



Linux Tutorial Part Two

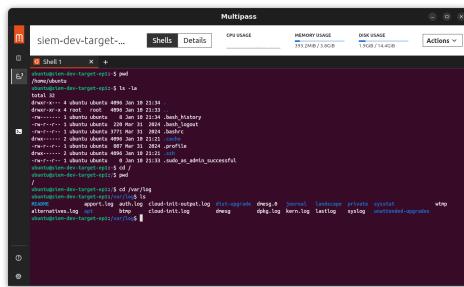
In this article we will cover:

- Directory Structure & Overview
 - Basic File System Navigation
 - File Manipulation Basics
 - System Logs & Processes Overview

The 'man' and 'help' commands followed by another command will display the "man pages" "help" information for that command. This documentation is useful, especially without internet. Most commands can be followed by '-h' or '--help' to list usage and options.  My biggest tip is learn how to research and find the answer. It's okay if you don't know or can't remember everything, no one does. There's a plethora of information on the internet, from vendor documentation and forums, to YouTube videos and blogs for almost anything. Finally, it's also okay to ask for help if you're struggling to find the answer.

Directory Structure & Overview

In linux, everything is a file. The base, or root, of the file system is represented as '`/`'. When you open a new terminal, you're typically going to be in your current user's home directory '`/home/$USER`', and have a '`~`' next to your prompt. The same is true for '`/`'.



A screenshot of a terminal window titled 'Shell1' within a 'Multipass' application. The terminal shows the command `ls -la` being run in the directory `/home/ubuntu`. The output lists several files and directories, including `Desktop`, `Downloads`, `Documents`, `Music`, `Pictures`, `Public`, and `Templates`. There are also hidden files like `.bashrc`, `.profile`, and `.Xauthority`. The terminal window has a dark background and light-colored text. At the bottom, there are tabs for 'Shells', 'Details', 'CPU Usage', 'Memory Usage', 'Disk Usage', and 'Actions'.

Use '`pwd`' at any time to print the path of your current directory. Display the contents of the current directory with '`ls`'. You can also show "hidden" files by using '`ls -a`', or get more info with '`ls -la`' (for a long list), some distributions may slightly differ in aliases.

Basic File System Navigation

Changing directories can be done by using '`cd`' followed by the directory name, or by the absolute path '`cd /var/log`'. You can change to your home directory from anywhere with '`cd ~`'.

From the root of the file system, list the contents 'ls -l'. You should see something similar to the output below.

```
ubuntu@siem-dev-target-epi:/ $ ls -l
total 76
lrwxrwxrwx  1 root root    7 Apr 22 2024 bin -> usr/bin
drwxr-xr-x  2 root root 4096 Feb 26 2024 bin usr-is-merged
drwxr-xr-x  5 root root 4096 Dec 13 12:57 boot
drwxr-xr-x 18 root root 3988 Jan 10 21:59 dev
drwxr-xr-x 106 root root 4096 Jan 10 21:34 etc
drwxr-xr-x  4 root root 4096 Jan 10 21:33 home
lrwxrwxrwx  1 root root    7 Apr 22 2024 lib -> usr/lib
drwxr-xr-x  2 root root 4096 Apr  8 2024 lib usr-is-merged
lrwxrwxrwx  1 root root    9 Apr 22 2024 lib64 -> usr/lib64
drwx----- 2 root root 16384 Dec 13 12:56 lost+found
drwxr-xr-x  2 root root 4096 Dec 13 12:53 media
drwxr-xr-x  2 root root 4096 Dec 13 12:53 mnt
drwxr-xr-x  2 root root 4096 Dec 13 12:53 opt
dr-xr-xr-x 167 root root    0 Jan 10 21:59 proc
drwx----- 3 root root 4096 Jan 11 16:11 root
drwxr-xr-x  27 root root 828 Jan 11 16:10 run
lrwxrwxrwx  1 root root    8 Apr 22 2024 sbin -> usr/sbin
drwxr-xr-x  2 root root 4096 Mar 31 2024 sbin usr-is-merged
drwxr-xr-x  2 root root 4096 Jan 10 21:21 snap
drwxr-xr-x  2 root root 4096 Dec 13 12:53 srv
dr-xr-xr-x 13 root root    0 Jan 11 16:24 sys
drwxrwxrwt 12 root root 4096 Jan 11 16:11 tmp
drwxr-xr-x 12 root root 4096 Dec 13 12:53 usr
drwxr-xr-x 13 root root 4096 Jan 10 21:21 var
ubuntu@siem-dev-target-epi:/ $
```

Notice, along the left column, you'll see the following data below. At a high level, these are permissions, 'r'=read, 'w'=write, 'x'=execute. The first character tells you the "type", 'd'=directory(folder), 'l'=link(symlink), and '-'=file. The next 3 are permissions for the "owner", next 3 for the "group", and the last 3 for "everyone else". The example above shows 2 columns displaying "root" all the way down, the first space is the "owner", second space is the "group".

Find the hierarchy table here:

The AI workspace that works for you. | Notion

A tool that connects everyday work into one space. It gives you and your teams AI tools—search, writing, note-taking—inside an all-in-one, flexible workspace.

https://www.notion.so/kishinlabs/Hierarchy-2e55f1724a0b80eda9b2e06abe3bdf57?source=copy_link

 **Notion**

/rite, plan, organize.
one connected workspace.



File Manipulation Basics

Creating, modifying, and deleting files is pretty straight forward. The commands we will need for now are `touch`, `mkdir`, `mv`, `rm`, `rmdir`, `nano`, and `cp`.

Start off by creating a new directory named "Notes" with '`mkdir Notes`' then use '`cd Notes`' to move into the directory. Obviously if we look, there's nothing here, using '`touch file.txt`' we can create a new file called `file.txt`. Nano is a simple text-based editor, use '`nano`

`file.txt`' to modify the new file, directions are in the photo below.

```
ubuntu@ljen-dev-target-opti2:~$ ls
ubuntu@ljen-dev-target-opti2:~$ mkdir Notes
ubuntu@ljen-dev-target-opti2:~$ ls
ubuntu@ljen-dev-target-opti2:~$ cd Notes
ubuntu@ljen-dev-target-opti2:/home/ubuntu$ ls
ubuntu@ljen-dev-target-opti2:/home/ubuntu$ touch file.txt
ubuntu@ljen-dev-target-opti2:/home/ubuntu$ ls
file.txt
ubuntu@ljen-dev-target-opti2:/home/ubuntu$ nano file.txt
ubuntu@ljen-dev-target-opti2:/home/ubuntu$ cp file.txt
cp: missing destination file operand after `file.txt'
Try `cp --help' for more information.
ubuntu@ljen-dev-target-opti2:/home/ubuntu$ cp file.txt /home/ubuntu
ubuntu@ljen-dev-target-opti2:/home/ubuntu$ ls
file.txt
ubuntu@ljen-dev-target-opti2:/home/ubuntu$ mv file.txt urgentfiles.txt
ubuntu@ljen-dev-target-opti2:/home/ubuntu$ ls
urgentfiles.txt
ubuntu@ljen-dev-target-opti2:/home/ubuntu$ cd
ubuntu@ljen-dev-target-opti2:~$ ls
notes file.txt
ubuntu@ljen-dev-target-opti2:~$ rm -r Notes
rm: failed to remove 'Notes': Directory not empty
ubuntu@ljen-dev-target-opti2:~$ rmdir Notes
ubuntu@ljen-dev-target-opti2:~$ ls
file.txt
```



Now say you want to copy that file, using '`cp`' we can do just that. Also note for the sake of demonstration I got 2 error messages. When you want to copy a file, you'll need to specify where you want it to go.

Copy the file to your users home directory '`cp file.txt /home/$user`'. You should have 2 copies now, 1 at `/home/user/Notes` and another at `/home/user`. Now rename the file in the Notes directory, the '`mv`' command can both move and rename files. Use '`mv file.txt urgentfiles.txt`' to rename the file, then assume it now contains sensitive data inside.

In the case you want to delete a directory, you can use '`rmdir`', however, the directory MUST already be empty for this command to work. If you '`mv`

urgentfiles.txt /home/user', you may then delete the directory.

Alternatively, you could, with caution, use '**rm -r**'
Notes', this will recursively delete the directory and all of the contents. If you opted to move the **urgentfiles.txt** file it should be in your home directory with **file.txt**. Use '**rm file.txt**' to remove the old file.

Bonus: Shred

The '**shred**' command can be used to overwrite and zero out file contents prior to deletion to ensure sensitive data cannot be recovered. Use '**cat** **urgentfiles.txt**' to see the data beforehand. Use '**shred** **urgentfiles.txt**' and you'll see the data is no longer recognizable.

A screenshot of a terminal window titled "Terminal". The window displays the command "shred -u -z -n 10 urgentfiles.txt" followed by its execution. The output shows the file being overwritten multiple times with random data, resulting in a mostly blank screen with some scattered characters.

System Logs & Processes Overview

Modern Linux systems often use systemd's **journald** for centralized, structured logging. This also supports

real-time monitoring and advanced filtering via the '`journctl`' command.

Another option is to use '`tail -f /var/log/syslog`' or '`/var/log/auth.log`', which will display the most recent logs and follow any new events. This can be useful for diagnosing user login or connectivity issues, as you'll see `auth.log` update in real time.

```
ubuntu@siem-dev-target-epi:~$ ls
ubuntu@siem-dev-target-epi:~$ ls
ubuntu@siem-dev-target-epi:~$ mkdir Notes
ubuntu@siem-dev-target-epi:~$ ls
Notes
ubuntu@siem-dev-target-epi:~$ cd Notes
ubuntu@siem-dev-target-epi:~/Notes$ ls
ubuntu@siem-dev-target-epi:~$ tail -f /var/log/syslog
2026-01-11T18:15:01.248629+00:00 siem-dev-target-epi CRON[147766]: (root) CMD (command -v debian-sai > /dev/null && debian-sai 1 1)
2026-01-11T18:17:01.286939+00:00 siem-dev-target-epi CRON[150111]: (root) CMD (cd / && run-parts --report /etc/cron.hourly)
2026-01-11T18:20:41.020881+00:00 siem-dev-target-epi systemd[1]: Starting sysstat-collect.service - system activity accounting tool...
2026-01-11T18:20:41.020881+00:00 siem-dev-target-epi systemd[1]: Finished sysstat-collect.service - system activity accounting tool.
2026-01-11T18:25:01.312045+00:00 siem-dev-target-epi CRON[159480]: (root) CMD (command -v debian-sai > /dev/null && debian-sai 1 1)
2026-01-11T18:30:20.999200+00:00 siem-dev-target-epi systemd[1]: Starting sysstat-collect.service - system activity accounting tool...
2026-01-11T18:30:21.017548+00:00 siem-dev-target-epi systemd[1]: sysstat-collect.service: Deactivated successfully.
2026-01-11T18:30:21.017964+00:00 siem-dev-target-epi systemd[1]: Finished sysstat-collect.service - system activity accounting tool.
2026-01-11T18:35:01.312045+00:00 siem-dev-target-epi CRON[171190]: (root) CMD (command -v debian-sai > /dev/null && debian-sai 1 1)
2026-01-11T18:36:50.404121+00:00 siem-dev-target-epi systemd[1]: Started session-24.scope - Session 24 of User ubuntu.
2026-01-11T18:37:13.970962+00:00 siem-dev-target-epi systemd[1]: Started session-25.scope - Session 25 of User ubuntu.
```

```
ubuntu@siem-dev-target-epi:~$ tail -f /var/log/auth.log
2026-01-11T18:15:01.253621+00:00 siem-dev-target-epi CRON[150765]: pam_unix(cron:session): session closed for user root
2026-01-11T18:17:01.287864+00:00 siem-dev-target-epi CRON[150110]: pam_unix(cron:session): session closed for user root(uid=0) by root(uid=0)
2026-01-11T18:25:01.290651+00:00 siem-dev-target-epi CRON[159470]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2026-01-11T18:25:01.306630+00:00 siem-dev-target-epi CRON[159480]: (root) CMD (command -v debian-sai > /dev/null && debian-sai 1 1)
2026-01-11T18:30:20.999200+00:00 siem-dev-target-epi systemd[1]: Starting sysstat-collect.service - system activity accounting tool...
2026-01-11T18:30:21.017548+00:00 siem-dev-target-epi systemd[1]: sysstat-collect.service: Deactivated successfully.
2026-01-11T18:30:21.017964+00:00 siem-dev-target-epi systemd[1]: Finished sysstat-collect.service - system activity accounting tool.
2026-01-11T18:35:01.311867+00:00 siem-dev-target-epi CRON[171190]: (root) CMD (command -v debian-sai > /dev/null && debian-sai 1 1)
2026-01-11T18:35:01.311867+00:00 siem-dev-target-epi CRON[171189]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2026-01-11T18:35:01.311867+00:00 siem-dev-target-epi CRON[171189]: pam_unix(cron:session): session closed for user root
2026-01-11T18:35:01.311867+00:00 siem-dev-target-epi CRON[171189]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2026-01-11T18:35:01.311867+00:00 siem-dev-target-epi CRON[171189]: pam_unix(cron:session): session closed for user root
2026-01-11T18:35:58.403924+00:00 siem-dev-target-epi sshd[173302]: Accepted publickey for ubuntu from 10.202.25.1 port 42792 ssh2: RSA SHA256:Tn9L6seewF8DH+k5eJc8n45N34CF42y4KFCbPqbET0
2026-01-11T18:36:50.403924+00:00 siem-dev-target-epi sshd[173302]: pam_unix(sshd:session): session opened for user ubuntu(uid=1000) by ubuntu(uid=1000)
2026-01-11T18:37:13.955987+00:00 siem-dev-target-epi sshd[173879]: Accepted publickey for ubuntu from 10.202.25.1 port 38888 ssh2: RSA SHA256:Tn9L6seewF8DH+k5eJc8n45N34CF42y4KFCbPqbET0
2026-01-11T18:37:13.957676+00:00 siem-dev-target-epi sshd[173879]: pam_unix(sshd:session): session opened for user ubuntu(uid=1000) by ubuntu(uid=1000)
2026-01-11T18:37:13.969633+00:00 siem-dev-target-epi systemd-logind[697]: New session 25 of user ubuntu.
```

System logs collect information about the operating system, including boot messages, kernel activities, hardware events, and startup processes. These logs are essential for diagnosing issues and monitoring overall system health. When it comes to the location of specific logs, it can differ depending on the distribution used. In Ubuntu, you can find some logs in `/var/log`.

```
ubuntu@siem-dev-target-ep1:~$ cd /var/log
ubuntu@siem-dev-target-ep1:/var/log$ ls
README      apport.log auth.log  cloud-init-output.log  dist-upgrade  dmesg.0   journal  landscape  private  sysstat      wtmp
alternatives.log apt      btmp     cloud-init.log       dmesg        dpkg.log  kern.log  lastlog    syslog    unattended-upgrades
ubuntu@siem-dev-target-ep1:/var/log$
```

Some require a specific command to display the logs, as mentioned above, others you can open with '**nano**'. The `/var/log/messages` and `/var/log/syslog` files are central repositories for general system messages.

Application logs record events specific to individual software applications, such as errors, warnings, and user activities. These logs help in diagnosing application-specific problems and analyzing performance. (`/var/log/httpd/access_log` and `/var/log/httpd/error_log` for Apache)

Security logs monitor authentication attempts, access control, and authorization events. Files like `/var/log/auth.log`, `/var/log/secure`, and `/var/log/faillog` are used to track user logins, failed attempts, and privilege escalations, making them vital for detecting potential security breaches. The **last** command will display recent failed login attempts.

Processes: Overview

Processes are exactly what they sound like, stuff running on the machine. Management is out of scope for this, but here are some ways to view some process information.

The `top` command is a way to see running processes, consumption, health, etc and refreshes every 2* seconds.

```
Top - 18:39:46 up 2:15, 4 users, load average: 0.01, 0.02, 0.12
Tasks: 113 total, 1 running, 112 sleeping, 0 stopped, 0 zombie
CPU(s): 0.4% us, 0.4% sy, 98.2% id, 0.0% wa, 0.0% hi, 0.0% si
Mem: 3983.8 total, 3344.7 free, 4614 used, 4664.5 buff/cache
Swap: 0.0 total, 0.0 free, 0.0 used, 3488.7 avail Mem

PID USER PR NI VIRT RES SHN S %CPU %MEM TIME+ COMMAND
 1 root 20 0 224M 320M 942.5 R 0.0 0.0 0:00.00 kworker/u:0
 2 root 20 0 0 0 0.0 S 0.0 0.0 0:00.00 kthread
 3 root 20 0 0 0 0.0 S 0.0 0.0 0:00.00 kworker/u:0-events_highpri
 4 root 20 0 0 0 0.0 S 0.0 0.0 0:00.00 kworker/u:0-kworker/u:0
 5 root 20 0 0 0 0.0 S 0.0 0.0 0:00.00 kworker/u:0-kworker/u:0
 6 root 20 0 0 0 0.0 S 0.0 0.0 0:00.00 kworker/u:0-kworker/u:0
 7 root 20 0 0 0 0.0 S 0.0 0.0 0:00.00 kworker/u:0-netns
 8 root 20 0 0 0 0.0 S 0.0 0.0 0:00.00 kworker/u:0-mem-events_highpri
 11 root 20 0 0 0 0.0 S 0.0 0.0 0:00.00 kworker/u:0-kworker/u:0
 13 root 20 0 0 0 0.0 S 0.0 0.0 0:00.00 kworker/u:0-kworker/u:0
 14 root 20 0 0 0 0.0 S 0.0 0.0 0:00.00 rcu_tasks_kthread
 15 root 20 0 0 0 0.0 S 0.0 0.0 0:00.00 rcu_tasks_rate_kthread
 16 root 20 0 0 0 0.0 S 0.0 0.0 0:00.00 rcu_tasks_rate_kthread
 17 root 20 0 0 0 0.0 S 0.0 0.0 0:00.00 ksoftirqd/0
 18 root 20 0 0 0 0.0 S 0.0 0.0 0:00.00 ksoftirqd/1
 19 root -51 0 0 0 0.0 S 0.0 0.0 0:00.00 ksoftirqd/2
 20 root -51 0 0 0 0.0 S 0.0 0.0 0:00.00 ksoftirqd/3
 21 root 20 0 0 0 0.0 S 0.0 0.0 0:00.00 cpubus/1
 22 root -51 0 0 0 0.0 S 0.0 0.0 0:00.00 tdf_wq/0
 23 root 20 0 0 0 0.0 S 0.0 0.0 0:00.00 ksoftirqd/4
 24 root 20 0 0 0 0.0 S 0.0 0.0 0:00.00 ksoftirqd/5
 25 root 20 0 0 0 0.0 S 0.0 0.0 0:00.00 ksoftirqd/6
 26 root 20 0 0 0 0.0 S 0.0 0.0 0:00.00 ksoftirqd/7
 27 root 20 0 0 0 0.0 S 0.0 0.0 0:00.00 kworker/u:0
 28 root 0:20 0 0 0 0.0 S 0.0 0.0 0:00.00 kworker/u:0-netns
 29 root 0:20 0 0 0 0.0 S 0.0 0.0 0:00.00 kworker/u:0-kworker/u:0
 30 root 20 0 0 0 0.0 S 0.0 0.0 0:00.00 khungakid
 31 root 20 0 0 0 0.0 S 0.0 0.0 0:00.00 oom_reaper
 32 root 20 0 0 0 0.0 S 0.0 0.0 0:00.00 oom_reaper
 33 root 0:20 0 0 0 0.0 S 0.0 0.0 0:00.00 kcompactd0
 34 root 20 0 0 0 0.0 S 0.0 0.0 0:00.00 kcompactd1
 35 root 20 0 0 0 0.0 S 0.0 0.0 0:00.00 kcompactd2
 36 root 20 0 0 0 0.0 S 0.0 0.0 0:00.00 kcompactd3
 37 root 20 0 0 0 0.0 S 0.0 0.0 0:00.00 kcompactd4
 38 root 39:19 0 0 0 0.5 0.0 0.0 0:00.00 khungakid
 39 root 0:20 0 0 0 0.1 0.0 0.0 0:00.00 kworker/u:0-klist
 40 root 0:20 0 0 0 0.1 0.0 0.0 0:00.00 kworker/u:0-klist
 41 root 0:20 0 0 0 0.1 0.0 0.0 0:00.00 kworker/u:0-blkg
 42 root -51 0 0 0 0.5 0.0 0.0 0:00.00 lruq/p:0-0
 43 root 0:20 0 0 0 0.1 0.0 0.0 0:00.00 kworker/u:0-tcp_d
```

Using `pstree` can show the process hierarchy.

```
ubuntu@stem-dev-target-epi1:~$ pstree
systemd--ModemManager---3*[{ModemManager}]
|-2*[agetty]
|`-cron
|-dbus-daemon
|-fwupd---5*[{fwupd}]
|-gpg-agent
|-multipathd---6*[{multipathd}]
|-polkitd---3*[{polkitd}]
|-rsyslogd---3*[{rsyslogd}]
|-sshd---sshd---sshd
|   |-2*[sshd---sshd---bash---tail]
|   |-sshd---sshd---bash---top
|   `|-sshd---sshd---bash---pstree
|-systemd---(sd-pam)
|-systemd-journal
|-systemd-logind
|-systemd-network
|-systemd-resolve
|-systemd-timesyn---{systemd-timesyn}
|-systemd-udevd
|-udisksd---5*[{udisksd}]
`-unattended-upgr---{unattended-upgr}
```

Using `ps aux` :

USER	PID	%CPU	%MEM	VSZ	RSS	TTY	STAT	START	TIME	COMMAND
root	1	0.0	0.3	22248	13252	?	Ss	16:03	0:01	/sbin/init
root	2	0.0	0.0	0	0	?	S	16:03	0:00	[kthreadd]
root	3	0.0	0.0	0	0	?	S	16:03	0:00	[pool_workqueue_release]
root	4	0.0	0.0	0	0	?	I<	16:03	0:00	[kworker/R-rCU_g]
root	5	0.0	0.0	0	0	?	I<	16:03	0:00	[kworker/R-rCU_p]
root	6	0.0	0.0	0	0	?	I<	16:03	0:00	[kworker/R-slub_]
root	7	0.0	0.0	0	0	?	I<	16:03	0:00	[kworker/R-netns]
root	9	0.0	0.0	0	0	?	I<	16:03	0:00	[kworker/0:0H-events_highpri]
root	12	0.0	0.0	0	0	?	I<	16:03	0:00	[kworker/R-mm_pe]
root	13	0.0	0.0	0	0	?	I	16:03	0:00	[rcu_tasks_kthread]
root	14	0.0	0.0	0	0	?	I	16:03	0:00	[rcu_tasks_rude_kthread]
root	15	0.0	0.0	0	0	?	I	16:03	0:00	[rcu_tasks_trace_kthread]
root	16	0.0	0.0	0	0	?	S	16:03	0:01	[ksoftirqd/0]
root	17	0.0	0.0	0	0	?	I	16:03	0:03	[rcu_preempt]
root	18	0.0	0.0	0	0	?	S	16:03	0:00	[migration/0]
root	19	0.0	0.0	0	0	?	S	16:03	0:00	[idle_inject/0]
root	20	0.0	0.0	0	0	?	S	16:03	0:00	[cpuhp/0]
root	21	0.0	0.0	0	0	?	S	16:03	0:00	[cpuhp/1]
root	22	0.0	0.0	0	0	?	S	16:03	0:00	[idle_inject/1]
root	23	0.0	0.0	0	0	?	S	16:03	0:00	[migration/1]
root	24	0.0	0.0	0	0	?	S	16:03	0:02	[ksoftirqd/1]
root	26	0.0	0.0	0	0	?	I<	16:03	0:00	[kworker/1:0H-events_highpri]
root	27	0.0	0.0	0	0	?	S	16:03	0:00	[kdevtmpfs]
root	28	0.0	0.0	0	0	?	I<	16:03	0:00	[kworker/R-inet_]
root	29	0.0	0.0	0	0	?	S	16:03	0:00	[kaudittd]
root	30	0.0	0.0	0	0	?	S	16:03	0:00	[khungtaskd]
root	32	0.0	0.0	0	0	?	S	16:03	0:00	[oom_reaper]
root	34	0.0	0.0	0	0	?	I<	16:03	0:00	[kworker/R-write]
root	35	0.0	0.0	0	0	?	S	16:03	0:00	[kcompactd0]
root	36	0.0	0.0	0	0	?	SN	16:03	0:00	[ksmd]
root	38	0.0	0.0	0	0	?	SN	16:03	0:00	[khugepaged]
root	39	0.0	0.0	0	0	?	I<	16:03	0:00	[kworker/R-kinte]
root	40	0.0	0.0	0	0	?	I<	16:03	0:00	[kworker/R-kblc]
root	41	0.0	0.0	0	0	?	I<	16:03	0:00	[kworker/R-blkg]
root	42	0.0	0.0	0	0	?	S	16:03	0:00	[irq/9-acpi]
root	43	0.0	0.0	0	0	?	I<	16:03	0:00	[kworker/R-tpm_d]
root	44	0.0	0.0	0	0	?	I<	16:03	0:00	[kworker/R-ata_s]
root	45	0.0	0.0	0	0	?	I<	16:03	0:00	[kworker/R-md]
root	46	0.0	0.0	0	0	?	I<	16:03	0:00	[kworker/R-md.bi]
root	47	0.0	0.0	0	0	?	I<	16:03	0:00	[kworker/R-edac-]
root	48	0.0	0.0	0	0	?	I<	16:03	0:00	[kworker/R-devfr]

```

Shell 1          Shell 2          Shell 3          Shell 4          +
systemd+ 637 0.0 0.2 19008 9472 ? Ss 16:04 0:00 /usr/lib/systemd/systemd-networkd
root 682 0.0 0.0 7224 2560 ? Ss 16:04 0:00 /usr/sbin/cron -f -P
message+ 683 0.0 0.1 9796 5376 ? Ss 16:04 0:00 @dbus-daemon --system --address=/systemd: --nofork --nopidfile --systemd-activation --syslog-only
root 697 0.0 0.2 18148 8704 ? Ss 16:04 0:00 /usr/lib/systemd/systemd-logind
syslog 715 0.0 0.1 222508 6144 ? Ss 16:04 0:00 /usr/sbin/rsyslogd -n -NONE
root 781 0.0 0.0 6148 2848 ttys0 Ss+ 16:04 0:00 /sbin/agetty -o -p -- \u --keep-baud 115200,57600,38400,9600 - vt220
root 793 0.0 0.5 118012 22912 ? Ss 16:04 0:00 /usr/bin/python3 /usr/share/unattended-upgrades/unattended-upgrade-shutdown --wait-for-signal
root 802 0.0 0.0 6104 1920 tty1 Ss+ 16:04 0:00 /sbin/agetty -o -p -- \u --noclear - linux
root 821 0.0 0.1 12020 7936 ? Ss 16:04 0:00 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
root 836 0.0 0.0 0 0 ? S 16:04 0:00 [psimon]
ubuntu 839 0.0 0.2 20288 11136 ? Ss 16:04 0:00 /usr/lib/systemd/systemd --user
ubuntu 840 0.0 0.0 21148 3516 ? S 16:04 0:00 (sd-pam)
root 1266 0.0 0.2 14740 9984 ? Ss 16:10 0:00 sshd: ubuntu [priv]
ubuntu 1323 0.1 0.1 14996 6820 ? S 16:10 0:18 sshd: ubuntu@notty
root 1400 0.0 0.2 14740 10112 ? Ss 16:10 0:00 sshd: ubuntu [priv]
ubuntu 1538 0.0 0.1 14996 6820 ? S 16:10 0:00 sshd: ubuntu@pts/0
ubuntu 1539 0.0 0.1 9192 5248 pts/0 Ss+ 16:10 0:00 -bash
polkittd 18989 0.0 0.1 308164 7888 ? Ss 16:25 0:00 /usr/lib/polkit-1/polkitd --no-debug
root 18991 0.0 0.3 469084 13568 ? Ss 16:25 0:00 /usr/libexec/udisks2/udisksd
root 19007 0.0 0.3 392088 12672 ? Ss 16:25 0:00 /usr/sbin/ModemManager
root 36156 0.0 1.0 600176 43220 ? Ss 16:39 0:02 /usr/libexec/fwupd/fwupd
root 36220 0.0 0.0 81808 2824 ? Ss 16:39 0:00 gpg-agent --homedir /var/lib/fwupd/gnupg --use-standard-socket --daemon
root 84200 0.0 0.0 0 0 ? I 17:20 0:02 [kworker/u:2-events]
root 99438 0.0 0.0 0 0 ? I 17:33 0:01 [kworker/u:1-events]
root 153428 0.0 0.0 0 0 ? I 18:19 0:00 [kworker/u:4:0-events_unbound]
root 165216 0.0 0.0 0 0 ? I 18:29 0:00 [kworker/u:4:3-events_power_efficient]
root 171348 0.0 0.0 0 0 ? I 18:35 0:00 [kworker/u:4:2-events_unbound]
root 173302 0.0 0.2 14736 10368 ? Ss 18:36 0:00 sshd: ubuntu [priv]
ubuntu 173400 0.0 0.1 14996 6816 ? S 18:36 0:00 sshd: ubuntu@pts/1
ubuntu 173401 0.0 0.1 9060 5120 pts/1 Ss+ 18:36 0:00 -bash
root 173879 0.0 0.2 14736 10368 ? Ss 18:37 0:00 sshd: ubuntu [priv]
ubuntu 173926 0.0 0.1 14992 6944 ? S 18:37 0:00 sshd: ubuntu@pts/2
ubuntu 173927 0.0 0.1 9060 5120 pts/2 Ss+ 18:37 0:00 -bash
root 177177 0.0 0.2 14736 10368 ? Ss 18:39 0:00 sshd: ubuntu [priv]
ubuntu 177234 0.0 0.1 14992 6944 ? S 18:39 0:00 sshd: ubuntu@pts/3
root 177236 0.0 0.0 0 0 ? I 18:39 0:00 [kworker/1:0-cgroup_destroy]
ubuntu 177237 0.0 0.1 9060 5120 pts/3 Ss 18:39 0:00 -bash
root 179717 0.0 0.0 0 0 ? I 18:42 0:00 [kworker/u:0]
root 181474 0.0 0.0 0 0 ? I 18:43 0:00 [kworker/u:4:4-events_unbound]
root 189165 0.0 0.0 0 0 ? I 18:50 0:00 [kworker/1:2]
root 189166 0.0 0.0 0 0 ? I 18:50 0:00 [kworker/1:3-events]
ubuntu 191156 0.0 0.1 11320 4352 pts/3 R+ 18:51 0:00 ps aux
ubuntu@sten-dev-target-epi:~$ 

```

Since everything in Linux is a file, the ' **Isof**' command (list open files) is powerful. Using ' **sudo Isof -i**' will show open "files" with IP, protocol information, and more.

Lastly, another command to consider getting familiar with is ' **ss**' . Check out the options and flags and give them a shot. I have included an example with ' **ss -tuln**' . Info can be piped or filtered via ' **grep**' .

```

ubuntu@siem-dev-target-epi:~$ sudo lsof -i
COMMAND   PID   USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
systemd      1   root    91u  IPv4  6614      0t0  TCP *:ssh (LISTEN)
systemd      1   root    92u  IPv6  6616      0t0  TCP *:ssh (LISTEN)
systemd-r  520  systemd-resolve  14u  IPv4  5506      0t0  UDP localdnsstub:domain
systemd-r  520  systemd-resolve  15u  IPv4  5507      0t0  TCP localdnsstub:domain (LISTEN)
systemd-r  520  systemd-resolve  16u  IPv4  5508      0t0  UDP localdnsproxy:domain
systemd-r  520  systemd-resolve  17u  IPv4  5509      0t0  TCP localdnsproxy:domain (LISTEN)
systemd-n  637  systemd-network  20u  IPv4  6524      0t0  UDP siem-dev-target-epi:multipass:bootpc
systemd-n  637  systemd-network  23u  IPv4  6519      0t0  UDP siem-dev-target-epi:bootpc
sshd     821   root    3u  IPv4  6614      0t0  TCP *:ssh (LISTEN)
sshd     821   root    4u  IPv6  6616      0t0  TCP *:ssh (LISTEN)
sshd    1266   root    4u  IPv4  9328      0t0  TCP siem-dev-target-epi:ssh->laptop-kishinlabs:49216 (ESTABLISHED)
sshd    1323  ubuntu    4u  IPv4  9328      0t0  TCP siem-dev-target-epi:ssh->laptop-kishinlabs:49216 (ESTABLISHED)
sshd    1400   root    4u  IPv4  8867      0t0  TCP siem-dev-target-epi:ssh->laptop-kishinlabs:49232 (ESTABLISHED)
sshd    1538  ubuntu    4u  IPv4  8867      0t0  TCP siem-dev-target-epi:ssh->laptop-kishinlabs:49232 (ESTABLISHED)
sshd    173302  root    4u  IPv4  191790      0t0  TCP siem-dev-target-epi:ssh->laptop-kishinlabs:42792 (ESTABLISHED)
sshd    173400  ubuntu    4u  IPv4  191790      0t0  TCP siem-dev-target-epi:ssh->laptop-kishinlabs:42792 (ESTABLISHED)
sshd    173879  root    4u  IPv4  192113      0t0  TCP siem-dev-target-epi:ssh->laptop-kishinlabs:38808 (ESTABLISHED)
sshd    173926  ubuntu    4u  IPv4  192113      0t0  TCP siem-dev-target-epi:ssh->laptop-kishinlabs:38808 (ESTABLISHED)
sshd    177177  root    4u  IPv4  195936      0t0  TCP siem-dev-target-epi:ssh->laptop-kishinlabs:53952 (ESTABLISHED)
sshd    177234  ubuntu    4u  IPv4  195936      0t0  TCP siem-dev-target-epi:ssh->laptop-kishinlabs:53952 (ESTABLISHED)
ubuntu@siem-dev-target-epi:~$ ss -tuln
Netid      State      Recv-Q      Send-Q      Local Address:Port          Peer Address:Port      Process
udp        UNCONN      0           0           127.0.0.54:53            0.0.0.0:*                  0.0.0.0:*
udp        UNCONN      0           0           127.0.0.53%lo:53          0.0.0.0:*
udp        UNCONN      0           0           10.202.25.20%ens3:68       0.0.0.0:*
udp        UNCONN      0           0           10.202.25.185%ens3:68      0.0.0.0:*
tcp        LISTEN      0           0           127.0.0.53:53             0.0.0.0:*
tcp        LISTEN      0           0           0.0.0.0:22                0.0.0.0:*
tcp        LISTEN      0           0           127.0.0.54:53             0.0.0.0:*
tcp        LISTEN      0           0           [::]:22                  [::]:*
ubuntu@siem-dev-target-epi:~$ 

```

This is a high level overview but we are only on part 2. (:

- **Alex a.k.a KishinInfosec 2025**



Hierarchy