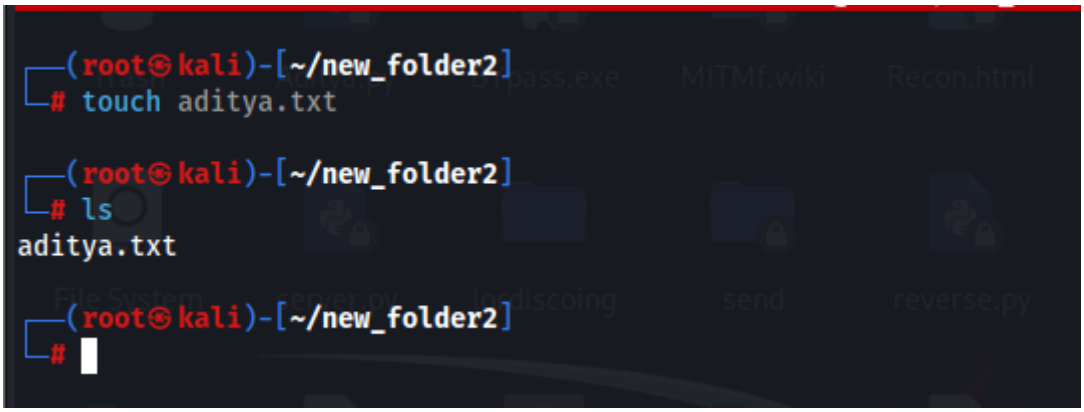
Day 26

Exploitation Analyst

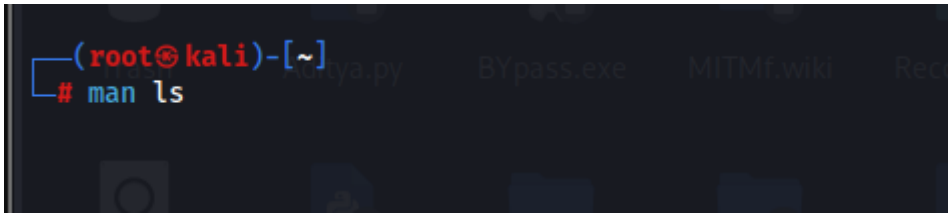
Some Basic Yet Important Linux Commands:

Touch file_name: to create a particular file.

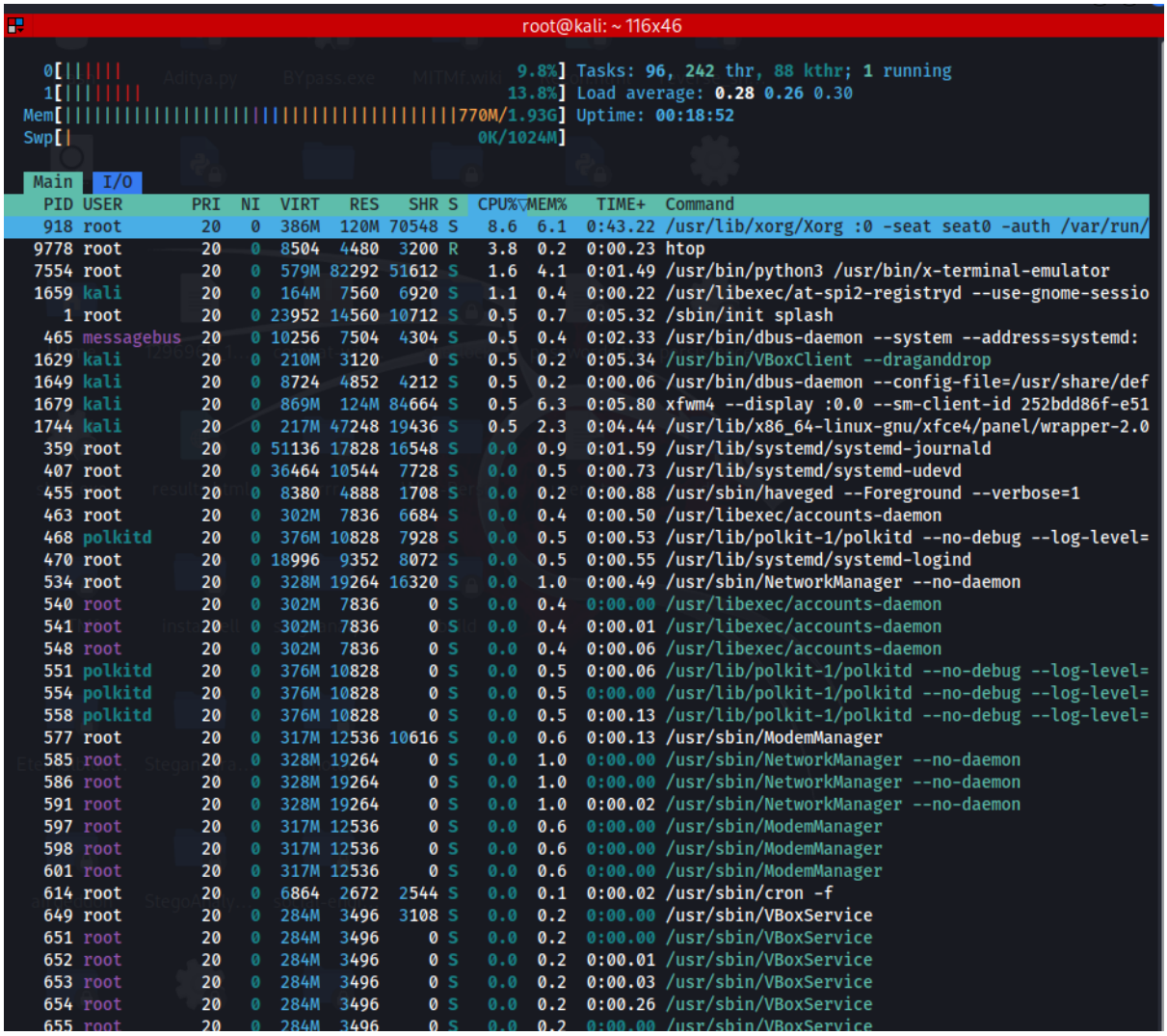


Cat file_name: to concatenate and display the content of file.

Man command_name: to get the manual for that command.

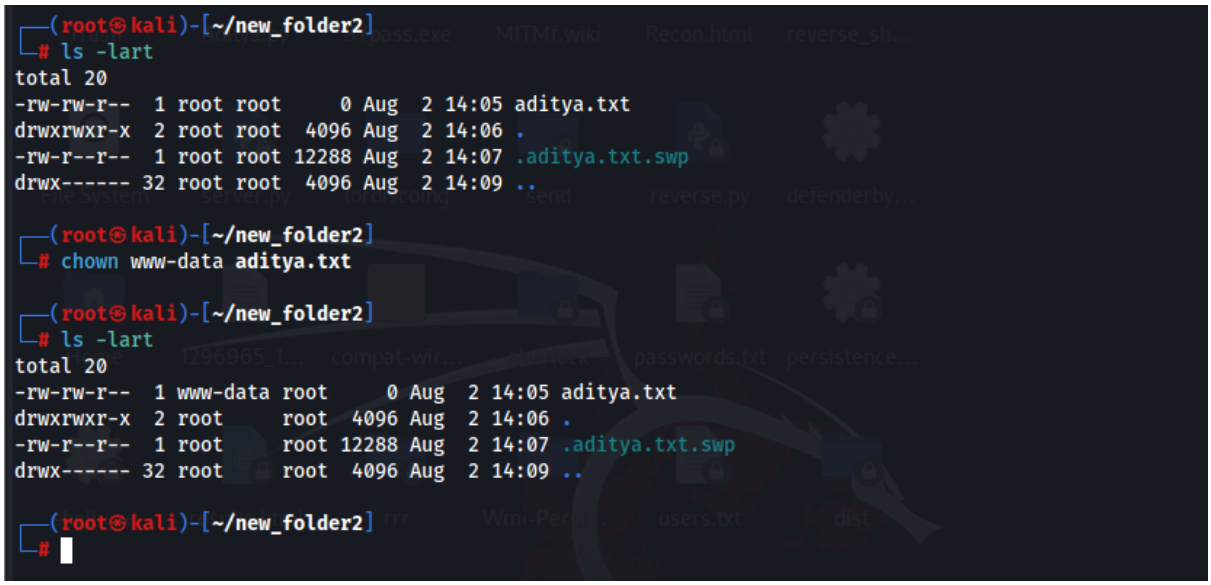


Htop: an interactive process viewer.

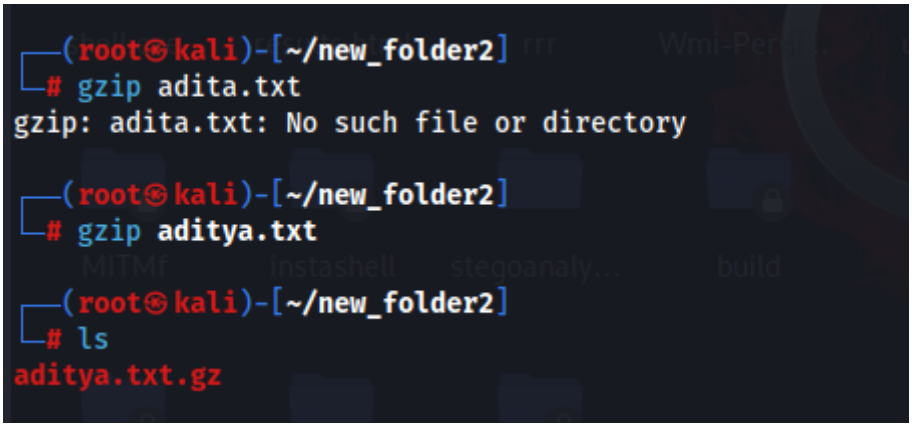


Chmod:

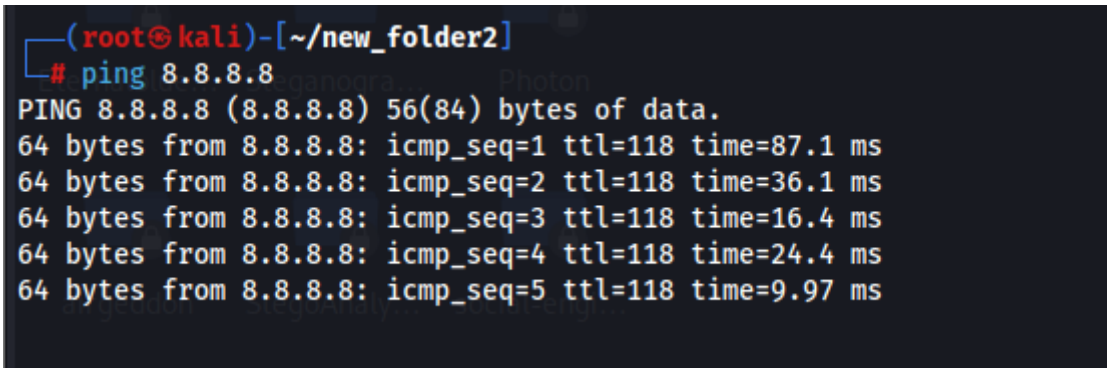
Chown: to change the owner of a file.



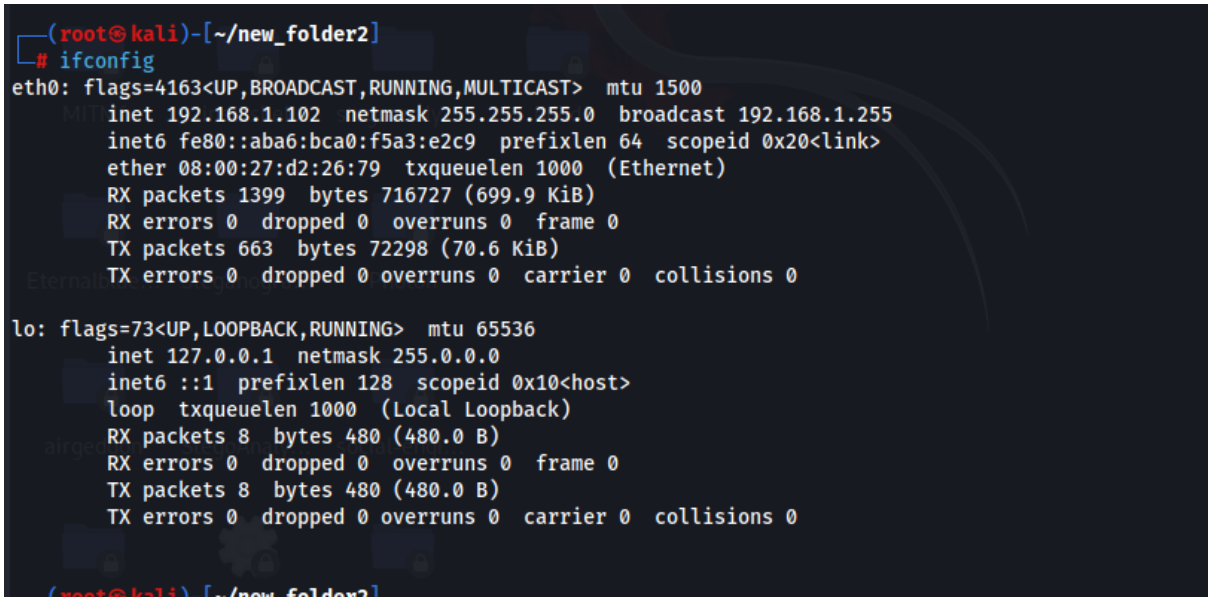
Gzip: compress file.



Ping: to test network connectivity.

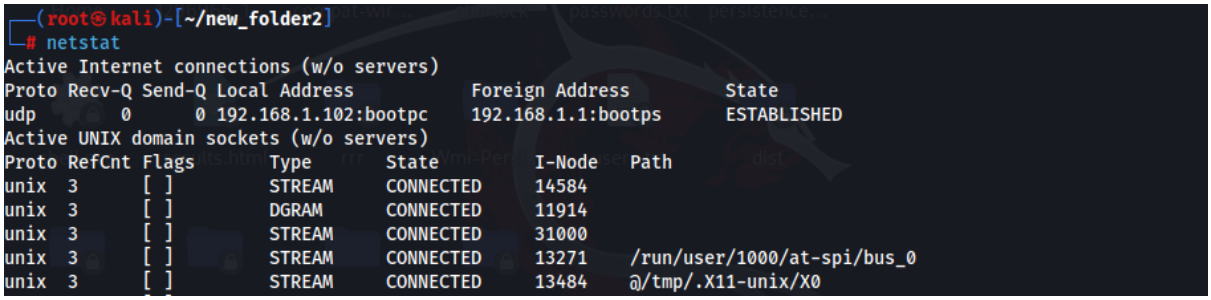


Ifconfig: to get the IP.



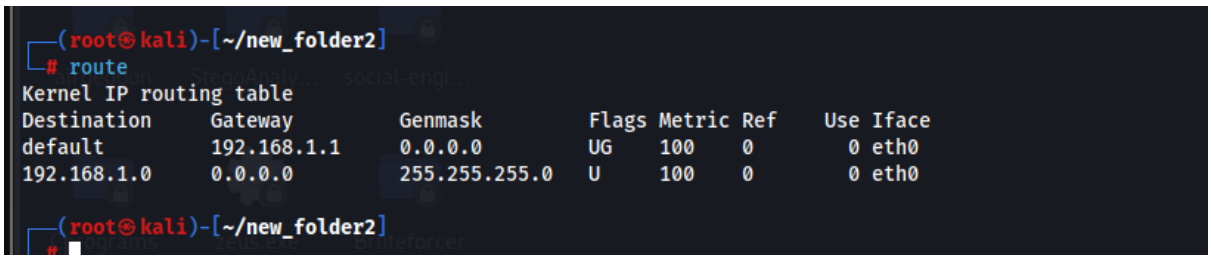
```
┌──(root㉿kali)-[~/new_folder2]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.102  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::aba6:bca0:f5a3:e2c9  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:d2:26:79  txqueuelen 1000  (Ethernet)
        RX packets 1399  bytes 716727 (699.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 663  bytes 72298 (70.6 KiB)
        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 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Netstat: to get the network monitoring.



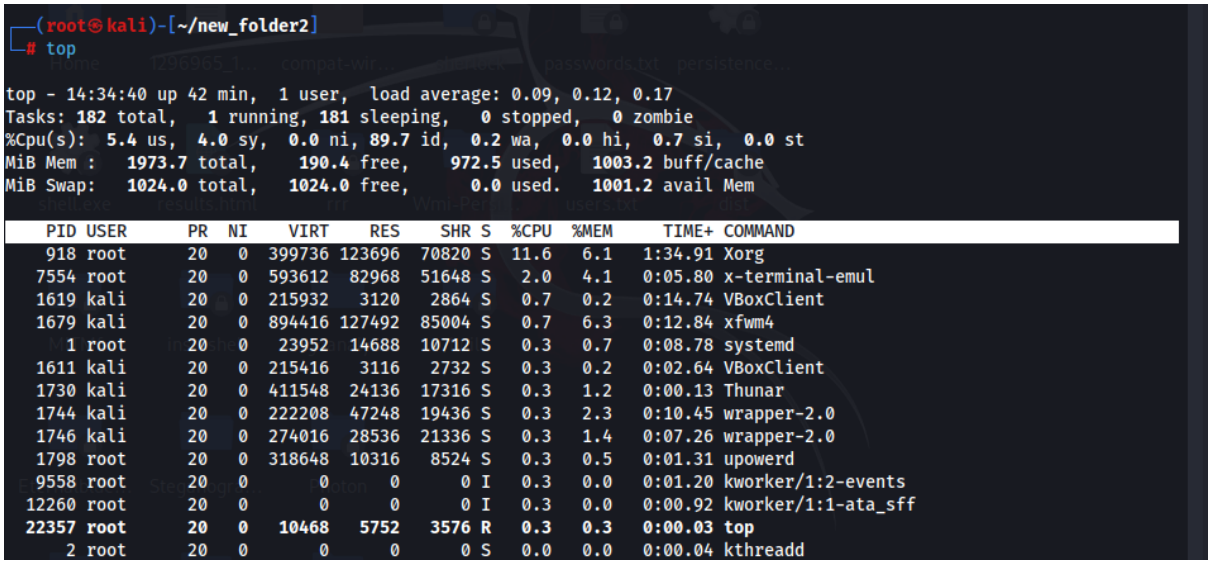
```
┌──(root㉿kali)-[~/new_folder2]
└─# netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 192.168.1.102:bootpc    192.168.1.1:bootps      ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  3      [ ]         STREAM     CONNECTED     14584
unix  3      [ ]         DGRAM      CONNECTED     11914
unix  3      [ ]         STREAM     CONNECTED     31000
unix  3      [ ]         STREAM     CONNECTED     13271    /run/user/1000/at-spi/bus_0
unix  3      [ ]         STREAM     CONNECTED     13484    @/tmp/.X11-unix/X0
```

Route: to view of configure the network routing tables.



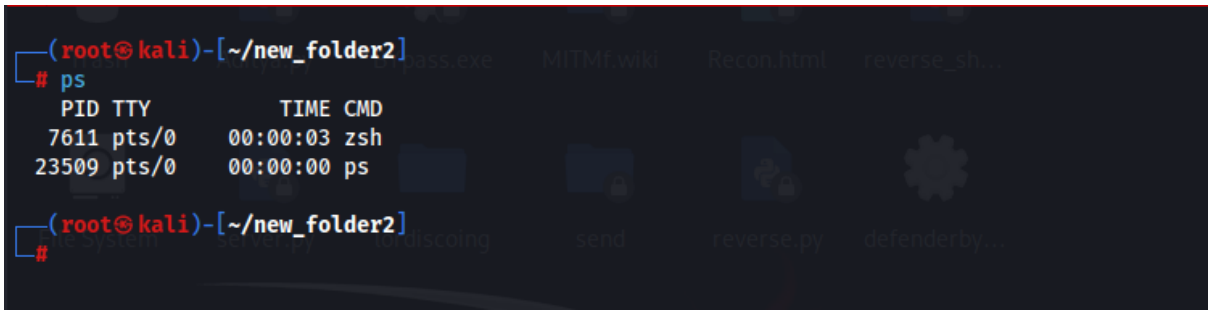
```
┌──(root㉿kali)-[~/new_folder2]
└─# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         192.168.1.1     0.0.0.0         UG    100    0        0 eth0
192.168.1.0     0.0.0.0         255.255.255.0   U     100    0        0 eth0

┌──(root㉿kali)-[~/new_folder2]
└─#
```

Top: for checking the usage by pc.



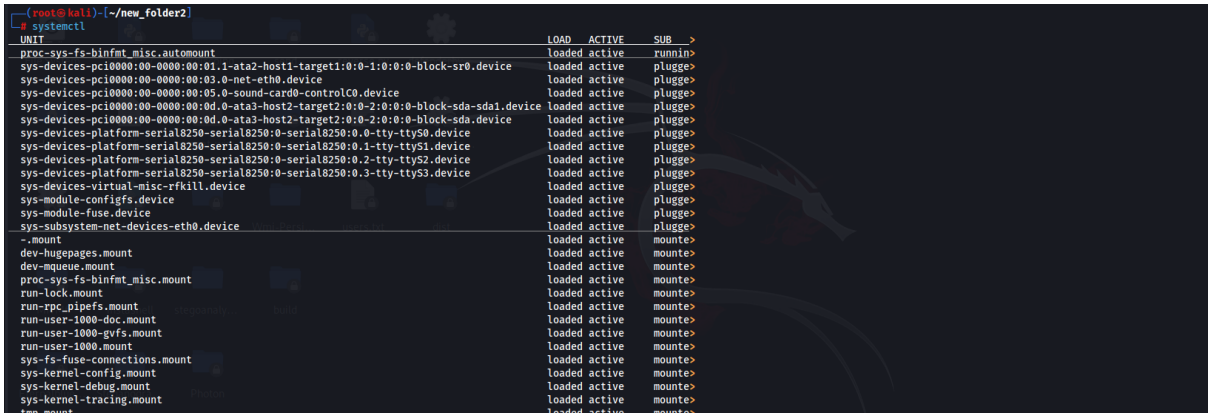
```
┌──(root㉿kali)-[~/new_folder2]
└─# top

top - 14:34:40 up 42 min,  1 user,  load average: 0.09, 0.12, 0.17
Tasks: 182 total,   1 running, 181 sleeping,   0 stopped,   0 zombie
%Cpu(s):  5.4 us,  4.0 sy,  0.0 ni, 89.7 id,  0.2 wa,  0.0 hi,  0.7 si,  0.0 st
MiB Mem :   1973.7 total,    190.4 free,    972.5 used,   1003.2 buff/cache
MiB Swap:   1024.0 total,   1024.0 free,      0.0 used.   1001.2 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
    918 root      20   0  399736 123696  70820 S  11.6   6.1   1:34.91 Xorg
   7554 root      20   0  593612  82968  51648 S   2.0   4.1   0:05.80 x-terminal-emul
   1619 kali      20   0  215932   3120   2864 S   0.7   0.2   0:14.74 VBoxClient
   1679 kali      20   0  894416 127492  85004 S   0.7   6.3   0:12.84 xfwm4
      1 root      20   0   23952  14688  10712 S   0.3   0.7   0:08.78 systemd
   1611 kali      20   0  215416   3116   2732 S   0.3   0.2   0:02.64 VBoxClient
   1730 kali      20   0  411548  24136  17316 S   0.3   1.2   0:00.13 Thunar
   1744 kali      20   0  222208  47248  19436 S   0.3   2.3   0:10.45 wrapper-2.0
   1746 kali      20   0  274016  28536  21336 S   0.3   1.4   0:07.26 wrapper-2.0
   1798 root      20   0  318648  10316   8524 S   0.3   0.5   0:01.31 upowerd
   9558 root      20   0       0      0      0 I   0.3   0.0   0:01.20 kworker/1:2-events
  12260 root      20   0       0      0      0 I   0.3   0.0   0:00.92 kworker/1:1-ata_sff
  22357 root      20   0   10468   5752   3576 R   0.3   0.3   0:00.03 top
      2 root      20   0       0      0      0 S   0.0   0.0   0:00.04 kthreadd
```

Ps: to get the list of current processes running.



```
┌──(root㉿kali)-[~/new_folder2]
└─# ps
    PID TTY          TIME CMD
   7611 pts/0    00:00:03 zsh
  23509 pts/0    00:00:00 ps

┌──(root㉿kali)-[~/new_folder2]
└─#
```

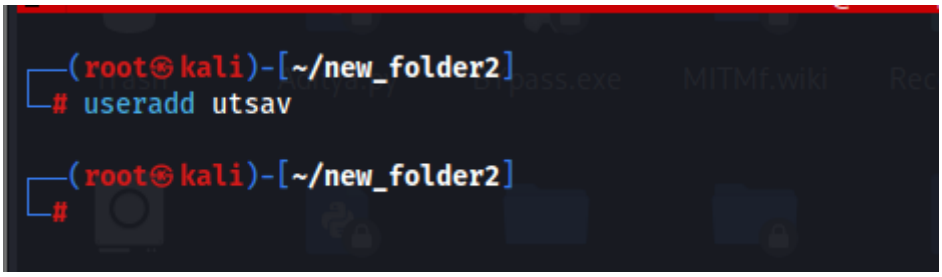
Systemctl: to get the controls system services and settings.



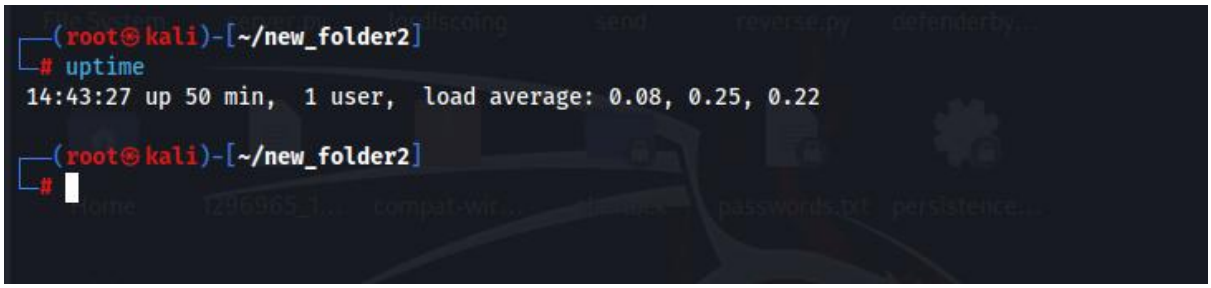
```
┌──(root㉿kali)-[~/new_folder2]
└─# systemctl
  UNIT                                                                LOAD   ACTIVE     SUB    >
  proc-sys-fs-binfmt_misc.automount                                   loaded active     runnin>
  sys-devices-pci0000:00-0000:00:01.1-ata2-host1-target1:0:0-1:0:0:0-block-sr0.device loaded active     plugge>
  sys-devices-pci0000:00-0000:00:03.0-net-eth0.device                 loaded active     plugge>
  sys-devices-pci0000:00-0000:00:05.0-sound-card0-controlC0.device    loaded active     plugge>
  sys-devices-pci0000:00-0000:00:0d.0-ata3-host2-target2:0:0-2:0:0:0-block-sda-sda1.device loaded active     plugge>
  sys-devices-pci0000:00-0000:00:0d.0-ata3-host2-target2:0:0-2:0:0:0-block-sda.device loaded active     plugge>
  sys-devices-platform-serial8250-serial8250:0-serial8250:0.0-tty-ttyS0.device loaded active     plugge>
  sys-devices-platform-serial8250-serial8250:0-serial8250:0.1-tty-ttyS1.device loaded active     plugge>
  sys-devices-platform-serial8250-serial8250:0-serial8250:0.2-tty-ttyS2.device loaded active     plugge>
  sys-devices-platform-serial8250-serial8250:0-serial8250:0.3-tty-ttyS3.device loaded active     plugge>
  sys-devices-virtual-misc-rfkill.device                              loaded active     plugge>
  sys-module-configfs.device                                          loaded active     plugge>
  sys-module-fuse.device                                              loaded active     plugge>
  sys-subsystem-net-devices-eth0.device                               loaded active     plugge>
  -.mount                                                             loaded active     mounte>
  dev-hugepages.mount                                                 loaded active     mounte>
  dev-mqueue.mount                                                    loaded active     mounte>
  proc-sys-fs-binfmt_misc.mount                                       loaded active     mounte>
  run-lock.mount                                                      loaded active     mounte>
  run-rpc_pipefs.mount                                                loaded active     mounte>
  run-user-1000-doc.mount                                             loaded active     mounte>
  run-user-1000-gvfs.mount                                            loaded active     mounte>
  run-user-1000.mount                                                 loaded active     mounte>
  sys-fs-fuse-connections.mount                                       loaded active     mounte>
  sys-kernel-config.mount                                             loaded active     mounte>
  sys-kernel-debug.mount                                              loaded active     mounte>
  sys-kernel-tracing.mount                                            loaded active     mounte>
```

```
┌──(root㉿kali)-[~/new_folder2]
└─# systemctl status apache2
○ apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
     Active: inactive (dead)
       Docs: https://httpd.apache.org/docs/2.4/

┌──(root㉿kali)-[~/new_folder2]
└─#
```

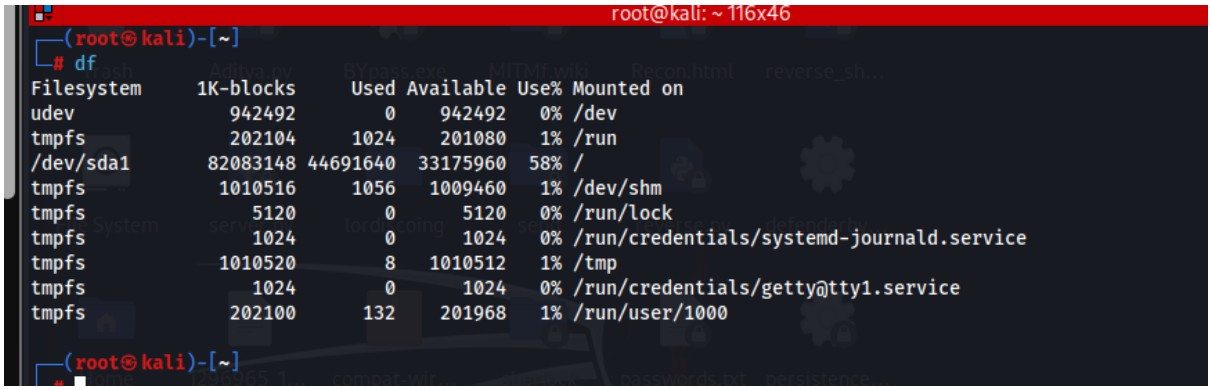
Useradd user_name: to add the new user.



Uptime: to get the uptime.

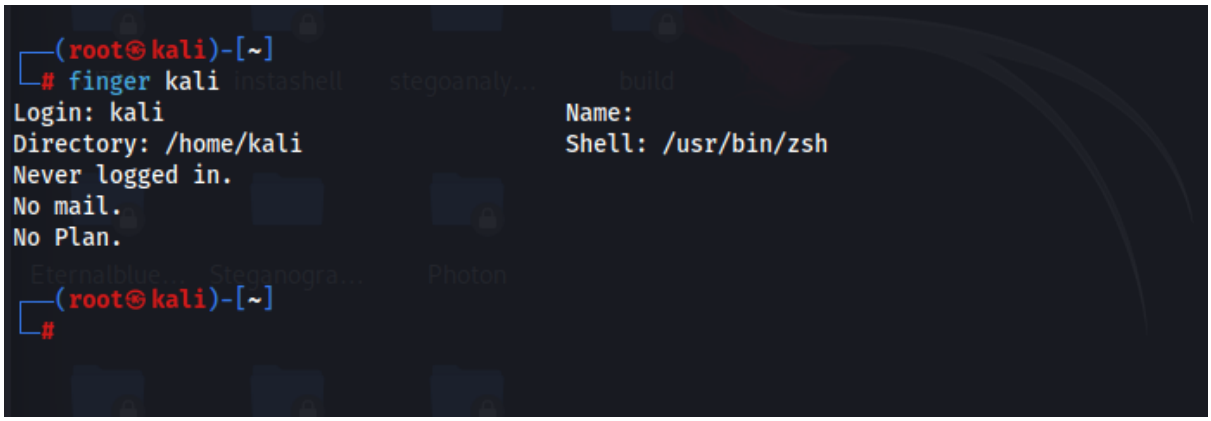


Df: to get the storage details.

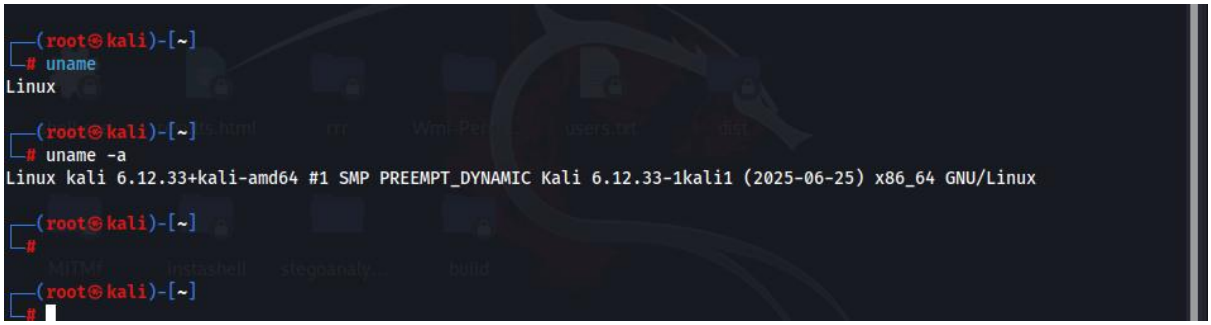


Whoami: to get the logged in user id name.

Finger user_idName: to get the information about the user.



Uname: to display the system information.



--The End--