

## LINUX Assignment

Student Name: MUHIRE BLANDE

Student ID:26295

---

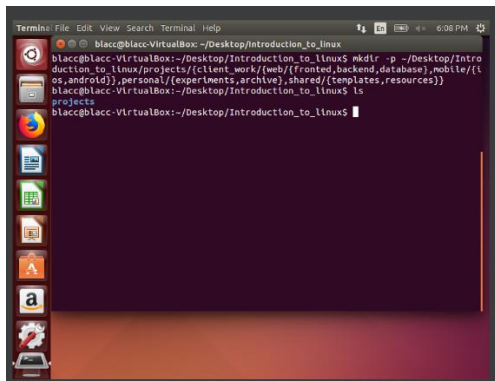
### Q1.

- **/etc** → contains system **configuration files** (e.g., /etc/passwd, /etc/shadow, /etc/ssh/sshd\_config). Attackers often target these.
  - **/bin** → contains **essential binaries** (ls, cp, bash). Could be replaced with trojans.
  - **/var** → contains **log files** (/var/log/auth.log, /var/log/syslog). Evidence of intrusions is here.
  - **/usr** → non-essential binaries, libraries, documentation. Attackers might modify installed apps.
  - **/tmp** → temporary storage, often abused for malicious scripts or uploads.
  - **/opt** → optional software location, less critical but still modifiable.
  - **/boot** → kernel and bootloader, rootkits may persist here.
  - **/home** → user files and hidden configs, SSH keys could be planted.
- 

### Q2.

mkdir -p

~Desktop/introduction\_to\_linux/projects/{client\_work/{web/{frontend,backend,database},mobile/{ios,android}},personal/{experiments,archive},shared/{templates,resources}}



---

### Q3. Navigation (relative paths, ≤3 cd)

*# Starting point*

```
pwd
/home/user/projects/client_work/web/frontend
```

*# Go to ~/projects/personal/experiments*

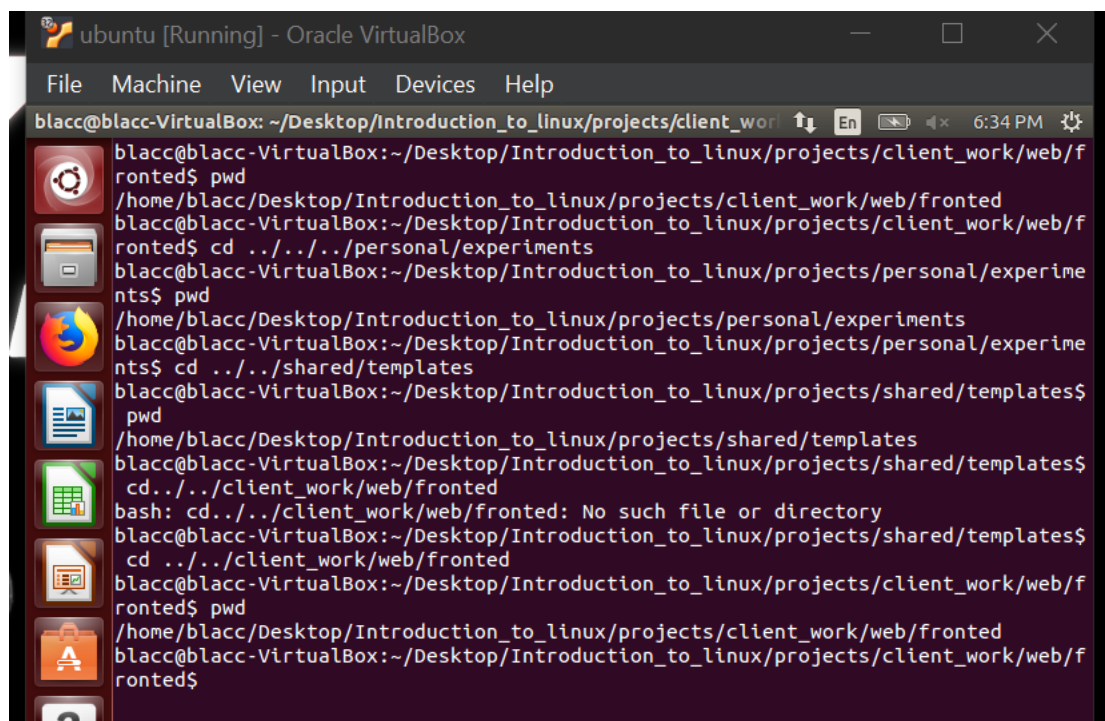
```
cd ../../../../personal/experiments
pwd
/home/user/projects/personal/experiments
```

*# Go to ~/projects/shared/templates*

```
cd ../../shared/templates
pwd
/home/user/projects/shared/templates
```

*# Return to original location*

```
cd ../../client_work/web/frontend
pwd
/home/user/projects/client_work/web/frontend
```



---

### Q4. Web project structure

*# HTML files*

```
touch index.html about.html contact.html page_{001..012}.html
```

```

blacc@blacc-VirtualBox:~/Desktop/Introduction_to_linux/projects/client_work/web/f
ronted$ touch index.html about.html contact.html page_{001..012}.html
blacc@blacc-VirtualBox:~/Desktop/Introduction_to_linux/projects/client_work/web/f
ronted$ ls -l
total 0
-rw-rw-r-- 1 blacc blacc 0 Sep 30 18:39 about.html
-rw-rw-r-- 1 blacc blacc 0 Sep 30 18:39 contact.html
-rw-rw-r-- 1 blacc blacc 0 Sep 30 18:39 index.html
-rw-rw-r-- 1 blacc blacc 0 Sep 30 18:39 page_001.html
-rw-rw-r-- 1 blacc blacc 0 Sep 30 18:39 page_002.html
-rw-rw-r-- 1 blacc blacc 0 Sep 30 18:39 page_003.html
-rw-rw-r-- 1 blacc blacc 0 Sep 30 18:39 page_004.html
-rw-rw-r-- 1 blacc blacc 0 Sep 30 18:39 page_005.html
-rw-rw-r-- 1 blacc blacc 0 Sep 30 18:39 page_006.html
-rw-rw-r-- 1 blacc blacc 0 Sep 30 18:39 page_007.html
-rw-rw-r-- 1 blacc blacc 0 Sep 30 18:39 page_008.html
-rw-rw-r-- 1 blacc blacc 0 Sep 30 18:39 page_009.html
-rw-rw-r-- 1 blacc blacc 0 Sep 30 18:39 page_010.html
-rw-rw-r-- 1 blacc blacc 0 Sep 30 18:39 page_011.html
-rw-rw-r-- 1 blacc blacc 0 Sep 30 18:39 page_012.html
blacc@blacc-VirtualBox:~/Desktop/Introduction_to_linux/projects/client_work/web/f
ronted$

```

### # CSS files

touch main.css reset.css theme\_{light,dark}.css mobile.css tablet.css  
desktop.css print.css

```

blacc@blacc-VirtualBox: ~/Desktop/Introduction_to_linux/projects/client_work
blacc@blacc-VirtualBox:~/Desktop/Introduction_to_linux/projects/client_work/web/f
ronted$ ls -l *.css
-rw-rw-r-- 1 blacc blacc 0 Sep 30 18:43 desktop.css
-rw-rw-r-- 1 blacc blacc 0 Sep 30 18:43 main.css
-rw-rw-r-- 1 blacc blacc 0 Sep 30 18:43 mobile.css
-rw-rw-r-- 1 blacc blacc 0 Sep 30 18:43 print.css
-rw-rw-r-- 1 blacc blacc 0 Sep 30 18:43 reset.css
-rw-rw-r-- 1 blacc blacc 0 Sep 30 18:43 tablet.css
-rw-rw-r-- 1 blacc blacc 0 Sep 30 18:43 theme_dark.css
-rw-rw-r-- 1 blacc blacc 0 Sep 30 18:43 theme_light.css
blacc@blacc-VirtualBox:~/Desktop/Introduction_to_linux/projects/client_work/web/f
ronted$

```

### # JavaScript files

touch script.js util.js config.js helper\_script.js test\_util.js app\_config.js

```

blacc@blacc-VirtualBox:~/Desktop/Introduction_to_linux/projects/client_work/web/f
ronted$ touch {Script,util,config,helper_script,test_util,app_config}.js
blacc@blacc-VirtualBox:~/Desktop/Introduction_to_linux/projects/client_work/web/f
ronted$ ls -l *.js
-rw-rw-r-- 1 blacc blacc 0 Sep 30 18:51 app_config.js
-rw-rw-r-- 1 blacc blacc 0 Sep 30 18:51 config.js
-rw-rw-r-- 1 blacc blacc 0 Sep 30 18:51 helper_script.js
-rw-rw-r-- 1 blacc blacc 0 Sep 30 18:51 Script.js
-rw-rw-r-- 1 blacc blacc 0 Sep 30 18:51 test_util.js
-rw-rw-r-- 1 blacc blacc 0 Sep 30 18:51 util.js
blacc@blacc-VirtualBox:~/Desktop/Introduction_to_linux/projects/client_work/web/f
ronted$

```

### # Backup files (20 total, 5 per Letter a-d)

touch {a,b,c,d}{1..5}.bak

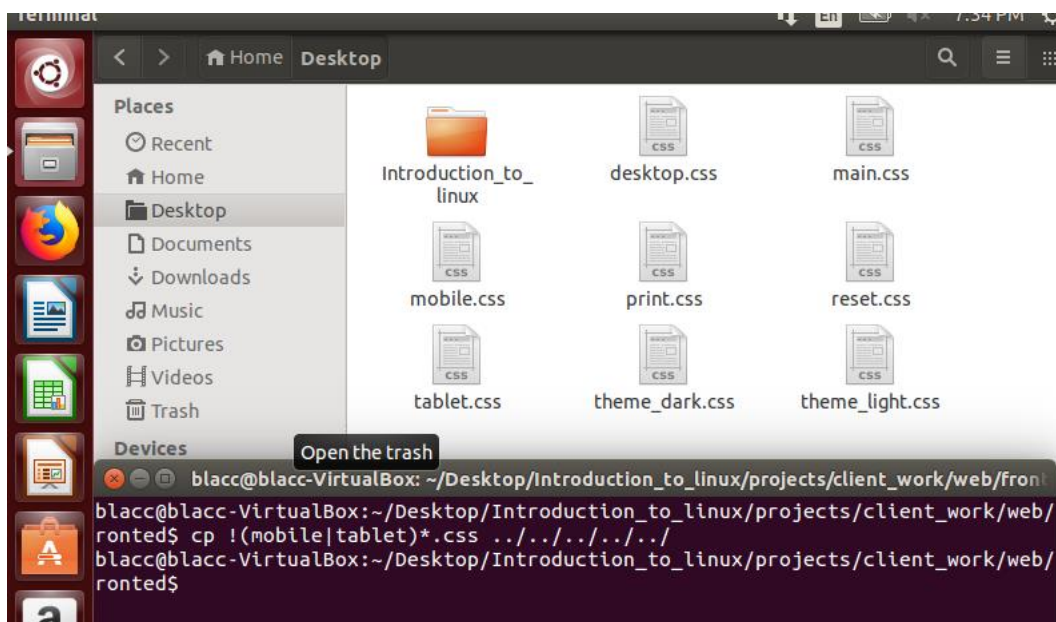
```
blacc@blacc-VirtualBox: ~/Desktop/Introduction_to_linux/projects/client_work/web/f
ronted$ touch {a,b,c,d}{1..5}.{bak,backup,bkp,old,save}
blacc@blacc-VirtualBox:~/Desktop/Introduction_to_linux/projects/client_work/web/f
ronted$ ls -l *.bak,*.backup,*.bkp,*.old,*.save
-rw-rw-r-- 1 blacc blacc 0 Sep 30 19:20 a1.backup
-rw-rw-r-- 1 blacc blacc 0 Sep 30 19:20 a1.bak
-rw-rw-r-- 1 blacc blacc 0 Sep 30 19:20 a1.bkp
-rw-rw-r-- 1 blacc blacc 0 Sep 30 19:20 a1.old
-rw-rw-r-- 1 blacc blacc 0 Sep 30 19:20 a1.save
-rw-rw-r-- 1 blacc blacc 0 Sep 30 19:20 a2.backup
-rw-rw-r-- 1 blacc blacc 0 Sep 30 19:20 a2.bak
-rw-rw-r-- 1 blacc blacc 0 Sep 30 19:20 a2.bkp
-rw-rw-r-- 1 blacc blacc 0 Sep 30 19:20 a2.old
-rw-rw-r-- 1 blacc blacc 0 Sep 30 19:20 a2.save
-rw-rw-r-- 1 blacc blacc 0 Sep 30 19:20 a3.backup
-rw-rw-r-- 1 blacc blacc 0 Sep 30 19:20 a3.bak
-rw-rw-r-- 1 blacc blacc 0 Sep 30 19:20 a3.bkp
-rw-rw-r-- 1 blacc blacc 0 Sep 30 19:20 a3.old
-rw-rw-r-- 1 blacc blacc 0 Sep 30 19:20 a3.save
-rw-rw-r-- 1 blacc blacc 0 Sep 30 19:20 a4.backup
-rw-rw-r-- 1 blacc blacc 0 Sep 30 19:20 a4.bak
-rw-rw-r-- 1 blacc blacc 0 Sep 30 19:20 a4.bkp
-rw-rw-r-- 1 blacc blacc 0 Sep 30 19:20 a4.old
-rw-rw-r-- 1 blacc blacc 0 Sep 30 19:20 a4.save
-rw-rw-r-- 1 blacc blacc 0 Sep 30 19:20 a5.backup
-rw-rw-r-- 1 blacc blacc 0 Sep 30 19:20 a5.bak
-rw-rw-r-- 1 blacc blacc 0 Sep 30 19:20 a5.bkp
-rw-rw-r-- 1 blacc blacc 0 Sep 30 19:20 a5.old
-rw-rw-r-- 1 blacc blacc 0 Sep 30 19:20 a5.save
-rw-rw-r-- 1 blacc blacc 0 Sep 30 19:20 b1.backup
```

## Q5. Wildcards practice

`mv *[0-9].* ../../../../personal/archive/`

```
blacc@blacc-VirtualBox:~/Desktop/Introduction_to_linux/projects/client_work/web/f
ronted$ mv *[0-9].* ../../../../personal/archive/
blacc@blacc-VirtualBox:~/Desktop/Introduction_to_linux/projects/client_work/web/f
ronted$
```

`cp !(mobile|tablet)*.css ../../../../../../../`



```
blacc@blacc-VirtualBox: ~/Desktop/Introduction_to_linux/projects/client_work/web/f
ronted$ cp !(mobile|tablet)*.css ../../../../../../../
blacc@blacc-VirtualBox:~/Desktop/Introduction_to_linux/projects/client_work/web/
ronted$
```

`ls ????.*`

```

blacc@blacc-VirtualBox: ~/Desktop/Introduction_to_linux/projects/client_work/web/
fronted$ ls ??? .*
ls: cannot access ??? : No such file or directory
.:
about.html      desktop.css      mobile.css       tablet.css       util.js
app_config.js   helper_script.js print.css        test_util.js
config.js       index.html       reset.css        theme_dark.css
contact.html    main.css         Script.js        theme_light.css

..:
backend database fronted
blacc@blacc-VirtualBox: ~/Desktop/Introduction_to_linux/projects/client_work/web/
fronted$

```

`ls [b-df-hj-np-tv-z]*`

```

blacc@blacc-VirtualBox: ~/Desktop/Introduction_to_linux/projects/client_work/web/
fronted$ ls [b-df-hj-np-tv-z]*
config.js      helper_script.js print.css       tablet.css      theme_light.css
contact.html   main.css         reset.css       test_util.js
desktop.css    mobile.css       Script.js       theme_dark.css
blacc@blacc-VirtualBox: ~/Desktop/Introduction_to_linux/projects/client_work/web/
fronted$

```

`ls *.*[a-zA-Z][a-zA-Z]`

```

blacc@blacc-VirtualBox: ~/Desktop/Introduction_to_linux/projects/client_work/web/
fronted$ ls *.*[a-zA-Z][a-zA-Z]
app_config.js config.js helper_script.js Script.js test_util.js util.js
blacc@blacc-VirtualBox: ~/Desktop/Introduction_to_linux/projects/client_work/web/
fronted$

```

## Q6. Brace expansion

`touch log_2024-{01..03}-{01..31}.txt`

```

blacc@blacc-VirtualBox: ~/Desktop/Introduction_to_linux/projects/client_work/web/
fronted$ touch log_2024-{01..03}-{01..31}.txt
blacc@blacc-VirtualBox: ~/Desktop/Introduction_to_linux/projects/client_work/web/
fronted$ ls l *.txt
ls: cannot access l: No such file or directory
log_2024-01-01.txt log_2024-01-25.txt log_2024-02-18.txt log_2024-03-11.txt
log_2024-01-02.txt log_2024-01-26.txt log_2024-02-19.txt log_2024-03-12.txt
log_2024-01-03.txt log_2024-01-27.txt log_2024-02-20.txt log_2024-03-13.txt
log_2024-01-04.txt log_2024-01-28.txt log_2024-02-21.txt log_2024-03-14.txt
log_2024-01-05.txt log_2024-01-29.txt log_2024-02-22.txt log_2024-03-15.txt
log_2024-01-06.txt log_2024-01-30.txt log_2024-02-23.txt log_2024-03-16.txt

```

`touch {web,api,db}_{dev,staging,prod}.conf`



```

blacc@blacc-VirtualBox:~/Desktop/Introduction_to_linux/projects/client_work/web/
fronted$ touch {web,api,db}_{dev,staging,prod}.conf
blacc@blacc-VirtualBox:~/Desktop/Introduction_to_linux/projects/client_work/web/
fronted$ ls -l *.conf
-rw-rw-r-- 1 blacc blacc 0 Oct  1 06:36 api_dev.conf
-rw-rw-r-- 1 blacc blacc 0 Oct  1 06:36 api_prod.conf
-rw-rw-r-- 1 blacc blacc 0 Oct  1 06:36 api_staging.conf
-rw-rw-r-- 1 blacc blacc 0 Oct  1 06:36 db_dev.conf
-rw-rw-r-- 1 blacc blacc 0 Oct  1 06:36 db_prod.conf
-rw-rw-r-- 1 blacc blacc 0 Oct  1 06:36 db_staging.conf
-rw-rw-r-- 1 blacc blacc 0 Oct  1 06:36 web_dev.conf
-rw-rw-r-- 1 blacc blacc 0 Oct  1 06:36 web_prod.conf
-rw-rw-r-- 1 blacc blacc 0 Oct  1 06:36 web_staging.conf
blacc@blacc-VirtualBox:~/Desktop/Introduction_to_linux/projects/client_work/web/
fronted$

```

`touch {A..C}{10..12}_{input,output}.txt`

```

blacc@blacc-VirtualBox:~/Desktop/Introduction_to_linux/projects/client_work/web/
fronted$ touch {A..C}{10..12}_{input,output}.txt
blacc@blacc-VirtualBox:~/Desktop/Introduction_to_linux/projects/client_work/web/
fronted$ ls -l *.txt
-rw-rw-r-- 1 blacc blacc 0 Oct  1 06:39 A10_input.txt
-rw-rw-r-- 1 blacc blacc 0 Oct  1 06:39 A10_output.txt
-rw-rw-r-- 1 blacc blacc 0 Oct  1 06:39 A11_input.txt
-rw-rw-r-- 1 blacc blacc 0 Oct  1 06:39 A11_output.txt
-rw-rw-r-- 1 blacc blacc 0 Oct  1 06:39 A12_input.txt
-rw-rw-r-- 1 blacc blacc 0 Oct  1 06:39 A12_output.txt
-rw-rw-r-- 1 blacc blacc 0 Oct  1 06:39 B10_input.txt
-rw-rw-r-- 1 blacc blacc 0 Oct  1 06:39 B10_output.txt
-rw-rw-r-- 1 blacc blacc 0 Oct  1 06:39 B11_input.txt
-rw-rw-r-- 1 blacc blacc 0 Oct  1 06:39 B11_output.txt
-rw-rw-r-- 1 blacc blacc 0 Oct  1 06:39 B12_input.txt
-rw-rw-r-- 1 blacc blacc 0 Oct  1 06:39 B12_output.txt
-rw-rw-r-- 1 blacc blacc 0 Oct  1 06:39 C10_input.txt
-rw-rw-r-- 1 blacc blacc 0 Oct  1 06:39 C10_output.txt
-rw-rw-r-- 1 blacc blacc 0 Oct  1 06:39 C11_input.txt
-rw-rw-r-- 1 blacc blacc 0 Oct  1 06:39 C11_output.txt
-rw-rw-r-- 1 blacc blacc 0 Oct  1 06:39 C12_input.txt

```

---

## Q7. Config file endings

```

echo "config test" > linux.txt
unix2dos linux.txt windows.txt

```

```

blacc@blacc-VirtualBox:~/Desktop/Introduction_to_linux/projects/client_work/web/
fronted$ echo "config test" > linux.txt unix2dos linux.txt windows.txt
blacc@blacc-VirtualBox:~/Desktop/Introduction_to_linux/projects/client_work/web/
fronted$

```

```

diff linux.txt windows.txt
cmp linux.txt windows.txt
comm linux.txt windows.txt

```

- Windows = CRLF, Linux = LF → tools show differences differently.
- Lesson: Cross-platform compatibility issues may break scripts.

---

## Q8. find for audit

---

## Q9. Large log file analysis

```
seq 1 250 > biglog.txt
```

```
blacc@blacc-VirtualBox:~/Desktop/Introduction_to_linux/projects/client_work/web/f
routed$ seq 1 250 > biglog.txt
blacc@blacc-VirtualBox:~/Desktop/Introduction_to_linux/projects/client_work/web/f
routed$
```

```
sed -n '100,150p' biglog.txt
```

```
blacc@blacc-VirtualBox:~/Desktop/Introduction_to_linux/projects/client_work/web/f
routed$ seq 1 250 > biglog.txt
blacc@blacc-VirtualBox:~/Desktop/Introduction_to_linux/projects/client_work/web/f
routed$ sed -n '100,500p' biglog.txt
100
101
102
103
```

```
grep -n '200' biglog.txt | tail -1
```

```
blacc@blacc-VirtualBox:~/Desktop/Introduction_to_linux/projects/client_work/web/f
routed$ grep -n '200' biglog.txt | tail -1
200:200
blacc@blacc-VirtualBox:~/Desktop/Introduction_to_linux/projects/client_work/web/f
routed$
```

```
grep -A5 -B5 '200' biglog.txt | tail -11
```

```
blacc@blacc-VirtualBox:~/Desktop/Introduction_to_linux/projects/client_work/web/f
routed$ grep -A5 -B5 '200' biglog.txt | tail -11
195
196
197
198
199
200
201
202
203
204
205
blacc@blacc-VirtualBox:~/Desktop/Introduction_to_linux/projects/client_work/web/f
routed$
```

```
time less biglog.txt
```

```
30
50
58
51
50
52
54
53
55
57
50
10
18
11
10
12
14
13
15
17
10
0
8
1
0
2
4
3
5
1
```

time cat biglog.txt

```
blacc@blacc-VirtualBox:~/Desktop/Introduction_to_linux/projects/client_work/web/f
ronted$ time cat biglog.txt
1
2
3
4
5
6
7
8
9
10
11
```

grep -n "error" biglog.txt

```
blacc@blacc-VirtualBox:~/Desktop/Introduction_to_linux/projects/client_work/web/f
ronted$ grep -n "error" biglog.txt
blacc@blacc-VirtualBox:~/Desktop/Introduction_to_linux/projects/client_work/web/f
ronted$
```

---

## Q10. find -exec automation

find . -type f ! -perm 755 -exec chmod 644 {} \;

```
blacc@blacc-VirtualBox:~/Desktop/Introduction_to_linux/projects/client_work/web/f
ronted$ sudo find . -type f ! -perm 755 -exec chmod 644 {} \;
[sudo] password for blacc:
blacc@blacc-VirtualBox:~/Desktop/Introduction_to_linux/projects/client_work/web/f
ronted$
```

find . -type f -mtime +30 -exec du -ch {} + | tail -1

```
blacc@blacc-VirtualBox:~/Desktop/Introduction_to_linux/projects/client_work/web/f
ronted$ find . -type f -mtime +30 -exec du -ch {} + | tail -1
blacc@blacc-VirtualBox:~/Desktop/Introduction_to_linux/projects/client_work/web/f
ronted$
```

find . -type f -name "\*.conf" -exec cp {} {}.backup \;



```
blacc@blacc-VirtualBox:~/Desktop/Introduction_to_linux/projects/client_work/web/f
ronted$ find . -type f -name "*.conf" -exec cp {} {}.backup \;
blacc@blacc-VirtualBox:~/Desktop/Introduction_to_linux/projects/client_work/web/f
ronted$
```

```
find . -name "*.tmp" -atime +7 -print
```

```
blacc@blacc-VirtualBox:~/Desktop/Introduction_to_linux/projects/client_work/web/f
ronted$ find . -name "*.tmp" -atime +7 -print
blacc@blacc-VirtualBox:~/Desktop/Introduction_to_linux/projects/client_work/web/f
ronted$
```

```
find . -name "*.tmp" -atime +7 -delete
```

```
blacc@blacc-VirtualBox:~/Desktop/Introduction_to_linux/projects/client_work/web/f
ronted$ find . -name "*.tmp" -atime +7 -delete
blacc@blacc-VirtualBox:~/Desktop/Introduction_to_linux/projects/client_work/web/f
ronted$
```

---

## Q11. Compression analysis

- 

---

## Q12. Archive management

mkdir text\_dir media\_dir

```
blacc@blacc-VirtualBox:~/Desktop/Introduction_to_linux/projects/client_work/web/f
ronted$ mkdir text
blacc@blacc-VirtualBox:~/Desktop/Introduction_to_linux/projects/client_work/web/f
ronted$ mkdir text_dir media_dir
blacc@blacc-VirtualBox:~/Desktop/Introduction_to_linux/projects/client_work/web/f
ronted$
```

echo "This is a text file for compression testing" > text\_dir/file1.txt

```
blacc@blacc-VirtualBox:~/Desktop/Introduction_to_linux/projects/client_work/web/f
ronted$ echo "THIS is a text file for compression testing">text_dir/file1.txt
blacc@blacc-VirtualBox:~/Desktop/Introduction_to_linux/projects/client_work/web/f
ronted$
```

echo "Another text file with different content" > text\_dir/file2.txt

```
blacc@blacc-VirtualBox:~/Desktop/Introduction_to_linux/projects/client_work/web/f
ronted$ echo "Aanother text file with different content">text_dir/file2.txt
blacc@blacc-VirtualBox:~/Desktop/Introduction_to_linux/projects/client_work/web/f
ronted$
```

---

## Q13. Backup rotation

- Daily incremental

```
tar --listed-incremental=daily.snar -czf daily_$(date +%F).tar.gz /data
```

- **Weekly full**

```
tar -czf full_weekly_$(date +%F).tar.gz /data
```

- **Monthly archive** → store in /backups/archive/.

- **Cleanup**

```
find /backups -type f -mtime +90 -delete
```

- **Verify**

```
tar -tvf archive.tar.gz  
md5sum archive.tar.gz
```

---

## Q14. User analysis

Id

```
blacc@blacc-VirtualBox:~/Desktop/Introduction_to_linux/projects/client_work/web/f  
ronted$ id  
uid=1000(blacc) gid=1000(blacc) groups=1000(blacc),4(adm),24(cdrom),27(sudo),30(d  
ip),46(plugdev),108(lpadmin),124(sambashare)  
blacc@blacc-VirtualBox:~/Desktop/Introduction_to_linux/projects/client_work/web/f  
ronted$
```

groups user1

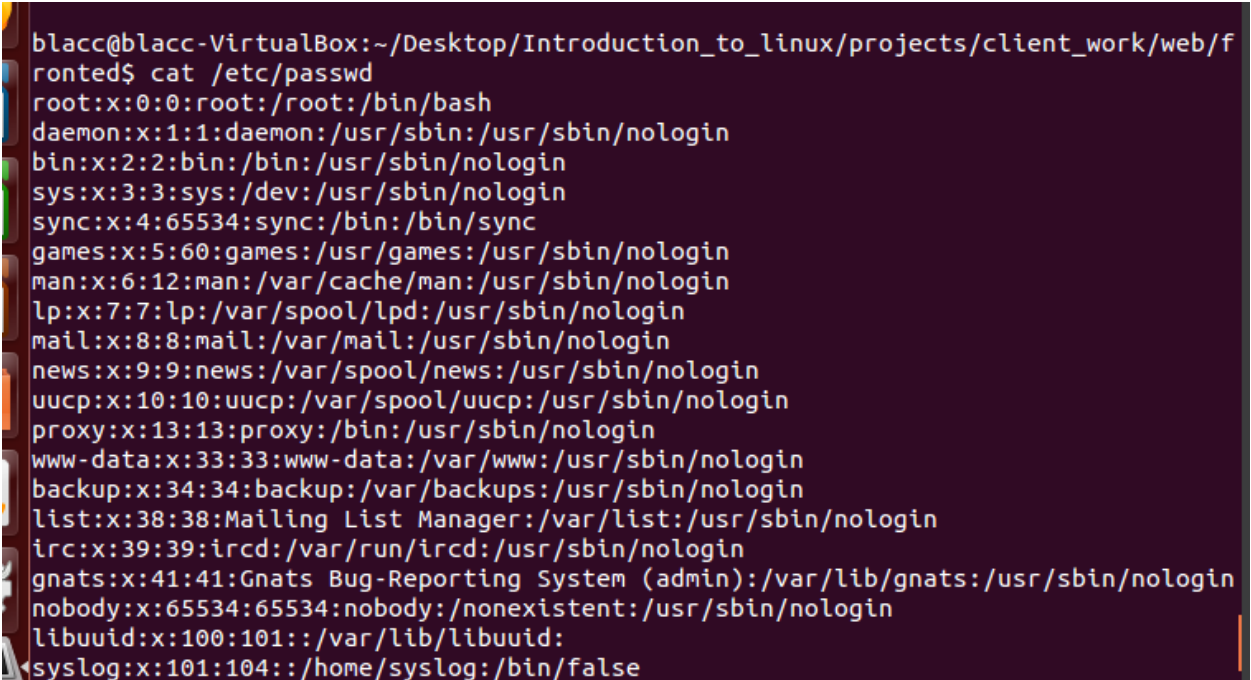
```
blacc@blacc-VirtualBox:~/Desktop/Introduction_to_linux/projects/client_work/web/f  
ronted$ groups user1  
groups: user1: no such user  
blacc@blacc-VirtualBox:~/Desktop/Introduction_to_linux/projects/client_work/web/f  
ronted$
```

groups user2

```
blacc@blacc-VirtualBox:~/Desktop/Introduction_to_linux/projects/client_work/web/f  
ronted$ groups user2  
groups: user2: no such user  
blacc@blacc-VirtualBox:~/Desktop/Introduction_to_linux/projects/client_work/web/f  
ronted$
```

cat /etc/passwd

- System users → UID <1000, nologin shells.
- Regular users → UID ≥1000, bash shell.

- 
- A terminal window with a dark purple background. The prompt is 'blacc@blacc-VirtualBox:~/Desktop/Introduction\_to\_linux/projects/client\_work/web/f'. The user has run 'cat /etc/passwd'. The output lists system users: root, daemon, bin, sys, sync, games, man, lp, mail, news, uucp, proxy, www-data, backup, list, irc, gnats, nobody, libuuid, and syslog. Each entry follows the format 'username:x:uid:gid:gecos:home:shell'.
- ```
blacc@blacc-VirtualBox:~/Desktop/Introduction_to_linux/projects/client_work/web/f
rooted$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
```

- Risk: if normal users belong to adm, sudo, etc. → privilege escalation.

---

## Q15. Group propagation

id

groups

newgrp groupname

- Groups for logs = adm, syslog.
- Groups for web = www-data.
- Groups for admin = sudo, wheel.
- Apply **principle of least privilege**.

---

## Q16. Sudo & escalation audit

sudo -l

```
blacc@blacc-VirtualBox:~/Desktop/Introduction_to_linux/projects/client_work/web/fronted$ sudo -l
[sudo] password for blacc:
Matching Defaults entries for blacc on blacc-VirtualBox:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User blacc may run the following commands on blacc-VirtualBox:
    (ALL : ALL) ALL
blacc@blacc-VirtualBox:~/Desktop/Introduction_to_linux/projects/client_work/web/fronted$
```

`sudo -i`

```
(ALL : ALL) ALL
blacc@blacc-VirtualBox:~/Desktop/Introduction_to_linux/projects/client_work/web/fronted$ sudo -i
root@blacc-VirtualBox:~#
```

`sudo su`

```
blacc@blacc-VirtualBox: /home/blacc/Desktop/Introduction_to_linux/projects/
blacc@blacc-VirtualBox:~/Desktop/Introduction_to_linux/projects/client_work/web/fronted$ sudo su
root@blacc-VirtualBox:/home/blacc/Desktop/Introduction_to_linux/projects/client_work/web/fronted#
```

`su -`

`sudo -u postgres psql`

- Risk: ALL=(ALL) NOPASSWD:ALL.
- Recommendation: restrict commands to roles.