

Day 26

Exploitation Analyst

Some Basic Yet Important Linux Commands:

Touch file_name: to create a particular file.

```
(root@kali)-[~/new_folder2]
# touch aditya.txt

(root@kali)-[~/new_folder2]
# ls
aditya.txt

(root@kali)-[~/new_folder2]
#
```

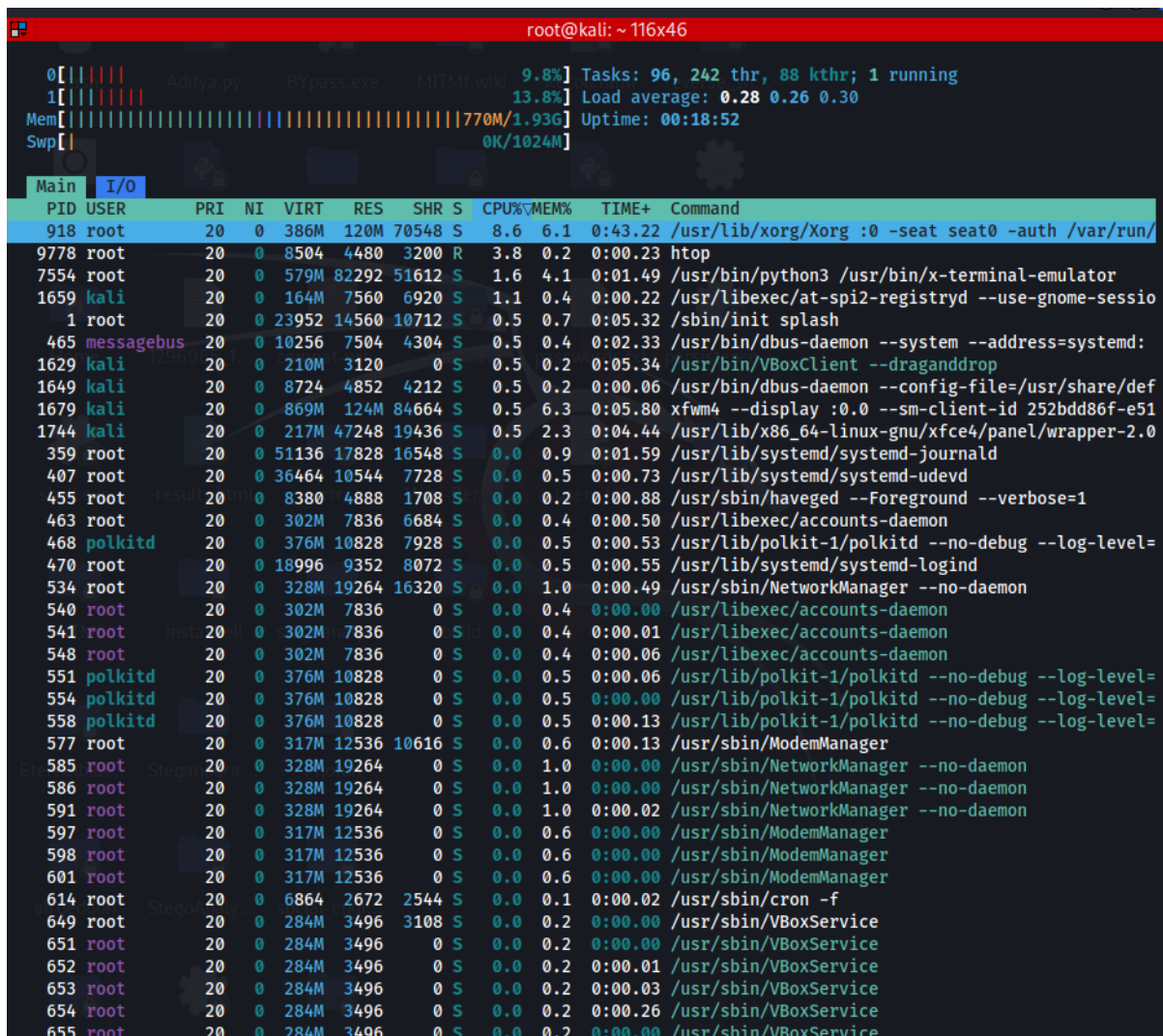
Cat file_name: to concatenate and display the content of file.

```
(root@kali)-[~]
# cat ad.txt
UEAkJHcwcMQ=
```

Man command_name: to get the manual for that command.

```
(root@kali)-[~]
# man ls
```

Htop: an interactive process viewer.



PID	USER	PRI	NI	VIRT	RES	SHR	S	CPU%	MEM%	TIME+	Command
918	root	20	0	386M	120M	70548	S	8.6	6.1	0:43.22	/usr/lib/xorg/Xorg :0 -seat seat0 -auth /var/run/
9778	root	20	0	8504	4480	3200	R	3.8	0.2	0:00.23	htop
7554	root	20	0	579M	82292	51612	S	1.6	4.1	0:01.49	/usr/bin/python3 /usr/bin/x-terminal-emulator
1659	kali	20	0	164M	7560	6920	S	1.1	0.4	0:00.22	/usr/libexec/at-spi2-registrd --use-gnome-sessio
1	root	20	0	23952	14560	10712	S	0.5	0.7	0:05.32	/sbin/init splash
465	messagebus	20	0	10256	7504	4304	S	0.5	0.4	0:02.33	/usr/bin/dbus-daemon --system --address=systemd:
1629	kali	20	0	210M	3120	0	S	0.5	0.2	0:05.34	/usr/bin/VBoxClient --draganddrop
1649	kali	20	0	8724	4852	4212	S	0.5	0.2	0:00.06	/usr/bin/dbus-daemon --config-file=/usr/share/def
1679	kali	20	0	869M	124M	84664	S	0.5	6.3	0:05.80	xfwm4 --display :0.0 --sm-client-id 252bdd86f-e51
1744	kali	20	0	217M	47248	19436	S	0.5	2.3	0:04.44	/usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0
359	root	20	0	51136	17828	16548	S	0.0	0.9	0:01.59	/usr/lib/systemd/systemd-journald
407	root	20	0	36464	10544	7728	S	0.0	0.5	0:00.73	/usr/lib/systemd/systemd-udevd
455	root	20	0	8380	4888	1708	S	0.0	0.2	0:00.88	/usr/sbin/haveged --Foreground --verbose=1
463	root	20	0	302M	7836	6684	S	0.0	0.4	0:00.50	/usr/libexec/accounts-daemon
468	polkitd	20	0	376M	10828	7928	S	0.0	0.5	0:00.53	/usr/lib/polkit-1/polkitd --no-debug --log-level=
470	root	20	0	18996	9352	8072	S	0.0	0.5	0:00.55	/usr/lib/systemd/systemd-logind
534	root	20	0	328M	19264	16320	S	0.0	1.0	0:00.49	/usr/sbin/NetworkManager --no-daemon
540	root	20	0	302M	7836	0	S	0.0	0.4	0:00.00	/usr/libexec/accounts-daemon
541	root	20	0	302M	7836	0	S	0.0	0.4	0:00.01	/usr/libexec/accounts-daemon
548	root	20	0	302M	7836	0	S	0.0	0.4	0:00.06	/usr/libexec/accounts-daemon
551	polkitd	20	0	376M	10828	0	S	0.0	0.5	0:00.06	/usr/lib/polkit-1/polkitd --no-debug --log-level=
554	polkitd	20	0	376M	10828	0	S	0.0	0.5	0:00.00	/usr/lib/polkit-1/polkitd --no-debug --log-level=
558	polkitd	20	0	376M	10828	0	S	0.0	0.5	0:00.13	/usr/lib/polkit-1/polkitd --no-debug --log-level=
577	root	20	0	317M	12536	10616	S	0.0	0.6	0:00.13	/usr/sbin/ModemManager
585	root	20	0	328M	19264	0	S	0.0	1.0	0:00.00	/usr/sbin/NetworkManager --no-daemon
586	root	20	0	328M	19264	0	S	0.0	1.0	0:00.00	/usr/sbin/NetworkManager --no-daemon
591	root	20	0	328M	19264	0	S	0.0	1.0	0:00.02	/usr/sbin/NetworkManager --no-daemon
597	root	20	0	317M	12536	0	S	0.0	0.6	0:00.00	/usr/sbin/ModemManager
598	root	20	0	317M	12536	0	S	0.0	0.6	0:00.00	/usr/sbin/ModemManager
601	root	20	0	317M	12536	0	S	0.0	0.6	0:00.00	/usr/sbin/ModemManager
614	root	20	0	6864	2672	2544	S	0.0	0.1	0:00.02	/usr/sbin/cron -f
649	root	20	0	284M	3496	3108	S	0.0	0.2	0:00.00	/usr/sbin/VBoxService
651	root	20	0	284M	3496	0	S	0.0	0.2	0:00.00	/usr/sbin/VBoxService
652	root	20	0	284M	3496	0	S	0.0	0.2	0:00.01	/usr/sbin/VBoxService
653	root	20	0	284M	3496	0	S	0.0	0.2	0:00.03	/usr/sbin/VBoxService
654	root	20	0	284M	3496	0	S	0.0	0.2	0:00.26	/usr/sbin/VBoxService
655	root	20	0	284M	3496	0	S	0.0	0.2	0:00.00	/usr/sbin/VBoxService

Chmod:



```
(root@kali)-[~]
# chmod 744 fake.crt
```

Chown: to change the owner of a file.

```
(root@kali)-[~/new_folder2]
# ls -lart
total 20
-rw-rw-r-- 1 root root 0 Aug 2 14:05 aditya.txt
drwxrwxr-x 2 root root 4096 Aug 2 14:06 .
-rw-r--r-- 1 root root 12288 Aug 2 14:07 .aditya.txt.swp
drwx----- 32 root root 4096 Aug 2 14:09 ..

(root@kali)-[~/new_folder2]
# chown www-data aditya.txt

(root@kali)-[~/new_folder2]
# ls -lart
total 20
-rw-rw-r-- 1 www-data root 0 Aug 2 14:05 aditya.txt
drwxrwxr-x 2 root root 4096 Aug 2 14:06 .
-rw-r--r-- 1 root root 12288 Aug 2 14:07 .aditya.txt.swp
drwx----- 32 root root 4096 Aug 2 14:09 ..

(root@kali)-[~/new_folder2]
#
```

Gzip: compress file.

```
(root@kali)-[~/new_folder2]
# gzip adita.txt
gzip: adita.txt: No such file or directory

(root@kali)-[~/new_folder2]
# gzip aditya.txt

(root@kali)-[~/new_folder2]
# ls
aditya.txt.gz
```

Ping: to test network connectivity.

```
(root@kali)-[~/new_folder2]
# 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=118 time=87.1 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=118 time=36.1 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=118 time=16.4 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=118 time=24.4 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=118 time=9.97 ms
```

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

(root@kali)~[~/new_folder2]
```

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 running
sys-devices-pci0000:00-0000:00:01.1-ata2-host1-target1:0:0-1:0:0:0-block-sr0.device loaded active plugged
sys-devices-pci0000:00-0000:00:03.0-net-eth0.device loaded active plugged
sys-devices-pci0000:00-0000:00:05.0-sound-card0-controlC0.device loaded active plugged
sys-devices-pci0000:00-0000:00:0d.0-ata3-host2-target2:0:0-2:0:0:0-block-sda-sda1.device loaded active plugged
sys-devices-pci0000:00-0000:00:0d.0-ata3-host2-target2:0:0-2:0:0:0-block-sda.device loaded active plugged
sys-devices-platform-serial8250-serial8250:0-0-tty-ttyS0.device loaded active plugged
sys-devices-platform-serial8250-serial8250:0-serial8250:0-1-tty-ttyS1.device loaded active plugged
sys-devices-platform-serial8250-serial8250:0-serial8250:0-2-tty-ttyS2.device loaded active plugged
sys-devices-platform-serial8250-serial8250:0-serial8250:0-3-tty-ttyS3.device loaded active plugged
sys-devices-virtual-misc-rfkill.device loaded active plugged
sys-module-configfs.device loaded active plugged
sys-module-fuse.device loaded active plugged
sys-subsystem-net-devices-eth0.device loaded active plugged
-.mount loaded active mount>
dev-hugepages.mount loaded active mount>
dev-mqueue.mount loaded active mount>
proc-sys-fs-binfmt_misc.mount loaded active mount>
run-lock.mount loaded active mount>
run-rpc_pipefs.mount loaded active mount>
run-user-1000-doc.mount loaded active mount>
run-user-1000-gvfs.mount loaded active mount>
run-user-1000.mount loaded active mount>
sys-fs-fuse-connections.mount loaded active mount>
sys-kernel-config.mount loaded active mount>
sys-kernel-debug.mount loaded active mount>
sys-kernel-tracing.mount loaded active mount>
```

```
(root@kali)-[~/new_folder2]
# systemctl status apache2
o 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.

```
(root@kali)-[~/new_folder2]
# useradd utsav

(root@kali)-[~/new_folder2]
#
```

Uptime: to get the uptime.

```
(root@kali)-[~/new_folder2]
# uptime
14:43:27 up 50 min, 1 user, load average: 0.08, 0.25, 0.22

(root@kali)-[~/new_folder2]
#
```

Df: to get the storage details.

```
root@kali: ~ 116x46
(root@kali)-[~]
# df
Filesystem      1K-blocks    Used Available Use% Mounted on
udev             942492         0   942492    0% /dev
tmpfs            202104       1024   201080    1% /run
/dev/sda1       82083148 44691640 33175960   58% /
tmpfs            1010516       1056  1009460    1% /dev/shm
tmpfs             5120         0     5120    0% /run/lock
tmpfs            1024         0     1024    0% /run/credentials/systemd-journald.service
tmpfs            1010520         8  1010512    1% /tmp
tmpfs            1024         0     1024    0% /run/credentials/getty@tty1.service
tmpfs            202100        132  201968    1% /run/user/1000

(root@kali)-[~]
#
```

Whoami: to get the logged in user id name.

```
(root@kali)~  
# whoami  
root  
(root@kali)~  
#
```

Finger user_idName: to get the information about the user.

```
(root@kali)~  
# finger kali  
Login: kali  
Directory: /home/kali  
Never logged in.  
No mail.  
No Plan.  
Name:  
Shell: /usr/bin/zsh  
(root@kali)~  
#
```

Uname: to display the system information.

```
(root@kali)~  
# uname  
Linux  
(root@kali)~  
# uname -a  
Linux kali 6.12.33+kali-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.33-1kali1 (2025-06-25) x86_64 GNU/Linux  
(root@kali)~  
#  
(root@kali)~  
#
```

--The End--