KALI LINUX

Coventry University

Softwarica

College of IT & E-commerce

Name: Abhishek Adhikari

Class: Foundation Group 37A

Email: adhikaryabhishek209@gmail.com

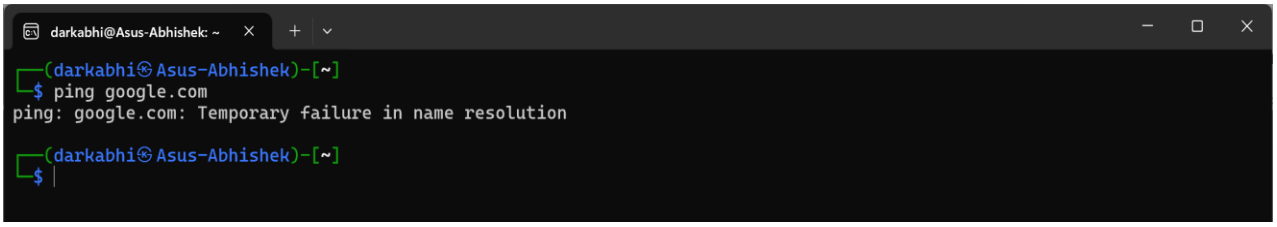
Submitted to Rikesh Maharjan

Table of Contents

Linux Fundamentals Examination

Setting up the terminal:

Visual: The terminal screen shows the command.



1. Basic Commands:

a) What does Type 2 **Hypervisor** do? Explain with examples?

A Type 2 Hypervisor, also known as a hosted hypervisor, runs on a conventional operating system and abstracts hardware resources to create and run virtual machines. Examples include VMware and Oracle VirtualBox.

b) While running “LS -lha” this command i am having an error. Why am I getting errors with proof of concept?

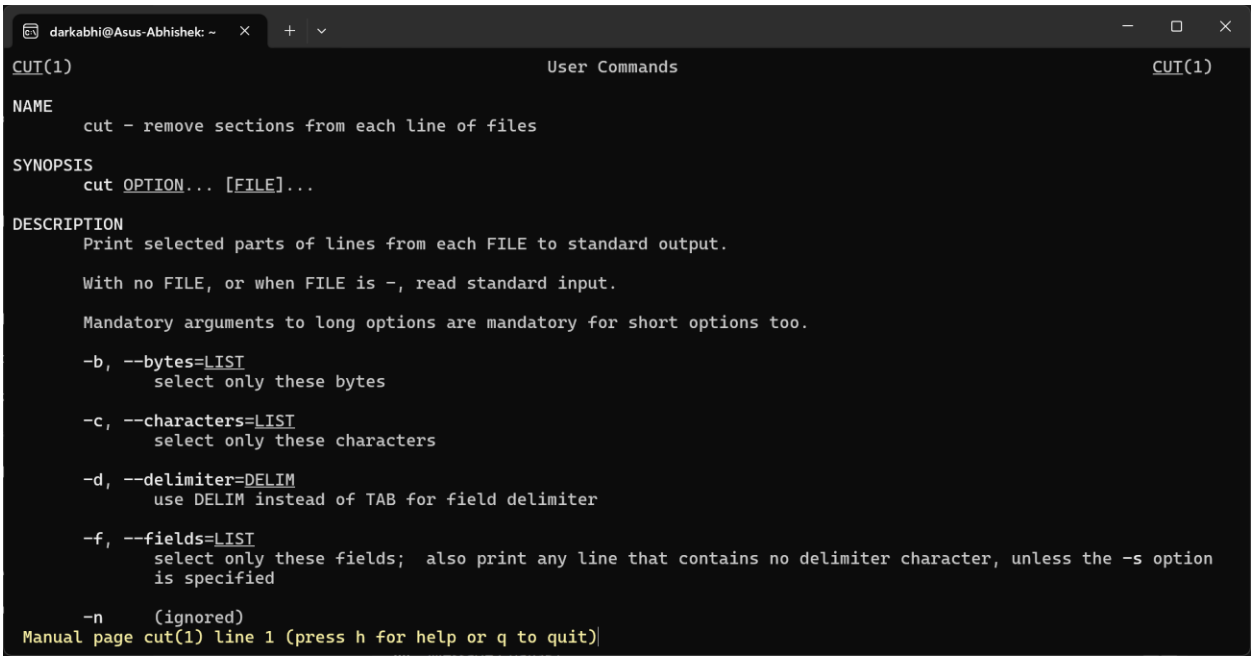
The command `*LS*` is incorrect because the correct command is ls. Linux is case-sensitive, so `*LS*` will not be recognized as a valid command.

- **Proof of concept:**

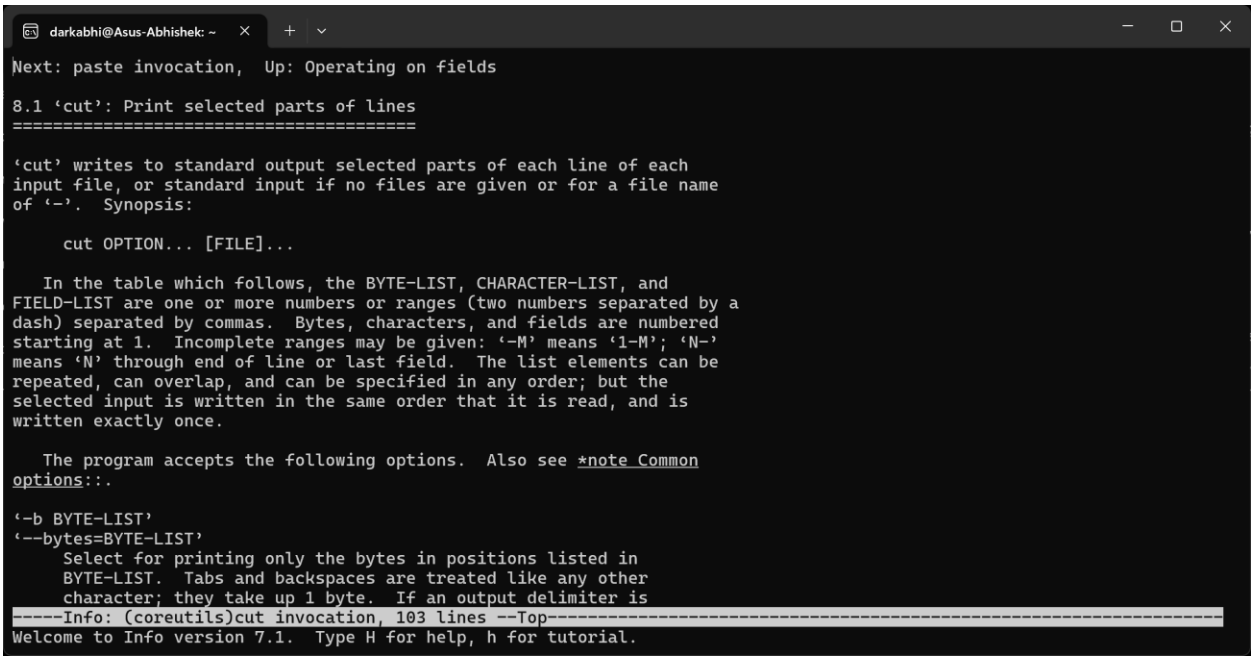
c) I don't know how to use the cut command in linux so What two commands can I use in Kali Linux to access detailed help and documentation for system commands, and how can I view examples of their usage?

You can use the following two commands to access help and documentation:

1. `*man*` cut – For example, man cut will show the manual for the cut command.

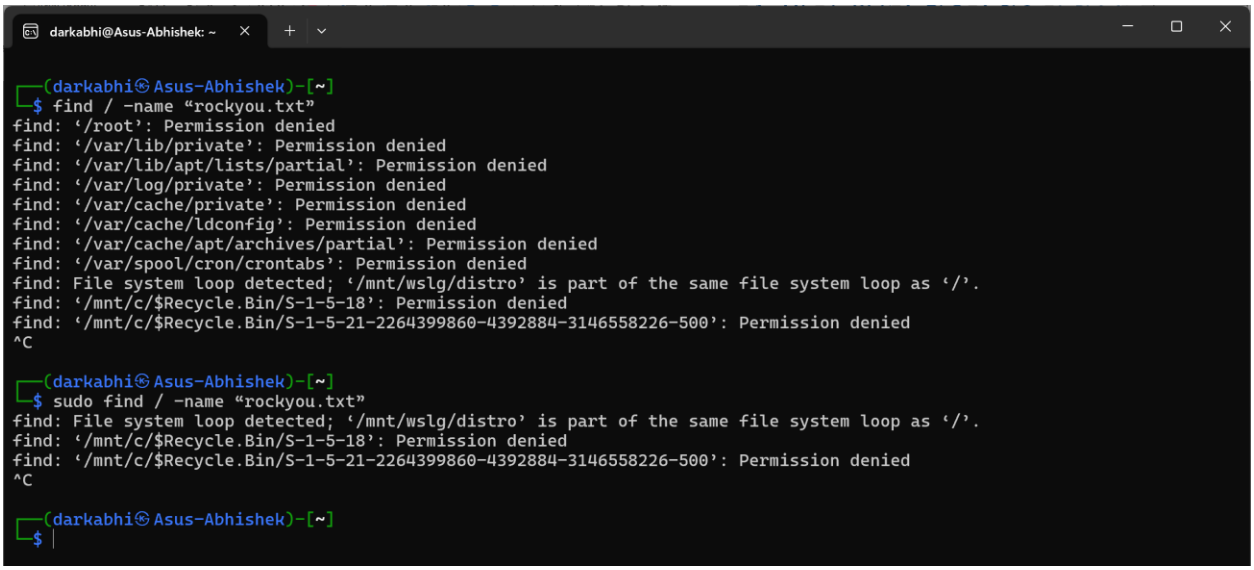


2. `*info*` cut – For example, info cut provides detailed information and examples.



d) Find rockyou.txt or rockyou.txt.gz file from your computer using find command?

This will search the entire file system for rockyou.txt but I use wsl and it didn't work even I fetched rockyou.txt file form github repository.



e) I need to find user accounts in my shadow file where the password field is specifically**!** * What command can I use to extract only these entries from the shadow file?

This will search the /etc/shadow file for entries and greps all content with “!” then cuts the second field of the output array splitting from “:” and console into the terminal.

f) What is the significance of 2 > /dev/null file?

It redirects standard error to /dev/null, which is a null file that discards all data written to it same as black hole of the universe which destroys the existence of the data.

g) What will happen when we provide 4777 permission to /bin/cat file? with proof of concept?

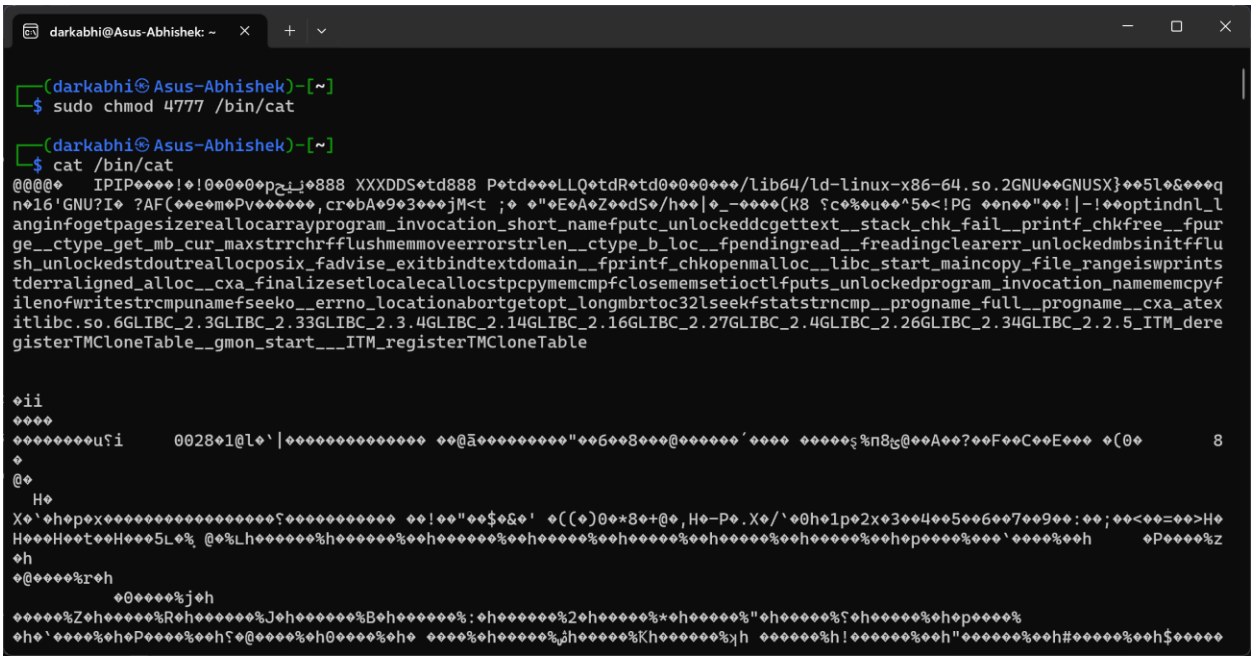
The permission 4777 means:

- **4 (SUID bit)**: The program will run as the owner.
- **7 (rwx)**: Read, write, and execute permissions for the owner, group, and others.

When setting 4777 permissions on /bin/cat, any user executing the cat command will do given command with root permissions, which is insecure or risky.

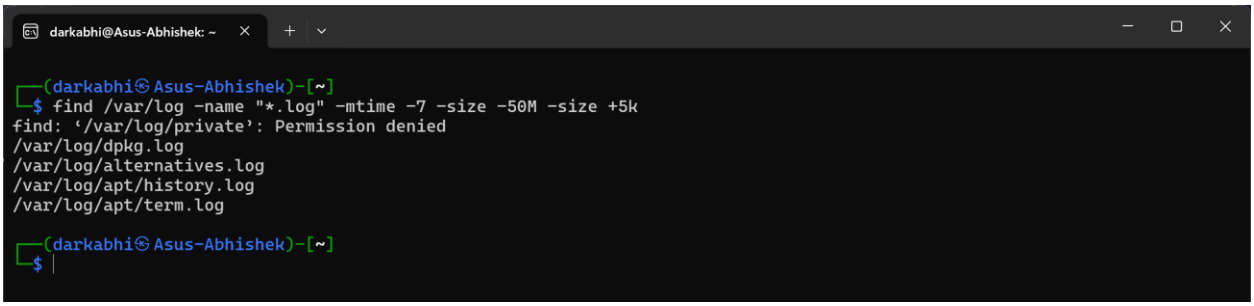
- **Proof of concept:**

  If a regular user runs the cat command, it will execute with elevated privileges.



h) How would you use the find command to locate all files in the /var/log directory that have a .log extension, were modified in the last 7 days, and are smaller than 50MB larger than 5KB?

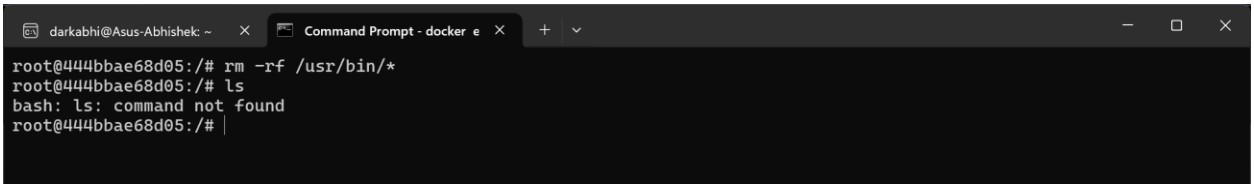
The find command is use to finding files and directories using flag -type f or d means file or directories by default it is f and -name flag is to tell it to search for the name given by the user also -mtime flag is to order for time duration and -size for file size here which is +5K means greater than 5 KB and -50M means less than 50 MB.



2. File System:

a) What happened when we run “sudo rm -rf /usr/bin/*” Describe this in brief, **if possible,** provide screenshots?

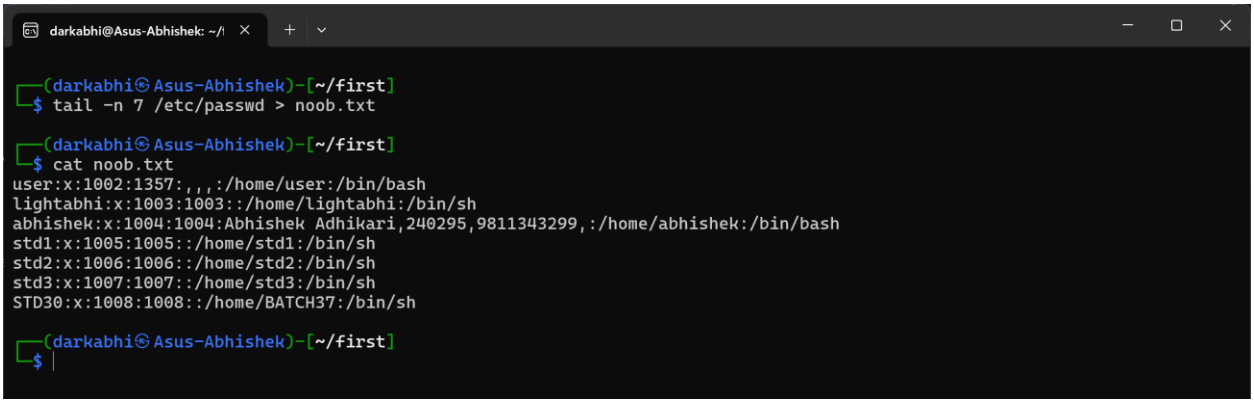
Running this command will recursively and forcefully remove all files in /usr/bin, which contains essential system binaries same as C: Drive in windows. It can break the operating system, making it unbootable or unusable system crasshes. Here, Docker virtual container is used to show the command as it will only crash the container which wont harm the system outside it.



3. Standard Redirection:

a) Display the last 7 lines of a passwd file onto the terminal and save it as noob.txt.

The `*tail*` command is use to display the context of the file from bottom and flag -n tells it to number of lines.



b) Redirect these lines to a new file called hacked.txt located in the /var/tmp directory.

The `*tail*` command is use to display the context of the file from bottom and flag -n tells it to number of lines and redirecting it into the /var/tmp/hacked.txt.

c) Verify that summary.txt contains the last 7 lines of noob.txt and ensure no extra or missing lines are present. What command can you use to confirm that hacked.txt matches the extracted lines from noob.txt?

The `*diff*` command is use to see the difference in 2 files. If null nothing means they are same.

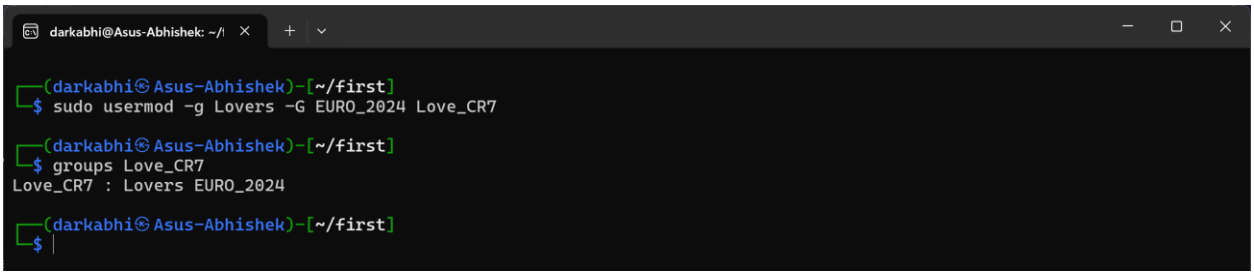
4. User Management and File Permissions:

a) Create a new user named "Love_CR7" with a unique password, a home directory in /home/Love_CR7, and a default shell of /bin/bash.

The `*useradd*` command is use to create new user and -m means make a home directory, -d means location of the home directory and -s means shell.

b) Add the user "Love_CR7" to the primary group "Lovers" and the secondary group "EURO_2024".

The `*usermod*` command is use to change the group of the user, flags -g means primary group and -G means secondary group.



c) Set the uid of LOVE_CR7 user as 1337 because it was my Lucky number.

The `*usermod -u*` command is use to change the iud of the group.

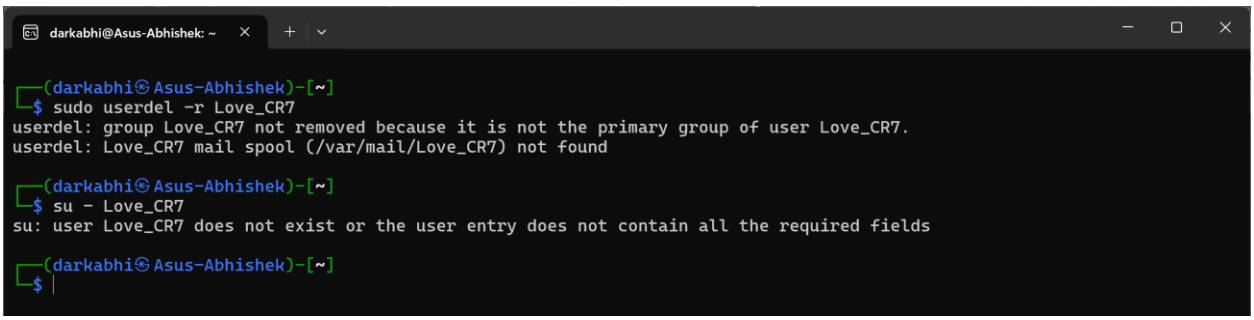
d) Create a file named "project_report.txt" in the home directory of "Love7" with the content "I love number 7 " and assign EURO_2024 group to this file.

e) Change the password for the user "Love_CR7" to a new password as “ronaldo7”.

The `*passwd*` command is use to change the password of the user.

f) Delete the user "Love_CR7" and their home directory.

The `*userdel*` command is use to delete the user and -r means all files and folder linked with the user's home directory



5. Virtualization:

a) What is Virtualization and why company need it also name 2 software which Provide virtualization platform.

Virtualization: Virtualization refers to creating a virtual version of something, such as operating systems, servers, or storage devices. Companies need virtualization to reduce hardware costs, improve scalability, and optimize resource usage. Examples of software include VMware and VirtualBox.

Why companies need it: Companies use virtualization to reduce hardware costs, improve scalability, enhance disaster recovery options, and simplify management.

Two software platforms:

- VMware
- VirtualBox

b) How can we install the kali linux in Virtual box or vmware if we have (kali.ova, kali.vdi, kali.iso)?

- For .ova file: In VirtualBox or VMware, go to "File" > "Import Appliance" and select the .ova file.
- For .vdi file: Create a new VM in VirtualBox, then use the .vdi as the virtual disk.
- For .iso file: Create a new VM and attach the .iso file as the installation medium.

6. Text Editor:

a) What command will you use to open the file "config.txt" in Vim?

The `*vim config.txt*`command is use to open the file in vim.

b) What is the difference between normal mode and insert mode in Vim?

Normal mode: Used for navigating and editing text (copy, paste, delete, etc.).

Insert mode: Used for entering and modifying text.

c) How can you undo the last change you made in Vim?

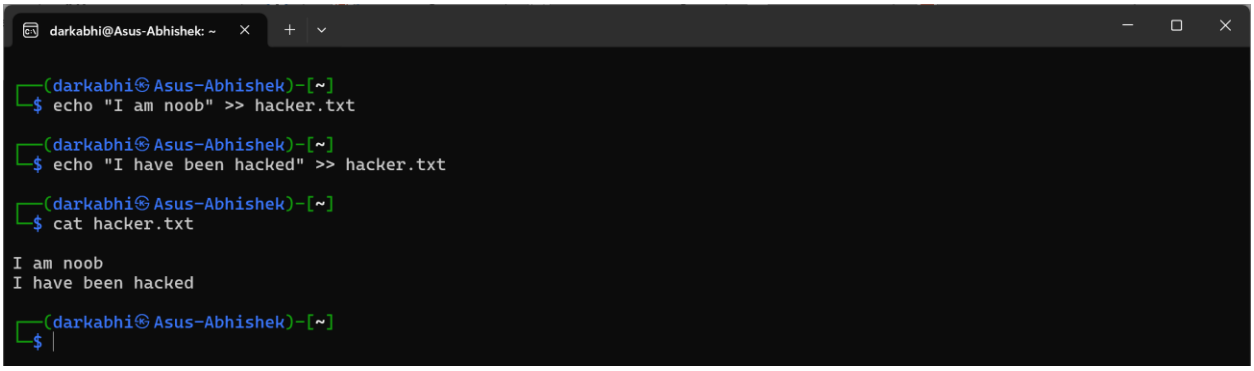
Press `*u* in normal mode to undo the last change.

d) What command will you use to save the changes and exit Vim?

The `*:wq*` command is use to save the changes and exit vim. Press `*esc*` and type `*:wq*` and then enter.

e) Write “I am noob” append this in hacker.txt and “i have been hacked” add this to hacker.txt file using echo command.

The `*echo*`command is use to write or append content to the file. > indicates write which will replace data of the file to user’s input and >> indicates append means adding data’s to the file.



7. Create a Directory (Garuda):

a) Set the directory permissions so that only the owner has read, write, and execute access. For the group and others, allow read and execute access only, using numeric notation. Ensure the directory is set as a restricted deletion flag to prevent group members from deleting files they don't own.

The `*mkdir*` command is use to make a new directory and `*chmod*` command is use to change the permission of the directory which indicates the permission of user, group and others. (read = **4**, write = **2**, execute = **1**)

- 755: Owner has full permissions, while the group and others can only read and execute.
- +t: Sets the sticky bit, preventing group members from deleting files they don't own.

b) Create three hidden files with different permissions inside the directory. (Using Character Notation)?

The `*touch*` command is use to create the file and . indicates the hidden file.

c) Set permissions for each file:

The `*chmod*` command is use to change the permission of the file which refers to (read = **4**, write = **2**, execute = **1**)

File 1: "Portugal.txt": Accessible only by the owner with read and write permissions and change the owner of the file to Love_CR7.

The `*chown*` command is use to change the owner of the file.

File 2: "Team_CR7.txt" - Accessible only by the group with read and write permissions also change the group owner as EURO_2024.

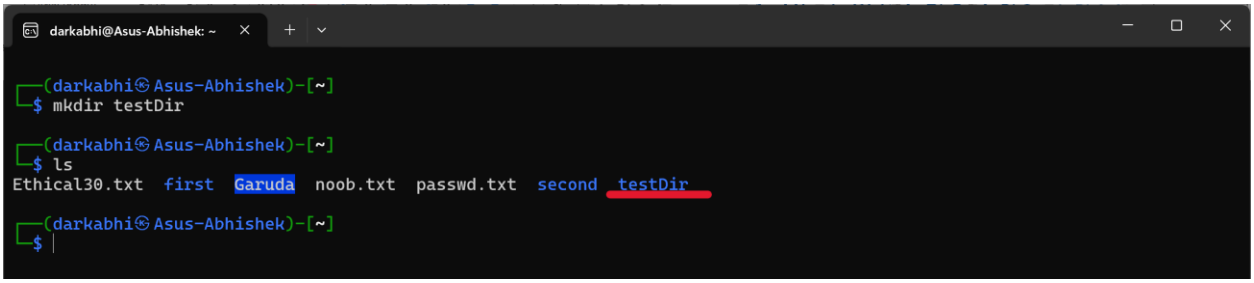
The `*chown*` command is use to change the owner of the file.

File 3: "public.txt" – Accessible to all users with read-only permissions and change the owner to Love_CR7 and group owner to EURO_2024.

8. Create and Understanding about Directory:

a) Create a directory named testDir

The `*mkdir*` command is use to make a new directory.

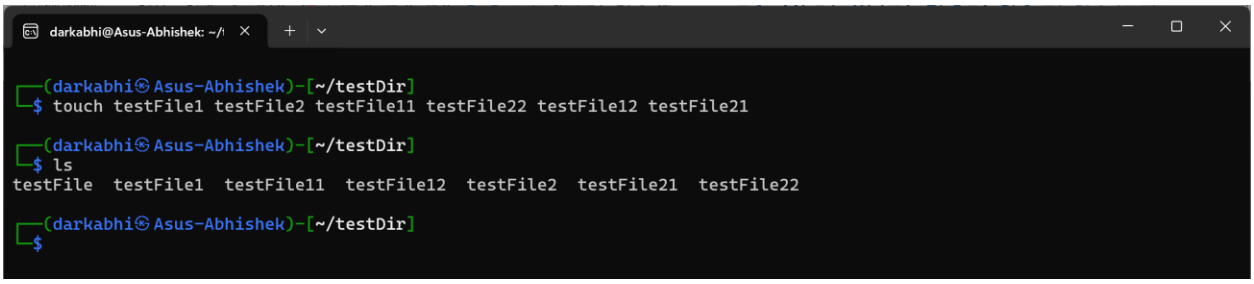


b) Within testDir, create an empty file named testFile

The `*touch*` command is use to make a new file.

c) Within testDir directory, use only one command to create the following empty files: testFile1, testFile2, testFile11, testFile22, testFile12, testFile21.

The `*touch*` command is use to make a multiple file separated by spaces.



d) Remove file(s) containing 1 in their file name without specifying their name

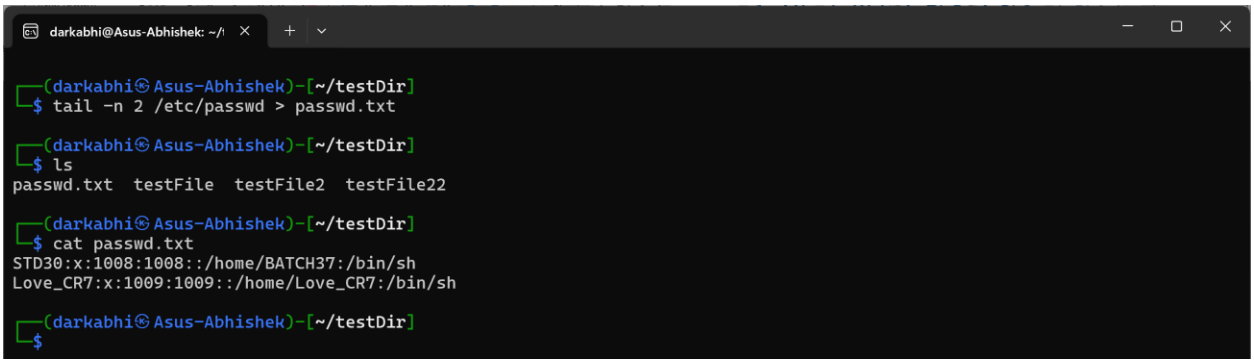
The `*rm*` command is use to remove the file and * indicates all or any but in this cane 1 is in the middle means anything 1 and anything then It remove the files containing 1.

e) Display the first 2 lines of /etc/passwd

The `*head -n 2*` command is use to display the file from top and flag -n 2 means numbers of line from above.

f) Create a file named passwd.txt that stores the last 2 lines of /etc/passwd

The `*tail -n 2*` command is use to display the file from bottom and flag -n 2 means numbers of line from bottom and > will create the file for us.


darkabhi@Asus-Abhishek: ~/t
(darkabhi㉿Asus-Abhishek)-[~/testDir]
$ tail -n 2 /etc/passwd > passwd.txt
(darkabhi㉿Asus-Abhishek)-[~/testDir]
$ ls
passwd.txt testFile testFile2 testFile22
(darkabhi㉿Asus-Abhishek)-[~/testDir]
$ cat passwd.txt
STD30:x:1008:1008::/home/BATCH37:/bin/sh
Love_CR7:x:1009:1009::/home/Love_CR7:/bin/sh
(darkabhi㉿Asus-Abhishek)-[~/testDir]
$