

# Assignment2

Name: AZE Solide

ID: 27396

Email: solideaze1251@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:**

```
solide@DESKTOP-GOD:~$ mkdir -p ~/projects/{client_work/{web/{frontend,backend},mobile},personal/{experiments,notes},shared/{templates,docs}}
solide@DESKTOP-GOD:~$ ls
Introduction_to_linux  command  projects
solide@DESKTOP-GOD:~$
```

## Q3. Navigation with ≤3 cd

**commands:**

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

```
pwd
```

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

```
pwd
```

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

```
pwd
```

### Screenshot:

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

```
solide@DESKTOP-GOD:~/projects/client_work/web/frontend$ ls
about.html  index.html  page_002.html  page_004.html  page_006.html  page_008.html  page_010.html
contact.html  page_001.html  page_003.html  page_005.html  page_007.html  page_009.html  page_012.html
solide@DESKTOP-GOD:~/projects/client_work/web/frontend$ touch index.html about.html contact.html page_{001,002,003,004,005,006,007,008,009,010,012}.html █
```

```

solide@DESKTOP-GOD:~/projects/client_work/web/frontend$ touch {script1,script2,util1,util2,config1,config2}.js
solide@DESKTOP-GOD:~/projects/client_work/web/frontend$ ls
about.html    desktop.css  page_001.html  page_005.html  page_009.html  reset.css    theme_dark.css
config1.js    index.html   page_002.html  page_006.html  page_010.html  script1.js   theme_light.css
config2.js    main.css     page_003.html  page_007.html  page_012.html  script2.js   util1.js
contact.html  mobile.css   page_004.html  page_008.html  print.css      tablet.css   util2.js
solide@DESKTOP-GOD:~/projects/client_work/web/frontend$

solide@DESKTOP-GOD:~/projects/client_work/web/frontend$ touch {a,b,c,d}{1,2,3,4,5}.bak
solide@DESKTOP-GOD:~/projects/client_work/web/frontend$ ls
a1.bak    b1.bak    c2.bak    contact.html  desktop.css  page_003.html  page_009.html  script2.js
a2.bak    b2.bak    c3.bak    d1.bak        index.html   page_004.html  page_010.html  tablet.css
a3.bak    b3.bak    c4.bak    d2.bak        main.css     page_005.html  page_012.html  theme_dark.css
a4.bak    b4.bak    c5.bak    d3.bak        mobile.css   page_006.html  print.css      theme_light.css
a5.bak    b5.bak    config1.js d4.bak        page_001.html page_007.html  reset.css      util1.js
about.html c1.bak    config2.js d5.bak        page_002.html page_008.html  script1.js     util2.js
solide@DESKTOP-GOD:~/projects/client_work/web/frontend$

solide@DESKTOP-GOD:~/projects/client_work/web/frontend$ touch {main,reset,theme_light,theme_dark,mobile,tablet,desktop,print}.css
solide@DESKTOP-GOD:~/projects/client_work/web/frontend$ ls
about.html    main.css    page_003.html  page_007.html  page_012.html  theme_dark.css
contact.html  mobile.css  page_004.html  page_008.html  print.css      theme_light.css
desktop.css   page_001.html page_005.html  page_009.html  reset.css
index.html    page_002.html page_006.html  page_010.html  tablet.css
solide@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:*

```

solide@DESKTOP-GOD:~/projects/client_work/web/frontend$ ls
about.html  desktop.css  main.css    print.css  tablet.css  theme_light.css
contact.html index.html  mobile.css  reset.css  theme_dark.css
solide@DESKTOP-GOD:~/projects/client_work/web/frontend$ cd ../../../../archive/
solide@DESKTOP-GOD:~/projects/archive$ ls
a1.bak  b1.bak  c1.bak  config1.js  d4.bak      page_004.html  page_009.html  util1.js
a2.bak  b2.bak  c2.bak  config2.js  d5.bak      page_005.html  page_010.html  util2.js
a3.bak  b3.bak  c3.bak  d1.bak      page_001.html  page_006.html  page_012.html
a4.bak  b4.bak  c4.bak  d2.bak      page_002.html  page_007.html  script1.js
a5.bak  b5.bak  c5.bak  d3.bak      page_003.html  page_008.html  script2.js
solide@DESKTOP-GOD:~/projects/archive$ cd ../../desktop/
solide@DESKTOP-GOD:~/projects/desktop$ ls
desktop.css  main.css  print.css  reset.css  theme_dark.css  theme_light.css
solide@DESKTOP-GOD:~/projects/desktop$ █

```

## 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:*

```

solide@DESKTOP-GOD:~/projects$ touch {web,api,db}_{dev,staging,prod}.conf
solide@DESKTOP-GOD:~/projects$ ls
api_dev.conf      log_2024-01-10.txt  log_2024-01-28.txt  log_2024-02-15.txt  log_2024-03-02.txt  log_2024-03-20.txt
api_prod.conf     log_2024-01-11.txt  log_2024-01-29.txt  log_2024-02-16.txt  log_2024-03-03.txt  log_2024-03-21.txt
api_staging.conf  log_2024-01-12.txt  log_2024-01-30.txt  log_2024-02-17.txt  log_2024-03-04.txt  log_2024-03-22.txt
archive           log_2024-01-13.txt  log_2024-01-31.txt  log_2024-02-18.txt  log_2024-03-05.txt  log_2024-03-23.txt
client_work       log_2024-01-14.txt  log_2024-02-01.txt  log_2024-02-19.txt  log_2024-03-06.txt  log_2024-03-24.txt
db_dev.conf       log_2024-01-15.txt  log_2024-02-02.txt  log_2024-02-20.txt  log_2024-03-07.txt  log_2024-03-25.txt
db_prod.conf      log_2024-01-16.txt  log_2024-02-03.txt  log_2024-02-21.txt  log_2024-03-08.txt  log_2024-03-26.txt
db_staging.conf   log_2024-01-17.txt  log_2024-02-04.txt  log_2024-02-22.txt  log_2024-03-09.txt  log_2024-03-27.txt
desktop           log_2024-01-18.txt  log_2024-02-05.txt  log_2024-02-23.txt  log_2024-03-10.txt  log_2024-03-28.txt
log_2024-01-01.txt log_2024-01-19.txt  log_2024-02-06.txt  log_2024-02-24.txt  log_2024-03-11.txt  log_2024-03-29.txt
log_2024-01-02.txt log_2024-01-20.txt  log_2024-02-07.txt  log_2024-02-25.txt  log_2024-03-12.txt  log_2024-03-30.txt
log_2024-01-03.txt log_2024-01-21.txt  log_2024-02-08.txt  log_2024-02-26.txt  log_2024-03-13.txt  log_2024-03-31.txt
log_2024-01-04.txt log_2024-01-22.txt  log_2024-02-09.txt  log_2024-02-27.txt  log_2024-03-14.txt  personal
log_2024-01-05.txt log_2024-01-23.txt  log_2024-02-10.txt  log_2024-02-28.txt  log_2024-03-15.txt  shared
log_2024-01-06.txt log_2024-01-24.txt  log_2024-02-11.txt  log_2024-02-29.txt  log_2024-03-16.txt  web_dev.conf
log_2024-01-07.txt log_2024-01-25.txt  log_2024-02-12.txt  log_2024-02-30.txt  log_2024-03-17.txt  web_prod.conf
log_2024-01-08.txt log_2024-01-26.txt  log_2024-02-13.txt  log_2024-02-31.txt  log_2024-03-18.txt  web_staging.conf
log_2024-01-09.txt log_2024-01-27.txt  log_2024-02-14.txt  log_2024-03-01.txt  log_2024-03-19.txt
solide@DESKTOP-GOD:~/projects$ █

```

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

```
solide@DESKTOP-GOD:~/projects$ ls
archive client_work desktop personal shared
solide@DESKTOP-GOD:~/projects$ touch log_2024-{01,02,03}-{01..31}.txt
solide@DESKTOP-GOD:~/projects$ ls
archive          log_2024-01-18.txt  log_2024-02-07.txt  log_2024-02-27.txt  log_2024-03-16.txt
client_work      log_2024-01-19.txt  log_2024-02-08.txt  log_2024-02-28.txt  log_2024-03-17.txt
desktop         log_2024-01-20.txt  log_2024-02-09.txt  log_2024-02-29.txt  log_2024-03-18.txt
log_2024-01-01.txt log_2024-01-21.txt  log_2024-02-10.txt  log_2024-02-30.txt  log_2024-03-19.txt
log_2024-01-02.txt log_2024-01-22.txt  log_2024-02-11.txt  log_2024-02-31.txt  log_2024-03-20.txt
log_2024-01-03.txt log_2024-01-23.txt  log_2024-02-12.txt  log_2024-03-01.txt  log_2024-03-21.txt
log_2024-01-04.txt log_2024-01-24.txt  log_2024-02-13.txt  log_2024-03-02.txt  log_2024-03-22.txt
log_2024-01-05.txt log_2024-01-25.txt  log_2024-02-14.txt  log_2024-03-03.txt  log_2024-03-23.txt
log_2024-01-06.txt log_2024-01-26.txt  log_2024-02-15.txt  log_2024-03-04.txt  log_2024-03-24.txt
log_2024-01-07.txt log_2024-01-27.txt  log_2024-02-16.txt  log_2024-03-05.txt  log_2024-03-25.txt
log_2024-01-08.txt log_2024-01-28.txt  log_2024-02-17.txt  log_2024-03-06.txt  log_2024-03-26.txt
log_2024-01-09.txt log_2024-01-29.txt  log_2024-02-18.txt  log_2024-03-07.txt  log_2024-03-27.txt
log_2024-01-10.txt log_2024-01-30.txt  log_2024-02-19.txt  log_2024-03-08.txt  log_2024-03-28.txt
log_2024-01-11.txt log_2024-01-31.txt  log_2024-02-20.txt  log_2024-03-09.txt  log_2024-03-29.txt
log_2024-01-12.txt log_2024-02-01.txt  log_2024-02-21.txt  log_2024-03-10.txt  log_2024-03-30.txt
log_2024-01-13.txt log_2024-02-02.txt  log_2024-02-22.txt  log_2024-03-11.txt  log_2024-03-31.txt
log_2024-01-14.txt log_2024-02-03.txt  log_2024-02-23.txt  log_2024-03-12.txt  personal
log_2024-01-15.txt log_2024-02-04.txt  log_2024-02-24.txt  log_2024-03-13.txt  shared
log_2024-01-16.txt log_2024-02-05.txt  log_2024-02-25.txt  log_2024-03-14.txt
log_2024-01-17.txt log_2024-02-06.txt  log_2024-02-26.txt  log_2024-03-15.txt
solide@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:*

```
solide@DESKTOP-GOD:~/projects$ echo -e "This is a test file\nAnother line" > linux.txt
unix2dos linux.txt win.txt
unix2dos: converting file linux.txt to DOS format...
unix2dos: converting file win.txt to DOS format...
solide@DESKTOP-GOD:~/projects$ diff linux.txt win.txt
2a3
>
solide@DESKTOP-GOD:~/projects$ cmp linux.txt win.txt
cmp: EOF on linux.txt after byte 35, line 2
solide@DESKTOP-GOD:~/projects$ sort linux.txt -o linux.txt
sort win.txt -o win.txt
comm linux.txt win.txt

        Another line
        This is a test file
solide@DESKTOP-GOD:~/projects$
```

## 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:



```
solide@DESKTOP-GOD:~/projects$ find . -type f -size +$((du -cb * | grep total | cut -f1)/$(ls -l | wc -l)))c
./win.txt
./linux.txt
solide@DESKTOP-GOD:~/projects$ find . -type f -mtime -3 ! -mtime -1
solide@DESKTOP-GOD:~/projects$ find . -type d -empty -o -type d -exec sh -c 'ls -A "$1" | grep -q "^[.]" && echo "$1" _ {}' \;
find . -type f -perm -002
find . ! -user $(whoami) ! -user root
find . -type f \( -name '*~' -o -name '*.bak' -o -name '*.tmp' \)
./archive/a1.bak
./archive/a5.bak
./archive/d4.bak
./archive/b2.bak
./archive/b1.bak
./archive/c3.bak
./archive/d1.bak
./archive/d5.bak
./archive/d3.bak
./archive/d2.bak
./archive/c4.bak
./archive/a4.bak
./archive/a3.bak
./archive/b3.bak
./archive/b4.bak
./archive/a2.bak
./archive/c5.bak
./archive/b5.bak
./archive/c2.bak
./archive/c1.bak
solide@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:*

```
solide@DESKTOP-GOD:~/projects$ grep -n "ERROR" logfile.txt | tail -1
LINE=$(grep -n "ERROR" logfile.txt | tail -1 | cut -d: -f1)
tail -n +${(LINE-5)} logfile.txt | head -10
255:ERROR at line 250
250
ERROR at line 50
ERROR at line 100
ERROR at line 150
ERROR at line 200
ERROR at line 250

solide@DESKTOP-GOD:~/projects$ grep -n "ERROR" logfile.txt
251:ERROR at line 50
252:ERROR at line 100
253:ERROR at line 150
254:ERROR at line 200
255:ERROR at line 250
solide@DESKTOP-GOD:~/projects$ █
```



```
solide@DESKTOP-GOD:~/projects$ sed -n '76,125p' logfile.txt
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106

solide@DESKTOP-GOD:~/projects$ time cat logfile.txt > /dev/null
time less logfile.txt > /dev/null

real    0m0.003s
user    0m0.002s
sys     0m0.001s

real    0m0.017s
user    0m0.004s
sys     0m0.009s
```

## 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:

```
solide@DESKTOP-GOD:~/projects$ find . -type f ! -perm -755 -exec chmod 644 {} \;
solide@DESKTOP-GOD:~/projects$ find . -type f -mtime +30 -exec du -ch {} + | tail -1
solide@DESKTOP-GOD:~/projects$ find . -name "*.conf" -exec cp {} {}.backup \;
solide@DESKTOP-GOD:~/projects$ find . -name "*.tmp" -atime +7 -delete
solide@DESKTOP-GOD:~/projects$ ls
A10_input.txt      db_prod.conf      log_2024-01-23.txt  log_2024-02-20.txt  log_2024-03-17.txt
A10_output.txt     db_prod.conf.backup  log_2024-01-24.txt  log_2024-02-21.txt  log_2024-03-18.txt
A11_input.txt      db_staging.conf    log_2024-01-25.txt  log_2024-02-22.txt  log_2024-03-19.txt
A11_output.txt     db_staging.conf.backup  log_2024-01-26.txt  log_2024-02-23.txt  log_2024-03-20.txt
A12_input.txt      desktop           log_2024-01-27.txt  log_2024-02-24.txt  log_2024-03-21.txt
A12_output.txt     linux.txt         log_2024-01-28.txt  log_2024-02-25.txt  log_2024-03-22.txt
B10_input.txt      log_2024-01-01.txt  log_2024-01-29.txt  log_2024-02-26.txt  log_2024-03-23.txt
B10_output.txt     log_2024-01-02.txt  log_2024-01-30.txt  log_2024-02-27.txt  log_2024-03-24.txt
B11_input.txt      log_2024-01-03.txt  log_2024-01-31.txt  log_2024-02-28.txt  log_2024-03-25.txt
B11_output.txt     log_2024-01-04.txt  log_2024-02-01.txt  log_2024-02-29.txt  log_2024-03-26.txt
B12_input.txt      log_2024-01-05.txt  log_2024-02-02.txt  log_2024-02-30.txt  log_2024-03-27.txt
B12_output.txt     log_2024-01-06.txt  log_2024-02-03.txt  log_2024-02-31.txt  log_2024-03-28.txt
C10_input.txt      log_2024-01-07.txt  log_2024-02-04.txt  log_2024-03-01.txt  log_2024-03-29.txt
C10_output.txt     log_2024-01-08.txt  log_2024-02-05.txt  log_2024-03-02.txt  log_2024-03-30.txt
C11_input.txt      log_2024-01-09.txt  log_2024-02-06.txt  log_2024-03-03.txt  log_2024-03-31.txt
C11_output.txt     log_2024-01-10.txt  log_2024-02-07.txt  log_2024-03-04.txt  logfile.txt
C12_input.txt      log_2024-01-11.txt  log_2024-02-08.txt  log_2024-03-05.txt  personal
C12_output.txt     log_2024-01-12.txt  log_2024-02-09.txt  log_2024-03-06.txt  shared
api_dev.conf       log_2024-01-13.txt  log_2024-02-10.txt  log_2024-03-07.txt  web_dev.conf
api_dev.conf.backup  log_2024-01-14.txt  log_2024-02-11.txt  log_2024-03-08.txt  web_dev.conf.backup
api_prod.conf       log_2024-01-15.txt  log_2024-02-12.txt  log_2024-03-09.txt  web_prod.conf
api_prod.conf.backup  log_2024-01-16.txt  log_2024-02-13.txt  log_2024-03-10.txt  web_prod.conf.backup
api_staging.conf    log_2024-01-17.txt  log_2024-02-14.txt  log_2024-03-11.txt  web_staging.conf
api_staging.conf.backup  log_2024-01-18.txt  log_2024-02-15.txt  log_2024-03-12.txt  web_staging.conf.backup
archive            log_2024-01-19.txt  log_2024-02-16.txt  log_2024-03-13.txt  win.txt
client_work        log_2024-01-20.txt  log_2024-02-17.txt  log_2024-03-14.txt
db_dev.conf         log_2024-01-21.txt  log_2024-02-18.txt  log_2024-03-15.txt
db_dev.conf.backup  log_2024-01-22.txt  log_2024-02-19.txt  log_2024-03-16.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:*

```
solide@DESKTOP-GOD:~/projects$ ls
mkdir text_dir
echo "sample text" > text_dir/file1.txt
A10_input.txt      db_prod.conf      log_2024-01-23.txt  log_2024-02-20.txt  log_2024-03-17.txt
A10_output.txt     db_prod.conf.backup log_2024-01-24.txt  log_2024-02-21.txt  log_2024-03-18.txt
A11_input.txt      db_staging.conf    log_2024-01-25.txt  log_2024-02-22.txt  log_2024-03-19.txt
A11_output.txt     db_staging.conf.backup log_2024-01-26.txt  log_2024-02-23.txt  log_2024-03-20.txt
A12_input.txt      desktop            log_2024-01-27.txt  log_2024-02-24.txt  log_2024-03-21.txt
A12_output.txt     linux.txt          log_2024-01-28.txt  log_2024-02-25.txt  log_2024-03-22.txt
B10_input.txt      log_2024-01-01.txt  log_2024-01-29.txt  log_2024-02-26.txt  log_2024-03-23.txt
B10_output.txt     log_2024-01-02.txt  log_2024-01-30.txt  log_2024-02-27.txt  log_2024-03-24.txt
B11_input.txt      log_2024-01-03.txt  log_2024-01-31.txt  log_2024-02-28.txt  log_2024-03-25.txt
B11_output.txt     log_2024-01-04.txt  log_2024-02-01.txt  log_2024-02-29.txt  log_2024-03-26.txt
B12_input.txt      log_2024-01-05.txt  log_2024-02-02.txt  log_2024-02-30.txt  log_2024-03-27.txt
B12_output.txt     log_2024-01-06.txt  log_2024-02-03.txt  log_2024-02-31.txt  log_2024-03-28.txt
C10_input.txt      log_2024-01-07.txt  log_2024-02-04.txt  log_2024-03-01.txt  log_2024-03-29.txt
C10_output.txt     log_2024-01-08.txt  log_2024-02-05.txt  log_2024-03-02.txt  log_2024-03-30.txt
C11_input.txt      log_2024-01-09.txt  log_2024-02-06.txt  log_2024-03-03.txt  log_2024-03-31.txt
C11_output.txt     log_2024-01-10.txt  log_2024-02-07.txt  log_2024-03-04.txt  logfile.txt
C12_input.txt      log_2024-01-11.txt  log_2024-02-08.txt  log_2024-03-05.txt  personal
C12_output.txt     log_2024-01-12.txt  log_2024-02-09.txt  log_2024-03-06.txt  shared
api_dev.conf       log_2024-01-13.txt  log_2024-02-10.txt  log_2024-03-07.txt  text.tar.bz2
api_dev.conf.backup log_2024-01-14.txt  log_2024-02-11.txt  log_2024-03-08.txt  text.tar.gz
api_prod.conf      log_2024-01-15.txt  log_2024-02-12.txt  log_2024-03-09.txt  text.tar.xz
api_prod.conf.backup log_2024-01-16.txt  log_2024-02-13.txt  log_2024-03-10.txt  web_dev.conf
api_staging.conf   log_2024-01-17.txt  log_2024-02-14.txt  log_2024-03-11.txt  web_dev.conf.backup
api_staging.conf.backup log_2024-01-18.txt  log_2024-02-15.txt  log_2024-03-12.txt  web_prod.conf
archive            log_2024-01-19.txt  log_2024-02-16.txt  log_2024-03-13.txt  web_prod.conf.backup
client_work        log_2024-01-20.txt  log_2024-02-17.txt  log_2024-03-14.txt  web_staging.conf
db_dev.conf         log_2024-01-21.txt  log_2024-02-18.txt  log_2024-03-15.txt  web_staging.conf.backup
db_dev.conf.backup log_2024-01-22.txt  log_2024-02-19.txt  log_2024-03-16.txt  win.txt
solide@DESKTOP-GOD:~/projects$
```

```
solide@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
  adding: text_dir/ (stored 0%)
  adding: text_dir/file1.txt (stored 0%)
solide@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:

```
solide@DESKTOP-GOD:~/projects$ mkdir test_dir
echo "hello" > test_dir/file1.txt
echo "world" > test_dir/file2.conf

tar -cf archive.tar test_dir
zip -r archive.zip test_dir
  adding: test_dir/ (stored 0%)
  adding: test_dir/file1.txt (stored 0%)
  adding: test_dir/file2.conf (stored 0%)
solide@DESKTOP-GOD:~/projects$ tar -tf archive.tar
unzip -l archive.zip
test_dir/
test_dir/file1.txt
test_dir/file2.conf
Archive:  archive.zip
  Length      Date    Time    Name
  ----
  0      2025-09-27  18:04    test_dir/
  6      2025-09-27  18:04    test_dir/file1.txt
  6      2025-09-27  18:04    test_dir/file2.conf
  ----
  12
  3 files
solide@DESKTOP-GOD:~/projects$ echo "new content" > newfile.txt
tar -rf archive.tar newfile.txt

solide@DESKTOP-GOD:~/projects/demo_dir$ cd ..
solide@DESKTOP-GOD:~/projects$ zip -s 1m bad.zip demo_dir/*
  adding: demo_dir/file1.txt (stored 0%)
  adding: demo_dir/file2.txt (stored 0%)
solide@DESKTOP-GOD:~/projects$ zip -FF bad.zip --out fixed.zip
unzip fixed.zip
Fix archive (-FF) - salvage what can
Found end record (EOCDR) - says expect single disk archive
Scanning for entries...
Found spanning marker, but did not expect split (multi-disk) archive...
copying: demo_dir/file1.txt (9 bytes)
copying: demo_dir/file2.txt (9 bytes)
Central Directory found...
EOCDR found ( 1 350)...
Archive:  fixed.zip
replace demo_dir/file1.txt? [y]es, [n]o, [A]ll, [N]one, [r]ename: y
extracting: demo_dir/file1.txt
replace demo_dir/file2.txt? [y]es, [n]o, [A]ll, [N]one, [r]ename: A
extracting: demo_dir/file2.txt
solide@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:*

```
solide@DESKTOP-GOD:~/projects$ sudo adduser user1
sudo adduser user2
[sudo] password for solide:
info: Adding user `user1' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `user1' (1001) ...
info: Adding new user `user1' (1001) with group `user1 (1001)' ...
info: Creating home directory `/home/user1' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for user1
Enter the new value, or press ENTER for the default
    Full Name []: Solide
    Room Number []: 12
    Work Phone []: 0796606714
    Home Phone []: 555-555-555
    Other []:
Is the information correct? [Y/n] Y
info: Adding new user `user1' to supplemental / extra groups `users' ...
info: Adding user `user1' to group `users' ...
info: Adding user `user2' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `user2' (1002) ...
info: Adding new user `user2' (1002) with group `user2 (1002)' ...
info: Creating home directory `/home/user2' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
Sorry, passwords do not match.
passwd: Authentication token manipulation error
passwd: password unchanged
Try again? [y/N] y
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for user2
Enter the new value, or press ENTER for the default
    Full Name []: AZE
    Room Number []: 11
    Work Phone []: 0780384068
    Home Phone []:
    Other []:
Is the information correct? [Y/n] Y
info: Adding new user `user2' to supplemental / extra groups `users' ...
info: Adding user `user2' to group `users' ...
```

```

solide@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
solide:x:1000:1000::,/home/solide:/bin/bash
user1:x:1001:1001:Solide,12,0796606714,555-555-555:/home/user1:/bin/bash
user2:x:1002:1002:AZE,11,0780384068,:/home/user2:/bin/bash
solide@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:*

```
solide@DESKTOP-GOD:~$ sudo apt update
sudo apt install apache2
Hit:1 http://security.ubuntu.com/ubuntu noble-security InRelease
Hit:2 http://archive.ubuntu.com/ubuntu noble InRelease
Get:3 http://archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Hit:4 http://archive.ubuntu.com/ubuntu noble-backports InRelease
Get:5 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [1443 kB]
Get:6 http://archive.ubuntu.com/ubuntu noble-updates/universe amd64 Packages [1485 kB]
Fetched 3054 kB in 4s (691 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
17 packages can be upgraded. Run 'apt list --upgradable' to see them.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils libapr1t64 libaprutil1-dbd-sqlite3 libaprutil1-ldap libaprutil1t64
  liblua5.4-0 ssl-cert
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom www-browser ufw
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils libapr1t64 libaprutil1-dbd-sqlite3 libaprutil1-ldap
  libaprutil1t64 liblua5.4-0 ssl-cert
0 upgraded, 10 newly installed, 0 to remove and 17 not upgraded.
Need to get 2086 kB of archives.
After this operation, 8090 kB of additional disk space will be used.
```

```
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

solide@DESKTOP-GOD:~$ ls -l /var/log | grep group
ls -ld /var/www
cat /etc/sudoers
→ Users only in groups needed for their tasks.
drwxr-xr-x 3 solide solide 4096 Sep 27 19:59 /var/www
cat: /etc/sudoers: Permission denied
→: command not found
solide@DESKTOP-GOD:~$
```

## 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:*

```

solide@DESKTOP-GOD:~$ sudo -i
sudo su
su -
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.6.87.2-microsoft-standard-WSL2 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of Sat Sep 27 20:04:03 SAST 2025

System load:  0.03          Processes:            38
Usage of /:   0.2% of 1006.85GB Users logged in:       1
Memory usage: 5%          IPv4 address for eth0: 172.18.160.83
Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

https://ubuntu.com/engage/secure-kubernetes-at-the-edge

This message is shown once a day. To disable it please create the
/root/.hushlogin file.
root@DESKTOP-GOD:~# █

root@DESKTOP-GOD:~# sudo -u www-data ls /var/www
html
root@DESKTOP-GOD:~# grep "sudo" /var/log/auth.log
2025-09-23T13:18:43.491711+02:00 DESKTOP-GOD usermod[429]: add 'solide' to group 'sudo'
2025-09-23T13:18:43.491957+02:00 DESKTOP-GOD usermod[429]: add 'solide' to shadow group 'sudo'
2025-09-23T15:39:28.403300+02:00 DESKTOP-GOD sudo:    solide : TTY=pts/0 ; PWD=/home/solide ; USER=root ; COMMAND
=/usr/bin/apt update
2025-09-23T15:39:28.404815+02:00 DESKTOP-GOD sudo: pam_unix(sudo:session): session opened for user root(uid=0) b
y (uid=1000)
2025-09-23T15:39:53.258468+02:00 DESKTOP-GOD sudo: pam_unix(sudo:session): session closed for user root
2025-09-23T15:39:53.280651+02:00 DESKTOP-GOD sudo:    solide : TTY=pts/0 ; PWD=/home/solide ; USER=root ; COMMAND
=/usr/bin/apt install git -y
2025-09-23T15:39:53.283571+02:00 DESKTOP-GOD sudo: pam_unix(sudo:session): session opened for user root(uid=0) b
y (uid=1000)
2025-09-23T15:39:54.543082+02:00 DESKTOP-GOD sudo: pam_unix(sudo:session): session closed for user root
2025-09-27T17:17:33.502244+02:00 DESKTOP-GOD sudo:    solide : TTY=pts/0 ; PWD=/home/solide/projects ; USER=root
; COMMAND=/usr/bin/apt install dos2unix
2025-09-27T17:17:33.507192+02:00 DESKTOP-GOD sudo: pam_unix(sudo:session): session opened for user root(uid=0) b
y (uid=1000)
2025-09-27T17:17:38.718905+02:00 DESKTOP-GOD sudo: pam_unix(sudo:session): session closed for user root
2025-09-27T17:58:02.993509+02:00 DESKTOP-GOD sudo:    solide : TTY=pts/0 ; PWD=/home/solide/projects ; USER=root
; COMMAND=/usr/bin/apt update
2025-09-27T17:58:03.001537+02:00 DESKTOP-GOD sudo: pam_unix(sudo:session): session opened for user root(uid=0) b
y (uid=1000)
2025-09-27T17:58:10.395454+02:00 DESKTOP-GOD sudo: pam_unix(sudo:session): session closed for user root
2025-09-27T17:58:10.402937+02:00 DESKTOP-GOD sudo:    solide : TTY=pts/0 ; PWD=/home/solide/projects ; USER=root
; COMMAND=/usr/bin/apt install bzip2 xz-utils zip
2025-09-27T17:58:10.403427+02:00 DESKTOP-GOD sudo: pam_unix(sudo:session): session opened for user root(uid=0) b

```

## 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

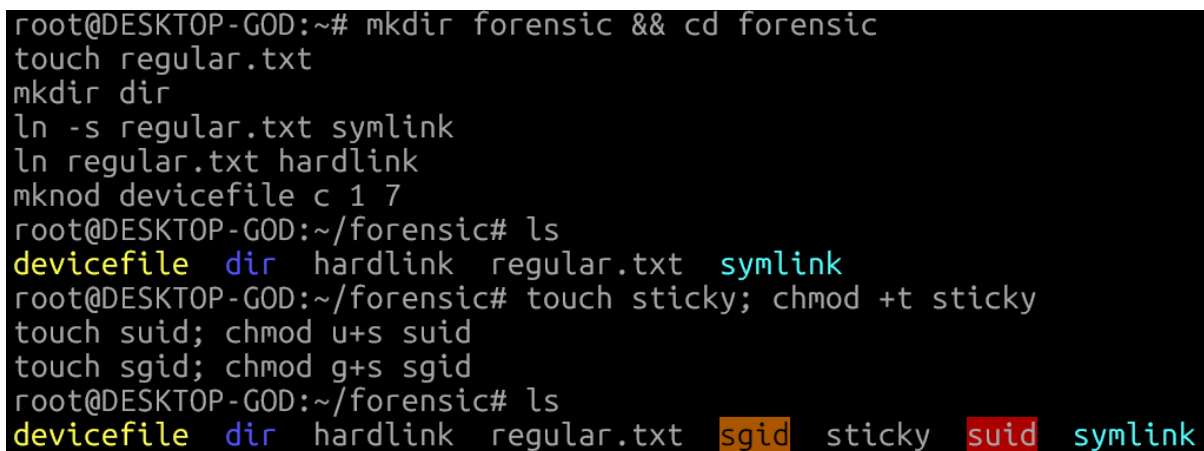
chown user1:user1 other.txt

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--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
-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--r-T 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# █

```