# Section 1: File and Directory Management

1. Display the current working directory.

The answer is: pwd.

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

The answer is: ls -a.

1. Change your directory to the `Desktop`.

The answer is: cd Desktop.

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

The answer is: mkdir dir1 dir2.

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

The answer is: touch dir1/file1.txt.

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

The answer is: touch dir2/file2.txt.

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

The answer is: nano dir1/file1.txt.

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

The answer is: cp ~/Desktop/dir1/file1.txt ~/Desktop/dir2/file2.txt.

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

The answer is: rm ~/Desktop/dir1/file1.txt.

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

The answer is: rmdir ~/Desktop/dir1.

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

The answer is: ifconfig > ~/Desktop/network\_info.txt.

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

The answer is: ls -l ~/Desktop.

# Section 2: Users and Groups Management

1. Create a new user with your name.

The answer is: sudo adduser your\_username.

1. Set a password for your user.

The answer is: sudo passwd your\_username.

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

The answer is: cat /etc/passwd | grep your\_username.

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

The answer is: sudo usermod -aG sudo your\_username.

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

The answer is: su - your\_username whoami.

1. Create a new group named `testgroup`.

The answer is: sudo groupadd testgroup.

1. Add your user to `testgroup`.

The answer is: sudo usermod -aG testgroup your\_username.

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

The answer is: sudo usermod -aG sudo testgroup.

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

The answer is: sudo deluser your\_username sudo.

1. Check if your user still have administrative privileges.

The answer is: sudo -l.

1. Check which groups your user belongs to.

The answer is: groups your\_username.

# Section 3: Permissions and Ownership

1. 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 .

The answer is: chmod 755 ~/Desktop/dir2/file2.txt.

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

The answer is: ls -l ~/Desktop/dir2/file2.txt.

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

The answer is: sudo chown your\_username ~/Desktop/dir2/file2.txt.

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

The answer is: ls -l ~/Desktop/dir2/file2.txt.

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

The answer is: sudo chown root ~/Desktop/dir2/file2.txt.

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

The answer is: chmod a+w ~/Desktop/dir2/file2.txt.

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

The answer is: chmod go-w ~/Desktop/dir2/file2.txt.

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

The answer is: rm ~/Desktop/dir2/file2.txt.

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

The answer is: chmod -R 755 ~/project.

# Section 4: Process Management

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

The answer is: sudo apt-get install htop.

1. Display all running processes.

The answer is: ps aux.

1. Display a tree of all running processes.

The answer is: pstree.

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

The answer is: htop.

1. Kill a process with a specific PID.

The answer is: kill PID.

1. Start an application and stop it using a command that kills processes by name(exeyes).

The answer is: pkill exeyes.

1. Restart the application, then stop it using the interactive process viewer.

The answer is: htop.

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

The answer is: exeyes & fg.

1. Check how long the system has been running.

The answer is: uptime

1. List all jobs running in the background.

The answer is: jobs.

# Section 5: Networking Commands

1. Display the network configuration.

The answer is: ifconfig.

1. Check the IP address of your machine.

The answer is: hostname -I.

1. Test connectivity to an external server.

The answer is: ping google.com.

1. Display the routing table.

The answer is: route -n.

1. Check the open ports and active connections.

The answer is: netstat -tuln.

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

The answer is: ifconfig.

1. Trace the route to an external server.

The answer is: traceroute google.com.

1. Find out the default gateway.

The answer is: ip route | grep default.

1. Check the MAC address of your network interface.

The answer is: ifconfig | grep ether.

1. Ensure that the VM can access external networks.

The answer is: ping -c 4 google.com.

# Section 6: UFW Firewall

1. Enable the firewall.

The answer is: sudo ufw enable.

1. Allow SSH connections through the firewall.

The answer is: sudo ufw allow ssh.

1. Deny all incoming traffic by default.

The answer is: sudo ufw default deny incoming.

1. Allow HTTP and HTTPS traffic.

The answer is: sudo ufw allow http , sudo ufw allow https.

1. Allow port 20 .

The answer is: sudo ufw allow 20.

1. Reset the firewall settings.

The answer is: sudo ufw reset.

1. Delete a rule from the firewall.

The answer is: sudo ufw delete allow ssh.

1. Disable the firewall.

The answer is: sudo ufw disable.

1. View the status of the firewall.

The answer is: sudo ufw status.

1. Log firewall activity and view it.

The answer is: sudo ufw logging on sudo tail -f /var/log/ufw.log.

# Section 7: Searching and System Information

1. Delete the command history.

The answer is: history -c.

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

The answer is: grep kali /etc/passwd.

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

The answer is: grep kali /etc/group.

1. Locate the `passwd` file.

The answer is: locate passwd.

1. Locate the shadow file and open it.

The answer is: locate shadow sudo cat /etc/shadow.

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

The answer is: find /etc -name "\*.conf".

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

The answer is: grep -r "specific\_word" /var/log.

1. View the system’s kernel version.

The answer is: uname -r.

1. Display the system’s memory usage.

The answer is: free -h.

1. Show the system’s disk usage.

The answer is: df -h.

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

The answer is: uptime.

1. Display the current logged-in users.

The answer is: who.

1. Check the identity of the current user.

The answer is: whoam.

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

The answer is: sudo cat /var/log/auth.log.

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

The answer is: sudo shred -u /var/log/auth.log.

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

The answer is: sudo passwd -l username.

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

The answer is: chsh -s /bin/bash username.

1. Display the system's boot messages.

The answer is: dmesg.

تم بحمد الله.