial seq for "icmp" (incremented as well,
                          default from 1), or some constant destination
                          port for other methods (with default of 80 for
                          "tcp", 53 for "udp", etc.)
  -t tos --tos=tos        Set the TOS (IPv4 type of service) or TC (IPv6
                          traffic class) value for outgoing packets
  -l flow_label --flowlabel=flow_label
                          Use specified flow_label for IPv6 packets
  -w MAX,HERE,NEAR --wait=MAX,HERE,NEAR
                          Wait for a probe no more than HERE (default 3)
                          times longer than a response from the same hop,
                          or no more than NEAR (default 10) times than some
                          next hop, or MAX (default 5.0) seconds (float
                          point values allowed too)
  -q nqueries --queries=nqueries
                          Set the number of probes per each hop. Default is
                          3
  -r                      Bypass the normal routing and send directly to a
                          host on an attached network
  -s src_addr --source=src_addr
                          Use source src_addr for outgoing packets
  -z sendwait --sendwait=sendwait
                          Minimal time interval between probes (default 0).
                          If the value is more than 10, then it specifies a
                          number in milliseconds, else it is a number of
                          seconds (float point values allowed too)
  -e --extensions         Show ICMP extensions (if present), including MPLS
  -d --as-path-lookups     Perform AS path lookups in routing registries and
```

4. tracepath:

used to trace the route that packets take to reach a destination host on a network. However, `tracepath` is often available on Linux systems as a simplified version of `traceroute` with a different output format.

```
dumascus@damascus-soham:~$ tracepath

Usage
  tracepath [options] <destination>

Options:
  -4                use IPv4
  -6                use IPv6
  -b                print both name and ip
  -l <length>       use packet <length>
  -m <hops>         use maximum <hops>
  -n                no dns name resolution
  -p <port>         use destination <port>
  -V                print version and exit
  <destination>    dns name or ip address

For more details see tracepath(8).
dumascus@damascus-soham:~$
```

5. ping:

It's used to test the connectivity between your computer and a remote host on a network, typically a web server or another computer

```
dumascus@damascus-soham:~$ ping google.com
PING google.com(bom12s14-in-x0e.1e100.net (2404:6800:4009:827::200e)) 56 data bytes
64 bytes from bom12s14-in-x0e.1e100.net (2404:6800:4009:827::200e): icmp_seq=1 ttl=55 time=389 ms
64 bytes from bom12s14-in-x0e.1e100.net (2404:6800:4009:827::200e): icmp_seq=2 ttl=55 time=227 ms
64 bytes from bom12s14-in-x0e.1e100.net (2404:6800:4009:827::200e): icmp_seq=3 ttl=55 time=250 ms
64 bytes from bom12s14-in-x0e.1e100.net (2404:6800:4009:827::200e): icmp_seq=4 ttl=55 time=272 ms
64 bytes from bom12s14-in-x0e.1e100.net (2404:6800:4009:827::200e): icmp_seq=5 ttl=55 time=295 ms
64 bytes from bom12s14-in-x0e.1e100.net (2404:6800:4009:827::200e): icmp_seq=6 ttl=55 time=75.5 ms
64 bytes from bom12s14-in-x0e.1e100.net (2404:6800:4009:827::200e): icmp_seq=7 ttl=55 time=239 ms
64 bytes from bom12s14-in-x0e.1e100.net (2404:6800:4009:827::200e): icmp_seq=8 ttl=55 time=364 ms
64 bytes from bom12s14-in-x0e.1e100.net (2404:6800:4009:827::200e): icmp_seq=9 ttl=55 time=388 ms
64 bytes from bom12s14-in-x0e.1e100.net (2404:6800:4009:827::200e): icmp_seq=10 ttl=55 time=207 ms
```

6.netstat:

It is used to display network-related information, including network connections, routing tables, interface statistics, and more.

```
dumascus@damascus-soham:~$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address          Foreign Address         State
tcp        0      0 damascus-soham:47736   52.139.250.209:https    ESTABLISHED
tcp        0      0 damascus-soham:53806   server-54-239-216:https ESTABLISHED
tcp        0      0 damascus-soham:54660   ec2-3-227-82-29.c:https ESTABLISHED
tcp        0      0 damascus-soham:47726   52.139.250.209:https    ESTABLISHED
tcp        0      0 damascus-soham:58982   52.139.250.209:https    ESTABLISHED
tcp6       0      0 damascus-soham:58244   2a04:4e42:24::485:https ESTABLISHED
tcp6       0      0 damascus-soham:51700   sc-in-xbc.1e100.net:5228 ESTABLISHED
udp        0      0 damascus-soham:bootpc  _gateway:bootps        ESTABLISHED

Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix    3      [ ]       SEQPACKET  CONNECTED    28645     @7d000
unix    3      [ ]       SEQPACKET  CONNECTED    41158     @3b911
unix    2      [ ]       DGRAM      CONNECTED    77333     /run/wpa_supplicant/wlp1s0
unix    2      [ ]       DGRAM      CONNECTED    28407     /run/user/1000/systemd/notify
unix    2      [ ]       DGRAM      CONNECTED    27431     @a6db7
unix    3      [ ]       SEQPACKET  CONNECTED    41156     @0bc6a
unix    5      [ ]       DGRAM      CONNECTED    21991     /run/systemd/notify
unix    2      [ ]       DGRAM      CONNECTED    22007     /run/systemd/journal/syslog
unix    19      [ ]       DGRAM      CONNECTED    22016     /run/systemd/journal/dev-log
unix    10      [ ]       DGRAM      CONNECTED    22018     /run/systemd/journal/socket
unix    3      [ ]       SEQPACKET  CONNECTED    41150     @30a8b
unix    3      [ ]       SEQPACKET  CONNECTED    41151     @a4146
unix    3      [ ]       SEQPACKET  CONNECTED    28644     @3812c
unix    3      [ ]       STREAM     CONNECTED    73511
unix    3      [ ]       STREAM     CONNECTED    28627
unix    3      [ ]       STREAM     CONNECTED    35003
unix    3      [ ]       STREAM     CONNECTED    40163
unix    3      [ ]       STREAM     CONNECTED    39014     /run/user/1000/at-spi/bus
unix    3      [ ]       STREAM     CONNECTED    35104
unix    3      [ ]       STREAM     CONNECTED    40016     /run/user/1000/bus
unix    3      [ ]       STREAM     CONNECTED    23503
unix    3      [ ]       STREAM     CONNECTED    20406
unix    3      [ ]       STREAM     CONNECTED    28618
unix    3      [ ]       STREAM     CONNECTED    35033
unix    3      [ ]       STREAM     CONNECTED    34643
unix    3      [ ]       STREAM     CONNECTED    20204
unix    3      [ ]       STREAM     CONNECTED    27770     /run/systemd/journal/stdout
unix    3      [ ]       STREAM     CONNECTED    85026
unix    3      [ ]       STREAM     CONNECTED    41985     /run/user/1000/bus
unix    3      [ ]       STREAM     CONNECTED    16236     /run/dbus/system_bus_socket
unix    3      [ ]       STREAM     CONNECTED    38285     /run/user/1000/at-spi/bus
unix    3      [ ]       STREAM     CONNECTED    39064
unix    3      [ ]       STREAM     CONNECTED    41068     /run/systemd/journal/stdout
unix    3      [ ]       STREAM     CONNECTED    35140     /run/user/1000/at-spi/bus
unix    3      [ ]       STREAM     CONNECTED    35124
unix    3      [ ]       STREAM     CONNECTED    41055
unix    3      [ ]       STREAM     CONNECTED    43083
unix    3      [ ]       STREAM     CONNECTED    34650
unix    3      [ ]       STREAM     CONNECTED    35013
unix    3      [ ]       STREAM     CONNECTED    28079     /run/systemd/journal/stdout
unix    3      [ ]       STREAM     CONNECTED    36547     /run/user/1000/bus
unix    3      [ ]       STREAM     CONNECTED    34884     /run/systemd/journal/stdout
unix    3      [ ]       DGRAM      CONNECTED    28488
```

7.nslookup:

It is used to perform DNS (Domain Name System) lookups to query DNS servers and retrieve information about domain names or IP addresses.

```
dumascus@damascus-soham:~$ nslookup google.com
Server:          127.0.0.53
Address:         127.0.0.53#53

Non-authoritative answer:
Name:   google.com
Address: 172.217.166.46
Name:   google.com
Address: 2404:6800:4009:811::200e

dumascus@damascus-soham:~$
```

8.dig :

It is used to perform various DNS-related queries, such as looking up DNS records, resolving domain names to IP addresses, and querying DNS servers.

```
dumascus@damascus-soham:~$ dig

; <<>> DiG 9.18.12-0ubuntu0.22.04.2-Ubuntu <<>>
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 33725
;; flags: qr rd ra; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 14

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
; .                        IN      NS

;; ANSWER SECTION:
.                9587    IN      NS      g.root-servers.net.
.                9587    IN      NS      j.root-servers.net.
.                9587    IN      NS      e.root-servers.net.
.                9587    IN      NS      l.root-servers.net.
.                9587    IN      NS      d.root-servers.net.
.                9587    IN      NS      a.root-servers.net.
.                9587    IN      NS      b.root-servers.net.
.                9587    IN      NS      i.root-servers.net.
.                9587    IN      NS      m.root-servers.net.
.                9587    IN      NS      h.root-servers.net.
.                9587    IN      NS      c.root-servers.net.
.                9587    IN      NS      k.root-servers.net.
.                9587    IN      NS      f.root-servers.net.

;; ADDITIONAL SECTION:
g.root-servers.net. 58385   IN      A        192.112.36.4
g.root-servers.net. 58385   IN      AAAA     2001:500:12::d0d
j.root-servers.net. 54824   IN      A        192.58.128.30
j.root-servers.net. 54825   IN      AAAA     2001:503:c27::2:30
e.root-servers.net. 58384   IN      A        192.203.230.10
e.root-servers.net. 58384   IN      AAAA     2001:500:a8::e
l.root-servers.net. 55388   IN      A        199.7.83.42
l.root-servers.net. 55388   IN      AAAA     2001:500:9f::42
d.root-servers.net. 58384   IN      A        199.7.91.13
d.root-servers.net. 58384   IN      AAAA     2001:500:2d::d
a.root-servers.net. 9584    IN      A        198.41.0.4
a.root-servers.net. 9694    IN      AAAA     2001:503:ba3e::2:30
b.root-servers.net. 58383   IN      A        199.9.14.201

;; Query time: 244 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Sun Sep 10 22:36:04 IST 2023
;; MSG SIZE rcvd: 519

dumascus@damascus-soham:~$
```

9.route :

It allows you to examine the routing table, add or delete static routes, and configure routing parameters.

```
dumascus@damascus-soham:~$ route
Kernel IP routing table
Destination      Gateway         Genmask         Flags Metric Ref    Use Iface
default          _gateway       0.0.0.0         UG    600    0      0 wlp1s0
link-local       0.0.0.0        255.255.0.0     U     1000    0      0 docker0
172.17.0.0       0.0.0.0        255.255.0.0     U      0      0      0 docker0
192.168.43.0     0.0.0.0        255.255.255.0   U      600    0      0 wlp1s0
dumascus@damascus-soham:~$
```

10. Host:

The `host` command is used to perform DNS lookups for domain names, similar to `nslookup` and `dig`.

It can be used to retrieve information about domain names or IP addresses.

```
dumascus@damascus-soham:~$ host
Usage: host [-aCdilrTVVw] [-c class] [-N ndots] [-t type] [-W time]
          [-R number] [-m flag] [-p port] hostname [server]
  -a is equivalent to -v -t ANY
  -A is like -a but omits RRSIG, NSEC, NSEC3
  -c specifies query class for non-IN data
  -C compares SOA records on authoritative nameservers
  -d is equivalent to -v
  -l lists all hosts in a domain, using AXFR
  -m set memory debugging flag (trace|record|usage)
  -N changes the number of dots allowed before root lookup is done
  -p specifies the port on the server to query
  -r disables recursive processing
  -R specifies number of retries for UDP packets
  -s a SERVFAIL response should stop query
  -t specifies the query type
  -T enables TCP/IP mode
  -U enables UDP mode
  -v enables verbose output
  -V print version number and exit
  -w specifies to wait forever for a reply
  -W specifies how long to wait for a reply
  -4 use IPv4 query transport only
  -6 use IPv6 query transport only
dumascus@damascus-soham:~$
```

11.arp;

is used to display and manipulate the ARP cache on a computer.

It allows you to view the mapping between IP addresses and MAC (Media Access Control) addresses on your local network.

```
dumascus@dumascus-soham:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
_gateway                 ether    72:5a:ac:ba:2c:7a    C                     wlp1s
0
dumascus@dumascus-soham:~$
```

12.iwconfig:

The `iwconfig` command is used to configure and display wireless network interface settings on Linux systems.

It provides information about wireless network interfaces, including SSID, signal strength, and encryption settings.

```
dumascus@dumascus-soham:~$ iwconfig
lo                no wireless extensions.

wlp1s0            IEEE 802.11  ESSID:"Galaxy J86C7A"
                  Mode:Managed  Frequency:2.412 GHz  Access Point: 72:5A:AC:BA:2C:7A
                  Bit Rate=72.2 Mb/s   Tx-Power=20 dBm
                  Retry short limit:7   RTS thr:off   Fragment thr:off
                  Power Management:on
                  Link Quality=70/70  Signal level=-30 dBm
                  Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
                  Tx excessive retries:0  Invalid misc:12  Missed beacon:0

docker0          no wireless extensions.

dumascus@dumascus-soham:~$
```


13.curl:

The `curl` command is a versatile tool for making HTTP requests from the command line.

It can be used to retrieve content from web servers, interact with APIs, and perform file transfers using various protocols.

[illegible]

14.wget:

The `wget` command is a command-line utility for downloading files from the internet.

It allows you to download files from FTP, HTTP, and HTTPS servers, and it supports resuming interrupted downloads.

```
dumascus@damascus-sohan:~$ wget https://google.com
--2023-09-10 22:43:31-- https://google.com/
Resolving google.com (google.com)... 2404:6800:4009:80c::200e, 172.217.166.46
Connecting to google.com (google.com)|2404:6800:4009:80c::200e|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://www.google.com/ [following]
--2023-09-10 22:43:33-- https://www.google.com/
Resolving www.google.com (www.google.com)... 2404:6800:4009:82b::2004, 172.217.27.196
Connecting to www.google.com (www.google.com)|2404:6800:4009:82b::2004|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'index.html'

index.html          [ <=> ] 20.34K 67.7KB/s in 0.3s

2023-09-10 22:43:35 (67.7 KB/s) - 'index.html' saved [20826]

dumascus@damascus-sohan:~$
```


15.telnet :

The `telnet` command is used to establish text-based connections to remote servers and network devices.

It is often used for testing network connectivity and for accessing remote systems, although it is less secure than SSH.

```
dumascus@damascus-soham:~$ telnet google.com 80
Trying 2404:6800:4009:80c::200e...
Connected to google.com.
Escape character is '^['.
```

16.whois :

The `whois` command is used to query WHOIS databases to retrieve information about domain names, IP addresses, and network registrations.

It provides details about domain ownership, contact information, and registration dates.

```
dumascus@damascus-soham:~$ whois
Usage: whois [OPTION]... OBJECT...

-h HOST, --host HOST    connect to server HOST
-p PORT, --port PORT    connect to PORT
-I                      query whois.iana.org and follow its referral
-H                      hide legal disclaimers
    --verbose           explain what is being done
    --no-recursion      disable recursion from registry to registrar servers
    --help              display this help and exit
    --version           output version information and exit

These flags are supported by whois.ripe.net and some RIPE-like servers:
-l                      find the one level less specific match
-L                      find all levels less specific matches
-m                      find all one level more specific matches
-M                      find all levels of more specific matches
-C                      find the smallest match containing a mnt-irt attribute
-X                      exact match
-b                      return brief IP address ranges with abuse contact
-B                      turn off object filtering (show email addresses)
-G                      turn off grouping of associated objects
-d                      return DNS reverse delegation objects too
-i ATTR[,ATTR]...       do an inverse look-up for specified ATTRIBUTES
-T TYPE[,TYPE]...       only look for objects of TYPE
-K                      only primary keys are returned
-r                      turn off recursive look-ups for contact information
-R                      force to show local copy of the domain object even
                        if it contains referral
-a                      also search all the mirrored databases
-s SOURCE[,SOURCE]...   search the database mirrored from SOURCE
-g SOURCE:FIRST-LAST    find updates from SOURCE from serial FIRST to LAST
-t TYPE                 request template for object of TYPE
-v TYPE                 request verbose template for object of TYPE
-q [version|sources|types] query specified server info
dumascus@damascus-soham:~$
```

17.ifplugstatus:

The `ifplugstatus` command is used to check the status of Ethernet cable connections on network interfaces.

It can indicate whether a network cable is plugged in or unplugged.

```
dumascus@damascus-  
dumascus@damascus-soham:~$ ifplugstatus  
lo: link beat detected  
wlp1s0: link beat detected  
docker0: unplugged  
dumascus@damascus-soham:~$
```

18.nload:

The `nload` command is a console-based network traffic monitoring tool.

It displays real-time statistics about network interfaces, including bandwidth usage and traffic distribution.

```
dumascus@damascus-soham: ~  
Device docker0 [172.17.0.1] (1/3):  
===== Incoming: =====  
Curr: 0.00 Bit/s  
Avg: 0.00 Bit/s  
Min: 0.00 Bit/s  
Max: 0.00 Bit/s  
Ttl: 0.00 Byte  
Outgoing:  
Curr: 0.00 Bit/s  
Avg: 0.00 Bit/s  
Min: 0.00 Bit/s  
Max: 0.00 Bit/s  
Ttl: 0.00 Byte
```

19.mail:

The `mail` command is used for sending and receiving email from the command line on Unix-like systems.

- It allows you to compose and send emails and read email messages in your mailbox.