Section 1: File and Directory Management

1. Display the current working directory.

pwd

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

ls -la

3. Change your directory to the `Desktop`.

cd ~/Desktop

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

mkdir dir1 dir2

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

touch dir1/file1.txt

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

touch dir2/file2.txt

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

nano dir1/file1.txt

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

cp dir1/file1.txt dir2/file2.txt

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

rm dir1/file1.txt

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

rmdir dir1

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

ifconfig > ~/Desktop/network\_info.txt

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

ls -la ~/Desktop

Section 2: Users and Groups Management

13. Create a new user with your name.

sudo adduser Ahmed

14. Set a password for your user.

passwd Ahmed

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

cat /etc/passwd | grep Ahmed

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

sudo usermod -aG sudo Ahmed

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

su – Ahmed

18. Create a new group named `testgroup`.

sudo groupadd testgroup

19. Add your user to `testgroup`.

sudo usermod -aG testgroup Ahmed

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

sudo usermod -aG sudo testgroup

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

sudo deluser Ahmed sudo

22. Check if your user still have administrative privileges.

groups Ahmed

23. Check which groups your user belongs to.

groups

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 .

chmod 751 ~/Desktop/dir2/file2.txt

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

ls -l ~/Desktop/dir2/file2.txt

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

sudo chown Ahmed~/Desktop/dir2/file2.txt

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

ls -l ~/Desktop/dir2/file2.txt

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

sudo chown root ~/Desktop/dir2/file2.txt

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

chmod a+w ~/Desktop/dir2/file2.txt

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

chmod go-w ~/Desktop/dir2/file2.txt

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

rm ~/Desktop/dir2/file2.txt

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.

ps aux

35. Display a tree of all running processes.

pstree

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

htop

37. Kill a process with a specific PID.

kill <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.

exeyes & # Start the application

pkill exeyes # Stop it

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

exeyes & # Run in the background

fg # Bring to foreground

41. Check how long the system has been running.

uptime

42. List all jobs running in the background.

jobs

Section 5: Networking Commands

43. Display the network configuration.

ifconfig

44. Check the IP address of your machine.

hostname -I

45. Test connectivity to an external server.

ping -c 4 google.com

46. Display the routing table.

route -n

47. Check the open ports and active connections.

netstat -tuln

48. Show the IP address of the host machine and the VM, and verify if they are on the same network.

ifconfig # Check your IPs

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.

ip link show

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.

grep kali /etc/passwd

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

grep kali /etc/group

66. Locate the `passwd` file.

locate passwd

67. Locate the shadow file and open it.

locate shadow

sudo cat /etc/shadow

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

find /etc -type f -name "\*.conf "

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

grep -r "specific\_word" /var/log

70. View the system’s kernel version.

uname -r

71. Display the system’s memory usage.

free -h

72. Show the system’s disk usage.

df -h

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

uptime

74. Display the current logged-in users.

who

75. Check the identity of the current user.

whoami

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

cat /var/log/auth.log

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

sudo shred -u /var/log/auth.log

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

sudo passwd -l username

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.

dmesg