

Linux lab2

Name :Israa Mohamed Gaber

Part1

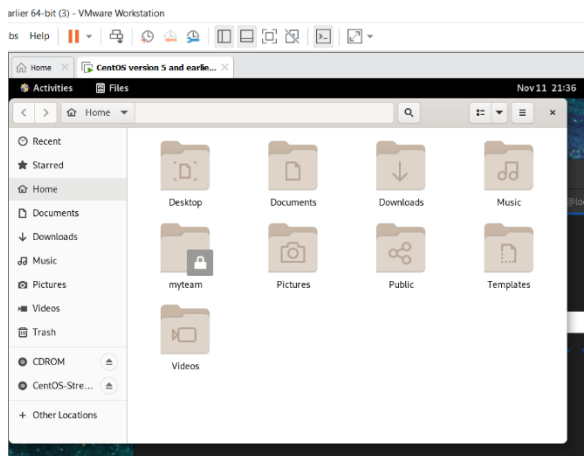
Part 1

1. Create a folder called myteam in your home directory and change its permissions to read only for the owner.
2. Log out and log in with another user
3. Try to access (by cd command) the folder (myteam) then log out back to your account
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)
 - Change your default permissions to be as above.
 - What is the maximum permission a file can have, by default when it is just created? And what is that for the directory?
 - Change your default permissions to be no permission to everyone then create a directory and a file to verify.
5. What are the minimum permissions needed for:
 - Copy a directory (permission for source directory and permissions for target parent directory)
 - Copy a file (permission for source file and permission for target parent directory)
 - Delete a file
 - Change to a directory
 - List a directory content (ls command)
 - View a file content (more/cat command)
 - Modify a file content
6. Create a file with permission 444. Try to edit it and remove it. Note what happened.
7. What is the difference between the "x" permission for a file and for a directory?

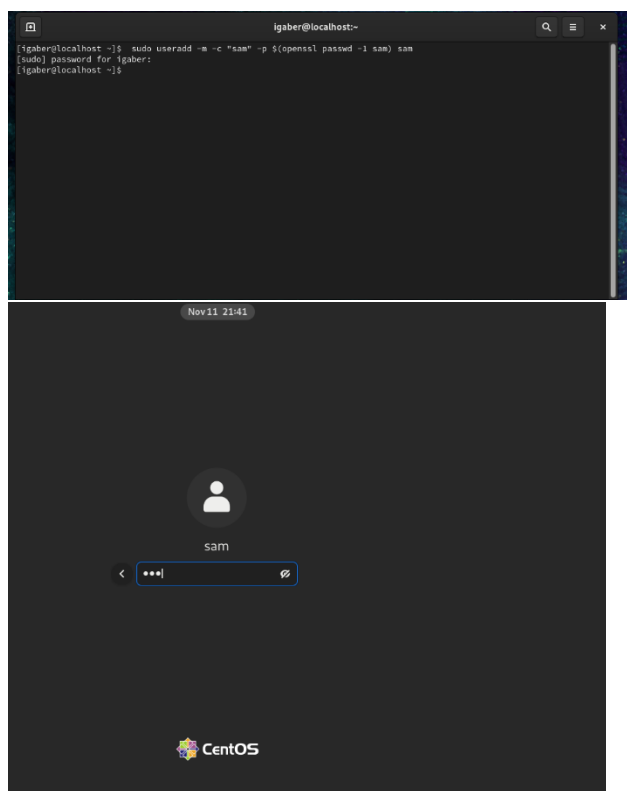
1. Create a folder called myteam in your home directory and change its permissions to read-only for the owner.

```
[igaber@localhost home]$ mkdir ~/myteam  
chmod 400 ~/myteam  
ls -ld myteam
```

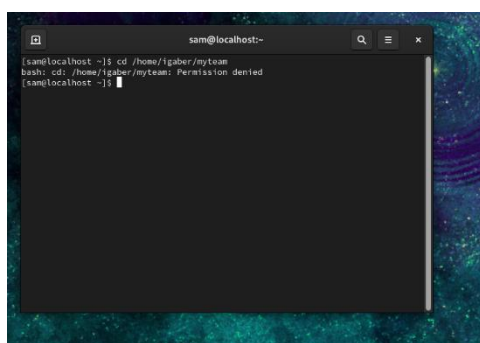
```
[igaber@localhost home]$ mkdir ~/myteam  
chmod 400 ~/myteam  
ls -ld myteam
```



2. Log out and log in with another user.



3. Try to access (by cd command) the folder (myteam) then log out back to your account.
[sam@localhost home]\$ cd /home/igaber/myteam



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 others (using chmod in 2 different ways).

```
[igaber@localhost home]$ chmod u=rw,g=wx,o=x oldpasswd  
[igaber@localhost home]$ chmod 751 oldpasswd
```

5. What are the minimum permissions needed for.

Copy a directory: x on the source and target directories, r for reading the contents.

Copy a file: r permission on the file and w on the target directory.

Delete a file: w and x on the directory containing the file.

Change to a directory: x on the directory.

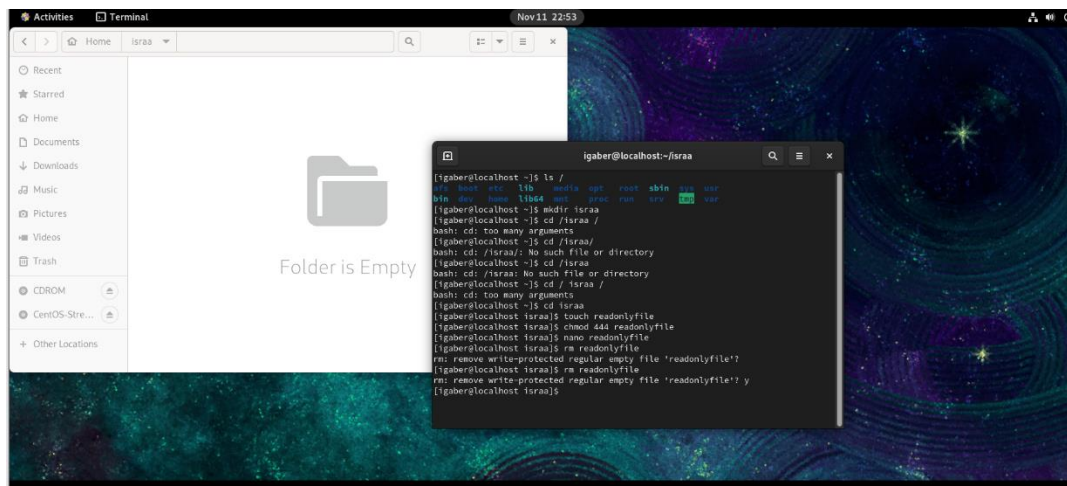
List a directory content (ls command): r and x on the directory.

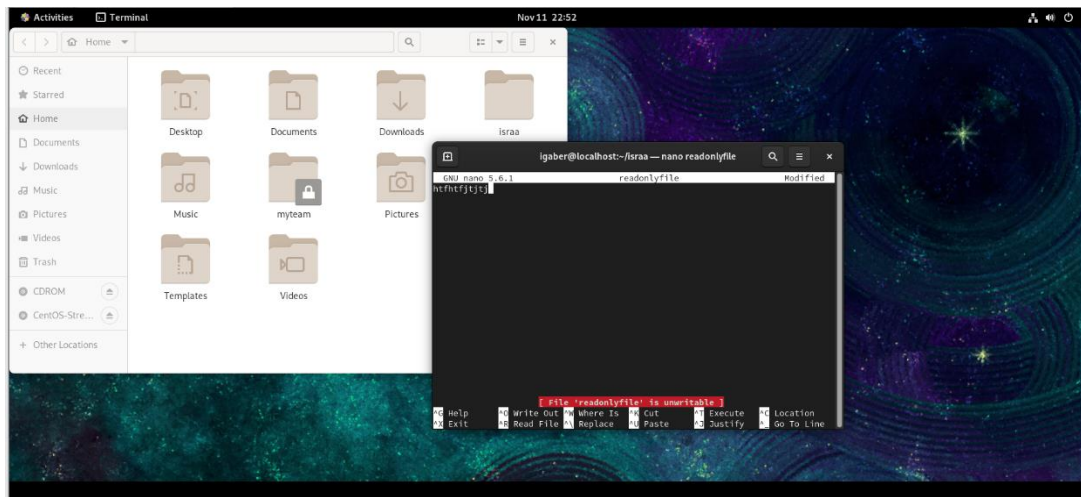
View a file content (more/cat command): r on the file.

Modify a file content: w on the file.

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

```
[igaber@localhost ~]$ mkdir israa  
[igaber@localhost ~]$ cd israa  
[igaber@localhost israa]$ touch readonlyfile  
[igaber@localhost israa]$ chmod 444 readonlyfile  
[igaber@localhost israa]$ nano readonlyfile  
[igaber@localhost israa]$ rm readonlyfile  
rm: remove write-protected regular empty file 'readonlyfile'?  
[igaber@localhost israa]$ rm readonlyfile  
rm: remove write-protected regular empty file 'readonlyfile'? y
```





Editing will fail because 444 only allows read permissions.
Deletion will succeed

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

For a file, x means it is executable (you can run it as a program).

For a directory, x allows you to enter the directory and access its contents (required for listing and changing directories).

Part2

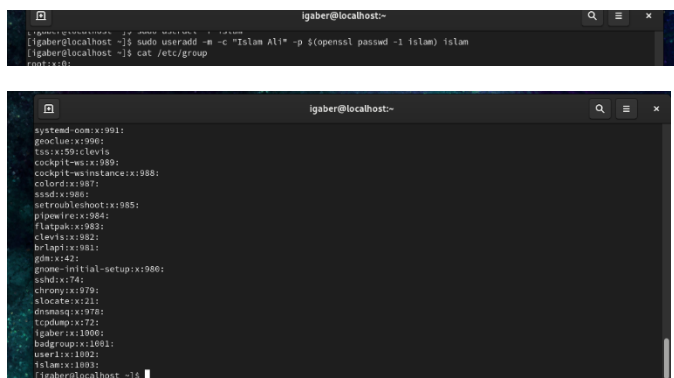
Part 2

1. Create a user account with the following attribute
 - username: islam
 - Full name/comment: Islam Ali
 - Password: islam
2. Create a user account with the following attribute
 - Username: baduser
 - Full name/comment: Bad User
 - Password: baduser
3. Create a supplementary (Secondary) group called pgroup with group ID of 30000
4. Create a supplementary group called badgroup
5. Add islam user to the pgroup group as a supplementary group
6. Modify the password of islam's account to password
7. Modify islam's account so the password expires after 30 days
8. Lock bad user account so he can't log in
9. Delete bad user account
10. Delete the supplementary group called badgroup.

1. Create a user account for islam

```
[igaber@localhost ~]$ sudo useradd -m -c "Islam Ali" -p $(openssl passwd -1 islam) islam
```

```
[igaber@localhost ~]$ cat /etc/group
```



```
igaber@localhost:~$ cat /etc/group
systemd-core:x:991:
geoclue:x:996:
tss:x:59:clevis
cockpit-ws:x:1009:
cockpit-ws-instance:x:988:
colord:x:987:
sssd:x:986:
setroubleshoot:x:985:
pipewire:x:984:
flatpak:x:983:
clevis:x:982:
brlapi:x:981:
gnome:x:42:
gnome-initial-setup:x:980:
sshd:x:74:
chrony:x:1079:
slocate:x:21:
dnsmasq:x:1978:
tcpdump:x:172:
igaber:x:1000:
badgroup:x:1001:
user1:x:1002:
islam:x:1003:
root:x:0:
```

2. Create a user account for baduser

```
[igaber@localhost ~]$ sudo useradd -m -c "Bad User" -p $(openssl passwd -1 baduser) baduser
```

```
[igaber@localhost ~]$ cat /etc/group
```



```
islam:x:1003:
igaber@localhost:~$ sudo useradd -m -c "Bad User" -p $(openssl passwd -1 baduser) baduser
igaber@localhost:~$ cat /etc/group
root:x:0:
bin:x:1:
```

```
igaber@localhost:~$ cat /etc/group
geoclue:x:986:
tss:x:59:clevis
cockpit-ws:x:989:
cockpit-ws-instance:x:988:
colord:x:987:
sssd:x:986:
setroubleshoot:x:985:
pipewire:x:984:
flatpak:x:983:
clevis:x:982:
brlapi:x:981:
gdm:x:42:
gnome-initial-setup:x:980:
sddm:x:74:
chrony:x:979:
sllocate:x:21:
dnsmasq:x:978:
tcpdump:x:72:
igaber:x:1000:
badgroup:x:1001:
user1:x:1002:
talam:x:1003:
baduser:x:1004:
[igaber@localhost ~]$
```

3. Create a supplementary (secondary) group called progroup with a group ID of 30000:

```
[igaber@localhost ~]$ sudo groupadd -g 30000 progroup
```

```
[igaber@localhost ~]$ cat /etc/group
```

```
baduser:x:1004:
[igaber@localhost ~]$ sudo groupadd -g 30000 progroup
[igaber@localhost ~]$ cat /etc/group
root:x:0:
```

```
igaber@localhost:~$ cat /etc/group
geoclue:x:986:
tss:x:59:clevis
cockpit-ws:x:989:
cockpit-ws-instance:x:988:
colord:x:987:
sssd:x:986:
setroubleshoot:x:985:
pipewire:x:984:
flatpak:x:983:
clevis:x:982:
brlapi:x:981:
gdm:x:42:
gnome-initial-setup:x:980:
sddm:x:74:
chrony:x:979:
sllocate:x:21:
dnsmasq:x:978:
tcpdump:x:72:
igaber:x:1000:
badgroup:x:1001:
user1:x:1002:
talam:x:1003:
baduser:x:1004:
progroup:x:30000:
[igaber@localhost ~]$
```

4. Create another supplementary group called badgroup:

```
[igaber@localhost ~]$ sudo groupadd badgroup
```

```
[igaber@localhost ~]$ cat /etc/group
```

```
[igaber@localhost ~]$ sudo groupadd badgroup
[igaber@localhost ~]$ cat /etc/group
root:x:0:
```

```
ristation
version 5 and earlier...
Nov 11 19:46
igaber@localhost:~$ cat /etc/group
geoclue:x:986:
tss:x:59:clevis
cockpit-ws:x:989:
cockpit-ws-instance:x:988:
colord:x:987:
sssd:x:986:
setroubleshoot:x:985:
pipewire:x:984:
flatpak:x:983:
clevis:x:982:
brlapi:x:981:
gdm:x:42:
gnome-initial-setup:x:980:
sddm:x:74:
chrony:x:979:
sllocate:x:21:
dnsmasq:x:978:
tcpdump:x:72:
igaber:x:1000:
user1:x:1002:
talam:x:1003:
baduser:x:1004:
progroup:x:30000:
badgroup:x:30001:
[igaber@localhost ~]$
```

5. Add islam user to the proggroup as a supplementary group:

```
[igaber@localhost ~]$ sudo usermod -aG proggroup islam
```

```
[igaber@localhost ~]$ groups islam
```

```
baduser@dev:~$  
[igaber@localhost ~]$ sudo usermod -aG proggroup islam  
[igaber@localhost ~]$ groups islam  
islam : islam proggroup  
[igaber@localhost ~]$
```

6. Modify the password of islam's account to password:

```
[igaber@localhost ~]$ echo "islam:password" | sudo chpasswd
```

```
[igaber@localhost ~]$ sudo chage -l islam
```

```
baduser@dev:~$  
[igaber@localhost ~]$ echo "islam:password" | sudo chpasswd  
[igaber@localhost ~]$ sudo chage -l islam  
Last password change : Nov 11, 2024  
Password expires : never  
Password inactive : never  
Account expires : never  
Minimum number of days between password change : 9  
Maximum number of days between password change : 99999  
Number of days of warning before password expires : 7  
[igaber@localhost ~]$
```

7. Set islam's password to expire after 30 days:

```
[igaber@localhost ~]$ sudo chage -M 30 islam
```

```
[igaber@localhost ~]$ sudo chage -l islam
```

```
[igaber@localhost ~]$ sudo chage -M 30 islam  
[igaber@localhost ~]$ sudo chage -l islam  
Last password change : Nov 11, 2024  
Password expires : Dec 11, 2024  
Password inactive : never  
Account expires : never  
Minimum number of days between password change : 9  
Maximum number of days between password change : 30  
Number of days of warning before password expires : 7  
[igaber@localhost ~]$
```

8. Lock baduser account so they can't log in:

```
[igaber@localhost ~]$ sudo usermod -L baduser
```

```
[igaber@localhost ~]$ sudo usermod -L baduser  
[igaber@localhost ~]$
```

9. Delete the baduser account:

```
[igaber@localhost ~]$ sudo userdel -r baduser
```

```
[igaber@localhost ~]$ cat /etc/group
```

```
[igaber@localhost ~]$ sudo userdel -r baduser  
[igaber@localhost ~]$ cat /etc/group  
root:x:0:
```



```
igaber@localhost:~$ cat /etc/passwd
geoclue:x:990:
tss:x:59:clevis
cockpit-ws:x:1989:
cockpit-wsinstance:x:988:
colord:x:987:
sssd:x:985:
setroubleshoot:x:985:
pipewire:x:984:
tatsp:x:1983:
clevis:x:982:
brlapi:x:981:
gdm:x:42:
gnome-initial-setup:x:980:
smbd:x:74:
chromy:x:979:
slocate:x:21:
dismag:x:978:
trojan:x:172:
igaber:x:1000:
user:x:1002:
islms:x:1003:
progroux:x:30000:islms
badgroup:x:30001:
igaber@localhost ~]$
```

10. Delete the supplementary group called badgroup:

[igaber@localhost ~]\$ sudo groupdel badgroup

```
badgroup:x:30001:
[igaber@localhost ~]$ sudo groupdel badgroup
[igaber@localhost ~]$
```