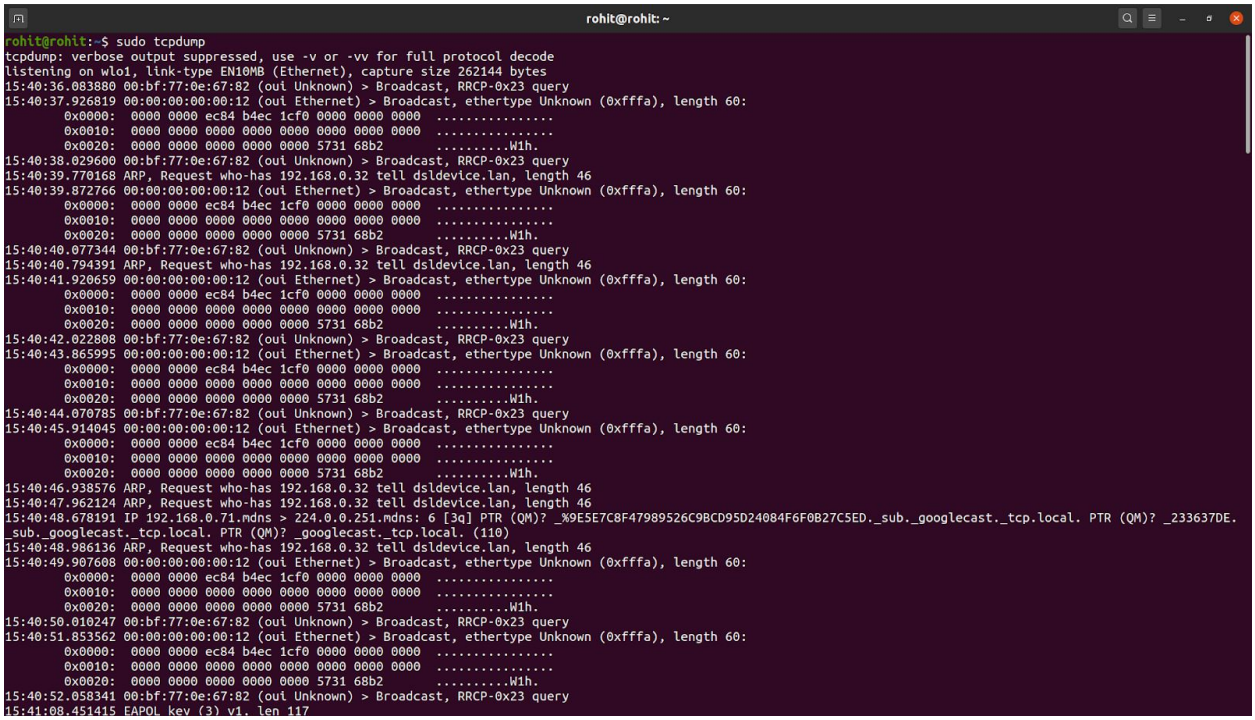
CS F303 Computer Networks
Lab1[25/01/2021]

Name: ROHIT GARG
ID: 2018A7PS0193G

1. tcpdump

tcpdump is a cmd-line sniffer that dumps traffic on a network. Requires super-user privileges. *tcpdump* prints out a description of the contents of packets on a network interface that match the boolean *expression*. Tcpdump is a utility that is used to capture and analyse packets on a network interface.



2. ifconfig

It stands for interface configuration. **ifconfig**(interface configuration) command is used to configure the kernel-resident network interfaces. It is used at the boot time to set up the interfaces as necessary. The output follows the following syntax: {interface_name, interface_status, broadcast_status, transmission_status, multicast…..}

```
rohit@rohit:~$ ifconfig
enx3c18a0955f87: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.33  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::ae08:1ee2:fd95:f9df  prefixlen 64  scopeid 0x20<link>
        ether 3c:18:a0:95:5f:87  txqueuelen 1000  (Ethernet)
        RX packets 622845  bytes 643269105 (643.2 MB)
        RX errors 0  dropped 8361  overruns 0  frame 0
        TX packets 234858  bytes 49340599 (49.3 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 6331  bytes 664778 (664.7 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 6331  bytes 664778 (664.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

3. dig

Dig is a DNS look-up utility. Dig is a command line tool for querying and analysing DNS name servers. It collects data about the domain name servers.

```
rohit@rohit:~$ dig

; <<>> DiG 9.16.1-Ubuntu <<>>
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14780
;; flags: qr rd ra; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 1

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

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

;; Query time: 12 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Sat Jan 23 16:41:01 IST 2021
;; MSG SIZE  rcvd: 239
```

Here we are querying from using dig www.google.com. By default dig performs a lookup for an A record if no type argument is specified. The first line contains the version of dig[9.16.1] and global options are used. Question section displays the query while the answer section contains the desired record. We see that www.google.com, with a TTL of 171 seconds has an A record - 216.58.221.36. Last section displays the statistics i.e. query time.

```
rohit@rohit:~$ dig www.google.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60004
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.google.com.                        IN      A

;; ANSWER SECTION:
www.google.com.         171     IN      A       216.58.221.36

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Sat Jan 23 17:00:09 IST 2021
;; MSG SIZE  rcvd: 59
```

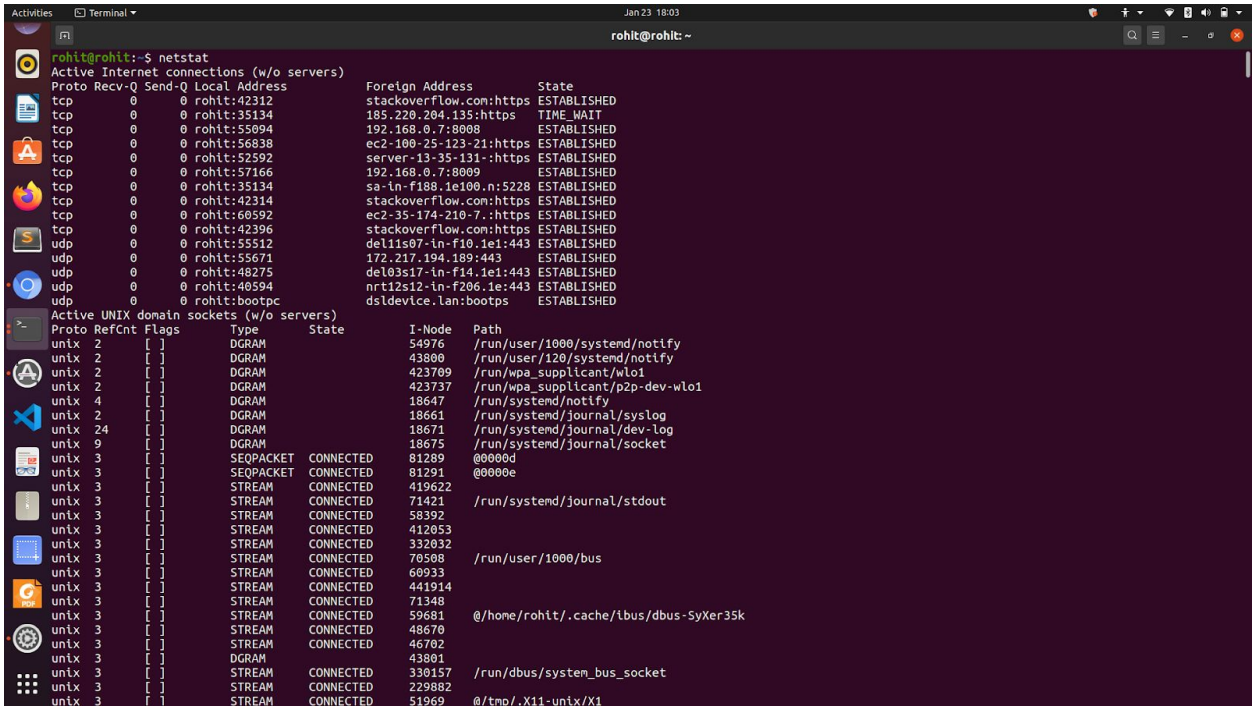
4. arp

It refers to Address Resolution Protocol. Arp manipulates or displays the kernel's IPv4 network neighbour cache.The primary function of this protocol is to resolve the IP address of a system to its mac address, and hence it works between level 2(Data link layer) and level 3(Network layer)

```
rohit@rohit:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
dsldevice.lan            ether   ec:84:b4:ec:1c:f0   C                     wlo1
```

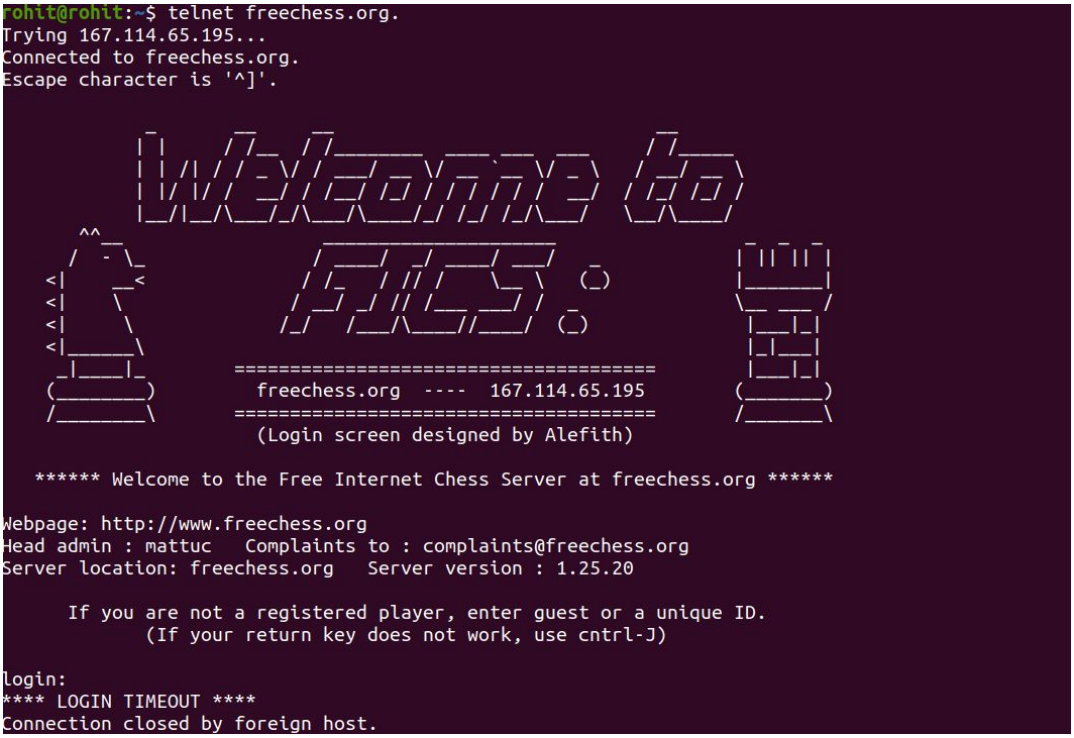
5. netstat

netstat is used to print network statistics like routing tables, active connections etc. Here, netstat displays the per protocol stats or network information for each port(TCP, UNIX) etc.



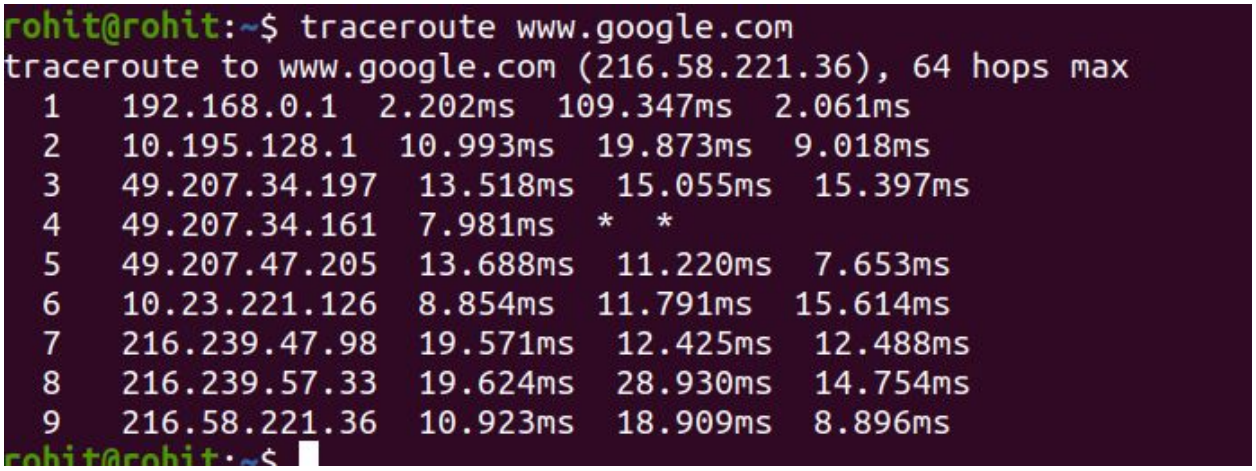
6. telnet

The telnet command is used to communicate with another host using the *TELNET* protocol. Used to send commands to remote servers. Here I remotely established a connection to freechess.org's server.



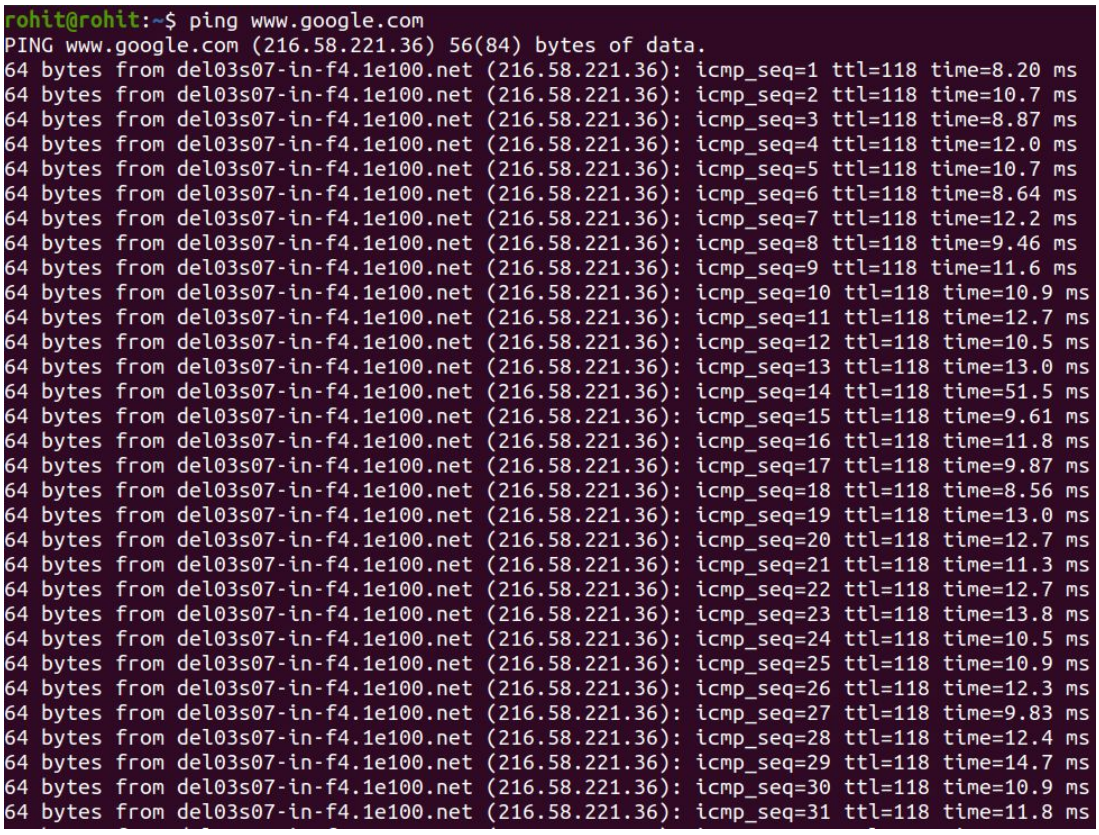
7. traceroute

traceroute command in Linux prints the route that a packet takes to reach the host. This command is useful when you want to know about the route and about all the hops that a packet takes. The first line of the traceroute output lists the destination system (www.google.com), destination IP address (216.58.221.36), and the maximum number of hops that will be used in the traceroute (64).The remainder of the output shows information on each hop, which is typically a router, in the path between the sender and the final destination.



8. ping

Used to check if a network is available and if the host is reachable. ping sends ICMP ECHO_REQUEST to network hosts.The **ping** command sends one datagram per second and prints one line of output for every response received.



9. top

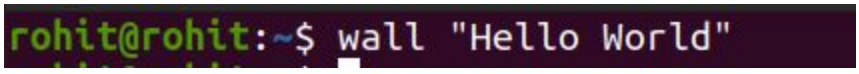
Displays the process table in linux. It can display system summary information as well as a list of processes or threads currently being managed by the Linux kernel.

```
top - 18:44:14 up  4:52,  1 user,  load average: 0.77, 0.72, 1.12
Tasks: 394 total,   1 running, 393 sleeping,   0 stopped,   0 zombie
%Cpu(s):  6.3 us,  1.4 sy,  0.0 ni, 91.6 id,  0.1 wa,  0.0 hi,  0.6 si,  0.0 st
MiB Mem :   7834.8 total,   2122.1 free,   3301.3 used,   2411.5 buff/cache
MiB Swap:   2048.0 total,   1771.4 free,    276.6 used.   3672.7 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
  14681 rohit     20   0 5943868 352748 120244 S  18.2   4.4  10:50.25 chrome
   3132 rohit     20   0 5266792 314388  96340 S  15.2   3.9  45:08.26 gnome-shell
   2784 rohit     20   0 1206692 102332  78616 S   8.3   1.3  29:25.14 Xorg
   5235 rohit     20   0 1483144 159824  74872 S   7.9   2.0  49:51.78 chrome
   5068 rohit     20   0 3830248 453668 113076 S   5.3   5.7  33:56.14 chrome
   4802 rohit     20   0  974416  57724  39484 S   3.0   0.7   1:14.53 gnome-terminal-
   2934 rohit     20   0  238064   7580   5824 S   1.3   0.1   0:43.76 ibus-daemon
   5245 rohit     20   0 1628440  96196  59476 S   1.3   1.2   6:13.46 chrome
  21592 rohit     20   0 2794940 120792  58788 S   1.0   1.5   1:33.96 FoxitReader
  20136 rohit     20   0 5920460 328936  96168 S   0.7   4.1   1:54.04 chrome
    309 root       0 -20       0      0      0 I   0.3   0.0   0:01.50 kworker/0:1H-events_highpri
   1302 root      20   0   81884   3844   3492 S   0.3   0.0   0:01.95 irqbalance
   2970 rohit     20   0  275124  25576  19084 S   0.3   0.3   0:11.21 ibus-extension-
   3028 rohit     20   0  162684   6852   6528 S   0.3   0.1   0:10.82 ibus-engine-sim
   5371 rohit     20   0 5789016 131792  80152 S   0.3   1.6   0:58.94 chrome
   7907 rohit     20   0 5772000 107280  82252 S   0.3   1.3   0:10.09 chrome
   7963 rohit     20   0 9815.0m 173556  93364 S   0.3   2.2   0:50.65 chrome
  27147 root      20   0       0      0      0 I   0.3   0.0   0:08.27 kworker/u16:56-i915
  30332 root      20   0       0      0      0 I   0.3   0.0   0:05.52 kworker/5:3-events
  33612 rohit     20   0 5850800 195168 117932 S   0.3   2.4   0:47.97 chrome
  38285 rohit     20   0   12364   4332   3392 R   0.3   0.1   0:00.16 top
      1 root      20   0  169820  12724   7884 S   0.0   0.2   0:45.09 systemd
      2 root      20   0       0      0      0 S   0.0   0.0   0:00.04 kthreadd
      3 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_gp
      4 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_par_gp
      6 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/0:0H-kblockd
      9 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 mm_percpu_wq
     10 root      20   0       0      0      0 S   0.0   0.0   0:00.86 ksoftirqd/0
     11 root      20   0       0      0      0 I   0.0   0.0   0:29.48 rcu_sched
     12 root      rt   0       0      0      0 S   0.0   0.0   0:00.09 migration/0
     13 root     -51   0       0      0      0 S   0.0   0.0   0:00.00 idle_inject/0
     14 root      20   0       0      0      0 S   0.0   0.0   0:00.00 cpuhp/0
     15 root      20   0       0      0      0 S   0.0   0.0   0:00.00 cpuhp/1
     16 root     -51   0       0      0      0 S   0.0   0.0   0:00.00 idle_inject/1
     17 root      rt   0       0      0      0 S   0.0   0.0   0:00.25 migration/1
     18 root      20   0       0      0      0 S   0.0   0.0   0:01.11 ksoftirqd/1
     20 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/1:0H-kblockd
     21 root      20   0       0      0      0 S   0.0   0.0   0:00.00 cpuhp/2
```

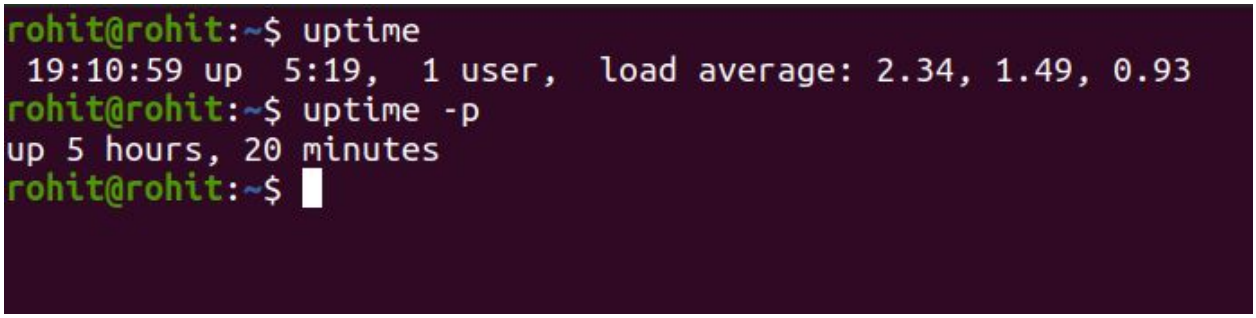
10. wall

wall command in Linux system is used to write a message to all users. In the below example, the message “Hello World” will be broadcasted to all users.



11. uptime

Uptime is a **command** that returns information about how long your system has been running together with the current time, number of users with running sessions, and the system load averages for the past 1, 5, and 15 minutes. As clear from the example the current time is 19:10:59, machine has been up since 5h 20mins with one user and system load average values have been shown.



12. nslookup

Nslookup command is used to query domain name servers and return the mapping from the domain name to IP address. Here we query server = 127.0.0.53 for domain name www.google.com and it returns us the IP address and port used. In this case, a **"non-authoritative answer"** notification is given, as the local DNS server was unable to answer the query itself, and instead had to contact one or more other name servers. IPv4 and IPv6(longer ones) addresses of www.google.com are returned .