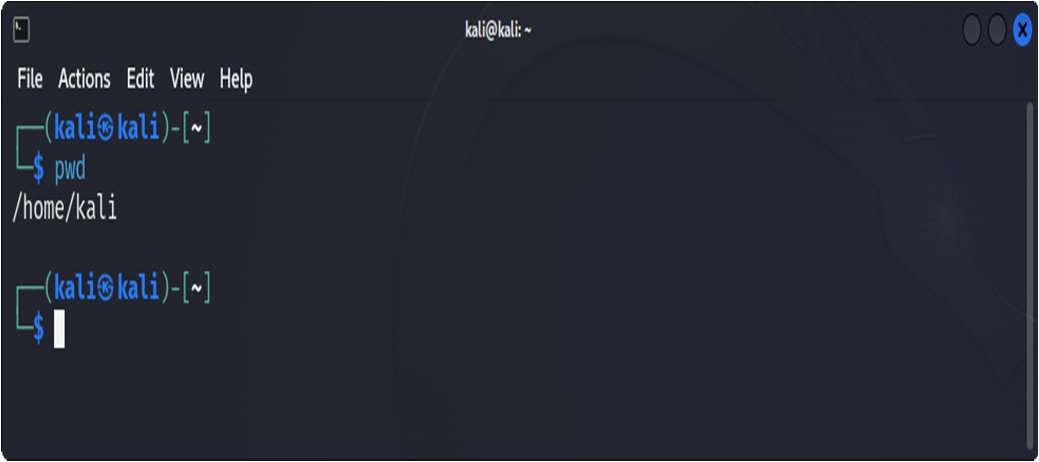
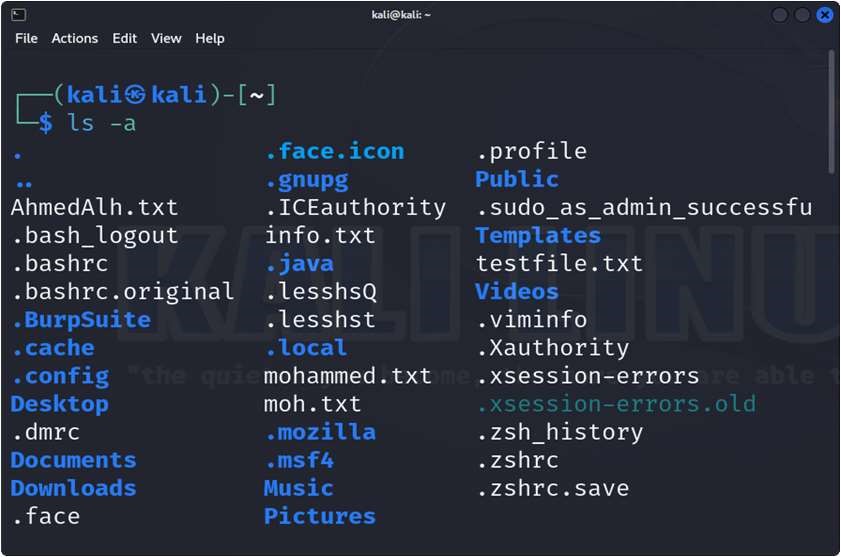
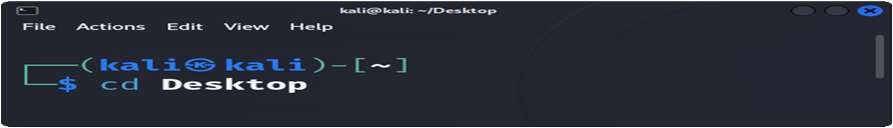
1- Display the current working directory:



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:



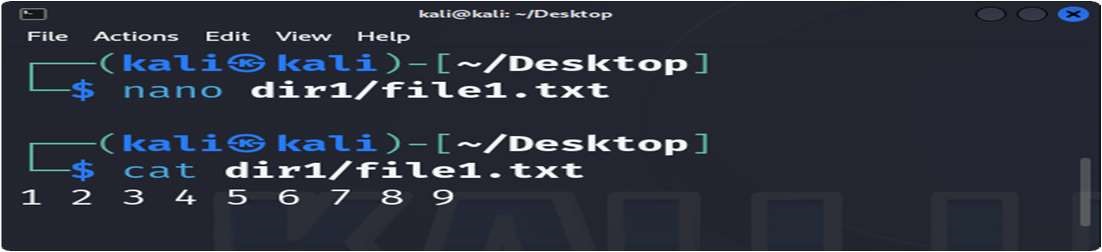
5-Inside `dir1`, create a file named `file1.txt`:



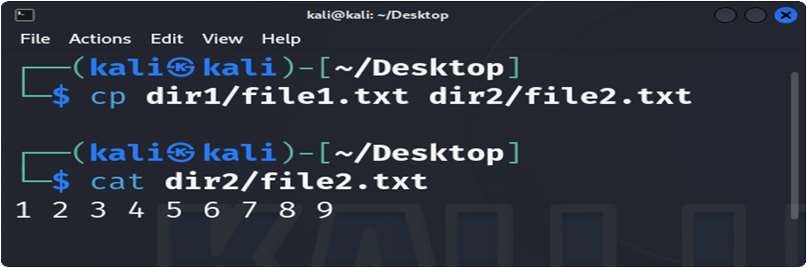
6- Inside `dir2`, create a file named `file2.txt`:



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



1. Copy the contents of `file1.txt` into `file2.txt`:



1. Delete `file1.txt` inside `dir1`:



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



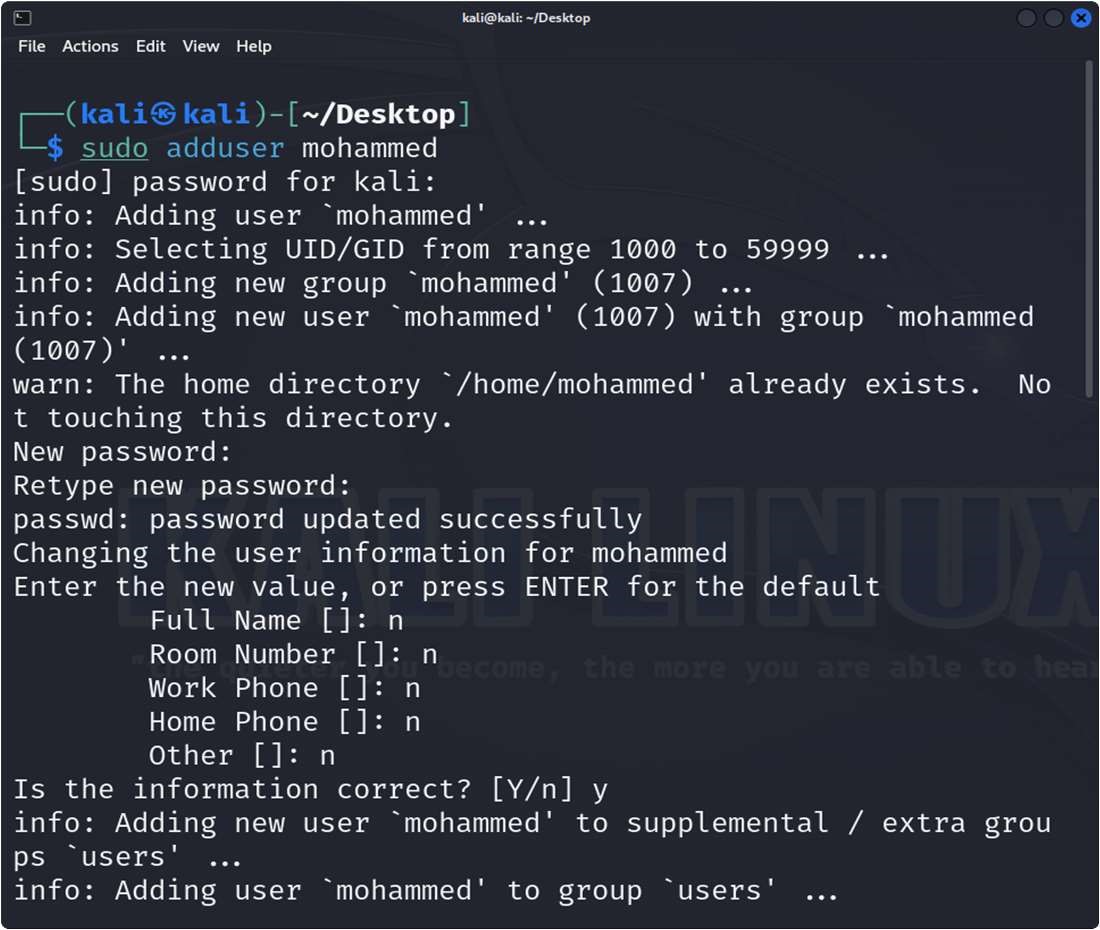
1. Redirect the output of the network configuration command to a file named `network\_info.txt` on the Desktop:



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

# 

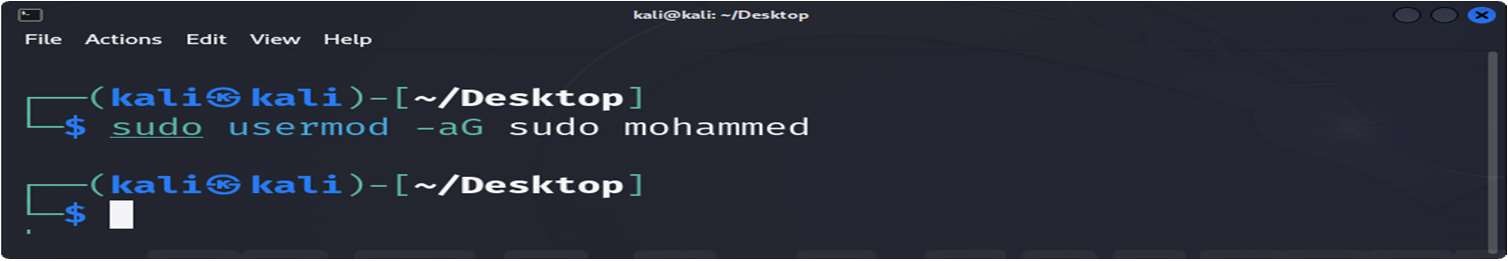
1. Create a new user with your name: 14- Set a password for your user



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



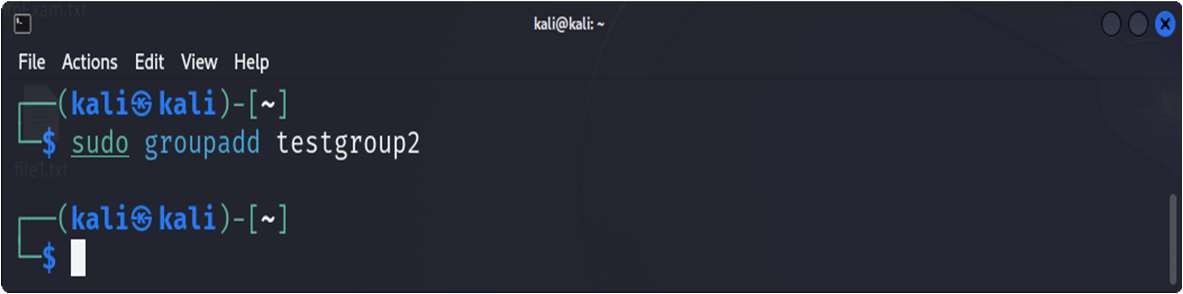
16. Add your user to the file that gives administrative privileges:



17- Switch to your user and confirm the user identity:



18. Create a new group named `testgroup`:



1. Add your user to `testgroup`:



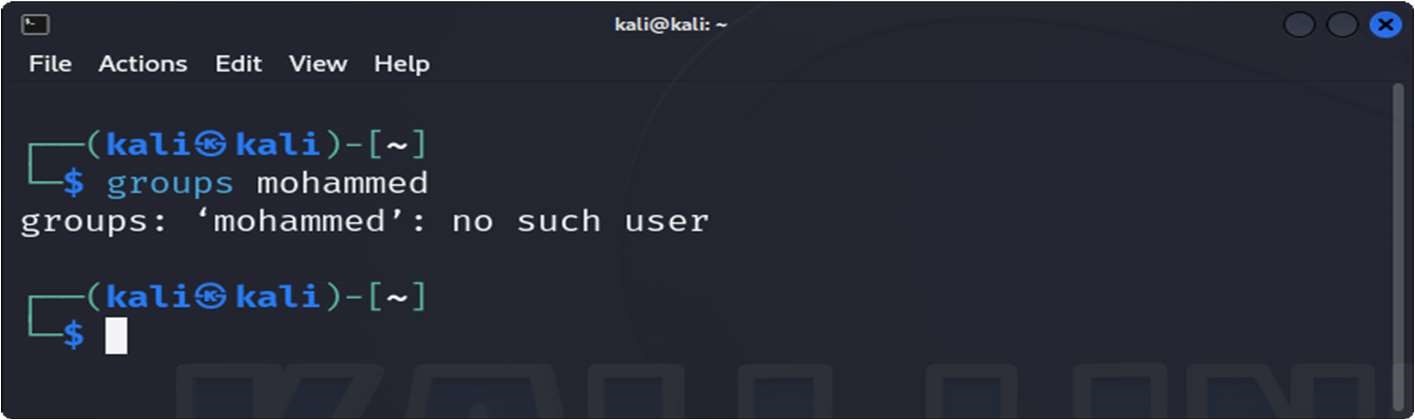
1. Add the group `testgroup` to the file that gives administrative privileges:



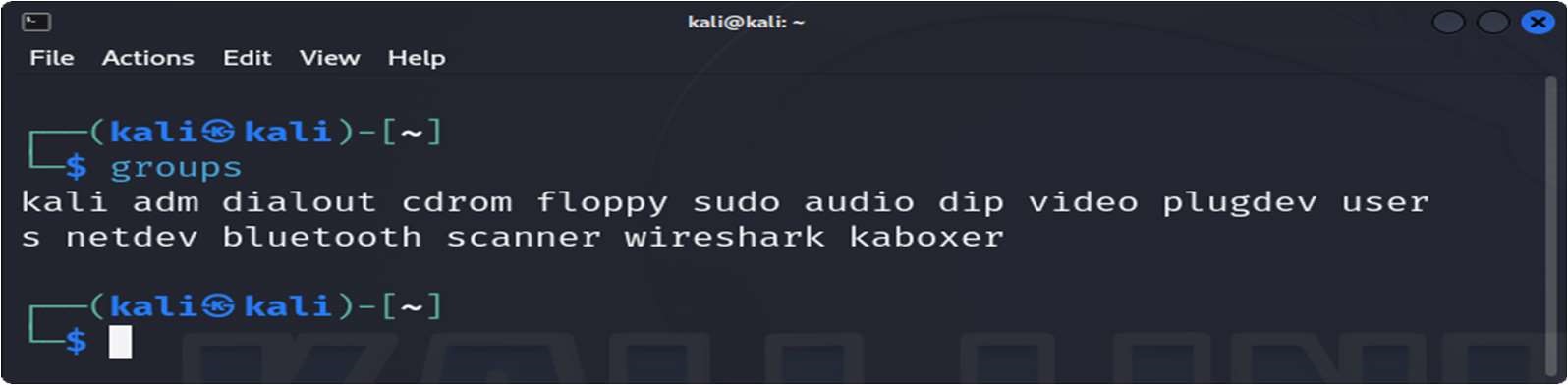
21. Remove your user from the file that gives administrative privileges:



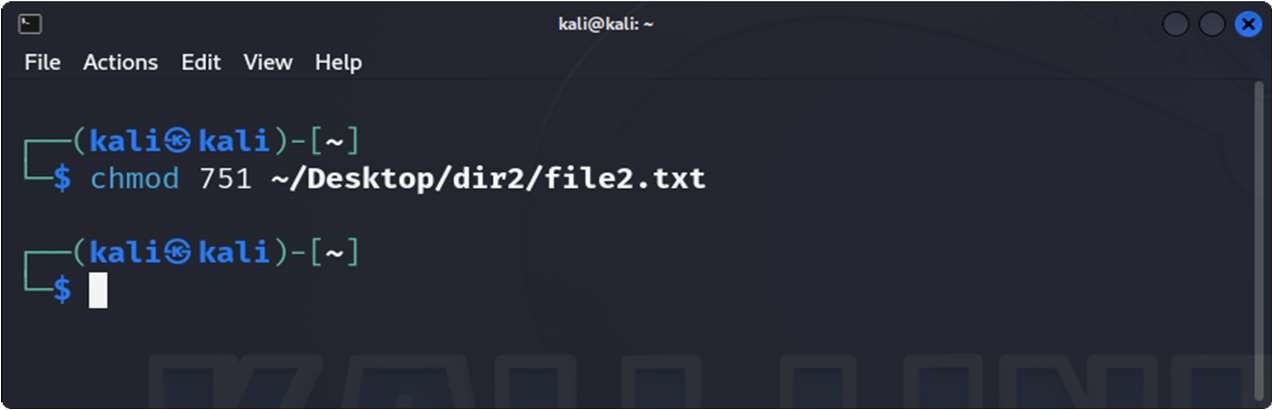
22- Check if your user still has administrative privileges:



23.-Check which groups your user belongs to:



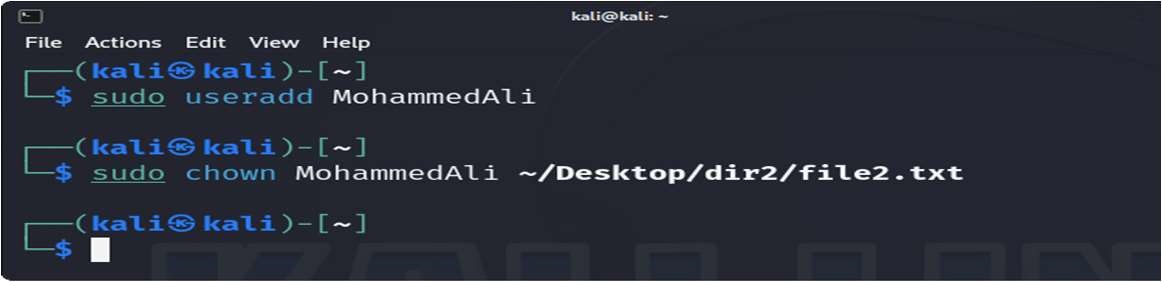
24-Set the permissions of `file2.txt`:



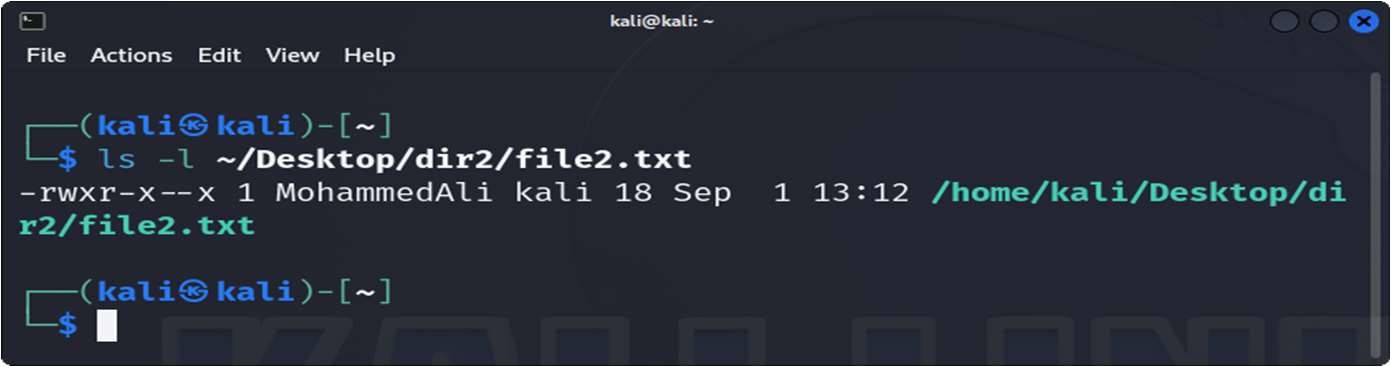
1. Check the permissions of `file2.txt`:

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

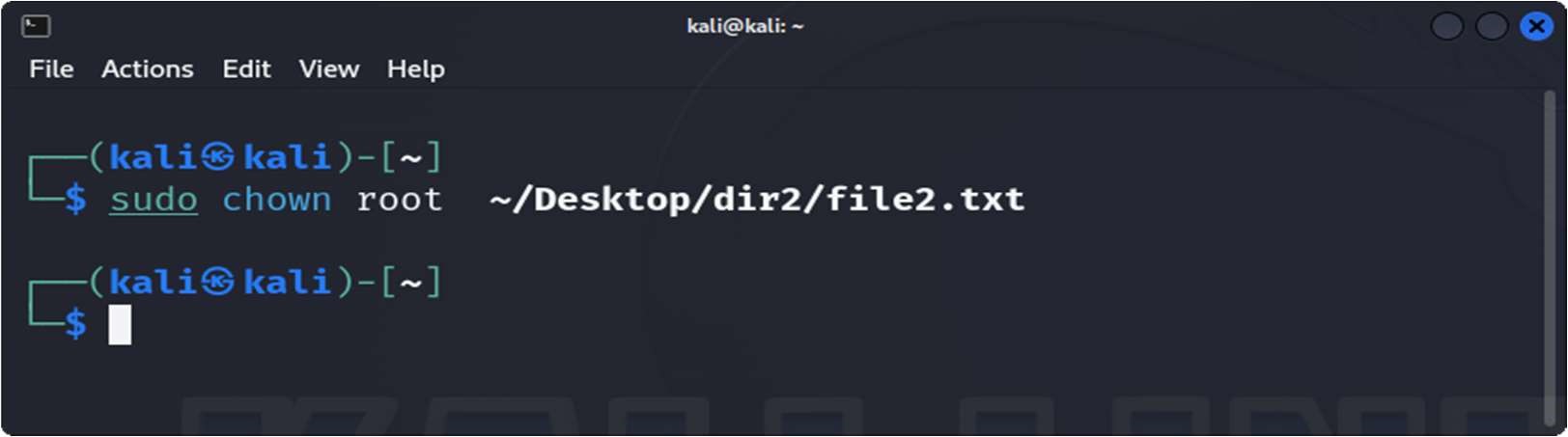
1. Change the ownership of `file2.txt` to your user:



27- Verify the ownership of `file2.txt`:



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

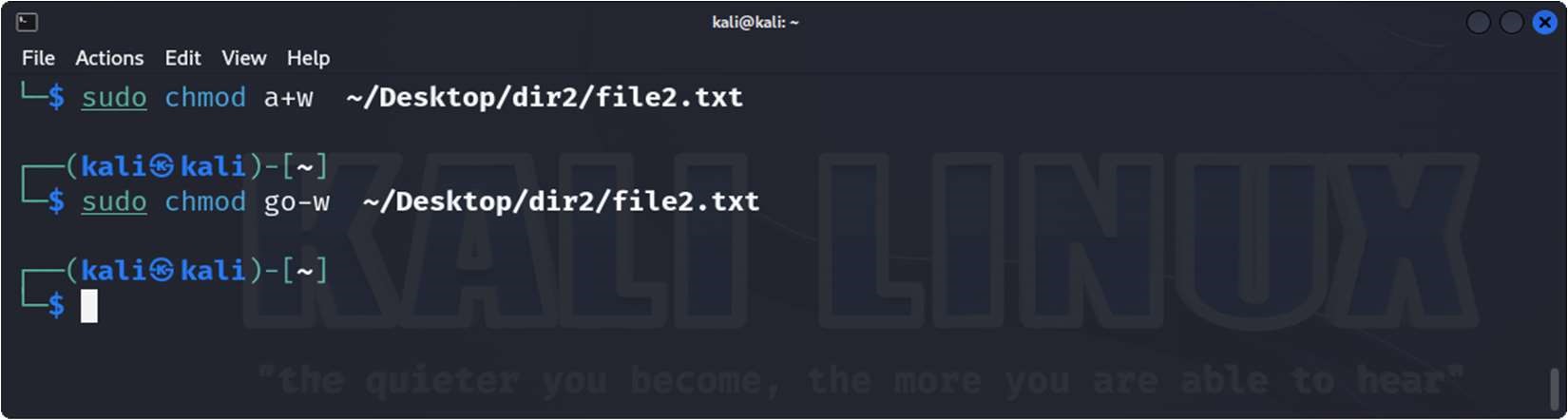


1. Grant write permission to everyone for `file2.txt`:



1. Remove the write permission for the group and others for

`file2.txt`:



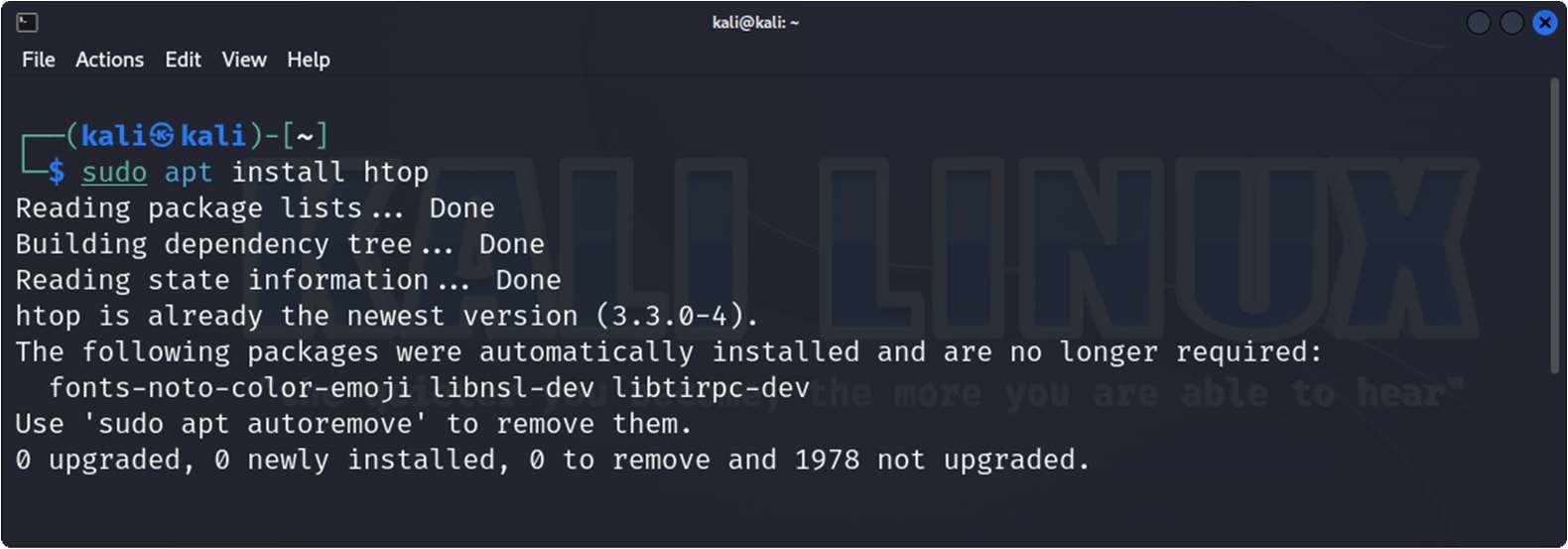
1. Delete `file2.txt` after making the necessary ownership and permission changes:



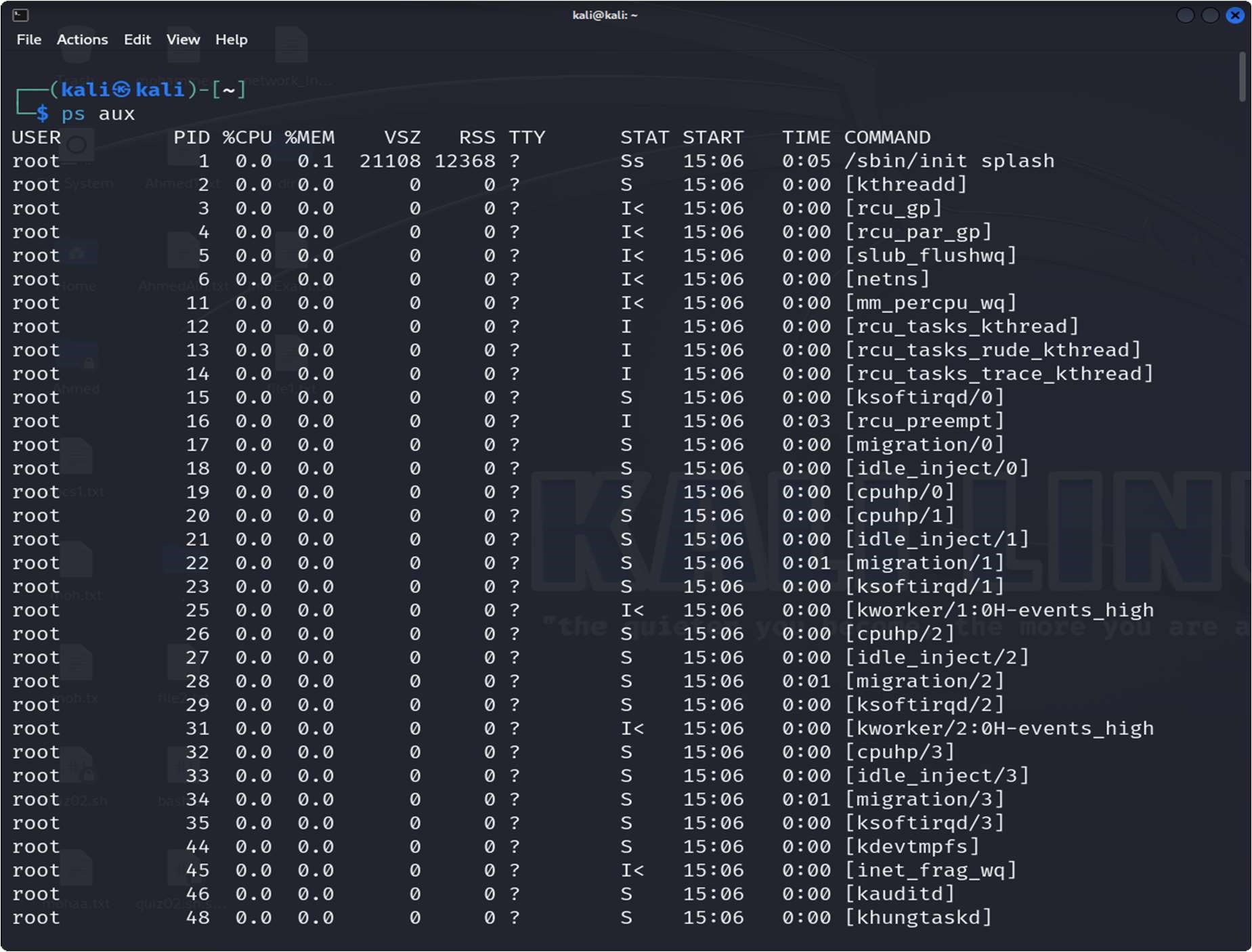
32- Command to recursively change the permissions of all files and directories inside a folder named `project` to `755`:



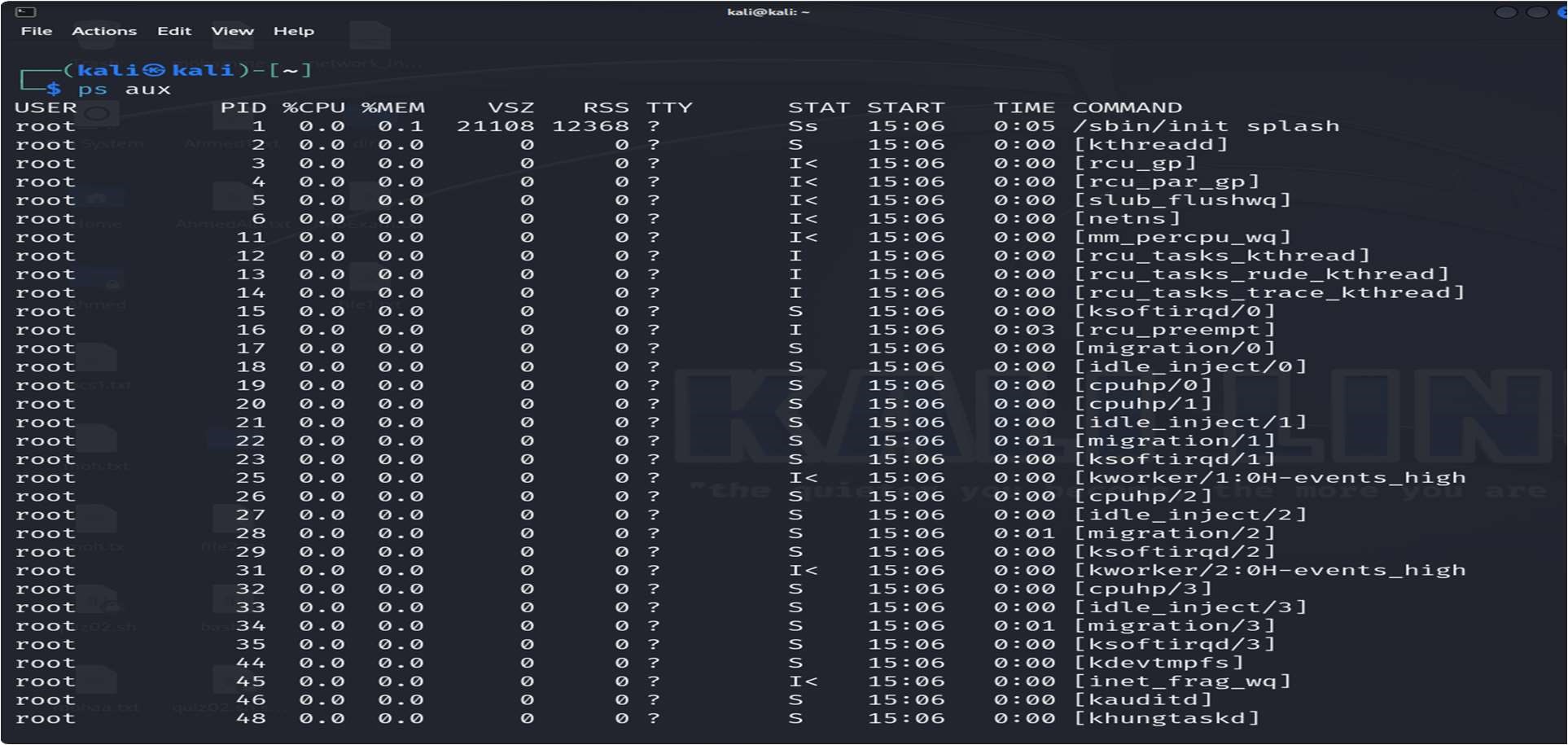
33. Install `htop`:



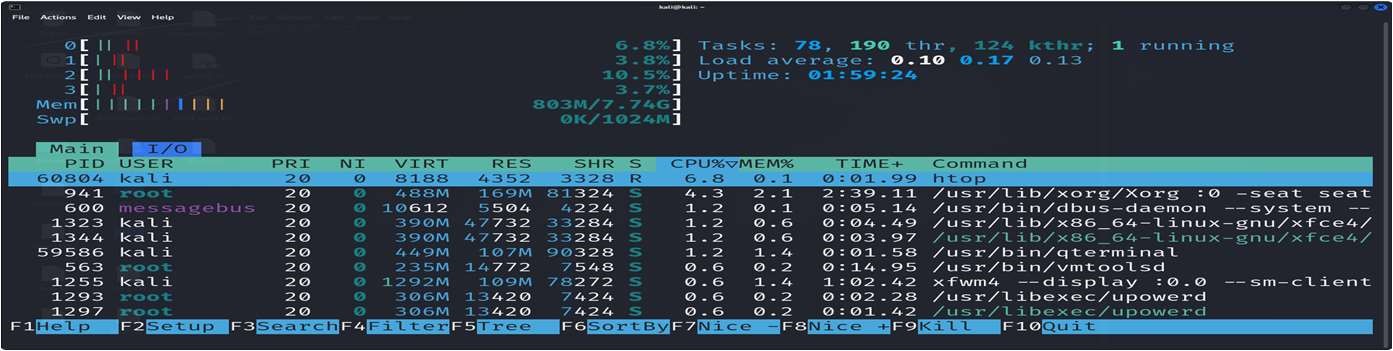
34.-Display all running processes:



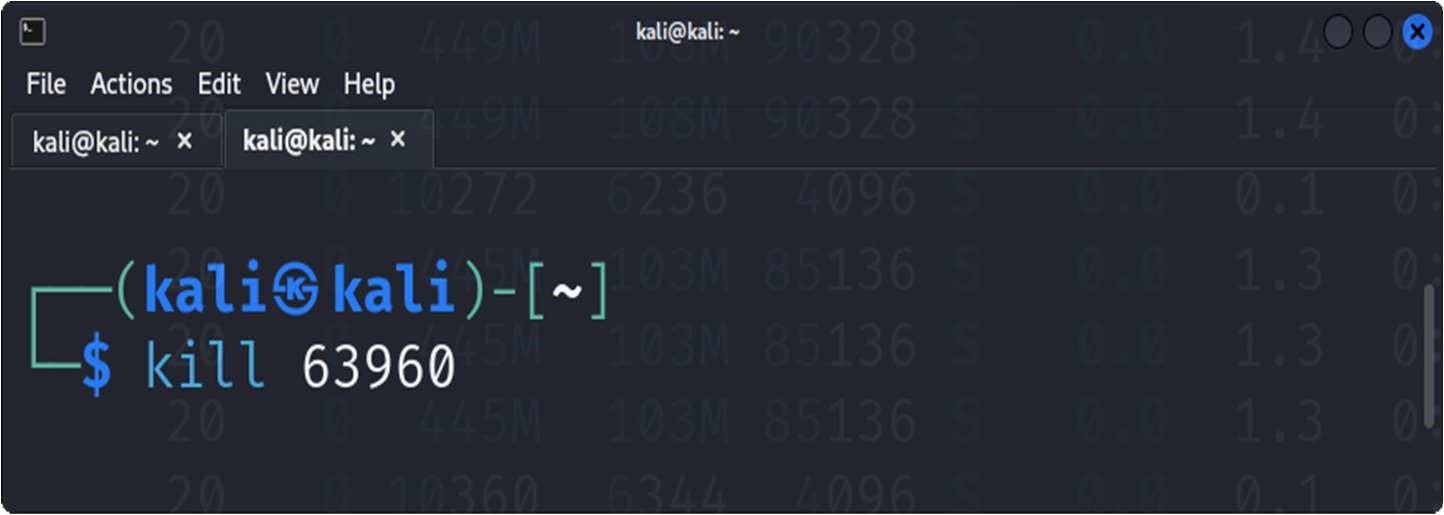
35-Display a tree of all running processes:



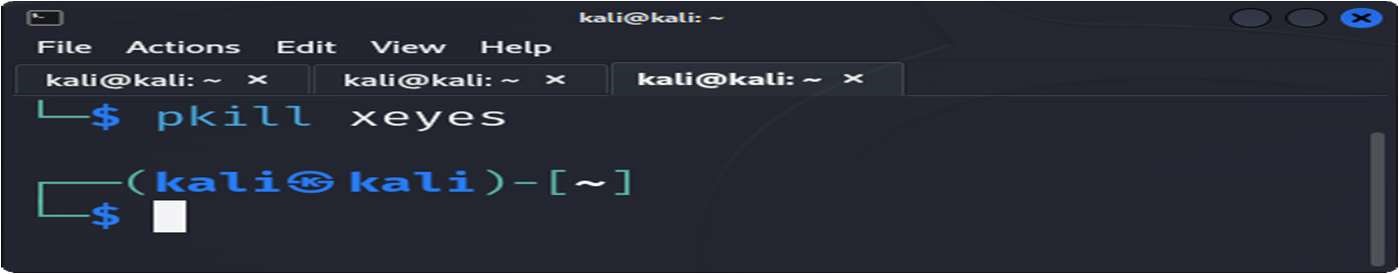
36. Open the interactive process viewer:



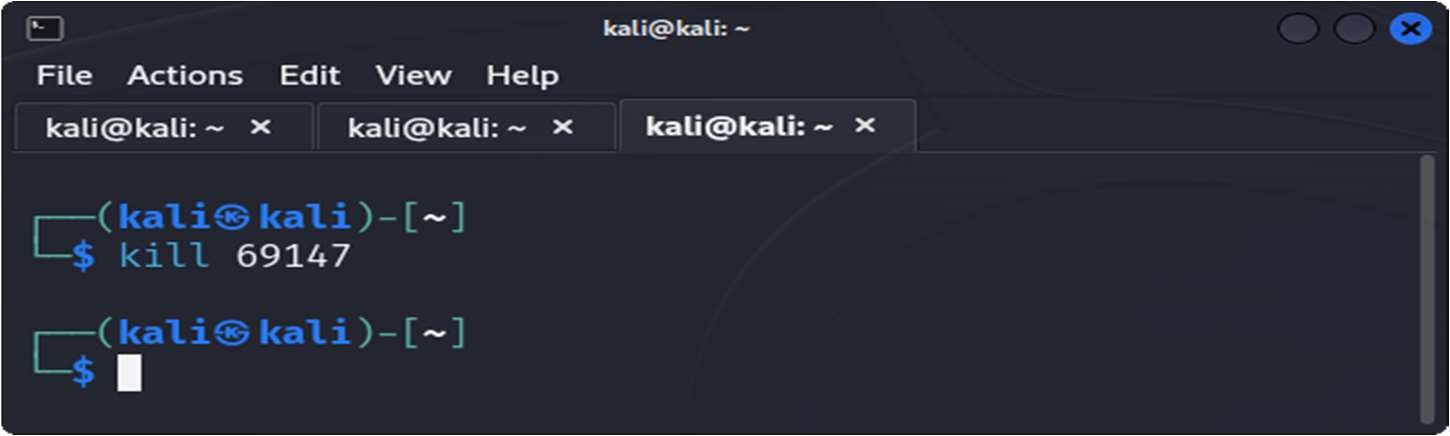
37-Kill a process with a specific PID:



38- Start an application and stop it using a command that kills processes by name:



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



1. Run a command in the background, then bring it to the foreground:



1. Check how long the system has been running:



42-List all jobs running in the background:



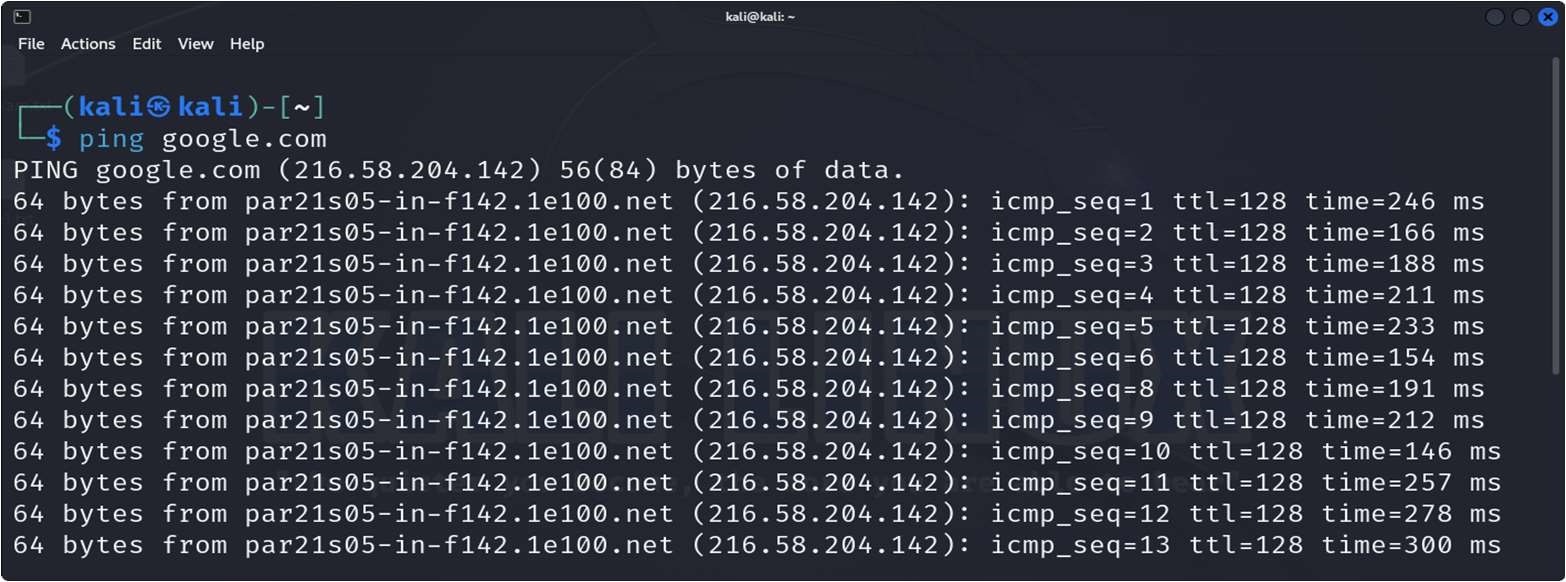
43. Display the network configuration:



44-Check the IP address of your machine:



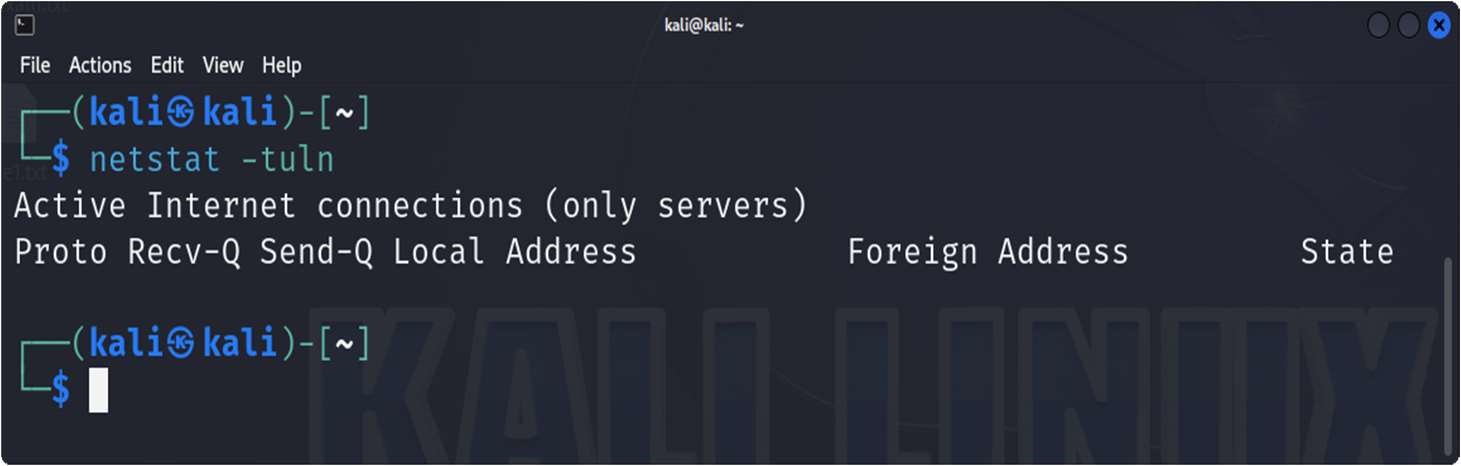
1. Test connectivity to an external server:



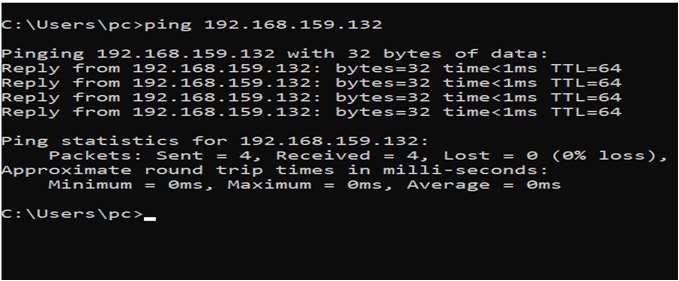
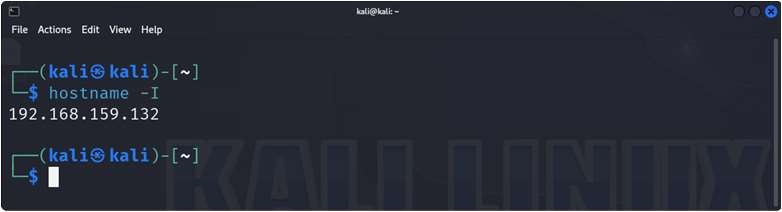
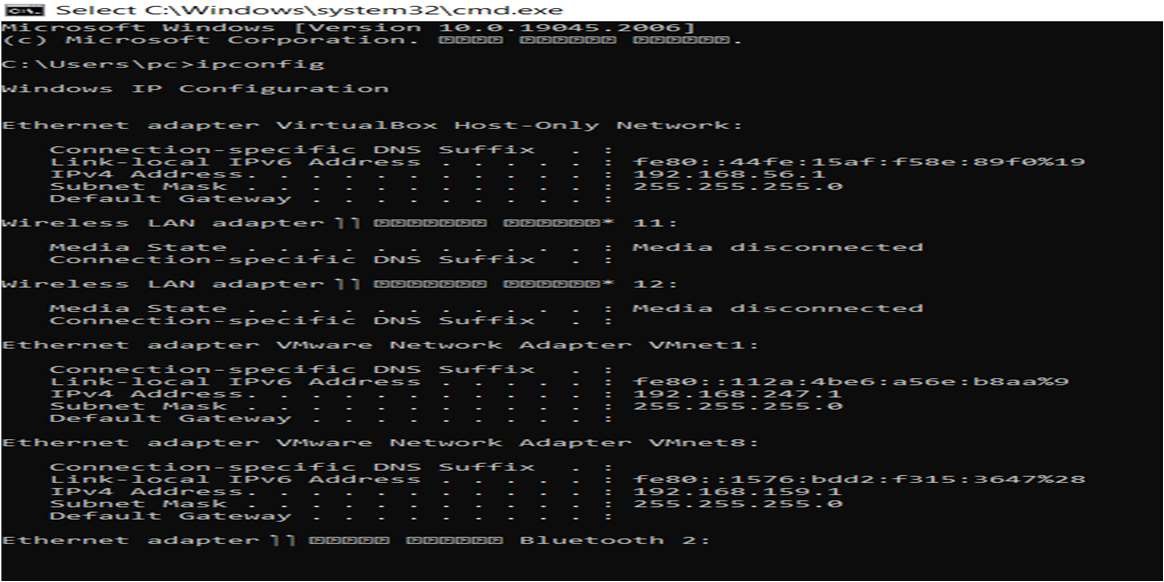
1. Display the routing table:



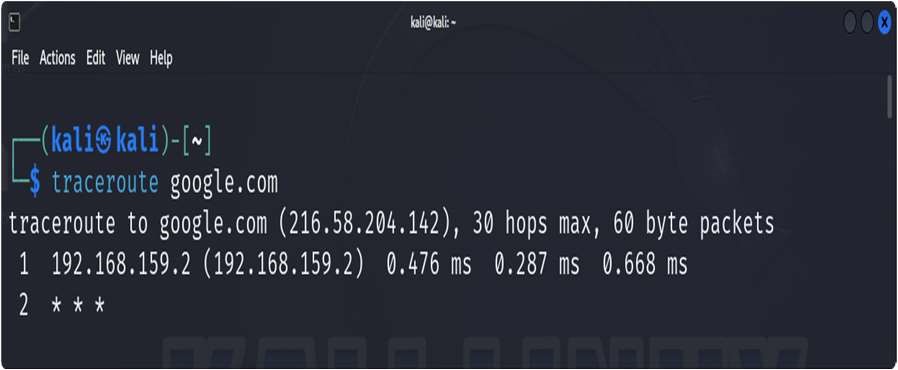
1. Check the open ports and active connections:



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



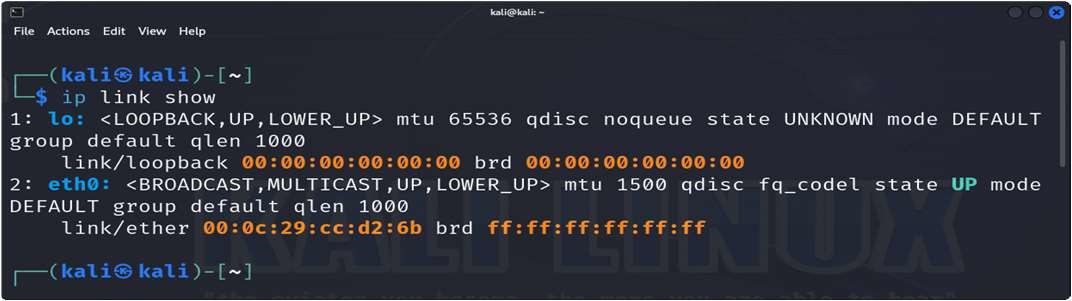
49-Trace the route to an external server:



1. Find out the default gateway:



1. Check the MAC address of your network interface:



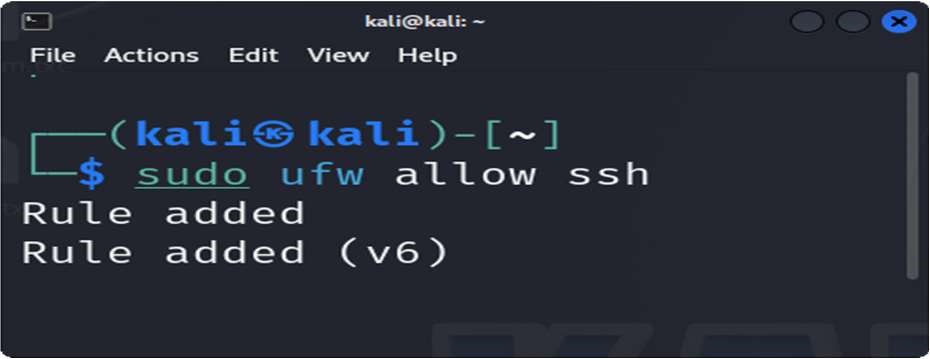
1. Ensure that the VM can access external networks:



1. Enable the firewall:



1. Allow SSH connections through the firewall:



55-Deny all incoming traffic by default:



56-Allow HTTP and HTTPS traffic:



1. Allow port 20:

1. Reset the firewall settings:



1. Delete a rule from the firewall:



1. Disable the firewall:



1. View the status of the firewall:



1. Log firewall activity and view it:



1. Delete the command history:



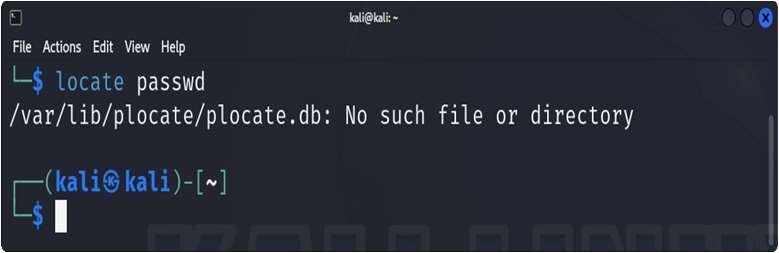
64. Search for `kali` in the `/etc/passwd` file:



65-Search for `kali` in the `/etc/group` file:



1. Locate the `passwd` file:



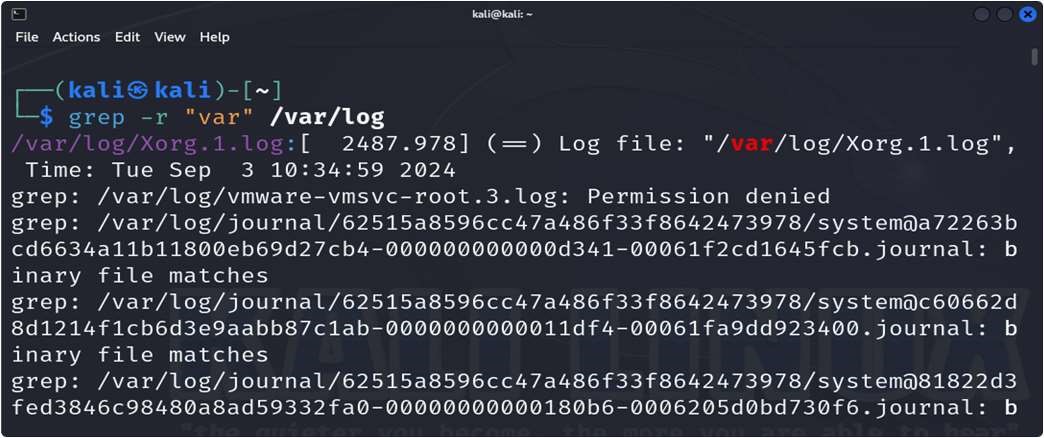
1. Locate the shadow file and open it:



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



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



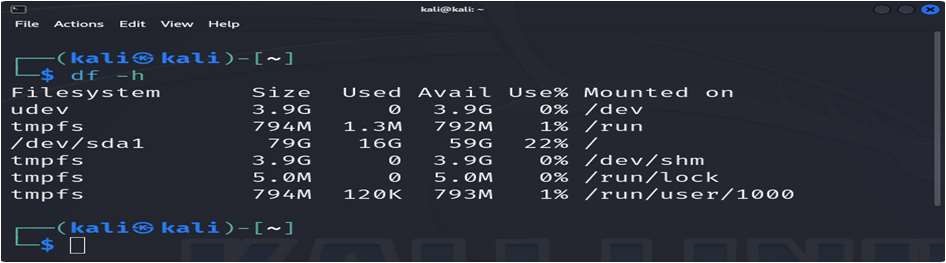
1. View the system’s kernel version:



1. Display the system’s memory usage:



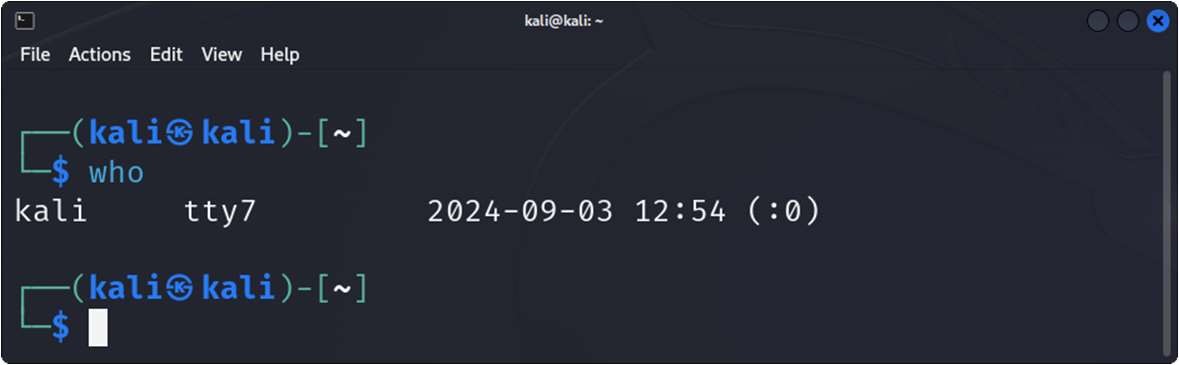
1. Show the system’s disk usage:



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



1. Display the current logged-in users:



1. Check the identity of the current user:



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



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



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



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



1. Display the system's boot messages:

