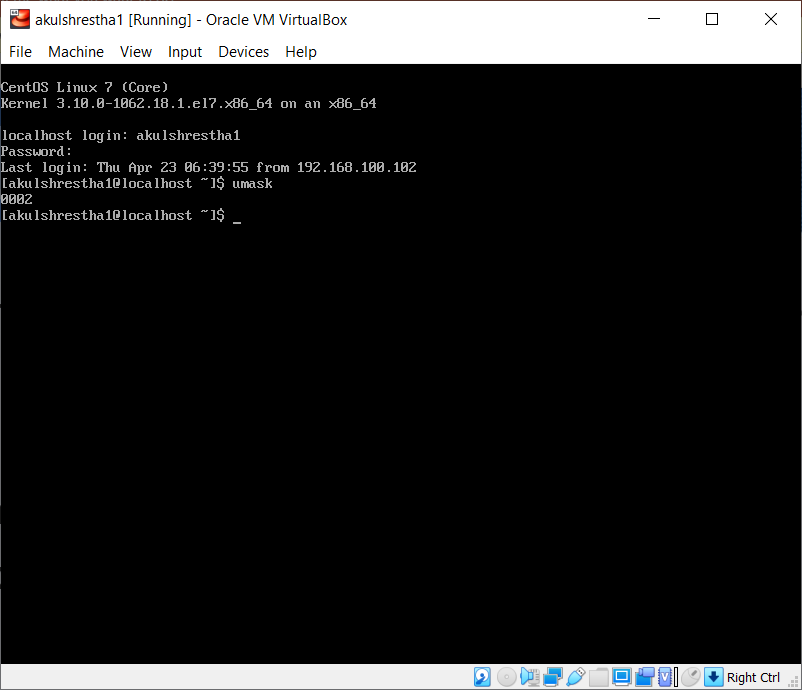
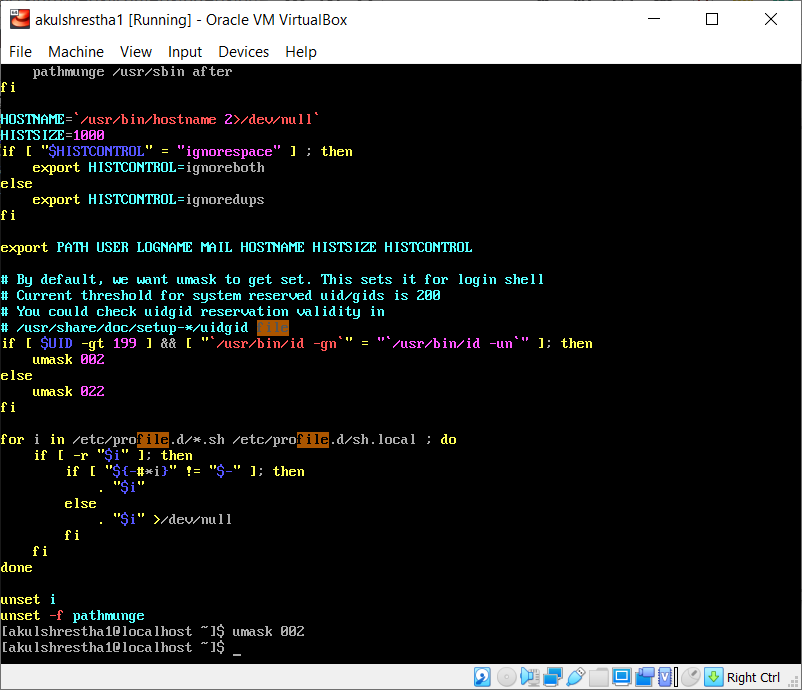
PART I

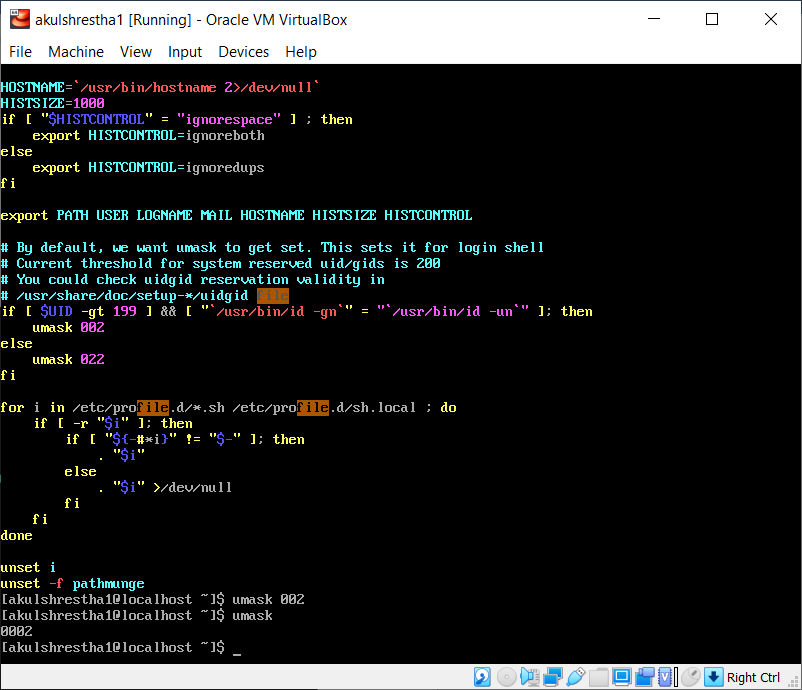
* Watch [File Permissions Video](https://www.youtube.com/watch?v=BmVmJi5dR9c) (10 mins)
* Login to your vm as a regular user
* Check your umask
* Change umask to 002
* Touch file myfile
* Are permissions rw-rw-r--?
* Remove write access to the group
* Create a new directory
* Check permissions
* Can you cd into the new directory?
* Go back to the parent folder
* Eliminate owner execution permission to the new directory
* Can you cd into the new directory?
* Change new directory permissions to 100?
* Can you cd into the new directory?
* Can you do ls?
* Explain

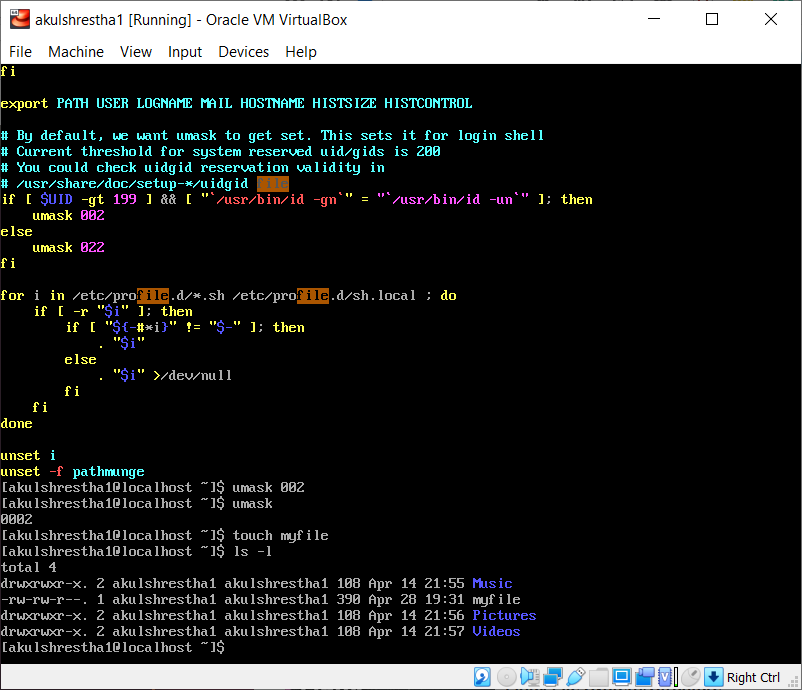
PART II

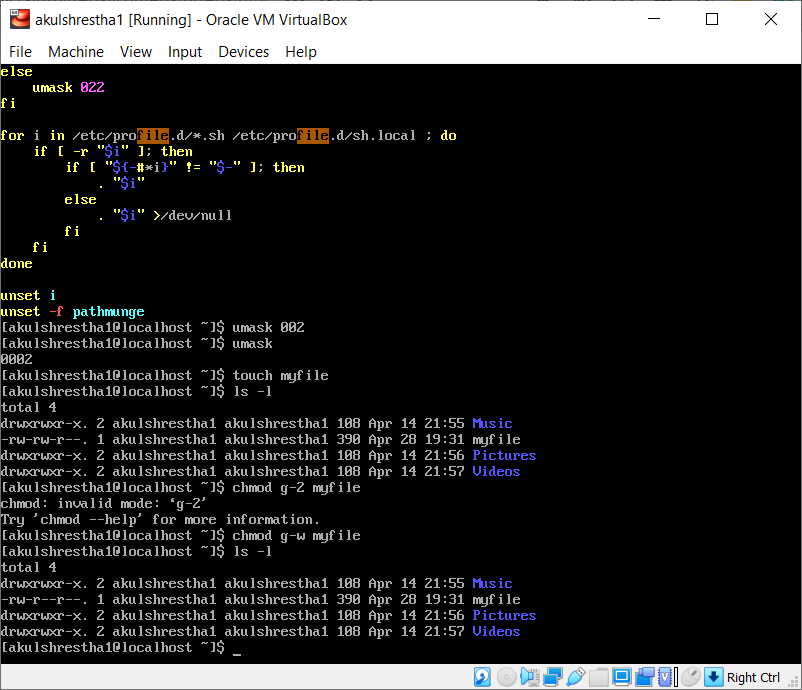
* As **regular user**, create a directory ($**mkdir ~/permissions)**
* Go to the new directory.**($cd ~/permissions)**
* Create a file owned by yourself in there.**($touch file)**
* Copy a file owned by root from /etc/ to your permissions dir. Who owns this file now?**($cp /etc/passswd .)**
* As **root**, create a file in the users ~/permissions directory.
* As **normal user**, look at who owns this file created by root.
* Change the ownership of all files in ~/permissions to yourself. (HINT: login as root)
* Make sure you have all rights to these files, and others can only read.
* With chmod, is 770 the same as rwxrwx--- ?
* With chmod, is 664 the same as r-xr-xr-- ?
* With chmod, is 400 the same as r-------- ?
* With chmod, is 734 the same as rwxr-xr-- ?
* Display the umask in octal and in symbolic form.
* Set the umask to 077, but use the symbolic format to set it. Verify that this works.
* Create a file as root, give only read to others. Can a normal user read this file ? Test writing to this file with vi.
* Create a file as normal user, give only read to others. Can another normal user read this file ? Test writing to this file with vi.
* Can root read this file? Can root write to this file with vi ?

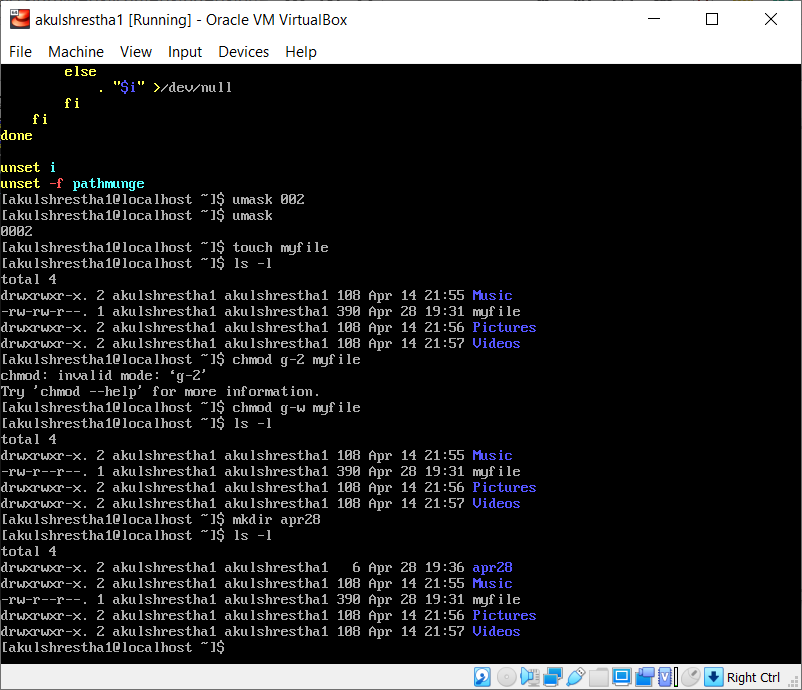


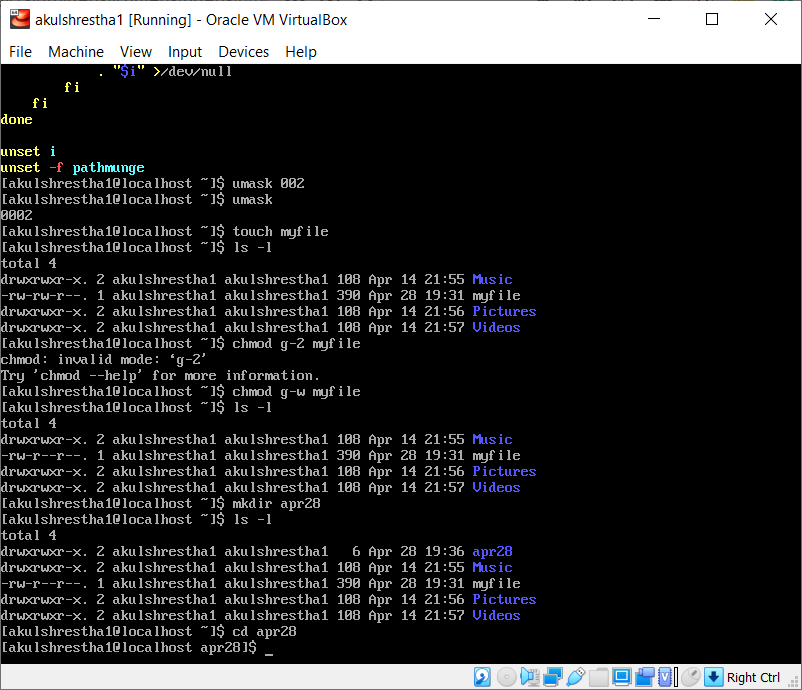


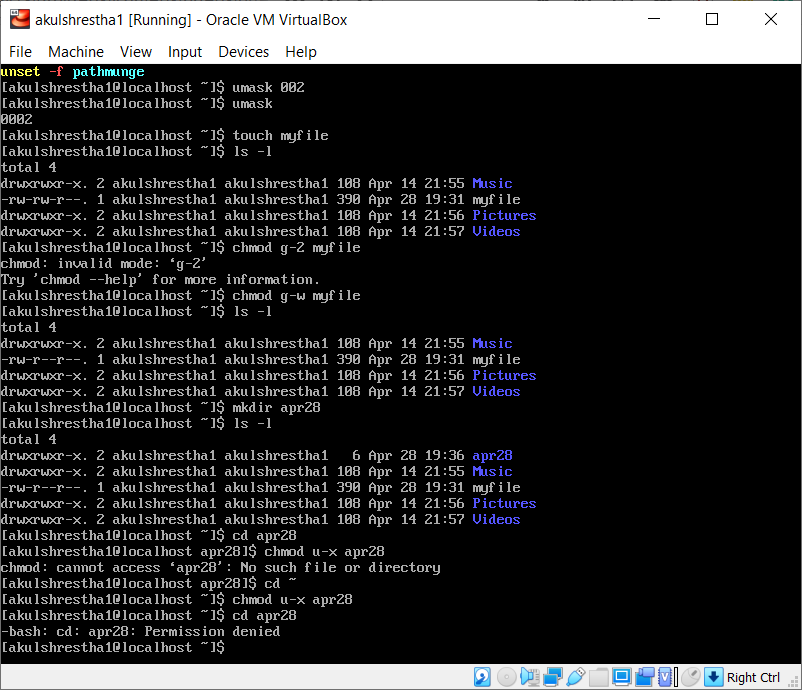


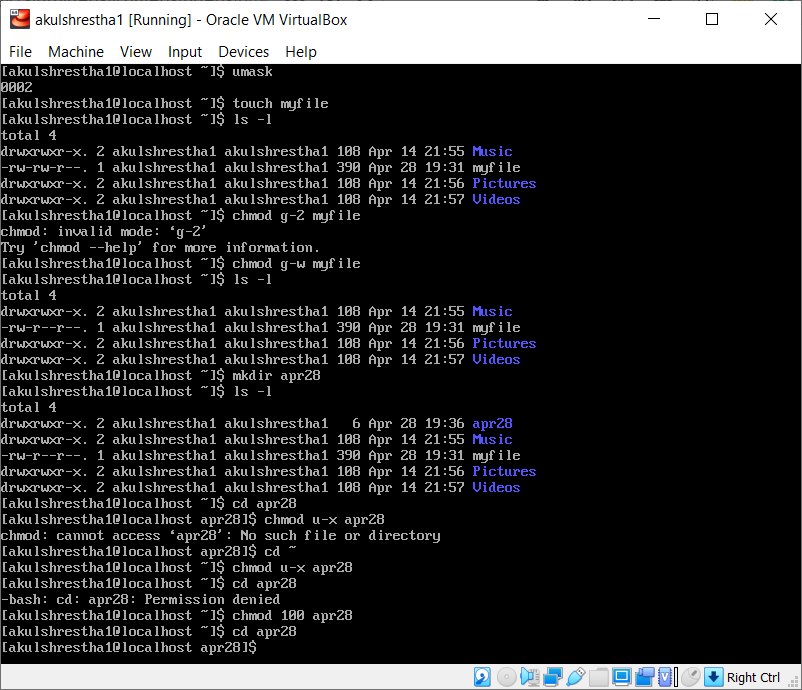


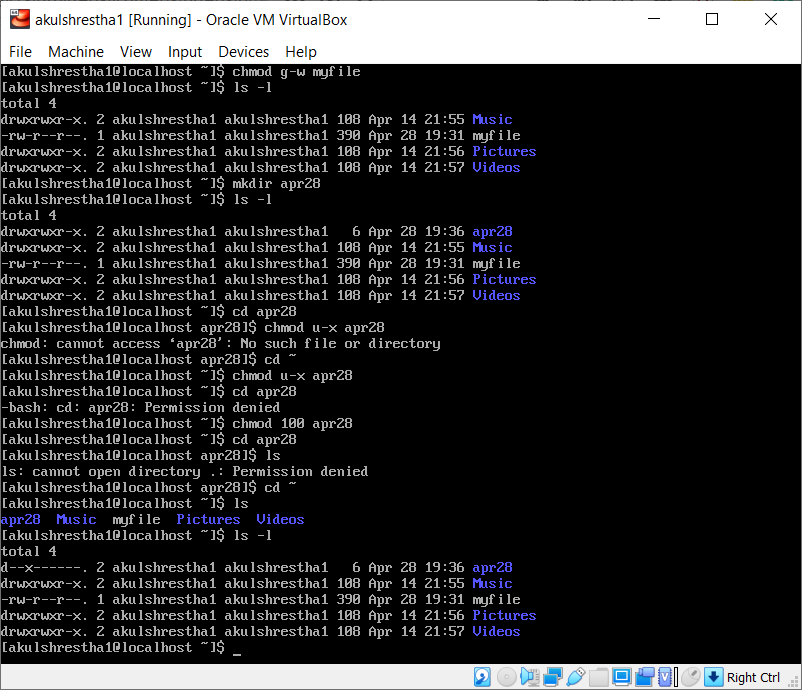












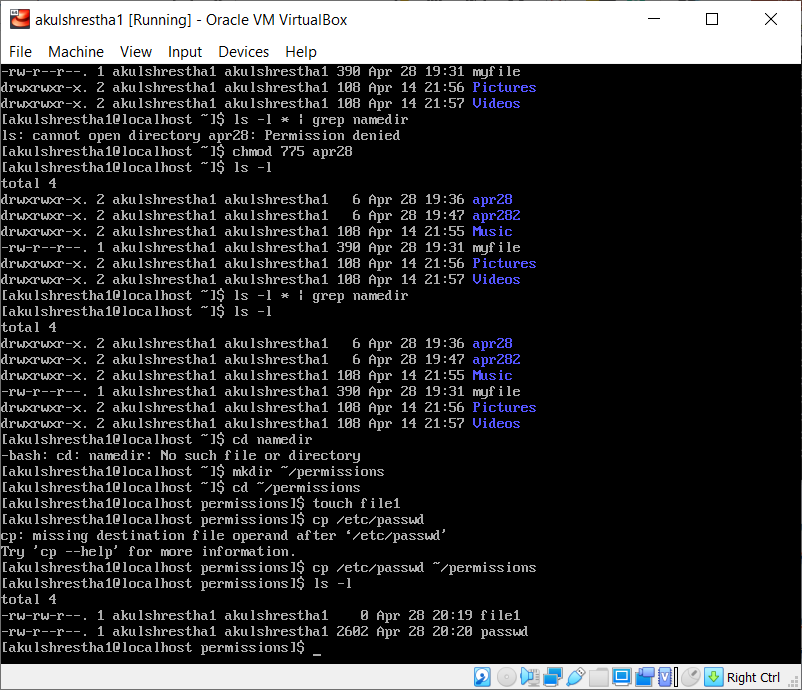
**17. Explanation** – The directory created with the name of apr28 now has permissions as:

Owner – x (can only execute or say cd)

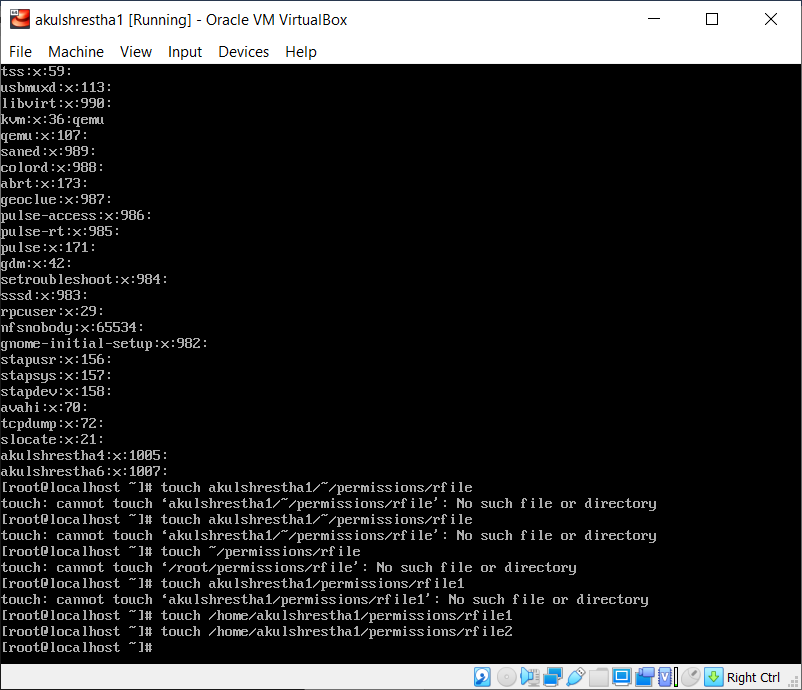
Both group and others have no permissions of read, write or execute.

PART II

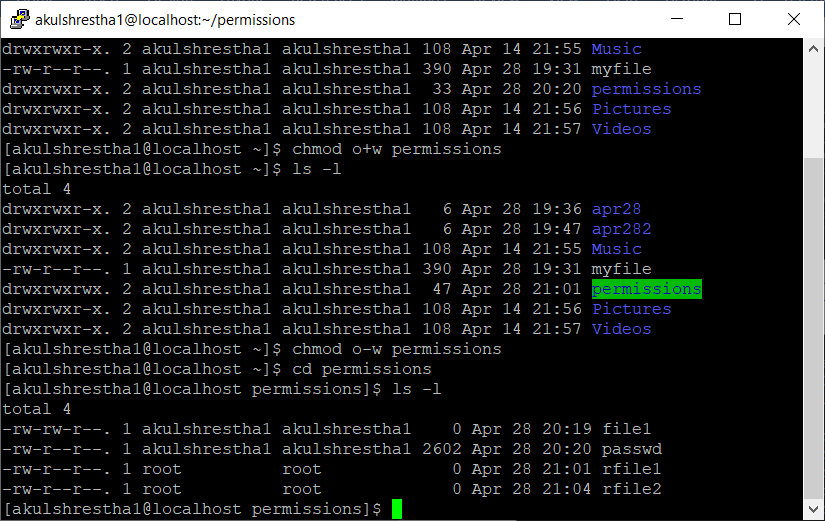
1. As **regular user**, create a directory #**mkdir ~/permissions.**
2. Go to the new directory. **$cd ~/permissions**
3. Create a file owned by yourself in there. **$touch file**
4. Copy a file owned by root from /etc/ to your permissions dir, who owns this file now ? **$cp /etc/passswd .**



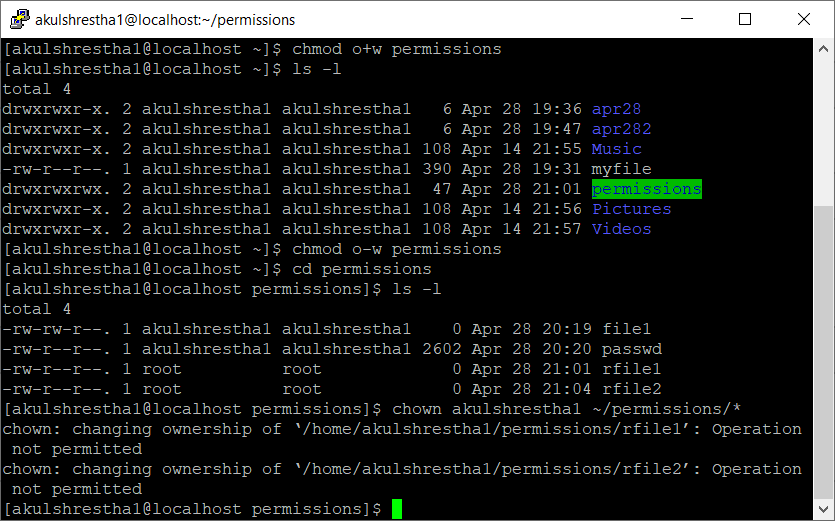
1. As **root**, create a file in the users ~/permissions directory.

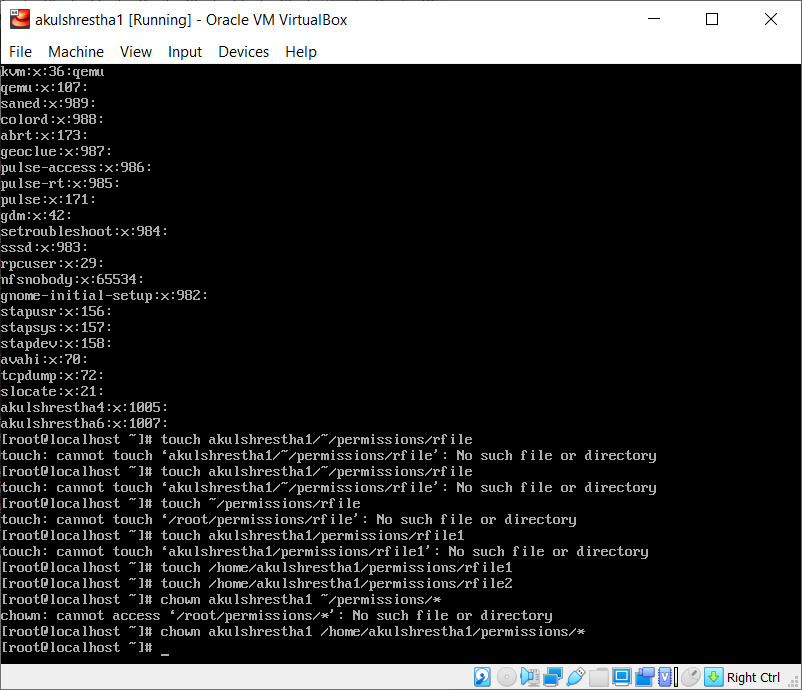


1. As **normal user**, look at who owns this file created by root.

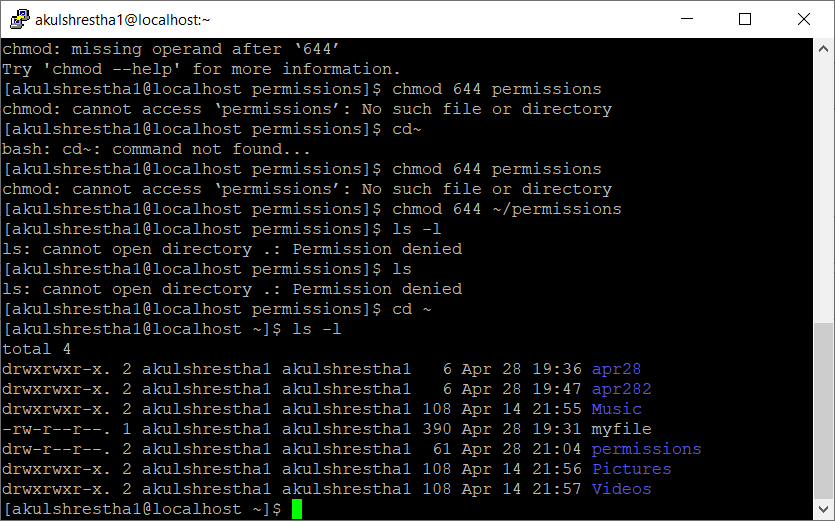


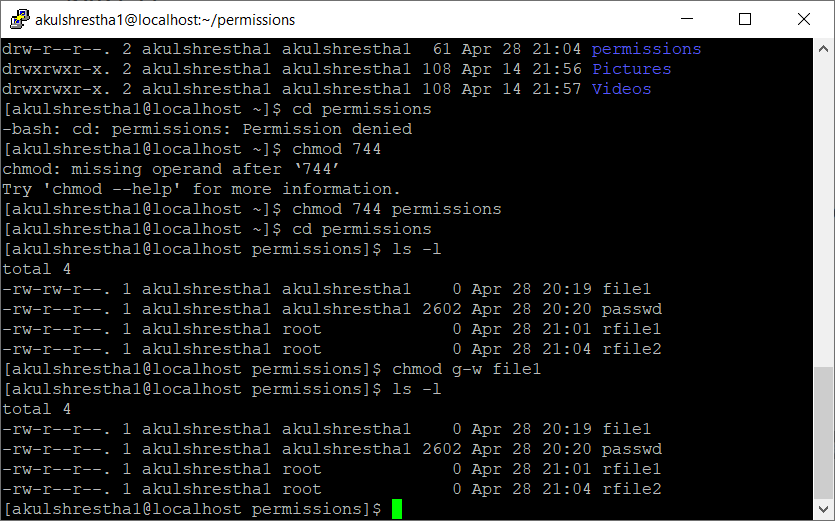
1. Change the ownership of all files in ~/permissions to yourself.

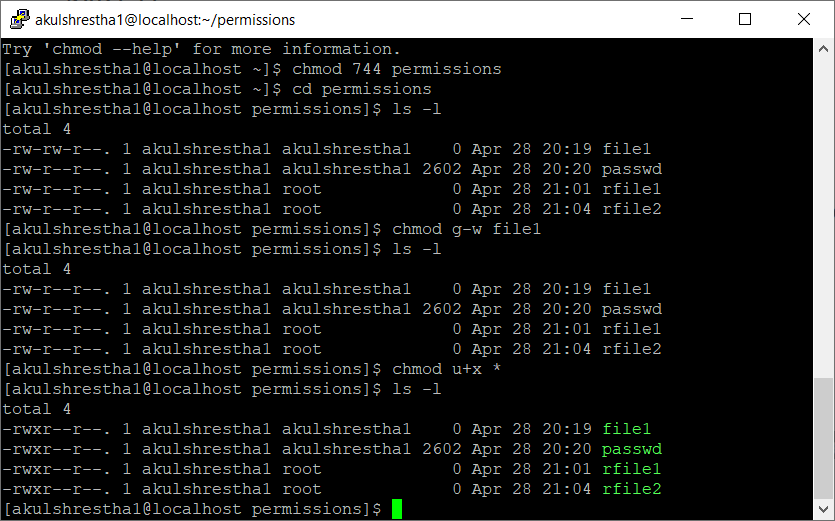




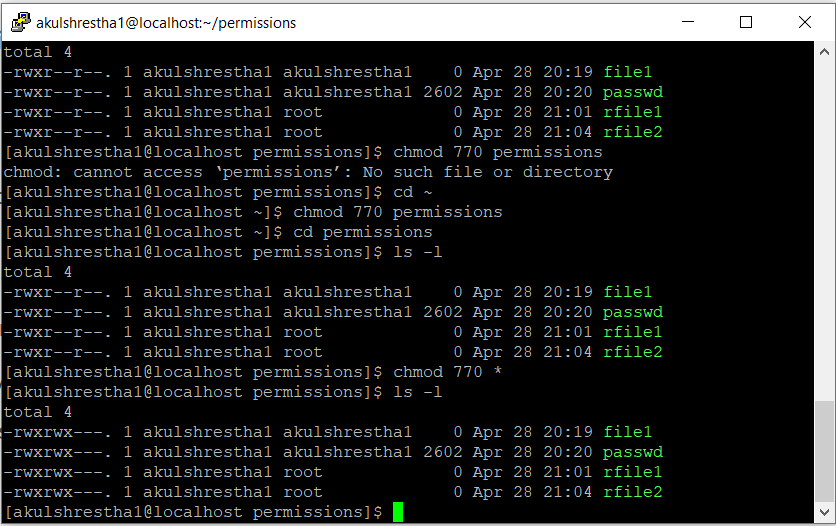
1. Make sure you have all rights to these files, and others can only read.



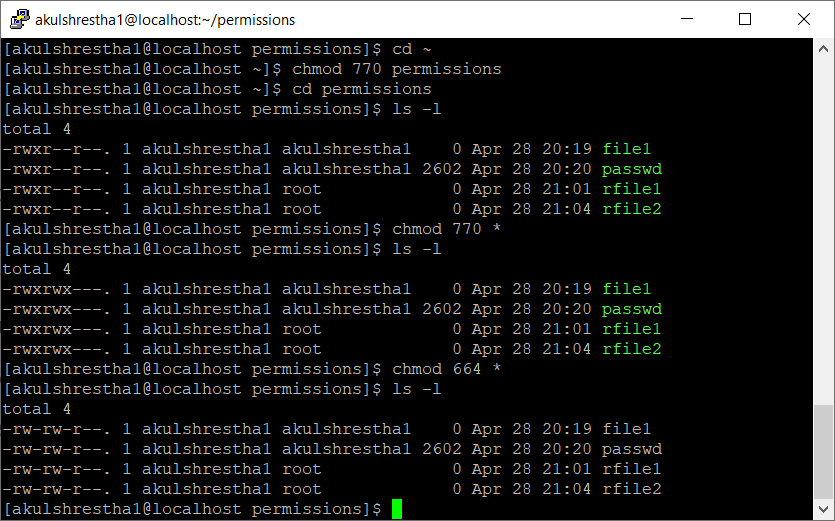




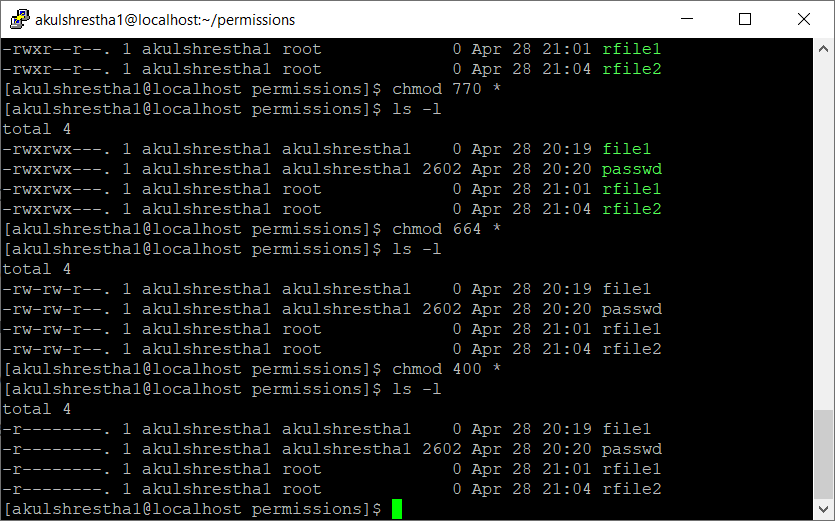
1. With chmod, is 770 the same as rwxrwx---? Yes



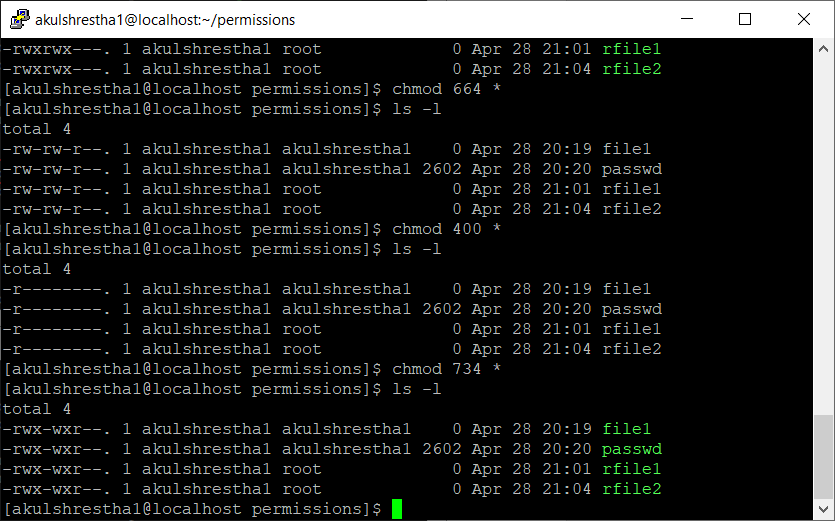
1. With chmod, is 664 the same as r-xr-xr--? No.



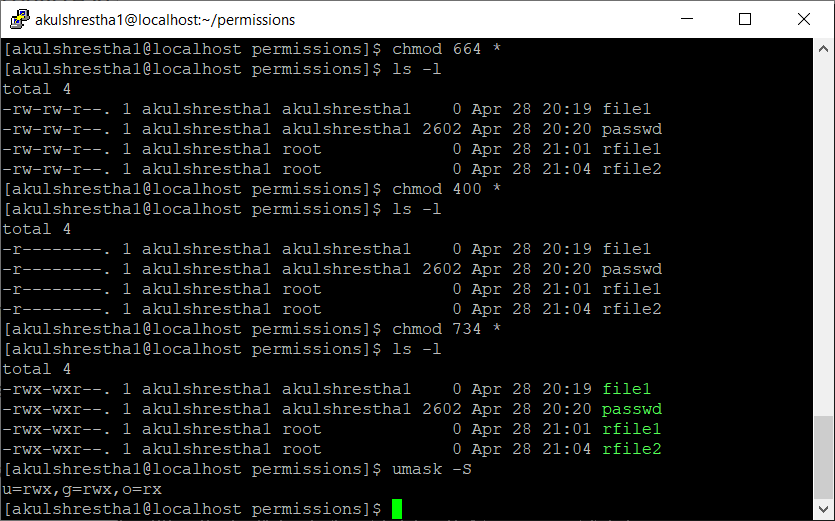
11. With chmod, is 400 the same as r--------? Yes.



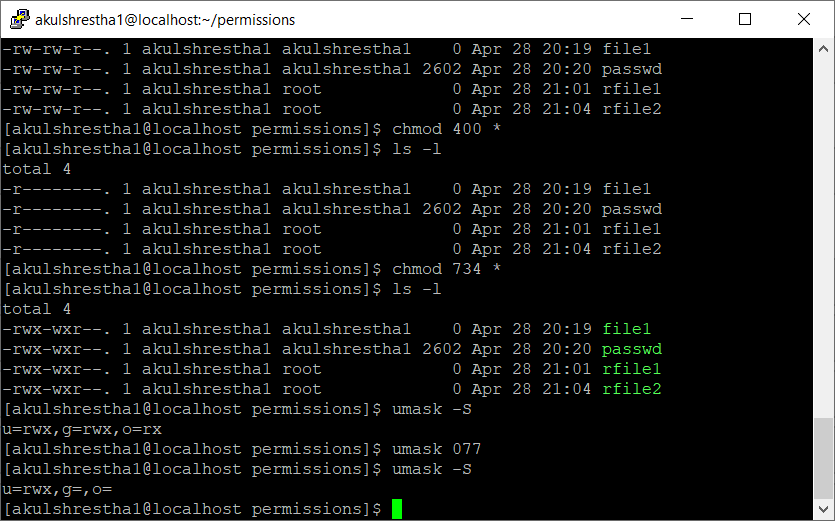
12. With chmod, is 734 the same as rwxr-xr-- ? No.



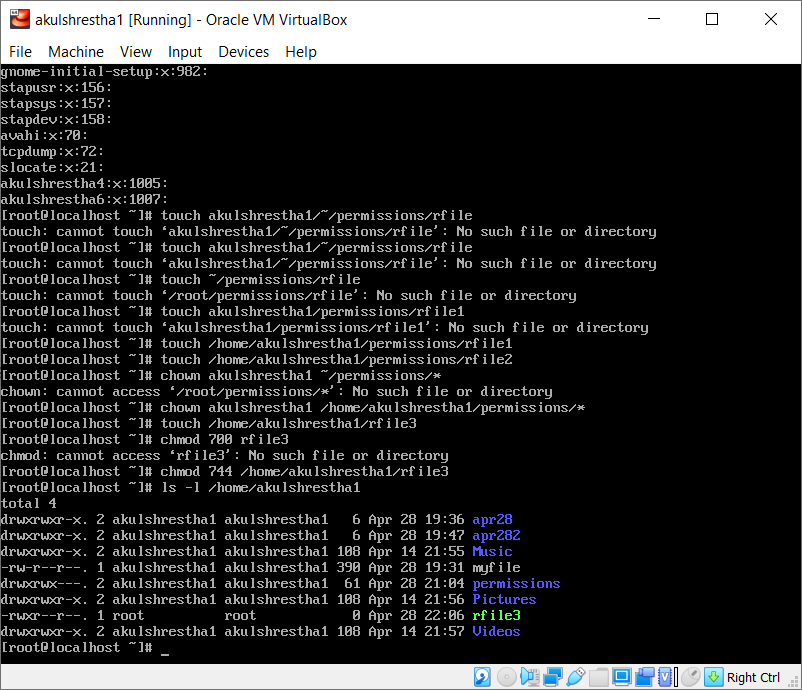
13. Display the umask in octal and in symbolic form.

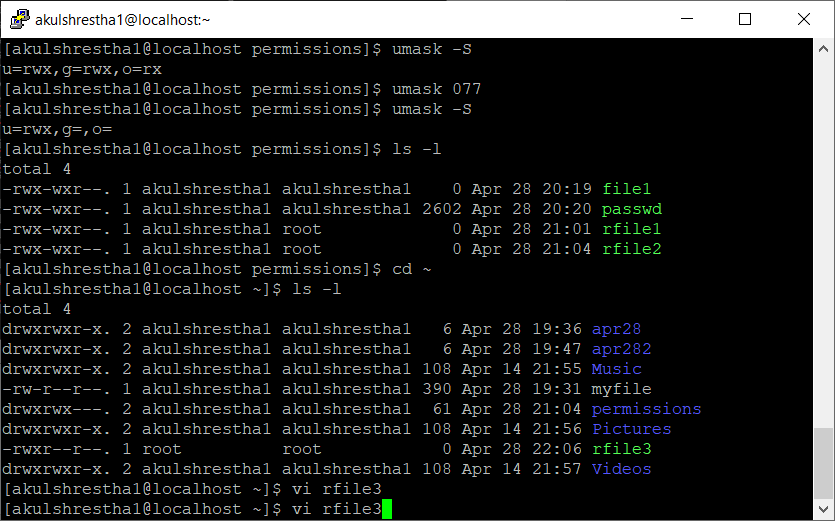


14. Set the umask to 077, but use the symbolic format to set it. Verify that this works.



15. Create a file as root, give only read to others. Can a normal user read this file? Test writing to this file with vi. Yes, a normal user can read this file. Writing is not permitted.

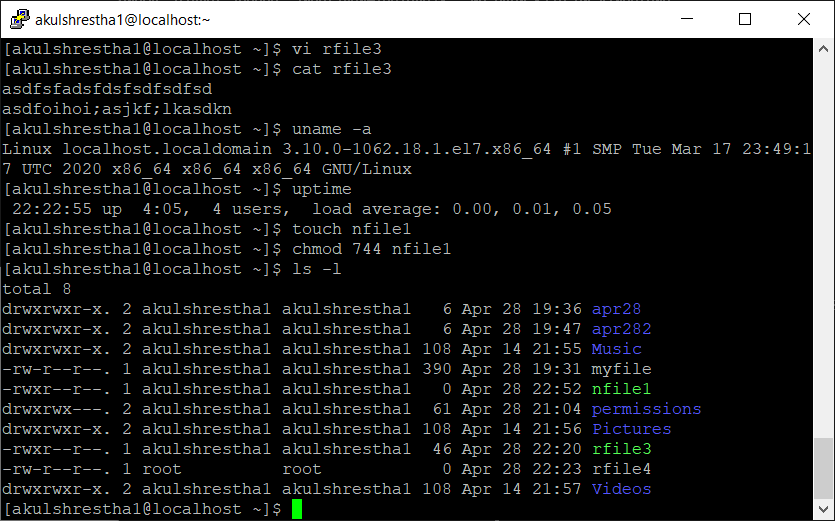


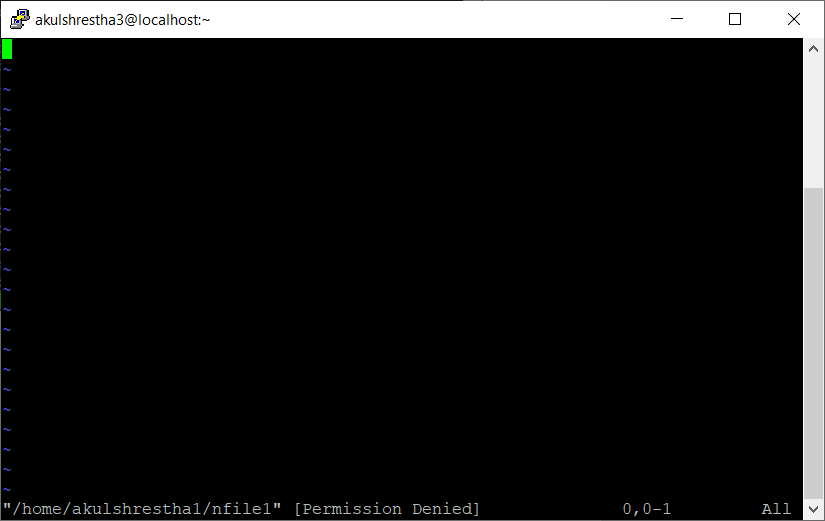




16. Create a file as normal user, give only read to others. Can another normal user read this file? Test writing to this file with vi.

Yes, another reader can read the file. But writing is not allowed.





17. Can root read this file? Can root write to this file with vi?

Yes, root can read the file. And root can write to this file with vi.

