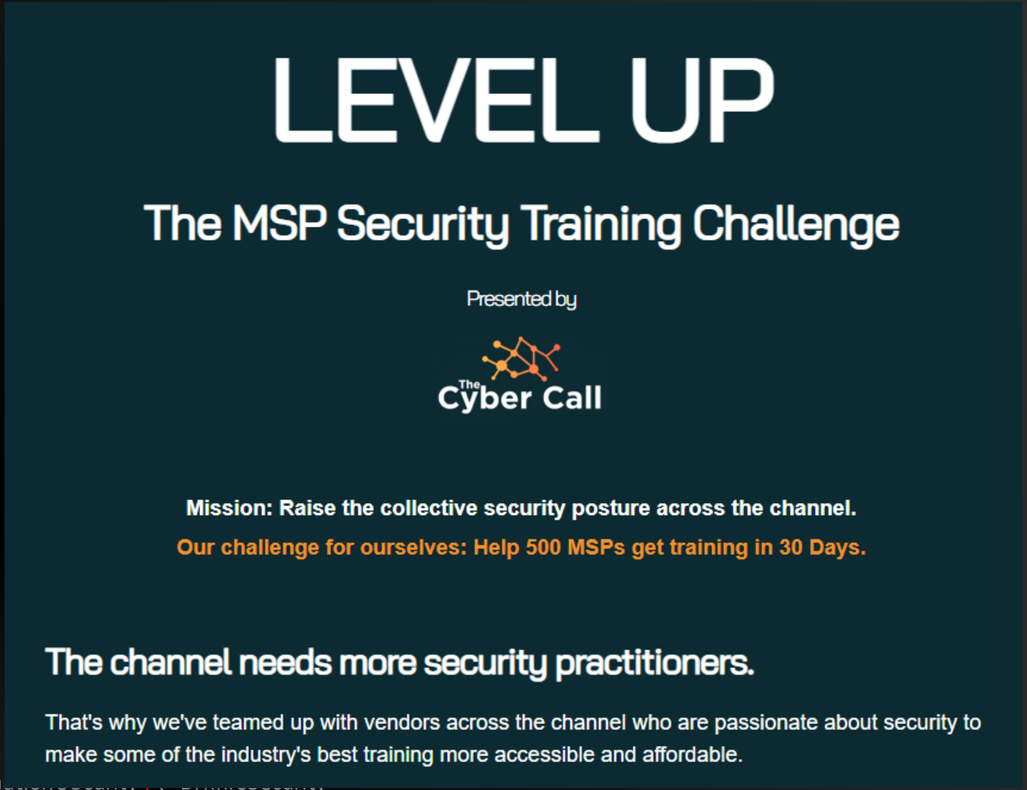
Getting Started With BHIS: SOC Analyst

John Strand

Big Thanks!!



LEVEL UP

The MSP Security Training Challenge

Presented by

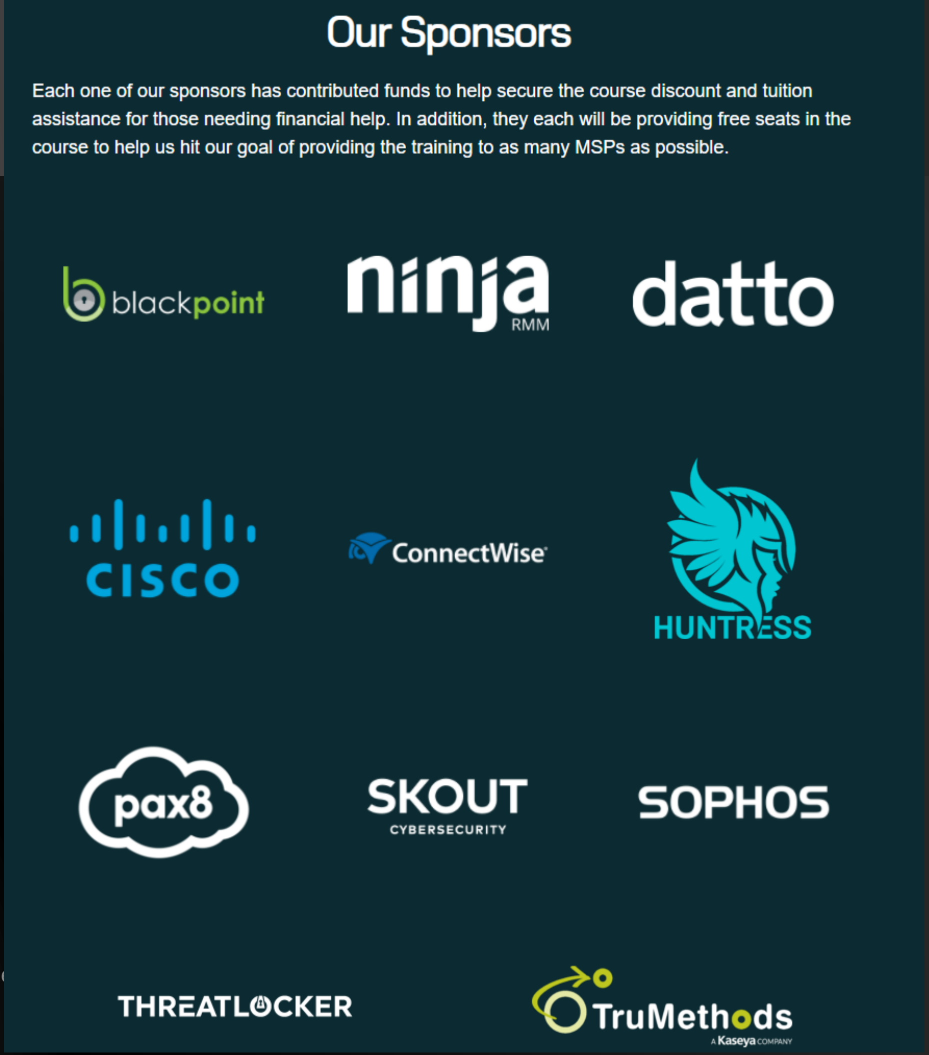
The Cyber Call

Mission: Raise the collective security posture across the channel.

Our challenge for ourselves: Help 500 MSPs get training in 30 Days.

The channel needs more security practitioners.

That's why we've teamed up with vendors across the channel who are passionate about security to make some of the industry's best training more accessible and affordable.



Our Sponsors

Each one of our sponsors has contributed funds to help secure the course discount and tuition assistance for those needing financial help. In addition, they each will be providing free seats in the course to help us hit our goal of providing the training to as many MSPs as possible.

blackpoint

ninja RMM

datto

cisco

ConnectWise

HUNTRESS

pax8

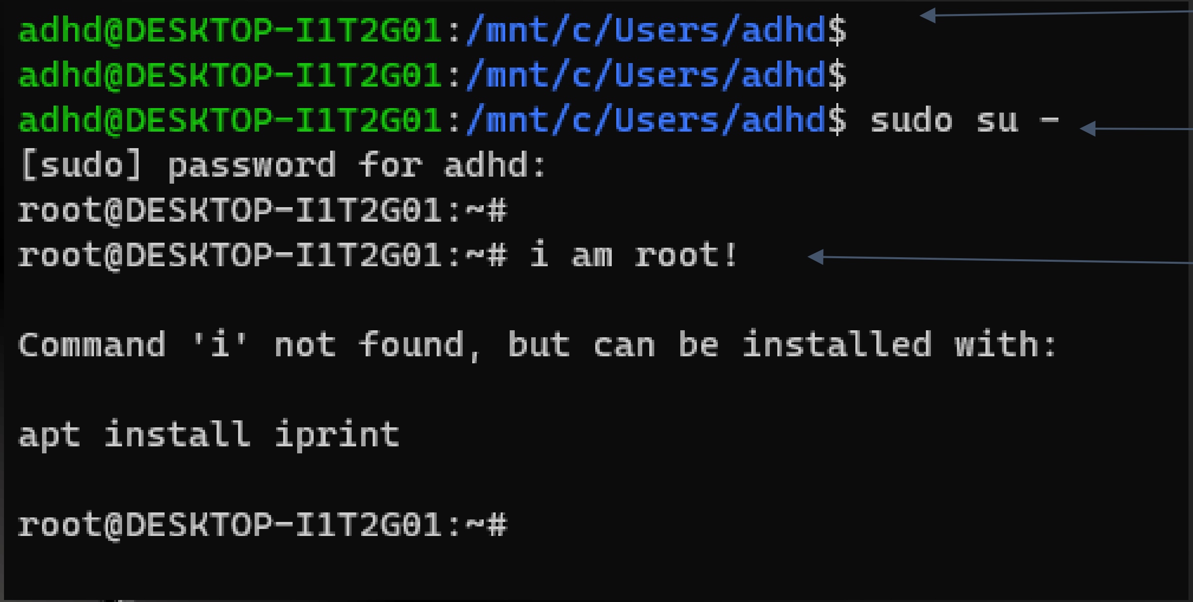
SKOUT CYBERSECURITY

SOPHOS

THREATLOCKER

TruMethods A Kaseya COMPANY

Users and Privileges

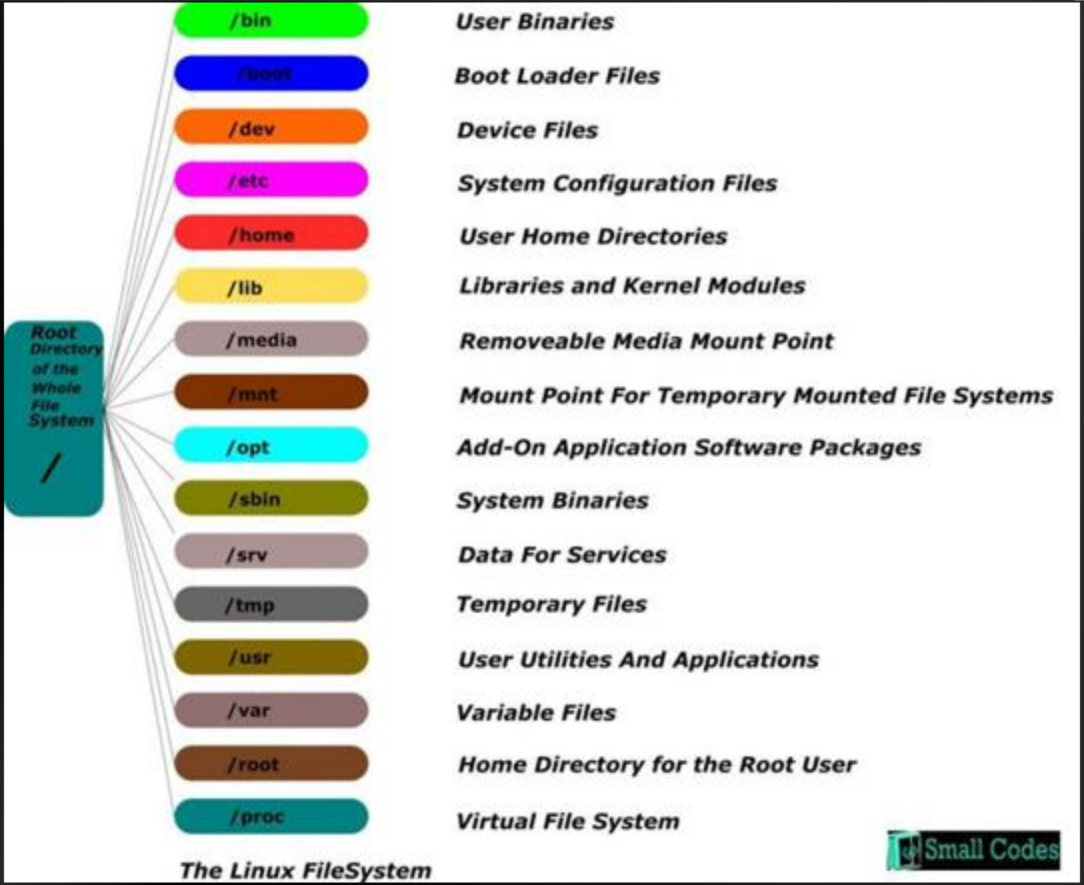


```
adhd@DESKTOP-I1T2G01:/mnt/c/Users/adhd$
adhd@DESKTOP-I1T2G01:/mnt/c/Users/adhd$
adhd@DESKTOP-I1T2G01:/mnt/c/Users/adhd$ sudo su -
[sudo] password for adhd:
root@DESKTOP-I1T2G01:~#
root@DESKTOP-I1T2G01:~# i am root!

Command 'i' not found, but can be installed with:

apt install iprint

root@DESKTOP-I1T2G01:~#
```

Not Root

Becoming Root

I Am Root!



Root Directory of the Whole File System

/

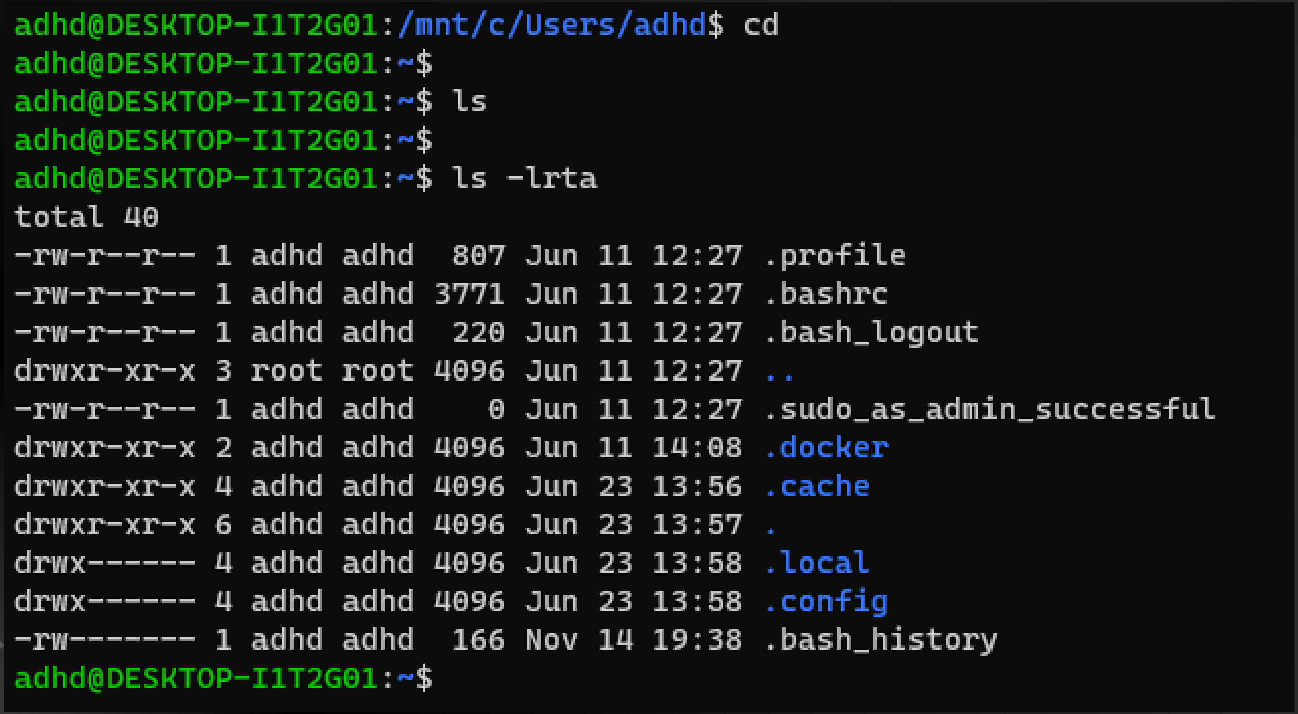
/bin	User Binaries
/boot	Boot Loader Files
/dev	Device Files
/etc	System Configuration Files
/home	User Home Directories
/lib	Libraries and Kernel Modules
/media	Removeable Media Mount Point
/mnt	Mount Point For Temporary Mounted File Systems
/opt	Add-On Application Software Packages
/sbin	System Binaries
/srv	Data For Services
/tmp	Temporary Files
/usr	User Utilities And Applications
/var	Variable Files
/root	Home Directory for the Root User
/proc	Virtual File System

The Linux FileSystem

Now.. Linux

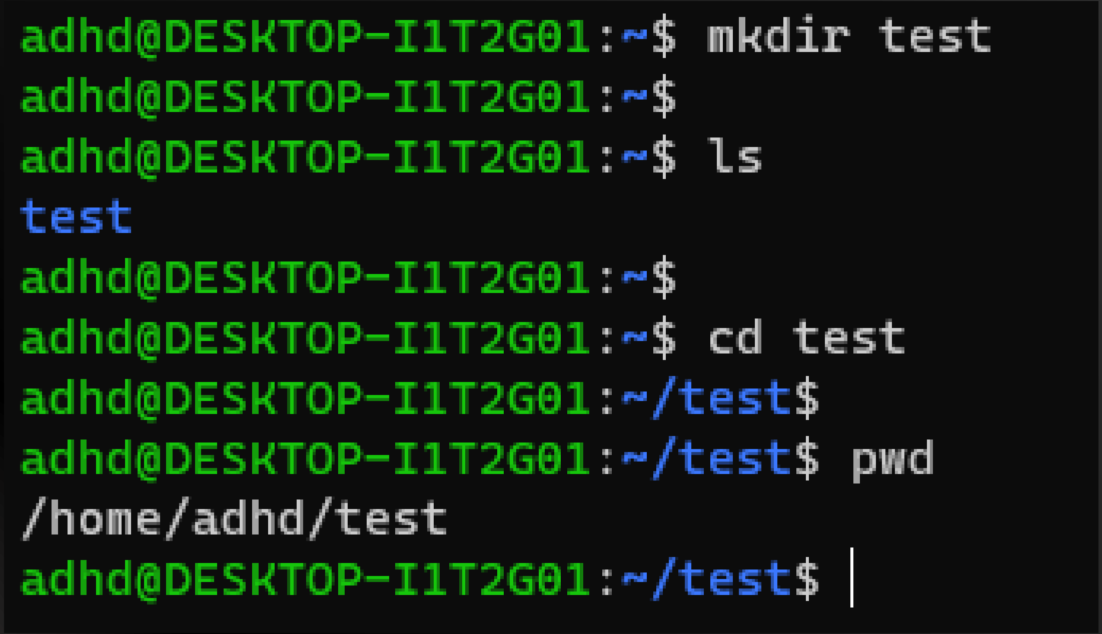
- In this section we will go through some core “live forensics” commands
- These are commands you should know and love
- They can mean the difference between a quick incident and a long painful one
- They can mean the difference between knowing, and just staring at a screen waiting for blinky lights to tell you things
- Plus… Linux is fun
- Why start with Linux????

Home Directories and ”Hidden” Files



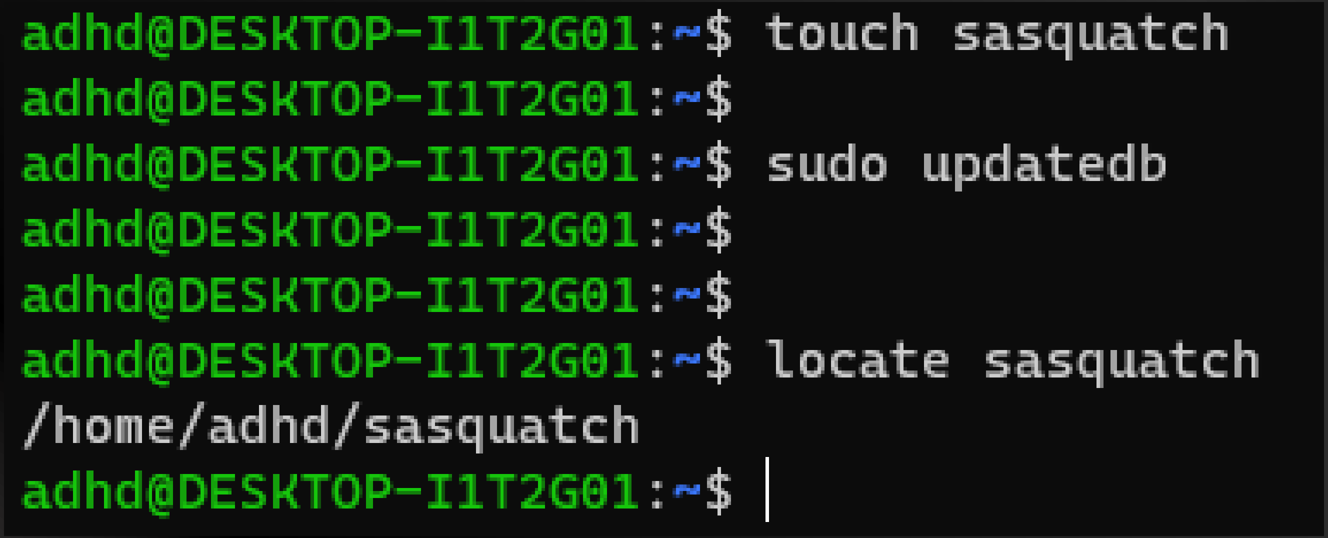
```
adhd@DESKTOP-I1T2G01:/mnt/c/Users/adhd$ cd
adhd@DESKTOP-I1T2G01:~$
adhd@DESKTOP-I1T2G01:~$ ls
adhd@DESKTOP-I1T2G01:~$
adhd@DESKTOP-I1T2G01:~$ ls -lrta
total 40
-rw-r--r-- 1 adhd adhd  807 Jun 11 12:27 .profile
-rw-r--r-- 1 adhd adhd 3771 Jun 11 12:27 .bashrc
-rw-r--r-- 1 adhd adhd  220 Jun 11 12:27 .bash_logout
drwxr-xr-x 3 root root 4096 Jun 11 12:27 ..
-rw-r--r-- 1 adhd adhd    0 Jun 11 12:27 .sudo_as_admin_successful
drwxr-xr-x 2 adhd adhd 4096 Jun 11 14:08 .docker
drwxr-xr-x 4 adhd adhd 4096 Jun 23 13:56 .cache
drwxr-xr-x 6 adhd adhd 4096 Jun 23 13:57 .
drwx------ 4 adhd adhd 4096 Jun 23 13:58 .local
drwx------ 4 adhd adhd 4096 Jun 23 13:58 .config
-rw------- 1 adhd adhd  166 Nov 14 19:38 .bash_history
adhd@DESKTOP-I1T2G01:~$
```

mkdir



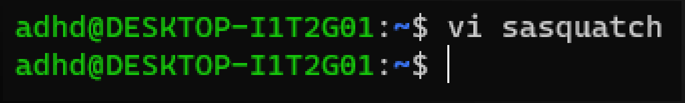
```
adhd@DESKTOP-I1T2G01:~$ mkdir test
adhd@DESKTOP-I1T2G01:~$
adhd@DESKTOP-I1T2G01:~$ ls
test
adhd@DESKTOP-I1T2G01:~$
adhd@DESKTOP-I1T2G01:~$ cd test
adhd@DESKTOP-I1T2G01:~/test$
adhd@DESKTOP-I1T2G01:~/test$ pwd
/home/adhd/test
adhd@DESKTOP-I1T2G01:~/test$
```

Finding Files With locate

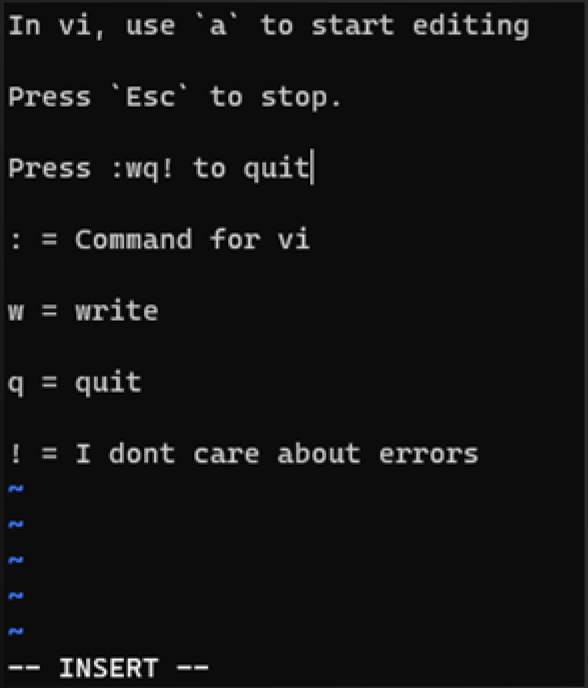


```
adhd@DESKTOP-I1T2G01:~$ touch sasquatch
adhd@DESKTOP-I1T2G01:~$
adhd@DESKTOP-I1T2G01:~$ sudo updatedb
adhd@DESKTOP-I1T2G01:~$
adhd@DESKTOP-I1T2G01:~$
adhd@DESKTOP-I1T2G01:~$ locate sasquatch
/home/adhd/sasquatch
adhd@DESKTOP-I1T2G01:~$
```

Editing files with vi

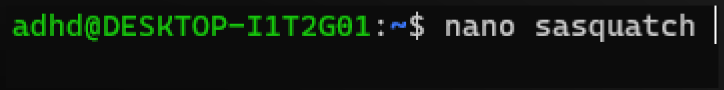


```
adhd@DESKTOP-I1T2G01:~$ vi sasquatch
adhd@DESKTOP-I1T2G01:~$
```

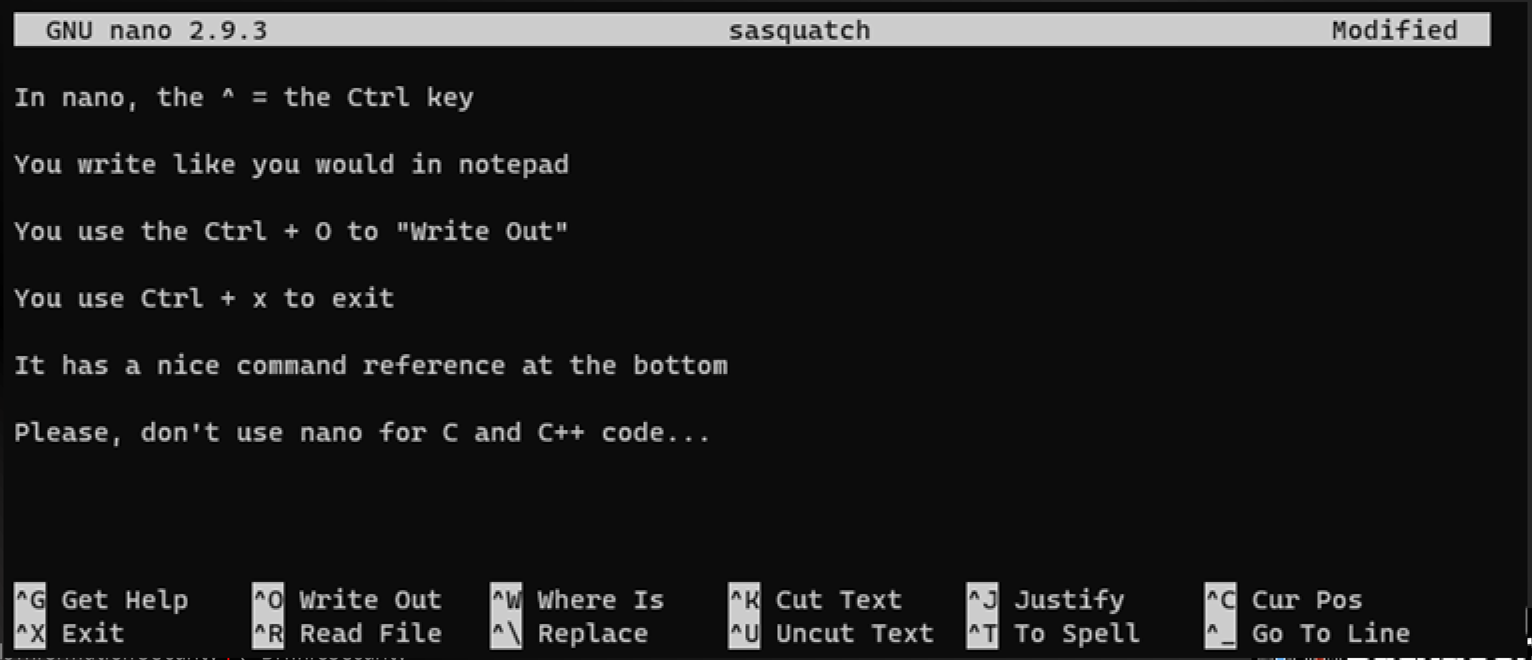


```
In vi, use `a` to start editing

Press `Esc` to stop.

Press :wq! to quit

: = Command for vi

w = write

q = quit

! = I dont care about errors
~
~
~
~
~
-- INSERT --
```

Editing files with nano

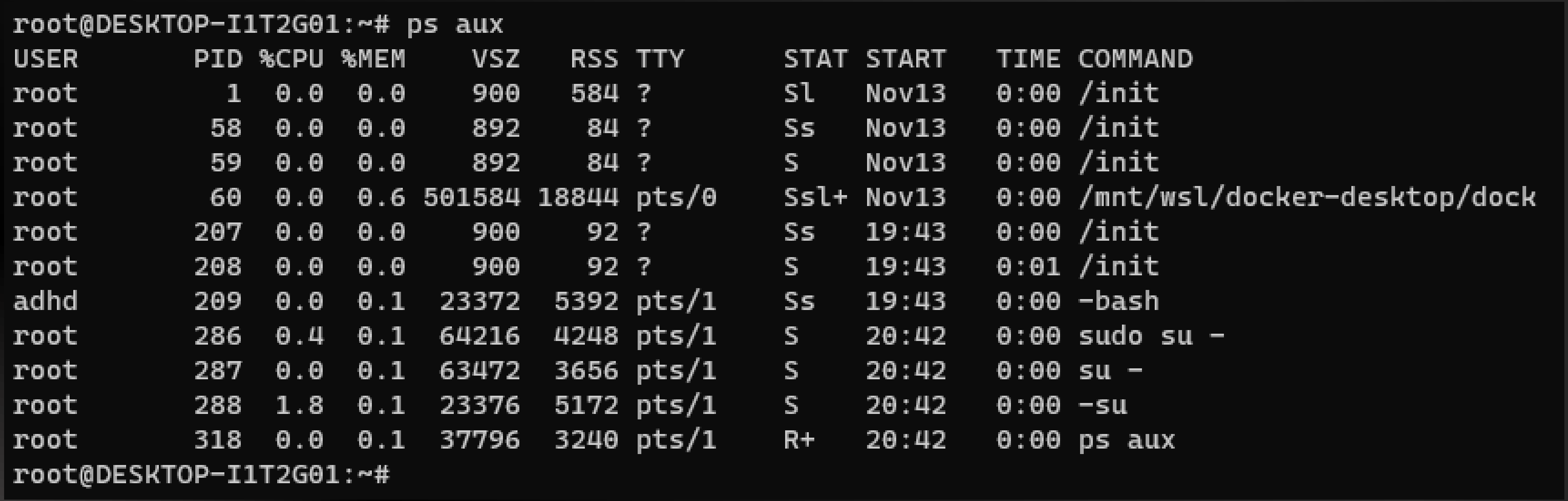


```
adhd@DESKTOP-I1T2G01:~$ nano sasquatch
```



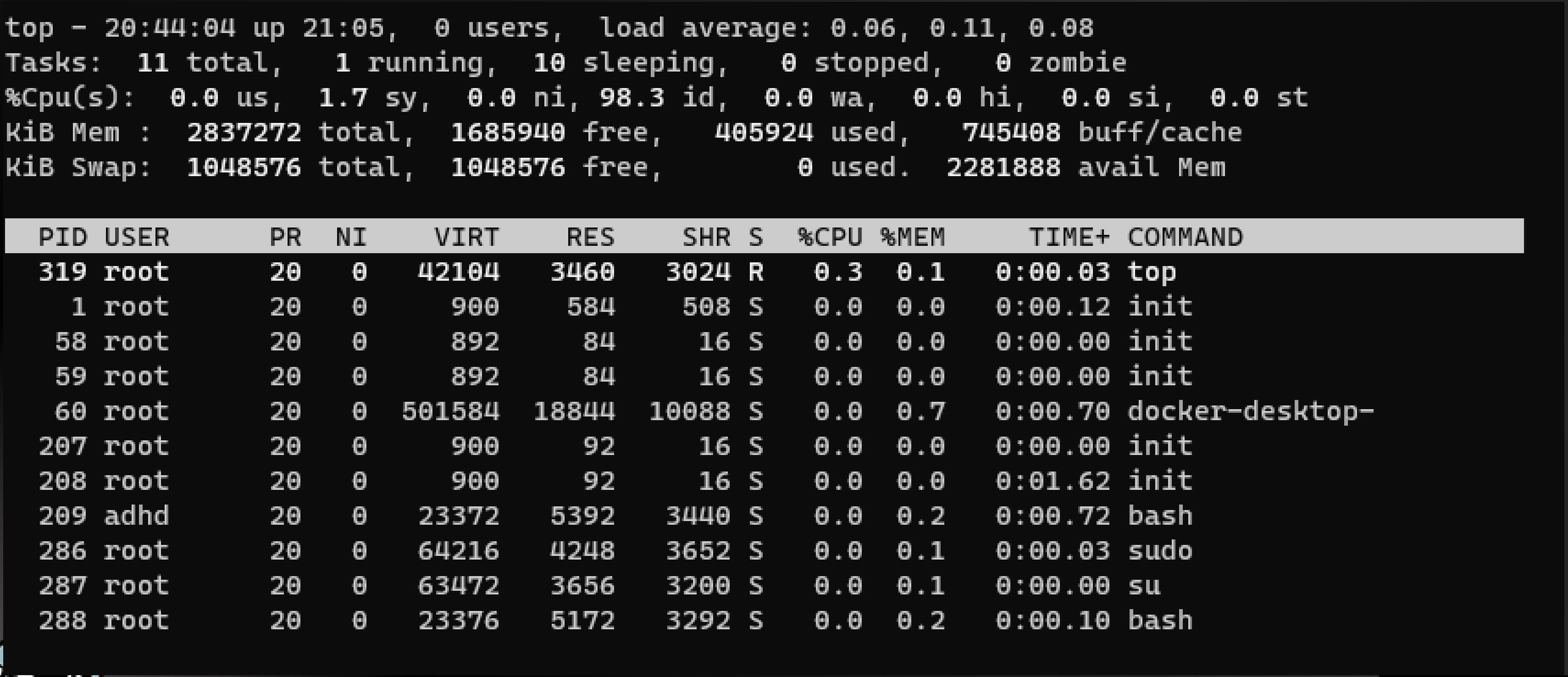
```
  GNU nano 2.9.3                     sasquatch                      Modified

In nano, the ^ = the Ctrl key

You write like you would in notepad

You use the Ctrl + O to "Write Out"

You use Ctrl + x to exit

It has a nice command reference at the bottom

Please, don't use nano for C and C++ code...




^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify     ^C Cur Pos
^X Exit        ^R Read File   ^\ Replace     ^U Uncut Text  ^T To Spell    ^_ Go To Line
```

Processes with ps aux



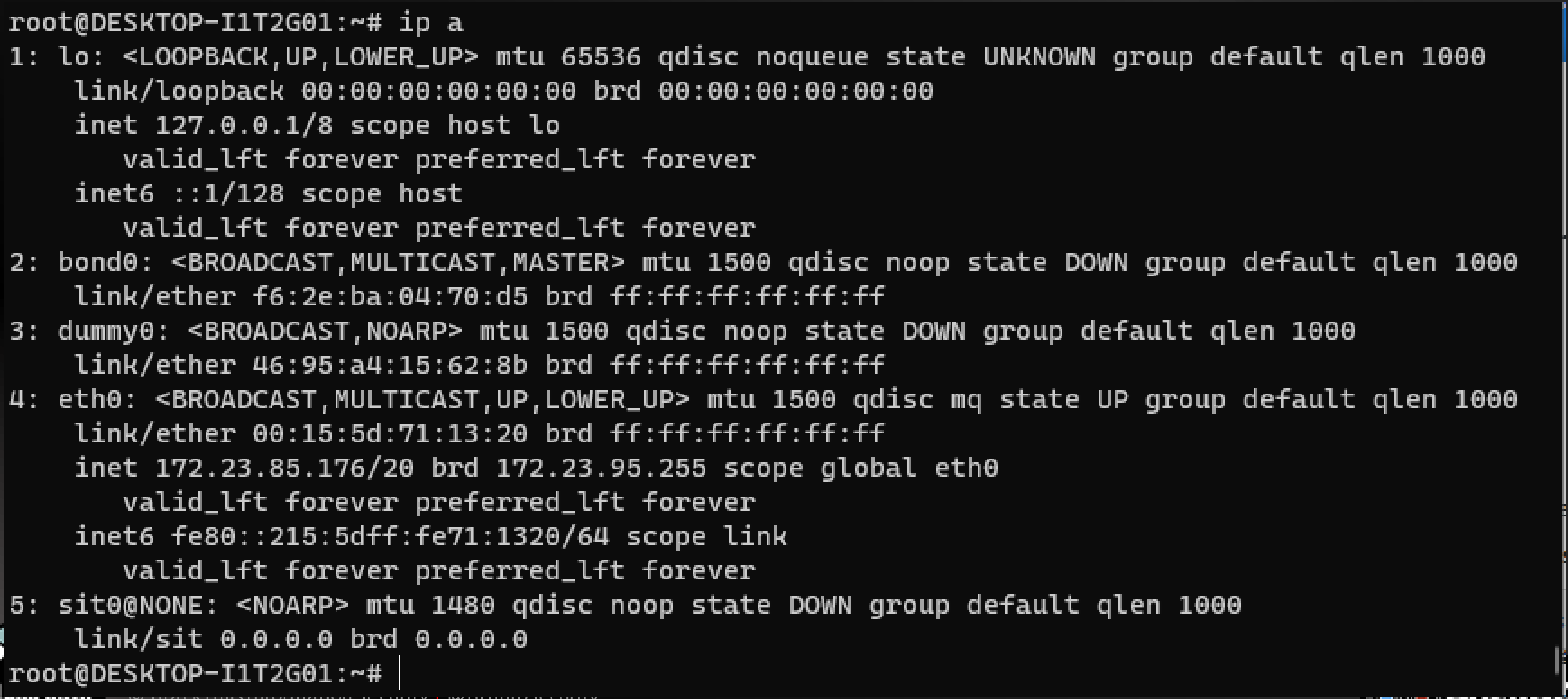
```
root@DESKTOP-I1T2G01:~# ps aux
USER         PID %CPU %MEM    VSZ   RSS TTY       STAT START   TIME COMMAND
root           1  0.0  0.0    900   584 ?         Sl   Nov13   0:00 /init
root          58  0.0  0.0    892    84 ?         Ss   Nov13   0:00 /init
root          59  0.0  0.0    892    84 ?         S    Nov13   0:00 /init
root          60  0.0  0.6 501584 18844 pts/0     Ssl+ Nov13   0:00 /mnt/wsl/docker-desktop/dock
root         207  0.0  0.0    900    92 ?         Ss   19:43   0:00 /init
root         208  0.0  0.0    900    92 ?         S    19:43   0:01 /init
adhd         209  0.0  0.1  23372  5392 pts/1     Ss   19:43   0:00 -bash
root         286  0.4  0.1  64216  4248 pts/1     S    20:42   0:00 sudo su -
root         287  0.0  0.1  63472  3656 pts/1     S    20:42   0:00 su -
root         288  1.8  0.1  23376  5172 pts/1     S    20:42   0:00 -su
root         318  0.0  0.1  37796  3240 pts/1     R+   20:42   0:00 ps aux
root@DESKTOP-I1T2G01:~#
```

Processes with top



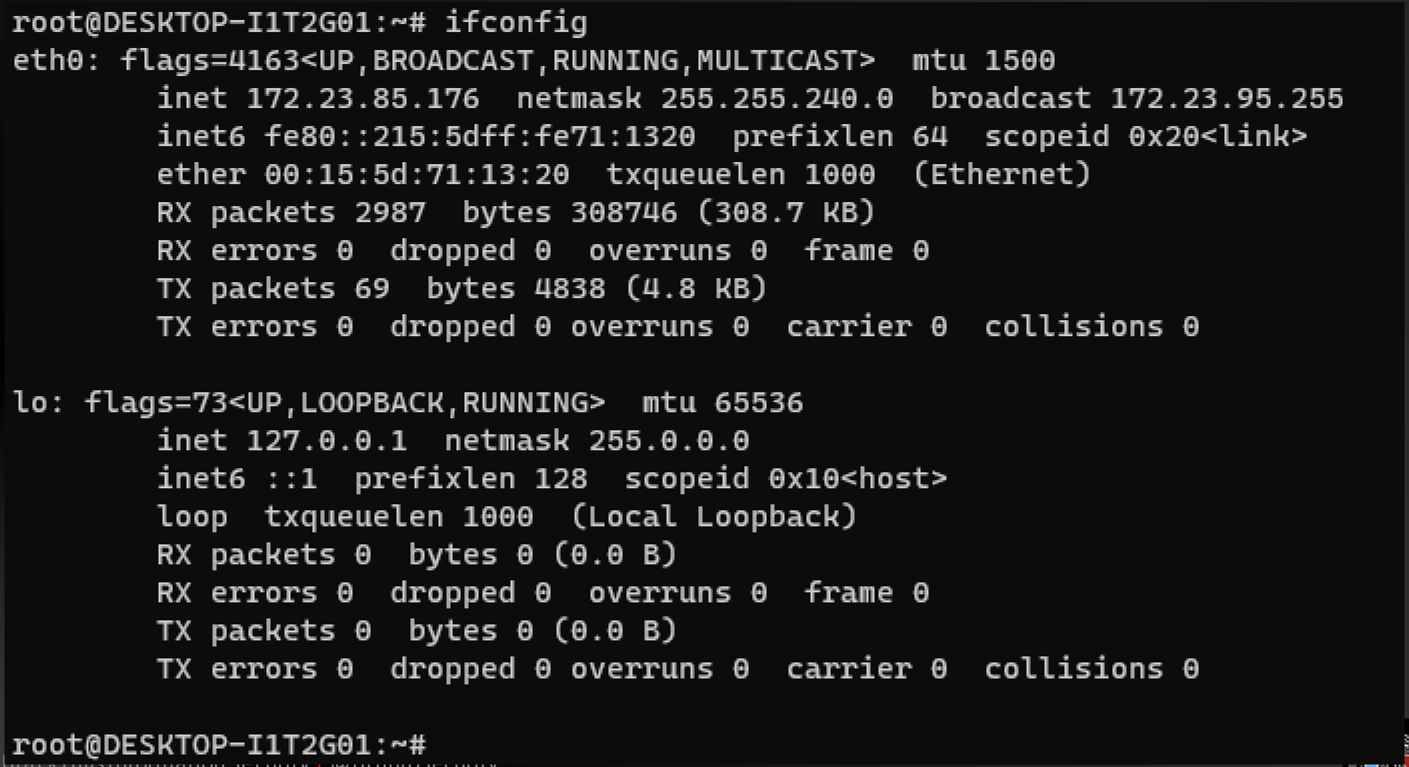
```
top - 20:44:04 up 21:05,  0 users,  load average: 0.06, 0.11, 0.08
Tasks:  11 total,   1 running,  10 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0.0 us,  1.7 sy,  0.0 ni, 98.3 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
KiB Mem :  2837272 total,  1685940 free,   405924 used,   745408 buff/cache
KiB Swap:  1048576 total,  1048576 free,        0 used.  2281888 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S  %CPU %MEM     TIME+ COMMAND
  319 root      20   0   42104   3460   3024 R   0.3  0.1   0:00.03 top
    1 root      20   0     900    584    508 S   0.0  0.0   0:00.12 init
   58 root      20   0     892     84     16 S   0.0  0.0   0:00.00 init
   59 root      20   0     892     84     16 S   0.0  0.0   0:00.00 init
   60 root      20   0  501584  18844  10088 S   0.0  0.7   0:00.70 docker-desktop-
  207 root      20   0     900     92     16 S   0.0  0.0   0:00.00 init
  208 root      20   0     900     92     16 S   0.0  0.0   0:01.62 init
  209 adhd      20   0   23372   5392   3440 S   0.0  0.2   0:00.72 bash
  286 root      20   0   64216   4248   3652 S   0.0  0.1   0:00.03 sudo
  287 root      20   0   63472   3656   3200 S   0.0  0.1   0:00.00 su
  288 root      20   0   23376   5172   3292 S   0.0  0.2   0:00.10 bash
```

IP info with ip a



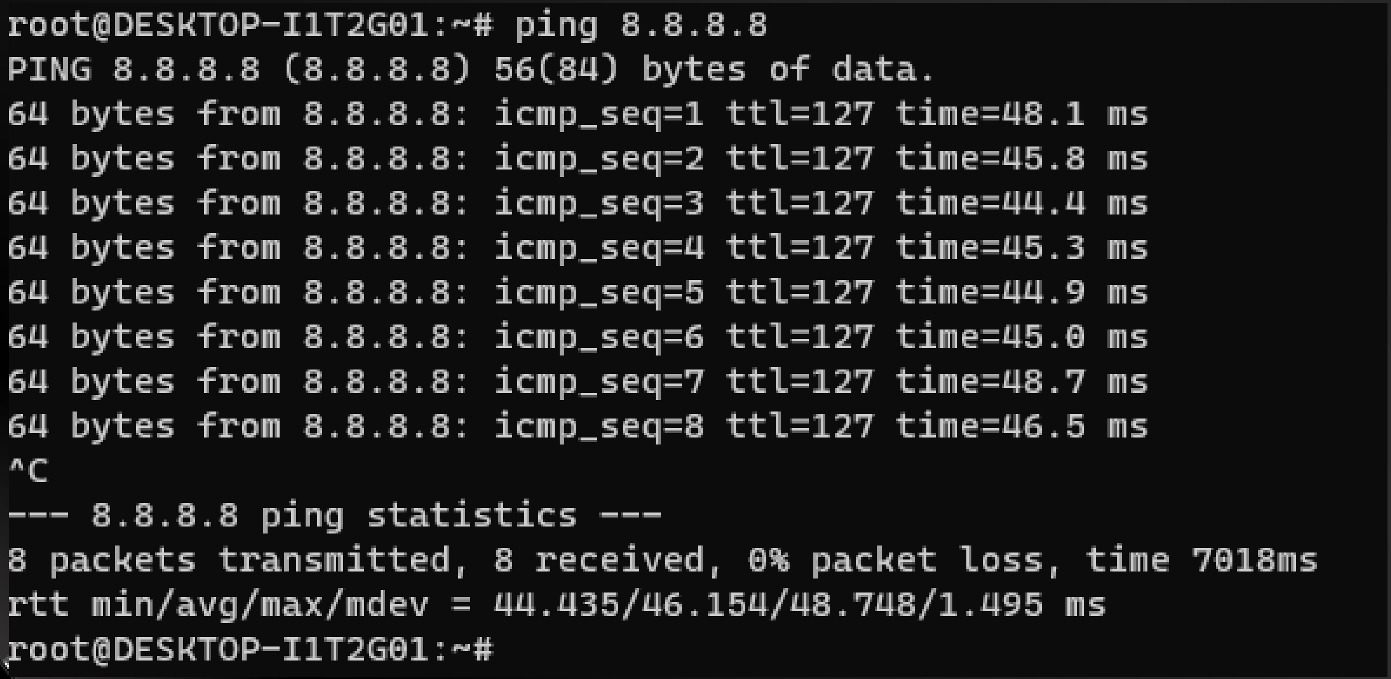
```
root@DESKTOP-I1T2G01:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: bond0: <BROADCAST,MULTICAST,MASTER> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether f6:2e:ba:04:70:d5 brd ff:ff:ff:ff:ff:ff
3: dummy0: <BROADCAST,NOARP> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 46:95:a4:15:62:8b brd ff:ff:ff:ff:ff:ff
4: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:15:5d:71:13:20 brd ff:ff:ff:ff:ff:ff
    inet 172.23.85.176/20 brd 172.23.95.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::215:5dff:fe71:1320/64 scope link
       valid_lft forever preferred_lft forever
5: sit0@NONE: <NOARP> mtu 1480 qdisc noop state DOWN group default qlen 1000
    link/sit 0.0.0.0 brd 0.0.0.0
root@DESKTOP-I1T2G01:~#
```

IP info with ifconfig



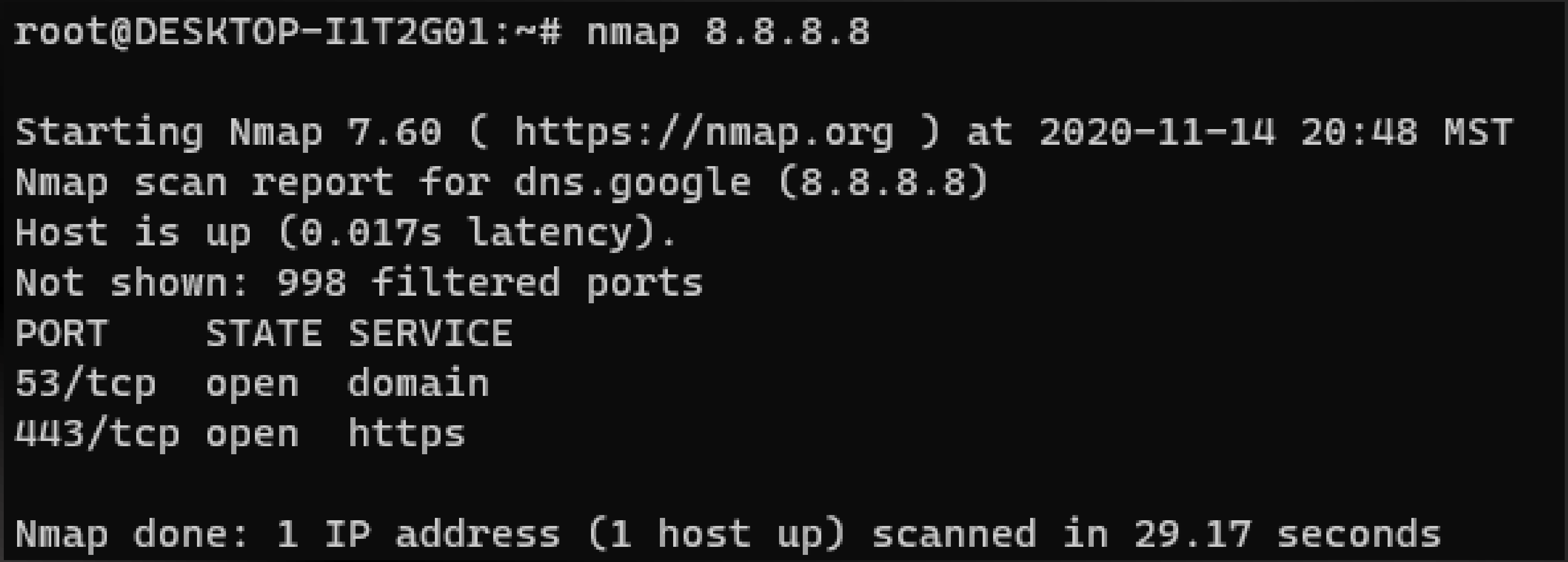
```
root@DESKTOP-I1T2G01:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.23.85.176  netmask 255.255.240.0  broadcast 172.23.95.255
        inet6 fe80::215:5dff:fe71:1320  prefixlen 64  scopeid 0x20<link>
        ether 00:15:5d:71:13:20  txqueuelen 1000  (Ethernet)
        RX packets 2987  bytes 308746 (308.7 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 69  bytes 4838 (4.8 KB)
        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 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

root@DESKTOP-I1T2G01:~#
```

ping



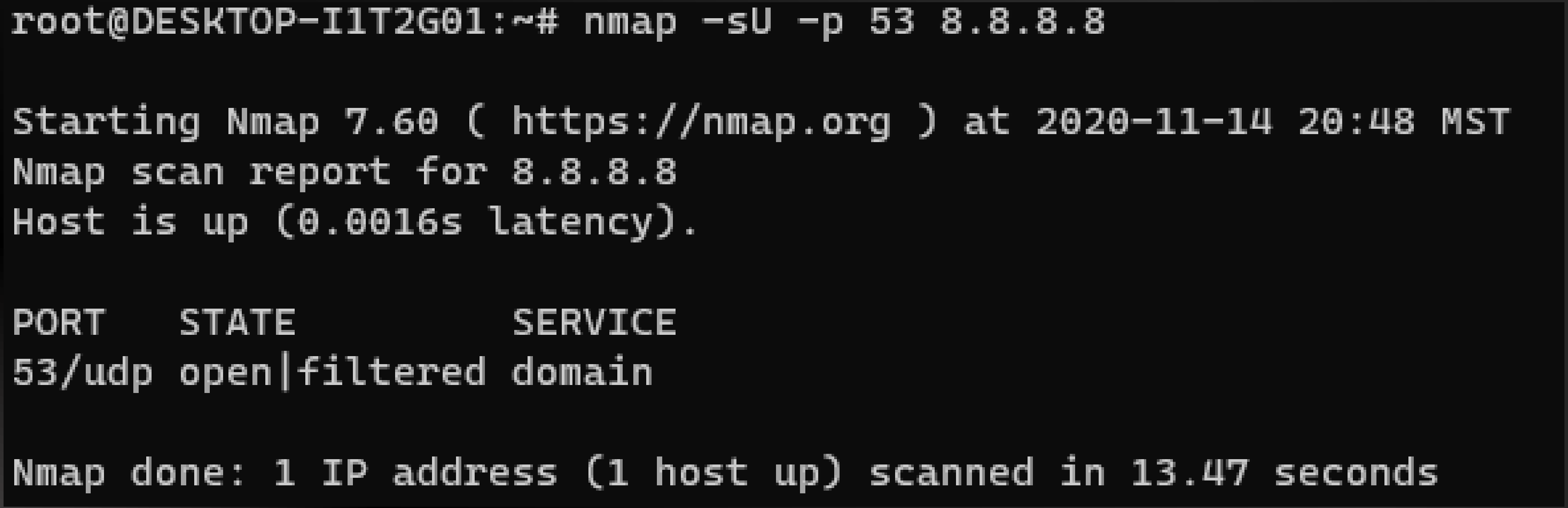
```
root@DESKTOP-I1T2G01:~# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=127 time=48.1 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=127 time=45.8 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=127 time=44.4 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=127 time=45.3 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=127 time=44.9 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=127 time=45.0 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=127 time=48.7 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=127 time=46.5 ms
^C
--- 8.8.8.8 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7018ms
rtt min/avg/max/mdev = 44.435/46.154/48.748/1.495 ms
root@DESKTOP-I1T2G01:~#
```

Open Remote Ports With Nmap



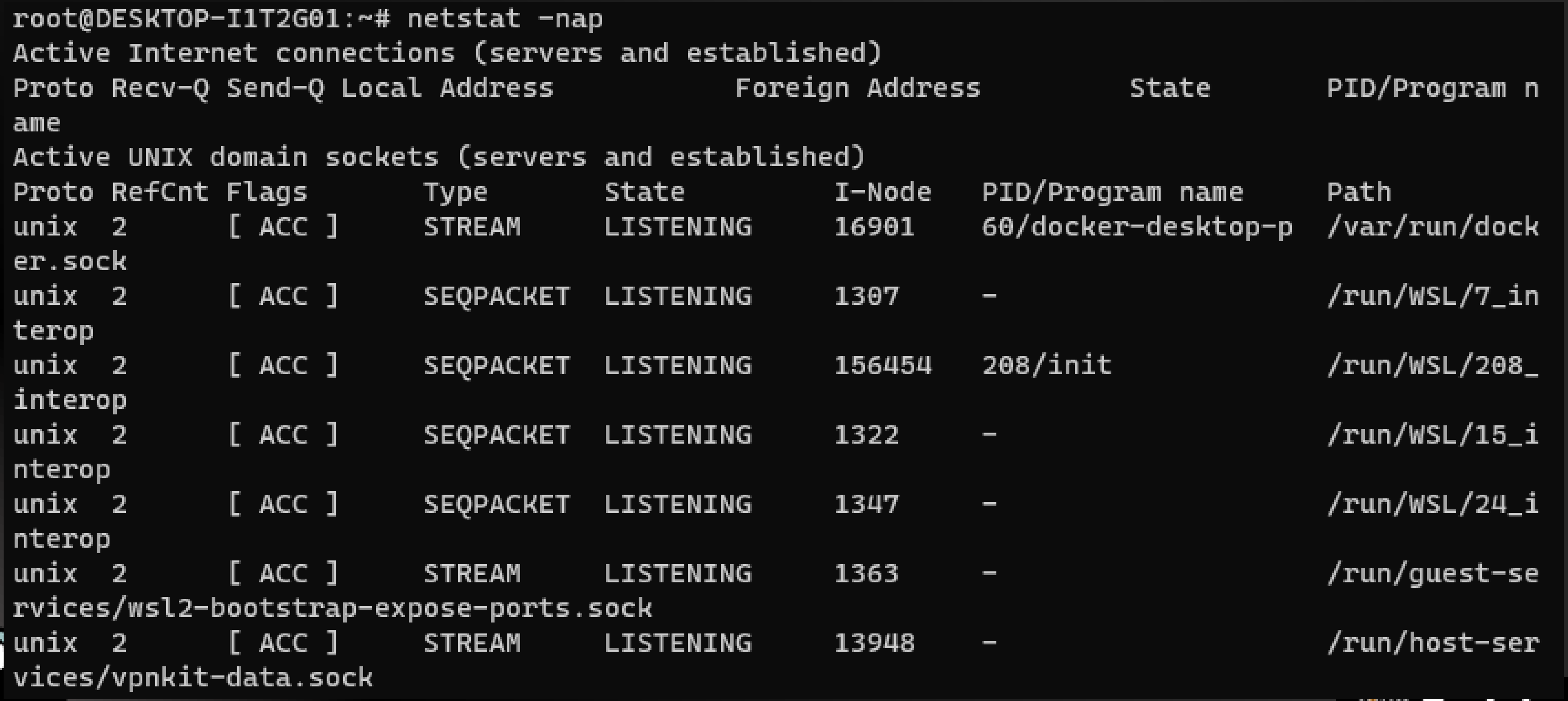
```
root@DESKTOP-I1T2G01:~# nmap 8.8.8.8

Starting Nmap 7.60 ( https://nmap.org ) at 2020-11-14 20:48 MST
Nmap scan report for dns.google (8.8.8.8)
Host is up (0.017s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
53/tcp  open  domain
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 29.17 seconds
```

Ping, Port, Parse....



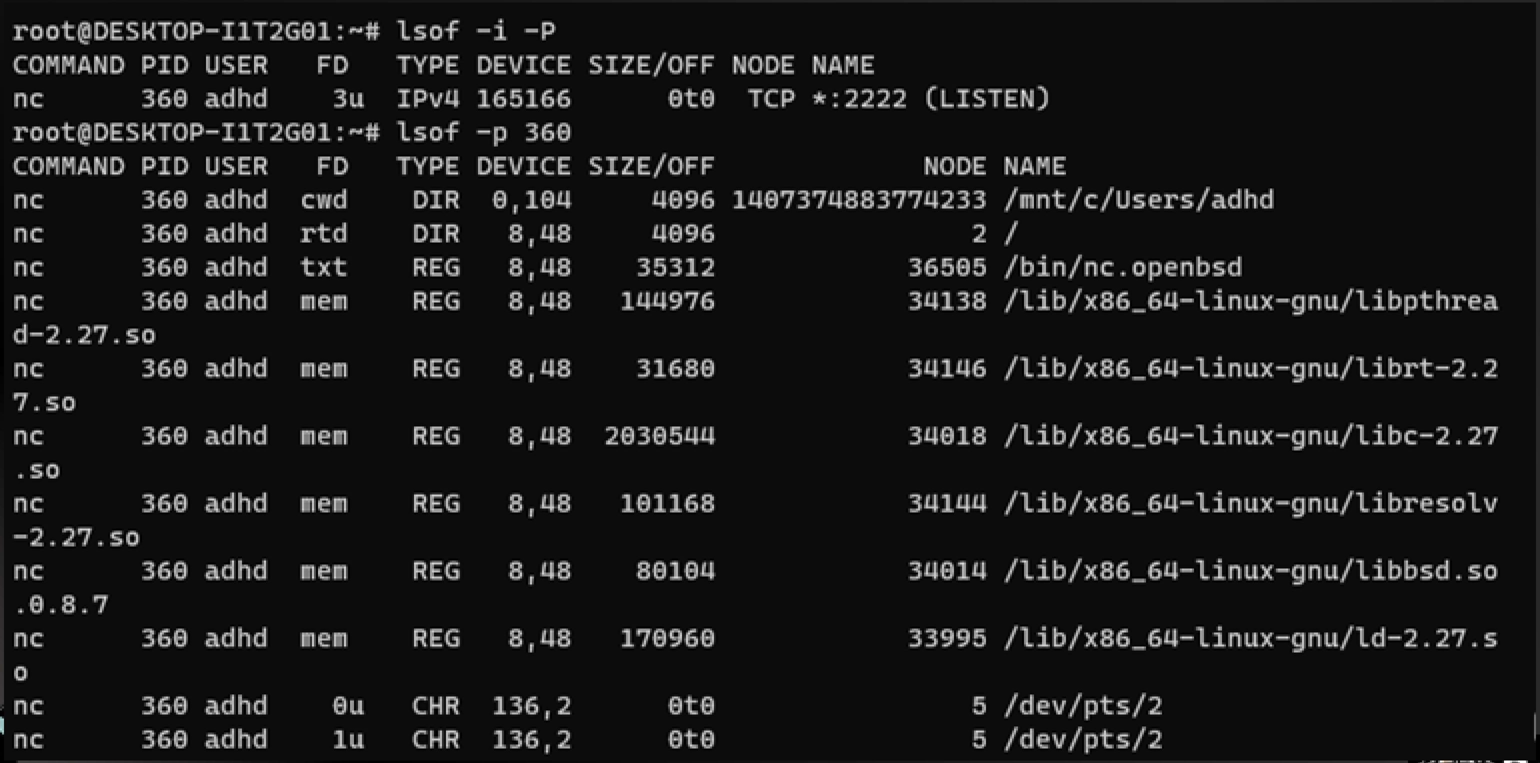
```
root@DESKTOP-I1T2G01:~# nmap -sU -p 53 8.8.8.8

Starting Nmap 7.60 ( https://nmap.org ) at 2020-11-14 20:48 MST
Nmap scan report for 8.8.8.8
Host is up (0.0016s latency).

PORT   STATE         SERVICE
53/udp open|filtered domain

Nmap done: 1 IP address (1 host up) scanned in 13.47 seconds
```

Network Connections: netstat



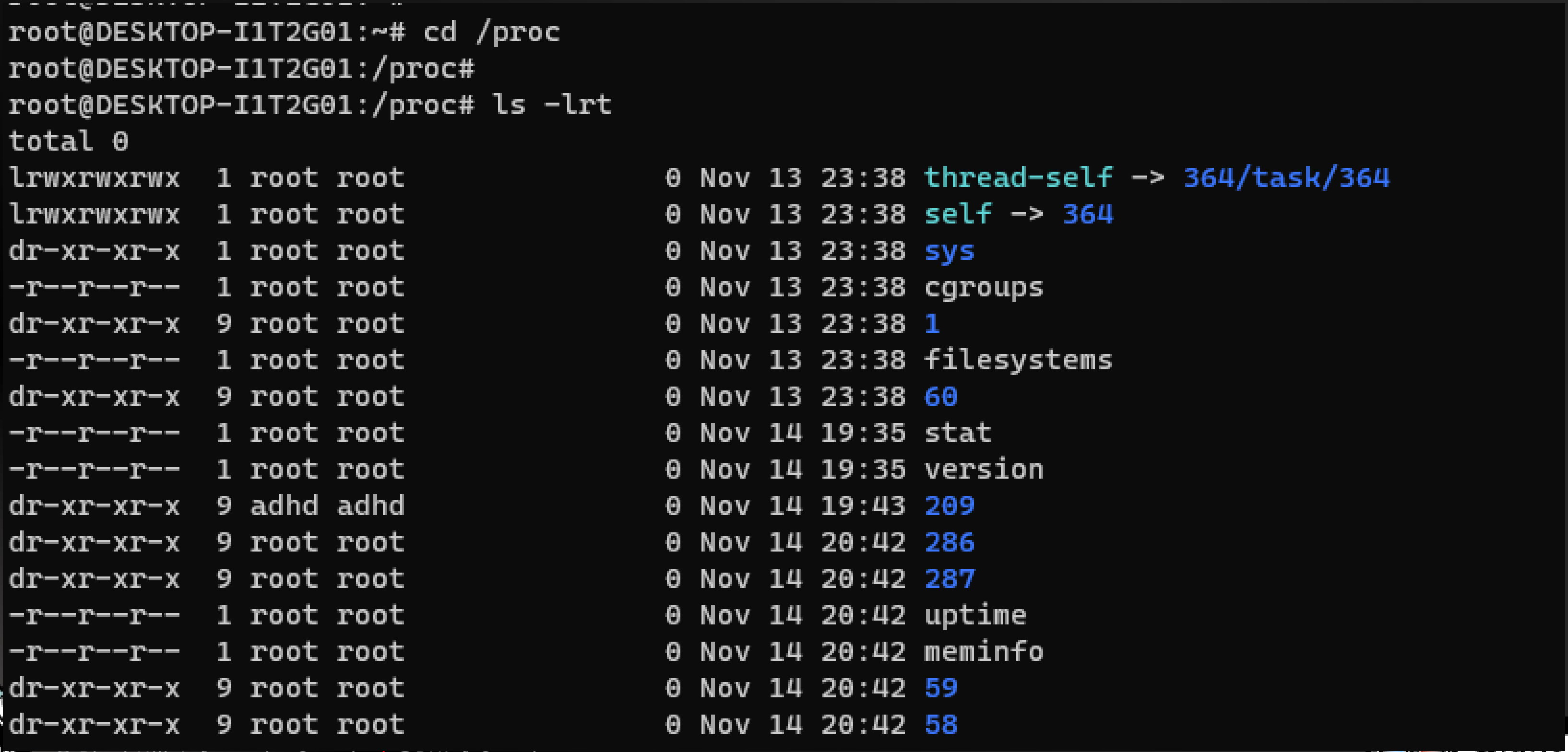
```
root@DESKTOP-I1T2G01:~# netstat -nap
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program n
ame
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node   PID/Program name     Path
unix  2      [ ACC ]     STREAM     LISTENING     16901    60/docker-desktop-p  /var/run/dock
er.sock
unix  2      [ ACC ]     SEQPACKET  LISTENING     1307     -                    /run/WSL/7_in
terop
unix  2      [ ACC ]     SEQPACKET  LISTENING     156454   208/init             /run/WSL/208_
interop
unix  2      [ ACC ]     SEQPACKET  LISTENING     1322     -                    /run/WSL/15_i
nterop
unix  2      [ ACC ]     SEQPACKET  LISTENING     1347     -                    /run/WSL/24_i
nterop
unix  2      [ ACC ]     STREAM     LISTENING     1363     -                    /run/guest-se
rvices/wsl2-bootstrap-expose-ports.sock
unix  2      [ ACC ]     STREAM     LISTENING     13948    -                    /run/host-ser
vices/vpnkit-data.sock
```

Network Connections: lsof -i -P



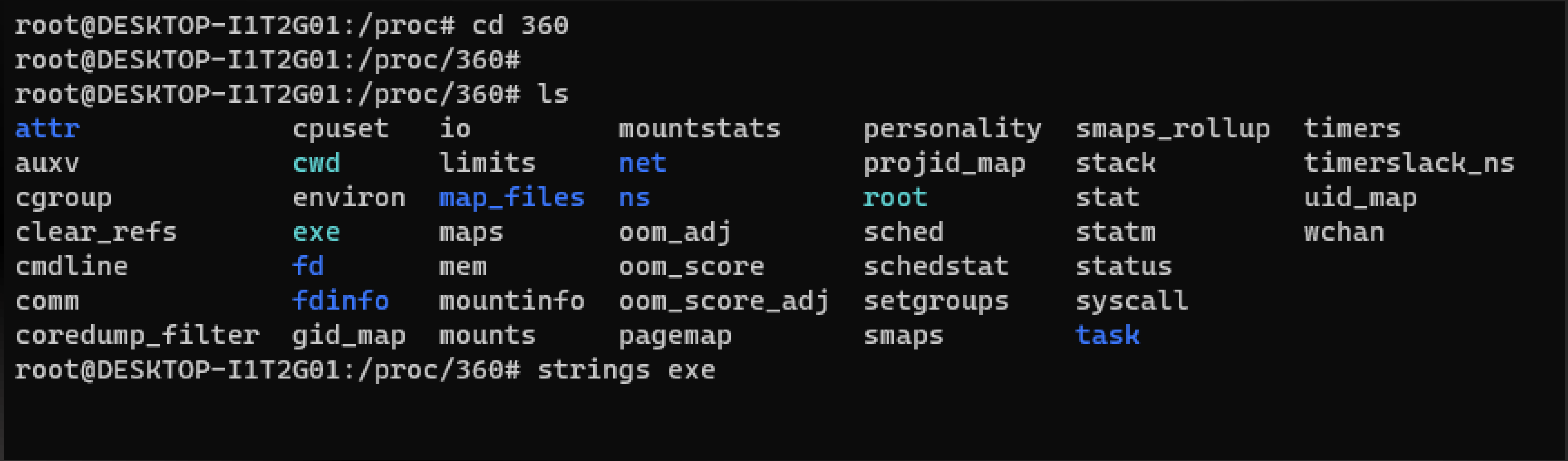
```
root@DESKTOP-I1T2G01:~# lsof -i -P
COMMAND PID USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
nc      360 adhd    3u  IPv4 165166      0t0  TCP *:2222 (LISTEN)
root@DESKTOP-I1T2G01:~# lsof -p 360
COMMAND PID USER   FD   TYPE DEVICE SIZE/OFF             NODE NAME
nc      360 adhd  cwd     DIR  0,104     4096 1407374883774233 /mnt/c/Users/adhd
nc      360 adhd  rtd     DIR   8,48     4096                2 /
nc      360 adhd  txt     REG   8,48    35312            36505 /bin/nc.openbsd
nc      360 adhd  mem     REG   8,48   144976            34138 /lib/x86_64-linux-gnu/libpthrea
d-2.27.so
nc      360 adhd  mem     REG   8,48    31680            34146 /lib/x86_64-linux-gnu/librt-2.2
7.so
nc      360 adhd  mem     REG   8,48  2030544            34018 /lib/x86_64-linux-gnu/libc-2.27
.so
nc      360 adhd  mem     REG   8,48   101168            34144 /lib/x86_64-linux-gnu/libresolv
-2.27.so
nc      360 adhd  mem     REG   8,48    80104            34014 /lib/x86_64-linux-gnu/libbsd.so
.0.8.7
nc      360 adhd  mem     REG   8,48   170960            33995 /lib/x86_64-linux-gnu/ld-2.27.s
o
nc      360 adhd    0u    CHR  136,2      0t0                5 /dev/pts/2
nc      360 adhd    1u    CHR  136,2      0t0                5 /dev/pts/2
```

Proc and Processes Part 1: proc



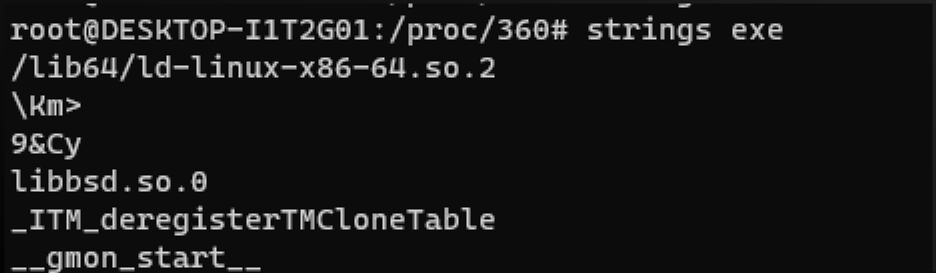
```
root@DESKTOP-I1T2G01:~# cd /proc
root@DESKTOP-I1T2G01:/proc#
root@DESKTOP-I1T2G01:/proc# ls -lrt
total 0
lrwxrwxrwx  1 root root              0 Nov 13 23:38 thread-self -> 364/task/364
lrwxrwxrwx  1 root root              0 Nov 13 23:38 self -> 364
dr-xr-xr-x  1 root root              0 Nov 13 23:38 sys
-r--r--r--  1 root root              0 Nov 13 23:38 cgroups
dr-xr-xr-x  9 root root              0 Nov 13 23:38 1
-r--r--r--  1 root root              0 Nov 13 23:38 filesystems
dr-xr-xr-x  9 root root              0 Nov 13 23:38 60
-r--r--r--  1 root root              0 Nov 14 19:35 stat
-r--r--r--  1 root root              0 Nov 14 19:35 version
dr-xr-xr-x  9 adhd adhd              0 Nov 14 19:43 209
dr-xr-xr-x  9 root root              0 Nov 14 20:42 286
dr-xr-xr-x  9 root root              0 Nov 14 20:42 287
-r--r--r--  1 root root              0 Nov 14 20:42 uptime
-r--r--r--  1 root root              0 Nov 14 20:42 meminfo
dr-xr-xr-x  9 root root              0 Nov 14 20:42 59
dr-xr-xr-x  9 root root              0 Nov 14 20:42 58
```

Proc and Processes Part 2: proc

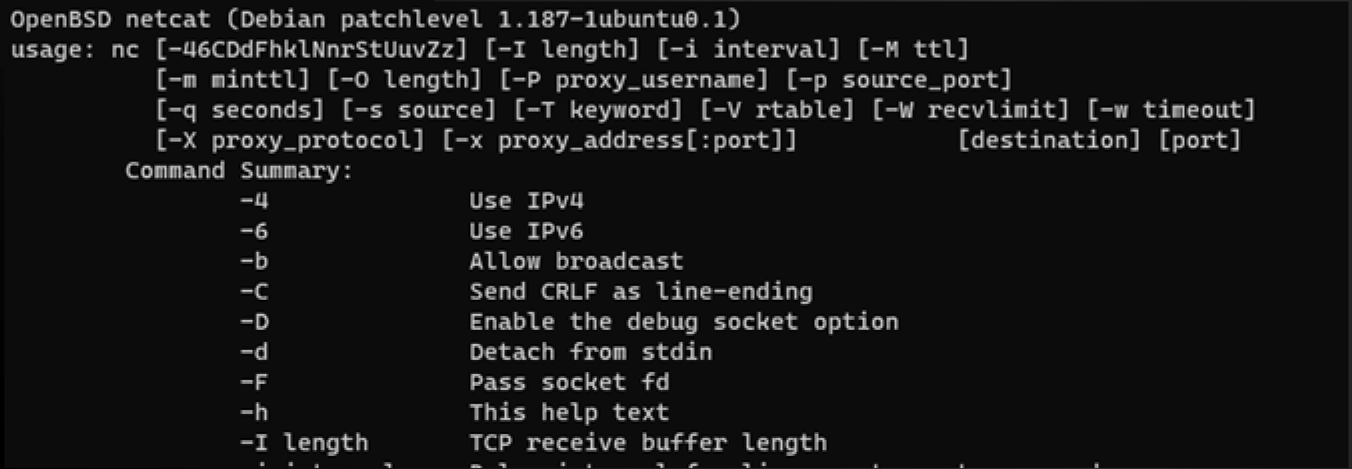


```
root@DESKTOP-I1T2G01:/proc# cd 360
root@DESKTOP-I1T2G01:/proc/360#
root@DESKTOP-I1T2G01:/proc/360# ls
attr             cpuset   io         mountstats     personality  smaps_rollup  timers
auxv             cwd      limits     net            projid_map   stack         timerslack_ns
cgroup           environ  map_files  ns             root         stat          uid_map
clear_refs       exe      maps       oom_adj        sched        statm         wchan
cmdline          fd       mem        oom_score      schedstat    status
comm             fdinfo   mountinfo  oom_score_adj  setgroups    syscall
coredump_filter  gid_map  mounts     pagemap        smaps        task
root@DESKTOP-I1T2G01:/proc/360# strings exe
```

Proc and Processes Part 3: Strings

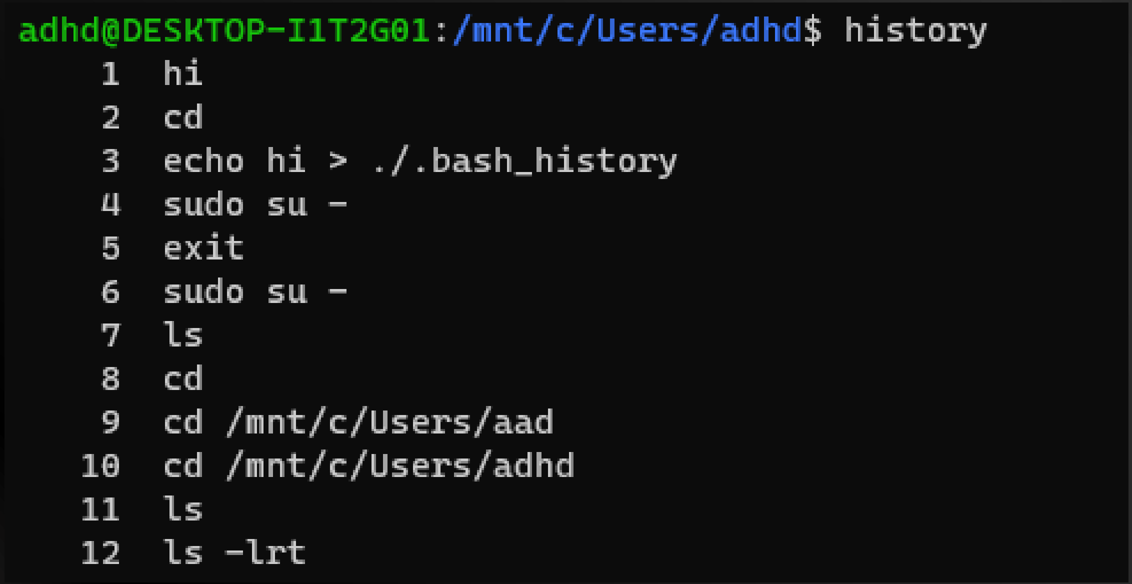


```
root@DESKTOP-I1T2G01:/proc/360# strings exe
/lib64/ld-linux-x86-64.so.2
\Km>
9&Cy
libbsd.so.0
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
arc4random_uniform
```



```
OpenBSD netcat (Debian patchlevel 1.187-1ubuntu0.1)
usage: nc [-46CDdFhklNnrStUuvZz] [-I length] [-i interval] [-M ttl]
          [-m minttl] [-O length] [-P proxy_username] [-p source_port]
          [-q seconds] [-s source] [-T keyword] [-V rtable] [-W recvlimit] [-w timeout]
          [-X proxy_protocol] [-x proxy_address[:port]]           [destination] [port]
        Command Summary:
                -4              Use IPv4
                -6              Use IPv6
                -b              Allow broadcast
                -C              Send CRLF as line-ending
                -D              Enable the debug socket option
                -d              Detach from stdin
                -F              Pass socket fd
                -h              This help text
                -I length       TCP receive buffer length
```

Bash History



```
adhd@DESKTOP-I1T2G01:/mnt/c/Users/adhd$ history
    1  hi
    2  cd
    3  echo hi > ./.bash_history
    4  sudo su -
    5  exit
    6  sudo su -
    7  ls
    8  cd
    9  cd /mnt/c/Users/aad
   10  cd /mnt/c/Users/adhd
   11  ls
   12  ls -lrt
```

LAB: Linux CLI