

◊ 1. Viewing All Processes

Command: `ps aux`

USER	PID	%CPU	%MEM	VSZ	RSS	TTY	STAT	START	TIME	COMMAND
root	1	1.9	0.6	22180	12900	?	Ss	08:23	0:00	/sbin/init splash
root	2	0.0	0.0	0	0	?	S	08:23	0:00	[kthreadd]
root	3	0.0	0.0	0	0	?	S	08:23	0:00	[pool_workqueue_release]
root	4	0.0	0.0	0	0	?	I<	08:23	0:00	[kworker/R-rcu_g]
root	5	0.0	0.0	0	0	?	I<	08:23	0:00	[kworker/R-rcu_p]
root	6	0.0	0.0	0	0	?	I<	08:23	0:00	[kworker/R-slub_]
root	7	0.0	0.0	0	0	?	I<	08:23	0:00	[kworker/R-netns]
root	8	0.0	0.0	0	0	?	I	08:23	0:00	[kworker/0:0-ata_sff]
root	9	0.0	0.0	0	0	?	I	08:23	0:00	[kworker/0:1-mm_percpu_wq]
root	10	0.0	0.0	0	0	?	I<	08:23	0:00	[kworker/0:0H-kblockd]
root	11	0.0	0.0	0	0	?	I	08:23	0:00	[kworker/u4:0-ext4-rsv-cor]
root	12	0.0	0.0	0	0	?	I<	08:23	0:00	[kworker/R-mm_pe]
root	13	0.0	0.0	0	0	?	I	08:23	0:00	[rcu_tasks_kthread]
root	14	0.0	0.0	0	0	?	I	08:23	0:00	[rcu_tasks_rude_kthread]
root	15	0.0	0.0	0	0	?	I	08:23	0:00	[rcu_tasks_trace_kthread]
root	16	0.2	0.0	0	0	?	S	08:23	0:00	[ksoftirqd/0]
root	17	0.2	0.0	0	0	?	I	08:23	0:00	[rcu_preempt]
root	18	0.0	0.0	0	0	?	S	08:23	0:00	[migration/0]
root	19	0.0	0.0	0	0	?	S	08:23	0:00	[idle_inject/0]
root	20	0.0	0.0	0	0	?	S	08:23	0:00	[cpuhp/0]
root	21	0.0	0.0	0	0	?				

:

♣ 2. Process Tree

Command: `pstree -p`

F S	UID	PID	PPID	C PRI	NI ADDR SZ	WCHAN TTY	TIME	CMD
0 S	1000	111468	111465	1 80	0 -	2531 sigsus pts/38	00:00:00	zsh
0 R	1000	111521	111468	0 80	0 -	2756 -	pts/38	00:00:00 ps
 [kali㉿kali)-[~]								
 \$ sudo lsof -p 111468								
[sudo] password for kali:								
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
zsh	111468	kali	cwd	DIR	8,1	4096	1179650	/home/kali
zsh	111468	kali	rtd	DIR	8,1	4096	2	/
zsh	111468	kali	txt	REG	8,1	869864	173666	/usr/bin/zsh
zsh	111468	kali	mem	REG	8,1	14464	1066721	/usr/lib/x86_64-linux-gnu/zsh/5.9/zsh/regex.so
zsh	111468	kali	mem	REG	8,1	209344	825805	/usr/share/zsh/functions/Misc.zwc
zsh	111468	kali	mem	REG	8,1	302784	826829	/usr/share/zsh/functions/Completion/Base.zwc
zsh	111468	kali	mem	REG	8,1	18752	1066720	/usr/lib/x86_64-linux-gnu/zsh/5.9/zsh/stat.so
zsh	111468	kali	mem	REG	8,1	3052896	435155	/usr/lib/locale/locale-archive
zsh	111468	kali	mem	REG	8,1	32520	1066742	/usr/lib/x86_64-linux-gnu/zsh/5.9/zsh/system.so
zsh	111468	kali	mem	REG	8,1	14600	1066722	/usr/lib/x86_64-linux-gnu/zsh/5.9/zsh/zleparameter.so
zsh	111468	kali	mem	REG	8,1	192136	825791	/usr/share/zsh/functions/Completion.zwc
zsh	111468	kali	mem	REG	8,1	49104	1066746	/usr/lib/x86_64-linux-gnu/zsh/5.9/zsh/parameter.so
zsh	111468	kali	mem	REG	8,1	39240	1066708	/usr/lib/x86_64-linux-gnu/zsh/5.9/zsh/zutil.so
zsh	111468	kali	mem	REG	8,1	159648	1066732	/usr/lib/x86_64-linux-gnu/zsh/5.9/zsh/complete.so
zsh	111468	kali	mem	REG	8,1	339744	1066715	/usr/lib/x86_64-linux-gnu/zsh/5.9/zsh/zle.so
zsh	111468	kali	mem	REG	8,1	1926256	439100	/usr/lib/x86_64-linux-gnu/libc.so.6
zsh	111468	kali	mem	REG	8,1	907784	439347	/usr/lib/x86_64-linux-gnu/libm.so.6
zsh	111468	kali	mem	REG	8,1	216368	439046	/usr/lib/x86_64-linux-gnu/libtinfo.so.6.4
zsh	111468	kali	mem	REG	8,1	47288	440000	/usr/lib/x86_64-linux-gnu/libcap.so.2.66
zsh	111468	kali	mem	REG	8,1	14536	1066711	/usr/lib/x86_64-linux-gnu/zsh/5.9/zsh/terminfo.so
zsh	111468	kali	mem	REG	8,1	27028	1064964	/usr/lib/x86_64-linux-gnu/gconv/gconv-modules.cache
zsh	111468	kali	mem	REG	8,1	210792	437939	/usr/lib/x86_64-linux-gnu/ld-linux-x86-64.so.2
zsh	111468	kali	0u	CHR	136,38	0t0	41	/dev/pts/38
zsh	111468	kali	1u	CHR	136,38	0t0	41	/dev/pts/38
zsh	111468	kali	2u	CHR	136,38	0t0	41	/dev/pts/38
zsh	111468	kali	10u	CHR	136,38	0t0	41	/dev/pts/38
zsh	111468	kali	12r	REG	8,1	192136	825791	/usr/share/zsh/functions/Completion.zwc
zsh	111468	kali	14r	REG	8,1	302784	826829	/usr/share/zsh/functions/Completion/Base.zwc
zsh	111468	kali	15r	REG	8,1	209344	825805	/usr/share/zsh/functions/Misc.zwc

:

3. Real-Time Process Monitoring

Command: `top`

top - 13:27:30 up 9 min, 1 user, load average: 0.26, 0.26, 0.17													
Tasks: 182 total, 4 running, 178 sleeping, 0 stopped, 0 zombie													
CPU(s): 2.7 us, 6.9 sy, 0.0 ni, 89.7 id, 0.2 wa, 0.0 hi, 0.5 si, 0.0 st													
MiB Mem : 1976.7 total, 468.1 free, 1185.7 used, 540.3 buff/cache													
MiB Swap : 1024.0 total, 1024.0 free, 0.0 used. 791.0 avail Mem													
PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND		
667	root	20	0	594480	308460	125484	R	9.0	15.2	0:19.65	Xorg		
5927	kali	20	0	545308	47856	35152	R	4.2	2.4	0:00.32	xfce4-screensho		
986	kali	20	0	1052184	126472	77868	R	1.9	6.2	0:05.86	xfwm4		
5742	kali	20	0	462820	104540	88852	S	1.6	5.2	0:00.52	qterminal		
1055	kali	20	0	290400	47116	19200	S	0.6	2.3	0:03.09	panel-13-cpugra		
253	root	20	0	0	0	0	I	0.3	0.0	0:01.15	kworker/1:3-events		
923	kali	20	0	217468	3328	2816	S	0.3	0.2	0:00.74	VBoxClient		
931	kali	20	0	217984	3072	2688	S	0.3	0.2	0:01.83	VBoxClient		
1016	kali	20	0	217576	3200	2816	S	0.3	0.2	0:00.22	VBoxClient		
1057	kali	20	0	424064	32108	20824	S	0.3	1.6	0:03.04	panel-15-genmon		
1171	kali	20	0	448532	54024	31104	S	0.3	2.7	0:00.50	blueman-applet		
2115	kali	20	0	462380	103892	88424	S	0.3	5.1	0:00.50	qterminal		
5811	kali	20	0	11804	5632	3456	R	0.3	0.3	0:00.05	top		
1	root	20	0	22176	12772	9572	S	0.0	0.6	0:00.75	systemd		
2	root	20	0	0	0	0	S	0.0	0.0	0:00.01	kthreadd		
3	root	20	0	0	0	0	S	0.0	0.0	0:00.00	pool_workqueue_release		
4	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/R-rcu_g		
5	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/R-rcu_p		
6	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/R-slub_		
7	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/R-netns		
12	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/R-mm_pe		
13	root	20	0	0	0	0	I	0.0	0.0	0:00.00	rcu_tasks_kthread		
14	root	20	0	0	0	0	I	0.0	0.0	0:00.00	rcu_tasks_rude_kthread		
15	root	20	0	0	0	0	I	0.0	0.0	0:00.00	rcu_tasks_trace_kthread		
16	root	20	0	0	0	0	S	0.0	0.0	0:00.19	ksoftirqd/0		
17	root	20	0	0	0	0	I	0.0	0.0	0:00.90	rcu_preempt		
18	root	rt	0	0	0	0	S	0.0	0.0	0:00.01	migration/0		
19	root	-51	0	0	0	0	S	0.0	0.0	0:00.00	idle_inject/0		
20	root	20	0	0	0	0	S	0.0	0.0	0:00.00	cpuhp/0		
21	root	20	0	0	0	0	S	0.0	0.0	0:00.00	cpuhp/1		
22	root	-51	0	0	0	0	S	0.0	0.0	0:00.00	idle_inject/1		
23	root	rt	0	0	0	0	S	0.0	0.0	0:00.24	migration/1		
24	root	20	0	0	0	0	S	0.0	0.0	0:00.24	ksoftirqd/1		
26	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/1:0H-events_highpri		
27	root	20	0	0	0	0	I	0.0	0.0	0:00.00	kworker/u5:0-events_unbound		
28	root	20	0	0	0	0	I	0.0	0.0	0:00.04	kworker/u6:0-writeback		
30	root	20	0	0	0	0	I	0.0	0.0	0:00.00	kworker/u6:1-events_unbound		
31	root	20	0	0	0	0	S	0.0	0.0	0:00.01	kdevtmpfs		
32	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/R-inet_		
33	root	20	0	0	0	0	I	0.0	0.0	0:01.17	kworker/u5:1-flush-8:0		
34	root	20	0	0	0	0	S	0.0	0.0	0:00.00	kworker/u5:2-kerninit		

:*

4. Adjusting Process Priority

Command 1: nice -n 10 sleep 300 & **Command 2:** renice -n -5 -p 3050 ↗

```
zsh: corrupt history file /home/kali/.zsh_history
└─(kali㉿kali)-[~]
└─$ nice -n 10 sleep 300 &
[1] 9277

└─(kali㉿kali)-[~]
└─$ sudo renice -n -5 -p 9277
[sudo] password for kali:
9277 (process ID) old priority 15, new priority -5

└─(kali㉿kali)-[~]
└─$ █
```

🔧 5. CPU Affinity

Command 1: taskset -cp 3050 Command 2: taskset -cp 1 3050

```
—(kali㉿kali)-[~]
$ ps -u$USER | head -5
 PID TTY      TIME CMD
 805 ?        00:00:00 systemd
 806 ?        00:00:00 (sd-pam)
 822 ?        00:00:00 pipewire
 823 ?        00:00:00 pipewire
```

```
—(kali㉿kali)-[~]
$ sleep 300 &
1] 103133
```

```
—(kali㉿kali)-[~]
$ nproc
```

```
—(kali㉿kali)-[~]
$ taskset -cp 103133
pid 103133's current affinity list: 0,1
```

```
—(kali㉿kali)-[~]
$ taskset -cp 1 103133
pid 103133's current affinity list: 0,1
pid 103133's new affinity list: 1
```

```
—(kali㉿kali)-[~]
$ █
```

6. I/O Scheduling Priority

Command: ionice -c 3 -p 3050 📽

```
$ ps
  PID TTY      TIME CMD
105594 pts/28  00:00:00 zsh
105659 pts/28  00:00:00 ps

(kali㉿kali)-[~]
$ ps -l
F S  UID      PID  PPID C PRI NI ADDR SZ WCHAN TTY          TIME CMD
0 S  1000  105594 105591 0 80   0 - 2531 sigsus pts/28  00:00:00 zsh
0 R  1000  105722 105594 0 80   0 - 2756 -      pts/28  00:00:00 ps

(kali㉿kali)-[~]
$ sudo ionice -p 105594
[sudo] password for kali:
none: prio 0

(kali㉿kali)-[~]
$ sudo ionice -c 3 -p 105594

(kali㉿kali)-[~]
$ █
```

7. File Descriptors Used by a Process

Command: lsof -p 3050 | head -5 📽

```
F S  UID      PID  PPID C PRI NI ADDR SZ WCHAN TTY          TIME CMD
0 S  1000  111468 111465 1 80   0 - 2531 sigsus pts/38  00:00:00 zsh
0 R  1000  111521 111468 0 80   0 - 2756 -      pts/38  00:00:00 ps

(kali㉿kali)-[~]
$ sudo lsof -p 111468
[sudo] password for kali:
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
zsh    111468 kali cwd DIR  8,1    4096 1179650 /home/kali
zsh    111468 kali rtd DIR  8,1    4096 2 /
zsh    111468 kali txt REG  8,1  869864 173666 /usr/bin/zsh
zsh    111468 kali mem REG  8,1  14464 1066721 /usr/lib/x86_64-linux-gnu/zsh/5.9/zsh/regex.so
zsh    111468 kali mem REG  8,1  209344 825805 /usr/share/zsh/functions/Misc.zwc
zsh    111468 kali mem REG  8,1  302784 826829 /usr/share/zsh/functions/Completion/Base.zwc
zsh    111468 kali mem REG  8,1  18752 1066720 /usr/lib/x86_64-linux-gnu/zsh/5.9/zsh/stat.so
zsh    111468 kali mem REG  8,1  3052896 435155 /usr/lib/locale/locale-archive
zsh    111468 kali mem REG  8,1  32520 1066742 /usr/lib/x86_64-linux-gnu/zsh/5.9/zsh/system.so
zsh    111468 kali mem REG  8,1  14600 1066722 /usr/lib/x86_64-linux-gnu/zsh/5.9/zsh/zleparameter.so
zsh    111468 kali mem REG  8,1  192136 825791 /usr/share/zsh/functions/Completion.zwc
zsh    111468 kali mem REG  8,1  49104 1066746 /usr/lib/x86_64-linux-gnu/zsh/5.9/zsh/parameter.so
zsh    111468 kali mem REG  8,1  39240 1066708 /usr/lib/x86_64-linux-gnu/zsh/5.9/zsh/zutil.so
zsh    111468 kali mem REG  8,1  159648 1066732 /usr/lib/x86_64-linux-gnu/zsh/5.9/zsh/complete.so
zsh    111468 kali mem REG  8,1  339744 1066715 /usr/lib/x86_64-linux-gnu/zsh/5.9/zsh/zle.so
zsh    111468 kali mem REG  8,1  1926256 439100 /usr/lib/x86_64-linux-gnu/libc.so.6
zsh    111468 kali mem REG  8,1  907784 439347 /usr/lib/x86_64-linux-gnu/libm.so.6
zsh    111468 kali mem REG  8,1  216368 439046 /usr/lib/x86_64-linux-gnu/libtinfo.so.6.4
zsh    111468 kali mem REG  8,1  47288 440000 /usr/lib/x86_64-linux-gnu/libcap.so.2.66
zsh    111468 kali mem REG  8,1  14536 1066711 /usr/lib/x86_64-linux-gnu/zsh/5.9/zsh/terminfo.so
zsh    111468 kali mem REG  8,1  27028 1064964 /usr/lib/x86_64-linux-gnu/gconv/gconv-modules.cache
zsh    111468 kali mem REG  8,1  210792 437939 /usr/lib/x86_64-linux-gnu/ld-linux-x86-64.so.2
zsh    111468 kali 0u  CHR 136,38 0t0  41 /dev/pts/38
zsh    111468 kali 1u  CHR 136,38 0t0  41 /dev/pts/38
zsh    111468 kali 2u  CHR 136,38 0t0  41 /dev/pts/38
zsh    111468 kali 10u CHR 136,38 0t0  41 /dev/pts/38
zsh    111468 kali 12r REG  8,1  192136 825791 /usr/share/zsh/functions/Completion.zwc
zsh    111468 kali 14r REG  8,1  302784 826829 /usr/share/zsh/functions/Completion/Base.zwc
zsh    111468 kali 15r REG  8,1  209344 825805 /usr/share/zsh/functions/Misc.zwc
```

8. Trace System Calls of a Process

Command: strace -p 3050 📽

```
kali㉿kali:~$ strace -p 3050
strace: Process 3050 attached
restart_syscall(<... resuming interrupted nanosleep
...>) = 0
nanosleep({tv_sec=300, tv_nsec=0}, 0x7ffd4a60d8b0)
= ? ERESTART_RESTARTBLOCK (Interrupted by signal)
kali㉿kali:~$
```

:

🔗 9. Find Process Using a Port

Command: sudo fuser -n tcp 8080 📽

```
zsh: corrupt history file /home/kali/.zsh_history
└─(kali㉿kali)-[~]
└─$ ps -l
F S      UID      PID  PPID  C PRI  NI ADDR SZ WCHAN  TTY          TIME CMD
0 S  1000  149826 149809  1 80    0 -  2530 sigsus pts/43  00:00:00 zsh
0 R  1000  149900 149826 25 80    0 -  2756 -      pts/43  00:00:00 ps

└─(kali㉿kali)-[~]
└─$ sudo fuser -n tcp 149826
[sudo] password for kali:

└─(kali㉿kali)-[~]
└─$ sudo fuser -n tcp 149826
```

📊 10. Per-Process Statistics

Command: pidstat -p 3050 2 3 📽

```
└─(kali㉿kali)-[~]
└─$ pidstat -p 152358 2 3
Linux 6.6.9-amd64 (kali)           11/03/2025       _x86_64_        (2 CPU)
           CPU load average: 0.00 0.00 0.00
   CPU   %usr %system  %guest   %wait   %CPU   CPU  Command
 04:50:45 AM 1000     0.00    0.00    0.00    0.00    0.00    0  zsh
 04:50:47 AM 1000     0.00    0.00    0.00    0.00    0.00    0  zsh
 04:50:49 AM 1000     0.00    0.00    0.00    0.00    0.00    0  zsh
 04:50:51 AM 1000     0.00    0.00    0.00    0.00    0.00    0  zsh
Average:     1000     0.00    0.00    0.00    0.00    0.00    -  zsh

└─(kali㉿kali)-[~]
└─$
```

🔒 11. Control Groups (cgroups)

Command Sequence:

```
sudo cgcreate -g cpu,memory:/testgroup
echo 50000 | sudo tee /sys/fs/cgroup/cpu/testgroup/cpu.cfs_quota_us
```

```
echo 100M | sudo tee /sys/fs/cgroup/memory/testgroup/memory.limit_in_bytes
echo 3050 | sudo tee /sys/fs/cgroup/cpu/testgroup/cgroup.procs
```



```
kali@kali:~$ sudo cgcreate -g cpu,memory:/testgroup
```

Limit CPU and Memory:

```
echo 50000 | sudo tee /sys/fs/cgroup/cpu/testgroup/cps_quota_us
echo 100M | sudo tee /sys/fs/cgroup/memory/testgroup/memory.limit_in_bytes
```

Add Process (PID 3050) to cgroup:

```
echo 3050 | sudo tee /sys/fs/cgroup/cpu/testgroup/cgroup.procs
```

```
kali@kali:~$
```

⌚ 12. Alternatives to nice / renice

You can show **one example** among these for demonstration, like: `sudo chrt -f 50 sleep 1000`

```
kali@kali:~ $ sudo chrt -f 50 sleep 1000
kali@kali:~ $ chrt -p 3050
pid 3050: sched fifo priority 50
kali@kali:~ $ ionice -c 2 -n 7 tar -czf backup.tar.gz
/home
kali@kali:~ $ taskset -c 1 firefox
30012          sudo cgcreate -g cpu,memory:/lowprio
kali@kali:~ $ echo 20000 | sudo tee /sys/fs/cgroup/cpu/cst
cpu/lowrro.procs
kali@kali:~ $ echo 200M | sudo tee /sys/fs/cgroup/memory/po
mprio/memory.limit_in_bytes
kali@kali:~ $ echo 1234 | sudo tee /sys/fs/cgroup/cpu/lowp
rio/cgroup.procs
kali@kali:~ $ systemd-run --scope -p CPUWeight=200 stress --cpu 4
kali@kali:~ $ sudo schedtool -R -p 10 3050
```
