Users and Access Control

Lab

This work is about proving that you understand Linux permissions as statements about who can do what. You will create controlled-access conditions, test them by assuming different identities, and translate the results into plain language. Nothing here is about memorizing chmod values. Everything is about verifying that your mental model matches reality.

What this work actually does

You will:

- Create test users and groups to represent identities.
- Create files and directories that represent assets.
- Set permissions deliberately to express specific access decisions.
- Test those decisions by running commands as another user.
- Translate permission settings into clear English statements.
- Remove everything when finished so the system returns to a clean state.

The key mechanic is verification. You do not assume permissions work. You prove they work by attempting access as the test user.

Tools you will use

You are expected to use only standard Linux utilities.

Identity and ownership:

- `useradd, userdel`
- `groupadd, groupdel`
- `usermod`
- `id`
- `getent`
- `whoami`

Files and directories:

- `mkdir`
- `touch`
- `ls -l`
- `stat`
- `pwd`

Permissions:

- `chmod`
- `chown`
- `chgrp`

Testing access:

- `sudo -u <user>`
- `cat`
- `echo`
- `ls`
- `cd`

Cleanup:

- `rm`
- `rm -r`

If you are unsure which command to use, look it up (`man`). Choosing the correct tool is part of the work.

Rules

- Do all work in a dedicated test directory.
- Do not change permissions on real system files.
- Do not use your regular user as the test identity.
- Always test access using `sudo -u` rather than guessing.
- Translate every permission into plain language before moving on.
- Clean up all users, groups, and files at the end.

Step 1: Create test identities

Create one test group and one test user:

- Group name: lab3grp
- User name: lab3user

Add the user to the group.

Verify:

- The user exists.
- The group exists.
- The user is a member of the group.

Write down, in plain language:

- Which group does the lab3user belong to?

Step 2: Create test objects

Create a working directory for this exercise. Inside it, create:

- One regular file.
- One subdirectory.
- One file inside that subdirectory.

You are free to name them, but keep names consistent and straightforward.

Verify:

- All files and directories exist.
- You know which user owns them and which group they belong to.

Step 3: Deliberate permission setup

Configure permissions so that:

- The owner can read and write everything.
- Members of lab3grp can read some things and write some things.
- Others have restricted access.

Do not copy examples from memory. Decide what access you want first, then set permissions to match that decision.

For each file or directory, write one sentence: "Owner can ___. Group can ___. Others can ___."

Step 4: Test as the other user

Use sudo -u lab3user to test access.

For each file and directory, test:

- Can the test user read it?
- Can the test user write to it?
- Can the test user enter the directory?

Record what actually happens, not what you expected.

If access does not behave as intended:

- Adjust permissions.
- Retest.
- Update your English description.

Iteration is expected.

Step 5: The mystery directory

Create a directory with the following properties:

- lab3user can enter the directory.
- lab3user cannot list the directory contents.
- lab3user can read a specific file inside the directory if the filename is known.

Place a file inside the directory and verify:

- `ls` fails for lab3user.
- `cat` works for lab3user when given the full path.

Write, in plain language:

- What does execute permission mean on a directory?
- Why are listing and entering different actions?

Step 6: Translate permissions to English

For every file and directory you created, write:

- The owner.
- The group.
- One sentence describing exactly who can do what.

Example format: "The owner can read and modify this file. Members of lab3grp can read it but cannot modify it. All other users cannot access it."

If you cannot write this sentence confidently, revisit the permissions and retest.

Step 7: Clean up

Remove:

- All files and directories created for this work.
- The lab3user account.
- The lab3grp group.

Verify:

- The user no longer exists.
- The group no longer exists.
- No test files remain.

What to notice

- Permissions express trust decisions, not syntax.
- Group membership is often the real boundary.
- The directory execute controls traversal, not execution.
- Testing as another user quickly exposes incorrect assumptions.
- If you cannot describe access in English, you do not yet understand it.

Submission

Submit a short write-up that includes:

- The English permission statements for each object.
- One mistake you made and how testing revealed it.
- A brief explanation of the mystery directory in plain language.

The system should be unchanged after cleanup. The evidence should be your understanding, not leftover files.