

SMARTBRIDGE EXTERNSHIP

(Cyber Threat Intelligence (SIEM Analyst with IBM Qradar))

NAME: MALLA SRIRAJ

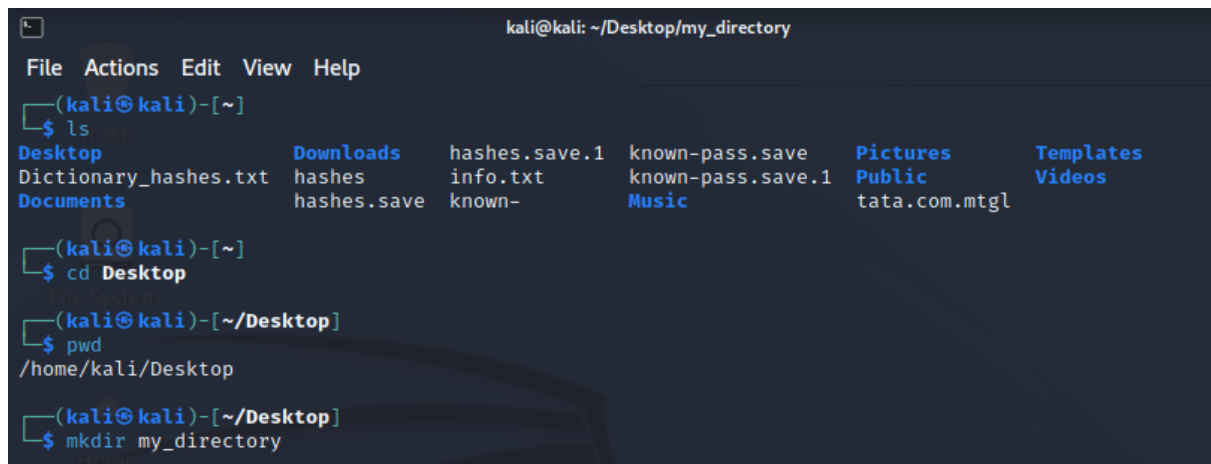
REG.NO: 20BCN7117

CAMPUS : VIT AP UNIVERSITY

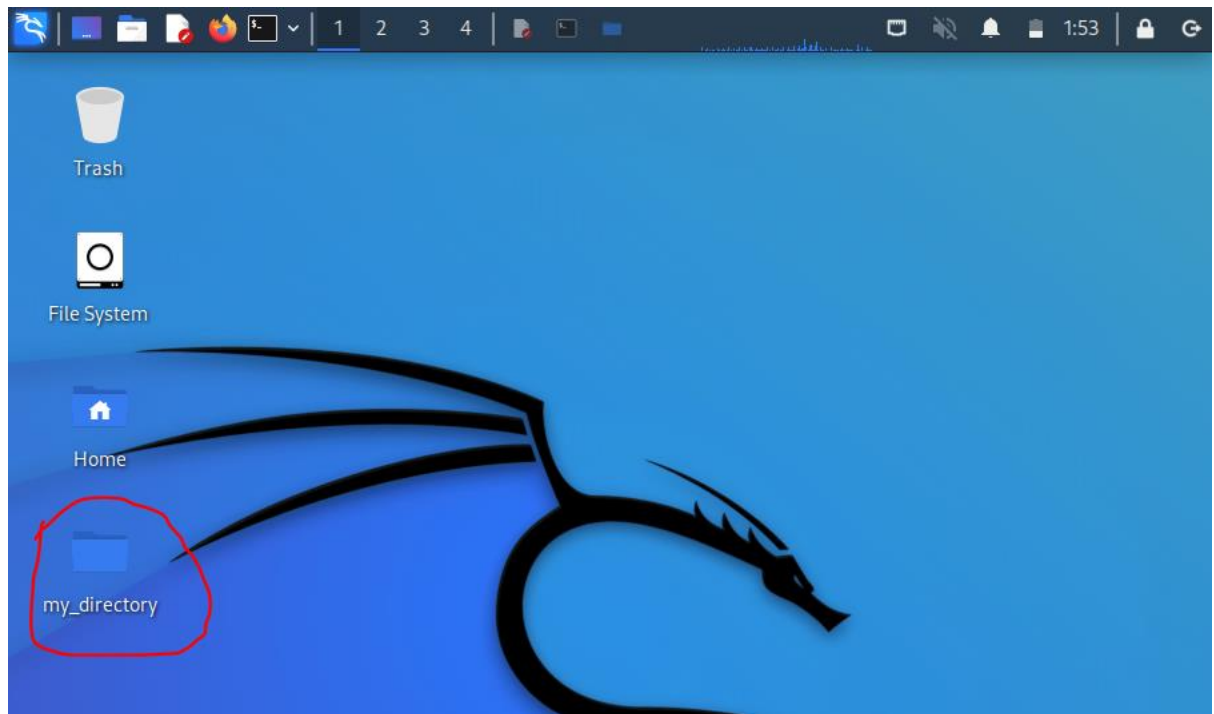
Assignment: Bash Shell Basics

Task 1: File and Directory Manipulation

1. Create a directory called "my_directory".

A terminal window titled 'kali@kali: ~/Desktop/my_directory' showing the steps to create a directory. The user runs 'ls' to list files in the home directory, then 'cd Desktop' to move to the Desktop directory, then 'pwd' to confirm the current directory is '/home/kali/Desktop', and finally 'mkdir my_directory' to create the new directory.

```
kali@kali: ~/Desktop/my_directory
File Actions Edit View Help
(kali@kali)-[~]
$ ls
Desktop      Downloads    hashes.save.1  known-pass.save  Pictures      Templates
Dictionary_hashes.txt hashes        info.txt       known-pass.save.1 Public         Videos
Documents    hashes.save  known-         Music            tata.com.mtg1
(kali@kali)-[~]
$ cd Desktop
(kali@kali)-[~/Desktop]
$ pwd
/home/kali/Desktop
(kali@kali)-[~/Desktop]
$ mkdir my_directory
```



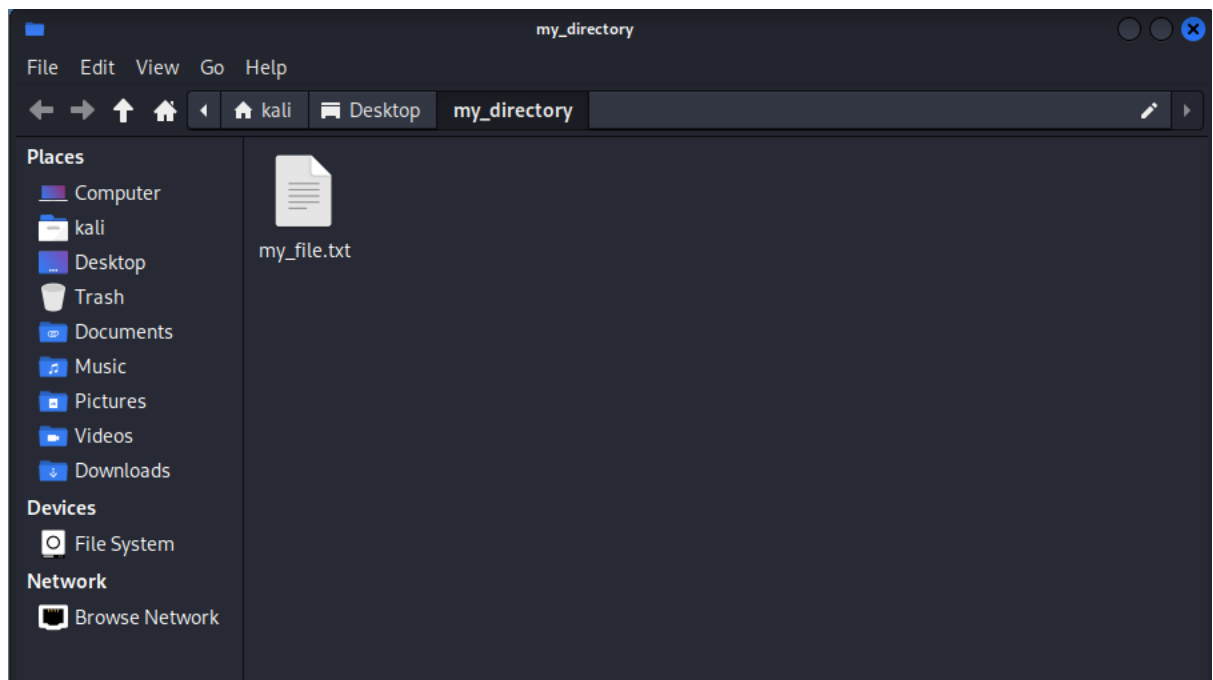
2. Navigate into the "my_directory".

```
(kali㉿kali)-[~/Desktop]
$ mkdir my_directory

(kali㉿kali)-[~/Desktop]
$ cd my_directory
```

3. Create an empty file called "my_file.txt".

```
(kali㉿kali)-[~/Desktop/my_directory]
$ touch my_file.txt
```



4. List all the files and directories in the current directory.

```
(kali㉿kali)-[~/Desktop/my_directory]
$ ls
my_file.txt
```

5. Rename "my_file.txt" to "new_file.txt".

```
(kali㉿kali)-[~/Desktop/my_directory]
$ mv my_file.txt new_file.txt
```

6. Display the content of "new_file.txt" using a pager tool of your choice.

```
(kali㉿kali)-[~/Desktop/my_directory]
$ less new_file.txt
```

7. Append the text "Hello, World!" to "new_file.txt".

```
(kali㉿kali)-[~/Desktop/my_directory]
$ echo "Hello, World!" >> new_file.txt
dquote>
```

8. Create a new directory called "backup" within "my_directory".

```
(kali㉿kali)-[~/Desktop/my_directory]
$ mkdir backup
```

9. Move "new_file.txt" to the "backup" directory.

```
(kali㉿kali)-[~/Desktop/my_directory]
$ mv new_file.txt backup/
```

10. Verify that "new_file.txt" is now located in the "backup" directory.

```
(kali㉿kali)-[~/Desktop/my_directory]
$ ls backup/
new_file.txt
```

11. Delete the "backup" directory and all its contents.

```
(kali㉿kali)-[~/Desktop/my_directory]
$ rm -r backup
```

Task 2: Permissions and Scripting

- Create a new file called "my_script.sh".

```
(kali㉿kali)-[~/Desktop/my_directory]
$ touch my_script.sh
```

- Edit "my_script.sh" using a text editor of your choice and add the following lines:

```
bash
#!/bin/bash
echo "Welcome to my script!"
echo "Today's date is $(date)."
```

Save and exit the file.

```
(kali㉿kali)-[~/Desktop/my_directory]
$ #!/bin/bash
echo "Welcome to my script!"
echo "Today's date is $(date)."
```

quote>

- Make "my_script.sh" executable.

```
(kali㉿kali)-[~/Desktop/my_directory]
$ chmod +x my_script.sh
```

- Run "my_script.sh" and verify that the output matches the expected result.

```
(kali㉿kali)-[~/Desktop/my_directory]
$ ./my_script.sh
```

Task 3: Command Execution and Pipelines

- List all the processes running on your system using the "ps" command.

```
(kali㉿kali)-[~/Desktop/my_directory]
$ ps aux
```

USER	PID	%CPU	%MEM	VSZ	RSS	TTY	STAT	START	TIME	COMMAND
root	1	0.0	0.5	167948	12048	?	Ss	01:26	0:02	/sbin/init splash
root	2	0.0	0.0	0	0	?	S	01:26	0:00	[kthreadd]
root	3	0.0	0.0	0	0	?	I<	01:26	0:00	[rcu_gp]
root	4	0.0	0.0	0	0	?	I<	01:26	0:00	[rcu_par_gp]
root	5	0.0	0.0	0	0	?	I<	01:26	0:00	[netns]
root	7	0.0	0.0	0	0	?	I<	01:26	0:00	[kworker/0:0H-events_highpri]
root	9	0.0	0.0	0	0	?	I<	01:26	0:00	[kworker/0:1H-events_highpri]
root	10	0.0	0.0	0	0	?	I<	01:26	0:00	[mm_percpu_wq]
root	11	0.0	0.0	0	0	?	I	01:26	0:00	[rcu_tasks_kthread]
root	12	0.0	0.0	0	0	?	I	01:26	0:00	[rcu_tasks_rude_kthread]
root	13	0.0	0.0	0	0	?	I	01:26	0:00	[rcu_tasks_trace_kthread]
root	14	0.0	0.0	0	0	?	S	01:26	0:00	[ksoftirqd/0]
root	15	0.0	0.0	0	0	?	I	01:26	0:02	[rcu_preempt]
root	16	0.0	0.0	0	0	?	S	01:26	0:00	[migration/0]
root	17	0.0	0.0	0	0	?	I	01:26	0:00	[kworker/0:1-events]
root	18	0.0	0.0	0	0	?	S	01:26	0:00	[cpuhp/0]
root	19	0.0	0.0	0	0	?	S	01:26	0:00	[cpuhp/1]
root	20	0.0	0.0	0	0	?	S	01:26	0:00	[migration/1]
root	21	0.0	0.0	0	0	?	S	01:26	0:00	[ksoftirqd/1]
root	23	0.0	0.0	0	0	?	I<	01:26	0:00	[kworker/1:0H-events_highpri]
root	26	0.0	0.0	0	0	?	S	01:26	0:00	[kdevtmpfs]
root	27	0.0	0.0	0	0	?	I<	01:26	0:00	[inet_frag_wq]
root	28	0.0	0.0	0	0	?	S	01:26	0:00	[kauditd]
root	29	0.0	0.0	0	0	?	S	01:26	0:00	[khungtaskd]
root	30	0.0	0.0	0	0	?	S	01:26	0:00	[oom_reaper]
root	31	0.0	0.0	0	0	?	I<	01:26	0:00	[writeback]
root	32	0.0	0.0	0	0	?	S	01:26	0:00	[kcompactd0]
root	33	0.0	0.0	0	0	?	SN	01:26	0:00	[ksmd]
root	34	0.0	0.0	0	0	?	SN	01:26	0:00	[khugepaged]
root	35	0.0	0.0	0	0	?	I<	01:26	0:00	[kintegrityd]
root	36	0.0	0.0	0	0	?	I<	01:26	0:00	[kblockd]
root	37	0.0	0.0	0	0	?	I<	01:26	0:00	[blkcg_punt_bio]
root	38	0.0	0.0	0	0	?	I<	01:26	0:00	[tpm_dev_wq]
root	39	0.0	0.0	0	0	?	I<	01:26	0:00	[edac-poller]
root	40	0.0	0.0	0	0	?	I<	01:26	0:00	[devfreq_wq]
root	41	0.0	0.0	0	0	?	S	01:26	0:00	[kswapd0]
root	50	0.0	0.0	0	0	?	I<	01:26	0:00	[kthrotld]
root	52	0.0	0.0	0	0	?	I<	01:26	0:00	[acpi_thermal_pm]
root	53	0.0	0.0	0	0	?	I<	01:26	0:00	[kworker/1:1H-events_highpri]
root	54	0.0	0.0	0	0	?	I<	01:26	0:00	[mld]
root	55	0.0	0.0	0	0	?	I<	01:26	0:00	[ipv6_addrconf]
root	60	0.0	0.0	0	0	?	I<	01:26	0:00	[kstrp]
root	65	0.0	0.0	0	0	?	I<	01:26	0:00	[zswap-shrink]
root	66	0.0	0.0	0	0	?	I<	01:26	0:00	[kworker/u5:0]
root	132	0.0	0.0	0	0	?	I<	01:26	0:00	[ata_sff]
root	133	0.0	0.0	0	0	?	I<	01:26	0:00	[cryptd]

```

root      133 0.0 0.0 0 0 ? I< 01:26 0:00 [cryptd]
root      136 0.0 0.0 0 0 ? S 01:26 0:00 [scsi_ah_0]
root      137 0.0 0.0 0 0 ? S 01:26 0:00 [scsi_ah_1]
root      138 0.0 0.0 0 0 ? I< 01:26 0:00 [scsi_tmfx_1]
root      139 0.0 0.0 0 0 ? I< 01:26 0:00 [scsi_tmfx_0]
root      147 0.0 0.0 0 0 ? S 01:26 0:00 [scsi_ah_2]
root      148 0.0 0.0 0 0 ? I< 01:26 0:00 [scsi_tmfx_2]
root      189 0.0 0.0 0 0 ? S 01:26 0:01 [irq/18-vmmwfx]
root      197 0.0 0.0 0 0 ? S 01:26 0:00 [card0-crtc0]
root      199 0.0 0.0 0 0 ? S 01:26 0:00 [card0-crtc1]
root      202 0.0 0.0 0 0 ? S 01:26 0:00 [card0-crtc2]
root      203 0.0 0.0 0 0 ? S 01:26 0:00 [card0-crtc3]
root      205 0.0 0.0 0 0 ? S 01:26 0:00 [card0-crtc4]
root      207 0.0 0.0 0 0 ? S 01:26 0:00 [card0-crtc5]
root      208 0.0 0.0 0 0 ? S 01:26 0:00 [card0-crtc6]
root      209 0.0 0.0 0 0 ? S 01:26 0:00 [card0-crtc7]
root      244 0.0 0.0 0 0 ? S 01:26 0:00 [jbd2/sda1-8]
root      245 0.0 0.0 0 0 ? I< 01:26 0:00 [ext4-rsv-conver]
root      295 0.0 1.3 58028 28100 ? Ss 01:26 0:00 /lib/systemd/systemd-journald
root      323 0.0 0.3 25848 6676 ? Ss 01:26 0:00 /lib/systemd/systemd-udev
root      387 0.0 0.2 8228 4996 ? Ss 01:26 0:00 /usr/sbin/haveged --foreground --verbose=1
root      405 0.0 0.0 0 0 ? I< 01:26 0:00 [rpciod]
root      406 0.0 0.0 0 0 ? I< 01:26 0:00 [xprtiod]
root      409 0.0 0.1 6808 2916 ? Ss 01:26 0:00 /usr/sbin/cron -f
message+ 410 0.0 0.2 11140 5936 ? Ss 01:26 0:01 /usr/bin/dbus-daemon --system --address=sh
root      413 0.0 0.5 237016 11496 ? Ssl 01:26 0:01 /usr/libexec/polkitd --no-debug
root      415 0.0 0.2 222368 4416 ? Ssl 01:26 0:00 /usr/sbin/rsyslogd -n -iNONE
root      417 0.0 0.4 25792 8356 ? Ss 01:26 0:00 /lib/systemd/systemd-logind
root      499 0.0 1.1 259464 24084 ? Ssl 01:26 0:00 /usr/sbin/NetworkManager --no-daemon
root      500 0.0 0.5 243824 11956 ? Ssl 01:26 0:00 /usr/sbin/ModemManager
root      510 0.0 0.1 294172 3164 ? Sl 01:26 0:00 /usr/sbin/VBoxService
root      526 0.0 0.3 310032 7888 ? Ssl 01:26 0:00 /usr/sbin/lightdm
root      541 2.3 5.8 379020 117872 tty7 Ssl+ 01:26 1:10 /usr/lib/xorg/Xorg :0 -seat seat0 -auth /v
root      542 0.0 0.0 5820 856 tty1 Ss+ 01:26 0:00 /sbin/agetty -o -p -- \u --noclear - linux
rtkit     673 0.0 0.1 153944 2984 ? Ssl 01:26 0:00 /usr/libexec/rtkit-daemon
root      723 0.0 0.4 163676 8644 ? Sl 01:27 0:00 lightdm --session-child 14 23
kali      731 0.0 0.5 19448 10824 ? Ss 01:27 0:00 /lib/systemd/systemd --user
kali      732 0.0 0.1 169084 3188 ? S 01:27 0:00 (sd-pam)
kali      747 0.0 0.3 36956 6744 ? S<sl 01:27 0:00 /usr/bin/pipewire
kali      748 0.0 0.3 20812 7324 ? Ssl 01:27 0:00 /usr/bin/pipewire-media-session
kali      749 0.0 1.7 652224 35408 ? Ssl 01:27 0:00 /usr/bin/pulseaudio --daemonize=no --log-t
kali      751 0.0 0.5 240904 12020 ? Ssl 01:27 0:00 /usr/bin/gnome-keyring-daemon --foreground
kali      753 0.0 0.2 10440 5800 ? Ss 01:27 0:01 /usr/bin/dbus-daemon --session --address=s
kali      760 0.0 1.3 269036 27772 ? Ssl 01:27 0:01 xfce4-session
kali      815 0.0 0.0 20248 476 ? S 01:27 0:00 /usr/bin/VBoxClient --clipboard
kali      817 0.0 0.2 152516 4252 ? Sl 01:27 0:00 /usr/bin/VBoxClient --clipboard
kali      826 0.0 0.0 20248 472 ? S 01:27 0:00 /usr/bin/VBoxClient --seamless
kali      828 0.0 0.1 152484 2648 ? Sl 01:27 0:00 /usr/bin/VBoxClient --seamless
kali      835 0.0 0.0 20248 476 ? S 01:27 0:00 /usr/bin/VBoxClient --draganddrop
kali      836 0.3 0.1 153000 2776 ? Sl 01:27 0:10 /usr/bin/VBoxClient --draganddrop
kali      839 0.0 0.0 20248 476 ? S 01:27 0:00 /usr/bin/VBoxClient --vmsvga
kali      840 0.0 0.1 152728 3924 ? Sl 01:27 0:00 /usr/bin/VBoxClient --vmsvga

```

```

kali      840 0.0 0.1 152728 3924 ? Sl 01:27 0:00 /usr/bin/VBoxClient --vmsvga
kali      847 0.0 0.0 8008 852 ? Ss 01:27 0:00 /usr/bin/ssh-agent x-session-manager
kali      857 0.0 0.6 312220 12372 ? Ssl 01:27 0:00 /usr/libexec/at-spi-bus-launcher
kali      863 0.0 0.2 9880 4904 ? S 01:27 0:00 /usr/bin/dbus-daemon --config-file=/usr/sh
kali      867 0.0 0.3 231584 6188 ? Sl 01:27 0:00 /usr/lib/x86_64-linux-gnu/xfce4/xfconf/xf
kali      872 0.0 0.5 165520 10336 ? Sl 01:27 0:00 /usr/libexec/at-spi2-registryd --use-gnome
kali      883 0.0 0.2 81320 5624 ? Sls 01:27 0:00 /usr/bin/gpg-agent --supervised
kali      885 0.7 5.4 933184 110580 ? Sl 01:27 0:22 xfwm4 --display :0.0 --sm-client-id 2818c4
kali      888 0.0 0.5 238672 12088 ? Ssl 01:27 0:00 /usr/libexec/gvfsd
kali      892 0.0 0.4 381508 8712 ? Sl 01:27 0:00 /usr/libexec/gvfsd-fuse /run/user/1000/gvf
kali      910 0.0 1.5 231592 30808 ? Sl 01:27 0:00 xfsettingsd --display :0.0 --sm-client-id
root      913 0.0 0.4 308684 9244 ? Ssl 01:27 0:00 /usr/libexec/upowerd
kali      919 0.1 2.3 476864 46736 ? Sl 01:27 0:05 xfce4-panel --display :0.0 --sm-client-id
kali      923 0.3 2.9 490516 58920 ? Sl 01:27 0:10 Thunar --sm-client-id 25c0101fb-ed50-45f2-
kali      928 0.0 2.4 335232 48936 ? Sl 01:27 0:00 /usr/lib/x86_64-linux-gnu/xfce4/panel/wrap
kali      929 0.1 2.7 475860 55968 ? Sl 01:27 0:05 xfdesktop --display :0.0 --sm-client-id 28
kali      932 1.3 1.5 205004 31868 ? Sl 01:27 0:39 /usr/lib/x86_64-linux-gnu/xfce4/panel/wrap
kali      933 0.0 1.3 341148 27000 ? Sl 01:27 0:00 /usr/lib/x86_64-linux-gnu/xfce4/panel/wrap
kali      934 0.6 1.5 350980 30784 ? Sl 01:27 0:18 /usr/lib/x86_64-linux-gnu/xfce4/panel/wrap
kali      935 0.1 2.2 593948 46212 ? Sl 01:27 0:04 /usr/lib/x86_64-linux-gnu/xfce4/panel/wrap
kali      936 0.0 2.1 326144 42876 ? Sl 01:27 0:00 /usr/lib/x86_64-linux-gnu/xfce4/panel/wrap
kali      937 0.0 2.2 391716 46176 ? Sl 01:27 0:01 /usr/lib/x86_64-linux-gnu/xfce4/panel/wrap
kali      940 0.0 2.1 334240 42692 ? Sl 01:27 0:00 /usr/lib/x86_64-linux-gnu/xfce4/panel/wrap
kali      969 0.0 1.9 390520 40192 ? Ssl 01:27 0:00 /usr/lib/x86_64-linux-gnu/xfce4/notifyd/xf
kali      991 0.0 1.3 193760 26772 ? Sl 01:27 0:00 xfce4-power-manager --restart --sm-client-
kali      996 0.0 1.5 432776 31944 ? Sl 01:27 0:00 light-locker
kali      1003 0.0 0.5 851440 11096 ? Sl 01:27 0:00 xiccd
kali      1011 0.0 0.3 235164 7084 ? Sl 01:27 0:00 /usr/libexec/geoclue-2.0/demos/agent
kali      1012 0.0 0.3 157600 6264 ? Ssl 01:27 0:00 /usr/libexec/dconf-service
kali      1022 0.0 2.6 374816 54688 ? Sl 01:27 0:01 /usr/bin/python3 /usr/bin/blueman-applet
colorord 1028 0.0 0.8 243564 17692 ? Ssl 01:27 0:00 /usr/libexec/colorord
kali      1044 0.0 0.8 187292 17848 ? Sl 01:27 0:00 /usr/lib/policykit-1-gnome/polkit-gnome-au
kali      1053 0.0 2.4 551360 49196 ? Sl 01:27 0:00 nm-applet
kali      1054 0.0 0.2 14764 4064 ? Ssl 01:27 0:00 xcape -e Super_L Control_L Escape
kali      1071 0.0 0.7 351832 16060 ? Ssl 01:27 0:00 /usr/libexec/gvfs-udisks2-volume-monitor
root      1088 0.0 0.7 395776 15096 ? Ssl 01:27 0:00 /usr/libexec/udisks2/udisksd
kali      1113 0.0 0.4 313532 10100 ? Ssl 01:27 0:00 /usr/libexec/gvfs-afc-volume-monitor
kali      1118 0.0 0.4 234468 8616 ? Ssl 01:27 0:00 /usr/libexec/gvfs-mtp-volume-monitor
kali      1126 0.0 0.4 235424 9240 ? Ssl 01:27 0:00 /usr/libexec/gvfs-gphoto2-volume-monitor
kali      1130 0.0 0.4 234648 8568 ? Ssl 01:27 0:00 /usr/libexec/gvfs-goa-volume-monitor
kali      1138 0.0 0.6 312784 12276 ? Sl 01:27 0:00 /usr/libexec/gvfsd-trash --spawner :1.17 /
kali      1147 0.0 0.4 161060 8704 ? Ssl 01:27 0:00 /usr/libexec/gvfsd-metadata
kali      1167 0.0 0.3 48024 7008 ? Ss 01:27 0:00 /usr/libexec/bluetooth/obexd
kali      1454 0.5 5.1 434264 104860 ? Rl 01:28 0:14 /usr/bin/qterminal
kali      1461 0.2 0.3 10760 6612 pts/0 Ss 01:28 0:08 /usr/bin/zsh
root      6558 0.0 0.0 0 0 ? I 01:48 0:01 [kworker/0:2-events]
root      6564 0.0 0.0 0 0 ? I 01:48 0:01 [kworker/1:2-events]
root      7100 0.0 0.0 0 0 ? I 01:50 0:00 [kworker/u4:2-flush-8:0]
root      11440 0.0 0.0 0 0 ? I 02:07 0:00 [kworker/u4:1+events_unbound]
kali      11547 0.4 2.9 478324 60308 ? Sl 02:07 0:01 mousepad /home/kali/Desktop/my_directory/m
root      11921 0.0 0.0 0 0 ? I 02:09 0:00 [kworker/1:3-ata_sff]
root      13134 0.0 0.0 0 0 ? I 02:14 0:00 [kworker/1:0-ata_sff]

```

- Use the "grep" command to filter the processes list and display only the processes with "bash" in their name.

```
(kali㉿kali)-[~/Desktop/my_directory]
$ ps aux | grep bash

kali          13682  0.0  0.1  6300  2172 pts/0    R+   02:16   0:00 grep --color=auto bash
```

- Use the "wc" command to count the number of lines in the filtered output.

```
(kali㉿kali)-[~/Desktop/my_directory]
$ ps aux | grep bash | wc -l

1
```