LAB SHEET 3
Access Control & ACLs on Linux

Madene Meriem Group 01

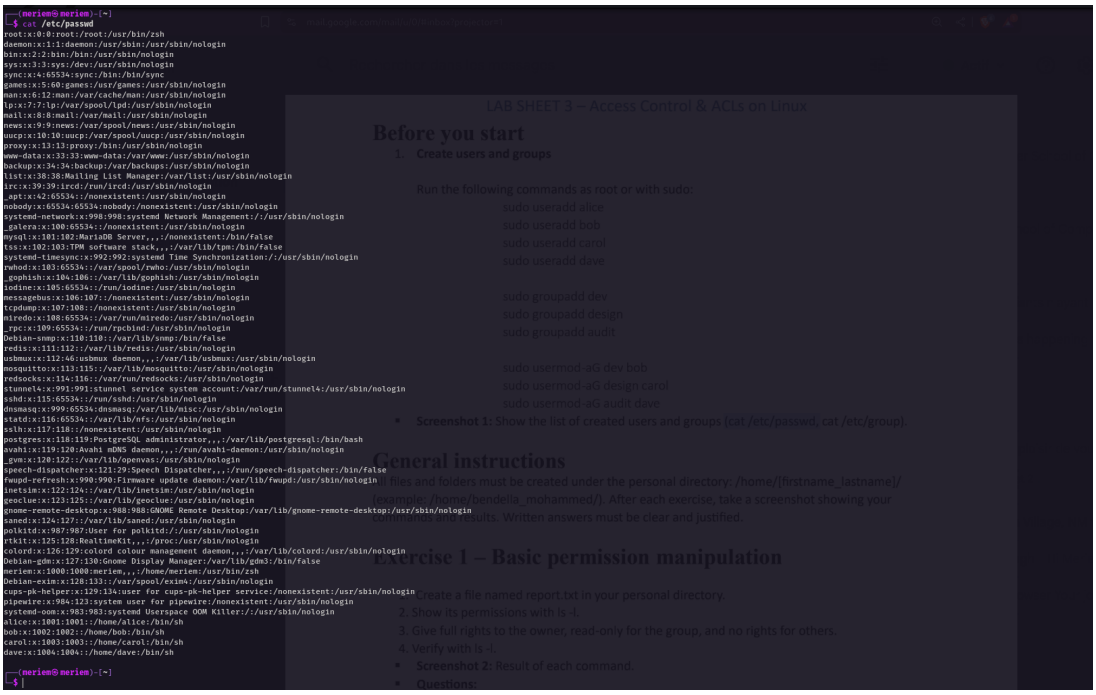
October 22, 2025

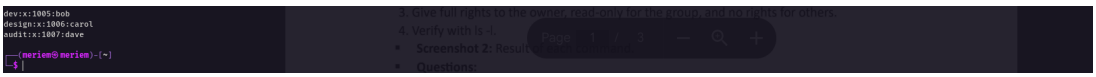
1 Setup - Users and Groups

Commands executed:

```
sudo useradd alice
sudo useradd bob
sudo useradd carol
sudo useradd dave
sudo groupadd dev
sudo groupadd design
sudo groupadd audit
sudo usermod -aG dev bob
sudo usermod -aG design carol
sudo usermod -aG audit dave
cat /etc/passwd
cat /etc/group
```

Screenshot 1:



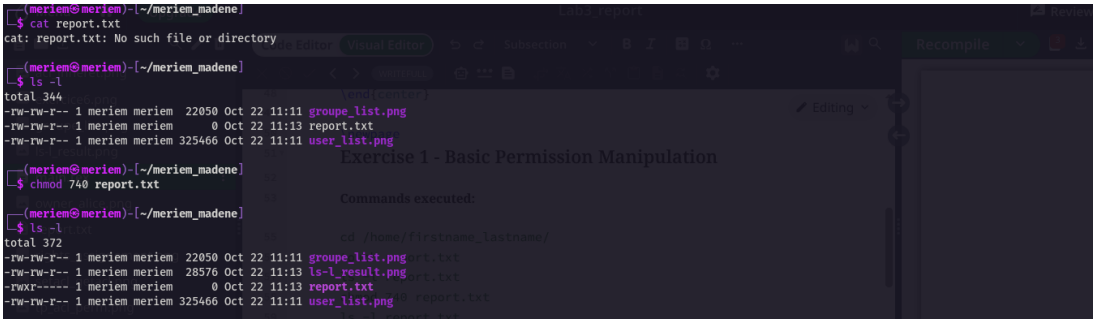


2 Exercise 1 - Basic Permission Manipulation

Commands executed:

```
cd /home/firstname_lastname/
touch report.txt
ls -l report.txt
chmod 740 report.txt
ls -l report.txt
```

Screenshot 2:



2.1 Questions

What is the numeric value corresponding to these rights?

The numeric value is 740: owner = 7 for all the rights / group = 4 for read only / others = 0 for no rights

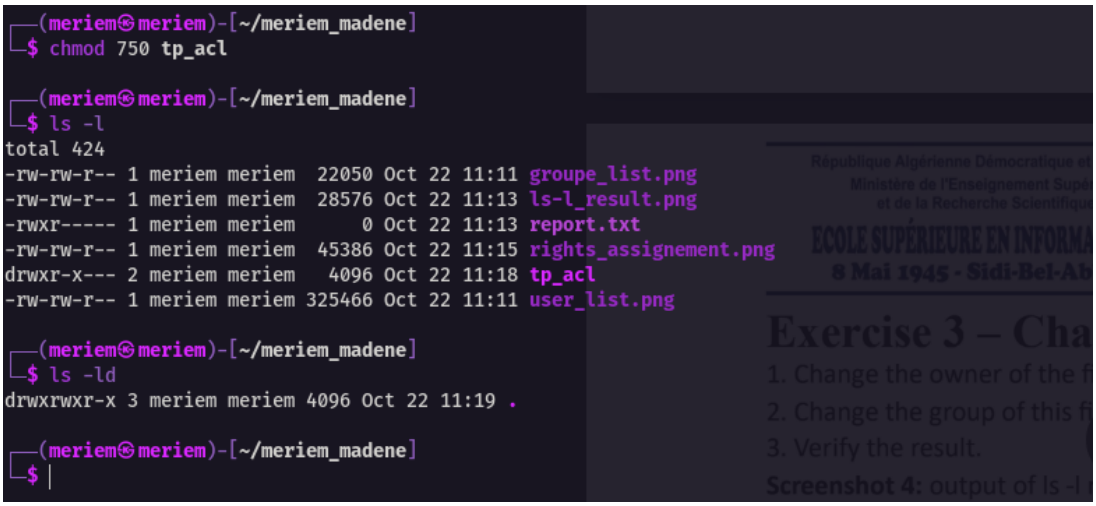
Is the principle of least privilege respected? Why? Yes the principle is respected here because we are giving to each user the only privileges they need .

3 Exercise 2 - Directory Management

Commands executed:

```
mkdir tp_acl
chmod 750 tp_acl
ls -ld tp_acl
```

Screenshot 3:



3.1 Question

What is the difference between the execute right on a file and on a directory?

Execute on a file allows running it as a program. Execute on a directory allows accessing its contents (entering with cd and listing files). Without execute on a directory, you cannot access files inside even if you have read permission.

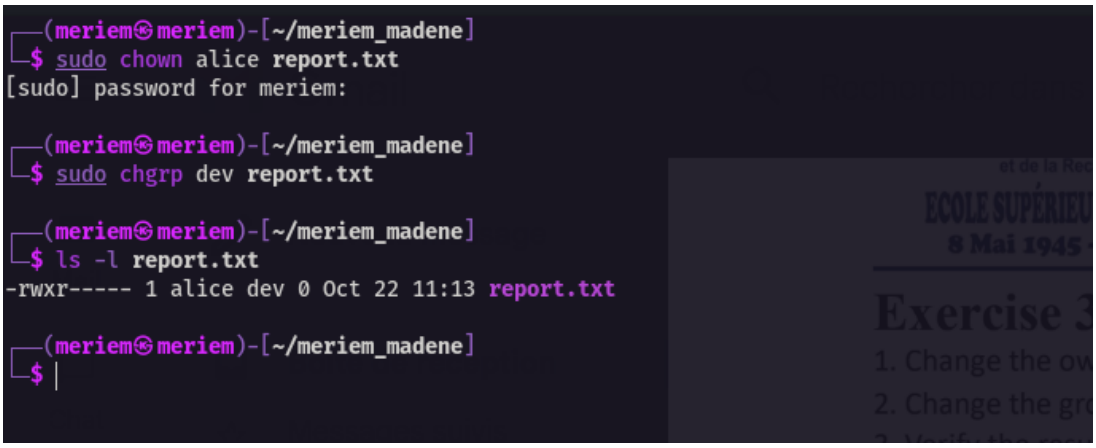
Execute on file allows executing the file itself , whule the execute in the folder allows access to the content of the folder like cd command , because if we remove exe on dir you won't access the files inside

4 Exercise 3 - Change Owner and Group

Commands executed:

```
sudo chown alice report.txt
sudo chgrp dev report.txt
ls -l report.txt
```

Screenshot 4:



4.1 Question

What is the difference between chown and chgrp?

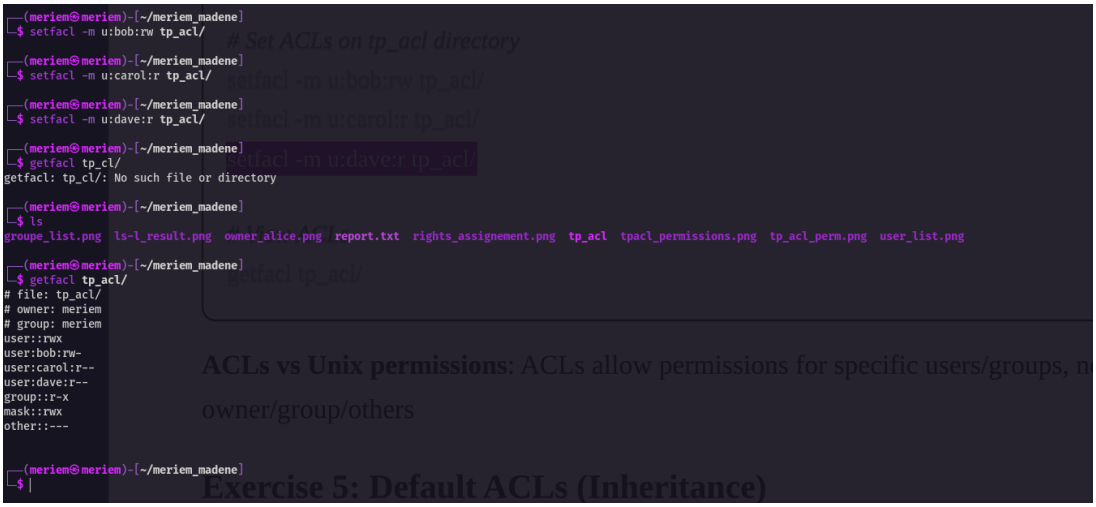
chown changes the owner of a file, while chgrp changes only the group. You can also use chown to change both at once with the syntax: chown user:group file.

5 Exercise 4 - ACL: Fine-grained Access Control

Commands executed:

```
sudo apt install acl -y
setfacl -m u:bob:rw tp_acl/
setfacl -m u:carol:r tp_acl/
setfacl -m u:dave:r tp_acl/
getfacl tp_acl/
```

Screenshot 5:



5.1 Question

What is the difference between an ACL and classic Unix permissions?

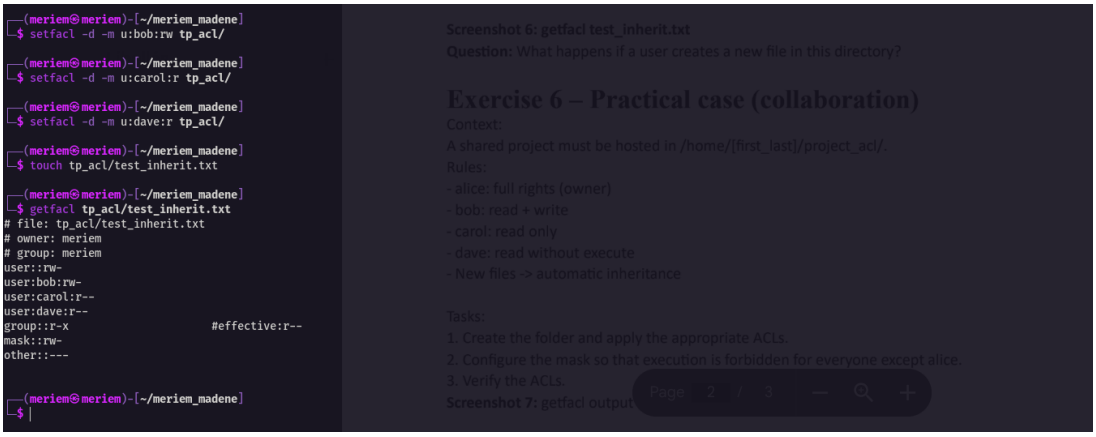
Classic Unix permissions only support three permission levels (owner, group, others). ACLs allow setting specific permissions for multiple individual users and groups, providing fine-grained access control beyond the traditional model.

6 Exercise 5 - ACL Inheritance

Commands executed:

```
setfacl -m d:u:bob:rw tp_acl/
setfacl -m d:u:carol:r tp_acl/
setfacl -m d:u:dave:r tp_acl/
touch tp_acl/test_inherit.txt
getfacl tp_acl/test_inherit.txt
```

Screenshot 6:



6.1 Question

What happens if a user creates a new file in this directory?

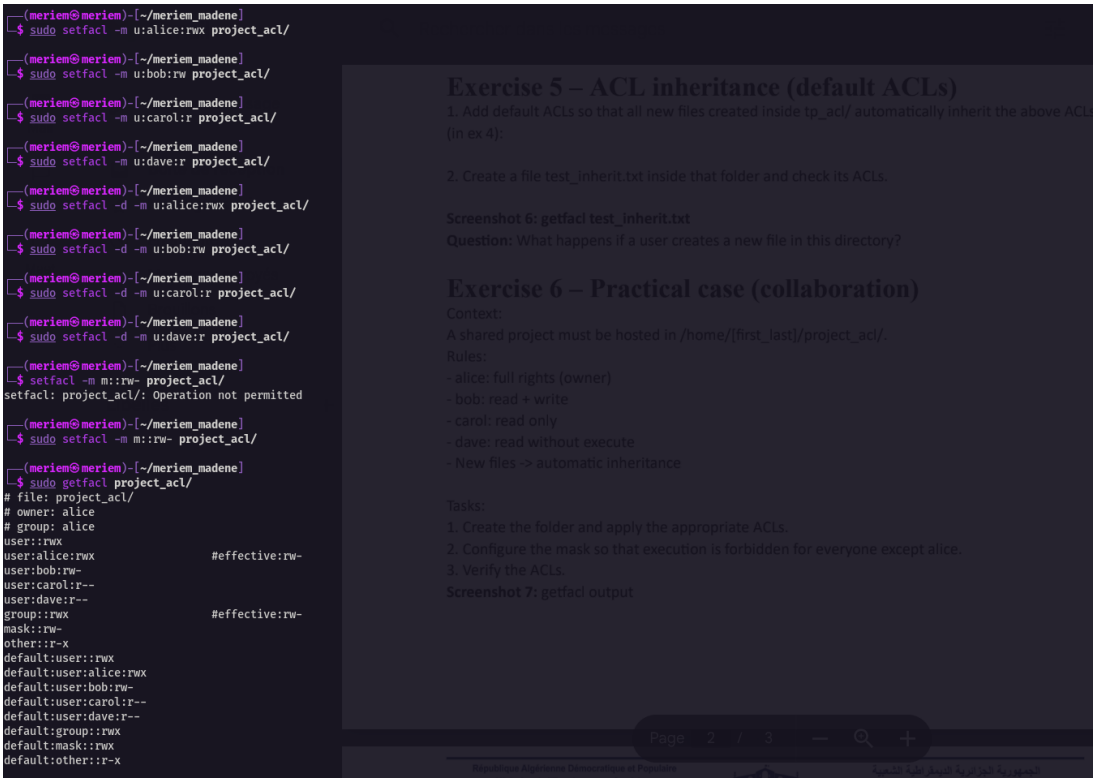
When a user creates a new file in this directory, it automatically inherits the default ACLs that were set on the parent directory. This ensures consistent permissions for all new files without manual configuration.

7 Exercise 6 - Practical Case

Commands executed:

```
mkdir project_acl
sudo chown alice project_acl
setfacl -m u:alice:rwx project_acl/
setfacl -m u:bob:rw project_acl/
setfacl -m u:carol:r project_acl/
setfacl -m u:dave:r project_acl/
setfacl -m d:u:alice:rwx project_acl/
setfacl -m d:u:bob:rw project_acl/
setfacl -m d:u:carol:r project_acl/
setfacl -m d:u:dave:r project_acl/
setfacl -m m::rw project_acl/
getfacl project_acl/
```

Screenshot 7:



8 Exercise 7 - Attack Simulation and Remediation

Commands executed:

```
ssh student@<metasploitable_ip>
cd /home/student/
touch secret.txt
chmod 777 secret.txt
ls -l secret.txt

# From another user
su - otheruser
echo "unauthorized access" >> /home/student/secret.txt
cat /home/student/secret.txt

# Fix (as student)
chmod 600 secret.txt
ls -l secret.txt

# Test fix
su - otheruser
cat /home/student/secret.txt
```

Screenshot 10:

screenshot10.png

8.1 Questions

What is the security flaw here?

The security flaw is that chmod 777 gives full permissions (read, write, execute) to everyone on the system. Any user can read sensitive data, modify the file content, or delete it entirely. This violates confidentiality and integrity principles.

How to fix it? (Apply least privilege)

Apply chmod 600 to restrict access to only the owner. This gives read and write permissions only to the file owner, with no access for group or others, following the principle of least privilege.