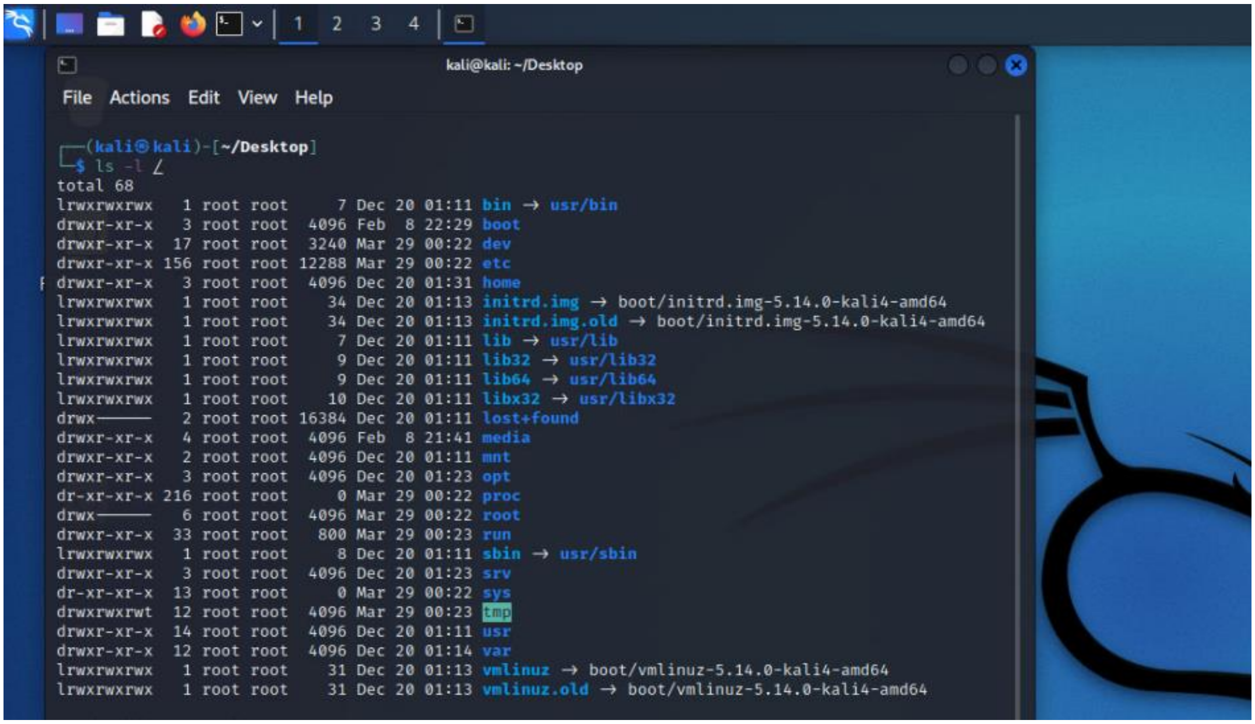
Part I: Linux File Structure and Important Files

Step-1

One of the most interesting parts of kali linux is the way their Files are structured. There is a main folder called **“/”** with-in which all of the subfolders exist.”**/home**” is for user personal files,”**/etc.**” has system and configuration files,”**/boot**” contains boot and kernel files, etc.

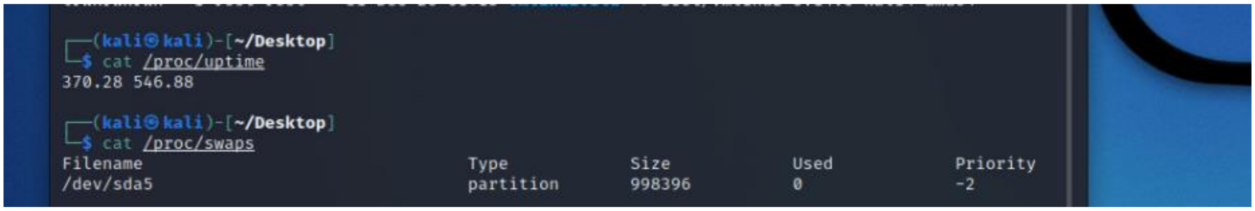


```
┌──(kali㉿kali)-[~/Desktop]
└─$ ls -l /
total 68
lrwxrwxrwx   1 root root     7 Dec 20 01:11 bin → usr/bin
drwxr-xr-x   3 root root  4096 Feb  8 22:29 boot
drwxr-xr-x  17 root root  3240 Mar 29 00:22 dev
drwxr-xr-x 156 root root 12288 Mar 29 00:22 etc
drwxr-xr-x   3 root root  4096 Dec 20 01:31 home
lrwxrwxrwx   1 root root    34 Dec 20 01:13 initrd.img → boot/initrd.img-5.14.0-kali4-amd64
lrwxrwxrwx   1 root root    34 Dec 20 01:13 initrd.img.old → boot/initrd.img-5.14.0-kali4-amd64
lrwxrwxrwx   1 root root     7 Dec 20 01:11 lib → usr/lib
lrwxrwxrwx   1 root root     9 Dec 20 01:11 lib32 → usr/lib32
lrwxrwxrwx   1 root root     9 Dec 20 01:11 lib64 → usr/lib64
lrwxrwxrwx   1 root root    10 Dec 20 01:11 libx32 → usr/libx32
drwx------   2 root root 16384 Dec 20 01:11 lost+found
drwxr-xr-x   4 root root  4096 Feb  8 21:41 media
drwxr-xr-x   2 root root  4096 Dec 20 01:11 mnt
drwxr-xr-x   3 root root  4096 Dec 20 01:23 opt
dr-xr-xr-x 216 root root     0 Mar 29 00:22 proc
drwx------   6 root root  4096 Mar 29 00:22 root
drwxr-xr-x  33 root root   800 Mar 29 00:23 run
lrwxrwxrwx   1 root root     8 Dec 20 01:11 sbin → usr/sbin
drwxr-xr-x   3 root root  4096 Dec 20 01:23 srv
dr-xr-xr-x  13 root root     0 Mar 29 00:22 sys
drwxrwxrwt  12 root root  4096 Mar 29 00:23 tmp
drwxr-xr-x  14 root root  4096 Dec 20 01:11 usr
drwxr-xr-x  12 root root  4096 Dec 20 01:14 var
lrwxrwxrwx   1 root root    31 Dec 20 01:13 vmlinuz → boot/vmlinuz-5.14.0-kali4-amd64
lrwxrwxrwx   1 root root    31 Dec 20 01:13 vmlinuz.old → boot/vmlinuz-5.14.0-kali4-amd64
```

If you go to the root folder **“/”** and then use the “**ls -l**” command it is going to display all of the subfolders for you.

Step-2

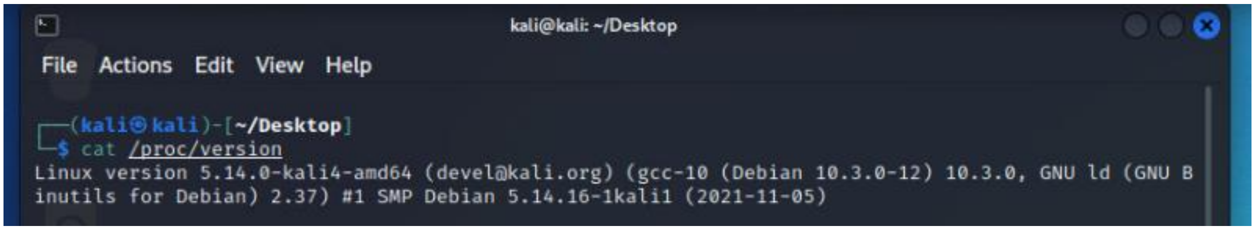
Kali linux has some important files that contains useful information.” **/etc/apt/sources.list**” contains sources list of Debian packages.”**/etc/passwd**” has local user account information.”**/etc/shadow**” contain local user password (**hash form**),”**/proc/crypto**” List all ciphers etc.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ cat /proc/uptime
370.28 546.88

┌──(kali㉿kali)-[~/Desktop]
└─$ cat /proc/swaps
Filename                                Type            Size            Used            Priority
/dev/sda5                               partition       998396          0               -2
```

”**/proc/uptime**” Returns two values; first is the total number of seconds the system has been switched on. The second is the sum of the idle time of all the processors

“**/proc/swaps**” Contains information about system swap space.

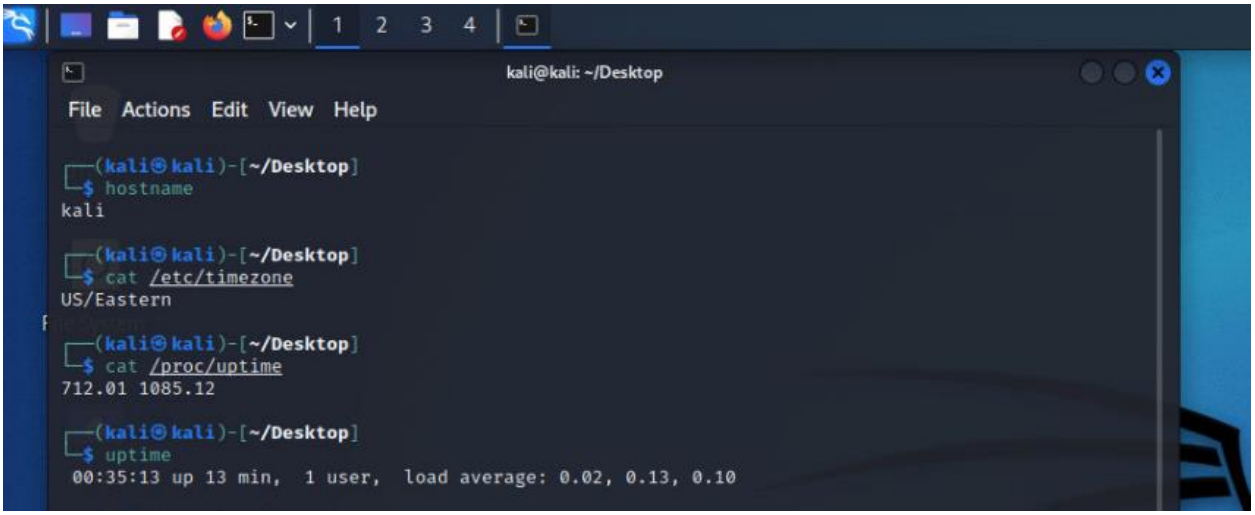


```
┌──(kali㉿kali)-[~/Desktop]
└─$ cat /proc/version
Linux version 5.14.0-kali4-amd64 (devel@kali.org) (gcc-10 (Debian 10.3.0-12) 10.3.0, GNU ld (GNU B
inutils for Debian) 2.37) #1 SMP Debian 5.14.16-1kali1 (2021-11-05)
```

PART II: COLLECTING BASIC VOLATILE INFORMATION

Step-3

Here we are using hostname to check our profile name and read the time zone and the system uptime



```
┌──(kali㉿kali)-[~/Desktop]
└─$ hostname
kali

┌──(kali㉿kali)-[~/Desktop]
└─$ cat /etc/timezone
US/Eastern

┌──(kali㉿kali)-[~/Desktop]
└─$ cat /proc/uptime
712.01 1085.12

┌──(kali㉿kali)-[~/Desktop]
└─$ uptime
 00:35:13 up 13 min,  1 user,  load average: 0.02, 0.13, 0.10
```

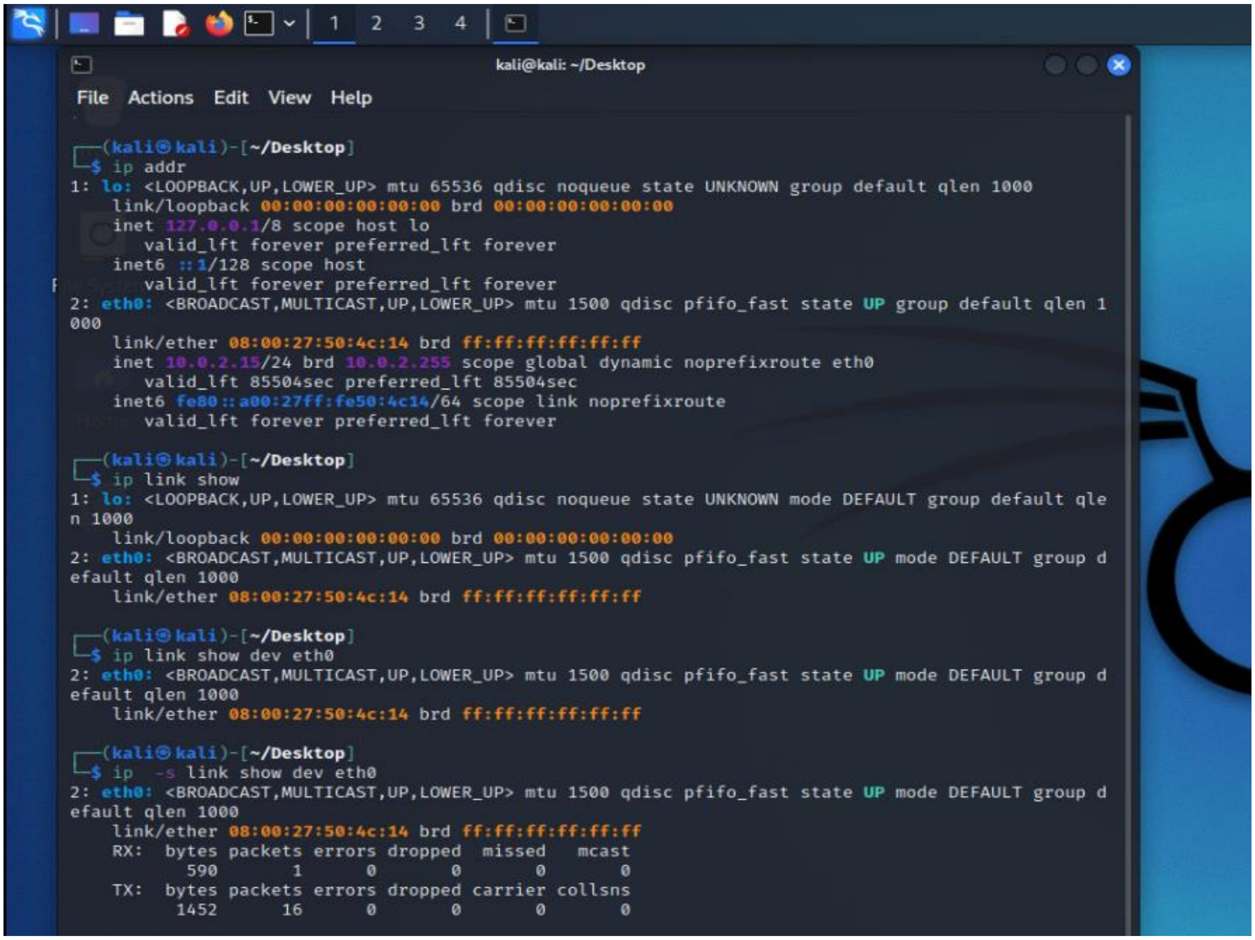
Step-4

In this part we are collecting network information.

“**Ip addr**” is used to display id address of all the interfaces

“**Ip link show**” is used to list down all of the interfaces

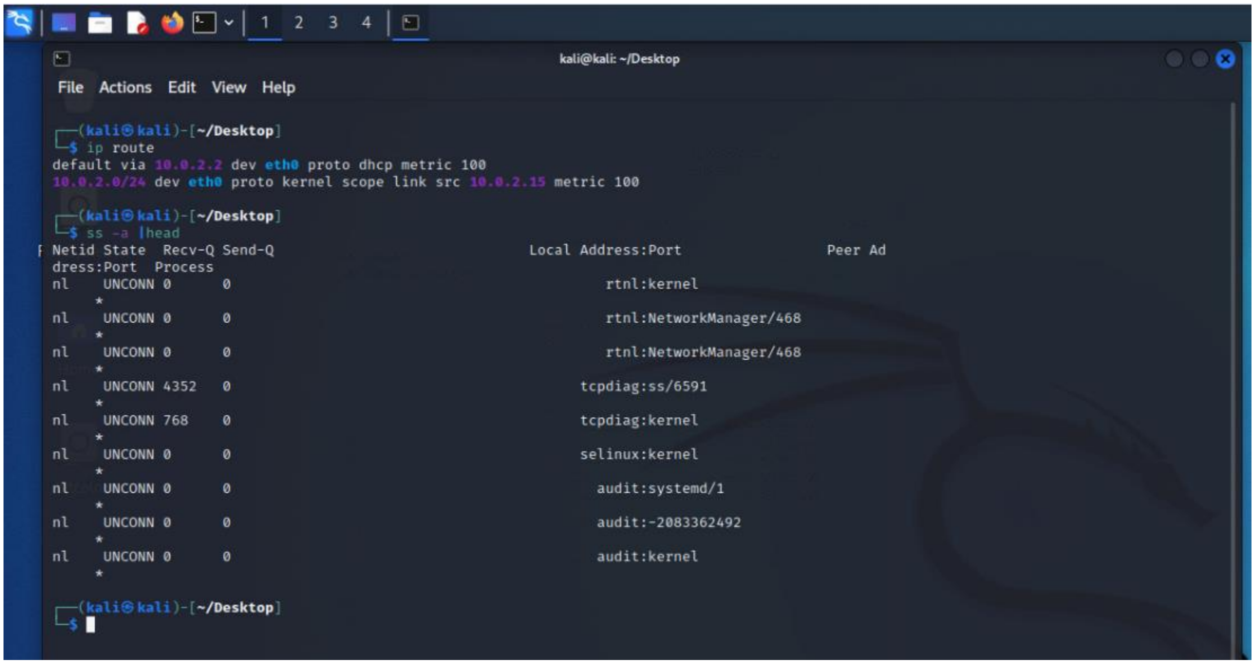
“**Ip link show dev (interface-name)**” shows information related to the specific interface



```
┌──(kali㉿kali)-[~/Desktop]
└─$ ip addr
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: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1
000
    link/ether 08:00:27:50:4c:14 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 85504sec preferred_lft 85504sec
    inet6 fe80::a00:27ff:fe50:4c14/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(kali㉿kali)-[~/Desktop]
└─$ ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group default qle
n 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP mode DEFAULT group d
efault qlen 1000
    link/ether 08:00:27:50:4c:14 brd ff:ff:ff:ff:ff:ff

┌──(kali㉿kali)-[~/Desktop]
└─$ ip link show dev eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP mode DEFAULT group d
efault qlen 1000
    link/ether 08:00:27:50:4c:14 brd ff:ff:ff:ff:ff:ff

┌──(kali㉿kali)-[~/Desktop]
└─$ ip  -s link show dev eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP mode DEFAULT group d
efault qlen 1000
    link/ether 08:00:27:50:4c:14 brd ff:ff:ff:ff:ff:ff
    RX:  bytes packets errors dropped  missed   mcast
           590       1      0       0       0       0
    TX:  bytes packets errors dropped carrier collsns
          1452      16      0       0       0       0
```

"Ip route default" is used to show the default route or the gateway

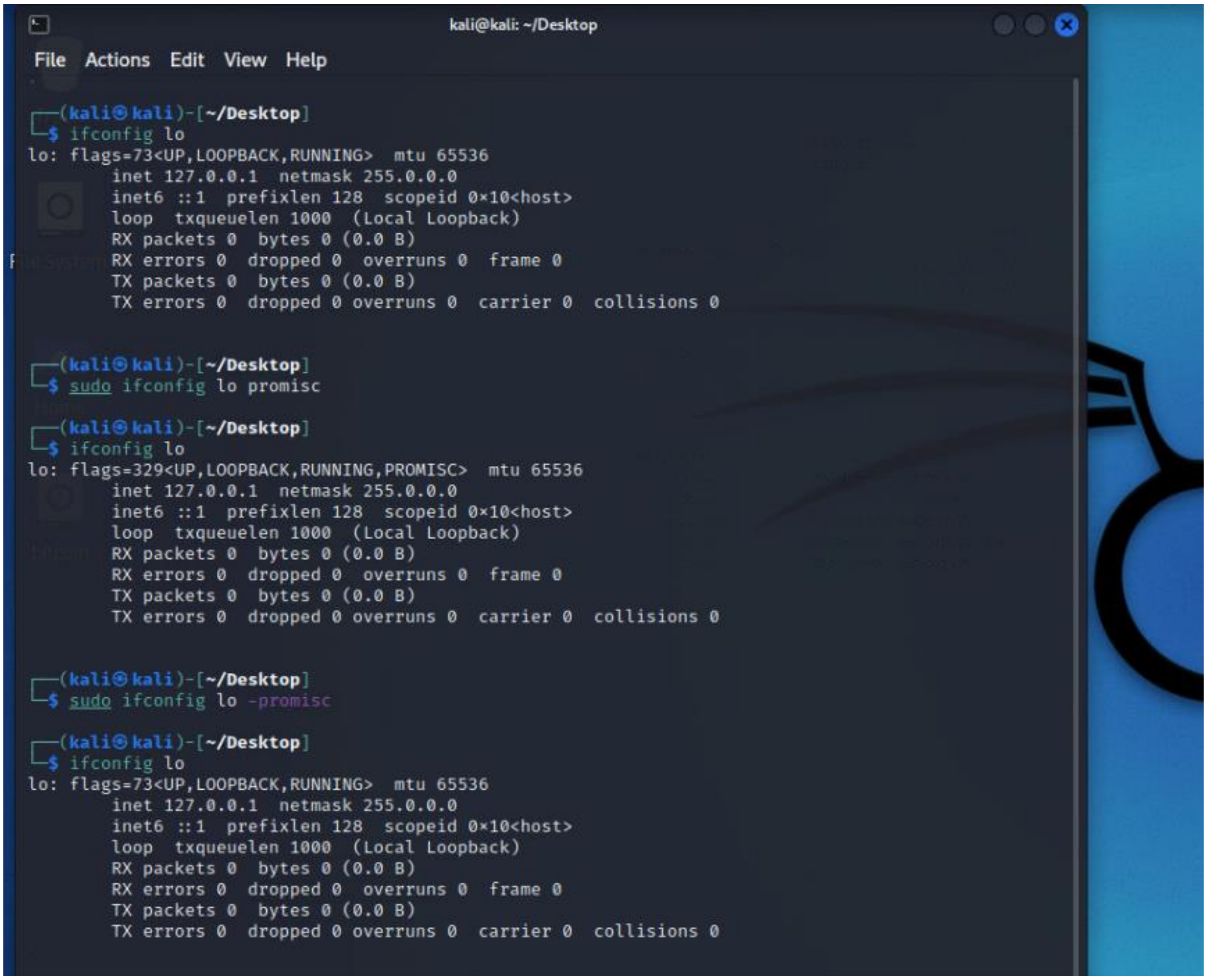
"**Ss -a | head**" Display socket statistics



```
┌──(kali㉿kali)-[~/Desktop]
└─$ ip route
default via 10.0.2.2 dev eth0 proto dhcp metric 100
10.0.2.0/24 dev eth0 proto kernel scope link src 10.0.2.15 metric 100

┌──(kali㉿kali)-[~/Desktop]
└─$ ss -a |head
Netid State  Recv-Q Send-Q                            Local Address:Port                 Peer Ad
dress:Port  Process
nl    UNCONN 0      0                                       rtnl:kernel
     *
nl    UNCONN 0      0                                       rtnl:NetworkManager/468
     *
nl    UNCONN 0      0                                       rtnl:NetworkManager/468
     *
nl    UNCONN 4352   0                                    tcpdiag:ss/6591
     *
nl    UNCONN 768    0                                    tcpdiag:kernel
     *
nl    UNCONN 0      0                                    selinux:kernel
     *
nl    UNCONN 0      0                                      audit:systemd/1
     *
nl    UNCONN 0      0                                      audit:-2083362492
     *
nl    UNCONN 0      0                                      audit:kernel
     *

┌──(kali㉿kali)-[~/Desktop]
└─$ 
```

Step-5

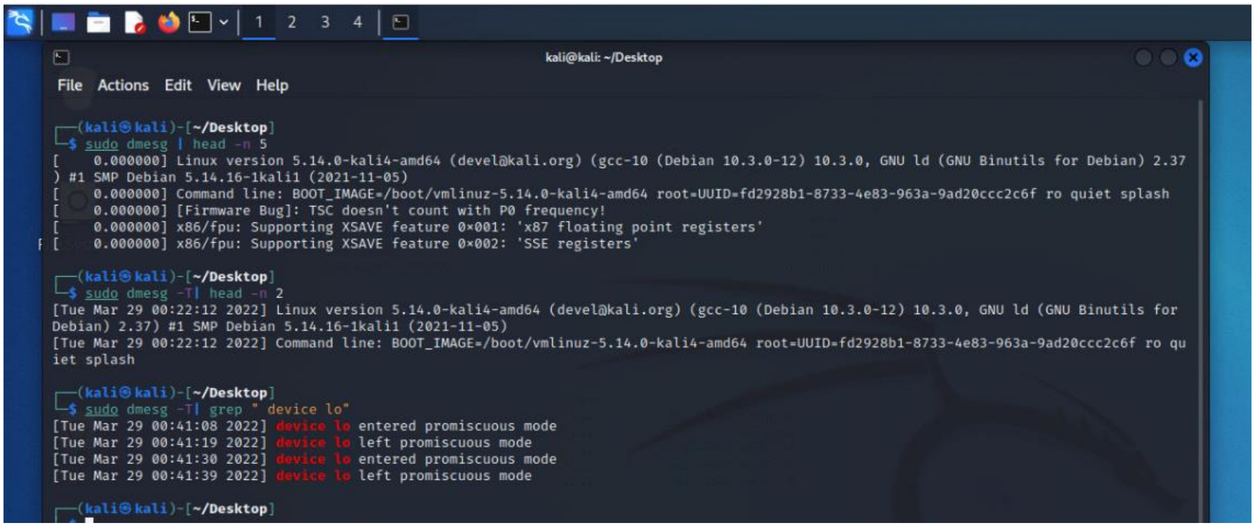
Here we set our interface in **promiscuous mode** and saw that the number of packets increases this means that they might be accepting malicious packets.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ ifconfig lo
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


┌──(kali㉿kali)-[~/Desktop]
└─$ sudo ifconfig lo promisc

┌──(kali㉿kali)-[~/Desktop]
└─$ ifconfig lo
lo: flags=329<UP,LOOPBACK,RUNNING,PROMISC>  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


┌──(kali㉿kali)-[~/Desktop]
└─$ sudo ifconfig lo -promisc

┌──(kali㉿kali)-[~/Desktop]
└─$ ifconfig lo
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
```

Step-6

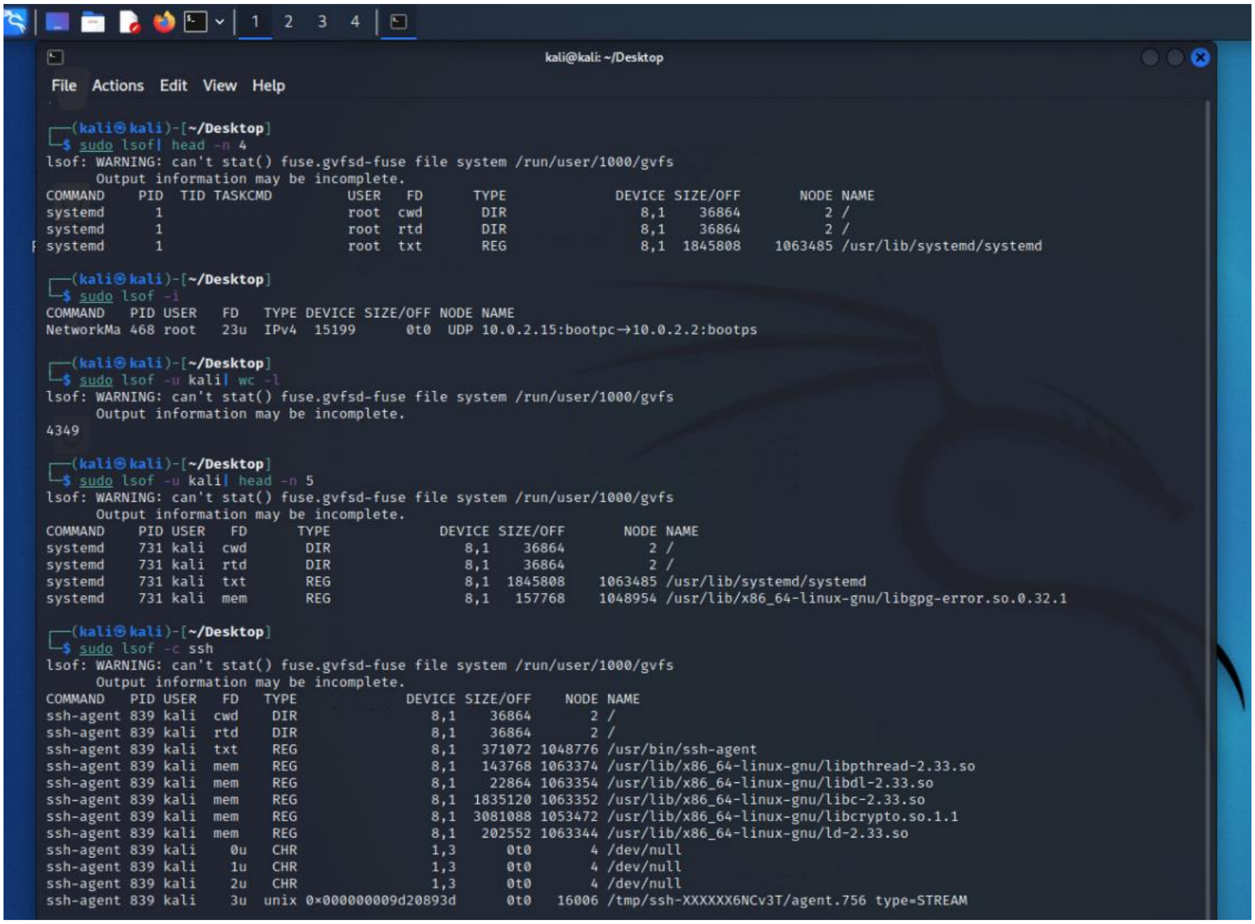
The **dmesg** command is used to retrieve the Kernel messages to help investigators track actions performed on the investigated machine. This command displays all messages since the kernel is started.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo dmesg | head -n 5
[    0.000000] Linux version 5.14.0-kali4-amd64 (devel@kali.org) (gcc-10 (Debian 10.3.0-12) 10.3.0, GNU ld (GNU Binutils for Debian) 2.37
) #1 SMP Debian 5.14.16-1kali1 (2021-11-05)
[    0.000000] Command line: BOOT_IMAGE=/boot/vmlinuz-5.14.0-kali4-amd64 root=UUID=fd2928b1-8733-4e83-963a-9ad20ccc2c6f ro quiet splash
[    0.000000] [Firmware Bug]: TSC doesn't count with P0 frequency!
[    0.000000] x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point registers'
[    0.000000] x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'

┌──(kali㉿kali)-[~/Desktop]
└─$ sudo dmesg -T| head -n 2
[Tue Mar 29 00:22:12 2022] Linux version 5.14.0-kali4-amd64 (devel@kali.org) (gcc-10 (Debian 10.3.0-12) 10.3.0, GNU ld (GNU Binutils for
Debian) 2.37) #1 SMP Debian 5.14.16-1kali1 (2021-11-05)
[Tue Mar 29 00:22:12 2022] Command line: BOOT_IMAGE=/boot/vmlinuz-5.14.0-kali4-amd64 root=UUID=fd2928b1-8733-4e83-963a-9ad20ccc2c6f ro qu
iet splash

┌──(kali㉿kali)-[~/Desktop]
└─$ sudo dmesg -T| grep " device lo"
[Tue Mar 29 00:41:08 2022] device lo entered promiscuous mode
[Tue Mar 29 00:41:19 2022] device lo left promiscuous mode
[Tue Mar 29 00:41:30 2022] device lo entered promiscuous mode
[Tue Mar 29 00:41:39 2022] device lo left promiscuous mode

┌──(kali㉿kali)-[~/Desktop]
```

Step-7

Lsof is used to see all of the open files



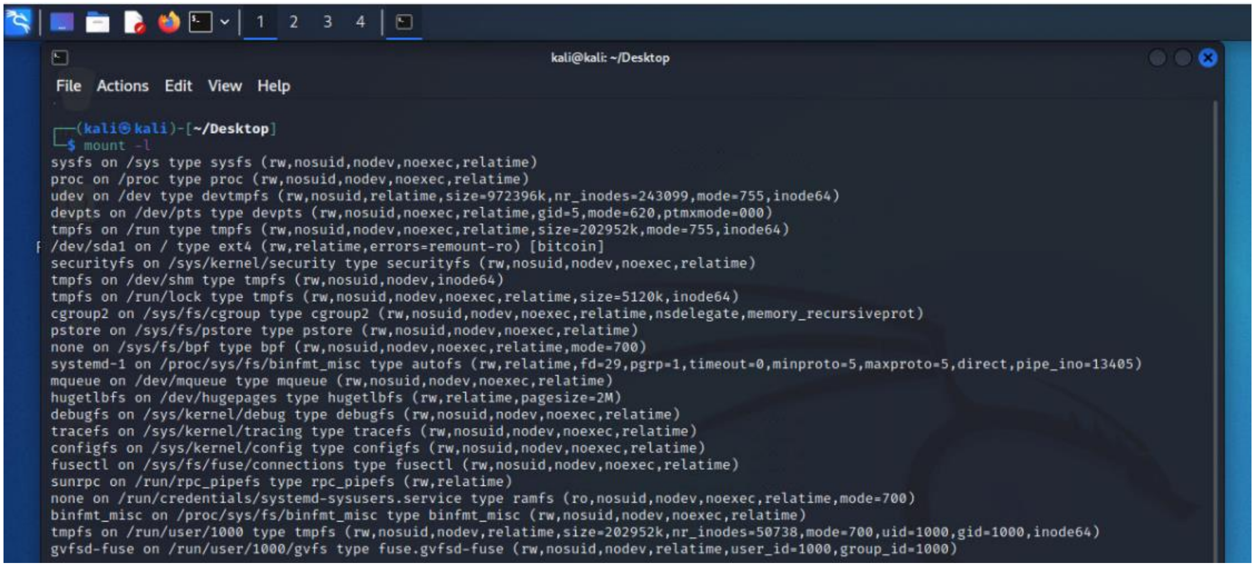
```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo lsof| head -n 4
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1000/gvfs
      Output information may be incomplete.
COMMAND     PID  TID TASKCMD          USER   FD      TYPE             DEVICE SIZE/OFF       NODE NAME
systemd       1                       root  cwd       DIR                8,1    36864          2 /
systemd       1                       root  rtd       DIR                8,1    36864          2 /
systemd       1                       root  txt       REG                8,1  1845808    1063485 /usr/lib/systemd/systemd

┌──(kali㉿kali)-[~/Desktop]
└─$ sudo lsof -i
COMMAND   PID USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
NetworkMa 468 root   23u  IPv4  15199      0t0  UDP 10.0.2.15:bootpc→10.0.2.2:bootps

┌──(kali㉿kali)-[~/Desktop]
└─$ sudo lsof -u kali| wc -l
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1000/gvfs
      Output information may be incomplete.
4349

┌──(kali㉿kali)-[~/Desktop]
└─$ sudo lsof -u kali| head -n 5
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1000/gvfs
      Output information may be incomplete.
COMMAND     PID USER   FD      TYPE             DEVICE SIZE/OFF       NODE NAME
systemd     731 kali  cwd       DIR                8,1    36864          2 /
systemd     731 kali  rtd       DIR                8,1    36864          2 /
systemd     731 kali  txt       REG                8,1  1845808    1063485 /usr/lib/systemd/systemd
systemd     731 kali  mem       REG                8,1   157768    1048954 /usr/lib/x86_64-linux-gnu/libgpg-error.so.0.32.1

┌──(kali㉿kali)-[~/Desktop]
└─$ sudo lsof -c ssh
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1000/gvfs
      Output information may be incomplete.
COMMAND   PID USER   FD   TYPE             DEVICE SIZE/OFF    NODE NAME
ssh-agent 839 kali  cwd    DIR                8,1    36864       2 /
ssh-agent 839 kali  rtd    DIR                8,1    36864       2 /
ssh-agent 839 kali  txt    REG                8,1   371072 1048776 /usr/bin/ssh-agent
ssh-agent 839 kali  mem    REG                8,1   143768 1063374 /usr/lib/x86_64-linux-gnu/libpthread-2.33.so
ssh-agent 839 kali  mem    REG                8,1    22864 1063354 /usr/lib/x86_64-linux-gnu/libdl-2.33.so
ssh-agent 839 kali  mem    REG                8,1  1835120 1063352 /usr/lib/x86_64-linux-gnu/libc-2.33.so
ssh-agent 839 kali  mem    REG                8,1  3081088 1053472 /usr/lib/x86_64-linux-gnu/libcrypto.so.1.1
ssh-agent 839 kali  mem    REG                8,1   202552 1063344 /usr/lib/x86_64-linux-gnu/ld-2.33.so
ssh-agent 839 kali    0u   CHR                1,3      0t0       4 /dev/null
ssh-agent 839 kali    1u   CHR                1,3      0t0       4 /dev/null
ssh-agent 839 kali    2u   CHR                1,3      0t0       4 /dev/null
ssh-agent 839 kali    3u  unix 0x000000009d20893d      0t0   16006 /tmp/ssh-XXXXXX6NCv3T/agent.756 type=STREAM
```

“**lsof -u <user>**” is used to display files opened by a specific user

“**lsof -c <process-name>**” Display all opened files by particular process.

Step-8

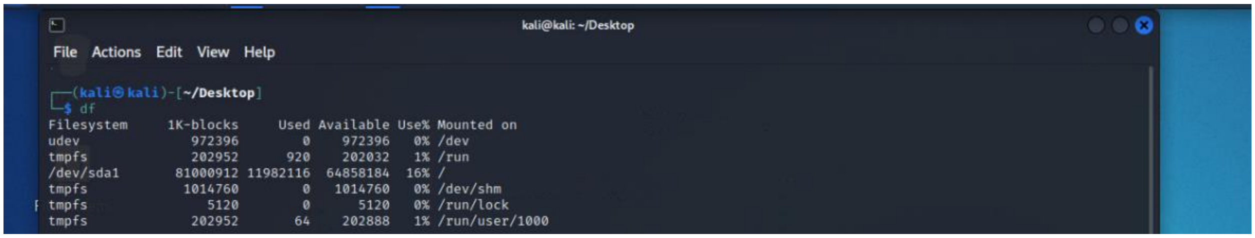
The command “**mount**” list the mounted file systems.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ mount -l
sysfs on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
udev on /dev type devtmpfs (rw,nosuid,relatime,size=972396k,nr_inodes=243099,mode=755,inode64)
devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000)
tmpfs on /run type tmpfs (rw,nosuid,nodev,noexec,relatime,size=202952k,mode=755,inode64)
/dev/sda1 on / type ext4 (rw,relatime,errors=remount-ro) [bitcoin]
securityfs on /sys/kernel/security type securityfs (rw,nosuid,nodev,noexec,relatime)
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev,inode64)
tmpfs on /run/lock type tmpfs (rw,nosuid,nodev,noexec,relatime,size=5120k,inode64)
cgroup2 on /sys/fs/cgroup type cgroup2 (rw,nosuid,nodev,noexec,relatime,nsdelegate,memory_recursiveprot)
pstore on /sys/fs/pstore type pstore (rw,nosuid,nodev,noexec,relatime)
none on /sys/fs/bpf type bpf (rw,nosuid,nodev,noexec,relatime,mode=700)
systemd-1 on /proc/sys/fs/binfmt_misc type autofs (rw,relatime,fd=29,pgrp=1,timeout=0,minproto=5,maxproto=5,direct,pipe_ino=13405)
mqueue on /dev/mqueue type mqueue (rw,nosuid,nodev,noexec,relatime)
hugetlbfs on /dev/hugepages type hugetlbfs (rw,relatime,pagesize=2M)
debugfs on /sys/kernel/debug type debugfs (rw,nosuid,nodev,noexec,relatime)
tracefs on /sys/kernel/tracing type tracefs (rw,nosuid,nodev,noexec,relatime)
configfs on /sys/kernel/config type configfs (rw,nosuid,nodev,noexec,relatime)
fusectl on /sys/fs/fuse/connections type fusectl (rw,nosuid,nodev,noexec,relatime)
sunrpc on /run/rpc_pipefs type rpc_pipefs (rw,relatime)
none on /run/credentials/systemd-sysusers.service type ramfs (ro,nosuid,nodev,noexec,relatime,mode=700)
binfmt_misc on /proc/sys/fs/binfmt_misc type binfmt_misc (rw,nosuid,nodev,noexec,relatime)
tmpfs on /run/user/1000 type tmpfs (rw,nosuid,nodev,relatime,size=202952k,nr_inodes=50738,mode=700,uid=1000,gid=1000,inode64)
gvfsd-fuse on /run/user/1000/gvfs type fuse.gvfsd-fuse (rw,nosuid,nodev,relatime,user_id=1000,group_id=1000)
```

Step-9

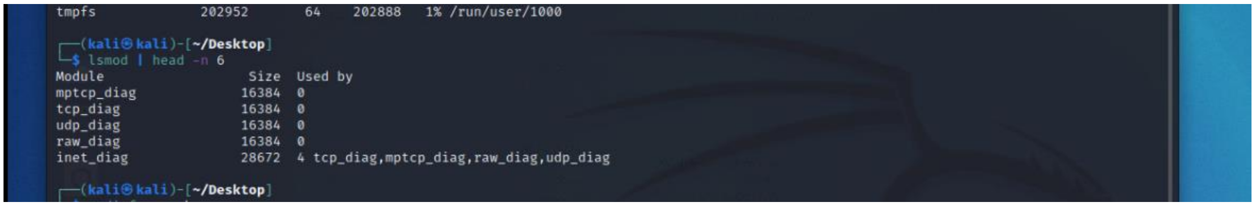
“**df**” displays the amounts of free.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ df
Filesystem     1K-blocks     Used Available Use% Mounted on
udev              972396        0    972396   0% /dev
tmpfs             202952      920    202032   1% /run
/dev/sda1       81000912 11982116  64858184  16% /
tmpfs            1014760        0   1014760   0% /dev/shm
tmpfs               5120        0      5120   0% /run/lock
tmpfs             202952       64    202888   1% /run/user/1000
```

Step-10

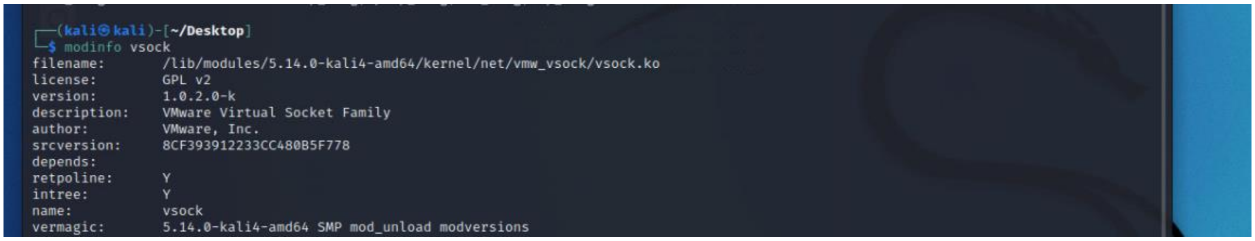
To display the kernel loaded modules, use the **lsmod** command



```
tmpfs             202952       64    202888   1% /run/user/1000

┌──(kali㉿kali)-[~/Desktop]
└─$ lsmod | head -n 6
Module                  Size  Used by
mptcp_diag             16384  0
tcp_diag               16384  0
udp_diag               16384  0
raw_diag               16384  0
inet_diag              28672  4 tcp_diag,mptcp_diag,raw_diag,udp_diag

┌──(kali㉿kali)-[~/Desktop]
```

Step-11

modinfo to display the information of a particular module



```
┌──(kali㉿kali)-[~/Desktop]
└─$ modinfo vsock
filename:       /lib/modules/5.14.0-kali4-amd64/kernel/net/vmw_vsock/vsock.ko
license:        GPL v2
version:        1.0.2.0-k
description:    VMware Virtual Socket Family
author:         VMware, Inc.
srcversion:     8CF393912233CC480B5F778
depends:
retpoline:      Y
intree:         Y
name:           vsock
vermagic:       5.14.0-kali4-amd64 SMP mod_unload modversions
```

Step-12&13

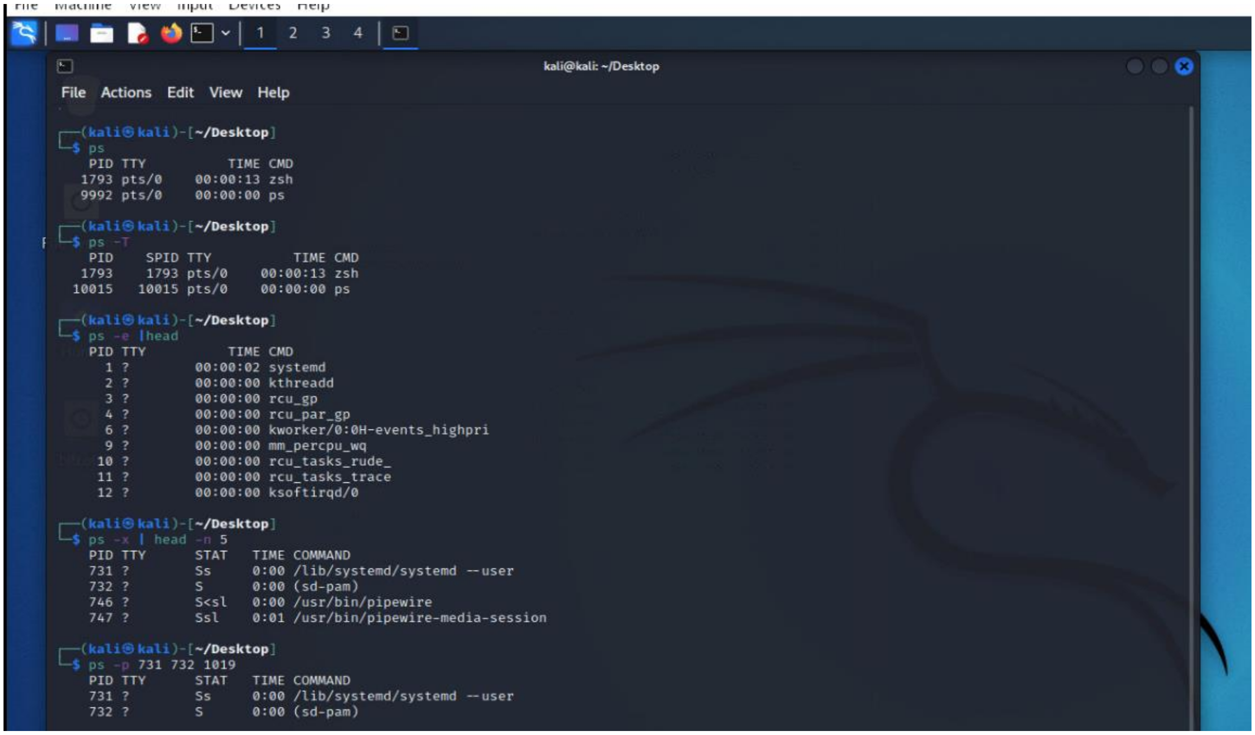
Another great command to use is “**ps**”, it is used to list down all of the process id’s

“**Ps -T**” list processes for current terminal

“**Ps -e| head**” list all processes

“**Ps -x | head -n 5**” list processes associated with current user

“Ps -s <PID> | head” list processes attributed to a particular session

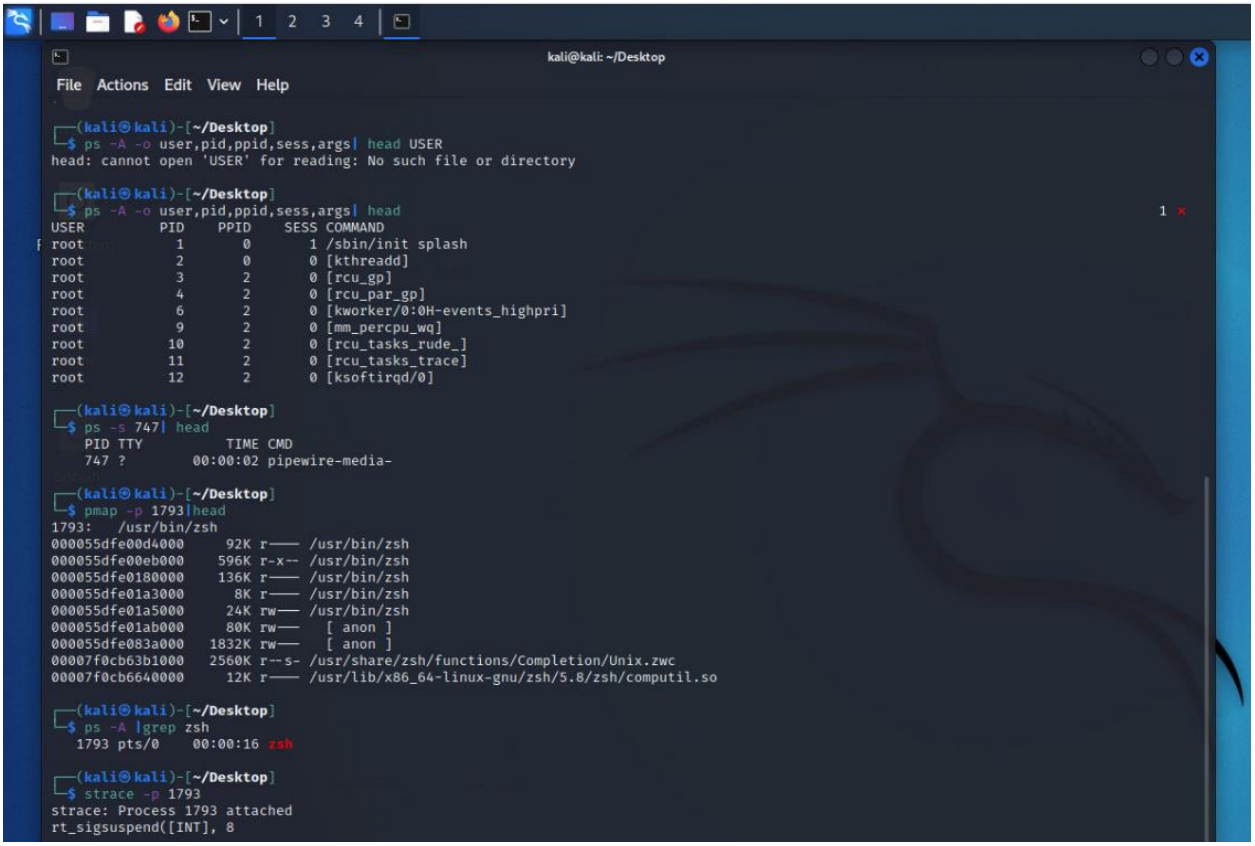

File Machine View Input Devices Help
1
2
3
4
kali@kali: ~/Desktop
File Actions Edit View Help

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ps
    PID TTY          TIME CMD
   1793 pts/0    00:00:13 zsh
   9992 pts/0    00:00:00 ps

┌──(kali㉿kali)-[~/Desktop]
└─$ ps -T
    PID    SPID TTY          TIME CMD
   1793    1793 pts/0    00:00:13 zsh
  10015   10015 pts/0    00:00:00 ps

┌──(kali㉿kali)-[~/Desktop]
└─$ ps -e |head
    PID TTY          TIME CMD
      1 ?        00:00:02 systemd
      2 ?        00:00:00 kthreadd
      3 ?        00:00:00 rcu_gp
      4 ?        00:00:00 rcu_par_gp
      6 ?        00:00:00 kworker/0:0H-events_highpri
      9 ?        00:00:00 mm_percpu_wq
     10 ?        00:00:00 rcu_tasks_rude_
     11 ?        00:00:00 rcu_tasks_trace
     12 ?        00:00:00 ksoftirqd/0

┌──(kali㉿kali)-[~/Desktop]
└─$ ps -x | head -n 5
    PID TTY      STAT   TIME COMMAND
    731 ?        Ss     0:00 /lib/systemd/systemd --user
    732 ?        S      0:00 (sd-pam)
    746 ?        S<sl   0:00 /usr/bin/pipewire
    747 ?        Ssl    0:01 /usr/bin/pipewire-media-session

┌──(kali㉿kali)-[~/Desktop]
└─$ ps -p 731 732 1019
    PID TTY      STAT   TIME COMMAND
    731 ?        Ss     0:00 /lib/systemd/systemd --user
    732 ?        S      0:00 (sd-pam)
```

Step-14&15

“**pmap**” is used to report on the memory map of a particular process.

strace is used to trace the system calls and signals issued by a particular process.

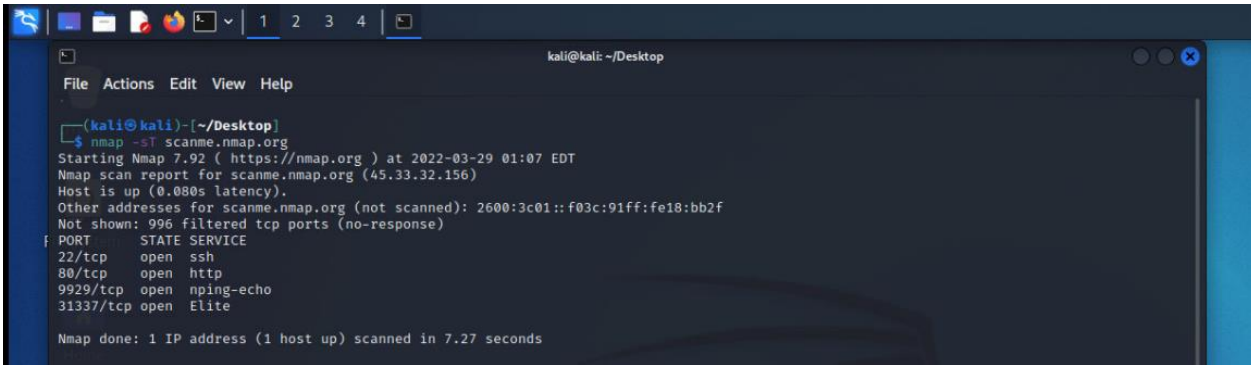


```
┌──(kali㉿kali)-[~/Desktop]
└─$ ps -A -o user,pid,ppid,sess,args| head USER
head: cannot open 'USER' for reading: No such file or directory

┌──(kali㉿kali)-[~/Desktop]
└─$ ps -A -o user,pid,ppid,sess,args| head
USER         PID    PPID    SESS COMMAND
root           1       0       1 /sbin/init splash
root           2       0       0 [kthreadd]
root           3       2       0 [rcu_gp]
root           4       2       0 [rcu_par_gp]
root           6       2       0 [kworker/0:0H-events_highpri]
root           9       2       0 [mm_percpu_wq]
root          10       2       0 [rcu_tasks_rude_]
root          11       2       0 [rcu_tasks_trace]
root          12       2       0 [ksoftirqd/0]

┌──(kali㉿kali)-[~/Desktop]
└─$ ps -s 747| head
    PID TTY          TIME CMD
    747 ?        00:00:02 pipewire-media-

┌──(kali㉿kali)-[~/Desktop]
└─$ pmap -p 1793|head
1793:   /usr/bin/zsh
000055dfe00d4000     92K r---- /usr/bin/zsh
000055dfe00eb000    596K r-x-- /usr/bin/zsh
000055dfe0180000    136K r---- /usr/bin/zsh
000055dfe01a3000      8K r---- /usr/bin/zsh
000055dfe01a5000     24K rw--- /usr/bin/zsh
000055dfe01ab000     80K rw---   [ anon ]
000055dfe083a000   1832K rw---   [ anon ]
00007f0cb63b1000   2560K r--s- /usr/share/zsh/functions/Completion/Unix.zwc
00007f0cb6640000     12K r---- /usr/lib/x86_64-linux-gnu/zsh/5.8/zsh/computil.so

┌──(kali㉿kali)-[~/Desktop]
└─$ ps -A |grep zsh
   1793 pts/0    00:00:16 zsh

┌──(kali㉿kali)-[~/Desktop]
└─$ strace -p 1793
strace: Process 1793 attached
rt_sigsuspend([INT], 8
```

PART III: LINUX FIREWALL, SSH SERVICE, AND PORT SCANNING USING NMAP

Step-16&17

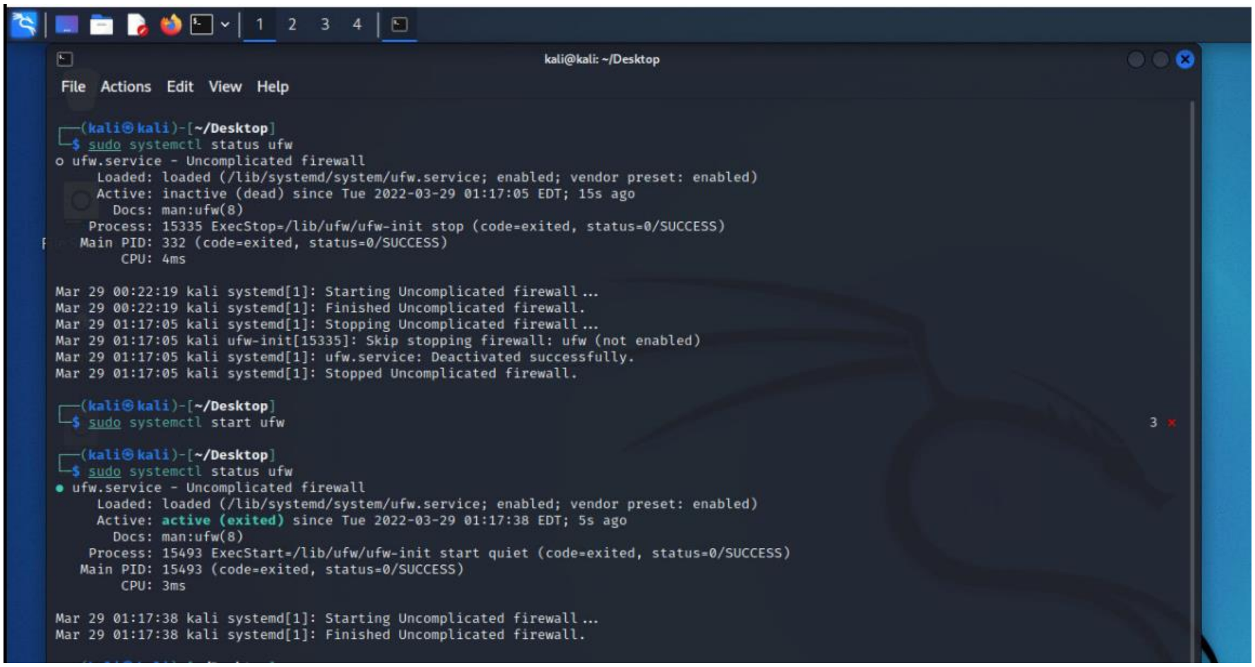
Nmap is a powerful tool used for port scanning



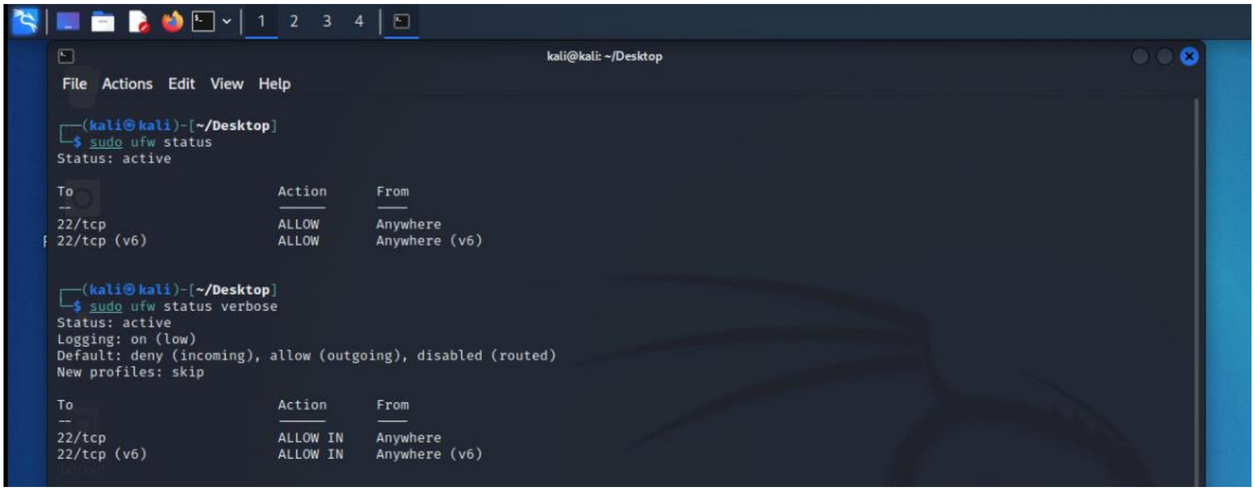
```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sT scanme.nmap.org
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-29 01:07 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.080s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite

Nmap done: 1 IP address (1 host up) scanned in 7.27 seconds
```

Step-18&19

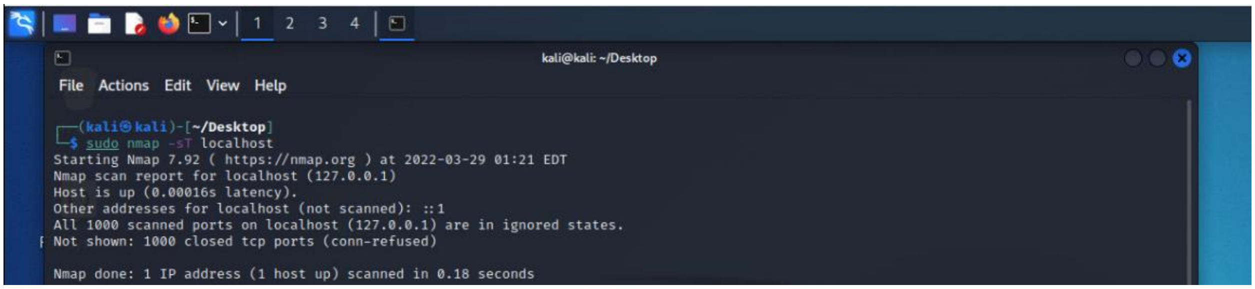
Firewall **ufw** is used to filter the port and drop the **nmap** packets, it is a security tool that is used by many companies



```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo systemctl status ufw
○ ufw.service - Uncomplicated firewall
     Loaded: loaded (/lib/systemd/system/ufw.service; enabled; vendor preset: enabled)
     Active: inactive (dead) since Tue 2022-03-29 01:17:05 EDT; 15s ago
       Docs: man:ufw(8)
    Process: 15335 ExecStop=/lib/ufw/ufw-init stop (code=exited, status=0/SUCCESS)
   Main PID: 332 (code=exited, status=0/SUCCESS)
        CPU: 4ms

Mar 29 00:22:19 kali systemd[1]: Starting Uncomplicated firewall ...
Mar 29 00:22:19 kali systemd[1]: Finished Uncomplicated firewall.
Mar 29 01:17:05 kali systemd[1]: Stopping Uncomplicated firewall ...
Mar 29 01:17:05 kali ufw-init[15335]: Skip stopping firewall: ufw (not enabled)
Mar 29 01:17:05 kali systemd[1]: ufw.service: Deactivated successfully.
Mar 29 01:17:05 kali systemd[1]: Stopped Uncomplicated firewall.

┌──(kali㉿kali)-[~/Desktop]
└─$ sudo systemctl start ufw                                                  3 ✗

┌──(kali㉿kali)-[~/Desktop]
└─$ sudo systemctl status ufw
● ufw.service - Uncomplicated firewall
     Loaded: loaded (/lib/systemd/system/ufw.service; enabled; vendor preset: enabled)
     Active: active (exited) since Tue 2022-03-29 01:17:38 EDT; 5s ago
       Docs: man:ufw(8)
    Process: 15493 ExecStart=/lib/ufw/ufw-init start quiet (code=exited, status=0/SUCCESS)
   Main PID: 15493 (code=exited, status=0/SUCCESS)
        CPU: 3ms

Mar 29 01:17:38 kali systemd[1]: Starting Uncomplicated firewall ...
Mar 29 01:17:38 kali systemd[1]: Finished Uncomplicated firewall.
```



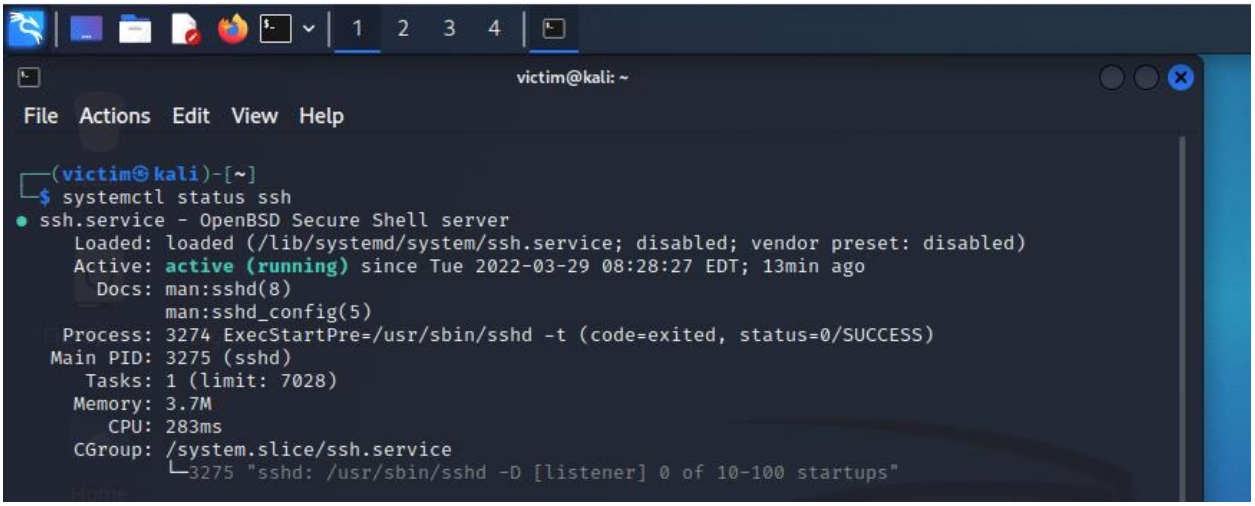
```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW       Anywhere
22/tcp (v6)                ALLOW       Anywhere (v6)


┌──(kali㉿kali)-[~/Desktop]
└─$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW IN    Anywhere
22/tcp (v6)                ALLOW IN    Anywhere (v6)
```



```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -sT localhost
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-29 01:21 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00016s latency).
Other addresses for localhost (not scanned): ::1
All 1000 scanned ports on localhost (127.0.0.1) are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
```

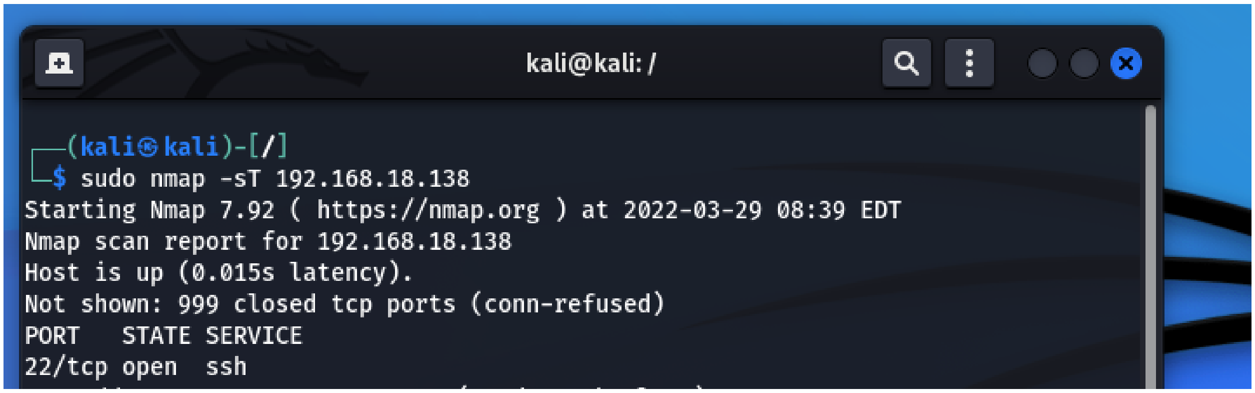
Here we are going to establish ssh connection using openssh, we have installed openssh on victim’s machine and using our machine we will connect to it.

“**ssh victim@<ip>**”

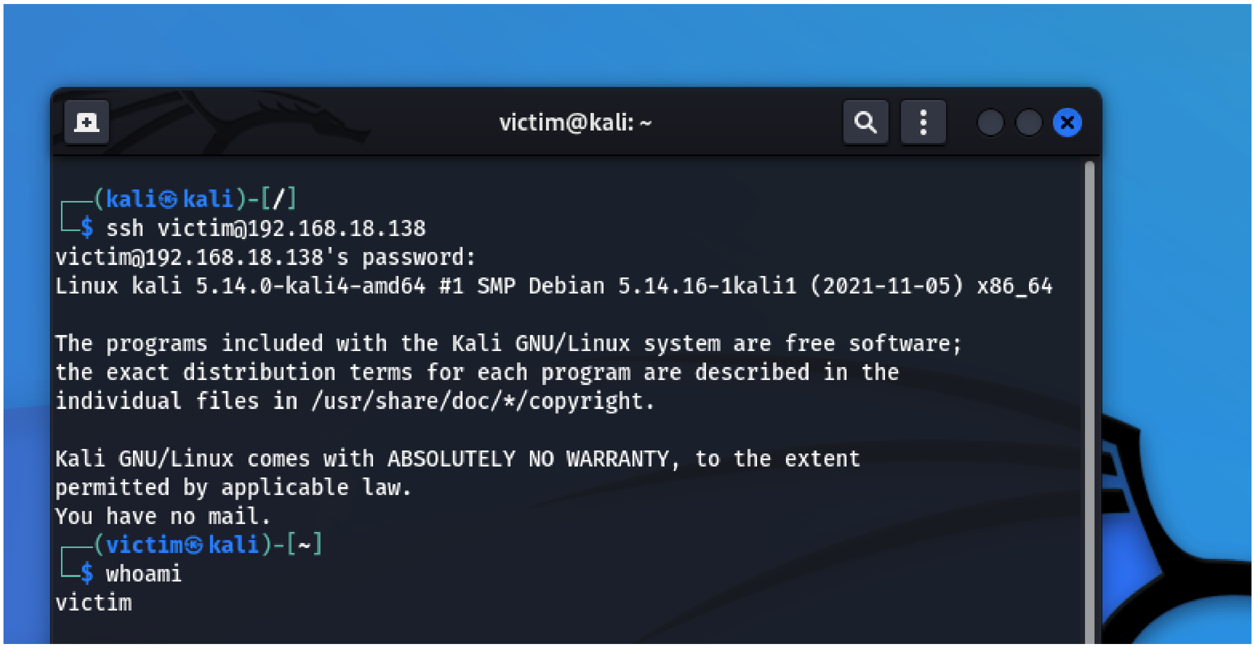


```
┌──(victim㉿kali)-[~]
└─$ systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; disabled; vendor preset: disabled)
     Active: active (running) since Tue 2022-03-29 08:28:27 EDT; 13min ago
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 3274 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 3275 (sshd)
      Tasks: 1 (limit: 7028)
     Memory: 3.7M
        CPU: 283ms
     CGroup: /system.slice/ssh.service
             └─3275 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"
```

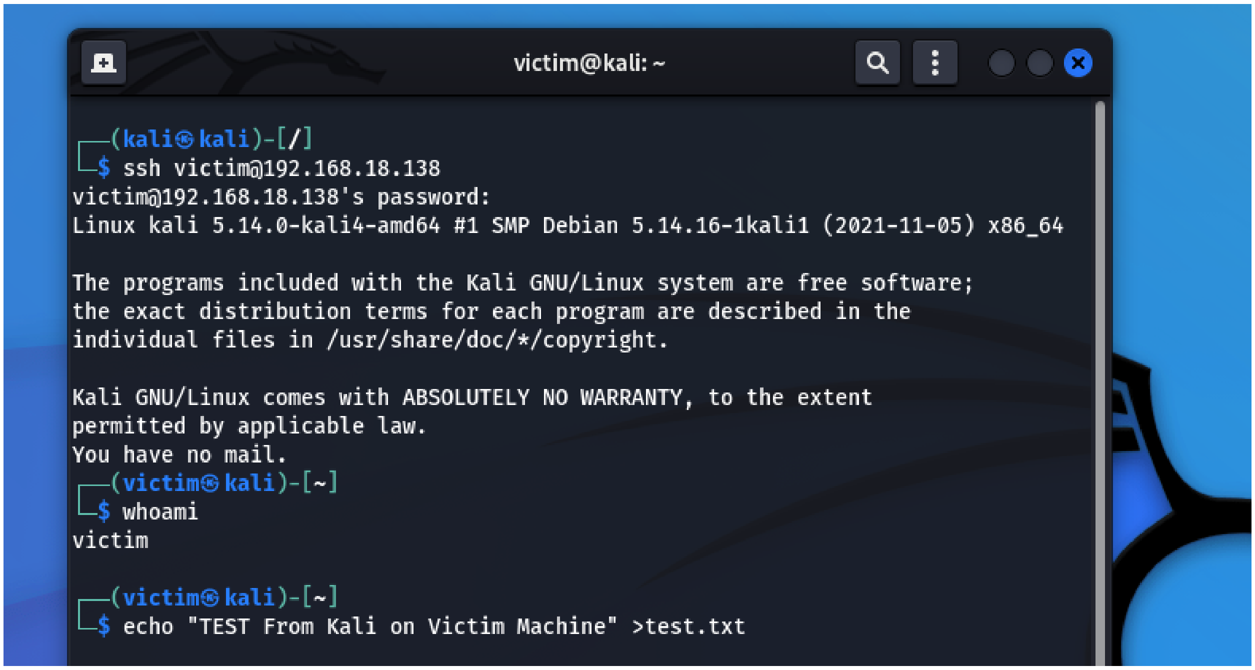
Here we have scanned the device to see if ssh port 22 is open



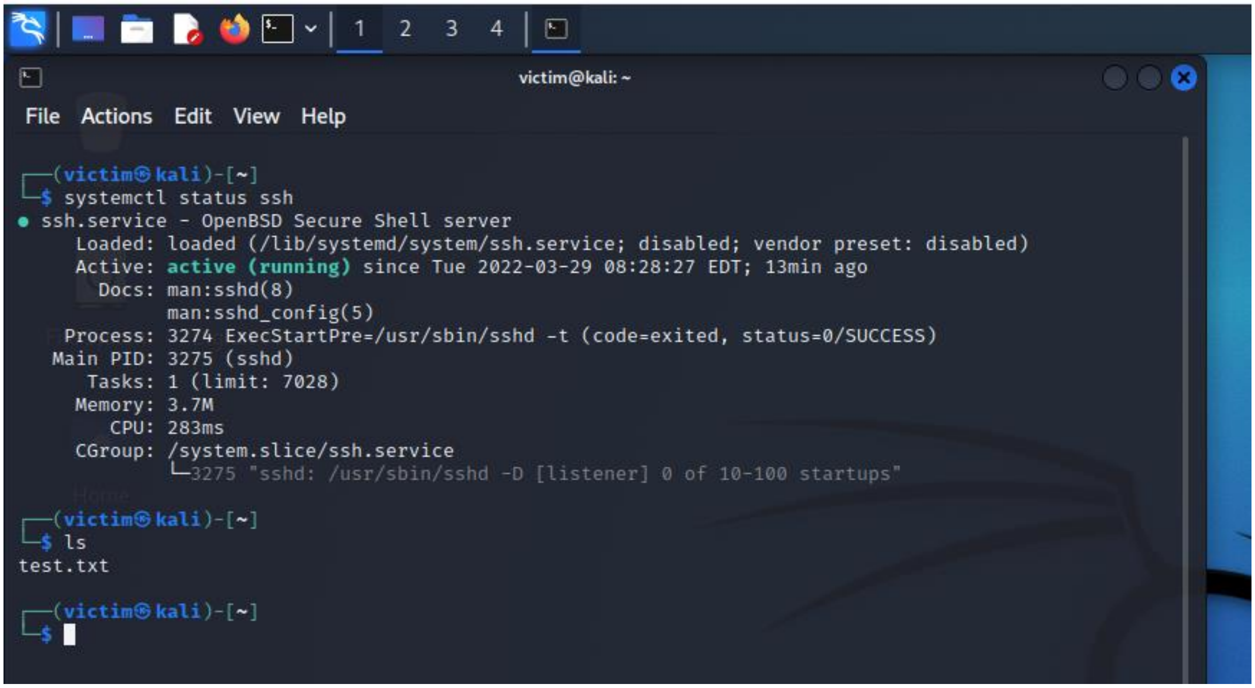
```
┌──(kali㉿kali)-[/]
└─$ sudo nmap -sT 192.168.18.138
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-29 08:39 EDT
Nmap scan report for 192.168.18.138
Host is up (0.015s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
```



```
┌──(kali㉿kali)-[/]
└─$ ssh victim@192.168.18.138
victim@192.168.18.138's password:
Linux kali 5.14.0-kali4-amd64 #1 SMP Debian 5.14.16-1kali1 (2021-11-05) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have no mail.
┌──(victim㉿kali)-[~]
└─$ whoami
victim
```



```
┌──(kali㉿kali)-[/]
└─$ ssh victim@192.168.18.138
victim@192.168.18.138's password:
Linux kali 5.14.0-kali4-amd64 #1 SMP Debian 5.14.16-1kali1 (2021-11-05) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have no mail.
┌──(victim㉿kali)-[~]
└─$ whoami
victim

┌──(victim㉿kali)-[~]
└─$ echo "TEST From Kali on Victim Machine" >test.txt
```



```
┌──(victim㉿kali)-[~]
└─$ systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; disabled; vendor preset: disabled)
     Active: active (running) since Tue 2022-03-29 08:28:27 EDT; 13min ago
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 3274 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 3275 (sshd)
      Tasks: 1 (limit: 7028)
     Memory: 3.7M
        CPU: 283ms
     CGroup: /system.slice/ssh.service
             └─3275 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

┌──(victim㉿kali)-[~]
└─$ ls
test.txt

┌──(victim㉿kali)-[~]
└─$ 
```

SUMMARY

We have learned a lot about linux from the file structure to the remote connection. In the first part we looked how the linux files are evenly structured in descending order, then we saw the important files that are used to extract useful information. In the second part we collected basic linux information such as hostname, time zone, uptime, network interface, default route, socket statistics, we also saw how dangerous is promiscuous mode is that allows malicious packets to infect the system. We also looked over the commands like dmesg, lsof, mount, df, lsmod and modinfo. Another very useful command is ps that is used to display the list of processes running. In third part we make use of firewall to block the packets to see our open ports and then we installed openssh which is used to establish secure connection between two devices. At the end we successfully connected to the victim’s machine using ssh and wrote a test.txt file remotely