Htop

the htop command is interactive, real time monitoring.
Its considered improved and more user friendly then top command.
why to use htop then top?

- Providing enhanced Interface: better visual appearing, color-coded
- Tree view: providing parent-child relationship between processes
- easy to navigate between processes.
- killing process is easy

Intsallation:

sudo apt install htop (ubuntu)
sudo yum install epel-release, sudo yum install htop (centos)
sudo dnf install htop (fedora)
brew install htop (mac)

Output:

System Processes
CPU Usage Graph:
green: User Processes
red: System processes
Blue: low priority (nice) processes
orange: I/O wait time

--> f6 to sort and choose the particular option for sorting.
--> select any process which you want to kill then press f9 or fn+f9 and then select SIGTERM and send.
It will terminate the process.

to understand all flags you can execute: htop --help
user specific process: htop -u sonam
for getting details of specific processes: htop -p 450,455,468

Free command
The free command to display memory usage — including RAM and swap.
it provides the details like how memory is used , free, shared, cached and available in system.
Output details

total: total installed memory (RAM)
used: memory currently used by processes total - free - cache

free: not used memory

buff/cache: used by buffers and page cache

available: calculated memory available to stat new app without req of swapping

Run command:

free (provide details in bytes)

free -h (human redable)

free -h -s 3 (every 3 seconds it calculates)

free -h -t (showing total for RAM + SWAP)

NICE & RENICE

nice is used to start process with some specific priority

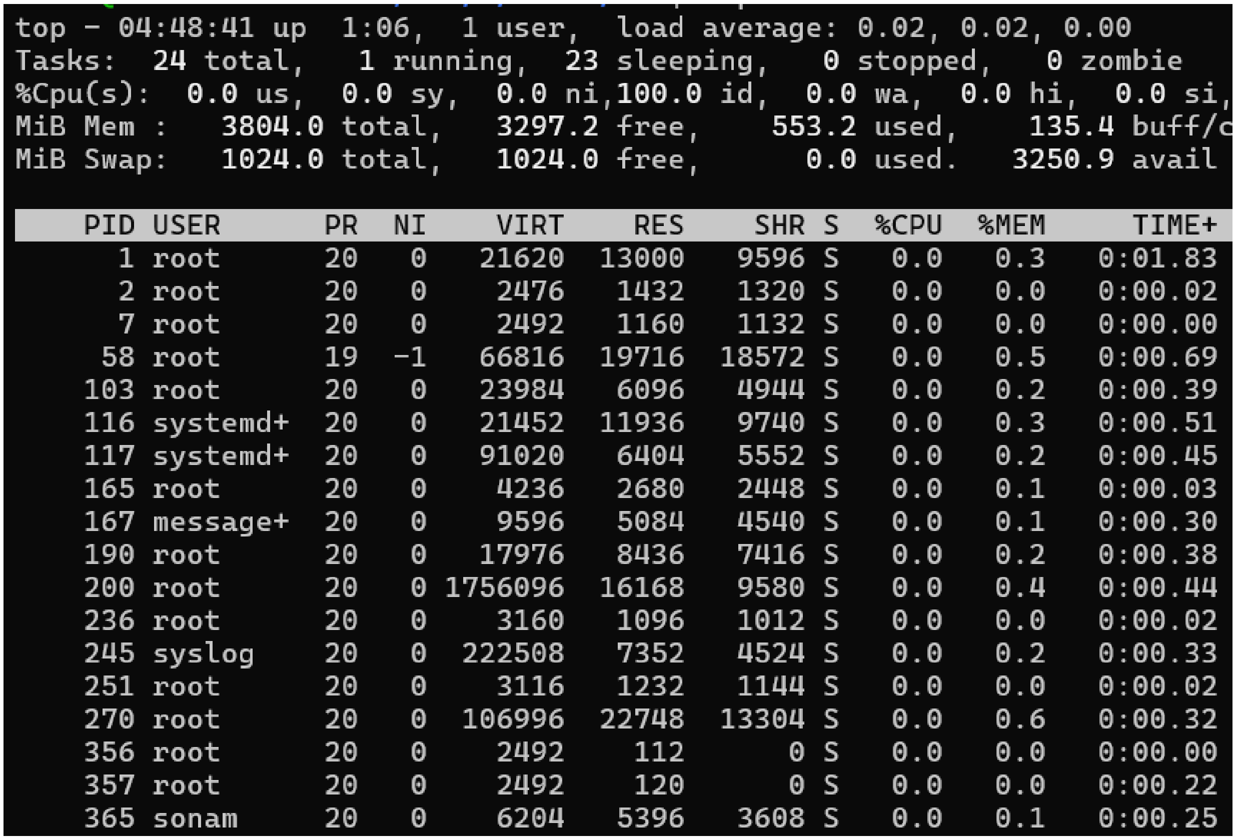
renice command is used to change the priority of existing process.

Each process has a nice value randing from -20 to 19

-20 (Highest Priority)

19 (lowest priority)

By deafult new process start with nice value 0.



```
top - 04:48:41 up  1:06,  1 user,  load average: 0.02, 0.02, 0.00
Tasks:  24 total,   1 running,  23 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0.0 us,  0.0 sy,  0.0 ni,100.0 id,  0.0 wa,  0.0 hi,  0.0 si,
MiB Mem :   3804.0 total,   3297.2 free,    553.2 used,    135.4 buff/c
MiB Swap:   1024.0 total,   1024.0 free,      0.0 used.   3250.9 avail

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+
      1 root      20   0   21620  13000   9596 S   0.0   0.3   0:01.83
      2 root      20   0    2476   1432   1320 S   0.0   0.0   0:00.02
      7 root      20   0    2492   1160   1132 S   0.0   0.0   0:00.00
     58 root      19  -1   66816  19716  18572 S   0.0   0.5   0:00.69
    103 root      20   0   23984   6096   4944 S   0.0   0.2   0:00.39
    116 systemd+  20   0   21452  11936   9740 S   0.0   0.3   0:00.51
    117 systemd+  20   0   91020   6404   5552 S   0.0   0.2   0:00.45
    165 root      20   0    4236   2680   2448 S   0.0   0.1   0:00.03
    167 message+  20   0    9596   5084   4540 S   0.0   0.1   0:00.30
    190 root      20   0   17976   8436   7416 S   0.0   0.2   0:00.38
    200 root      20   0 1756096  16168   9580 S   0.0   0.4   0:00.44
    236 root      20   0    3160   1096   1012 S   0.0   0.0   0:00.02
    245 syslog    20   0  222508   7352   4524 S   0.0   0.2   0:00.33
    251 root      20   0    3116   1232   1144 S   0.0   0.0   0:00.02
    270 root      20   0  106996  22748  13304 S   0.0   0.6   0:00.32
    356 root      20   0    2492    112      0 S   0.0   0.0   0:00.00
    357 root      20   0    2492    120      0 S   0.0   0.0   0:00.22
    365 sonam     20   0    6204   5396   3608 S   0.0   0.1   0:00.25
```

Here you can see priority and nice value.

Priority is 20 and if the nice value is -1 then priority becomes 19

Higher the value means its having low priority (the process is "nicer" to others)

Lower the nice value mean higher priority (requires root access for negative value)

Start a process with nice value 10

nice -n 10 script-name

Let's Create a Script

cd developers

nano myscript.sh

```
#!/bin/bash
echo "Start my Script with priority $(nice)"
sleep 100 ## I want to continue run this process
echo "Script completed Successfully"
```

ctrl+O then enter then ctrl+x

else use vi editor

vi myscript.sh enter the above code (to type the code press I for insert)

once code written press esc then type :wq! then enter

To run it normally use sh script-name.

To run the script: sh myscript.sh &

(run it in background using & symbol)

it will show you the console output which you can close using ctrl+c

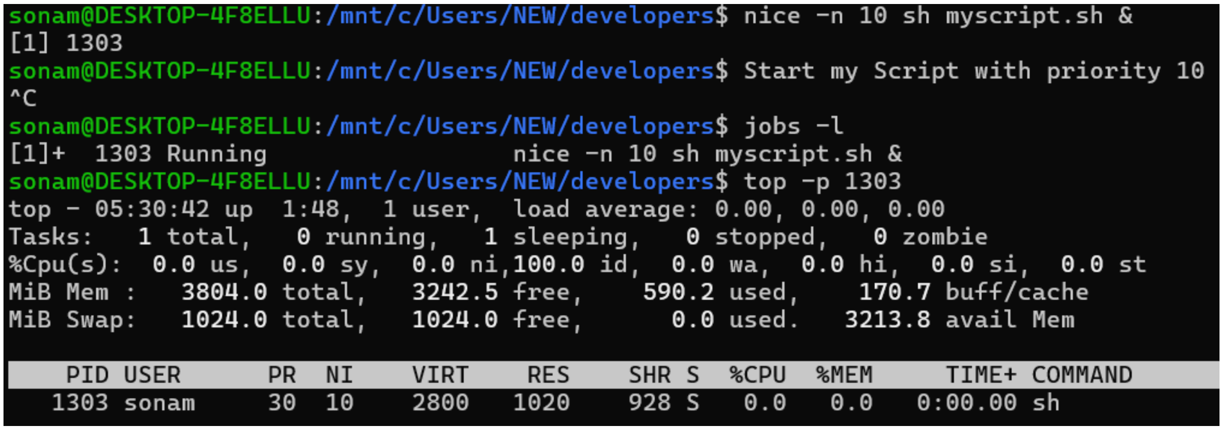
then check process id using: jobs -l (take process ID)

check priority using top command: top -p pID

(you can see the default priority is 0)

Let's say I want to start with priority 10: nice -n 10 sh myscript.sh &

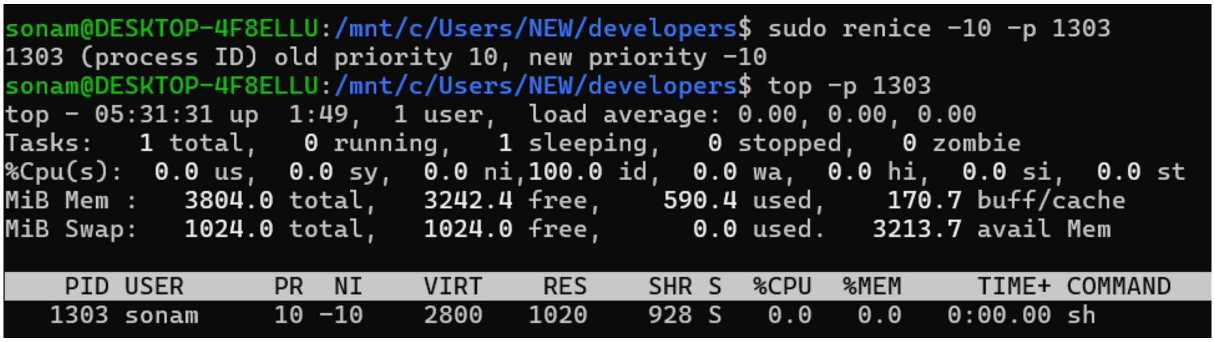
again same get id and check using top command.



```
sonam@DESKTOP-4F8ELLU:/mnt/c/Users/NEW/developers$ nice -n 10 sh myscript.sh &
[1] 1303
sonam@DESKTOP-4F8ELLU:/mnt/c/Users/NEW/developers$ Start my Script with priority 10
^C
sonam@DESKTOP-4F8ELLU:/mnt/c/Users/NEW/developers$ jobs -l
[1]+  1303 Running                 nice -n 10 sh myscript.sh &
sonam@DESKTOP-4F8ELLU:/mnt/c/Users/NEW/developers$ top -p 1303
top - 05:30:42 up  1:48,  1 user,  load average: 0.00, 0.00, 0.00
Tasks:   1 total,   0 running,   1 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0.0 us,  0.0 sy,  0.0 ni,100.0 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
MiB Mem :   3804.0 total,   3242.5 free,    590.2 used,    170.7 buff/cache
MiB Swap:   1024.0 total,   1024.0 free,      0.0 used.   3213.8 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
 1303 sonam     30  10    2800   1020    928 S   0.0   0.0   0:00.00 sh
```

Now you can change priority using renice.

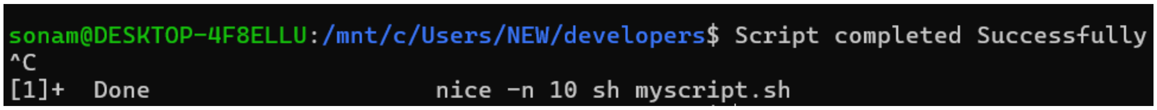


```
sonam@DESKTOP-4F8ELLU:/mnt/c/Users/NEW/developers$ sudo renice -10 -p 1303
1303 (process ID) old priority 10, new priority -10
sonam@DESKTOP-4F8ELLU:/mnt/c/Users/NEW/developers$ top -p 1303
top - 05:31:31 up  1:49,  1 user,  load average: 0.00, 0.00, 0.00
Tasks:   1 total,   0 running,   1 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0.0 us,  0.0 sy,  0.0 ni,100.0 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
MiB Mem :   3804.0 total,   3242.4 free,    590.4 used,    170.7 buff/cache
MiB Swap:   1024.0 total,   1024.0 free,      0.0 used.   3213.7 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
   1303 sonam     10 -10    2800   1020    928 S   0.0   0.0   0:00.00 sh
```

This is how we can change priority of processes.

once the process completed you can do ctrl+c



```
sonam@DESKTOP-4F8ELLU:/mnt/c/Users/NEW/developers$ Script completed Successfully
^C
[1]+  Done                    nice -n 10 sh myscript.sh
```

Network commands

traceroute: tool which is used to trace the path between system and remote host.

traceroute shows hops(router/gateways) that a packet passes through to reach the destination.

You can identify where the network is creating issue or delay happening.

install: sudo apt install traceroute or sudo apt install inetutils-traceroute

traceroute google.com

tracing the hop and 3 responces

- * * (no response, blocked by ICMP time exceeded

traceroute -m 15 google.com (set hops)

traceroute -w 2 google.com (wait time in seconds)

nslookup command

network administration command line tool which is used to trigger DNS and get domain name and IP address

-- get the IP address of Domain

-- get the domain name

-- query specific DNS server

installation:

sudo apt install bind9-dnsutils or sudo apt install dnsutils

nslookup google.com

nslookup github.com (get IP of Domain)

nslookup 8.8.8.8 (IP to domain)

It is showing 2 Adrress

Server: DNS Server where nslookup is performing query.

it can be local DNS server kind of router or

public IP (8.8.8.8)

Address: IP address of DNS server

tcpdump command

Powerful packet sniffer and network analyzer.

It captures packets going through network interfaces, helping you to debug network issues.

analyze protocols, security monitoring.

How it works?

- captures raw packets
- can filter based on protocols, IPs and ports

sudo apt install tcpdump (install)

run at root because it needs permission.

capture the output

```
    sudo tcpdump -i eth0 -w capture.pcap
```

for furthure analysis you canread this file

    using command: tcpdump -r capture.pcap

GUI level analysis you can use WireShark and open this file inside the same.