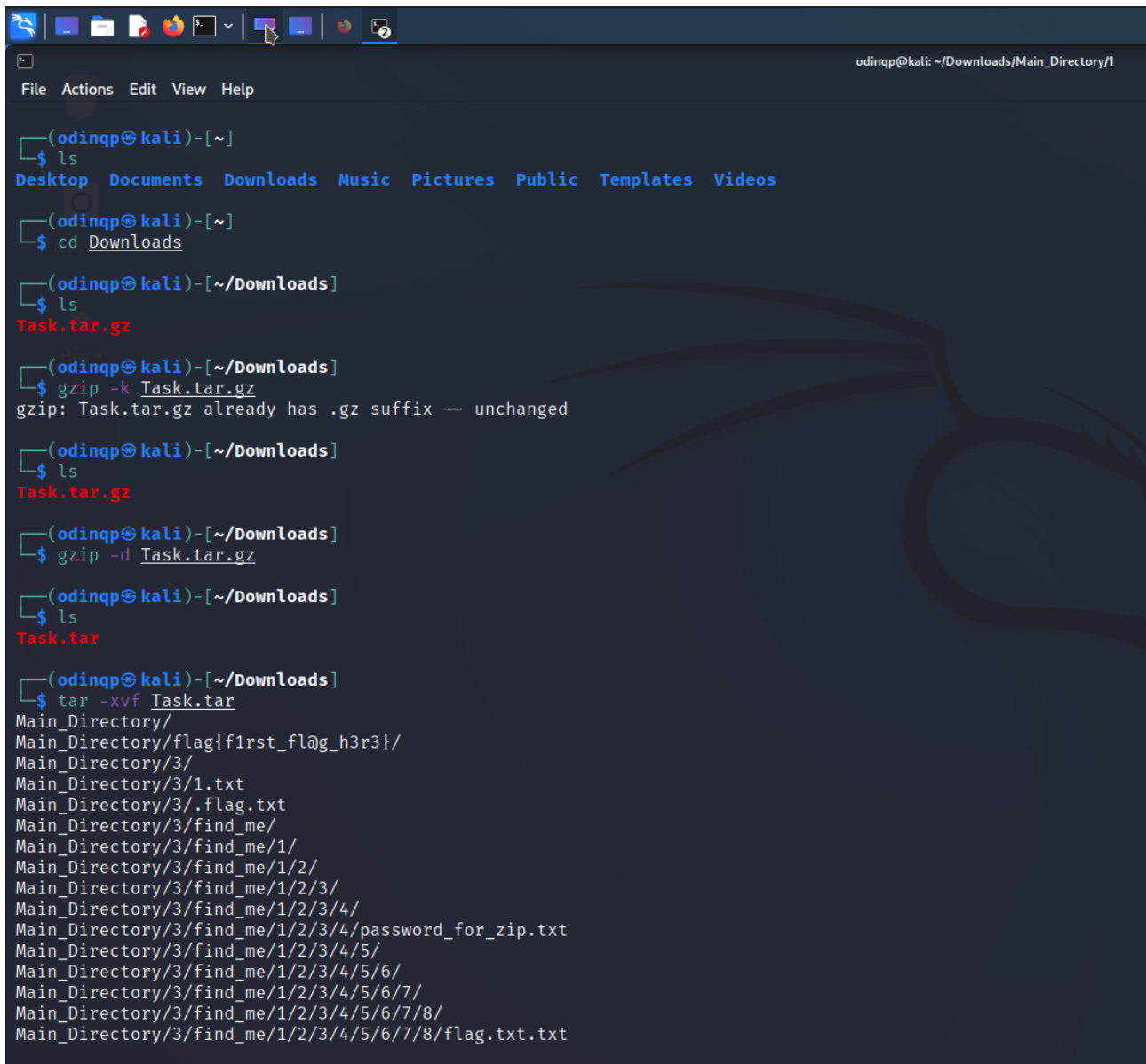


Task-5 _ Cybersecurity domain. Part-1

A terminal window on a Kali Linux system. The window title is 'odinqp@kali: ~/Downloads/Main_Directory/1'. The terminal shows a series of commands and their outputs. The user starts in the home directory, lists files, moves to the Downloads directory, lists files again, and then performs a series of file operations including gzip compression, listing, gzip decompression, and tar extraction. The final output shows a directory tree structure.

```
(odinqp@kali)-[~]
$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos

(odinqp@kali)-[~]
$ cd Downloads

(odinqp@kali)-[~/Downloads]
$ ls
Task.tar.gz

(odinqp@kali)-[~/Downloads]
$ gzip -k Task.tar.gz
gzip: Task.tar.gz already has .gz suffix -- unchanged

(odinqp@kali)-[~/Downloads]
$ ls
Task.tar.gz

(odinqp@kali)-[~/Downloads]
$ gzip -d Task.tar.gz

(odinqp@kali)-[~/Downloads]
$ ls
Task.tar

(odinqp@kali)-[~/Downloads]
$ tar -xvf Task.tar
Main_Directory/
Main_Directory/flag{f1rst_fl@g_h3r3}/
Main_Directory/3/
Main_Directory/3/1.txt
Main_Directory/3/.flag.txt
Main_Directory/3/find_me/
Main_Directory/3/find_me/1/
Main_Directory/3/find_me/1/2/
Main_Directory/3/find_me/1/2/3/
Main_Directory/3/find_me/1/2/3/4/
Main_Directory/3/find_me/1/2/3/4/password_for_zip.txt
Main_Directory/3/find_me/1/2/3/4/5/
Main_Directory/3/find_me/1/2/3/4/5/6/
Main_Directory/3/find_me/1/2/3/4/5/6/7/
Main_Directory/3/find_me/1/2/3/4/5/6/7/8/
Main_Directory/3/find_me/1/2/3/4/5/6/7/8/flag.txt.txt
```

```
(odinqp@kali)-[~/Downloads/Main_Directory]
$ tree -a
.
├── 1
│   ├── .flag{Y0u_f0und_th3_hidd3n_dir!}
│   ├── zipped_flag
│   │   └── zipped_flag.txt
│   └── zipped_flag.zip
├── 3
│   ├── 1.txt
│   ├── 2.txt
│   ├── find_me
│   │   ├── 1
│   │   │   ├── 2
│   │   │   │   ├── 3
│   │   │   │   │   ├── 4
│   │   │   │   │   │   ├── 5
│   │   │   │   │   │   │   ├── 6
│   │   │   │   │   │   │   │   ├── 7
│   │   │   │   │   │   │   │   │   ├── 8
│   │   │   │   │   │   │   │   │   └── flag.txt.txt
│   │   │   │   │   │   └── password_for_zip.txt
│   └── .flag.txt
├── 4
│   ├── 1.txt
│   ├── 2.txt
│   ├── 3.txt
│   ├── 4.txt
│   ├── 5.txt
│   └── .image.png
├── 5
│   ├── .compare_me1.txt
│   ├── .compare_me2.txt
│   ├── execute_me.sh
│   └── reverse_me.txt
└── flag{f1rst_fl@g_h3r3}
```

16 directories, 17 files

Found 2 flags,

flag{Y0u_f0und_th3_hidd3n_dir!}

flag{f1rst_fl@g_h3r3}

```
File Actions Edit View Help
Main_Directory/5/.compare_me2.txt
Main_Directory/5/.compare_me1.txt
Main_Directory/1/
Main_Directory/1/.flag{Y0u_f0und_th3_hidd3n_dir!}/
Main_Directory/1/zipped_flag.zip

(odinqp@kali)-[~/Downloads]
$ ls
Main_Directory Task.tar

(odinqp@kali)-[~/Downloads]
$ cd Main_Directory

(odinqp@kali)-[~/Downloads/Main_Directory]
$ ls
1 3 4 5 flag{f1rst_fl@g_h3r3}

(odinqp@kali)-[~/Downloads/Main_Directory]
$ file *
1: directory
3: directory
4: directory
5: directory
flag{f1rst_fl@g_h3r3}: directory

(odinqp@kali)-[~/Downloads/Main_Directory]
$ cd 1

(odinqp@kali)-[~/Downloads/Main_Directory/1]
$ ls
zipped_flag.zip

(odinqp@kali)-[~/Downloads/Main_Directory/1]
$ man zip

(odinqp@kali)-[~/Downloads/Main_Directory/1]
$ unzip zipped_flag.zip
Archive: zipped_flag.zip
creating: zipped_flag/
[zipped_flag.zip] zipped_flag/zipped_flag.txt password:
password incorrect--reenter:
skipping: zipped_flag/zipped_flag.txt incorrect password

(odinqp@kali)-[~/Downloads/Main_Directory/1]
$
```

```
odinqp@kali: ~/Downloads/Main_Directory/5
File Actions Edit View Help
(odinqp@kali)-[~/Downloads/Main_Directory]
$ cd 1
(odinqp@kali)-[~/Downloads/Main_Directory/1]
$ unzip zipped_flag.zip
Archive:  zipped_flag.zip
[zipped_flag.zip] zipped_flag/zipped_flag.txt password:
extracting: zipped_flag/zipped_flag.txt
(odinqp@kali)-[~/Downloads/Main_Directory/1]
$ ls
zipped_flag  zipped_flag.zip
(odinqp@kali)-[~/Downloads/Main_Directory/1]
$ cd zipped_flag
(odinqp@kali)-[~/Downloads/Main_Directory/1/zipped_flag]
$ ls
zipped_flag.txt
(odinqp@kali)-[~/Downloads/Main_Directory/1/zipped_flag]
$ cat zipped_flag.txt
flag{e@5y_p@ssw0rd!}
(odinqp@kali)-[~/Downloads/Main_Directory/1/zipped_flag]
$ cd ..
(odinqp@kali)-[~/Downloads/Main_Directory/1]
$ cd ..
(odinqp@kali)-[~/Downloads/Main_Directory]
$ ls
1 3 4 5 flag{f1rst_flg_h3r3}
(odinqp@kali)-[~/Downloads/Main_Directory]
$ cd 4
(odinqp@kali)-[~/Downloads/Main_Directory/4]
$ ls
1.txt 2.txt 3.txt 4.txt 5.txt
(odinqp@kali)-[~/Downloads/Main_Directory/4]
$ cat 1.txt
```

Found one flag in 1 directory,

flag{e@5y_p@ssw0rd!}

-- “zip_file_huh?” zip file password

```
odinqp@kali: ~/Downloads/Main_Directory/3
File Actions Edit View Help

(odinqp@kali)-[~/Downloads/Main_Directory/3]
$ cat 2.txt
No Flag here

(odinqp@kali)-[~/Downloads/Main_Directory/3]
$ cd find_me/1/2/3/4/5/6/7/8

(odinqp@kali)-[~/.../5/6/7/8]
$ ls -a
.  ..  flag.txt.txt

(odinqp@kali)-[~/.../5/6/7/8]
$ cat flag.txt.txt
flag{Y0u_f0und_m3!}

(odinqp@kali)-[~/.../5/6/7/8]
$

(odinqp@kali)-[~/.../5/6/7/8]
$ cd ..

(odinqp@kali)-[~/.../4/5/6/7]
$ cd ..

(odinqp@kali)-[~/.../3/4/5/6]
$ cd ..

(odinqp@kali)-[~/.../2/3/4/5]
$ cd ..

(odinqp@kali)-[~/.../1/2/3/4]
$ ls
5 password_for_zip.txt

(odinqp@kali)-[~/.../1/2/3/4]
$ cat password_for_zip.txt
zip_file_huh?

(odinqp@kali)-[~/.../1/2/3/4]
$ cd ..

(odinqp@kali)-[~/.../find_me/1/2/3]
$ cd ..
```

Found one flag and password for zip file that is in directory 1.

flag{Y0u_f0und_m3!}

and password is zip_file_huh?

```

(odinqp@kali)-[~/Downloads/Main_Directory/4]
$ cat 2.txt

(odinqp@kali)-[~/Downloads/Main_Directory/4]
$ cat 3.txt

(odinqp@kali)-[~/Downloads/Main_Directory/4]
$ cat 4.txt
flag{m3ow_m3ow_cat!}

(odinqp@kali)-[~/Downloads/Main_Directory/4]
$ cat 5.txt

(odinqp@kali)-[~/Downloads/Main_Directory/4]
$ ls -a
.  ..  1.txt  2.txt  3.txt  4.txt  5.txt  .image.png

(odinqp@kali)-[~/Downloads/Main_Directory/4]
$ cat .image.png
flag{t3xt_15_n0t_h1dd3n!}

(odinqp@kali)-[~/Downloads/Main_Directory/4]
$

(odinqp@kali)-[~/Downloads/Main_Directory/4]
$ cd ..

(odinqp@kali)-[~/Downloads/Main_Directory]
$ ls
1  3  4  5  flag{f1rst_fl@g_h3r3}

(odinqp@kali)-[~/Downloads/Main_Directory]
$ cd 5

(odinqp@kali)-[~/Downloads/Main_Directory/5]
$ ls
execute_me.sh  reverse_me.txt

(odinqp@kali)-[~/Downloads/Main_Directory/5]
$

```

```

(odinqp@kali)-[~/Downloads/Main_Directory/5]
$ ls
execute_me.sh  reverse_me.txt

(odinqp@kali)-[~/Downloads/Main_Directory/5]
$ ./execute_me.sh
flag{3x3cut10n_d0n3!}

```

Found two flags in directory 4.
 flag{t3xt_15_n0t_h1dd3n!}
 flag{m3ow_m3ow_cat!}

Found a flag as a executable in directory 5.
 flag{3x3cut10n_d0n3!}

```
(odinqp@kali)-[~/Downloads/Main_Directory/5]
$ tac reverse_me.txt
f
l
Devices
a
g
File System
{
network
t
Browse Network
@
c
-
1
5
-
f
u
n
!
}
```

```
(odinqp@kali)-[~/Downloads/Main_Directory/5]
$ ls -la
.  ..  .compare_me1.txt  .compare_me2.txt  execute_me.sh  reverse_me.txt
```

another flag in directory 5.

[flag{t@c_15_fun!}](#)

and use diff to find another flag.

[flag{d1ff_15_u53ful!}](#)

```

(odinqp@kali)-[~/Downloads/Main_Directory/5]
$ diff -w .compare_me1.txt .compare_me2.txt
83c83
< f
___ File System
> z
173c173
< l
___
> z Home
340c340
< a
___
> z
431c431
< g
___
> z
585c585
< {
___
> z
601d600
< d
665c664,665
< 1
___
> z
> z
769c769
< f
___
> z
876c876
< f
___
> z
938c938
< _
___
> z
1398a1399
> z
1403d1403
< 1

```

flag{d1ff_15_u53ful!}

```

odinqp@kali: ~/Downloads/Main_Directory/3
odinqp@kali: ~/Downloads/Main_Directory/3
odinqp@kali)-[~/Downloads/Main_Directory/3]
$ tree -a
.
├── 1.txt
├── 2.txt
├── find_me
│   ├── 1
│   │   ├── 2
│   │   │   ├── 3
│   │   │   │   ├── 4
│   │   │   │   │   ├── 5
│   │   │   │   │   │   ├── 6
│   │   │   │   │   │   │   ├── 7
│   │   │   │   │   │   │   │   ├── 8
│   │   │   │   │   │   │   │   │   ├── flag.txt.txt
│   │   │   │   │   │   │   │   │   └── password_for_zip.txt
├── .flag.txt
└── 9 directories, 5 files

(odinqp@kali)-[~/Downloads/Main_Directory/3]
$ cat 1.txt | grep flag
wngdlipephgylfuexfriazan enplcuyhdgrazq flag{gr3p_finds_flags!} edzqpgtzovjlsscuypdzlycte yxvllxajmimxogfiduzrmu qdpqjzdxegymzlwspeliz gokobhcpeusa yfnueguqugdjgl cqnrxsidxbdvuliwtbschhkgjtiqqxvfd vxkwqnb
zd0lqtjbgmqnbcidewovszllrkbecwtl

(odinqp@kali)-[~/Downloads/Main_Directory/3]
$

```



```
(odinqp@kali)-[~/Downloads/Main_Directory/3]
$ ls -a
.  ..  1.txt  2.txt  find_me  .flag.txt

(odinqp@kali)-[~/Downloads/Main_Directory/3]
$ cat .flag.txt
flag{h1dden_fil3!}
```

Found 2 other flags in directory 3

flag{h1dden_fil3!}

flag{gr3p_f1nds_fl@g3!}

Part-2

Write a bash script to echo your name 25 times

```
$ prog1.sh
shell > $ prog1.sh
1  #! /usr/bin/bash
2
3  for i in {1..25}
4  do
5      echo Pranav
6  done
7
8
```

Output:

[illegible]

What command should I use to display the first 30 entries of syslog file?

Input:

head -n 30 var/log/syslog

```
(root@kali) ~/Documents
# head -n 30 /var/log/syslog
Feb 27 00:48:22 kali systemd[1]: rsyslog.service: Sent signal SIGHUP to main process 404 (rsyslogd) on client request.
Feb 27 00:48:22 kali systemd[1]: logrotate.service: Deactivated successfully.
Feb 27 00:48:22 kali systemd[1]: Finished Rotate log files.
Feb 27 00:48:22 kali lightdm[633]: Error getting user list from org.freedesktop.Accounts: GDBus.Error:org.freedesktop.DBus.Error.ServiceUnknown: The name org.freedesktop.Accounts was not provided by any .service files
Feb 27 00:48:22 kali systemd[1]: Created slice User Slice of UID 132.
Feb 27 00:48:22 kali systemd[1]: Starting User Runtime Directory /run/user/132...
Feb 27 00:48:22 kali systemd[1]: Finished User Runtime Directory /run/user/132.
Feb 27 00:48:22 kali systemd[1]: Starting User Manager for UID 132...
Feb 27 00:48:22 kali systemd[637]: Queued start job for default target Main User Target.
Feb 27 00:48:22 kali systemd[637]: Created slice User Application Slice.
Feb 27 00:48:22 kali systemd[637]: Created slice User Core Session Slice.
Feb 27 00:48:22 kali systemd[637]: Reached target Paths.
Feb 27 00:48:22 kali systemd[637]: Reached target Timers.
Feb 27 00:48:22 kali systemd[637]: Starting D-Bus User Message Bus Socket...
Feb 27 00:48:22 kali systemd[637]: Listening on GnuPG network certificate management daemon.
Feb 27 00:48:22 kali systemd[637]: Listening on GnuPG cryptographic agent and passphrase cache (access for web browsers).
Feb 27 00:48:22 kali systemd[637]: Listening on GnuPG cryptographic agent and passphrase cache (restricted).
Feb 27 00:48:22 kali systemd[637]: Listening on GnuPG cryptographic agent (ssh-agent emulation).
Feb 27 00:48:22 kali systemd[637]: Listening on GnuPG cryptographic agent and passphrase cache.
Feb 27 00:48:22 kali systemd[637]: Listening on PipeWire Multimedia System Socket.
Feb 27 00:48:22 kali systemd[637]: Listening on Sound System.
Feb 27 00:48:22 kali systemd[637]: Listening on D-Bus User Message Bus Socket.
Feb 27 00:48:22 kali systemd[637]: Reached target Sockets.
Feb 27 00:48:22 kali systemd[637]: Reached target Basic System.
Feb 27 00:48:22 kali systemd[1]: Started User Manager for UID 132.
Feb 27 00:48:22 kali systemd[1]: Started Session c1 of User lightdm.
Feb 27 00:48:22 kali systemd[637]: Started PipeWire Multimedia Service.
Feb 27 00:48:22 kali systemd[637]: Started PipeWire Media Session Manager.
Feb 27 00:48:22 kali systemd[637]: Starting Sound Service...
Feb 27 00:48:23 kali dbus-daemon[396]: [system] Activating via systemd: service name='org.freedesktop.RealtimeKit1' unit='rtkit-daemon.service' requested by '1:15' (uid=132 pid=653 comm="/usr/bin/pipewire-media-session ")
(root@kali) ~/Documents
```

What command should I use to display the last 30 entries of syslog file?

Tail -n 30 var/log/syslog

```
(root@kali)-[~/Documents]
# tail -n 30 /var/log/syslog
Feb 27 01:02:48 kali hide.me[2431]: Main: [ERR] No Access-Token available
Feb 27 01:02:48 kali systemd[1]: hide.me@usa.service: Failed with result 'protocol'.
Feb 27 01:02:48 kali systemd[1]: Failed to start Hide.me CLI connection to usa.
Feb 27 01:02:53 kali systemd[1]: hide.me@usa.service: Scheduled restart job, restart counter is at 165.
Feb 27 01:02:53 kali systemd[1]: Stopped Hide.me CLI connection to usa.
Feb 27 01:02:53 kali systemd[1]: Starting Hide.me CLI connection to usa...
Feb 27 01:02:53 kali hide.me[2438]: Main: [ERR] No Access-Token available
Feb 27 01:02:53 kali systemd[1]: hide.me@usa.service: Failed with result 'protocol'.
Feb 27 01:02:53 kali systemd[1]: Failed to start Hide.me CLI connection to usa.
Feb 27 01:02:58 kali systemd[1]: hide.me@usa.service: Scheduled restart job, restart counter is at 166.
Feb 27 01:02:58 kali systemd[1]: Stopped Hide.me CLI connection to usa.
Feb 27 01:02:58 kali systemd[1]: Starting Hide.me CLI connection to usa...
Feb 27 01:02:58 kali hide.me[2445]: Main: [ERR] No Access-Token available
Feb 27 01:02:58 kali systemd[1]: hide.me@usa.service: Failed with result 'protocol'.
Feb 27 01:02:58 kali systemd[1]: Failed to start Hide.me CLI connection to usa.
Feb 27 01:03:03 kali systemd[1]: hide.me@usa.service: Scheduled restart job, restart counter is at 167.
Feb 27 01:03:03 kali systemd[1]: Stopped Hide.me CLI connection to usa.
Feb 27 01:03:03 kali systemd[1]: Starting Hide.me CLI connection to usa...
Feb 27 01:03:03 kali hide.me[2452]: Main: [ERR] No Access-Token available
Feb 27 01:03:03 kali systemd[1]: hide.me@usa.service: Failed with result 'protocol'.
Feb 27 01:03:03 kali systemd[1]: Failed to start Hide.me CLI connection to usa.
Feb 27 01:03:08 kali systemd[1]: Starting Cleanup of Temporary Directories...
Feb 27 01:03:08 kali systemd[1]: systemd-tmpfiles-clean.service: Deactivated successfully.
Feb 27 01:03:08 kali systemd[1]: Finished Cleanup of Temporary Directories.
Feb 27 01:03:09 kali systemd[1]: hide.me@usa.service: Scheduled restart job, restart counter is at 168.
Feb 27 01:03:09 kali systemd[1]: Stopped Hide.me CLI connection to usa.
Feb 27 01:03:09 kali systemd[1]: Starting Hide.me CLI connection to usa...
Feb 27 01:03:09 kali hide.me[2460]: Main: [ERR] No Access-Token available
Feb 27 01:03:09 kali systemd[1]: hide.me@usa.service: Failed with result 'protocol'.
Feb 27 01:03:09 kali systemd[1]: Failed to start Hide.me CLI connection to usa.
```

What command should I use to arrange the entries of a file:

Alphabetically

sort filename

Reverse order

sort -r filename

Numerical order

sort -n filename

Copee is a hard-working cop. He found a case and almost at the verge of cracking it. It could be his best breakthrough. He has the list of criminals but lots of duplicates are there. He needs to find the only one that is different . He sought your help. How will you sort this issue?

```
(root@kali)~/Documents
# cat >> text.txt
pranav
jack
pranav
^C
File System
(root@kali)~/Documents
# cat text.txt
pranav
jack
pranav
ome
(root@kali)~/Documents
# sort text.txt | uniq -u
jack
Firefox ESR
(root@kali)~/Documents
#
```

sort filename | uniq -u

What are the Three parts of file's permission?

Read(4)(-r)

write(2)(-w)

execute(1)(-x)

Done by

Pranav A N [ch.en.u4cys21056]