

Linux_Assignment2

Qn1: `/bin` → Essential binaries. Core commands (e.g., `ls`, `cp`) live here and could be replaced with malicious versions.

etc → **System configuration files.** Attackers may modify settings here (like /etc/passwd, network configs).

```
user@Jason MINGW64 /  
$ cd /etc  
  
user@Jason MINGW64 /etc  
$ ls  
DIR_COLORS docx2txt.config gitattributes hosts install-options.txt msystem.d/ nanorc nsswitch.conf pkcs11/ profile protocols ssh/  
bash.bashrc fstab gitconfig inputrc msystem mtab@ networks package-versions.txt pki/ profile.d/ services tigrc  
  
user@Jason MINGW64 /etc  
$
```

– /var → Log files. Logs are usually in /var/log, showing evidence of intrusions.
(using Ubuntu because in gitbush it wasn't found)

```
ubuntu1@Ubuntu1:~$ cd /
ubuntu1@Ubuntu1:/$ cd var
ubuntu1@Ubuntu1:/var$ ls
backups  crash  local  log  metrics  run  spool
cache    lib    lock   mail  opt      snap  tmp
ubuntu1@Ubuntu1:/var$
```

___ /usr → Additional binaries and software; less critical than /bin but can hold apps an attacker may alter.

```
user@Jason MINGW64 /
$ cd usr

user@Jason MINGW64 /usr
$ ls
bin/  etc/  lib/  libexec/  share/  ssl/
```

___ /tmp → Temporary files; often used by attackers to store scripts or payloads.

Name: Irumva Jason ID:27241 Date:Fri/26th/2025

```
user@Jason MINGW64 /  
$ cd tmp  
user@Jason MINGW64 /tmp  
$ ls  
4b42b0dc-eb56-4030-956e-4100898d5fff6.tmp  
6a20cc1e-2005-4382-bf71-8fee3c1c8df1.tmp  
6cb58f5a-31d6-43cf-a598-cb113a953b25.tmp  
80e88b7e-5581-47f6-bcf8-1abf6cddc17e.tmp  
97f52c2f-b67c-4e32-8775-e2abfb4e8a9a.tmp  
99664771-6042-462f-889c-8424c4919239.tmp  
AC_drop.{12d34_56n78_90s12_34m56}.png  
AC_item.{12d34_56n78_90s12_34m56}.png  
AdobeARM.log  
.AdobeARM.NotLocked.log  
.Air_Cooler_drop.{12d34_56n78_90s12_34m56}.png  
.Air_Cooler_item.{12d34_56n78_90s12_34m56}.png  
Alarm_drop.{12d34_56n78_90s12_34m56}.png  
Alarm_item.{12d34_56n78_90s12_34m56}.png  
Appliance_drop.{12d34_56n78_90s12_34m56}.png  
Appliance_item.{12d34_56n78_90s12_34m56}.png  
.Assignment1.(2).pdf  
.Assignment1.pdf  
.Atm_Pressure_Monitor_drop.{12d34_56n78_90s12_34m56}.png  
.Atm_Pressure_Monitor_item.{12d34_56n78_90s12_34m56}.png  
BIT7C40.tmp  
Battery_drop.{12d34_56n78_90s12_34m56}.png  
Battery_item.{12d34_56n78_90s12_34m56}.png  
Beacon_drop.{12d34_56n78_90s12_34m56}.png  
Beacon_item.{12d34_56n78_90s12_34m56}.png  
Blower_drop.{12d34_56n78_90s12_34m56}.png  
Blower_item.{12d34_56n78_90s12_34m56}.png  
.Bluetooth_Speaker_drop.{12d34_56n78_90s12_34m56}.png  
.Bluetooth_Speaker_item.{12d34_56n78_90s12_34m56}.png  
.Carbon_Dioxide_Detector_drop.{12d34_56n78_90s12_34m56}.png  
.Carbon_Dioxide_Detector_item.{12d34_56n78_90s12_34m56}.png  
.Carbon_Monoxide_Detector_drop.{12d34_56n78_90s12_34m56}.png  
.Carbon_Monoxide_Detector_item.{12d34_56n78_90s12_34m56}.png  
.Ceiling_Fan_drop.{12d34_56n78_90s12_34m56}.png  
.Ceiling_Fan_item.{12d34_56n78_90s12_34m56}.png  
.Ceiling_Sprinkler_drop.{12d34_56n78_90s12_34m56}.png  
.Ceiling_Sprinkler_item.{12d34_56n78_90s12_34m56}.png  
Cellular_Network_Intro.pdf  
DOAA39.tmp  
.Diagnostics/  
.Dimmable_LED_drop.{12d34_56n78_90s12_34m56}.png  
.Dimmable_LED_item.{12d34_56n78_90s12_34m56}.png  
Door_drop.{12d34_56n78_90s12_34m56}.png  
Door_item.{12d34_56n78_90s12_34m56}.png  
E09F06BC-BA8E-44EB-B000-2E07901c4D2F.vhdx  
Fire_Monitor_drop.{12d34_56n78_90s12_34m56}.png  
Fire_Monitor_item.{12d34_56n78_90s12_34m56}.png  
Fire_Sprinkler_drop.{12d34_56n78_90s12_34m56}.png  
JASON-20250925-1555.log  
JASON-20250925-1604.log  
JASON-20250925-1608.log  
JASON-20250925-1611.log  
JASON-20250925-2120.log  
JASON-20250925-2313.log  
LCD_drop.{12d34_56n78_90s12_34m56}.png  
LCD_item.{12d34_56n78_90s12_34m56}.png  
LED_drop.{12d34_56n78_90s12_34m56}.png  
LED_item.{12d34_56n78_90s12_34m56}.png  
.Lawn_Sprinkler_drop.{12d34_56n78_90s12_34m56}.png  
.Lawn_Sprinkler_item.{12d34_56n78_90s12_34m56}.png  
Light_drop.{12d34_56n78_90s12_34m56}.png  
Light_item.{12d34_56n78_90s12_34m56}.png  
.Low/  
.Membrane_Potentiometer_drop.{12d34_56n78_90s12_34m56}.png  
.Membrane_Potentiometer_item.{12d34_56n78_90s12_34m56}.png  
Metal_Sensor_drop.{12d34_56n78_90s12_34m56}.png  
Metal_Sensor_item.{12d34_56n78_90s12_34m56}.png  
Motion_Detector_drop.{12d34_56n78_90s12_34m56}.png  
Motion_Detector_item.{12d34_56n78_90s12_34m56}.png  
Motion_Sensor_drop.{12d34_56n78_90s12_34m56}.png  
Motion_Sensor_item.{12d34_56n78_90s12_34m56}.png  
Motor_drop.{12d34_56n78_90s12_34m56}.png  
Motor_item.{12d34_56n78_90s12_34m56}.png  
NotifyIconGeneratedAuidmid.13891581813397914303.png  
NotifyIconGeneratedAuidmid.14575584466138870523.png  
NotifyIconGeneratedAuidmid.2790618668974223932.png  
NotifyIconGeneratedAuidmid.3669257153276901705.png  
.Old_Car_drop.{12d34_56n78_90s12_34m56}.png  
Old_Car_item.{12d34_56n78_90s12_34m56}.png  
Photo_Sensor_drop.{12d34_56n78_90s12_34m56}.png  
Photo_Sensor_item.{12d34_56n78_90s12_34m56}.png  
.PhotoCache/  
Piezo_Speaker_drop.{12d34_56n78_90s12_34m56}.png  
Piezo_Speaker_item.{12d34_56n78_90s12_34m56}.png  
Portable_Music_Player_drop.{12d34_56n78_90s12_34m56}.png  
Potentiometer_drop.{12d34_56n78_90s12_34m56}.png  
Potentiometer_item.{12d34_56n78_90s12_34m56}.png  
Power_Meter_drop.{12d34_56n78_90s12_34m56}.png  
Power_Meter_item.{12d34_56n78_90s12_34m56}.png  
Push_Button_Toggle_Switch_drop.{12d34_56n78_90s12_34m56}.png  
Push_Button_Toggle_Switch_item.{12d34_56n78_90s12_34m56}.png  
Push_Button_drop.{12d34_56n78_90s12_34m56}.png  
Push_Button_item.{12d34_56n78_90s12_34m56}.png  
RFID_Card_drop.{12d34_56n78_90s12_34m56}.png  
RFID_Card_item.{12d34_56n78_90s12_34m56}.png
```

__ /opt → Optional software; could hold installed malware if attackers drop custom tools

```
ubuntu1@Ubuntu1:/$ cd opt  
ubuntu1@Ubuntu1:/opt$ ls  
ubuntu1@Ubuntu1:/opt$ 
```

__ /boot → Bootloader and kernel; tampering here can compromise system startup.

```
ubuntu1@Ubuntu1:/$ cd boot  
ubuntu1@Ubuntu1:/boot$ ls  
config-6.11.0-17-generic  
config-6.11.0-24-generic  
grub  
initrd.img  
initrd.img-6.11.0-17-generic  
initrd.img-6.11.0-24-generic  
initrd.img.old  
memtest86+ia32.bin  
memtest86+ia32.efi
```

```
memtest86+x64.bin  
memtest86+x64.efi  
System.map-6.11.0-17-generic  
System.map-6.11.0-24-generic  
vmlinuz  
vmlinuz-6.11.0-17-generic  
vmlinuz-6.11.0-24-generic  
vmlinuz.old
```

__ /home → User files; attackers might modify personal scripts or plant backdoors.

Name: Irumva Jason ID:27241 Date:Fri/26th/2025

```
ubuntu1@Ubuntu1:~$ cd home
ubuntu1@Ubuntu1:~/home$ ls
alec alex ftpuser jayftp jordan jordan ubuntu1
ubuntu1@Ubuntu1:~/home$ █
```

Qn2:Creation of Directory with Minimum Code

Using: mkdir -p

~/projects/{client_work/{web/{frontend,backend,database},mobile/{ios,android}},
personal/{experiments,archive},shared/{templates,resources}}}

To verify the structure: ls -R ~/projects

tree ~/projects

```
user@Jason MINGW64 ~
$ mkdir -p ~/projects/{client_work/{web/{frontend,backend,database},mobile/{ios,android}},personal/shared}
user@Jason MINGW64 ~
$ tree ~/projects
bash: tree: command not found

user@Jason MINGW64 ~
$ ls -R ~/projects
tree ~/projects
/c/Users/user/projects:
client_work/ personal/ shared/
/mobile/ web/
/c/Users/user/projects/client_work/mobile:
android/ ios/
/c/Users/user/projects/client_work/mobile/android:
/c/Users/user/projects/client_work/mobile/ios:
/c/Users/user/projects/client_work/web:
backend/ database/ frontend/
/c/Users/user/projects/client_work/web/backend:
/c/Users/user/projects/client_work/web/database:
/c/Users/user/projects/client_work/web/frontend:
/c/Users/user/projects/personal:
archive/ experiments/
/c/Users/user/projects/personal/archive:
/c/Users/user/projects/personal/experiments:
/c/Users/user/projects/shared:
resources/ templates/
/c/Users/user/projects/shared/resources:
/c/Users/user/projects/shared/templates:
```

Qn3: Navigating to the Directory: ~/projects/client_work/web/frontend

```
user@Jason MINGW64 ~
$ cd projects/client_work/web/frontend
user@Jason MINGW64 ~/projects/client_work/web/frontend
$ ...
```

From ~/projects/client_work/web/frontend → ~/projects/personal/experiments

Name: Irumva Jason ID:27241 Date:Fri/26th/2025

```
user@Jason MINGW64 ~/projects/client_work/web/frontend
$ cd ../../..../personal/experiments

user@Jason MINGW64 ~/projects/personal/experiments
$ pwd
/c/Users/user/projects/personal/experiments
```

From ~ / projects / personal / experiments → ~ / projects / shared / templates

```
user@Jason MINGW64 ~/projects/personal/experiments
$ cd ../../shared/templates

user@Jason MINGW64 ~/projects/shared/templates
$ pwd
/c/Users/user/projects/shared/templates
```

From ~ / projects / shared / templates → back to
~ / projects / client _ work / web / frontend (Initially where I was).

```
user@Jason MINGW64 ~/projects/shared/templates
$ cd ../../client_work/web/frontend

user@Jason MINGW64 ~/projects/client_work/web/frontend
$ pwd
/c/Users/user/projects/client_work/web/frontend
```

Qn4: Using the “mkdir -p” I created and navigated to my Parents directory web _ project and

created there bas project folders css,js and backups

```
user@Jason MINGW64 ~
$ cd web_Project

user@Jason MINGW64 ~/web_Project
$ ls
backups/  css/  js/
user@Jason MINGW64 ~/web_Project
```

I created 15 HTML files in the parents directory web _ Project

Name: Irumva Jason ID:27241 Date:Fri/26th/2025

```
user@Jason MINGW64 ~/web_Project
$ touch index.html about.html contact.html \
    page_{001..012}.html

user@Jason MINGW64 ~/web_Project
$ ls
about.html  contact.html  index.html  page_001.html  page_003.html  page_005.html  page_007.html
backups/      css/          js/        page_002.html  page_004.html  page_006.html  page_008.html

user@Jason MINGW64 ~/web_Project
$
```

__ 8 css files as named in the question are also created in there respective directory
css

```
user@Jason MINGW64 ~/web_Project
$ cd css

user@Jason MINGW64 ~/web_Project/css
$ touch main.css reset.css theme_light.css theme_dark.css \
    mobile.css tablet.css desktop.css print.css

user@Jason MINGW64 ~/web_Project/css
$ ls
desktop.css  main.css  mobile.css  print.css  reset.css  tablet.css  theme_dark.css  theme_light.css

user@Jason MINGW64 ~/web_Project/css
$
```

__ I also navigated back to the parent directory and switched to the js directory for javascript files and created the 6 js files as required with respective naming

```
user@Jason MINGW64 ~/web_Project
$ cd js

user@Jason MINGW64 ~/web_Project/js
$ touch script.js script_util.js script_config.js \
    util.js util_helper.js config.js

user@Jason MINGW64 ~/web_Project/js
$ ls
config.js  script.js  script_config.js  script_util.js  util.js  util_helper.js

user@Jason MINGW64 ~/web_Project/js
```

__ Back to the parent dierectory using “cd ..” I navigated to backups directory and also created 20 required files as required

Name: Irumva Jason ID:27241 Date:Fri/26th/2025

```
user@Jason MINGW64 ~/web_Project
$ cd backups
touch a{1..5}.bak b{1..5}.tmp c{1..5}.old d{1..5}.backup
user@Jason MINGW64 ~/web_Project
$ cd backups

user@Jason MINGW64 ~/web_Project/backups
$ ls
a1.bak  a2.bak  a3.bak  a4.bak  a5.bak  b1.tmp  b2.tmp  b3.tmp  b4.tmp  b5.tmp  c1.old  c2.old  c3.old  c4.old  c5.old  d1.backup  d2.back

user@Jason MINGW64 ~/web_Project/backups
$ |
```

Qn5: Moving all files ending in numbers (like page_001.html) to archive/

```
user@Jason MINGW64 ~/web_Project
$ ls
about.html  contact.html  index.html  page_001.html  page_003.html  page_005.html  page_007.html
backups/    css/          js/         page_002.html  page_004.html  page_006.html  page_008.html

user@Jason MINGW64 ~/web_Project
$ mkdir -p archive

user@Jason MINGW64 ~/web_Project
$ mv *[0-9].* archive/

user@Jason MINGW64 ~/web_Project
$ ls
about.html  archive/  backups/  contact.html  css/  index.html  js/
archive/    backups/  contact.html  css/  index.html  js/
index.html  js/        page_001.html  page_003.html  page_005.html  page_007.html
page_001.html  page_002.html  page_003.html  page_004.html  page_006.html  page_008.html
```

Copying all CSS files **except those containing mobile or tablet** → desktop/

Name: Irumva Jason ID:27241 Date:Fri/26th/2025

```
user@Jason MINGW64 ~/web_Project/css
$ mkdir -p desktop

user@Jason MINGW64 ~/web_Project/css
$ ls
desktop/ desktop.css main.css mobile.css print.css reset.css tablet.css

user@Jason MINGW64 ~/web_Project/css
$ for file in *.css; do
    if [[ "$file" != *mobile* && "$file" != *tablet* ]]; then
        cp "$file" desktop/
    fi
done

user@Jason MINGW64 ~/web_Project/css
$ cd desktop

user@Jason MINGW64 ~/web_Project/css/desktop
$ ls
desktop.css main.css print.css reset.css theme_dark.css theme_light.css

user@Jason MINGW64 ~/web_Project/css/desktop
$ |
```

___ Listing only files with **exactly 3 characters before the dot**

```
user@Jason MINGW64 ~/web_Project
$ ls ???.*
gym.txt man.js tim.html

user@Jason MINGW64 ~/web_Project
$
```

___ Finding files starting with any **consonant** (not a vowel)

Name: Irumva Jason ID:27241 Date:Fri/26th/2025

```
user@Jason MINGW64 ~/web_Project
$ ls [bcdfghjklmnpqrstuvwxyzBCDFGHJKLMNPQRSTUVWXYZ]*
contact.html gym.txt man.js tim.html

backups:
a1.bak a2.bak a3.bak a4.bak a5.bak b1.tmp b2.tmp b3.tmp b4.tmp b5.tmp c1.old c2.old

css:
desktop/ desktop.css main.css mobile.css print.css reset.css tablet.css theme_dark.css

js:
config.js script.js script_config.js script_util.js util.js util_helper.js

user@Jason MINGW64 ~/web_Project
$ |
```

Identifying files where the extension has exactly 2 characters

```
user@Jason MINGW64 ~/web_Project
$ ls *.[a-zA-Z][a-zA-Z]
man.js

user@Jason MINGW64 ~/web_Project
$ ls js *.[a-zA-Z][a-zA-Z]
man.js

js:
config.js script.js script_config.js script_util.js util.js util_helper.js

user@Jason MINGW64 ~/web_Project
$
```

Name: Irumva Jason ID:27241 Date:Fri/26th/2025

Qn6: Log files for every day of 1st Quarter 2024

```
user@Jason MINGW64 ~
$ mkdir -p logs

user@Jason MINGW64 ~
$ cd logs

user@Jason MINGW64 ~/logs
$ for month in {01..03}; do
    for day in {01..31}; do
        if [[ $month -eq 02 && $day -gt 29 ]]; then continue; fi
        if [[ $month =~ 04|06|09|11 && $day -gt 30 ]]; then continue; fi
        touch log_2024-$month-$day.txt
    done
done
bash: [: 08: value too great for base (error token is "08")
bash: [: 09: value too great for base (error token is "09")

user@Jason MINGW64 ~/logs
$ ls
log_2024-01-01.txt  log_2024-01-11.txt  log_2024-01-21.txt  log_2024-01-31.txt  log_2024-02-10.txt  log_2024-02-20.txt  log_2024-02-20.txt  log_2024-02-20.txt
log_2024-01-02.txt  log_2024-01-12.txt  log_2024-01-22.txt  log_2024-02-01.txt  log_2024-02-11.txt  log_2024-02-21.txt  log_2024-02-21.txt  log_2024-02-21.txt
log_2024-01-03.txt  log_2024-01-13.txt  log_2024-01-23.txt  log_2024-02-02.txt  log_2024-02-12.txt  log_2024-02-22.txt  log_2024-02-22.txt  log_2024-02-22.txt
log_2024-01-04.txt  log_2024-01-14.txt  log_2024-01-24.txt  log_2024-02-03.txt  log_2024-02-13.txt  log_2024-02-23.txt  log_2024-02-23.txt  log_2024-02-23.txt
log_2024-01-05.txt  log_2024-01-15.txt  log_2024-01-25.txt  log_2024-02-04.txt  log_2024-02-14.txt  log_2024-02-24.txt  log_2024-02-24.txt  log_2024-02-24.txt
log_2024-01-06.txt  log_2024-01-16.txt  log_2024-01-26.txt  log_2024-02-05.txt  log_2024-02-15.txt  log_2024-02-25.txt  log_2024-02-25.txt  log_2024-02-25.txt
log_2024-01-07.txt  log_2024-01-17.txt  log_2024-01-27.txt  log_2024-02-06.txt  log_2024-02-16.txt  log_2024-02-26.txt  log_2024-02-26.txt  log_2024-02-26.txt
log_2024-01-08.txt  log_2024-01-18.txt  log_2024-01-28.txt  log_2024-02-07.txt  log_2024-02-17.txt  log_2024-02-27.txt  log_2024-02-27.txt  log_2024-02-27.txt
log_2024-01-09.txt  log_2024-01-19.txt  log_2024-01-29.txt  log_2024-02-08.txt  log_2024-02-18.txt  log_2024-02-28.txt  log_2024-02-28.txt  log_2024-02-28.txt
log_2024-01-10.txt  log_2024-01-20.txt  log_2024-01-30.txt  log_2024-02-09.txt  log_2024-02-19.txt  log_2024-02-29.txt  log_2024-02-29.txt  log_2024-02-29.txt

user@Jason MINGW64 ~/logs
$ |
```

__Configuration files for dev, staging, production across 3 services

```
user@Jason MINGW64 ~
$ mkdir -p configs

user@Jason MINGW64 ~
$ touch configs/{web,api,db}_{dev,staging,prod}.conf

user@Jason MINGW64 ~
$ ls configs
api_dev.conf  api_staging.conf  db_prod.conf    web_dev.conf   web_staging.conf
api_prod.conf  db_dev.conf      db_staging.conf  web_prod.conf
```

__Test files combining letters A-C with numbers 10-12 plus suffixes input and output

```
user@Jason MINGW64 ~
$ mkdir -p tests

user@Jason MINGW64 ~
$ touch tests/{A,B,C}_{10..12}_{input,output}.txt

user@Jason MINGW64 ~
$ ls tests
A_10_input.txt  A_11_output.txt  B_10_input.txt  B_11_output.txt  C_10_input.txt  C_11_output.txt
A_10_output.txt A_12_input.txt  B_10_output.txt  B_12_input.txt  C_10_output.txt  C_12_input.txt
A_11_input.txt  A_12_output.txt B_11_input.txt  B_12_output.txt  C_11_input.txt  C_12_output.txt
```

QN7: Creating Two similar files with the same content

```
user@Jason MINGW64 ~/prac
$ #Linux line ending #lf

user@Jason MINGW64 ~/prac
$ echo -e "server=localhost\nport=8080\nmode=dev" > config_linux.txt

user@Jason MINGW64 ~/prac
$ #Windows line endings

user@Jason MINGW64 ~/prac
$ echo -e "server=localhost\r\nport=8080\r\nmode=dev" > config_windows.txt
```

```
user@Jason MINGW64 ~/prac
$ cat config_windows.txt config_linux.txt

server=localhost
port=8080
mode=dev
server=localhost
port=8080
mode=dev

user@Jason MINGW64 ~/prac
$
```

Comparison:

Diff: Shows the lines as different even though visually identical.

Reason: it detects line ending differences (\n vs \r\n).

```
user@Jason MINGW64 ~/prac
$ diff config_linux.txt config_windows.txt
1,2c1,2
< server=localhost
< port=8080
---
> server=localhost
> port=8080
```

cmp: Reports the first differing byte position.

More “raw,” byte-level comparison, doesn’t care about lines.

```
user@Jason MINGW64 ~/prac
$ cmp config_linux.txt config_windows.txt
config_linux.txt config_windows.txt differ: char 17, line 1
user@Jason MINGW64 ~/prac
```

comm:

Expects sorted input line by line.

Treats the whole line as different because of the extra \r.

```
user@Jason MINGW64 ~/prac
$ comm config_linux.txt config_windows.txt
server=localhost
comm: file 1 is not in sorted order
port=8080
mode=dev
      server=localhost
comm: file 2 is not in sorted order
      port=8080
      mode=dev
comm: input is not in sorted order
```

Lesson on cross-platform compatibility

Windows uses **CRLF** (\r\n) line endings.

Linux/Unix uses **LF** (\n).

Tools see these as differences, even if text looks identical.

This is why configs, scripts, or code may break when moved between systems.

Qn8: Creating Test Environment

Name: Irumva Jason ID:27241 Date:Fri/26th/2025

```
ubuntu1@Ubuntu1:~$ mkdir -p audit_env/{docs,logs,tmp,hidden,emp
ubuntu1@Ubuntu1:~$ cd audit_env
ubuntu1@Ubuntu1:~/audit_env$ echo "Report" > docs/report.txt
ubuntu1@Ubuntu1:~/audit_env$ head -c 1K </dev/urandom > docs/l
1.bin
ubuntu1@Ubuntu1:~/audit_env$ head -c 2K </dev/urandom > docs/l
2.bin
ubuntu1@Ubuntu1:~/audit_env$ touch -t 202409010101 logs/old.log
# very old
ubuntu1@Ubuntu1:~/audit_env$ touch -t 202509250101 logs/recent.
# ~72h ago
ubuntu1@Ubuntu1:~/audit_env$ touch -t 202509270101 logs/today.log
# within 24h
ubuntu1@Ubuntu1:~/audit_env$ touch hidden/.secret hidden/.config
ubuntu1@Ubuntu1:~/audit_env$ mkdir empty/dir
ubuntu1@Ubuntu1:~/audit_env$ touch tmp/file.tmp tmp/data~ tmp/ne
s.bak
ubuntu1@Ubuntu1:~/audit_env$ touch docs/open.txt
ubuntu1@Ubuntu1:~/audit_env$ chmod 666 docs/open.txt
ubuntu1@Ubuntu1:~/audit_env$
```

Using the Find command to find files that are larger than the average size

```
ubuntu1@Ubuntu1:~/audit_env$ avg=$(find . -type f -pri
awk '{sum+=$1; n++} END{if(n>0) print int(sum/n)}')
ubuntu1@Ubuntu1:~/audit_env$ find . -type f -size +"${
./docs/large1.bin
./docs/large2.bin
```

Files that were modified within last 72h but not last 24h

```
ubuntu1@Ubuntu1:~/audit_env$ find . -type f -mtime -3 !
./logs/today.log
ubuntu1@Ubuntu1:~/audit_env$
```

Empty Directories or Containing only hidden files

Name: Irumva Jason ID:27241 Date:Fri/26th/2025

```
ubuntu1@Ubuntu1:~/audit_env$ find . -type d -empty
find . -type d ! -empty -exec sh -c '
for d; do
    files=$(ls -A "$d")
    [[ -n "$files" && "$files" == .* ]] && echo "$d"
done
' sh {} +
./empty/dir
sh: 4: [: not found
```

__World-writable files

```
ubuntu1@Ubuntu1:~$ find . -type f -perm -002
./Desktop/prac/games.txt
./doc.txt
./audit_env/docs/open.txt
ubuntu1@Ubuntu1:~$
```

__Owned by users rather than me or root

```
ubuntu1@Ubuntu1:~$ find . -type f ! -user $USER ! -user
./audit_env/docs/otheruser_testfile.txt
ubuntu1@Ubuntu1:~$
```

__Temporaly/backup files (*.tmp, *~, *.bak)

```
ubuntu1@Ubuntu1:~$ find . -type f \(
-name '*.tmp' -o -
-name '*.bak' \)
./audit_env/tmp/file.tmp
./audit_env/tmp/notes.bak
./audit_env/tmp/data~
```

Qn9: Creating a large log file

```
longtime@Ubuntu1:~$ mkdir -p log_test
ubuntu1@Ubuntu1:~$ cd log_test
ubuntu1@Ubuntu1:~/log_test$ for i in {1..250}; do
    if (( i % 20 == 0 )); then
        echo "$i: ERROR Something went wrong" >> system.log
    else
        echo "$i: INFO Normal operation" >> system.log
    fi
done
```

Displaying 50Lines

```
ubuntu1@Ubuntu1:~/log_test$ total=$(wc -l < system.log)
start=$((total/2 - 25))
sed -n "$((start+1)),$((start+50))p" system.log
101: INFO Normal operation
102: INFO Normal operation
103: INFO Normal operation
104: INFO Normal operation
105: INFO Normal operation
106: INFO Normal operation
107: INFO Normal operation
108: INFO Normal operation
109: INFO Normal operation
110: INFO Normal operation
111: INFO Normal operation
112: INFO Normal operation
113: INFO Normal operation
114: INFO Normal operation
115: INFO Normal operation
116: INFO Normal operation
117: INFO Normal operation
118: INFO Normal operation
119: INFO Normal operation
120: ERROR Something went wrong
121: INFO Normal operation
122: INFO Normal operation
```

```
130: INFO Normal operation
131: INFO Normal operation
132: INFO Normal operation
133: INFO Normal operation
134: INFO Normal operation
135: INFO Normal operation
136: INFO Normal operation
137: INFO Normal operation
138: INFO Normal operation
139: INFO Normal operation
140: ERROR Something went wrong
141: INFO Normal operation
142: INFO Normal operation
143: INFO Normal operation
144: INFO Normal operation
```

— Finding the **last occurrence** of a word (ERROR) with 5 lines of context

```
ubuntu1@Ubuntu1:~/log_test$ grep -n -B5 -A5 "ERROR" syst
ail -n 11
235-235: INFO Normal operation
236-236: INFO Normal operation
237-237: INFO Normal operation
238-238: INFO Normal operation
239-239: INFO Normal operation
240-240: ERROR Something went wrong
241-241: INFO Normal operation
242-242: INFO Normal operation
243-243: INFO Normal operation
244-244: INFO Normal operation
245-245: INFO Normal operation
```

Comparing the efficiency of viewing with different tools, “less” and “cat”

less is more efficient over SSH → it **fetches and displays pages**, unlike cat which sends the full file at once. **cat** streams the entire file immediately → can be slow on large files, consumes bandwidth. **less** displays **one screen at a time**, fetches data as needed → saves bandwidth, easier to scroll/search.

```
1: INFO Normal operation
2: INFO Normal operation
3: INFO Normal operation
4: INFO Normal operation
5: INFO Normal operation
6: INFO Normal operation
7: INFO Normal operation
8: INFO Normal operation
9: INFO Normal operation
10: INFO Normal operation
11: INFO Normal operation
12: INFO Normal operation
13: INFO Normal operation
14: INFO Normal operation
15: INFO Normal operation
16: INFO Normal operation
17: INFO Normal operation
18: INFO Normal operation
19: INFO Normal operation
20: ERROR Something went wrong
21: INFO Normal operation
22: INFO Normal operation
23: INFO Normal operation
24: INFO Normal operation
25: INFO Normal operation
```

__Extracting **only lines with error patterns**, preserving line numbers

```
ubuntu1@Ubuntu1:~/log_test$ grep -n "ERROR" system.log
20:20: ERROR Something went wrong
40:40: ERROR Something went wrong
60:60: ERROR Something went wrong
80:80: ERROR Something went wrong
100:100: ERROR Something went wrong
120:120: ERROR Something went wrong
140:140: ERROR Something went wrong
160:160: ERROR Something went wrong
180:180: ERROR Something went wrong
200:200: ERROR Something went wrong
220:220: ERROR Something went wrong
240:240: ERROR Something went wrong
ubuntu1@Ubuntu1:~/log_test$
```

Qn10: Changing Permissions

```
ubuntu1@Ubuntu1:~/audit_env$ sudo find . -type f ! -perm
    chmod 644 {} \;
ubuntu1@Ubuntu1:~/audit_env$ ls -l
total 20
drwxrwxr-x 2 ubuntu1 ubuntu1 4096 Sep 28 17:25 docs
drwxrwxr-x 3 ubuntu1 ubuntu1 4096 Sep 28 17:06 empty
drwxrwxr-x 2 ubuntu1 ubuntu1 4096 Sep 28 17:06 hidden
drwxrwxr-x 2 ubuntu1 ubuntu1 4096 Sep 28 17:05 logs
drwxrwxr-x 2 ubuntu1 ubuntu1 4096 Sep 28 17:06 tmp
ubuntu1@Ubuntu1:~/audit_env$
```

__Calculate total disk space used by files older than 30 days

```
ubuntu1@Ubuntu1:~$ find . -type f -mtime +30 -exec du -c
ail -n 1
15M      total
ubuntu1@Ubuntu1:~$
```

__Backing up all configuration files (*.conf)

```
ubuntu1@Ubuntu1:~$ find . -type f -name "*.conf" -exec cp {} backup \;
ubuntu1@Ubuntu1:~$ find . -type f -name "*.conf"
./snap/snap-store/1270/.config/fontconfig/fonts.conf
./snap/firefox/6836/.config/fontconfig/fonts.conf
./snap/firefox/6738/.config/fontconfig/fonts.conf
./snap/snapd-desktop-integration/315/.config/fontconfig/
./snap/snapd-desktop-integration/253/.config/fontconfig/
./snap/firmware-updater/167/.config/fontconfig/fonts.conf
./.config/rygel.conf
ubuntu1@Ubuntu1:~$ find . -type f -name "*.conf.backup"
./snap/snap-store/1270/.config/fontconfig/fonts.conf.backup
./snap/firefox/6836/.config/fontconfig/fonts.conf.backup
./snap/firefox/6738/.config/fontconfig/fonts.conf.backup
```

___ Removing temporary files **safely** (not accessed recently)

```
user@Jason MINGW64 /tmp
$ find . -type f -name "*.tmp" -atime +2 -ok rm {} \;
< rm ... ./chrome_BITS_17016_2018478794/BITAB92.tmp > ?
< rm ... ./chrome_BITS_3116_1848273277/BIT4B41.tmp > ?
< rm ... ./edge_BITS_17524_1846704566/BIT7169.tmp > ?
< rm ... ./edge_BITS_3848_92016272/BITFDA1.tmp > ?
< rm ... ./edge_BITS_6932_630254930/BITCF4B.tmp > ?
< rm ... ./edge_BITS_8852_1501710232/BITF591.tmp > ?
```

___ Showing how to preview dangerous operations before executing them.

Always **preview with find first** before -exec.

Use -ok instead of -exec for destructive commands.

You can replace dangerous commands with echo first to verify:

Name: Irumva Jason ID:27241 Date:Fri/26th/2025

```
ubuntu1@Ubuntu1:~$ sudo find . -type f -name "*.tmp" -atime +1 | xargs rm {} \;
find: './run/user/1000/gvfs': Permission denied
find: './run/user/1000/doc': Permission denied
```

Qn11: Creating test directories and files

```
ubuntu1@Ubuntu1:~$ mkdir -p ~/compression_test/{media,test}
ubuntu1@Ubuntu1:~$ cp /usr/share/backgrounds/*.jpg ~/compression_test/media/ 2>/dev/null
ubuntu1@Ubuntu1:~$ cp /usr/share/sounds/* ~/compression_test/test/ 2>/dev/null
ubuntu1@Ubuntu1:~$ echo "This is a sample log file" > ~/compression_test/text/log.txt
ubuntu1@Ubuntu1:~$ yes "Some repeated text line" | head -n 1000 > ~/compression_test/text/biglog.txt
ubuntu1@Ubuntu1:~$ ls
audit_env           data.csv    Downloads   Music      Template
combined.log        Desktop     log_test    Pictures   textde
combine.log         doc.txt     mcbishop   Public    Video
compression_test    Documents   media      snap
ubuntu1@Ubuntu1:~$ ls compression_test
media   text
```

Creating archives with different algorithms

```
ubuntu1@Ubuntu1:~$ tar -cvf media_bz2.tar ~/compression_test/media/
&& bzip2 media_bz2.tar
tar: Removing leading `/' from member names
/home/ubuntu1/compression_test/media/
/home/ubuntu1/compression_test/media/Province_of_the_sunrise_by_orbitelambda.jpg
/home/ubuntu1/compression_test/media/Clouds_by_Tibor_Molnár.jpg
/home/ubuntu1/compression_test/media/Monument_valley_by_da.jpg
```

Name: Irumva Jason ID:27241 Date:Fri/26th/2025

```
ubuntu1@Ubuntu1:~$ tar -cvf text_bz2.tar ~/compression_test/text  
& bzip2 text_bz2.tar  
tar: Removing leading `/' from member names  
/home/ubuntu1/compression_test/text/  
/home/ubuntu1/compression_test/text/log.txt  
/home/ubuntu1/compression_test/text/biglog.txt  
ubuntu1@Ubuntu1:~$ # xz  
tar -cvf media_xz.tar ~/compression_test/media && xz media_xz.tar  
tar: Removing leading `/' from member names  
/home/ubuntu1/compression_test/media/  
/home/ubuntu1/compression_test/media/Province_of_the_source_by_orbitelambda.jpg  
/home/ubuntu1/compression_test/media/Clouds_by_Tibor_Mokoszki.jpg  
/home/ubuntu1/compression_test/media/Monument_valley_by_nszki.jpg  
ubuntu1@Ubuntu1:~$ zip -r media.zip ~/compression_test/media/  
updating: home/ubuntu1/compression_test/media/ (stored 0%)  
updating: home/ubuntu1/compression_test/media/Province_of_the_source_by_orbitelambda.jpg (deflated 53%)  
updating: home/ubuntu1/compression_test/media/Clouds_by_Tibor_Mokoszki.jpg (deflated 2%)  
updating: home/ubuntu1/compression_test/media/Monument_valley_by_nszki.jpg (deflated 0%)  
ubuntu1@Ubuntu1:~$ ls  
audit_env           media_bz2.tar        test_text.tar.gz  
combined.log         media_bz2.tar.bz2      test_text.tar.xz  
combine.log          media.tar.gz        test_text.zip  
compression_test     media_xz.tar        text_bz2.tar  
data.csv            media_xz.tar.xz      text_bz2.tar.bz2  
Desktop             media.zip          textdata  
doc.txt             Music              text.tar.gz  
Documents           Pictures           text_xz.tar  
Downloads           Public             text_xz.tar.xz  
log_test            snap               text.zip  
... .
```

___Measuring sizes

```
ubuntu1@Ubuntu1:~$ ls -lh media* text*
-rw-rw-r-- 1 ubuntu1 ubuntu1 7.1M Sep 28 22:37 media_bz2
-rw-rw-r-- 1 ubuntu1 ubuntu1 6.2M Sep 28 22:36 media_bz2
-rw-rw-r-- 1 ubuntu1 ubuntu1 6.2M Sep 28 22:34 media.tar
-rw-rw-r-- 1 ubuntu1 ubuntu1 7.1M Sep 28 22:39 media_xz
-rw-rw-r-- 1 ubuntu1 ubuntu1 6.2M Sep 28 22:36 media_xz
-rw-rw-r-- 1 ubuntu1 ubuntu1 6.2M Sep 28 22:39 media.zip
-rw-rw-r-- 1 ubuntu1 ubuntu1 1.2M Sep 28 22:38 text_bz2
-rw-rw-r-- 1 ubuntu1 ubuntu1 463 Sep 28 22:36 text_bz2
-rw-rw-r-- 1 ubuntu1 ubuntu1 3.2K Sep 28 22:36 text.tar
-rw-rw-r-- 1 ubuntu1 ubuntu1 1.2M Sep 28 22:39 text_xz
-rw-rw-r-- 1 ubuntu1 ubuntu1 500 Sep 28 22:36 text_xz
-rw-rw-r-- 1 ubuntu1 ubuntu1 3.6K Sep 28 22:40 text.zip

media:
total 28K
-rw-r--r-- 1 ubuntu1 ubuntu1 1.2K Sep 28 22:28 debian-l
-rw-r--r-- 1 ubuntu1 ubuntu1 2.4K Sep 28 22:28 hplj1020_
-rw-r--r-- 1 ubuntu1 ubuntu1 2.3K Sep 28 22:28 language-
ng
-rw-r--r-- 1 ubuntu1 ubuntu1 4.6K Sep 28 22:28 ubuntu-l
rk.png
-rw-r--r-- 1 ubuntu1 ubuntu1 5.2K Sep 28 22:28 ubuntu-l
g
```

___Measuring speed (compression time)

```
ubuntu1@Ubuntu1:~$ time tar -czf test_text.tar.gz ~/compressions/test/text
tar: Removing leading '/' from member names

real    0m0.070s
user    0m0.016s
sys     0m0.023s
ubuntu1@Ubuntu1:~$ time tar -cjf test_text.tar.bz2 ~/compressions/test/text
tar: Removing leading '/' from member names

real    0m0.601s
user    0m0.133s
sys     0m0.203s
ubuntu1@Ubuntu1:~$ time tar -cJf test_text.tar.xz ~/compressions/test/text
tar: Removing leading '/' from member names

real    0m0.086s
user    0m0.036s
sys     0m0.027s
ubuntu1@Ubuntu1:~$ time zip -r test_text.zip ~/compressions/test/text
updating: home/ubuntu1/compression_test/text/ (stored 0%)
updating: home/ubuntu1/compression_test/text/log.txt (stored 0%)
```

Expected results (analysis)

- **Media (.jpg, .mp4, .zip):** Already compressed → all methods show little/no size reduction, only wasted CPU time. Best to just archive (tar without compression).
- **Text files (logs, configs):**

gzip: Fast, good compression.

bzip2: **Better compression** but slower.

xz: **Best compression ratio** but **slowest**.

zip: Cross-platform, moderate compression.

Recommendation for automated backups

- Use **tar + gzip (.tar.gz)**: good balance of speed + compression, widely supported.
- For **long-term archival storage** (rare restores, max space-saving) → tar + xz.
- For **media files** → just tar (no compression) to save time/CPU.

Qn12: Creating sample archives

```
ubuntu1@Ubuntu1:~$ mkdir -p ~/archives_demo/{logs,configs,media}
ubuntu1@Ubuntu1:~$ echo "log1" > ~/archives_demo/logs/log1.txt
echo "log2" > ~/archives_demo/logs/log2.txt
echo "config1" > ~/archives_demo/configs/app.conf
echo "config2" > ~/archives_demo/configs/db.conf
echo "mediafile" > ~/archives_demo/media/media.txt
ubuntu1@Ubuntu1:~$ tar -czf logs.tar.gz -C ~/archives_demo logs
tar -cjf configs.tar.bz2 -C ~/archives_demo configs
zip -r media.zip ~/archives_demo/media
      adding: home/ubuntu1/archives_demo/media/ (stored 0%)
      adding: home/ubuntu1/archives_demo/media/media.txt (stored 0%)
ubuntu1@Ubuntu1:~$ ls archives_demo/
logs  configs  media
```

— Safely examining archive contents (no extraction)

Name: Irumva Jason ID:27241 Date:Fri/26th/2025

```
ubuntu1@Ubuntu1:~$ tar -tzf logs.tar.gz
logs/Home
logs/log1.txt
logs/log2.txt
ubuntu1@Ubuntu1:~$ tar -tjf configs.tar.bz2
configs/
configs/db.conf
configs/app.conf
ubuntu1@Ubuntu1:~$ unzip -l media.zip
Archive: media.zip
      Length      Date  Time    Name
-----  -----
          0 2025-09-28 22:32  home/ubuntu1/compression_test/media/
  1408323 2025-09-28 22:32  home/ubuntu1/compression_test/media/
Province_of_the_south_of_france_by_orbitelambda.jpg
   4032506 2025-09-28 22:32  home/ubuntu1/compression_test/media/
Clouds_by_Tibor_Mokanszki.jpg
   1957897 2025-09-28 22:32  home/ubuntu1/compression_test/media/
Monument_valley_by_orbitelambda.jpg
          0 2025-09-28 23:15  home/ubuntu1/archives_demo/media/
         10 2025-09-28 23:15  home/ubuntu1/archives_demo/media/med
ia.txt
-----
      7398736
ubuntu1@Ubuntu1:~$
```

__Extracting only matching files

Name: Irumva Jason ID:27241 Date:Fri/26th/2025

```
ubuntu1@Ubuntu1:~$ tar -xjf configs.tar.bz2 --wildcards
ubuntu1@Ubuntu1:~$ ls configs/*.conf
configs/app.conf  configs/db.conf
ubuntu1@Ubuntu1:~$ unzip media.zip */media.txt'
Archive: media.zip
  extracting: home/ubuntu1/archives_demo/media/media.txt
ubuntu1@Ubuntu1:~$ cat extracted/*/media.txt
cat: 'extracted/*/media.txt': No such file or directory
ubuntu1@Ubuntu1:~$ cat archives_demo/media/media.txt
mediafile
.....
ubuntu1@Ubuntu1:~$ tar -xzf logs.tar.gz logs/log1.txt
ubuntu1@Ubuntu1:~$ cat logs/log1.txt
log1
ubuntu1@Ubuntu1:~$
```

___Updating existing archives without full recreation

```
ubuntu1@Ubuntu1:~$ tar -rf logs.tar logs/log3.txt      # a
gzip logs.tar
tar: logs/log3.txt: Cannot stat: No such file or directo
tar: Exiting with failure status due to previous errors
gzip: logs.tar.gz already exists; do you wish to overwri
)? y
ubuntu1@Ubuntu1:~$ tar -tzf logs.tar.gz
```

___Handling corrupted archives

```
ubuntu1@Ubuntu1:~$ cp logs.tar.gz broken.tar.gz
ubuntu1@Ubuntu1:~$ truncate -s -10 broken.tar.gz      # chop
  bytes
ubuntu1@Ubuntu1:~$ tar -tzf broken.tar.gz
gzip: stdin: unexpected end of file
tar: Child returned status 1
tar: Error is not recoverable: exiting now
ubuntu1@Ubuntu1:~$ gzip -tv broken.tar.gz
broken.tar.gz:
gzip: broken.tar.gz: unexpected end of file
.....
```

__Merging contents into a single new archive

```
ubuntu1@Ubuntu1:~$ ls -R ~/merged
```

```
/home/ubuntu1/merged:
```

```
configs home
```

```
/home/ubuntu1/merged/configs:
```

```
app.conf db.conf
```

```
/home/ubuntu1/merged/home:
```

```
ubuntu1
```

```
/home/ubuntu1/merged/home/ubuntu1:
```

```
archives_demo compression_test
```

```
/home/ubuntu1/merged/home/ubuntu1/archives_demo:
```

```
media
```

```
/home/ubuntu1/merged/home/ubuntu1/archives_demo/media:
```

```
media.txt
```

```
/home/ubuntu1/merged/home/ubuntu1/compression_test:
```

Qn13:Setting up Backup directories and sample data

Name: Irumva Jason ID:27241 Date:Fri/26th/2025

```
ubuntu1@Ubuntu1:~$ mkdir -p ~/prod_data
ubuntu1@Ubuntu1:~$ echo "file1" > ~/prod_data/app.log
ubuntu1@Ubuntu1:~$ echo "file2" > ~/prod_data/config.cfg
ubuntu1@Ubuntu1:~$ ls -l ~/prod_data
total 8
-rw-rw-r-- 1 ubuntu1 ubuntu1 6 Sep 29 14:12 app.log
-rw-rw-r-- 1 ubuntu1 ubuntu1 6 Sep 29 14:12 config.cfg
```

```
ubuntu1@Ubuntu1:~$ mkdir -p ~/backups/{daily,weekly,monthly}
ubuntu1@Ubuntu1:~$ ls -R ~/backups
/home/ubuntu1/backups:
daily monthly weekly

/home/ubuntu1/backups/daily:

/home/ubuntu1/backups/monthly:

/home/ubuntu1/backups/weekly:
```

```
ubuntu1@Ubuntu1:~$ mkdir -p ~/data
ubuntu1@Ubuntu1:~$ echo "file1" > ~/data/file1.txt
ubuntu1@Ubuntu1:~$ echo "file2" > ~/data/file2.txt
ubuntu1@Ubuntu1:~$ ls -l ~/data
total 8
-rw-rw-r-- 1 ubuntu1 ubuntu1 6 Sep 29 14:32 file1.txt
-rw-rw-r-- 1 ubuntu1 ubuntu1 6 Sep 29 14:33 file2.txt
ubuntu1@Ubuntu1:~$
```

_____ Daily incremental backup (using --listed-incremental)

Name: Irumva Jason ID:27241 Date:Fri/26th/2025

```
ubuntu1@Ubuntu1:~$ # 1. Make sure full structure exists
mkdir -p ~/backups/daily

# 2. Create the snapshot file
touch ~/backups/daily.snap

# 3. Run incremental backup again
tar --listed-incremental=~/backups/daily.snap -czpf ~/backups/daily/backup_$(date +%F).tar.gz ~/data

# 4. Verify contents
tar -tzf ~/backups/daily/backup_$(date +%F).tar.gz
tar: ~/backups/daily.snap: Cannot open: No such file or directory
tar: Removing leading '/' from member names
tar: Exiting with failure status due to previous errors
home/ubuntu1/data/
home/ubuntu1/data/file1.txt
home/ubuntu1/data/file2.txt
ubuntu1@Ubuntu1:~$
```

__ Weekly full backup

```
ubuntu1@Ubuntu1:~$ tar --listed-incremental=/dev/null -czpf ~/backups/weekly/full_$(date +%F).tar.gz ~/data
tar: Removing leading '/' from member names
tar: /dev/null: Cannot truncate: Invalid argument
tar: Exiting with failure status due to previous errors
ubuntu1@Ubuntu1:~$ tar -tzf ~/backups/weekly/full_$(date +%F).tar.gz
tar: Removing leading '/' from member names
tar: home/ubuntu1/data/:
tar: home/ubuntu1/data/file1.txt
tar: home/ubuntu1/data/file2.txt
tar: Exiting with failure status due to previous errors
ubuntu1@Ubuntu1:~$
```

Name: Irumva Jason ID:27241 Date:Fri/26th/2025

__MonthlyArchive

```
ubuntu1@Ubuntu1:~$ tar -czpf ~/backups/monthly/archive_$(date +'%Y-%m').tar.gz ~/data
tar: Removing leading `/' from member names
ubuntu1@Ubuntu1:~$ tar -tzf ~/backups/monthly/archive_$(date +'%Y-%m').tar.gz
home/ubuntu1/data/
home/ubuntu1/data/file2.txt
home/ubuntu1/data/file1.txt
ubuntu1@Ubuntu1:~$
```

__Automatic cleanup (keep last 7 daily, 4 weekly, 12 monthly)

```
ubuntu1@Ubuntu1:~$ cd home
ubuntu1@Ubuntu1:~/home$ ls
ubuntu1
ubuntu1@Ubuntu1:~/home$ find ~/backups/daily -type f -mtime -1 -exec echo rm {} \;
ubuntu1@Ubuntu1:~/home$ find ~/backups/weekly -type f -mtime -28 -exec echo rm {} \;
ubuntu1@Ubuntu1:~/home$ find ~/backups/monthly -type f -mtime -365 -exec echo rm {} \;
ubuntu1@Ubuntu1:~/home$ find ~/backups/daily -type f -mtime -1
ubuntu1@Ubuntu1:~/home$ find ~/backups/weekly -type f -mtime -28
find ~/backups/monthly -type f -mtime +365
find: invalid argument `+28find' to `-mtime'
ubuntu1@Ubuntu1:~/home$ find ~/backups/monthly -type f -mtime +365
ubuntu1@Ubuntu1:~/home$
```

__Verifying backup integrity

Name: Irumva Jason ID:27241 Date:Fri/26th/2025

```
ubuntu1@Ubuntu1:~$ tar -tzf ~/backups/daily/backup_$(date +'%Y-%m-%d').tar.gz > /dev/null && echo "OK"
OK
ubuntu1@Ubuntu1:~$ tar -tzf ~/backups/daily/backup_$(date +'%Y-%m-%d').tar.gz > /dev/null && echo "OK"
OK
```

Qn14: Checking my current user context(ubuntu1)

```
ubuntu1@Ubuntu1:~$ whoami
ubuntu1
ubuntu1@Ubuntu1:~$ id
uid=1000(ubuntu1) gid=1000(ubuntu1) groups=1000(ubuntu1)
dm),24(cdrom),27(sudo),30(dip),46(plugdev),100(users),11
admin
ubuntu1@Ubuntu1:~$ groups
ubuntu1 adm cdrom sudo dip plugdev users lpadmin
ubuntu1@Ubuntu1:~$
```

Creating a test user to compare groups:

```
ubuntu1@Ubuntu1:~$ sudo useradd -m testuser
[sudo] password for ubuntu1:
ubuntu1@Ubuntu1:~$ id testuser
uid=1002(testuser) gid=1002(testuser) groups=1002(testuse
ubuntu1@Ubuntu1:~$ groups testuser
testuser : testuser
ubuntu1@Ubuntu1:~$
```

Observation: system accounts usually have limited groups, regular users often in sudo, users, etc.

```
ubuntu1@Ubuntu1:~$ groups
ubuntu1 adm cdrom sudo dip plugdev users lpadmin
ubuntu1@Ubuntu1:~$ groups testuser
testuser : testuser
ubuntu1@Ubuntu1:~$
```

Examining /etc/passwd entries

System users: UID < 1000, login shell usually /usr/sbin/nologin or /bin/false, no home directory for normal login.

Regular users: UID \geq 1000, valid shell (e.g., /bin/bash), home directory /home/username.

```
ubuntu1@Ubuntu1:~$ 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:/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/no
```

```
gnome-initial-setup:x:119:65534::/run/gnome-initial-setup
bin/false
gdm:x:120:121:Gnome Display Manager:/var/lib/gdm3:/bin/false
nm-openvpn:x:121:122:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
ubuntu1:x:1000:1000:ubuntu1:/home/ubuntu1:/bin/bash
sshd:x:123:65534::/run/sshd:/usr/sbin/nologin
otheruser:x:1001:1001::/home/otheruser:/bin/bash
testuser:x:1002:1002::/home/testuser:/bin/sh
ubuntu1@Ubuntu1:~$
```

- Comparing groups with a system user

Risk: If a regular user is added to groups like root or adm, they could:

- Read/write sensitive files
- Change system configurations
- Escalate privileges

```
ubuntu1@Ubuntu1:~$ id root  
uid=0(root) gid=0(root) groups=0(root)  
ubuntu1@Ubuntu1:~$ id testuser  
uid=1002(testuser) gid=1002(testuser) groups=1002(testus  
ubuntu1@Ubuntu1:~$
```

Qn15: Checking current effective vs configured groups

```
ubuntu1@Ubuntu1:~$ id  
uid=1000(ubuntu1) gid=1000(ubuntu1) groups=1000(ubuntu1),  
dm,24(cdrom),27(sudo),30(dip),46(plugdev),100(users),114  
admin)  
ubuntu1@Ubuntu1:~$ groups  
ubuntu1 adm cdrom sudo dip plugdev users lpadmin  
ubuntu1@Ubuntu1:~$
```

— Demonstrating re-login requirement

```
ubuntu1@Ubuntu1:~$ sudo useradd -m colleague
ubuntu1@Ubuntu1:~$ sudo passwd ubuntu
passwd: user 'ubuntu' does not exist
ubuntu1@Ubuntu1:~$ sudo passwd colleague
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: password updated successfully
ubuntu1@Ubuntu1:~$ sudo usermod -aG adm colleague
ubuntu1@Ubuntu1:~$ id colleague
uid=1003(colleague) gid=1003(colleague) groups=1003(colle
e),4(adm)
ubuntu1@Ubuntu1:~$ groups colleague
colleague : colleague adm
ubuntu1@Ubuntu1:~$ groups
ubuntu1 adm cdrom sudo dip plugdev users lpadmin
ubuntu1@Ubuntu1:~$
```

After relog-in:

```
ubuntu1@Ubuntu1:~$ id colleague
uid=1003(colleague) gid=1003(colleague) groups=1003(colle
e),4(adm)
ubuntu1@Ubuntu1:~$ groups colleague
colleague : colleague adm
ubuntu1@Ubuntu1:~$
```

Identifying groups for common resources(Also checking group ownership and web files)

Resource	Typical Group
System logs (/var/log)	adm, syslog
Web server files	www-data
Administrative functions	sudo, wheel

Group ownership:

Name: Irumva Jason ID:27241 Date:Fri/26th/2025

9 18:22	syslog			
-rw-r-----	1 syslog	adm	1010276	
3 16:12	syslog.1			
-rw-r-----	1 syslog	adm	1105674	
9 06:02	syslog.2.gz			
-rw-r-----	1 syslog	adm	470459	
1 20:47	syslog.3.gz			
-rw-r-----	1 syslog	adm	1306329	
4 07:01	syslog.4.gz			
drwxr-xr-x	2 root	root	4096	
8 15:55	sysstat			
-rw-r-----	1 syslog	adm	161707	
9 18:20	ufw.log			
-rw-r-----	1 syslog	adm	4235	
6 12:02	ufw.log.1			
-rw-r-----	1 syslog	adm	3586	
8 21:20	ufw.log.2.gz			
-rw-r-----	1 syslog	adm	6311	
1 20:47	ufw.log.3.gz			
-rw-r-----	1 syslog	adm	27058	
1 18:23	ufw.log.4.gz			
drwxr-x---	2 root	adm	4096	
9 06:02	unattended-upgrades			
-rwxr--r--	1 root	root	514	
9 19:35	vboxpostinstall.log			

Name: Irumva Jason ID:27241 Date:Fri/26th/2025

```
ubuntu1@Ubuntu1:~$ ls -l /var/log
total 11212
-rw-r--r-- 1 root          root      2948
8 16:39 alternatives.log
-rw-r--r-- 1 root          root    29390
9 15:27 alternatives.log.1
-rw-r----- 1 root          adm     1532
9 15:09 apport.log
-rw-r----- 1 root          adm     1815
8 22:51 apport.log.1
-rw-r----- 1 root          adm     266
8 19:30 apport.log.2.gz
-rw-r----- 1 root          adm     116
2 21:25 apport.log.3.gz
drwxr-xr-x 2 root          root    4096
8 16:39 apt
-rw-r----- 1 syslog        adm    95976
9 18:21 auth.log
-rw-r----- 1 syslog        adm   18333
3 16:12 auth.log.1
-rw-r----- 1 syslog        adm   10613
9 06:02 auth.log.2.gz
-rw-r----- 1 syslog        adm    8827
1 20:47 auth.log.3.gz
-rw-r----- 1 syslog        adm   22374
4 07:01 auth.log.4.gz
```

Web files:

```
ubuntu1@Ubuntu1:/$ mkdir -p ~/www_test
touch ~/www_test/index.html
ls -l ~/www_test
total 0
-rw-rw-r-- 1 ubuntu1 ubuntu1 0 Sep 29 18:32 index.html
```

Principle of Least Privilege

Assign users **only to the groups they need** for their job.

Avoid giving access to root, adm, or sudo unless necessary.

Helps **limit potential damage** from mistakes or compromised accounts.

Qn16: Documenting my sudo permissions & restrictions

Showing what my user is allowed to do and inspect sudoers safely.

```
ubuntu1@Ubuntu1:/$ cd ~
ubuntu1@Ubuntu1:~$ sudo -l
[sudo] password for ubuntu1:
Matching Defaults entries for ubuntu1 on Ubuntu1:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/bin\:/snap/bin,
    use_pty

User ubuntu1 may run the following commands on Ubuntu1:
    (ALL : ALL) ALL
ubuntu1@Ubuntu1:~$ sudo cat /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as
#
# Please consider adding local content in /etc/sudoers.d
# directly modifying this file.
#
# See the man page for details on how to write a sudoers
#
Defaults      env_reset
Defaults      mail_badpass
Defaults      secure_path="/usr/local/sbin:/usr/local/bin:/sbin:/bin:/snap/bin"
```

```
# While you shouldn't normally run git as root, you need
# per Home
Defaults:%sudo env_keep += "GIT_AUTHOR_* GIT_COMMITTER_"

# Per-user preferences; root won't have sensible values f
Defaults:%sudo env_keep += "EMAIL DEBEMAIL DEBFULLNAME"

# "sudo scp" or "sudo rsync" should be able to use your S
Defaults:%sudo env_keep += "SSH_AGENT_PID SSH_AUTH_SOCK"

# Ditto for GPG agent
Defaults:%sudo env_keep += "GPG_AGENT_INFO"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin  ALL=(ALL) ALL
```

```
ubuntu1@Ubuntu1:~$ sudo ls -l /etc/sudoers.d
total 4
-r--r----- 1 root root 1068 Jan 29 2024 README
ubuntu1@Ubuntu1:~$ sudo sed -n '1,200D' /etc/sudoers.d/*
```

Name: Irumva Jason ID:27241 Date:Fri/26th/2025

```
ubuntu1@Ubuntu1:~$ sudo sed -n '1,200p' /etc/sudoers.d/*
true
#
# The default /etc/sudoers file created on installation does
# sudo package now includes the directive:
#
#      @includedir /etc/sudoers.d
# growthsstore
#
# This will cause sudo to read and parse any files in the
# directory that do not end in '~' or contain a '.' character
# exists. It is not an error if the directory does not exist.
#
# Note also, that because sudoers contents can vary widely
# is
# made to add this directive to existing sudoers files or
# l free
# to add the above directive to the end of your /etc/sudoers
# able
# this functionality for existing installations if you wish
# Sudo versions older than 1.9.1 will only support the old
# #includedir. That means that the sudo versions in Debian
# )
# and later will happily accept both @includedir and #include
#
```

```
ubuntu1@Ubuntu1:~$ sudo visudo -c
/etc/sudoers: parsed OK
/etc/sudoers.d/README: parsed OK
ubuntu1@Ubuntu1:~$ █
```

_____ Demonstrating difference: sudo -i vs sudo su vs su

Name: Irumva Jason ID:27241 Date:Fri/26th/2025

Each command below prints who you are, your HOME, and effective groups so you can inspect differences.

sudo -i : start a login shell as root (reads root's shell startup files)

sudo su : run su as root; typically gives a root shell (behavior depends on su flags)

su : switch user (requires target user's password unless run as root)

Example: run a command as another user "otheruser" (may prompt for password)

```
ubuntu1@Ubuntu1:~$ whoami; id; echo "----"
ubuntu1
uid=1000(ubuntu1) gid=1000(ubuntu1) groups=1000(ubuntu1)
dm),24(cdrom),27(sudo),30(dip),46(plugdev),100(users),11
admin)
-----
ubuntu1@Ubuntu1:~$ sudo -i -- bash -c 'whoami; echo "HOME"
OME"; id'
root
HOME=/root
uid=0(root) gid=0(root) groups=0(root)
ubuntu1@Ubuntu1:~$ sudo su -c 'whoami; echo "HOME=$HOME"
'
root
HOME=/root
uid=0(root) gid=0(root) groups=0(root)
ubuntu1@Ubuntu1:~$ sudo su -c 'whoami; echo "HOME=$HOME"
'
root
HOME=/root
uid=0(root) gid=0(root) groups=0(root)
ubuntu1@Ubuntu1:~$ su - otheruser -c 'whoami; echo "HOME
ME"; id'
Password:
su: Authentication failure
```

Run commands as specific users (not root)

Examples to execute a command as testuser (created recently)

Run a single command as testuser (using sudo)

```
ubuntu1@Ubuntu1:~$ sudo -u testuser id  
uid=1002(testuser) gid=1002(testuser) groups=1002(testus  
ubuntu1@Ubuntu1:~$ sudo -u testuser bash -c 'whoami; tou  
/tmp/testfile_by_testuser; ls -l /tmp/testfile_by_testus  
  
testuser  
-rwx-rw-r-- 1 testuser testuser 0 Sep 29 19:14 /tmp/testf  
_bytestuser  
ubuntu1@Ubuntu1:~$
```

Analyzing login / sudo patterns using logs

Commands to extract recent relevant entries

For systemd systems: SSH/session journal (last 7 days)

Show only sudo usage entries

List recent successful interactive logins

Name: Irumva Jason ID:27241 Date:Fri/26th/2025

```
ubuntu1@Ubuntu1:~$ sudo journalctl --since "7 days ago"
--TIMEFORMAT=iso8601
TEMU_UNIT=sshd.service | tail -n 200
-- No entries --
```

```
ubuntu1@Ubuntu1:~$ sudo grep -E "session opened|session closed|Accepted|Failed password|sudo" /var/log/auth.log | tail -n 200
2025-09-28T21:15:01.214382+00:00 Ubuntu1 CRON[6836]: pam_unix(cron:session): session closed for user root
2025-09-28T21:17:01.234813+00:00 Ubuntu1 CRON[6848]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
2025-09-28T21:17:01.360929+00:00 Ubuntu1 CRON[6848]: pam_unix(cron:session): session closed for user root
2025-09-28T21:25:01.422947+00:00 Ubuntu1 CRON[6899]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
2025-09-28T21:25:01.469652+00:00 Ubuntu1 CRON[6899]: pam_unix(cron:session): session closed for user root
2025-09-28T21:30:01.581945+00:00 Ubuntu1 CRON[6940]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
2025-09-28T21:30:01.596258+00:00 Ubuntu1 CRON[6940]: pam_unix(cron:session): session closed for user root
2025-09-28T21:35:01.678221+00:00 Ubuntu1 CRON[6968]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
```

Name: Irumva Jason ID:27241 Date:Fri/26th/2025

```
ubuntu1@Ubuntu1:~$ sudo grep -E "session opened|session ed|Accepted|Failed password|sudo" /var/log/secure | tail 200
grep: /var/log/secure: No such file or directory
ubuntu1@Ubuntu1:~$ sudo grep -i "sudo:" /var/log/auth.log /var/log/secure 2>/dev/null | tail -n 200
/var/log/auth.log:2025-09-23T20:46:13.884404+00:00 Ubuntu
udo: ubuntu1 : TTY=pts/0 ; PWD=/home/ubuntu1 ; USER=root
COMMAND=/usr/bin/cp -r /home/mcbishop/Practice/P1/Hi/P3
e/mcbishop/Practice/Command/
/var/log/auth.log:2025-09-23T20:46:13.893446+00:00 Ubuntu
udo: pam_unix(sudo:session): session opened for user root
d=0) by ubuntu1(uid=1000)
/var/log/auth.log:2025-09-23T20:46:13.895941+00:00 Ubuntu
udo: pam_unix(sudo:session): session closed for user root
/var/log/auth.log:2025-09-28T16:32:58.351364+00:00 Ubuntu
udo: ubuntu1 : TTY=pts/0 ; PWD=/home/ubuntu1 ; USER=root
COMMAND=/usr/bin/apt update
/var/log/auth.log:2025-09-28T16:32:58.362481+00:00 Ubuntu
udo: pam_unix(sudo:session): session opened for user root
d=0) by ubuntu1(uid=1000)
/var/log/auth.log:2025-09-28T16:33:21.992118+00:00 Ubuntu
udo: pam_unix(sudo:session): session closed for user root
/var/log/auth.log:2025-09-28T16:35:33.561464+00:00 Ubuntu
udo: ubuntu1 : TTY=pts/0 : PWD=/home/ubuntu1 : USER=roo
```

Name: Irumva Jason ID:27241 Date:Fri/26th/2025

```
ubuntu1@Ubuntu1:~$ sudo last -a | head -n 20
ubuntu1  tty2          Mon Sep 29 18:19  still logged in
tty2
ubuntu1  seat0         Mon Sep 29 18:19  still logged in
login screen
reboot   system boot   Mon Sep 29 18:16  still running
6.11.0-24-generic
colleagu tty3          Mon Sep 29 16:56 - crash (01:19)
tty3
colleagu seat0         Mon Sep 29 16:56 - crash (01:19)
login screen
ubuntu1  tty2          Mon Sep 29 16:54 - crash (01:21)
tty2
ubuntu1  seat0         Mon Sep 29 16:54 - 16:56 (00:02)
login screen
reboot   system boot   Mon Sep 29 16:54  still running
6.11.0-24-generic
ubuntu1  tty2          Mon Sep 29 15:56 - crash (00:58)
tty2
ubuntu1  seat0         Mon Sep 29 15:56 - crash (00:58)
login screen
ubuntu1  tty2          Mon Sep 29 14:09 - 15:56 (01:46)
tty2
ubuntu1  seat0         Mon Sep 29 14:09 - 15:56 (01:46)
login screen
reboot   system boot   Mon Sep 29 14:09  still running
```

Identifying overly permissive sudo configs (commands to find them)

Search for NOPASSWD, wildcard commands, or full ALL grants.

Find NOPASSWD entries

Find ALL=(ALL) grants to users/groups

Show per-user sudo rights for all non-system users

```
ubuntu1@Ubuntu1:~$ sudo grep -R "NOPASSWD" /etc/sudoers /  
/sudoers.d 2>/dev/null || echo "none found"  
none found  
ubuntu1@Ubuntu1:~$ sudo grep -R "ALL=(ALL)" /etc/sudoers  
c/sudoers.d 2>/dev/null || echo "none found"  
/etc/sudoers:%admin ALL=(ALL) ALL  
ubuntu1@Ubuntu1:~$ awk -F: '$3>=1000{print $1}' /etc/pass  
| while read u; do  
    echo "== sudo -l for $u ==";  
    sudo -l -U "$u" 2>/dev/null || echo "no data for $u";  
done  
== sudo -l for nobody ==  
User nobody is not allowed to run sudo on Ubuntu1.  
== sudo -l for ubuntu1 ==  
Matching Defaults entries for ubuntu1 on Ubuntu1:  
    env_reset, mail_badpass,  
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbi  
/usr/bin\:/sbin\:/bin\:/snap/bin,  
    use_pty  
  
User ubuntu1 may run the following commands on Ubuntu1:  
    (ALL : ALL) ALL  
== sudo -l for otheruser ==  
User otheruser is not allowed to run sudo on Ubuntu1.  
== sudo -l for testuser ==
```

Potential security concerns & concise improvements (apply these)

Concerns found by the commands above

NOPASSWD entries → command execution without authentication.

ALL=(ALL) grants → users can run any command as root.

Wildcard or path-writable command entries → attackers can replace binaries.

Excessive group membership (e.g., users in wheel/admin) → privilege creep.

Lack of logging/auditing → hard to trace misuse.

Recommended fixes (commands to implement or check)

1) Remove/replace NOPASSWD where not needed (use visudo to edit safely)

```
sudo visudo      # edit /etc/sudoers safely
```

```
sudo visudo -f /etc/sudoers.d/custom # edit drop-in files safely
```

2) Replace ALL with specific allowed commands (example)

```
in visudo: alice ALL=(root) /usr/bin/systemctl, /usr/bin/journalctl
```

3) Force TTY & require authentication

```
in sudoers: Defaults requiretty (RHEL) and remove NOPASSWD entries
```

4) Enable sudo logging (if not already)

```
sudo mkdir -p /var/log/sudo && sudo chown root:root /var/log/sudo
```

```
Ensure /etc/sudoers has Defaults logfile=/var/log/sudo/sudo.log
```

5) Use groups and least-privilege:

```
sudo groupadd backupops 2>/dev/null || true
```

```
add only necessary commands to group via sudoers file for group 'backupops'
```

6) Enforce MFA for sudo via PAM (installation/config needed; policy change)

(policy/config step; not a single command)

Qn17: Creating forensic directory tree (all inside ~/forensic_lab)

Name: Irumva Jason ID:27241 Date:Fri/26th/2025

```
ubuntu1@Ubuntu1:~$ mkdir -p ~/forensic_lab/{regular,dirs,perms,owners,archives,devices}
ubuntu1@Ubuntu1:~$ ls -ld ~/forensic_lab && ls -R ~/forensic_lab
drwxrwxr-x 9 ubuntu1 ubuntu1 4096 Sep 29 20:26 /home/ubuntu1/forensic_lab
/home/ubuntu1/forensic_lab:
archives devices dirs links owners perms regular

/home/ubuntu1/forensic_lab/archives:
/home/ubuntu1/forensic_lab/devices:
/home/ubuntu1/forensic_lab/dirs:
/home/ubuntu1/forensic_lab/links:
/home/ubuntu1/forensic_lab/owners:
/home/ubuntu1/forensic_lab/perms:
/home/ubuntu1/forensic_lab/regular:
```

___ Regular files (small, medium, large)

Directories with content

Name: Irumva Jason ID:27241 Date:Fri/26th/2025

```
ubuntu1@Ubuntu1:~$ echo "short" > ~/forensic_lab/regular/short.txt
ubuntu1@Ubuntu1:~$ yes "line" | head -n 1000 > ~/forensic_lab/regular/medium.txt
ubuntu1@Ubuntu1:~$ head -c 1M </dev/urandom > ~/forensic_lab/regular/large.bin
ubuntu1@Ubuntu1:~$ ls -lh ~/forensic_lab/regular
total 1.1M
-rw-rw-r-- 1 ubuntu1 ubuntu1 1.0M Sep 29 20:32 large.bin
-rw-rw-r-- 1 ubuntu1 ubuntu1 4.9K Sep 29 20:31 medium.txt
-rw-rw-r-- 1 ubuntu1 ubuntu1      6 Sep 29 20:31 small.txt
ubuntu1@Ubuntu1:~$ file ~/forensic_lab/regular/* | sed -z -e '3p'
/home/ubuntu1/forensic_lab/regular/large.bin:  data
/home/ubuntu1/forensic_lab/regular/medium.txt: ASCII text
/home/ubuntu1/forensic_lab/regular/small.txt:  ASCII text
ubuntu1@Ubuntu1:~$ mkdir -p ~/forensic_lab/dirs/{empty,onlyhidden,hasfiles}
ubuntu1@Ubuntu1:~$ touch ~/forensic_lab/dirs/onlyhidden/ret
ubuntu1@Ubuntu1:~$ touch ~/forensic_lab/dirs/hasfiles/a.txt
~/forensic_lab/dirs/hasfiles/b.txt
ubuntu1@Ubuntu1:~$ ls -laR ~/forensic_lab/dirs
/home/ubuntu1/forensic_lab/dirs:
total 20
```

Name: Irumva Jason ID:27241 Date:Fri/26th/2025

```
/home/ubuntu1/forensic_lab/dirs/empty:  
total 8  
drwxrwxr-x 2 ubuntu1 ubuntu1 4096 Sep 29 20:34 .  
drwxrwxr-x 5 ubuntu1 ubuntu1 4096 Sep 29 20:34 ..  
  
/home/ubuntu1/forensic_lab/dirs/hasfiles:  
total 8  
drwxrwxr-x 2 ubuntu1 ubuntu1 4096 Sep 29 20:34 .  
drwxrwxr-x 5 ubuntu1 ubuntu1 4096 Sep 29 20:34 ..  
-rw-rw-r-- 1 ubuntu1 ubuntu1 0 Sep 29 20:34 a.txt  
-rw-rw-r-- 1 ubuntu1 ubuntu1 0 Sep 29 20:34 b.txt
```

___ Symbolic link and hard link

Symlink

hardlink (same inode as small.txt)

Name: Irumva Jason ID:27241 Date:Fri/26th/2025

```
ubuntu1@Ubuntu1:~$ ln -s ~/forensic_lab/regular/small.txt  
forensic_lab/links/small_link.txt  
ubuntu1@Ubuntu1:~$ ln ~/forensic_lab/regular/small.txt ~/forensic_lab/links/small_hardlink.txt  
ubuntu1@Ubuntu1:~$ ls -li ~/forensic_lab/regular/small.txt  
/forensic_lab/links  
1573007 -rw-rw-r-- 2 ubuntu1 ubuntu1 6 Sep 29 20:31 /  
/ubuntu1/forensic_lab/regular/small.txt  
  
/home/ubuntu1/forensic_lab/links:  
total 4  
1573007 -rw-rw-r-- 2 ubuntu1 ubuntu1 6 Sep 29 20:31 smallhardlink.txt  
1573016 lrwxrwxrwx 1 ubuntu1 ubuntu1 44 Sep 29 20:38 small_link.txt  
ubuntu1@Ubuntu1:~$ stat -c "%n → %F" ~/forensic_lab/links/small_link.txt  
2>/dev/null || true  
/home/ubuntu1/forensic_lab/links/small_hardlink.txt → regular file  
/home/ubuntu1/forensic_lab/links/small_link.txt → symbolic link
```

Device file (requires root) — *simulated* character device (e.g., /dev/null-like)

creating a character device with major=1 minor=3 (null) — needs sudo

```
ubuntu1@Ubuntu1:~$ sudo mknod ~/forensic_lab/devices/null_chr c 1 3  
[sudo] password for ubuntu1:  
ubuntu1@Ubuntu1:~$ sudo chown root:root ~/forensic_lab/devices/null_chr  
ubuntu1@Ubuntu1:~$ ls -l ~/forensic_lab/devices  
total 0  
crw-r----- 1 root root 1, 3 Sep 29 20:40 null_chr  
ubuntu1@Ubuntu1:~$ file -s ~/forensic_lab/devices/null_chr  
/home/ubuntu1/forensic_lab/devices/null_chr: empty
```

___Permission combinations including special bits
creating target files/dirs.

Setting bits: setuid, setgid, sticky, world-writable...

```
ubuntu1@Ubuntu1:~$ touch ~/forensic_lab/perms/runme ~/fo  
rensic_lab/perms/gdirfile  
ubuntu1@Ubuntu1:~$ mkdir -p ~/forensic_lab/perms/sticky_d  
ubuntu1@Ubuntu1:~$ chmod 4755 ~/forensic_lab/perms/runme  
ubuntu1@Ubuntu1:~$ chmod 2755 ~/forensic_lab/perms/gdirf  
ubuntu1@Ubuntu1:~$ chmod 1777 ~/forensic_lab/perms/sticky_d  
r  
ubuntu1@Ubuntu1:~$ chmod 666 ~/forensic_lab/perms/world_w  
rite  
chmod: cannot access '/home/ubuntu1/forensic_lab/perms/wor  
ld_write': No such file or directory  
ubuntu1@Ubuntu1:~$ mkdir 666 ~/forensic_lab/perms/world_w  
rite  
ubuntu1@Ubuntu1:~$ chmod 666 ~/forensic_lab/perms/world_w  
rite  
ubuntu1@Ubuntu1:~$ touch ~/forensic_lab/perms/world_writ  
ubuntu1@Ubuntu1:~$ ls -l ~/forensic_lab/perms  
total 8  
-rwxr-sr-x 1 ubuntu1 ubuntu1 0 Sep 29 20:42 gdirfile  
-rwsr-xr-x 1 ubuntu1 ubuntu1 0 Sep 29 20:42 runme  
drwxrwxrwt 2 ubuntu1 ubuntu1 4096 Sep 29 20:42 sticky_d  
drw-rw-rw- 2 ubuntu1 ubuntu1 4096 Sep 29 20:45 world_wri  
ubuntu1@Ubuntu1:~$ getfacl ~/forensic_lab/perms 2>/dev/n  
| sed -n '1,50p'  
# file: home/ubuntu1/forensic_lab/perms
```

___Files with different ownership patterns

Name: Irumva Jason ID:27241 Date:Fri/26th/2025

making a file owned by root (requires sudo)

a file owned by current user (already)

```
ubuntu1@Ubuntu1:~$ touch ~/forensic_lab/owners/root_owned.txt
ubuntu1@Ubuntu1:~$ sudo chown root:root ~/forensic_lab/owners/root_owned.txt
[sudo] password for ubuntu1:
ubuntu1@Ubuntu1:~$ touch ~/forensic_lab/owners/user_owned.txt
ubuntu1@Ubuntu1:~$ ls -l ~/forensic_lab/owners
total 0
-rw-rw-r-- 1 root      root      0 Sep 29 21:21 root_owned.txt
-rw-rw-r-- 1 ubuntu1   ubuntu1   0 Sep 29 21:22 user_owned.txt
ubuntu1@Ubuntu1:~$ stat -c "%n uid=%u(%U) gid=%g(%G)" ~/forensic_lab/owners/*
/home/ubuntu1/forensic_lab/owners/root_owned.txt uid=0(root)
gid=0(root)
/home/ubuntu1/forensic_lab/owners/user_owned.txt uid=1000(ubuntu1)
gid=1000(ubuntu1)
```

___Creating archives with different compression

creating sample files to archive

creating archives

Name: Irumva Jason ID:27241 Date:Fri/26th/2025

```
.gz -C ~/forensic_lab/archives/src .
ubuntu1@Ubuntu1:~$ tar -cjf ~/forensic_lab/archives/test.
.bz2 -C ~/forensic_lab/archives/src .
ubuntu1@Ubuntu1:~$ tar -cJf ~/forensic_lab/archives/test.
.xz -C ~/forensic_lab/archives/src .
ubuntu1@Ubuntu1:~$ zip -r ~/forensic_lab/archives/test.zip
~/forensic_lab/archives/src >/dev/null
ubuntu1@Ubuntu1:~$ tar -tzf ~/forensic_lab/archives/test.
.gz
.-
./b.log
./a.conf
ubuntu1@Ubuntu1:~$ tar -tjf ~/forensic_lab/archives/test.
.bz2 prac
.-
./
./b.log
./a.conf
ubuntu1@Ubuntu1:~$ tar -tJf ~/forensic_lab/archives/test.
.xz
unzip -l ~/forensic_lab/archives/test.zip
.-
./b.log
./a.conf
Archive: /home/ubuntu1/forensic_lab/archives/test.zip
      Length      Date      Time      Name
      -----      ----      ----      -----
      16005
3 files
ubuntu1@Ubuntu1:~$
```

___ Commands to analyze each element (quick investigators' toolbox with results shown)

file type

detailed metadata (owner/perm/ctime/mtime/atime)

find setuid/setgid/sticky/world-writable files

list symlinks and their targets

show inodes (to detect hardlinks)

examine archives without extracting (safe)

Name: Irumva Jason ID:27241 Date:Fri/26th/2025

```
ubuntu1@Ubuntu1:~$ file -s ~/forensic_lab/**/* 2>/dev/null | sed -ne '1,80p'  
/home/ubuntu1/forensic_lab/archives/src: directory  
/home/ubuntu1/forensic_lab/archives/test.tar.bz2: bzip2 compressed data, block size = 900k  
/home/ubuntu1/forensic_lab/archives/test.tar.gz: gzip compressed data, from Unix, original size modulo 2^32 204800  
/home/ubuntu1/forensic_lab/archives/test.tar.xz: XZ compressed data, checksum CRC64  
/home/ubuntu1/forensic_lab/archives/test.zip: Zip archive data, at least v1.0 to extract, compression method=deflate  
/home/ubuntu1/forensic_lab/devices/null_chr: empty  
/home/ubuntu1/forensic_lab/dirs/empty: directory  
/home/ubuntu1/forensic_lab/dirs/hasfiles: directory  
/home/ubuntu1/forensic_lab/dirs/onlyhidden: directory  
/home/ubuntu1/forensic_lab/links/small_hardlink.txt: ASCII text  
/home/ubuntu1/forensic_lab/links/small_link.txt: symbolic link to /home/ubuntu1/forensic_lab/regular/small.txt  
/home/ubuntu1/forensic_lab/owners/root_owned.txt: empty
```

Name: Irumva Jason ID:27241 Date:Fri/26th/2025

```
ubuntu1@Ubuntu1:~$ stat -c "%n | %F | %A | uid=%u(%U) gid=%G) | size=%s | atime=%x | mtime=%y | ctime=%z" ~/forensic_lab/**/* 2>/dev/null | sed -n '1,80p'
/home/ubuntu1/forensic_lab/archives/src | directory | drwxr-x | uid=1000(ubuntu1) gid=1000(ubuntu1) | size=4096 | atime=2025-09-29 21:23:38.087108208 +0000 | mtime=2025-09-29 21:23:27.507028740 +0000 | ctime=2025-09-29 21:23:27.507028740 +0000
/home/ubuntu1/forensic_lab/archives/test.tar.bz2 | regular file | -rw-rw-r-- | uid=1000(ubuntu1) gid=1000(ubuntu1) | size=217 | atime=2025-09-29 21:25:49.021134933 +0000 | mtime=2025-09-29 21:23:47.721181710 +0000 | ctime=2025-09-29 21:23:47.721181710 +0000
/home/ubuntu1/forensic_lab/archives/test.tar.gz | regular file | -rw-rw-r-- | uid=1000(ubuntu1) gid=1000(ubuntu1) | size=16 | atime=2025-09-29 21:25:32.720003423 +0000 | mtime=2025-09-29 21:23:38.104108338 +0000 | ctime=2025-09-29 21:23:38.104108338 +0000
/home/ubuntu1/forensic_lab/archives/test.tar.xz | regular file | -rw-rw-r-- | uid=1000(ubuntu1) gid=1000(ubuntu1) | size=60 | atime=2025-09-29 21:26:00.150225147 +0000 | mtime=2025-09-29 21:23:58.469263711 +0000 | ctime=2025-09-29 21:23:58.469263711 +0000
/home/ubuntu1/forensic_lab/archives/test.zip | regular file | -rw-rw-r-- | uid=1000(ubuntu1) gid=1000(ubuntu1) | size=
```

Name: Irumva Jason ID:27241 Date:Fri/26th/2025

```
ubuntu1@Ubuntu1:~$ find ~/forensic_lab -perm /4000 -o -perm /2000 -o -perm -0002 -o -perm /1000 -ls
ubuntu1@Ubuntu1:~$ find ~/forensic_lab -type l -ls
1573016          0 lrwxrwxrwx  1 ubuntu1  ubuntu1
p 29 20:38 /home/ubuntu1/forensic_lab/links/small_link.txt
/home/ubuntu1/forensic_lab/regular/small.txt
ubuntu1@Ubuntu1:~$ ls -liR ~/forensic_lab | sed -n '1,12G
/home/ubuntu1/forensic_lab:
total 28
1573005 drwxrwxr-x 3 ubuntu1  ubuntu1 4096 Sep 29 21:24 ar
es
1573006 drwxrwxr-x 2 ubuntu1  ubuntu1 4096 Sep 29 20:40 de
s
1572995 drwxrwxr-x 5 ubuntu1  ubuntu1 4096 Sep 29 20:34 di
1573000 drwxrwxr-x 2 ubuntu1  ubuntu1 4096 Sep 29 20:38 li
1573002 drwxrwxr-x 2 ubuntu1  ubuntu1 4096 Sep 29 21:22 ow
1573001 drwxrwxr-x 4 ubuntu1  ubuntu1 4096 Sep 29 20:45 pe
1572985 drwxrwxr-x 2 ubuntu1  ubuntu1 4096 Sep 29 20:32 re
r

/home/ubuntu1/forensic_lab/archives:
total 20
1573033 drwxrwxr-x 2 ubuntu1  ubuntu1 4096 Sep 29 21:23 sr
1573038 -rw-rw-r-- 1 ubuntu1  ubuntu1   217 Sep 29 21:23 te
ar.bz2
```

Name: Irumva Jason ID:27241 Date:Fri/26th/2025

```
ubuntu1@Ubuntu1:~$ tar -tzf ~/forensic_lab/archives/test.gz
gz   Home
./
./b.log
./a.conf
ubuntu1@Ubuntu1:~$ tar -tjf ~/forensic_lab/archives/test.bz2
bz2
./growthsstore
./b.log
./a.conf
ubuntu1@Ubuntu1:~$ unzip -l ~/forensic_lab/archives/test.zip
Archive: /home/ubuntu1/forensic_lab/archives/test.zip
      Length      Date      Time    Name
      -----      ----      ----
      0 2025-09-29 21:23  home/ubuntu1/forensic_lab/
ves/src/
      16000 2025-09-29 21:23  home/ubuntu1/forensic_lab/
ves/src/b.log
      5 2025-09-29 21:23  home/ubuntu1/forensic_lab/
ves/src/a.conf
      -----
      16005
      3 files
ubuntu1@Ubuntu1:~$
```

10) How an investigator uses this info (brief bullet points)

Use the outputs above to:

- Identify unexpected SUID/SGID binaries (may be used for privilege escalation).
- Detect world-writable files/dirs (can be abused to drop backdoors).
- Find device nodes in user-writable locations (suspicious; device nodes are rarely created in home dirs).
- Compare inodes to see hardlinks (hidden copies of files can be hidden via hardlinks).
- Follow symlink targets (symlink to sensitive files is a red flag).
- Check timestamps (mtime/ctime/atime) for tampering or timeline reconstruction.
- Inspect archive contents without extraction to find suspicious payloads.

Note: These are observations to draw from the commands I ran above.

File system artifacts that may indicate unauthorized access / compromise (brief)

- Unexpected setuid/setgid files added recently.
- Binaries with changed ctime/mtime but no package update.
- New device nodes or cron entries in nonstandard locations.
- World-writable directories where binaries/scripts are stored.
- Hidden files (dotfiles) with recent execution timestamps.
- Multiple hardlinks to suspicious binaries (hiding copies).
- Compressed archives with obfuscated names or nested payloads.
- Log files with gaps, truncated entries, or cleared logs (log tampering).