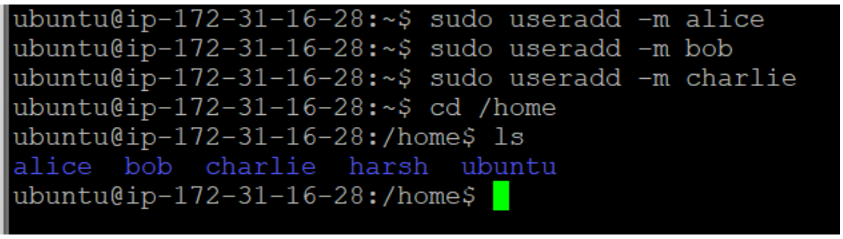
Assignment 3 - User & Group Management + File Security

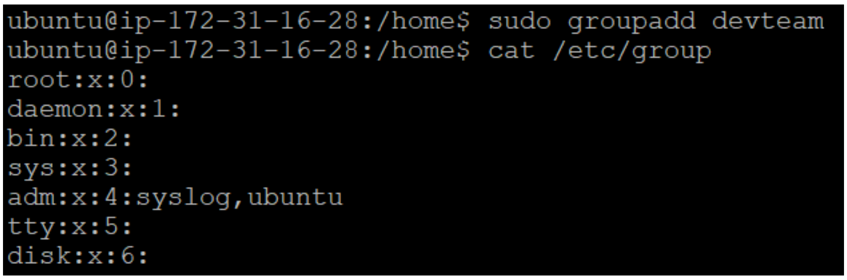
Part 1: User & Group Setup

1. Create the following users:
    - `alice`
    - `bob`
    - `charlie`

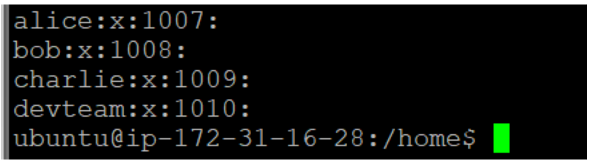


```
ubuntu@ip-172-31-16-28:~$ sudo useradd -m alice
ubuntu@ip-172-31-16-28:~$ sudo useradd -m bob
ubuntu@ip-172-31-16-28:~$ sudo useradd -m charlie
ubuntu@ip-172-31-16-28:~$ cd /home
ubuntu@ip-172-31-16-28:/home$ ls
alice  bob  charlie  harsh  ubuntu
ubuntu@ip-172-31-16-28:/home$ 
```

2. Create a group called:
    - `devteam`

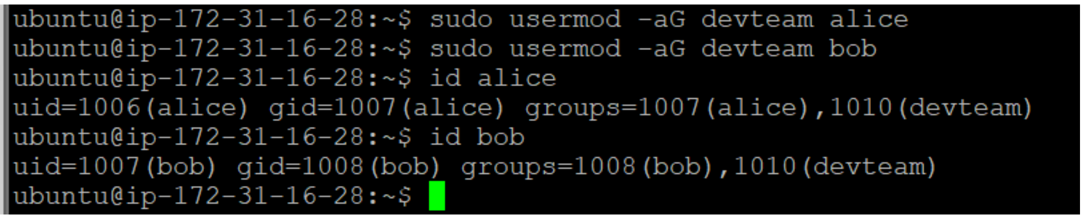


```
ubuntu@ip-172-31-16-28:/home$ sudo groupadd devteam
ubuntu@ip-172-31-16-28:/home$ cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog,ubuntu
tty:x:5:
disk:x:6:
```



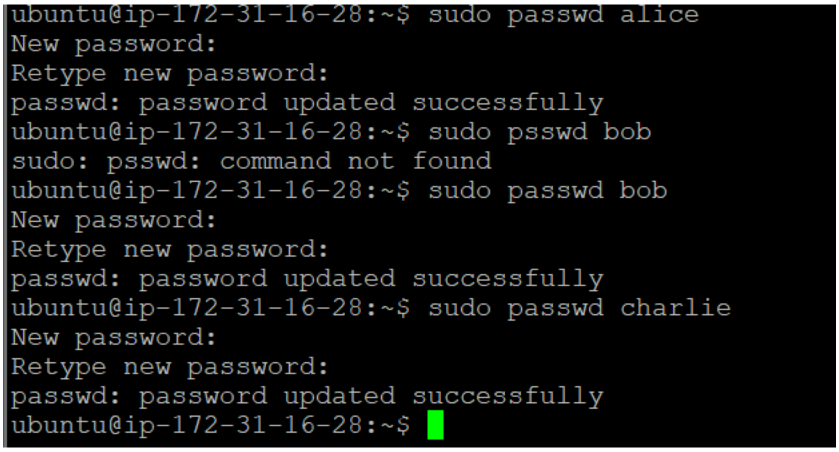
```
alice:x:1007:
bob:x:1008:
charlie:x:1009:
devteam:x:1010:
ubuntu@ip-172-31-16-28:/home$ 
```

3. Add users `alice` and `bob` to the `devteam` group.



```
ubuntu@ip-172-31-16-28:~$ sudo usermod -aG devteam alice
ubuntu@ip-172-31-16-28:~$ sudo usermod -aG devteam bob
ubuntu@ip-172-31-16-28:~$ id alice
uid=1006(alice) gid=1007(alice) groups=1007(alice),1010(devteam)
ubuntu@ip-172-31-16-28:~$ id bob
uid=1007(bob) gid=1008(bob) groups=1008(bob),1010(devteam)
ubuntu@ip-172-31-16-28:~$ 
```

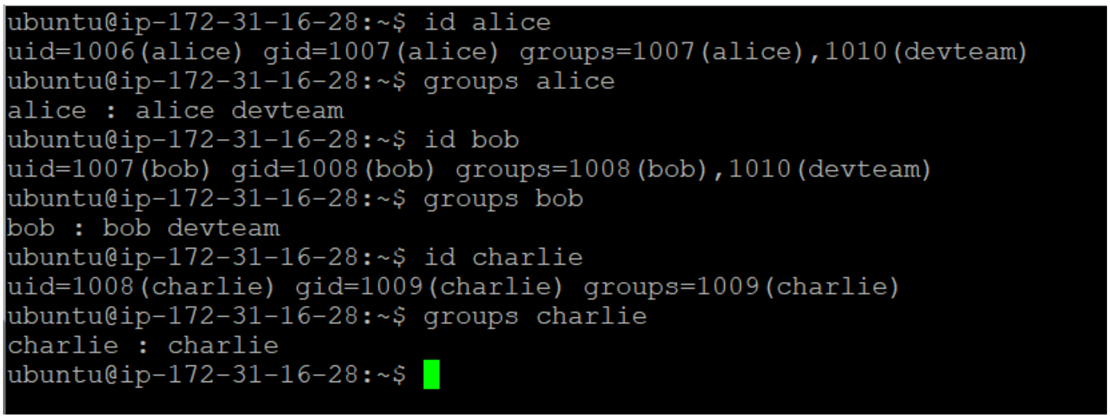
4. Set passwords for all users.



```
ubuntu@ip-172-31-16-28:~$ sudo passwd alice
New password:
Retype new password:
passwd: password updated successfully
ubuntu@ip-172-31-16-28:~$ sudo psswd bob
sudo: psswd: command not found
ubuntu@ip-172-31-16-28:~$ sudo passwd bob
New password:
Retype new password:
passwd: password updated successfully
ubuntu@ip-172-31-16-28:~$ sudo passwd charlie
New password:
Retype new password:
passwd: password updated successfully
ubuntu@ip-172-31-16-28:~$
```

5. Verify:

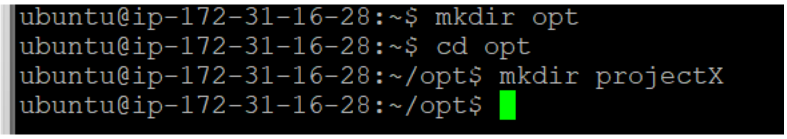
   ○ User IDs and group memberships using `id` and `groups`.



```
ubuntu@ip-172-31-16-28:~$ id alice
uid=1006(alice) gid=1007(alice) groups=1007(alice),1010(devteam)
ubuntu@ip-172-31-16-28:~$ groups alice
alice : alice devteam
ubuntu@ip-172-31-16-28:~$ id bob
uid=1007(bob) gid=1008(bob) groups=1008(bob),1010(devteam)
ubuntu@ip-172-31-16-28:~$ groups bob
bob : bob devteam
ubuntu@ip-172-31-16-28:~$ id charlie
uid=1008(charlie) gid=1009(charlie) groups=1009(charlie)
ubuntu@ip-172-31-16-28:~$ groups charlie
charlie : charlie
ubuntu@ip-172-31-16-28:~$
```

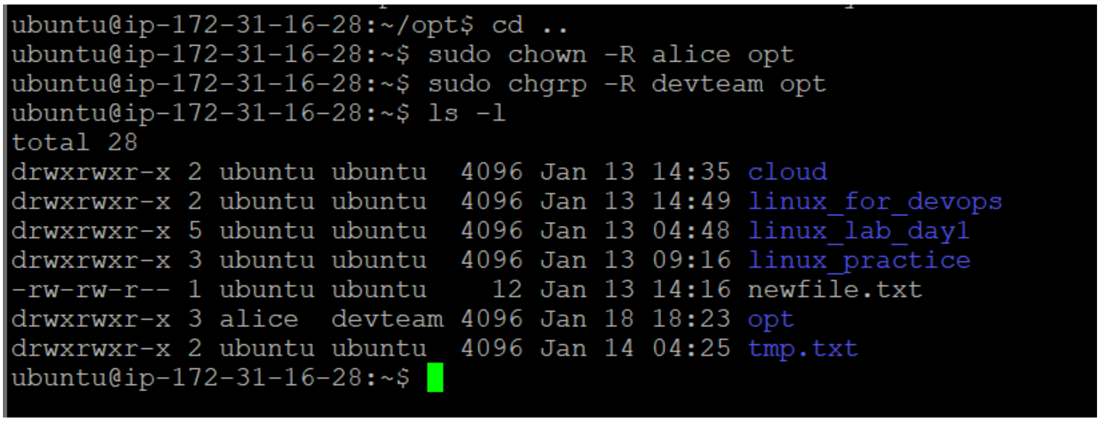
Part 2: File Ownership & Permissions

1. Create a directory: **`/opt/projectX`**



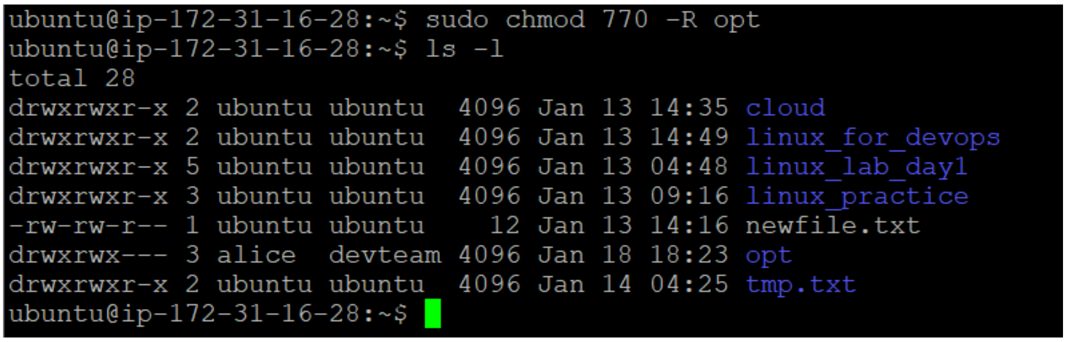
```
ubuntu@ip-172-31-16-28:~$ mkdir opt
ubuntu@ip-172-31-16-28:~$ cd opt
ubuntu@ip-172-31-16-28:~/opt$ mkdir projectX
ubuntu@ip-172-31-16-28:~/opt$
```

2. Change ownership:
    - Owner: `alice`
    - Group: `devteam`



```
ubuntu@ip-172-31-16-28:~/opt$ cd ..
ubuntu@ip-172-31-16-28:~$ sudo chown -R alice opt
ubuntu@ip-172-31-16-28:~$ sudo chgrp -R devteam opt
ubuntu@ip-172-31-16-28:~$ ls -l
total 28
drwxrwxr-x 2 ubuntu ubuntu  4096 Jan 13 14:35 cloud
drwxrwxr-x 2 ubuntu ubuntu  4096 Jan 13 14:49 linux_for_devops
drwxrwxr-x 5 ubuntu ubuntu  4096 Jan 13 04:48 linux_lab_day1
drwxrwxr-x 3 ubuntu ubuntu  4096 Jan 13 09:16 linux_practice
-rw-rw-r-- 1 ubuntu ubuntu    12 Jan 13 14:16 newfile.txt
drwxrwxr-x 3 alice  devteam 4096 Jan 18 18:23 opt
drwxrwxr-x 2 ubuntu ubuntu  4096 Jan 14 04:25 tmp.txt
ubuntu@ip-172-31-16-28:~$
```

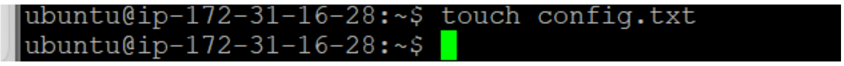
3. Apply permissions such that:
    - Owner & group → full access
    - Others → no access
4. Verify permissions using: **`ls -l`**



```
ubuntu@ip-172-31-16-28:~$ sudo chmod 770 -R opt
ubuntu@ip-172-31-16-28:~$ ls -l
total 28
drwxrwxr-x 2 ubuntu ubuntu  4096 Jan 13 14:35 cloud
drwxrwxr-x 2 ubuntu ubuntu  4096 Jan 13 14:49 linux_for_devops
drwxrwxr-x 5 ubuntu ubuntu  4096 Jan 13 04:48 linux_lab_day1
drwxrwxr-x 3 ubuntu ubuntu  4096 Jan 13 09:16 linux_practice
-rw-rw-r-- 1 ubuntu ubuntu    12 Jan 13 14:16 newfile.txt
drwxrwx--- 3 alice  devteam 4096 Jan 18 18:23 opt
drwxrwxr-x 2 ubuntu ubuntu  4096 Jan 14 04:25 tmp.txt
ubuntu@ip-172-31-16-28:~$
```

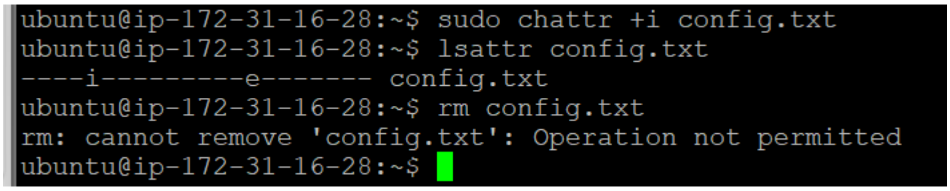
🔹 Part 3: File Attributes (Security Hardening)

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



```
ubuntu@ip-172-31-16-28:~$ touch config.txt
ubuntu@ip-172-31-16-28:~$
```

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-172-31-16-28:~$ sudo chattr +i config.txt
ubuntu@ip-172-31-16-28:~$ lsattr config.txt
----i---------e------- config.txt
ubuntu@ip-172-31-16-28:~$ rm config.txt
rm: cannot remove 'config.txt': Operation not permitted
ubuntu@ip-172-31-16-28:~$
```

Conceptual Questions

Why use groups instead of giving permissions to individual users?

Groups simplify permission management by assigning access to multiple users at once, and hence improves scalability, consistency and reduces administrative overhead.

When would an immutable file be useful in production?

For critical configuration or system files to prevent the accidental or malicious modification or deletion.

Why is /etc/shadow readable only by root?

It stores the encrypted user passwords and sensitive authentication data So restrictions prevents the credentials thefts and enhances the system Security.