**----------------------------------------------------------------------**

Section 1: File and Directory Management

1. \*\*Display the current working directory:\*\*

```bash

Pwd

```

1. \*\*List all the contents of your current directory, including hidden files:\*\*

```bash

Ls -a

```

1. \*\*Change your directory to the `Desktop`:\*\*

```bash

Cd ~/Desktop

```

1. \*\*Create two directories named `dir1` and `dir2` on the Desktop:\*\*

```bash

Mkdir dir1 dir2

```

1. \*\*Inside `dir1`, create a file named `file1.txt`:\*\*

```bash

Touch dir1/file1.txt

```

1. \*\*Inside `dir2`, create a file named `file2.txt`:\*\*

```bash

Touch dir2/file2.txt

```

1. \*\*Using nano or vim, write the numbers 1 to 9 Into `file1.txt`:\*\*

```bash

Nano dir1/file1.txt

```

(ثم اكتب الأرقام واحفظ الملف.)

1. \*\*From the home directory, copy the contents of `file1.txt` Into `file2.txt`:\*\*

```bash

Cp dir1/file1.txt dir2/file2.txt

```

1. \*\*From the home directory, delete `file1.txt` Inside `dir1`:\*\*

```bash

Rm dir1/file1.txt

```

1. \*\*Remove the directory `dir1` from the Desktop:\*\*

```bash

Rmdir dir1

```

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

```bash

Ifconfig > ~/Desktop/network\_info.txt

```

### Section 2: Users and Groups Management

1. \*\*Create a new user with your name:\*\*

```bash

Sudo adduser yourname

```

1. \*\*Set a password for your user:\*\*

```bash

Sudo passwd yourname

```

1. \*\*Open the file that contains user information:\*\*

```bash

Cat /etc/passwd

```

1. \*\*Add your user to the file that gives administrative privileges:\*\*

```bash

Sudo usermod -aG sudo yourname

```

1. \*\*Create a new group named `testgroup`:\*\*

```bash

Sudo groupadd testgroup

```

1. \*\*Add your user to `testgroup`:\*\*

```bash

Sudo usermod -aG testgroup yourname

```

1. \*\*Remove your user from the file that gives administrative privileges:\*\*

```bash

Sudo deluser yourname sudo

```

1. \*\*Check if your user still has administrative privileges:\*\*

```bash

Groups yourname

```

1. \*\*Check which groups your user belongs to:\*\*

```bash

Groups yourname

```

### Section 3: Permissions and Ownership

1. \*\*Set the permissions of `file2.txt` to allow the owner to read, write, and execute; the group to read and execute; and others to read:\*\*

```bash

Chmod 755 dir2/file2.txt

```

1. \*\*Check the permissions of `file2.txt`:\*\*

```bash

Ls -l dir2/file2.txt

```

1. \*\*Change the ownership of `file2.txt` to your user:\*\*

```bash

Sudo chown yourname:yourname dir2/file2.txt

```

1. \*\*Verify the ownership of `file2.txt`:\*\*

```bash

Ls -l dir2/file2.txt

```

1. \*\*Change back the ownership of a file `file2.txt`:\*\*

```bash

Sudo chown previous\_owner:previous\_group dir2/file2.txt

```

1. \*\*Grant write permission to everyone for `file2.txt`:\*\*

```bash

Chmod a+w dir2/file2.txt

```

1. \*\*Remove the write permission for the group and others for `file2.txt`:\*\*

```bash

Chmod go-w dir2/file2.txt

```

1. \*\*Delete `file2.txt` after making the necessary ownership and permission changes:\*\*

```bash

Rm dir2/file2.txt

```

1. \*\*Change the permissions of all files and directories Inside a folder named `project` to `755`:\*\*

```bash

Chmod -R 755 project/

```

### Section 4: Process Management

1. \*\*Install a system monitor tool that provides an interactive process viewer (htop):\*\*

```bash

Sudo apt install htop

```

1. \*\*Display all running processes:\*\*

```bash

Ps aux

```

1. \*\*Display a tree of all running processes:\*\*

```bash

Pstree

```

1. \*\*Open the interactive process viewer and Identify a process by Its PID:\*\*

```bash

Htop

```

1. \*\*Kill a process with a specific PID:\*\*

```bash

Kill PID\_NUMBER

```

1. \*\*Start an application and stop It using a command that kills processes by name:\*\*

```bash

Pkill application\_name

```

1. \*\*Restart the application, then stop It using the Interactive process viewer:\*\*

(قم بتشغيل التطبيق ثم استخدم `htop` لايقافه.)

1. \*\*Run a command in the background, then bring It to the foreground:\*\*

```bash

Command &

Fg

```

1. \*\*Check how long the system has been running:\*\*

```bash

Uptime

```

1. \*\*List all jobs running In the background:\*\*

```bash

Jobs

```

### Section 5: Networking Commands

1. \*\*Display the network configuration:\*\*

```bash

Ifconfig

```

1. \*\*Check the IP address of your machine:\*\*

```bash

Hostname -I

```

1. \*\*Test connectivity to an external server:\*\*

```bash

Ping external\_server\_ip\_or\_domain

```

1. \*\*Display the routing table:\*\*

```bash

Route -n

```

1. \*\*Check the open ports and active connections:\*\*

```bash

Netstat -tuln

```

1. \*\*Show the IP address of the host machine and the VM:\*\*

```bash

Ifconfig

```

1. \*\*Trace the route to an external server:\*\*

```bash

Traceroute external\_server\_ip\_or\_domain

```

1. \*\*Find the default gateway:\*\*

```bash

Ip route | grep default

```

1. \*\*Check the MAC address of your network Interface:\*\*

```bash

Ip link show

```

### Section 6: UFW Firewall

53. \*\*Enable the firewall:\*\*

```bash

Sudo ufw enable

```

54. \*\*Allow SSH connections through the firewall:\*\*

```bash

Sudo ufw allow ssh

```

55. \*\*Deny all incoming traffic by default:\*\*

```bash

Sudo ufw default deny incoming

```

56. \*\*Allow HTTP and HTTPS traffic:\*\*

```bash

Sudo ufw allow http

Sudo ufw allow https

```

57. \*\*Allow port 20:\*\*

```bash

Sudo ufw allow 20

```

58. \*\*Reset the firewall settings:\*\*

```bash

Sudo ufw reset

```

59. \*\*Delete a rule from the firewall:\*\*

```bash

Sudo ufw delete allow http

```

60. \*\*Disable the firewall:\*\*

```bash

Sudo ufw disable

```

61. \*\*View the status of the firewall:\*\*

```bash

Sudo ufw status

```

62. \*\*Log firewall activity and view It:\*\*

```bash

Sudo ufw logging on

Sudo less /var/log/ufw.log

```

### Section 7: Searching and System Information

63. \*\*Delete the command history:\*\*

```bash

History -c

```

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

```bash

Grep "kali" /etc/passwd

```

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

```bash

Grep "kali" /etc/group

```

66. \*\*Locate the `passwd` file:\*\*

```bash

Locate passwd

```

67. \*\*Locate the shadow file and open it:\*\*

```bash

Sudo less /etc/shadow

```

68. \*\*Search for all configuration files In the `/etc` directory:\*\*

```bash

Ls /etc/\*.conf

```

69. \*\*Search recursively for a specific word In the `/var/log` directory:\*\*

```bash

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

```

70. \*\*View the system’s kernel version:\*\*

```bash

Uname -r

```

71. \*\*Display the system’s memory usage:\*\*

```bash

Free -h

```