Name : Medhat Mohamed Sobhy
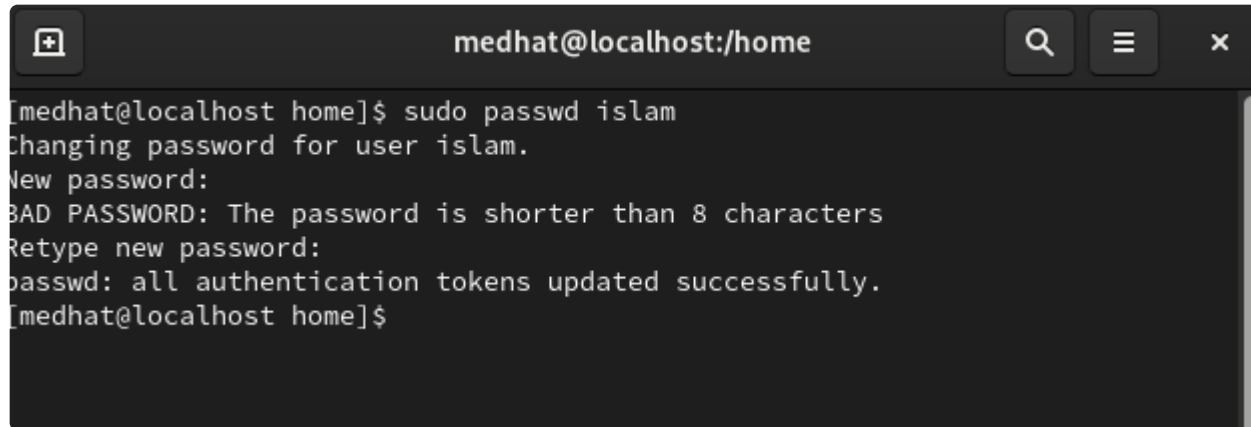

PART 1

1- Create a user account with the following attribute

- username: islam
- Full name/comment: Islam Ali

```
                         medhat@localhost:/home

[medhat@localhost ~]$ sudo useradd -c "Islam Ali" islam
[sudo] password for medhat:
[medhat@localhost ~]$ pwd
/home/medhat
[medhat@localhost ~]$ ls
Desktop  doc        Downloads  oldpasswd  Public     Videos
dir1     Documents  Music      Pictures   Templates
[medhat@localhost ~]$ cd ..
[medhat@localhost home]$ ls
d1  islam  medhat  user6
[medhat@localhost home]$
```
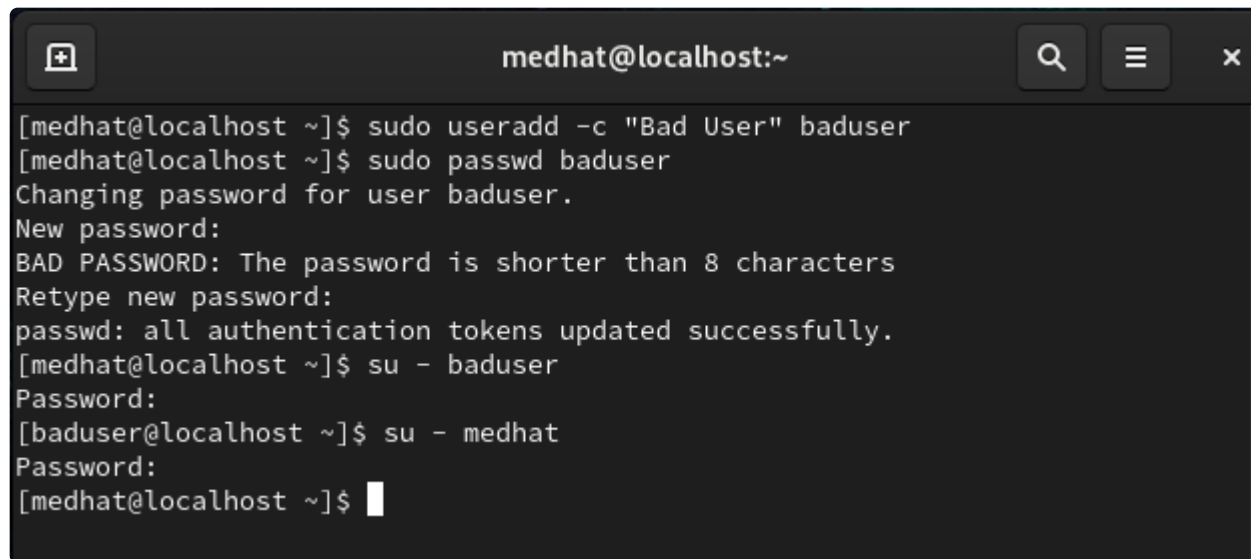
- Password: islam

```
[medhat@localhost home]$ sudo passwd islam
Changing password for user islam.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[medhat@localhost home]$
```

2- Create a user account with the following attribute

- Username: baduser
- Full name/comment: Bad User
- Password: baduser

```
[medhat@localhost ~]$ sudo useradd -c "Bad User" baduser
[medhat@localhost ~]$ sudo passwd baduser
Changing password for user baduser.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[medhat@localhost ~]$ su - baduser
Password:
[baduser@localhost ~]$ su - medhat
Password:
[medhat@localhost ~]$
```

3- Create a supplementary (Secondary) group called pgroup with group ID of 30000

```
[medhat@localhost ~]$ sudo groupadd -g 30000 pgroup
[medhat@localhost ~]$
```

```
ockpit-ws:x:989:
ockpit-wsinstance:x:988:
olord:x:987:
ssd:x:986:
etroubleshoot:x:985:
ipewire:x:984:
latpak:x:983:
levis:x:982:
rlapi:x:981:
dm:x:42:
nome-initial-setup:x:980:
shd:x:74:
hrony:x:979:
locate:x:21:
nsmasq:x:978:
cpdump:x:72:
edhat:x:1000:
ser6:x:1001:
1:x:1002:
ata:x:1003:
slam:x:1004:
aduser:x:1005:
group:x:30000:
medhat@localhost ~]$
```

4- Create a supplementary group called badgroup

```
[medhat@localhost ~]$ sudo groupadd badgroup
[medhat@localhost ~]$ sudo groupadd badgroup
groupadd: group 'badgroup' already exists
[medhat@localhost ~]$ grep badgroup /etc/group
badgroup:x:30001:
[medhat@localhost ~]$
```

5- Add islam user to the pgroup group as a supplementary group

```
[medhat@localhost ~]$ sudo usermod -a -G pgroup islam
[medhat@localhost ~]$ groups islam
islam : islam pgroup
[medhat@localhost ~]$
```

6- Modify the password of islam's account to password

7- Modify islam's account so the password expires after 30 days

```
[medhat@localhost ~]$ sudo passwd islam
Changing password for user islam.
New password:
BAD PASSWORD: The password fails the dictionary check - it is based on a diction
ary word
Retype new password:
passwd: all authentication tokens updated successfully.
[medhat@localhost ~]$ su - islam
Password:
[islam@localhost ~]$ su - medhat
Password:
[medhat@localhost ~]$ sudo chage -M 30 islam
[medhat@localhost ~]$ sudo chage -l islam
Last password change                                    : Dec 24, 2024
Password expires                                        : Jan 23, 2025
Password inactive                                       : never
Account expires                                         : never
Minimum number of days between password change          : 0
Maximum number of days between password change          : 30
Number of days of warning before password expires       : 7
[medhat@localhost ~]$
```

8- Lock bad user account so he can't log in

```
[medhat@localhost ~]$ sudo passwd -l baduser
Locking password for user baduser.
passwd: Success
[medhat@localhost ~]$ su - baduser
Password:
su: Authentication failure
[medhat@localhost ~]$ █
```

9- Delete bad user account

```
                           medhat@localhost:~                    Q  ≡  ×

[medhat@localhost ~]$ sudo userdel baduser
[medhat@localhost ~]$ grep bad /etc/passwd
[medhat@localhost ~]$ grep baduser /etc/passwd
[medhat@localhost ~]$
```

10- Delete the supplementary group called badgroup.

```
                           medhat@localhost:~                    Q  ≡  ×

[medhat@localhost ~]$ sudo groupdel pgroup
[medhat@localhost ~]$ grep pgroup /etc/group
[medhat@localhost ~]$ █
```

PART 2

1- Create a folder called myteam in your home directory and change its permissions to read only for the owner.

```
                           medhat@localhost:~                    Q  ≡  ×

[medhat@localhost ~]$ mkdir myteam
[medhat@localhost ~]$ chmod 400 myteam
[medhat@localhost ~]$ ls -ld myteam/
dr--------. 2 medhat medhat 6 Dec 24 13:47 myteam/
[medhat@localhost ~]$ █
```

2- Log out and log in with another

```
                          medhat@localhost:~              Q  ≡  ✕

[medhat@localhost ~]$ logout
[islam@localhost ~]$ su - medhat
Password:
[medhat@localhost ~]$
```

3- Try to access (by cd command) the folder (myteam) then log out back to your account

```
                          medhat@localhost:~              Q  ≡  ✕

[medhat@localhost ~]$ su - islam
Password:
[islam@localhost ~]$ pwd
/home/islam
[islam@localhost ~]$ ls
[islam@localhost ~]$ cd /home/medhat/myteam
-bash: cd: /home/medhat/myteam: Permission denied
[islam@localhost ~]$ su - medhat
Password:
[medhat@localhost ~]$ ls
Desktop  doc        Downloads  myteam      Pictures  Templates
dir1     Documents  Music      oldpasswd   Public    Videos
[medhat@localhost ~]$ cd myteam/
-bash: cd: myteam/: Permission denied
[medhat@localhost ~]$ ▊
```

4- Using the Command Line :

- Change the permissions of oldpasswd file to give the owner read and write permissions
  - and for group write and execute and execute only for the others (using chmod in 2 different ways)

```
⊞                    medhat@localhost:~              Q   ≡   ✕

[medhat@localhost ~]$ chmod 631 oldpasswd
[medhat@localhost ~]$ chmod u=rw, g=wx, o=x oldpasswd
chmod: invalid mode: 'u=rw,'
Try 'chmod --help' for more information.
[medhat@localhost ~]$ chmod u=rw oldpasswd
[medhat@localhost ~]$ chmod g=wx oldpasswd
[medhat@localhost ~]$ chmod o=x oldpasswd
[medhat@localhost ~]$
```

5- What are the minimum permissions needed for :

- Copy a directory (permission for source directory and permissions for target parent directory)
    - Source --> **Read** to read the contents of source directory and **Execute** to enter the source directory
    - Target --> Write to create a copy of the source directory in target directory and **Execute** to enter the target directory
- Copy a file (permission for source file and permission for target parent directory)
    - Source Directory --> **Execute**
    - Soure File --> **Read**
    - Target Directory --> **Execute** and **Write**
- Delete a file
    - **Execute** and **Write** permissions on the directory containing the file
- Change to a directory
    - **Execute** permission on the directory to be accessed
- List a directory content (ls command)
    - **Execute** and **Read** permissions
- View a file content (more/cat command)
    - **Execute** permission on the directory containing the file
    - **Read** permission on the file
- Modify a file content

- **Execute** permission on the directory containing the file
- **Write** permission on the file

6- Create a file with permission 444. Try to edit it and remove it. Note what happened

- couldn't edit the file
- couldn't remove the file

7- What is the difference between the "x" permission for a file and for a directory?

- **execute permission on a file** : the file is allowed to to be executed as script
- **Execute permission on a directory** : you're allowed to enter the directory >> required to access the content of the directory