LINUX ADMIN LAB-2

12 Abril 2023

Presented To

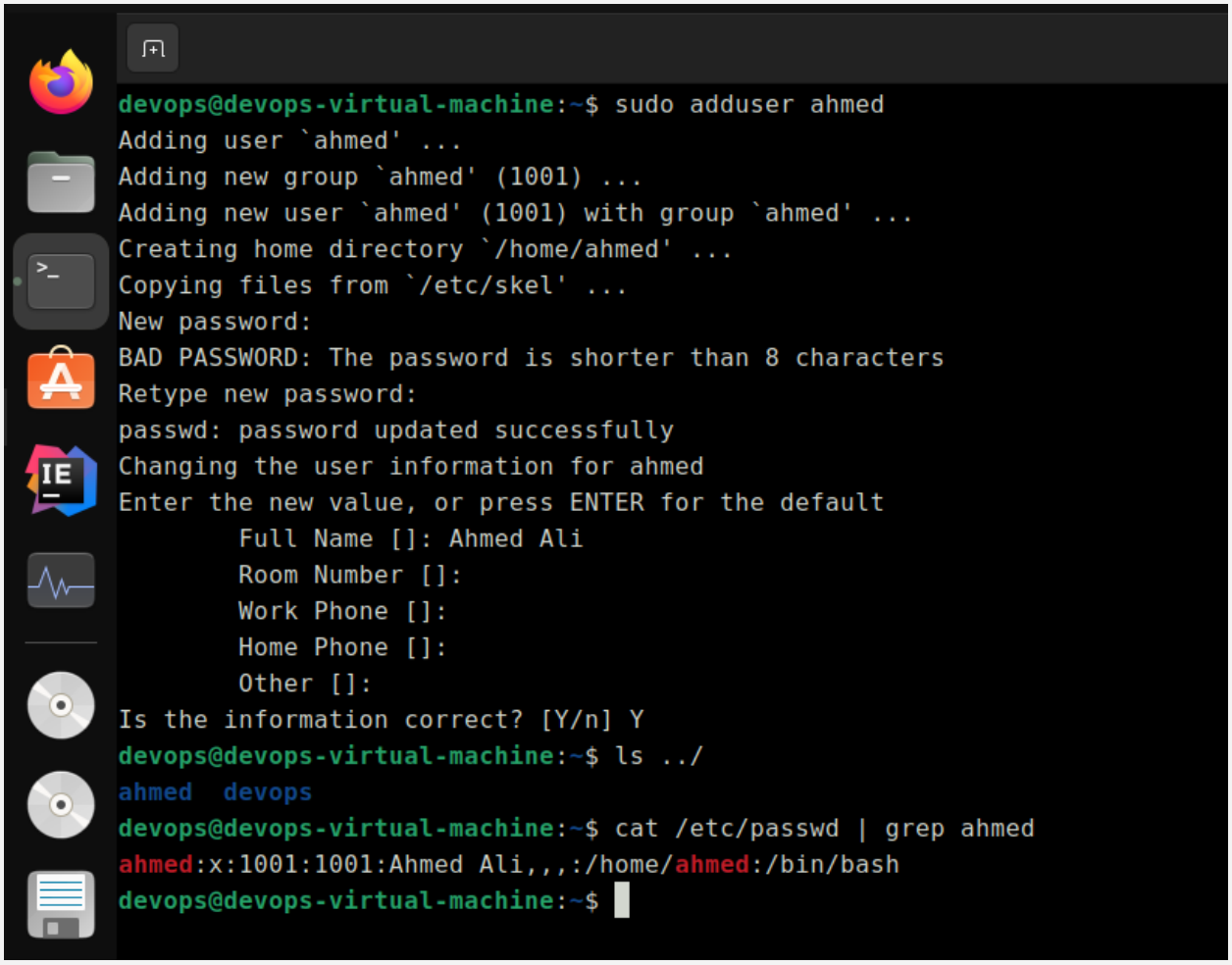
AHMED IBRAHIM

Presented By

ISLAM KHALED

1. Create a user account with the following attribute

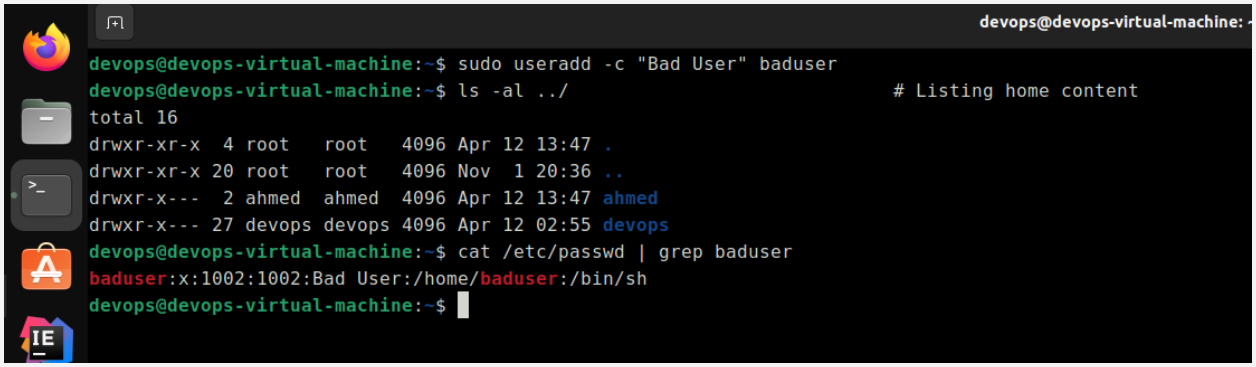
- **username: ahmed**
- **Full Name/comment: ahmed ali**
- **Password: ahmed**



Using adduser creates everything by default in an interactive, user-friendly way, and the shell directory is /bin/bash and it gave me the option to create the password.

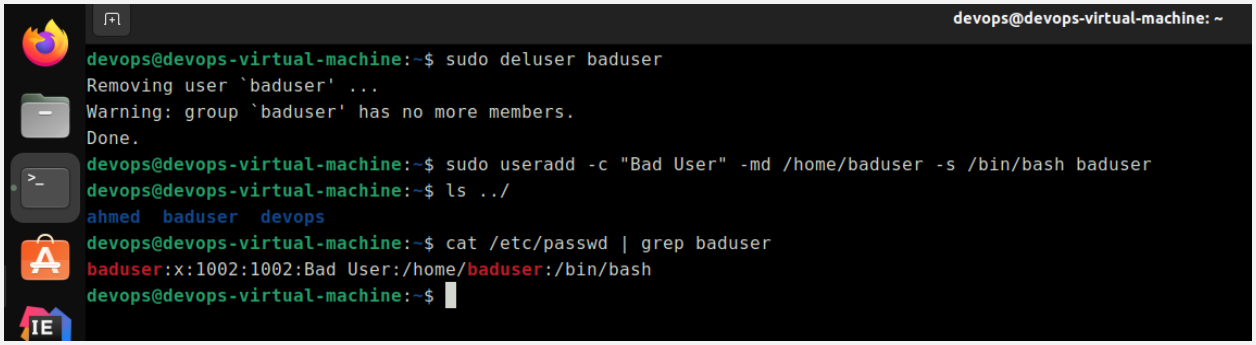
2. Create a user account with the following attribute

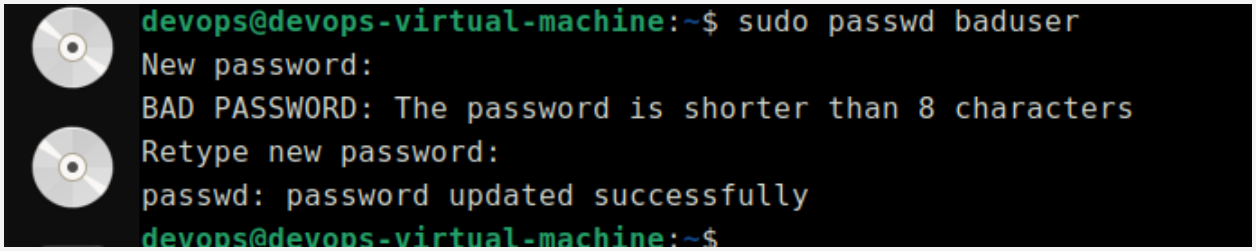
- **Username: baduser**
- **Full name/comment: Bad User**
- **Password: baduser**



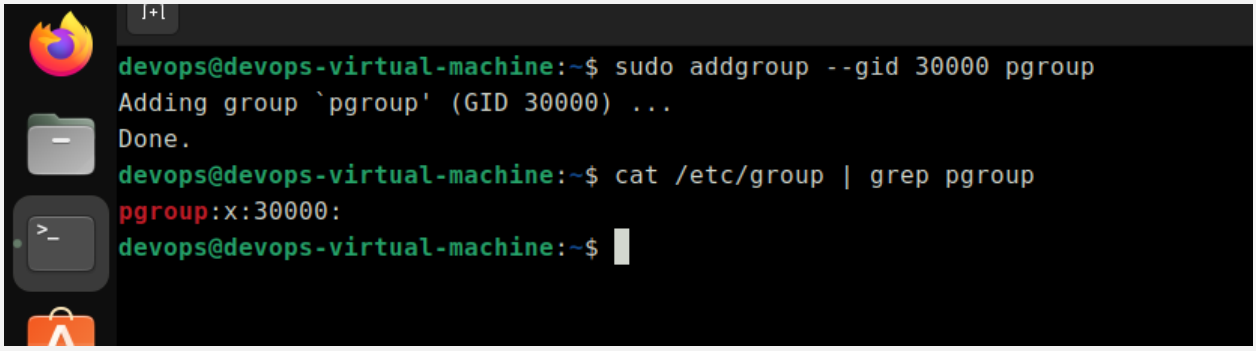
Here useradd didn't create the home directory, it didn't show me what's happening behind the scenes, and the shell directory is /bin/sh, and no option for password creation.

To overcome this we can use more options and then set the password:

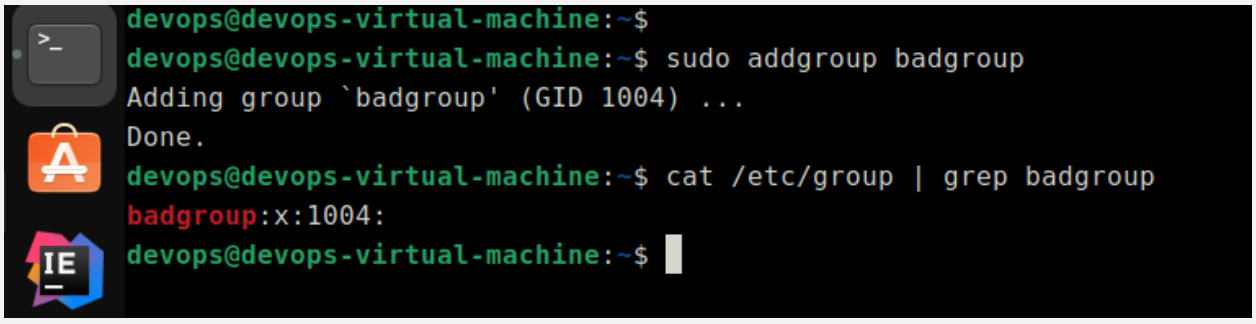




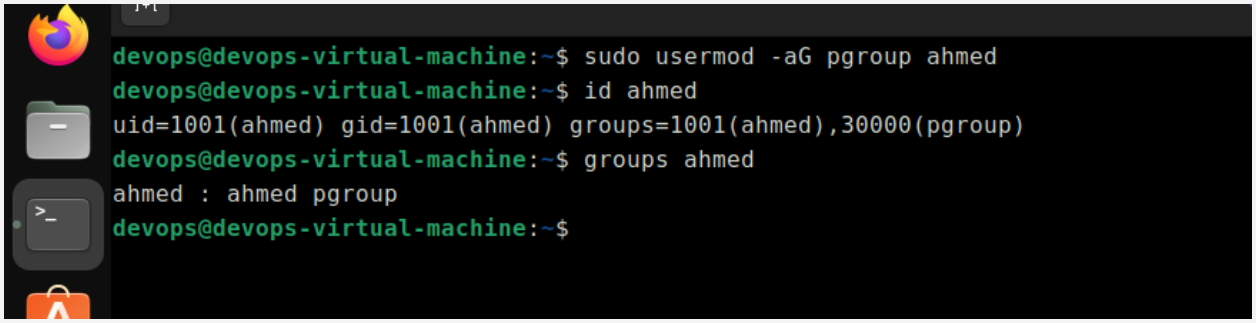
3. Create a supplementary (Secondary) group called pgroup with group ID of 30000



4. Create a supplementary group called badgroup



5. Add ahmed user to the pgroup group as a supplementary group



6. Modify the password of ahmed's account to password

```
devops@devops-virtual-machine:~$ sudo passwd ahmed
New password:
BAD PASSWORD: The password fails the dictionary check - it is based on a dictionary word
Retype new password:
passwd: password updated successfully
devops@devops-virtual-machine:~$
```

7. Modify ahmed's account so the password expires after 30 days

You can verify that the password expiration has been set with the -l option:

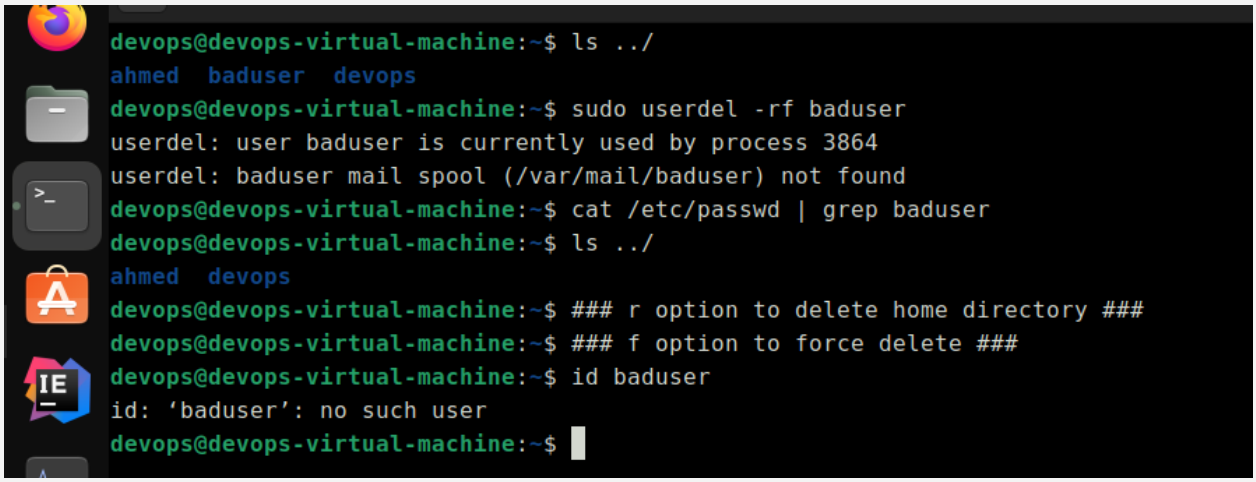
```
devops@devops-virtual-machine:~$ sudo chage -M 30 ahmed
devops@devops-virtual-machine:~$ sudo chage -l ahmed
Last password change                                    : 2023 ,11 أبر
Password expires                                        : 2023 ,11 ماي
Password inactive                                       : 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
devops@devops-virtual-machine:~$
```

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

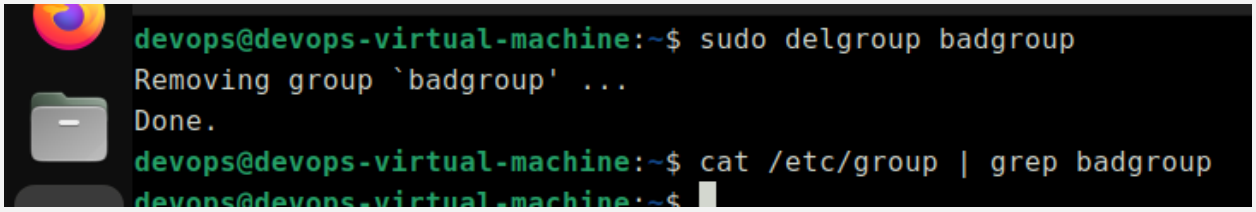
To view a list of locked users, you can use the passwd command with the -S option.

```
devops@devops-virtual-machine:~$ man usermod
devops@devops-virtual-machine:~$ sudo usermod -L baduser
devops@devops-virtual-machine:~$ sudo passwd -S baduser
baduser L 04/12/2023 0 99999 7 -1
devops@devops-virtual-machine:~$ ### L indicates Locked ###
devops@devops-virtual-machine:~$ su - baduser
Password:
su: Authentication failure
devops@devops-virtual-machine:~$
```

9. Delete bad user account



10. Delete the supplementary group called badgroup.



Important note:-

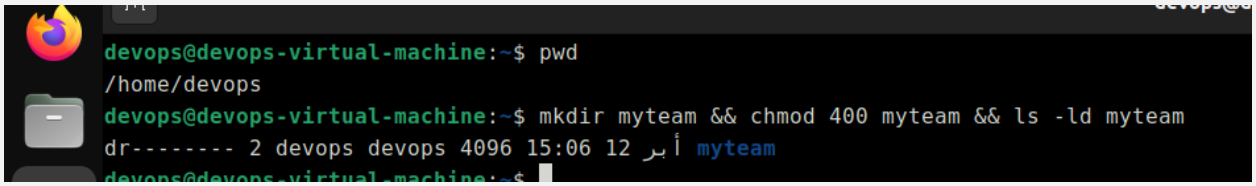
I used **adduser**, **addgroup**, **delgroup** because it's easier to deal with and more interactive as it shows confirmation messages for what's happening behind the scenes.

When I was deleting a user, I used **userdel** because it's more flexible with its option **-rf** which I needed in that case.

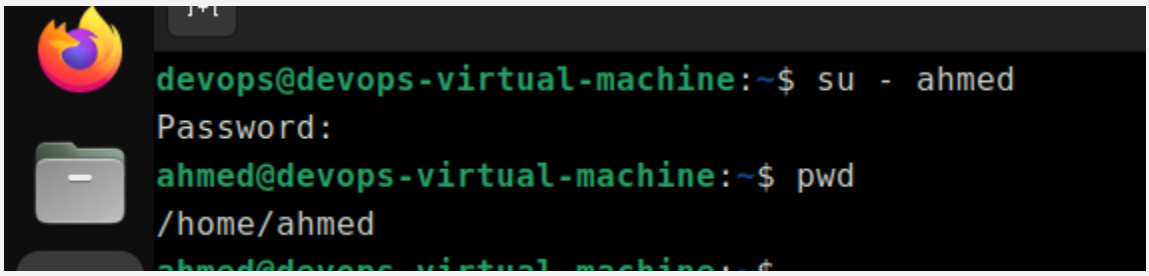
This shows the difference between the two methods, the first one **(adduser)** is easier and does a lot of work for you, but the second one **(useradd)** is far more flexible with a lot of options to manage.

Finally , we should use the second method (useradd) in bash scripting for automation and configuration as it's easier to tune and configure.

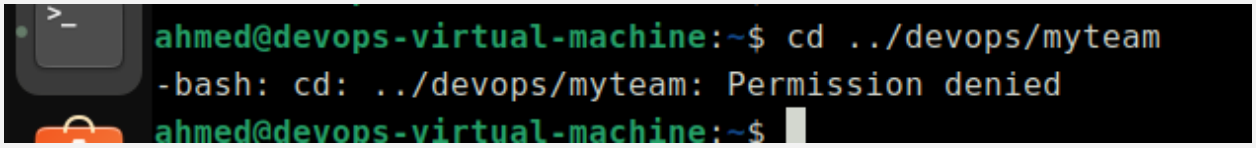
13. Create a folder called myteam in your home directory and change its permissions to read only for the owner.



14. Log out and log in by another user



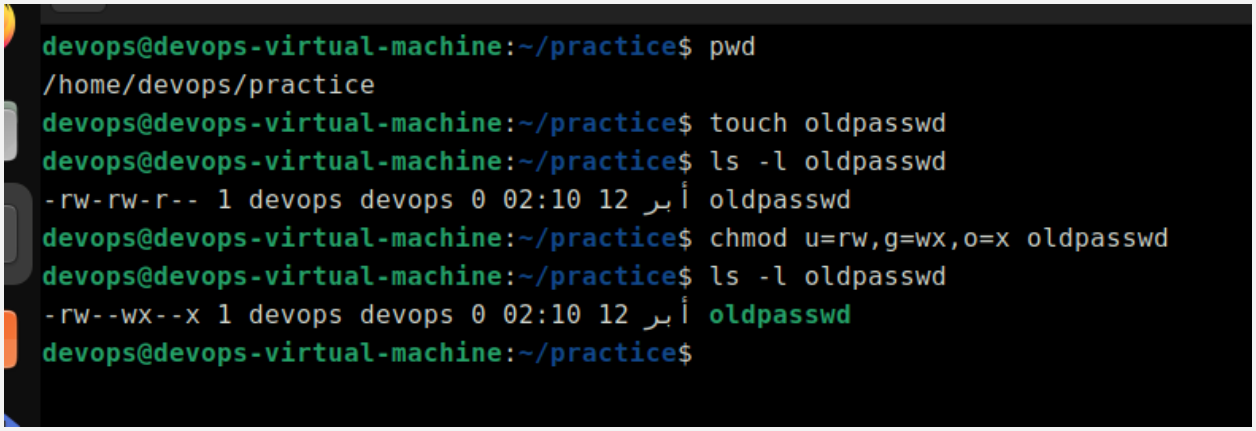
15. Try to access (by cd command) the folder (myteam)



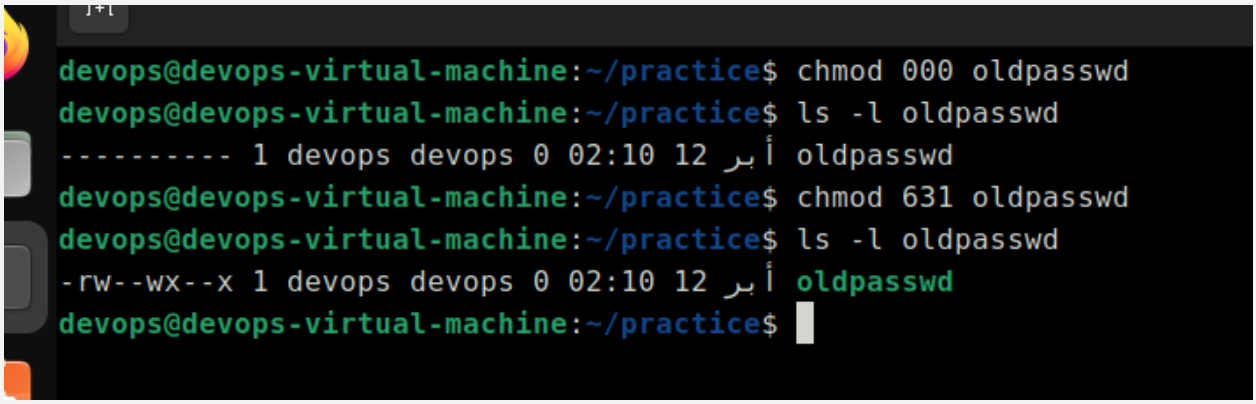
16. Using the command Line

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

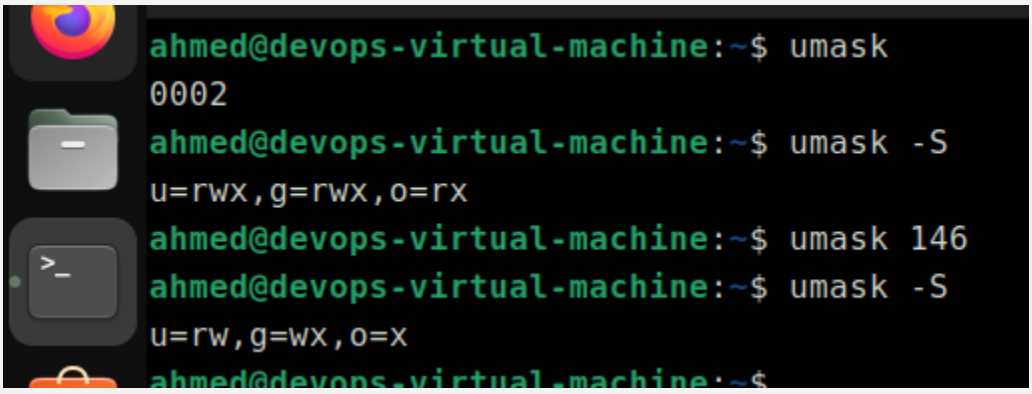
Using symbolic mode:



Using numeric mode:



- **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 directory?**

The maximum permission a file can have is 666, minus the umask value 002 = 664

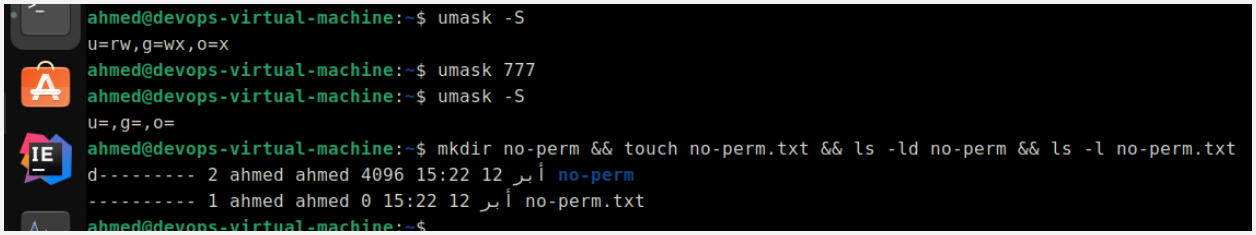
The maximum permission a directory can have is 777, minus the umask value 002 = 775

My default umask value is 002; it may differ for others.

The reason is that directories need the execute permission in order to be searchable.

Without the execute permission, users would not be able to enter the directory or access its contents.

• Change your default permissions to be no permission to everyone then create a directory and a file



17. What are the minimum permission needed for:

• Copy a directory (permission for source directory and permissions for target parent directory)

Read access to the source directory.

Write access to the target parent directory.

• Copy a file (permission for source file and and permission for target parent directory)

Read access to the source file.

Write access to the target parent directory.

• Delete a file

Write permission on the parent directory.

Read and execute permissions on the file.

• Change to a directory

Execute permission on the directory.

• List a directory content (ls command)

Read and Execute permission on the directory.

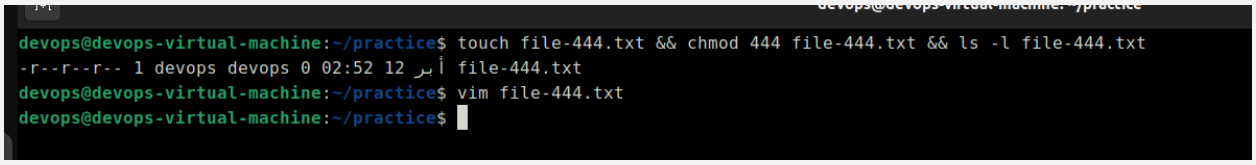
• View a file content (more/cat command)

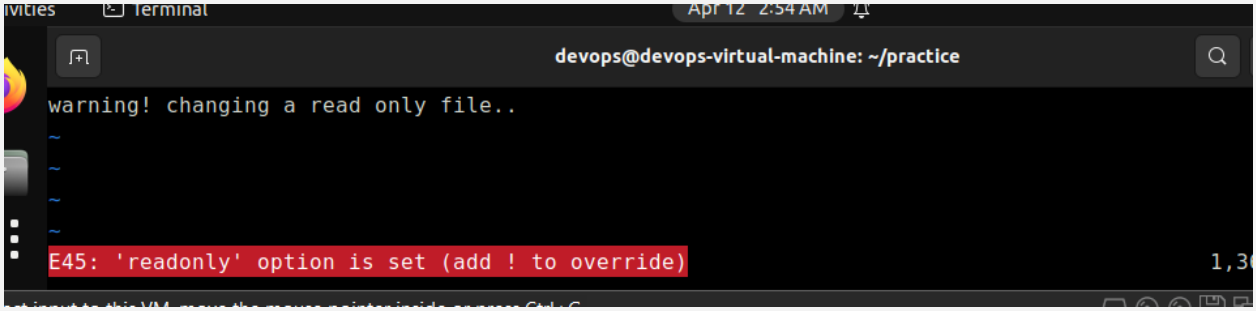
Read permission on the file.

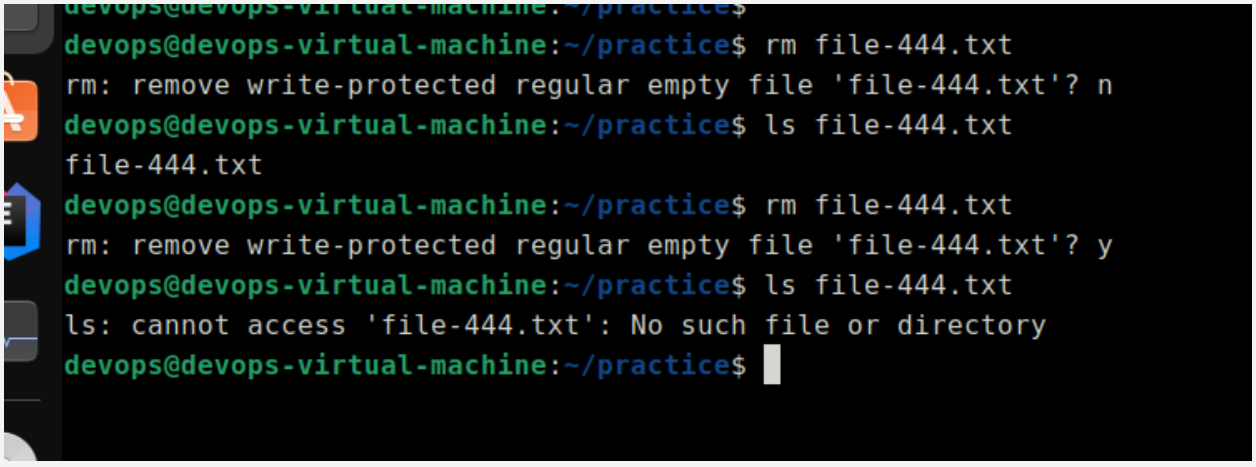
• Modify a file content

Write permission on the file.

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







Try to Edit : Displayed a warning because it's a read only file.

Try to Remove : Prompt a confirmation to remove a protected empty file.

19. What is the difference between the “x” permission for a file and for a directory?

For a file it controls whether the file can be executed as a program or script. For a directory it controls whether you can enter the directory and access its contents.