Assignment – 3

User & Group Management + File Security

- ## Tasks

Part 1: User & Group Setup

1. Create the following users:

○ Alice

○ bob

○ Charlie

```
ubuntu@ip-172-31-25-177:~$ sudo useradd alice
ubuntu@ip-172-31-25-177:~$ sudo useradd bob
ubuntu@ip-172-31-25-177:~$ sudo useradd charlie
```

```
ubuntu@ip-172-31-25-177:~$ tail /etc/passwd
polkitd:x:989:989:User for polkitd:/:/usr/sbin/nologin
ec2-instance-connect:x:109:65534::/nonexistent:/usr/sbin/nologin
_chrony:x:110:112:Chrony daemon,,,:/var/lib/chrony:/usr/sbin/nologin
ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash
meghna:x:1001:1001::/home/meghna:/bin/sh
testuser:x:1002:1002::/home/testuser:/bin/sh
mysql:x:111:113:MySQL Server,,,:/nonexistent:/bin/false
alice:x:1003:1005::/home/alice:/bin/sh
bob:x:1004:1006::/home/bob:/bin/sh
charlie:x:1005:1007::/home/charlie:/bin/sh
```

2. Create a group called:

○ devteam

```
ubuntu@ip-172-31-25-177:~$ sudo groupadd devteam
ubuntu@ip-172-31-25-177:~$ cat /etc/group
root:x:0:
```

```
developers:x:1004:meghna
mysql:x:113:
alice:x:1005:
bob:x:1006:
charlie:x:1007:
devteam:x:1008:
```

3. Add users Alice and bob to the devteam group.

```
ubuntu@ip-172-31-25-177:~$ sudo usermod -aG devteam alice
ubuntu@ip-172-31-25-177:~$ sudo usermod -aG devteam bob
ubuntu@ip-172-31-25-177:~$ id alice
uid=1003(alice) gid=1005(alice) groups=1005(alice),1008(devteam)
ubuntu@ip-172-31-25-177:~$ id bob
uid=1004(bob) gid=1006(bob) groups=1006(bob),1008(devteam)
```

4. Set passwords for all users

```
ubuntu@ip-172-31-25-177:~$ sudo passwd alice
New password:
Retype new password:
passwd: password updated successfully
ubuntu@ip-172-31-25-177:~$ sudo passwd bob
New password:
Retype new password:
passwd: password updated successfully
ubuntu@ip-172-31-25-177:~$ sudo passwd charlie
New password:
Retype new password:
passwd: password updated successfully
```

5. Verify:

   ○ User IDs and group memberships using id and groups.

```
ubuntu@ip-172-31-25-177:~$ id alice
uid=1003(alice) gid=1005(alice) groups=1005(alice),1008(devteam)
ubuntu@ip-172-31-25-177:~$ groups alice
alice : alice devteam
ubuntu@ip-172-31-25-177:~$ id bob
uid=1004(bob) gid=1006(bob) groups=1006(bob),1008(devteam)
ubuntu@ip-172-31-25-177:~$ groups bob
bob : bob devteam
ubuntu@ip-172-31-25-177:~$ id charlie
uid=1005(charlie) gid=1007(charlie) groups=1007(charlie)
ubuntu@ip-172-31-25-177:~$ groups charlie
charlie : charlie
```

Part 2: File Ownership & Permissions

1. Create a directory: /opt/project

```
ubuntu@ip-172-31-25-177:~$ mkdir opt
ubuntu@ip-172-31-25-177:~$ cd opt
ubuntu@ip-172-31-25-177:~/opt$ mkdir projectX
```

2. Change ownership:
   ○ Owner: alice
   ○ Group: devteam

```
ubuntu@ip-172-31-25-177:~$ sudo chown -R alice opt
ubuntu@ip-172-31-25-177:~$ sudo chgrp -R devteam opt
ubuntu@ip-172-31-25-177:~$ ls -l
total 12
drwxrwxr-x 8 ubuntu ubuntu  4096 Jan 13 05:27 linux_lab_day1
drwxrwxr-x 3 ubuntu ubuntu  4096 Jan 13 09:14 linux_practice
drwxrwxr-x 3 alice  devteam 4096 Jan 18 13:04 opt
```

3. Apply permissions such that:
   ○ Owner & group → full access
   ○ Others → no access

4. Verify permissions using: ls -l

```
ubuntu@ip-172-31-25-177:~$ sudo chmod 770 -R opt
ubuntu@ip-172-31-25-177:~$ ls -l
total 12
drwxrwxr-x 8 ubuntu ubuntu  4096 Jan 13 05:27 linux_lab_day1
drwxrwxr-x 3 ubuntu ubuntu  4096 Jan 13 09:14 linux_practice
drwxrwx--- 3 alice  devteam 4096 Jan 18 13:04 opt
```

Part 3: File Attributes (Security Hardening)

1. Create a file inside the directory: config.txt

```
ubuntu@ip-172-31-25-177:~$ touch config.txt
ubuntu@ip-172-31-25-177:~$
```

2. Make the file immutable so it cannot be deleted or modified accidentally.
3. Verify attributes using: lsattr
4. Attempt to delete or edit the file (observe behavior).

```
ubuntu@ip-172-31-25-177:~$ cd ~
ubuntu@ip-172-31-25-177:~$ sudo chattr +i config.txt
ubuntu@ip-172-31-25-177:~$ lsattr config.txt
----i---------e------- config.txt
ubuntu@ip-172-31-25-177:~$ rm config.txt
rm: cannot remove 'config.txt': Operation not permitted
```

<u>Conceptual Questions</u>

1. **Why use groups instead of giving permissions to individual users?**
   Using Groups makes permission management reliable. Access can be assigned to a group, rather than repeatedly assigning to individual users. It improves security. Users can be added or removed from group without changing permissions.

2. **Why would an immutable file be useful in production?**

Immutable files prevent accidental or unnecessary changes that might happen to important files. They protect the configuration files from being modified or deleted by any user.

3. **Why is /etc/shadow readable only by root?**
   /etc/shadow stores encrypted passwords. The access is restricted and only root can read it so that traffic from other users is prevented and attacks to breach passwords is avoided.