Lab 3: Users and Access Control

Step 1: Create Test Identities

Create Group:

- Command used:

```
❯ sudo addgroup lab3grp
[sudo] password for markus:
info: Selecting GID from range 1000 to 59999 ...
info: Adding group `lab3grp' (GID 1001) ...
```

Create User:

- Command used:

```
❯ sudo useradd -m -s /bin/bash lab3user
[sudo] password for markus:
```

- Command to add user to group:

```
❯ sudo usermod -aG lab3grp lab3user
```

Verification:

- Id:

```
❯ id lab3user
uid=1001(lab3user) gid=1002(lab3user) groups=1002(lab3user),1001(lab3grp)
```

- Group:

```
❯ getent group lab3grp
lab3grp:x:1001:lab3user
```

- Which group does the lab3user belong to
  - The `lab3user` belongs to the `lab3grp` group.

Step 2: Create Test Objects

Setup:

- Working directory created:

```
~ via 🐍 v3.14.2
❯ mkdir netsec-lab3
```

- Regular file created:

```
~ via 🐍 v3.14.2
❯ echo "this is some line" >>  netsec-lab3/file
```

- Subdirectory created:

```
~ via 🐍 v3.14.2
❯ mkdir  netsec-lab3/subdir
```

- File inside subdirectory:

```
~ via 🐍 v3.14.2
❯ echo "this is another line in the subdir" >>  netsec-lab3/subdir/subfile
```

Verification:

- `ls -l` output showing ownership/group:

```
❯ ls -l netsec-lab3/
total 4
-rw-rw-r-- 1 markus markus    0 Jan 20 11:49 file
drwxrwxr-x 2 markus markus 4096 Jan 20 11:50 subdir/
```

- Who owns them?
  - `markus` (me)
- Which group do they belong to?
  - they belong to `markus` group

Step 3: Deliberate Permission Setup

Configure Permissions:

- Goal: Owner (RWX), Group (some read/write), Others (restricted).
- Commands used:

```
~ via 🐍 v3.14.2
❯ sudo chgrp -R lab3grp netsec-lab3/

~ via 🐍 v3.14.2
❯ chmod 000 netsec-lab3/*

~ via 🐍 v3.14.2
❯ chmod 000 netsec-lab3

~ via 🐍 v3.14.2
❯ chmod u+rwx,g=xr,o= netsec-lab3

~ via 🐍 v3.14.2
❯ chmod u+rw,g=rw,o= netsec-lab3/file

~ via 🐍 v3.14.2
❯ chmod u+rw,g=,o= netsec-lab3/subdir/subfile

~ via 🐍 v3.14.2
❯ ls -al netsec-lab3/
total 16
drwxr-x---  3 markus lab3grp 4096 Jan 20 11:58 ./
drwxr-x--- 35 markus markus  4096 Jan 20 11:49 ../
-rw-rw----  1 markus lab3grp   18 Jan 20 11:58 file
drwx------  2 markus lab3grp 4096 Jan 20 11:50 subdir/

~ via 🐍 v3.14.2
❯ ls -al netsec-lab3/subdir/
total 12
drwx------ 2 markus lab3grp 4096 Jan 20 11:50 ./
drwxr-x--- 3 markus lab3grp 4096 Jan 20 11:58 ../
-rw------- 1 markus lab3grp   35 Jan 20 11:58 subfile
```

1. `netsec-lab3` : Owner can read, write, execute. Group can write and execute. Others are restricted/
2. `file` : Owner can read, write and execute. Group can read and write. Others are restricted.
3. `subdir` : Owner can read write and execute. Group is restricted. Others are restricted.
4. `subfile` : Owner can read and write. Groups is restricted. Others are restricted.

Step 4: Test as the Other User

Test Access (run as `lab3user`):

```
lab3user@markus:/home/markus$ ls
ls: cannot open directory '.': Permission denied
```

Didn't give permissions on my home dir, where the `netsec-lab3` file was created

Gave read and execute permissions, this'll be reverted after the lab

```
~ via 🐍 v3.14.2
❯ chmod o=rx /home/markus/

~ via 🐍 v3.14.2
❯ sudo su lab3user
lab3user@markus:/home/markus$ ls
 Applications    misc                      Public            term5-backup2
 Bolic.Backend   Music                     snap             'term5 (Copy)'
 Desktop         netsec-lab3               stylus-remap.py   Videos
 Documents       nvim-linux-x86_64.tar.gz  Templates
 Downloads       Pictures                  term5
 keyd            projects                  term5-backup
lab3user@markus:/home/markus$
```

- Can test user READ the file?
  - Yes, this is expected

```
lab3user@markus:/home/markus$ cat netsec-lab3/file
this is some line
```

- Can test user WRITE to the file?
  - Yes, this is the only file it has permission for.

```
lab3user@markus:/home/markus$ echo -e  "this is a try to write" >> netsec-
lab3/file
lab3user@markus:/home/markus$ cat netsec-lab3/file
this is some line
this is a try to write
```

- Can test user ENTER the directory?
  - No, which should happen.

```
lab3user@markus:/home/markus$ cd netsec-lab3/subdir/
bash: cd: netsec-lab3/subdir/: Permission denied
```

Reflections:

- All permissions against the created files were working as expected as I double checked them using `ls- al`. But since I created in my `/home/markus` directory I did have to add `+rx` for the new user to be able to access the file in my home directory.

Step 5: The Mystery Directory

Create a directory where:

- `lab3user` CAN enter.
- `lab3user` CANNOT list contents.
- `lab3user` CAN read a specific file if they know the name.

```
~ via 🐍 v3.14.2
❯ mkdir mystery

~ via 🐍 v3.14.2
❯ echo "This should be readable" >> mystery/canread

~ via 🐍 v3.14.2
❯ chmod 700 mystery/

~ via 🐍 v3.14.2
❯ chmod 700 mystery/canread

~ via 🐍 v3.14.2
❯ chmod g+xr mystery/canread

~ via 🐍 v3.14.2
❯ chmod g+x mystery

~ via 🐍 v3.14.2
❯ sudo chgrp -R lab3grp mystery/canread

~ via 🐍 v3.14.2
❯ sudo chgrp -R lab3grp mystery/

~ via 🐍 v3.14.2
```

```
❯ sudo su lab3user
lab3user@markus:/home/markus$ cd mystery/
lab3user@markus:/home/markus/mystery$ ls
ls: cannot open directory '.': Permission denied
lab3user@markus:/home/markus/mystery$ cat canread
This should be readable

~ via 🐍 v3.14.2 took 21s
❯ ls -al mystery/
total 12
drwx--x---  2 markus lab3grp 4096 Jan 20 13:20 ./
drwxr-xr-x 36 markus markus  4096 Jan 20 13:20 ../
-rwxr-x---  1 markus lab3grp   24 Jan 20 13:20 canread*
```

Verification:

- `ls` command (as lab3user):
  - Fails, since group doesn't have `r` on the directory
- `cat <full_path>` (as lab3user):
  - Works, since group has `x`

Explanation:

- What does **execute** permission mean on a directory?
  - `x` permissions means the user/group can execute command against the directory like `cd` but doesn't allow read commands like `ls`
- Why are **listing** and **entering** different actions?
  - Listing requires read permissions, entering requires execute permissions.

Step 6: Translate Permissions to English

For every object created, write:

1. **Object Name:** `netsec-lab3/`
   - Owner: `markus`
   - Group: `lab3grp`
   - **Sentence:** The owner can read, write, and execute. Members of `lab3grp` can read and execute. Others cannot access it.
2. **Object Name:** `netsec-lab3/file`
   - Owner: `markus`
   - Group: `lab3grp`

- **Sentence:** The owner can read and write. Members of `lab3grp` can read and write. Others cannot access it.

3. **Object Name:** `netsec-lab3/subdir/`
   - Owner: `markus`
   - Group: `lab3grp`
   - **Sentence:** "The owner can read, write, and execute. Members of `lab3grp` can enter but can't list contents. Others cannot access it."
4. **Object Name:** `mystery/`
   - Owner: `markus`
   - Group: `lab3grp`
   - **Sentence:** "The owner can read, write, and execute. Members of `lab3grp` can enter but can't list contents. Others cannot access it."
5. **Object Name:** `mystery/canread`
   - Owner: `markus`
   - Group: `lab3grp`
   - **Sentence:** "The owner can read, write, and execute. Members of `lab3grp` can read but only with the file name. Others cannot access it."

Step 7: Clean Up

Commands used:

- Remove files/directories: `rm -rf netsec-lab3 mystery`
- Remove user: `sudo userdel -r lab3user`
- Remove group: `sudo groupdel lab3grp`

Verification:

- User exists?
  - No

```
~ via 🐍 v3.14.2
❯ sudo userdel lab3user
userdel: user 'lab3user' does not exist
```

- Group exists?
  - No

```
~ via 🐍 v3.14.2
❯ sudo groupdel lab3grp
groupdel: group 'lab3grp' does not exist
```

- Files remain?
  - No

```
~ via 🐍 v3.14.2
❯ find mystery
find: ‘mystery’: No such file or directory

~ via 🐍 v3.14.2
❯ find netsec-lab3
find: ‘netsec-lab3’: No such file or directory
```

Submission Summary

- **One mistake you made and how testing revealed it:**
  - Forgot that I created the `netsec-lab3` file in my home directory so when I switched to the `lab3user` I couldn't access it, just had to provide permissions.
- **Brief explanation of the mystery directory in plain language:**
  - The directory acts a room with the lights off, if someone knows where to look (the name of the file) then they can read it, if not they can't see what the file is called.