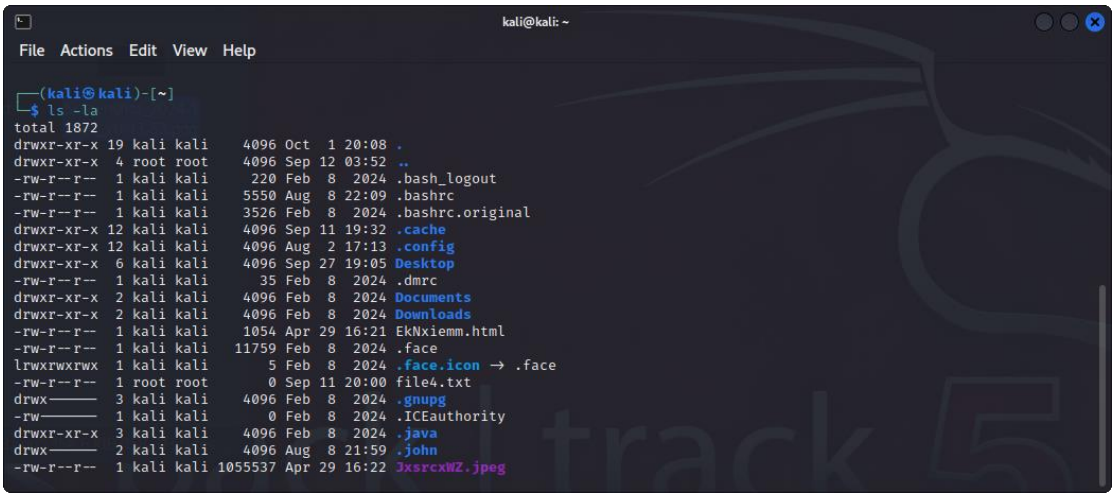
SECTION 1: FILE AND DIRECTORY MANAGEMENT

1. Display the current working directory.

2. List all the contents of your current directory, including hidden files



3. Change your directory to the `Desktop`.

4. Create two directories named `dir1` and `dir2` on the Desktop

5. Inside `dir1`, create a file named `file1.txt`.

6. Inside `dir2`, create a file named `file2.txt`.

7. Using nano or vim Write the numbers 1 to 9 into `file1.txt`.

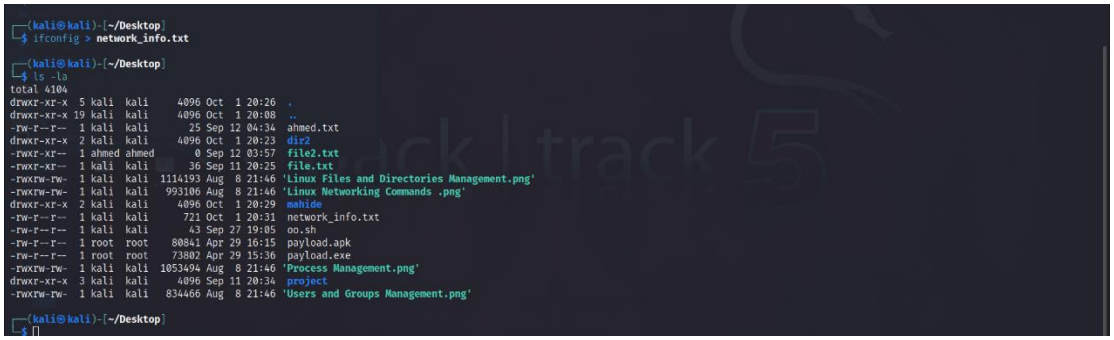
8. From the home directory Copy the contents of `file1.txt` into `file2.txt`.

9. From the home directory, delete `file1.txt` inside `dir1`.

10. Remove the directory `dir1` from the Desktop.

11. Redirect the output of the network configuration command to a file named `network_info.txt` on the Desktop.

12. Open the Desktop folder and show all files with detailed information.



Section 2: Users and Groups Management

13. Create a new user with your name.

14. Set a password for your user.

15. Open the file that contains user information and verify that your user has been added.

16. Add your user to the file that gives administrative privileges.

17. Switch to your user and confirm the user identity.

18. Create a new group named `testgroup`.

19. Add your user to `testgroup`.

20. Add the group `testgroup` to the file that gives administrative privileges.

21. Remove your user from the file that gives administrative privileges.

SECTION 3: PERMISSIONS AND OWNERSHIP

24. Set the permissions of `file2.txt` on the Desktop to allow the owner to read, write, and execute; the group to read and execute; and others to read .

25. Check the permissions of `file2.txt` to verify the change.

26. Change the ownership of `file2.txt` to your user.

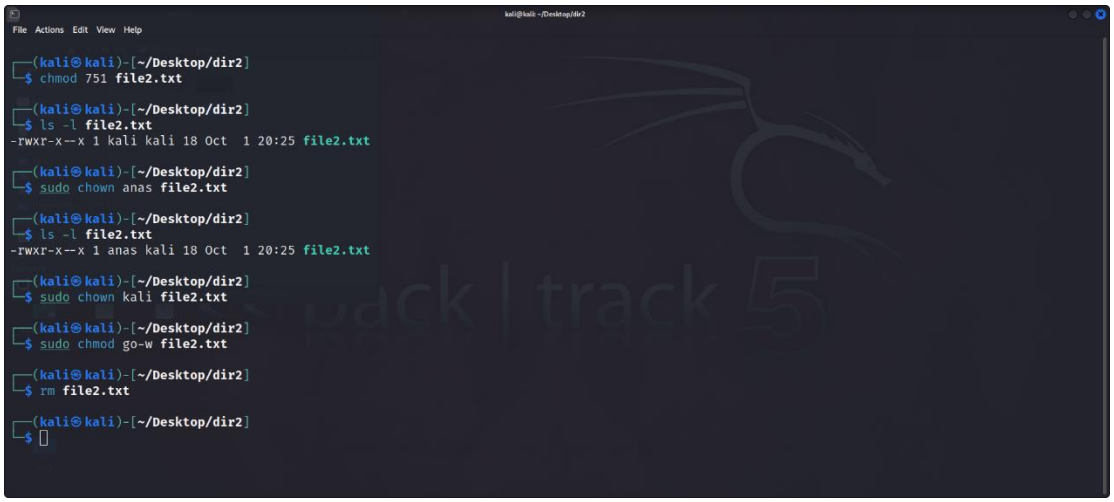
27. verify the ownership of `file2.txt`.

28. Change back the ownership of a file `file2.txt`

29. Grant write permission to everyone for `file2.txt`

30. Remove the write permission for the group and others for `file2.txt`.

31. Delete `file2.txt` after making the necessary ownership and permission changes.



32. What command would you use to recursively change the permissions of all files and directories inside a folder named `project` to `755`.

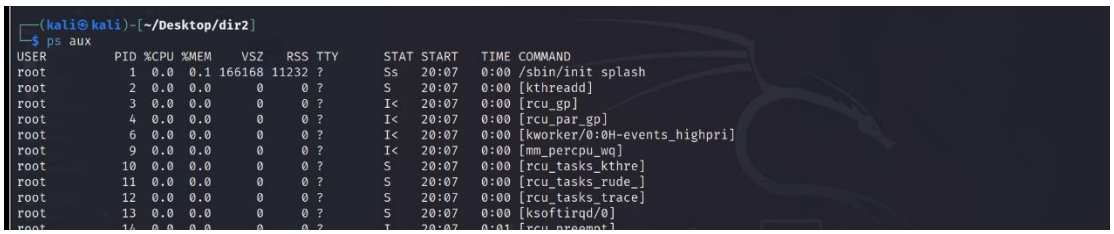
chmod -R 755 project/

SECTION 4: PROCESS MANAGEMENT

33. Install a system monitor tool that provides an interactive process viewer(htop).

```
sudo apt install htop
```

34. Display all running processes.



35. Display a tree of all running processes.

36. Open the interactive process viewer and identify a process by its PID.

```
htop
```

37. Kill a process with a specific PID.

38. Start an application and stop it using a command that kills processes by name(exeyes). 39. Restart the application, then stop it using the interactive process viewer.

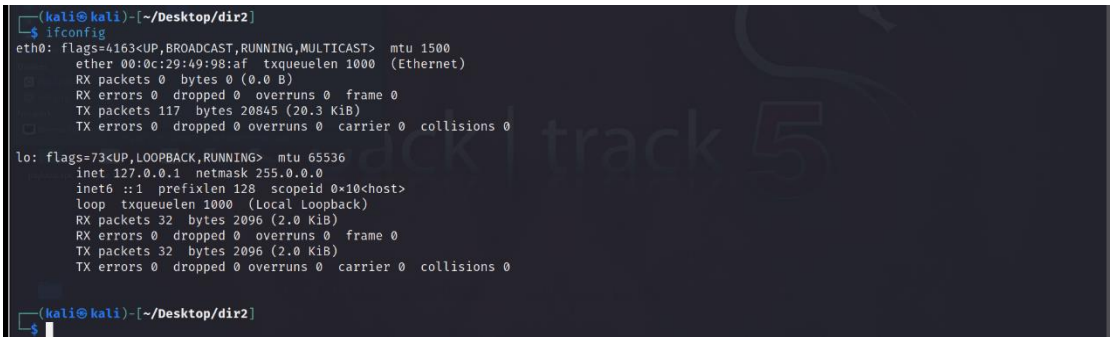
40. Run a command in the background, then bring it to the foreground(exeyes).

41. Check how long the system has been running.

42. List all jobs running in the background.

SECTION 5: NETWORKING COMMANDS

43. Display the network configuration.



45. Test connectivity to an external server.

ping -c 4 google.com

46. Display the routing table.

47. Check the open ports and active connections.

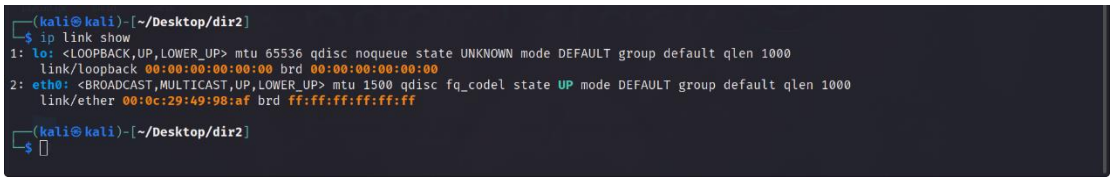
49. Trace the route to an external server.

traceroute google.com

50. Find out the default gateway.

ip route | grep default

51. Check the MAC address of your network interface.



52. Ensure that the VM can access external networks.

ping

SECTION 6: UFW FIREWALL

---

53. Enable the firewall.

sudo ufw enable

54. Allow SSH connections through the firewall.

sudo ufw allow ssh

55. Deny all incoming traffic by default.

```
sudo ufw default deny incoming
```

56. Allow HTTP and HTTPS traffic.

```
sudo ufw allow http
sudo ufw allow https
```

57. Allow port 20

```
sudo ufw allow 20
```

58. Reset the firewall settings.

```
sudo ufw reset
```

59. Delete a rule from the firewall.

```
sudo u fw delete allow ssh
```

60. Disable the firewall.

```
sudo ufw disable
```

61. View the status of the firewall.

```
sudo ufw status
```

62. Log firewall activity and view it.

```
sudo ufw logging on
cat /var/log/ufw.log
```

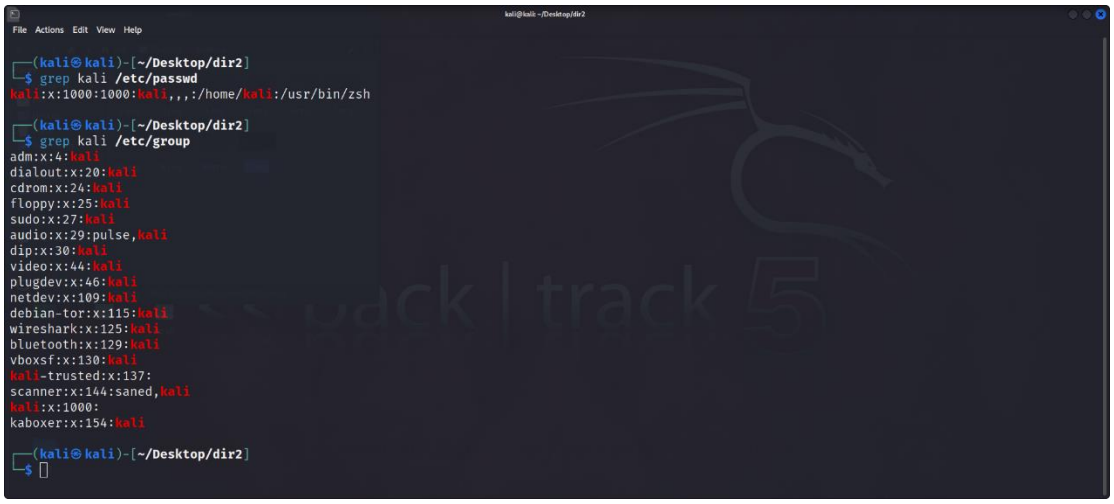
Section 7: Searching and System Information

63. Delete the command history.

```
history -c
```

64. Search for a kali in the `/etc/passwd` file.

65. Search for a kali in the `/etc/group` file.



66. Locate the `passwd` file.

67. Locate the shadow file and open it.

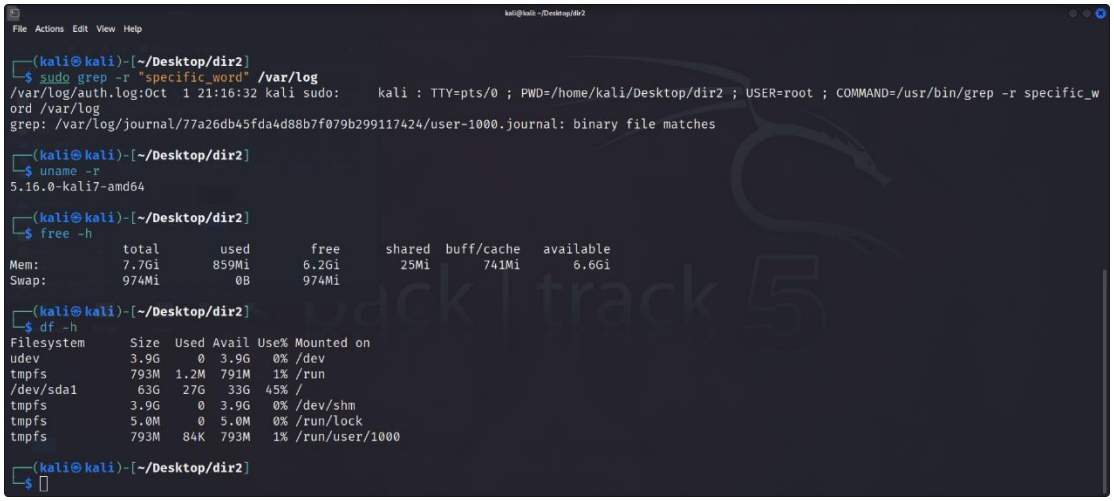
68. Search for all configuration files in the `/etc` directory.

69. Search recursively for a specific word in the `/var/log` directory.

70. View the system's kernel version.

71. Display the system's memory usage.

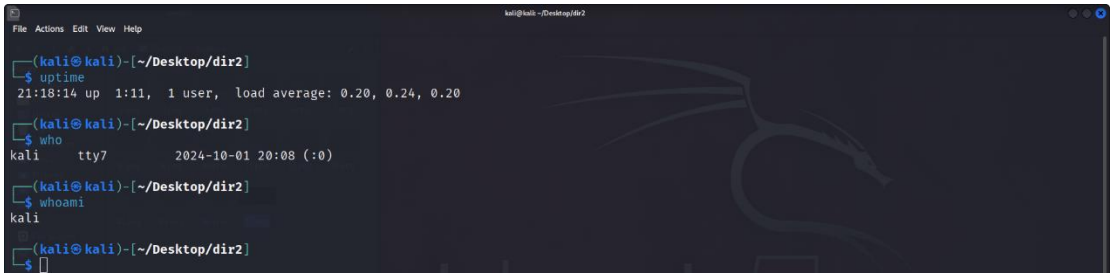
72. Show the system's disk usage.



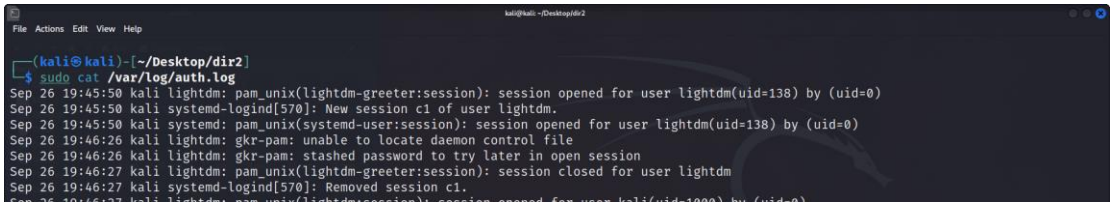
73. Check the system's uptime and load average.

74. Display the current logged-in users.

75. Check the identity of the current user.



76. View the `/var/log/auth.log` file.



77. Shred the `auth.log` file securely.

78. How do you lock a user account to prevent them from logging in.

79. What command would you use to change a user's default shell.

chsh -s /bin/bash username

80. Display the system's boot messages.