

Assignment 3 - User & Group Management + File Security

Part 1: User & Group Setup

1. Create the following users:

- alice
- bob
- charlie

```
ubuntu@ip-172-31-5-27:~/home$ sudo useradd -m alice
ubuntu@ip-172-31-5-27:~/home$ sudo useradd -m bob
ubuntu@ip-172-31-5-27:~/home$ sudo useradd -m charlie
ubuntu@ip-172-31-5-27:~/home$ cd /home
ubuntu@ip-172-31-5-27:/home$ ls
alice bob charlie test1 ubuntu uma
ubuntu@ip-172-31-5-27:/home$ █
```

2. Create a group called: devteam

```
ubuntu@ip-172-31-5-27:~/home$ sudo groupadd devteam
ubuntu@ip-172-31-5-27:~/home$ cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
```

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

```
root@ip-172-31-5-27:~# usermod -aG devteam alice
root@ip-172-31-5-27:~# usermod -aG devteam bob
```

4. Set passwords for all users.

```
root@ip-172-31-5-27:~# passwd alice
New password:
Retype new password:
passwd: password updated successfully
root@ip-172-31-5-27:~# passwd bob
New password:
Retype new password:
passwd: password updated successfully
root@ip-172-31-5-27:~# passwd charlie
New password:
Retype new password:
passwd: password updated successfully
root@ip-172-31-5-27:~#
```

5. Verify: User IDs and group memberships using id and groups.

```
root@ip-172-31-5-27:~# id alice
uid=1004(alice) gid=1005(alice) groups=1005(alice),1008(devteam)
root@ip-172-31-5-27:~# id bob
uid=1005(bob) gid=1006(bob) groups=1006(bob),1008(devteam)
root@ip-172-31-5-27:~# id charlie
uid=1006(charlie) gid=1007(charlie) groups=1007(charlie)
```

```
root@ip-172-31-5-27:~# groups alice
alice : alice devteam
root@ip-172-31-5-27:~# groups bob
bob : bob devteam
```

Part 2: File Ownership & Permissions

1. Create a directory: /opt/project

```
ubuntu@ip-172-31-5-27:~/opt
ubuntu@ip-172-31-5-27:~$ mkdir opt
ubuntu@ip-172-31-5-27:~$ cd opt
ubuntu@ip-172-31-5-27:~/opt$ mkdir projectX
ubuntu@ip-172-31-5-27:~/opt$ █
```

2. Change ownership:

- Owner: alice
- Group: devteam

```
ubuntu@ip-172-31-5-27:~$ sudo chown -R alice opt
ubuntu@ip-172-31-5-27:~$ sudo chgrp -R devteam opt
ubuntu@ip-172-31-5-27:~$ ls -l
total 12
drwxrwxr-x 5 ubuntu ubuntu 4096 Jan 14 05:03 linux_lab_day1
drwxrwxr-x 3 ubuntu ubuntu 4096 Jan 13 09:14 linux_practice
drwxrwxr-x 3 alice devteam 4096 Jan 18 14:56 opt
ubuntu@ip-172-31-5-27:~$ █
```

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

4. Verify permissions using: ls -l

```
ubuntu@ip-172-31-5-27:~$ sudo chmod 770 -R opt
ubuntu@ip-172-31-5-27:~$ ls -l
total 12
drwxrwxr-x 5 ubuntu ubuntu 4096 Jan 14 05:03 linux_lab_day1
drwxrwxr-x 3 ubuntu ubuntu 4096 Jan 13 09:14 linux_practice
drwxrwx--- 3 alice devteam 4096 Jan 18 14:56 opt
ubuntu@ip-172-31-5-27:~$ █
```

Part 3: File Attributes (Security Hardening)

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

```
ubuntu@ip-172-31-5-27:~$ touch config.txt  
ubuntu@ip-172-31-5-27:~$ █
```

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-172-31-5-27:~$ sudo chattr +i config.txt  
ubuntu@ip-172-31-5-27:~$ lsattr config.txt  
----i-----e----- config.txt  
ubuntu@ip-172-31-5-27:~$ rm config.txt  
rm: cannot remove 'config.txt': Operation not permitted  
ubuntu@ip-172-31-5-27:~$ █
```