

Assignment2

Name: MUGABO Serge

ID: 26065

Email: mugaboserge81@gmail.com

Q1. Investigating compromised system (/bin, /etc, /var, /usr, /tmp, /opt, /boot, /home)

- **/etc** → Contains system configuration files (attackers may alter passwd, shadow, sshd_config).
- **/bin** → Holds essential binaries (ls, cp, mv). Attackers could replace them with trojans.
- **/var** → Holds logs (/var/log), spool, mail. Logs may reveal intrusion evidence or be tampered with.
- **/usr** → User applications and binaries; less critical than /bin, but attackers might plant malware.
- **/tmp** → Temporary storage, world-writable. Often abused for malicious scripts.
- **/opt** → Optional software. Attackers might install hidden apps here.
- **/boot** → Kernel and bootloader files. Modifying = persistent rootkits.
- **/home** → User files; could contain malware, stolen data, or attacker accounts.

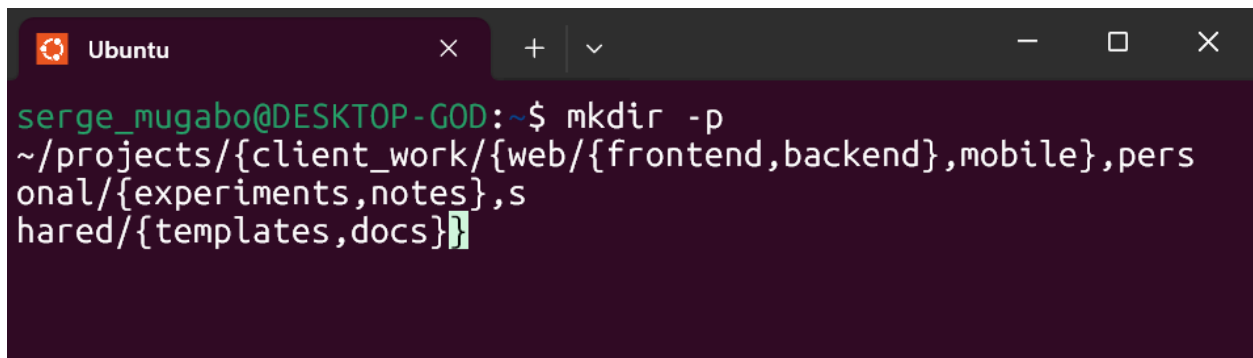
Q2. Create project structure with specific access patterns

commands:

```
mkdir -p
```

```
~/projects/{client_work/{web/{frontend,backend},mobile},personal/{experiments,notes},shared/{templates,docs}}
```

Screenshot:

A screenshot of a terminal window with a dark purple background. The window title bar shows 'Ubuntu' and standard window controls. The prompt is 'serge_mugabo@DESKTOP-GOD:~\$'. The command entered is 'mkdir -p ~/projects/{client_work/{web/{frontend,backend},mobile},personal/{experiments,notes},shared/{templates,docs}}'.

```
serge_mugabo@DESKTOP-GOD:~$ mkdir -p  
~/projects/{client_work/{web/{frontend,backend},mobile},pers  
onal/{experiments,notes},s  
hared/{templates,docs}}
```

Q3. Navigation with ≤ 3 cd

commands:

```
cd ../../../../personal/experiments
```

```
pwd
```

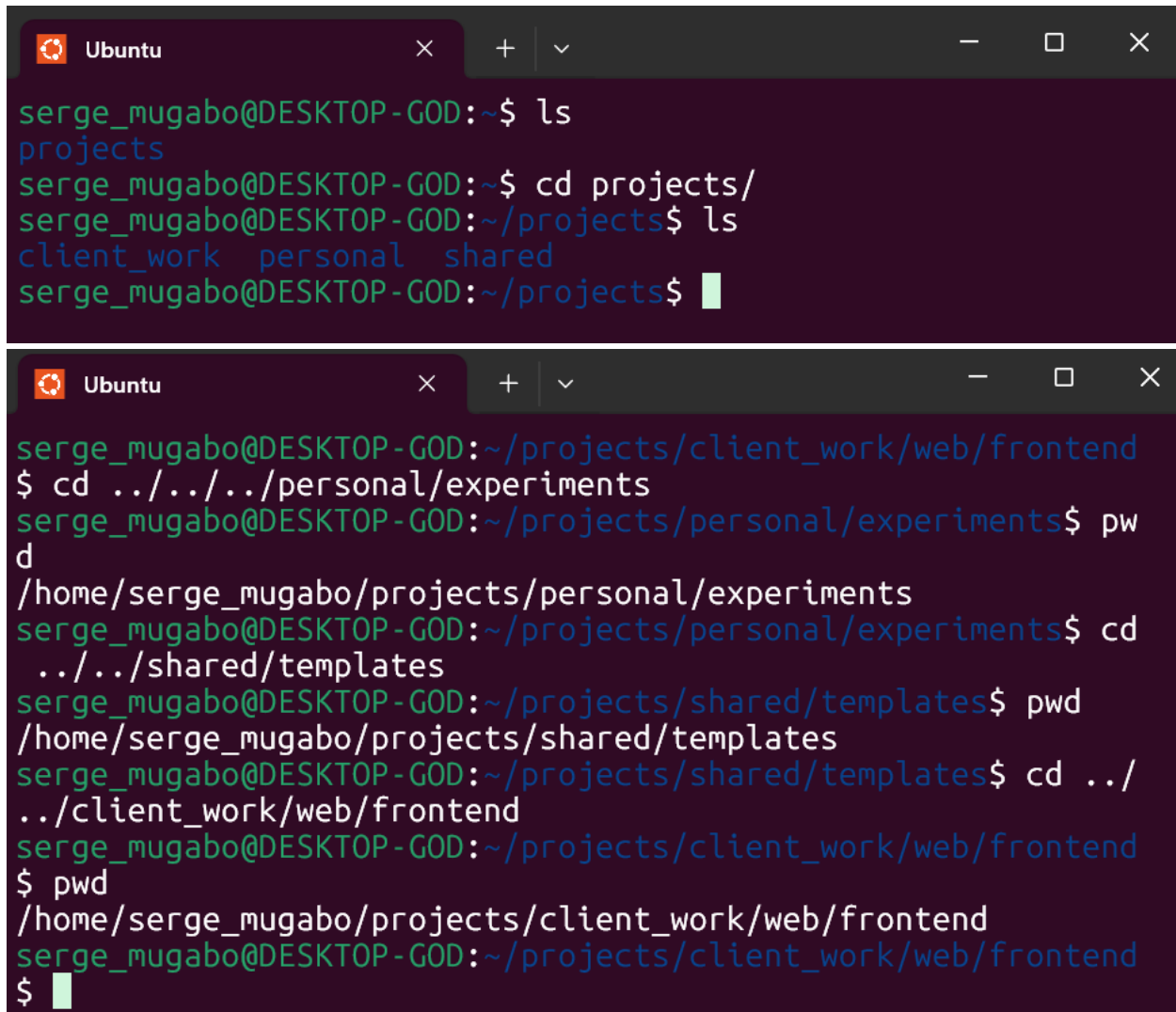
```
cd ../../shared/templates
```

```
pwd
```

```
cd ../../client_work/web/frontend
```

```
pwd
```

Screenshot:



The image shows two screenshots of a terminal window. The top screenshot shows the user navigating from the home directory to the 'projects' directory. The bottom screenshot shows the user navigating through a series of subdirectories: 'client_work/web/frontend', 'personal/experiments', 'shared/templates', and back to 'client_work/web/frontend'.

```
serge_mugabo@DESKTOP-GOD:~$ ls
projects
serge_mugabo@DESKTOP-GOD:~$ cd projects/
serge_mugabo@DESKTOP-GOD:~/projects$ ls
client_work  personal  shared
serge_mugabo@DESKTOP-GOD:~/projects$
```

```
serge_mugabo@DESKTOP-GOD:~/projects/client_work/web/frontend
$ cd ../../../../personal/experiments
serge_mugabo@DESKTOP-GOD:~/projects/personal/experiments$ pwd
/home/serge_mugabo/projects/personal/experiments
serge_mugabo@DESKTOP-GOD:~/projects/personal/experiments$ cd
../../shared/templates
serge_mugabo@DESKTOP-GOD:~/projects/shared/templates$ pwd
/home/serge_mugabo/projects/shared/templates
serge_mugabo@DESKTOP-GOD:~/projects/shared/templates$ cd ../
../client_work/web/frontend
serge_mugabo@DESKTOP-GOD:~/projects/client_work/web/frontend
$ pwd
/home/serge_mugabo/projects/client_work/web/frontend
serge_mugabo@DESKTOP-GOD:~/projects/client_work/web/frontend
$
```

Q4. Web project structure

Commands:

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

#CSS

```
touch {main,reset,theme_{light,dark},mobile,tablet,desktop,print}.css
```

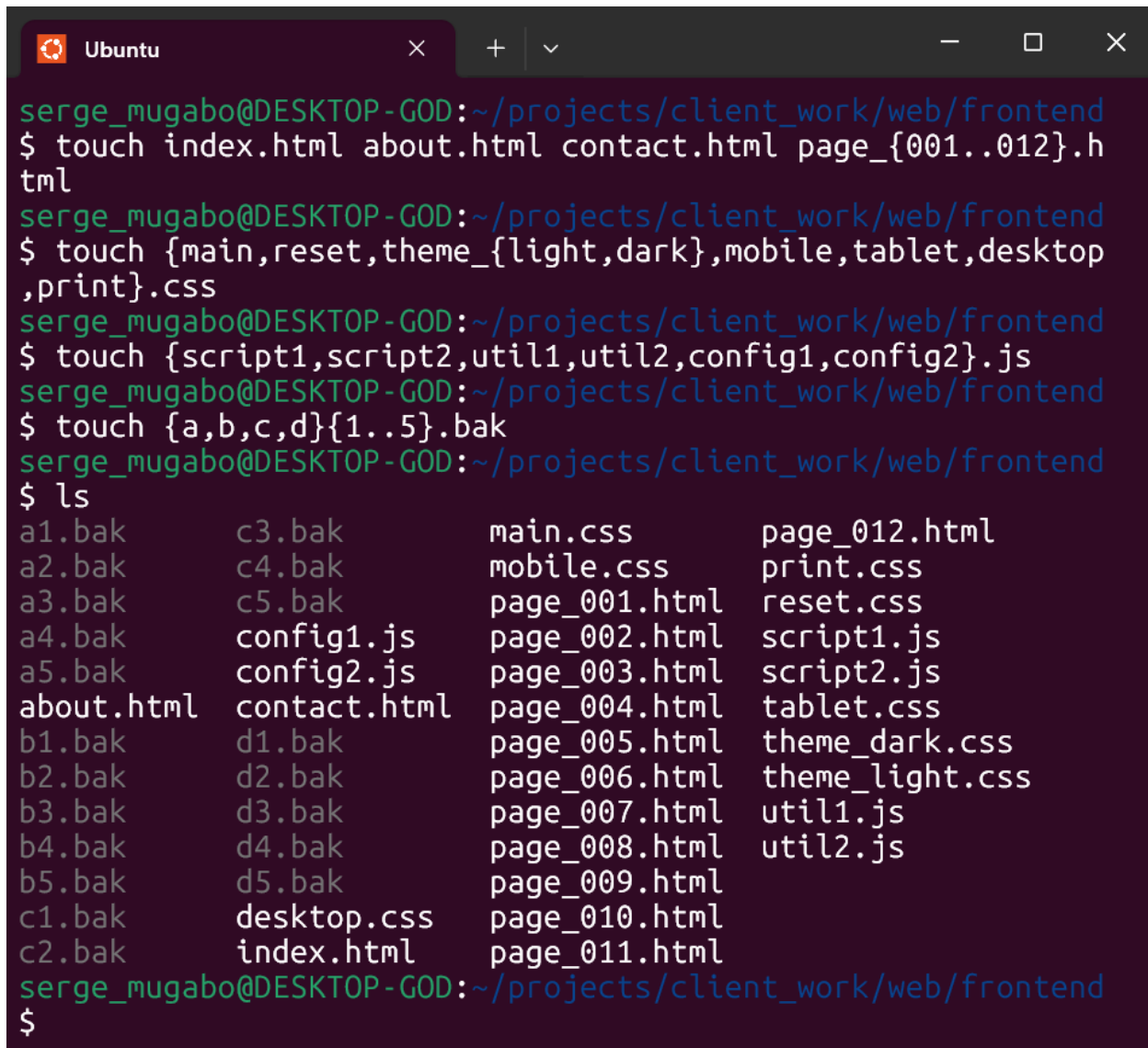
JS

```
touch {script1,script2,util1,util2,config1,config2}.js
```

Backup files (20: 5 each a*, b*, c*, d*)

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

Screenshot:

A screenshot of a terminal window titled 'Ubuntu' with standard window controls. The terminal shows a series of commands and their output. The user is in the directory ~/projects/client_work/web/frontend. The commands executed are: 1. touch index.html about.html contact.html page_{001..012}.html 2. touch {main,reset,theme_{light,dark},mobile,tablet,desktop,print}.css 3. touch {script1,script2,util1,util2,config1,config2}.js 4. touch {a,b,c,d}{1..5}.bak 5. ls. The output of the ls command is a four-column list of files: a1.bak, a2.bak, a3.bak, a4.bak, a5.bak, about.html, b1.bak, b2.bak, b3.bak, b4.bak, b5.bak, c1.bak, c2.bak, c3.bak, c4.bak, c5.bak, config1.js, config2.js, contact.html, d1.bak, d2.bak, d3.bak, d4.bak, d5.bak, desktop.css, index.html, main.css, mobile.css, page_001.html, page_002.html, page_003.html, page_004.html, page_005.html, page_006.html, page_007.html, page_008.html, page_009.html, page_010.html, page_011.html, page_012.html, print.css, reset.css, script1.js, script2.js, tablet.css, theme_dark.css, theme_light.css, util1.js, and util2.js.

```
serge_mugabo@DESKTOP-GOD:~/projects/client_work/web/frontend
$ touch index.html about.html contact.html page_{001..012}.h
tml
serge_mugabo@DESKTOP-GOD:~/projects/client_work/web/frontend
$ touch {main,reset,theme_{light,dark},mobile,tablet,desktop
,print}.css
serge_mugabo@DESKTOP-GOD:~/projects/client_work/web/frontend
$ touch {script1,script2,util1,util2,config1,config2}.js
serge_mugabo@DESKTOP-GOD:~/projects/client_work/web/frontend
$ touch {a,b,c,d}{1..5}.bak
serge_mugabo@DESKTOP-GOD:~/projects/client_work/web/frontend
$ ls
a1.bak      c3.bak      main.css    page_012.html
a2.bak      c4.bak      mobile.css  print.css
a3.bak      c5.bak      page_001.html reset.css
a4.bak      config1.js  page_002.html script1.js
a5.bak      config2.js  page_003.html script2.js
about.html  contact.html page_004.html tablet.css
b1.bak      d1.bak      page_005.html theme_dark.css
b2.bak      d2.bak      page_006.html theme_light.css
b3.bak      d3.bak      page_007.html util1.js
b4.bak      d4.bak      page_008.html util2.js
b5.bak      d5.bak      page_009.html
c1.bak      desktop.css page_010.html
c2.bak      index.html  page_011.html
serge_mugabo@DESKTOP-GOD:~/projects/client_work/web/frontend
$
```

Q5. Wildcards for file organization

Commands:

#Move files ending with numbers

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

#Copy CSS except mobile/tablet

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

#List files with 3 chars before dot

```
ls ???.*
```

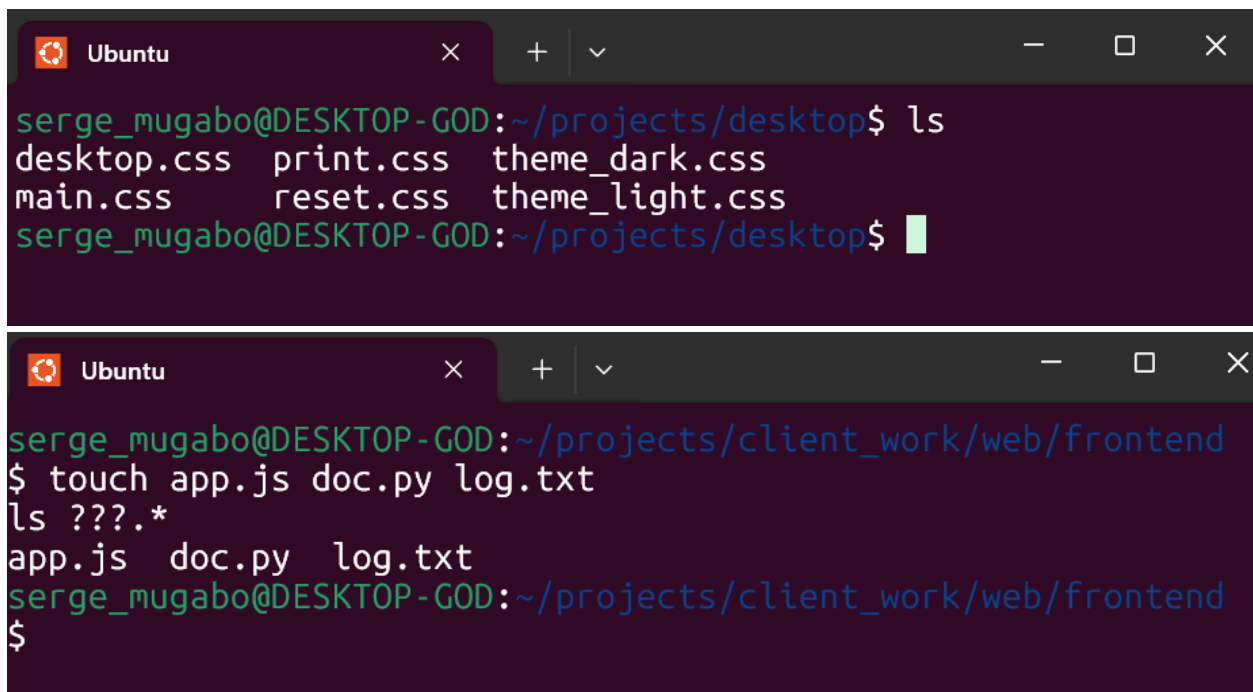
#Files starting with consonant

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

#Extensions with exactly 2 chars

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

Screenshot:



The image shows two screenshots of a terminal window on an Ubuntu system. The first screenshot shows a user running the command `ls` in the directory `~/projects/desktop`, listing files: `desktop.css`, `print.css`, `theme_dark.css`, `main.css`, `reset.css`, and `theme_light.css`. The second screenshot shows the user running `touch app.js doc.py log.txt` and then `ls ???.*` in the directory `~/projects/client_work/web/frontend`, listing the newly created files: `app.js`, `doc.py`, and `log.txt`.

```
serge_mugabo@DESKTOP-GOD:~/projects/desktop$ ls
desktop.css  print.css  theme_dark.css
main.css     reset.css  theme_light.css
serge_mugabo@DESKTOP-GOD:~/projects/desktop$

serge_mugabo@DESKTOP-GOD:~/projects/client_work/web/frontend
$ touch app.js doc.py log.txt
ls ???.*
app.js  doc.py  log.txt
serge_mugabo@DESKTOP-GOD:~/projects/client_work/web/frontend
$
```

```
serge_mugabo@DESKTOP-GOD:~/projects/client_work/web/frontend
$ ls [b-df-hj-np-tv-z]*
contact.html  log.txt      print.css    theme_dark.css
desktop.css   main.css     reset.css    theme_light.css
doc.py        mobile.css   tablet.css
serge_mugabo@DESKTOP-GOD:~/projects/client_work/web/frontend
$

serge_mugabo@DESKTOP-GOD:~/projects/client_work/web/frontend
$ ls *.*[a-zA-Z][a-zA-Z]
app.js  doc.py
serge_mugabo@DESKTOP-GOD:~/projects/client_work/web/frontend
$
```

Q6. Brace expansion patterns

Commands:

#Logs for Q1 2024

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

#Configs for 3 env × 3 services

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

#Test files A–C × 10–12 × input/output

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

Screenshot:

```
serge_mugabo@DESKTOP-GOD: ~/projects$ touch log_2024-{01..03}-{01..31}.txt
serge_mugabo@DESKTOP-GOD: ~/projects$ touch {web,api,db}_{dev,staging,prod}.conf
serge_mugabo@DESKTOP-GOD: ~/projects$ touch {A..C}{10..12}_{input,output}.txt
serge_mugabo@DESKTOP-GOD: ~/projects$ ls
A10_input.txt      log_2024-01-16.txt  log_2024-02-27.txt
A10_output.txt     log_2024-01-17.txt  log_2024-02-28.txt
A11_input.txt      log_2024-01-18.txt  log_2024-02-29.txt
A11_output.txt     log_2024-01-19.txt  log_2024-02-30.txt
A12_input.txt      log_2024-01-20.txt  log_2024-02-31.txt
A12_output.txt     log_2024-01-21.txt  log_2024-03-01.txt
B10_input.txt      log_2024-01-22.txt  log_2024-03-02.txt
B10_output.txt     log_2024-01-23.txt  log_2024-03-03.txt
B11_input.txt      log_2024-01-24.txt  log_2024-03-04.txt
B11_output.txt     log_2024-01-25.txt  log_2024-03-05.txt
B12_input.txt      log_2024-01-26.txt  log_2024-03-06.txt
B12_output.txt     log_2024-01-27.txt  log_2024-03-07.txt
C10_input.txt      log_2024-01-28.txt  log_2024-03-08.txt
C10_output.txt     log_2024-01-29.txt  log_2024-03-09.txt
C11_input.txt      log_2024-01-30.txt  log_2024-03-10.txt
C11_output.txt     log_2024-01-31.txt  log_2024-03-11.txt
C12_input.txt      log_2024-02-01.txt  log_2024-03-12.txt
C12_output.txt     log_2024-02-02.txt  log_2024-03-13.txt
api_dev.conf       log_2024-02-03.txt  log_2024-03-14.txt
api_prod.conf      log_2024-02-04.txt  log_2024-03-15.txt
api_staging.conf   log_2024-02-05.txt  log_2024-03-16.txt
archive            log_2024-02-06.txt  log_2024-03-17.txt
client_work        log_2024-02-07.txt  log_2024-03-18.txt
db_dev.conf        log_2024-02-08.txt  log_2024-03-19.txt
db_prod.conf       log_2024-02-09.txt  log_2024-03-20.txt
db_staging.conf    log_2024-02-10.txt  log_2024-03-21.txt
desktop            log_2024-02-11.txt  log_2024-03-22.txt
log_2024-01-01.txt log_2024-02-12.txt  log_2024-03-23.txt
log_2024-01-02.txt log_2024-02-13.txt  log_2024-03-24.txt
log_2024-01-03.txt log_2024-02-14.txt  log_2024-03-25.txt
log_2024-01-04.txt log_2024-02-15.txt  log_2024-03-26.txt
log_2024-01-05.txt log_2024-02-16.txt  log_2024-03-27.txt
log_2024-01-06.txt log_2024-02-17.txt  log_2024-03-28.txt
log_2024-01-07.txt log_2024-02-18.txt  log_2024-03-29.txt
log_2024-01-08.txt log_2024-02-19.txt  log_2024-03-30.txt
log_2024-01-09.txt log_2024-02-20.txt  log_2024-03-31.txt
log_2024-01-10.txt log_2024-02-21.txt  personal
log_2024-01-11.txt log_2024-02-22.txt  shared
log_2024-01-12.txt log_2024-02-23.txt  web_dev.conf
log_2024-01-13.txt log_2024-02-24.txt  web_prod.conf
log_2024-01-14.txt log_2024-02-25.txt  web_staging.conf
log_2024-01-15.txt log_2024-02-26.txt
serge_mugabo@DESKTOP-GOD: ~/projects$
```

Q7. Line endings comparison

Commands:

echo "Test file" > linux.txt

unix2dos linux.txt win.txt # creates Windows line endings

diff linux.txt win.txt

```
cmp linux.txt win.txt
```

```
comm linux.txt win.txt
```

Screenshot:


```
serge_mugabo@DESKTOP-GOD:~/projects$ echo "Test file" > linux.txt
serge_mugabo@DESKTOP-GOD:~/projects$ unix2dos -n linux.txt win.txt
unix2dos: converting file linux.txt to file win.txt in DOS format...
serge_mugabo@DESKTOP-GOD:~/projects$ diff linux.txt win.txt
cmp linux.txt win.txt
comm linux.txt win.txt
1c1
< Test file
- - -
> Test file
linux.txt win.txt differ: byte 10, line 1
Test file
Test file
serge_mugabo@DESKTOP-GOD:~/projects$
```

```
serge_mugabo@DESKTOP-GOD:~/projects$ echo "Test file" > linux.txt
serge_mugabo@DESKTOP-GOD:~/projects$ unix2dos linux.txt win.txt
unix2dos: command not found
serge_mugabo@DESKTOP-GOD:~/projects$ sudo apt update
sudo apt install dos2unix -y
[sudo] password for serge_mugabo:
Hit:1 http://archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:3 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Get:4 http://archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Get:5 http://archive.ubuntu.com/ubuntu noble/universe amd64 Packages [15.0 MB]
Get:6 http://security.ubuntu.com/ubuntu noble-security/main amd64 Packages [1171 kB]
Get:7 http://security.ubuntu.com/ubuntu noble-security/main Translation-en [198 kB]
Get:8 http://security.ubuntu.com/ubuntu noble-security/main amd64 Components [21.6 kB]
Get:9 http://security.ubuntu.com/ubuntu noble-security/main amd64 c-n-f Metadata [8744 B]
Get:10 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Packages [880 kB]
Get:11 http://security.ubuntu.com/ubuntu noble-security/universe Translation-en [195 kB]
Get:12 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Components [52.2 kB]
Get:13 http://security.ubuntu.com/ubuntu noble-security/universe amd64 c-n-f Metadata [18.0 kB]
Get:14 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Packages [1872 kB]
Get:15 http://security.ubuntu.com/ubuntu noble-security/restricted Translation-en [423 kB]
Get:16 http://archive.ubuntu.com/ubuntu noble/universe Translation-en [5982 kB]
Get:17 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Components [212 B]
Get:18 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 c-n-f Metadata [520 B]
Get:19 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 Packages [28.0 kB]
Get:20 http://security.ubuntu.com/ubuntu noble-security/multiverse Translation-en [5228 B]
Get:21 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 Components [212 B]
Get:22 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 c-n-f Metadata [384 B]
Get:23 http://archive.ubuntu.com/ubuntu noble/universe amd64 Components [3871 kB]
Get:24 http://archive.ubuntu.com/ubuntu noble/universe amd64 c-n-f Metadata [301 kB]
Get:25 http://archive.ubuntu.com/ubuntu noble/multiverse amd64 Packages [269 kB]
Get:26 http://archive.ubuntu.com/ubuntu noble/multiverse Translation-en [118 kB]
```

Q8. Find commands

commands:

#Larger than average

```
find . -type f -size +$(($(du -cb * | grep total | cut -f1)/$(ls -1 | wc -l)))c
```

#Modified in last 72h but not 24h

```
find . -type f -mtime -3 ! -mtime -1
```

#Empty dirs or only hidden files

```
find . -type d -empty -o -type d -exec sh -c 'ls -A "$1" | grep -q "^[.]"'  
&& echo "$1" _ {};
```

#World-writable

```
find . -type f -perm -002
```

#Owned by others

```
find . ! -user $(whoami) ! -user root
```

#Temp/backup

```
find . -type f ( -name '~' -o -name '.bak' -o -name '*.tmp' )
```

Screenshot:

A screenshot of a terminal window with a dark purple background. The window title bar shows 'Ubuntu' and standard window controls. The terminal text shows a user named 'serge_mugabo' at a prompt 'serge_mugabo@DESKTOP-GOD:~/projects\$'. They have entered a complex find command to search for files larger than the average file size in the current directory. The command is split across two lines. The output shows two files: './win.txt' and './linux.txt'. The prompt returns to 'serge_mugabo@DESKTOP-GOD:~/projects\$' with a cursor.

```
serge_mugabo@DESKTOP-GOD:~/projects$ find . -type f -siz  
e +$(($(du -cb * | grep total | cut -f1)/$(ls -1 | wc -l  
)))c  
./win.txt  
./linux.txt  
serge_mugabo@DESKTOP-GOD:~/projects$
```

```
serge_mugabo@DESKTOP-GOD:~/projects$ find . -type f -mtime -3 ! -mtime -1
serge_mugabo@DESKTOP-GOD:~/projects$
```

```
serge_mugabo@DESKTOP-GOD:~/projects$ find . -type d -empty -o -type d -exec sh -c 'ls -A "$1" | grep -q "^[.]" & echo "$1" _ {} \;
```

```
serge_mugabo@DESKTOP-GOD:~/projects$ find . -type f -perm -002
```

```
serge_mugabo@DESKTOP-GOD:~/projects$ find . ! -user $(whoami) ! -user root
```

```
serge_mugabo@DESKTOP-GOD:~/projects$
```

```
serge_mugabo@DESKTOP-GOD:~/projects$ find . -type f ( -name '~' -o -name '*.bak' -o -name '*.tmp' )
```

```
-bash: syntax error near unexpected token `('
```

```
serge_mugabo@DESKTOP-GOD:~/projects$ find . -type f \( -name '~' -o -name '*.bak' -o -name '*.tmp' \)
```

```
./archive/a3.bak
./archive/b1.bak
./archive/c2.bak
./archive/c4.bak
./archive/a1.bak
./archive/d5.bak
./archive/a2.bak
./archive/d1.bak
./archive/b3.bak
./archive/c3.bak
./archive/d3.bak
./archive/b4.bak
./archive/a5.bak
./archive/c5.bak
./archive/b2.bak
./archive/d2.bak
./archive/c1.bak
./archive/a4.bak
./archive/b5.bak
./archive/d4.bak
```

```
serge_mugabo@DESKTOP-GOD:~/projects$
```

Q9. Log file analysis (200+ lines)

Commands:

#Middle 50 lines

```
sed -n '76,125p' logfile.txt
```

#Last occurrence with context

```
grep -n "ERROR" logfile.txt | tail -1 tail -n + logfile.txt | head -10
```

#Timing

```
time cat logfile.txt > /dev/null time less logfile.txt > /dev/null
```

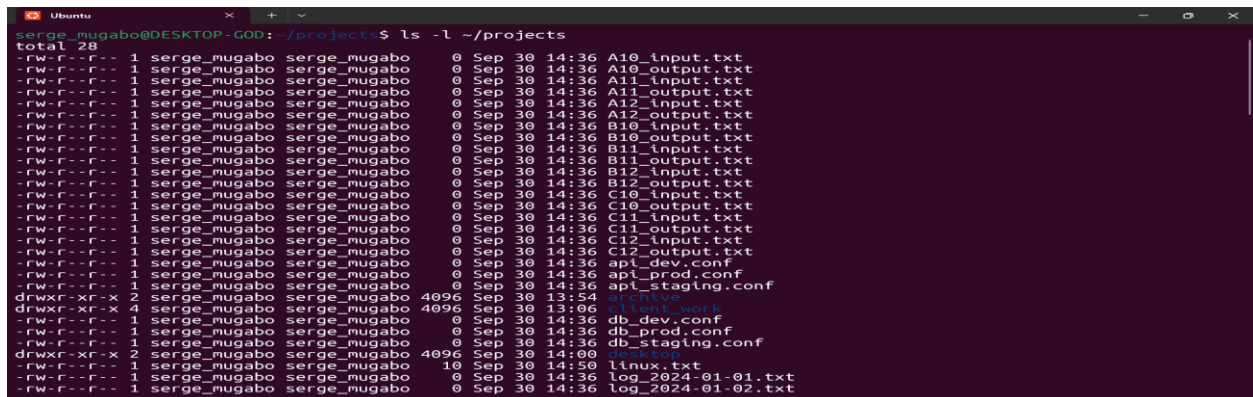
#Extract errors with line numbers

```
grep -n "ERROR" logfile.txt
```

#Why less > cat

less loads page by page → saves bandwidth in SSH.

Screenshot:



```
serge_mugabo@DESKTOP-GOD: ~/projects$ ls -l ~/projects
total 28
-rw-r--r-- 1 serge_mugabo serge_mugabo 0 Sep 30 14:36 A10_input.txt
-rw-r--r-- 1 serge_mugabo serge_mugabo 0 Sep 30 14:36 A10_output.txt
-rw-r--r-- 1 serge_mugabo serge_mugabo 0 Sep 30 14:36 A11_input.txt
-rw-r--r-- 1 serge_mugabo serge_mugabo 0 Sep 30 14:36 A11_output.txt
-rw-r--r-- 1 serge_mugabo serge_mugabo 0 Sep 30 14:36 A12_input.txt
-rw-r--r-- 1 serge_mugabo serge_mugabo 0 Sep 30 14:36 A12_output.txt
-rw-r--r-- 1 serge_mugabo serge_mugabo 0 Sep 30 14:36 B10_input.txt
-rw-r--r-- 1 serge_mugabo serge_mugabo 0 Sep 30 14:36 B10_output.txt
-rw-r--r-- 1 serge_mugabo serge_mugabo 0 Sep 30 14:36 B11_input.txt
-rw-r--r-- 1 serge_mugabo serge_mugabo 0 Sep 30 14:36 B11_output.txt
-rw-r--r-- 1 serge_mugabo serge_mugabo 0 Sep 30 14:36 B12_input.txt
-rw-r--r-- 1 serge_mugabo serge_mugabo 0 Sep 30 14:36 B12_output.txt
-rw-r--r-- 1 serge_mugabo serge_mugabo 0 Sep 30 14:36 C10_input.txt
-rw-r--r-- 1 serge_mugabo serge_mugabo 0 Sep 30 14:36 C10_output.txt
-rw-r--r-- 1 serge_mugabo serge_mugabo 0 Sep 30 14:36 C11_input.txt
-rw-r--r-- 1 serge_mugabo serge_mugabo 0 Sep 30 14:36 C11_output.txt
-rw-r--r-- 1 serge_mugabo serge_mugabo 0 Sep 30 14:36 C12_input.txt
-rw-r--r-- 1 serge_mugabo serge_mugabo 0 Sep 30 14:36 C12_output.txt
-rw-r--r-- 1 serge_mugabo serge_mugabo 0 Sep 30 14:36 apt_dev.conf
-rw-r--r-- 1 serge_mugabo serge_mugabo 0 Sep 30 14:36 apt_prod.conf
-rw-r--r-- 1 serge_mugabo serge_mugabo 0 Sep 30 14:36 apt_staging.conf
drwxr-xr-x 2 serge_mugabo serge_mugabo 4096 Sep 30 13:54 archive
drwxr-xr-x 4 serge_mugabo serge_mugabo 4096 Sep 30 13:06 client_work
-rw-r--r-- 1 serge_mugabo serge_mugabo 0 Sep 30 14:36 db_dev.conf
-rw-r--r-- 1 serge_mugabo serge_mugabo 0 Sep 30 14:36 db_prod.conf
-rw-r--r-- 1 serge_mugabo serge_mugabo 0 Sep 30 14:36 db_staging.conf
drwxr-xr-x 2 serge_mugabo serge_mugabo 4096 Sep 30 14:00 desktop
-rw-r--r-- 1 serge_mugabo serge_mugabo 10 Sep 30 14:50 linux.txt
-rw-r--r-- 1 serge_mugabo serge_mugabo 0 Sep 30 14:36 log_2024-01-01.txt
-rw-r--r-- 1 serge_mugabo serge_mugabo 0 Sep 30 14:36 log_2024-01-02.txt
```

```
serge_mugabo@DESKTOP-GOD:~/projects$ sed -n '76,125p' logfile.txt
sed: can't read logfile.txt: No such file or directory
serge_mugabo@DESKTOP-GOD:~/projects$ # from ~/projects
find . -maxdepth 4 -type f -iname "*log*"

# or look for exact name pattern (case sensitive)
find . -type f -name "logfile.txt"
./log_2024-03-30.txt
./log_2024-02-03.txt
./log_2024-01-03.txt
./log_2024-02-31.txt
./log_2024-03-25.txt
./log_2024-01-01.txt
./log_2024-01-26.txt
./log_2024-02-19.txt
./log_2024-03-17.txt
./log_2024-03-31.txt
./log_2024-02-28.txt
./log_2024-03-14.txt
./log_2024-01-28.txt
./log_2024-03-16.txt
./log_2024-03-15.txt
./log_2024-03-03.txt
./log_2024-01-16.txt
./log_2024-01-23.txt
./log_2024-01-29.txt
./log_2024-01-04.txt
./log_2024-02-16.txt
./log_2024-02-02.txt
./log_2024-02-25.txt
./log_2024-02-17.txt
./log_2024-02-10.txt
./log_2024-01-09.txt
./log_2024-03-05.txt
./log_2024-03-11.txt
./log_2024-03-22.txt
./log_2024-03-27.txt
./log_2024-01-19.txt
./log_2024-02-09.txt
./log_2024-02-12.txt
./log_2024-02-01.txt
./log_2024-03-12.txt
./log_2024-02-21.txt
./log_2024-03-18.txt
./log_2024-01-18.txt
./log_2024-01-25.txt
./log_2024-03-23.txt
./log_2024-03-21.txt
./log_2024-01-07.txt
./log_2024-03-09.txt
```

```
serge_mugabo@DESKTOP-GOD:~/projects$ time cat logfile.txt > /dev/null time
less logfile.txt > /dev/null
cat: logfile.txt: No such file or directory
cat: time: No such file or directory
cat: less: No such file or directory
cat: logfile.txt: No such file or directory

real    0m0.009s
user    0m0.003s
sys     0m0.001s
serge_mugabo@DESKTOP-GOD:~/projects$
```

Q10. Automating maintenance

commands:

#Permissions

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

#Disk space older than 30 days

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

#Backup .conf

```
find . -name "*.conf" -exec cp {} {}.backup ;
```

#Preview remove

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

Screenshot:

```
serge_mugabo@DESKTOP-GOD:~/projects$ find . -type f ! -perm -755 -exec chmo
d 644 {} \;
serge_mugabo@DESKTOP-GOD:~/projects$ find . -type f -mtime +30 -exec du -ch
{} + | tail -1
serge_mugabo@DESKTOP-GOD:~/projects$ find . -name "*.conf" -exec cp {} {}.b
ackup \;
serge_mugabo@DESKTOP-GOD:~/projects$ find . -name "*.tmp" -atime +7 -print
find . -name "*.tmp" -atime +delete
find: paths must precede expression: `find'
serge_mugabo@DESKTOP-GOD:~/projects$ find . -name "*.tmp" -atime +7 -print
serge_mugabo@DESKTOP-GOD:~/projects$ find . -name "*.tmp" -atime +7 -delete
serge_mugabo@DESKTOP-GOD:~/projects$ find . -name "*.tmp" -atime +7 -print
&& find . -name "*.tmp" -atime +7 -delete
serge_mugabo@DESKTOP-GOD:~/projects$ ls
A10_input.txt      log_2024-01-13.txt  log_2024-02-28.txt
A10_output.txt     log_2024-01-14.txt  log_2024-02-29.txt
A11_input.txt      log_2024-01-15.txt  log_2024-02-30.txt
A11_output.txt     log_2024-01-16.txt  log_2024-02-31.txt
A12_input.txt      log_2024-01-17.txt  log_2024-03-01.txt
A12_output.txt     log_2024-01-18.txt  log_2024-03-02.txt
B10_input.txt      log_2024-01-19.txt  log_2024-03-03.txt
B10_output.txt     log_2024-01-20.txt  log_2024-03-04.txt
B11_input.txt      log_2024-01-21.txt  log_2024-03-05.txt
B11_output.txt     log_2024-01-22.txt  log_2024-03-06.txt
B12_input.txt      log_2024-01-23.txt  log_2024-03-07.txt
B12_output.txt     log_2024-01-24.txt  log_2024-03-08.txt
C10_input.txt      log_2024-01-25.txt  log_2024-03-09.txt
C10_output.txt     log_2024-01-26.txt  log_2024-03-10.txt
C11_input.txt      log_2024-01-27.txt  log_2024-03-11.txt
C11_output.txt     log_2024-01-28.txt  log_2024-03-12.txt
C12_input.txt      log_2024-01-29.txt  log_2024-03-13.txt
C12_output.txt     log_2024-01-30.txt  log_2024-03-14.txt
api_dev.conf       log_2024-01-31.txt  log_2024-03-15.txt
api_dev.conf.backup log_2024-02-01.txt  log_2024-03-16.txt
api_prod.conf      log_2024-02-02.txt  log_2024-03-17.txt
api_prod.conf.backup log_2024-02-03.txt  log_2024-03-18.txt
api_staging.conf   log_2024-02-04.txt  log_2024-03-19.txt
api_staging.conf.backup log_2024-02-05.txt  log_2024-03-20.txt
archive            log_2024-02-06.txt  log_2024-03-21.txt
```

Q11.Compression analysis

commands:

```
tar -czf text.tar.gz text_dir
```

```
tar -cjf text.tar.bz2 text_dir
```

```
tar -cJf text.tar.xz text_dir
```



```
zip -r text.zip text_dir
```

Screenshot:

```
serge_mugabo@DESKTOP-GOD:~/projects$ tar -czf text.tar.gz text_dir
tar -cjf text.tar.bz2 text_dir
tar -cJf text.tar.xz text_dir
zip -r text.zip text_dir
updating: text_dir/ (stored 0%)
updating: text_dir/file1.txt (stored 0%)
updating: text_dir/file2.txt (stored 0%)
serge_mugabo@DESKTOP-GOD:~/projects$
```

```
serge_mugabo@DESKTOP-GOD:~/projects$ find . -type f | sort
./B11_output.txt
./B12_input.txt
./B12_output.txt
./C10_input.txt
./C10_output.txt
./C11_input.txt
./C11_output.txt
./C12_input.txt
./C12_output.txt
./api_dev.conf
./api_dev.conf.backup
./api_prod.conf
./api_prod.conf.backup
./api_staging.conf
./api_staging.conf.backup
./archive
./client_work
./db_dev.conf
./db_dev.conf.backup
./db_prod.conf
./db_prod.conf.backup
./db_staging.conf
./db_staging.conf.backup
./desktop
./linux.txt
./log_2024-01-01.txt
./log_2024-01-02.txt
./log_2024-01-03.txt
./log_2024-01-04.txt
./log_2024-01-05.txt
./log_2024-01-06.txt
./log_2024-01-07.txt
./log_2024-01-08.txt
./log_2024-01-09.txt
./log_2024-01-10.txt
./log_2024-01-11.txt
./log_2024-01-12.txt
./log_2024-01-13.txt
./log_2024-01-23.txt
./log_2024-01-24.txt
./log_2024-01-25.txt
./log_2024-01-26.txt
./log_2024-01-27.txt
./log_2024-01-28.txt
./log_2024-01-29.txt
./log_2024-01-30.txt
./log_2024-01-31.txt
./log_2024-02-01.txt
./log_2024-02-02.txt
./log_2024-02-03.txt
./log_2024-02-04.txt
./log_2024-02-05.txt
./log_2024-02-06.txt
./log_2024-02-07.txt
./log_2024-02-08.txt
./log_2024-02-09.txt
./log_2024-02-10.txt
./log_2024-02-11.txt
./log_2024-02-12.txt
./log_2024-02-13.txt
./log_2024-02-14.txt
./log_2024-02-15.txt
./log_2024-02-16.txt
./log_2024-02-17.txt
./log_2024-02-18.txt
./log_2024-02-19.txt
./log_2024-02-20.txt
./log_2024-02-21.txt
./log_2024-02-22.txt
./log_2024-02-23.txt
./log_2024-02-24.txt
./log_2024-02-25.txt
./log_2024-02-26.txt
./log_2024-02-27.txt
./log_2024-02-28.txt
./log_2024-02-29.txt
./log_2024-03-08.txt
./log_2024-03-09.txt
./log_2024-03-10.txt
./log_2024-03-11.txt
./log_2024-03-12.txt
./log_2024-03-13.txt
./log_2024-03-14.txt
./log_2024-03-15.txt
./log_2024-03-16.txt
./log_2024-03-17.txt
./log_2024-03-18.txt
./log_2024-03-19.txt
./log_2024-03-20.txt
./log_2024-03-21.txt
./log_2024-03-22.txt
./log_2024-03-23.txt
./log_2024-03-24.txt
./log_2024-03-25.txt
./log_2024-03-26.txt
./log_2024-03-27.txt
./log_2024-03-28.txt
./log_2024-03-29.txt
./log_2024-03-30.txt
./log_2024-03-31.txt
./personal
./shared
./text.tar.bz2
./text.tar.gz
./text.tar.xz
./text.zip
./text_dir
./web_dev.conf
./web_dev.conf.backup
./web_prod.conf
./web_prod.conf.backup
./web_staging.conf
./web_staging.conf.backup
./win.txt
serge_mugabo@DESKTOP-GOD:~/projects$
```

Q12. Archive operations

commands:

#Examine without extract

```
tar -tf archive.tar unzip -l archive.zip
```

#Extract specific

```
tar -xf archive.tar "*.conf"
```

#Update existing archive

```
tar -rf archive.tar newfile.txt
```

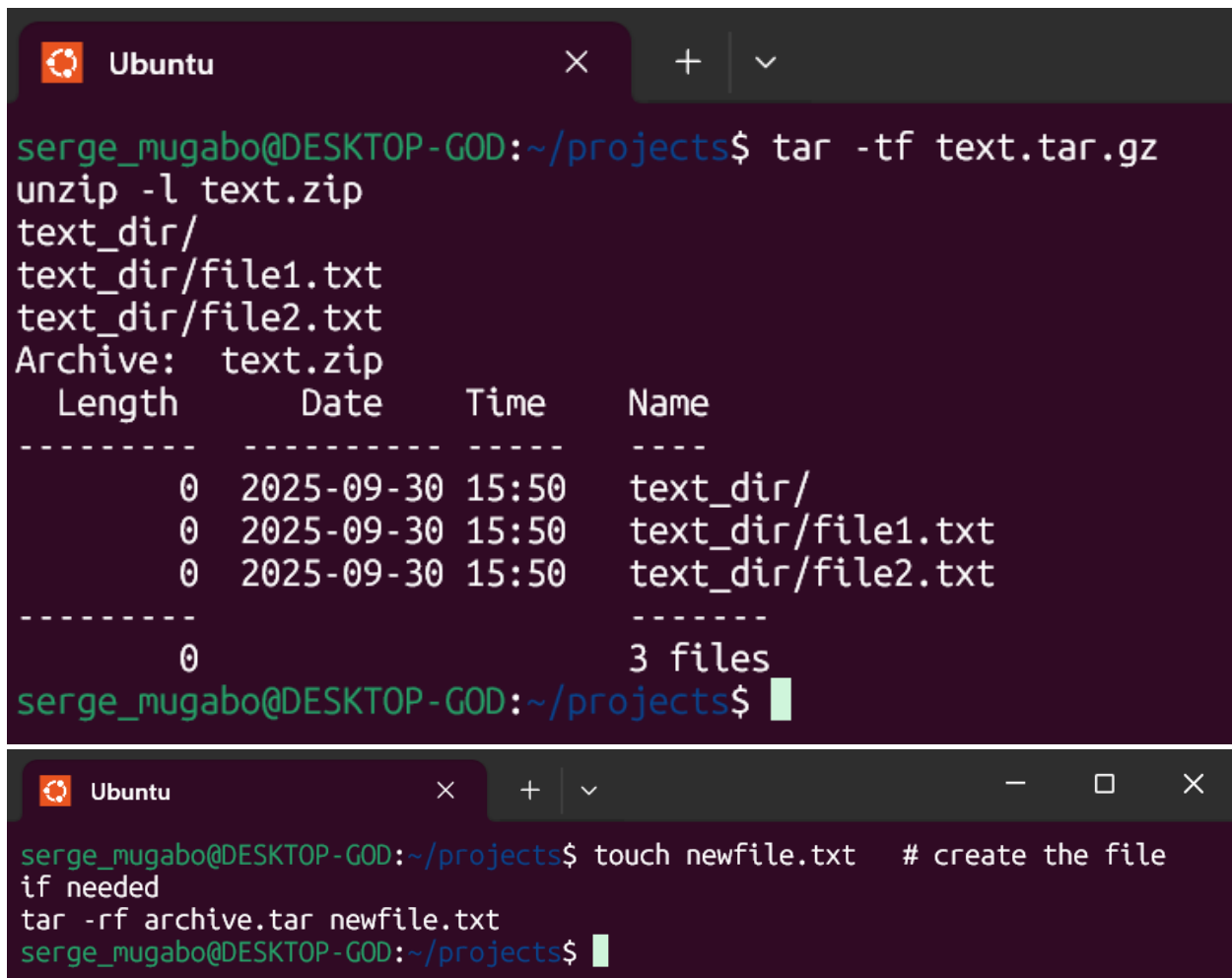
#Handle corruption

```
zip -FF bad.zip --out fixed.zip
```

#Merge multiple archives

```
tar -Af combined.tar part1.tar
```

Screenshot:



The image shows two screenshots of a terminal window. The top screenshot shows the command `tar -tf text.tar.gz` being executed, which lists the contents of the archive. The output shows a directory `text_dir/` and two files `text_dir/file1.txt` and `text_dir/file2.txt`. The bottom screenshot shows the command `touch newfile.txt` being executed, followed by `tar -rf archive.tar newfile.txt`, which adds the new file to the archive.

```
serge_mugabo@DESKTOP-GOD:~/projects$ tar -tf text.tar.gz
unzip -l text.zip
text_dir/
text_dir/file1.txt
text_dir/file2.txt
Archive:  text.zip
Length      Date       Time       Name
-----
0  2025-09-30 15:50  text_dir/
0  2025-09-30 15:50  text_dir/file1.txt
0  2025-09-30 15:50  text_dir/file2.txt
-----
0                               3 files
serge_mugabo@DESKTOP-GOD:~/projects$
```

```
serge_mugabo@DESKTOP-GOD:~/projects$ touch newfile.txt # create the file
if needed
tar -rf archive.tar newfile.txt
serge_mugabo@DESKTOP-GOD:~/projects$
```

13. Backup rotation strategy

- **Daily incremental** → `rsync --link-dest`
- **Weekly full** → `tar -czf full_week_$(date +%F).tar.gz`
- **Monthly archive** → stored offsite, named `YYYY-MM.tar.gz`.
- **Auto cleanup** → `find /backups -mtime +90 -delete`.
- **Integrity check** → `tar -tvf` or `md5sum`.
- Naming prevents conflict: `backup_type_date.tar.gz`.

Q14. User access troubleshooting

commands:

#Current user context

`id`

#Compare groups

`groups user1 groups user2`

#/etc/passwd patterns

`cat /etc/passwd`

Screenshot:

```
serge_mugabo@DESKTOP-GOD:~/projects$ id
uid=1000(serge_mugabo) gid=1000(serge_mugabo) groups=1000(serge_mugabo),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),100(users)
serge_mugabo@DESKTOP-GOD:~/projects$ groups serge_mugabo
serge_mugabo : serge_mugabo adm cdrom sudo dip plugdev users
serge_mugabo@DESKTOP-GOD:~/projects$ groups root
root : root
serge_mugabo@DESKTOP-GOD:~/projects$

serge_mugabo@DESKTOP-GOD:~/projects$ 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:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
systemd-timesync:x:996:996:systemd Time Synchronization:/:/usr/sbin/nologin
dhcpcd:x:100:65534:DHCP Client Daemon,,,:/usr/lib/dhcpcd:/bin/false
messagebus:x:101:101::/nonexistent:/usr/sbin/nologin
syslog:x:102:102::/nonexistent:/usr/sbin/nologin
systemd-resolve:x:991:991:systemd Resolver:/:/usr/sbin/nologin
uidd:x:103:103::/run/uidd:/usr/sbin/nologin
landscape:x:104:105::/var/lib/landscape:/usr/sbin/nologin
polkitd:x:990:990:User for polkitd:/:/usr/sbin/nologin
serge_mugabo:x:1000:1000:,,,:/home/serge_mugabo:/bin/bash
serge_mugabo@DESKTOP-GOD:~/projects$
```

15. Group membership propagation

Commands:

#Current vs configured

id groups

#Requires re-login

su - user

#Groups for logs/web/admin

ls -l /var/log | grep group ls -ld /var/www cat /etc/sudoers

#Principle of least privilege

→ Users only in groups needed for their tasks.

Screenshot:

```

root@DESKTOP-GOD:~# cat /etc/passwd | cut -d: -f1
root
daemon
bin
sys
sync
games
man
lp
mail
news
uucp
proxy
www-data
backup
list
irc
_apt
nobody
systemd-network
systemd-timesync
dhcpcd
messagebus
syslog
systemd-resolve
uidd
landscape
polkitd
serge_mugabo
root@DESKTOP-GOD:~# groups serge_mugabo
groups root
serge_mugabo : serge_mugabo adm cdrom sudo dip plugdev users
root : root
root@DESKTOP-GOD:~#

```

```

GNU nano 7.2 /etc/sudoers.tmp
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults      env_reset
Defaults      mail_badpass
Defaults      secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"

# This fixes CVE-2005-4890 and possibly breaks some versions of kdesu
# (#1011624, https://bugs.kde.org/show_bug.cgi?id=452532)
Defaults      use_pty

# This preserves proxy settings from user environments of root
# equivalent users (group sudo)
#Defaults:%sudo env_keep += "http_proxy https_proxy ftp_proxy all_proxy no_proxy"

# This allows running arbitrary commands, but so does ALL, and it means
# different sudoers have their choice of editor respected.
#Defaults:%sudo env_keep += "EDITOR"

Read 57 lines
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_ Go To Line  M-E Redo

```

Q16. Privilege escalation audit

commands:

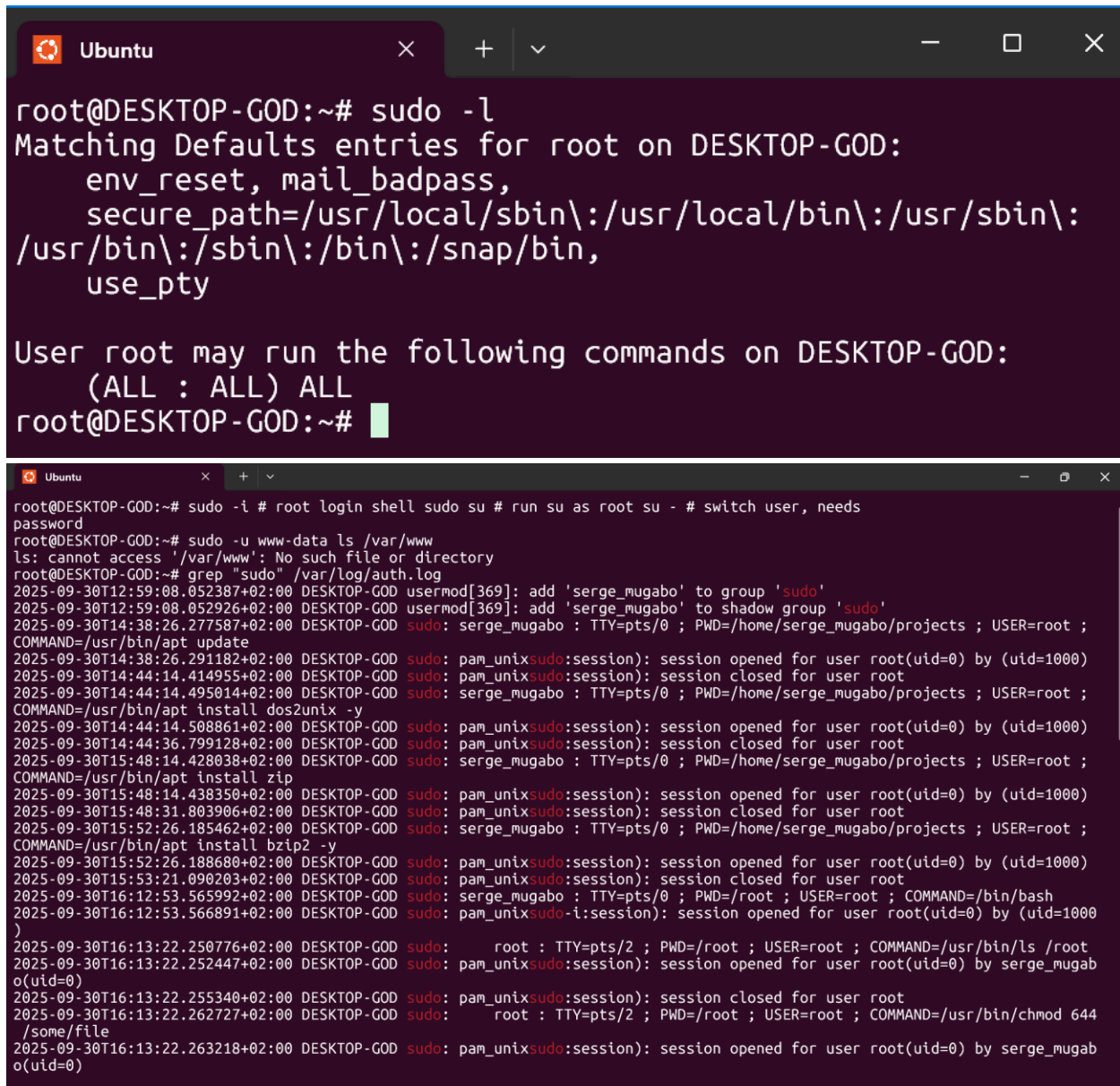
`sudo -l`

`sudo -i` # root login shell
`sudo su` # run su as root
`su -` # switch user, needs password

`sudo -u www-data ls /var/www`

`grep "sudo" /var/log/auth.log`

Screenshot:



The image shows two screenshots of a terminal window on an Ubuntu system. The top screenshot shows the output of the `sudo -l` command, displaying the matching Defaults entries for the root user on DESKTOP-GOD. The bottom screenshot shows the output of the `grep "sudo" /var/log/auth.log` command, displaying a series of audit logs for sudo sessions.

```
root@DESKTOP-GOD:~# sudo -l
Matching Defaults entries for root on DESKTOP-GOD:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User root may run the following commands on DESKTOP-GOD:
(ALL : ALL) ALL
root@DESKTOP-GOD:~#
```

```
root@DESKTOP-GOD:~# sudo -i # root login shell sudo su # run su as root su - # switch user, needs
password
root@DESKTOP-GOD:~# sudo -u www-data ls /var/www
ls: cannot access '/var/www': No such file or directory
root@DESKTOP-GOD:~# grep "sudo" /var/log/auth.log
2025-09-30T12:59:08.052387+02:00 DESKTOP-GOD usermod[369]: add 'serge_mugabo' to group 'sudo'
2025-09-30T12:59:08.052926+02:00 DESKTOP-GOD usermod[369]: add 'serge_mugabo' to shadow group 'sudo'
2025-09-30T14:38:26.277587+02:00 DESKTOP-GOD sudo: serge_mugabo : TTY=pts/0 ; PWD=/home/serge_mugabo/projects ; USER=root ;
COMMAND=/usr/bin/apt update
2025-09-30T14:38:26.291182+02:00 DESKTOP-GOD sudo: pam_unix:sudo:session): session opened for user root(uid=0) by (uid=1000)
2025-09-30T14:44:14.414955+02:00 DESKTOP-GOD sudo: pam_unix:sudo:session): session closed for user root
2025-09-30T14:44:14.495014+02:00 DESKTOP-GOD sudo: serge_mugabo : TTY=pts/0 ; PWD=/home/serge_mugabo/projects ; USER=root ;
COMMAND=/usr/bin/apt install dos2unix -y
2025-09-30T14:44:14.508861+02:00 DESKTOP-GOD sudo: pam_unix:sudo:session): session opened for user root(uid=0) by (uid=1000)
2025-09-30T14:44:36.799128+02:00 DESKTOP-GOD sudo: pam_unix:sudo:session): session closed for user root
2025-09-30T15:48:14.428038+02:00 DESKTOP-GOD sudo: serge_mugabo : TTY=pts/0 ; PWD=/home/serge_mugabo/projects ; USER=root ;
COMMAND=/usr/bin/apt install zip
2025-09-30T15:48:14.438350+02:00 DESKTOP-GOD sudo: pam_unix:sudo:session): session opened for user root(uid=0) by (uid=1000)
2025-09-30T15:48:31.803906+02:00 DESKTOP-GOD sudo: pam_unix:sudo:session): session closed for user root
2025-09-30T15:52:26.185462+02:00 DESKTOP-GOD sudo: serge_mugabo : TTY=pts/0 ; PWD=/home/serge_mugabo/projects ; USER=root ;
COMMAND=/usr/bin/apt install bzip2 -y
2025-09-30T15:52:26.188680+02:00 DESKTOP-GOD sudo: pam_unix:sudo:session): session opened for user root(uid=0) by (uid=1000)
2025-09-30T15:53:21.090203+02:00 DESKTOP-GOD sudo: pam_unix:sudo:session): session closed for user root
2025-09-30T16:12:53.565992+02:00 DESKTOP-GOD sudo: serge_mugabo : TTY=pts/0 ; PWD=/root ; USER=root ; COMMAND=/bin/bash
2025-09-30T16:12:53.566891+02:00 DESKTOP-GOD sudo: pam_unix:sudo-i:session): session opened for user root(uid=0) by (uid=1000)
)
2025-09-30T16:13:22.250776+02:00 DESKTOP-GOD sudo: root : TTY=pts/2 ; PWD=/root ; USER=root ; COMMAND=/usr/bin/ls /root
2025-09-30T16:13:22.252447+02:00 DESKTOP-GOD sudo: pam_unix:sudo:session): session opened for user root(uid=0) by serge_mugab
o(uid=0)
2025-09-30T16:13:22.255340+02:00 DESKTOP-GOD sudo: pam_unix:sudo:session): session closed for user root
2025-09-30T16:13:22.262727+02:00 DESKTOP-GOD sudo: root : TTY=pts/2 ; PWD=/root ; USER=root ; COMMAND=/usr/bin/chmod 644
/some/file
2025-09-30T16:13:22.263218+02:00 DESKTOP-GOD sudo: pam_unix:sudo:session): session opened for user root(uid=0) by serge_mugab
o(uid=0)
```

Q17. Forensic setup

commands:

```
mkdir forensic && cd forensic
```

```
touch regular.txt
```

```
mkdir dir
```

```
ln -s regular.txt symlink
```

```
ln regular.txt hardlink
```

```
mknod devicefile c 1 7
```

```
touch sticky; chmod +t sticky
```

```
touch suid; chmod u+s suid
```

```
touch sgid; chmod g+s sgid
```

```
chown root:root regular.txt
```

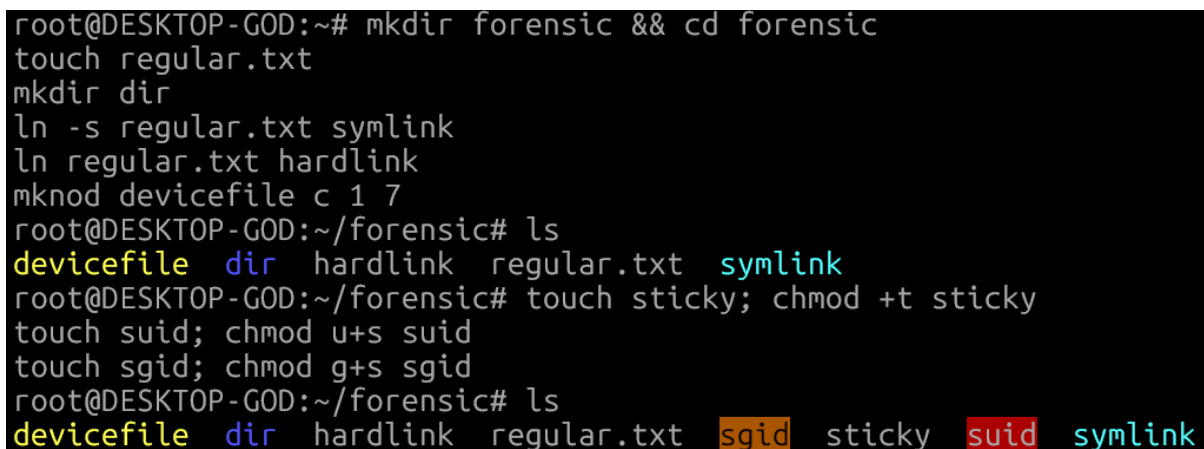
```
chown user1:user1 other.txt
```

```
tar -czf test.tar.gz *
```

```
zip test.zip *
```

```
ls -l, stat, file, tar -tvf, unzip -l
```

Screenshot:



```
root@DESKTOP-GOD:~# mkdir forensic && cd forensic
touch regular.txt
mkdir dir
ln -s regular.txt symlink
ln regular.txt hardlink
mknod devicefile c 1 7
root@DESKTOP-GOD:~/forensic# ls
devicefile  dir  hardlink  regular.txt  symlink
root@DESKTOP-GOD:~/forensic# touch sticky; chmod +t sticky
touch suid; chmod u+s suid
touch sgid; chmod g+s sgid
root@DESKTOP-GOD:~/forensic# ls
devicefile  dir  hardlink  regular.txt  sgid  sticky  suid  symlink
```

```
root@DESKTOP-GOD:~/forensic# cd ~/forensic
ls -l
echo "forensic test" > other.txt
sudo adduser user1          # only if user1 doesn't exist
chown user1:user1 other.txt
total 8
crw-r--r-- 1 root  root  1, 7 Sep 27 20:06 devicefile
drwxr-xr-x 2 root  root 4096 Sep 27 20:06 dir
-rw-r--r-- 2 root  root   0 Sep 27 20:06 hardlink
-rw-r--r-- 1 user1 user1 14 Sep 27 20:08 other.txt
-rw-r--r-- 2 root  root   0 Sep 27 20:06 regular.txt
-rw-r-Sr-- 1 root  root   0 Sep 27 20:06 sgid
-rw-r--r-T 1 root  root   0 Sep 27 20:06 sticky
-rwSr--r-- 1 root  root   0 Sep 27 20:06 suid
lrwxrwxrwx 1 root  root  11 Sep 27 20:06 symlink -> regular.txt
root@DESKTOP-GOD:~/forensic# chown root:root regular.txt
chown user1:user1 other.txt
root@DESKTOP-GOD:~/forensic# tar -czf test.tar.gz *
zip test.zip *
    zip warning: ignoring special file: devicefile
adding: dir/ (stored 0%)
adding: hardlink (stored 0%)
adding: other.txt (stored 0%)
adding: regular.txt (stored 0%)
adding: sgid (stored 0%)
adding: sticky (stored 0%)
adding: suid (stored 0%)
adding: symlink (stored 0%)
adding: test.tar.gz (stored 0%)
```

```

root@DESKTOP-GOD:~/forensic# ls -l ; stat regular.txt ; file regular.txt ; tar -tvf test.tar.gz ; unzip -l test.zip
total 16
crw-r--r-- 1 root root 1, 7 Sep 27 20:06 devicefile
drwxr-xr-x 2 root root 4096 Sep 27 20:06 dir
-rw-r--r-- 2 root root 0 Sep 27 20:06 hardlink
-rw-r--r-- 1 user1 user1 14 Sep 27 20:08 other.txt
-rw-r--r-- 2 root root 0 Sep 27 20:06 regular.txt
-rw-r--r-- 1 root root 0 Sep 27 20:06 sgid
-rw-r--r-- 1 root root 0 Sep 27 20:06 sticky
-rwSr--r-- 1 root root 0 Sep 27 20:06 suid
lrwxrwxrwx 1 root root 11 Sep 27 20:06 symlink -> regular.txt
-rw-r--r-- 1 root root 322 Sep 27 20:10 test.tar.gz
-rw-r--r-- 1 root root 1638 Sep 27 20:10 test.zip
File: regular.txt
Size: 0          Blocks: 0          IO Block: 4096   regular empty file
Device: 8,48    Inode: 44977       Links: 2
Access: (0644/-rw-r--r--)  Uid: ( 0/   root)   Gid: ( 0/   root)
Access: 2025-09-27 20:10:12.546565477 +0200
Modify: 2025-09-27 20:06:24.887787284 +0200
Change: 2025-09-27 20:10:02.011978842 +0200
Birth: 2025-09-27 20:06:24.887787284 +0200
regular.txt: empty
crw-r--r-- root/root      1,7 2025-09-27 20:06 devicefile
drwxr-xr-x root/root      0 2025-09-27 20:06 dir/
-rw-r--r-- root/root      0 2025-09-27 20:06 hardlink
-rw-r--r-- user1/user1    14 2025-09-27 20:08 other.txt
lrwxr--r-- root/root      0 2025-09-27 20:06 regular.txt link to hardlink
-rw-r--r-- root/root      0 2025-09-27 20:06 sgid
-rw-r--r-- root/root      0 2025-09-27 20:06 sticky
-rwSr--r-- root/root      0 2025-09-27 20:06 suid
lrwxrwxrwx root/root      0 2025-09-27 20:06 symlink -> regular.txt
Archive: test.zip
Length      Date       Time      Name
-----
0 2025-09-27 20:06 dir/
0 2025-09-27 20:06 hardlink
14 2025-09-27 20:08 other.txt
0 2025-09-27 20:06 regular.txt
0 2025-09-27 20:06 sgid
0 2025-09-27 20:06 sticky
0 2025-09-27 20:06 suid
0 2025-09-27 20:06 symlink
322 2025-09-27 20:10 test.tar.gz
-----
336
9 files
root@DESKTOP-GOD:~/forensic#

```