1. **Task 4: VPN and MAC Address Practice + UNIX User Password Management**

**Part 1: VPN Configuration**

1. Research and explain the purpose of a VPN and its role in enhancing network security.

The goal of a VPN is to encrypt your internet traffic so that unauthorised parties cannot read it because data eavesdropping is a common risk when operating public Wi-Fi networks, this is mainly important.  
  
**IP Address Masking:** Your true IP address is hidden when you use a VPN server to route your connection. This lets you access content that could be blocked in your area   
  
**Secure Remote Access:** VPN give employees of businesses the ability to safely access company resources from distant locations while protecting sensitive data while it is being transferred.

**Role in Enhancing Network Security**

1. **Protection on Public Networks**: Public Wi-Fi networks are often unsecured, making them prime targets for cybercriminals. VPN safeguard your data by encrypting the connection, reducing the risk of data breaches.
2. **Bypassing Censorship and Restrictions**: In regions with strict internet censorship, VPN allow users to access blocked websites and services by routing their connection through servers in different locations.
3. **Enhanced Privacy**: VPN avert Internet Service Providers (ISPs) and other entities from monitoring your online activities, ensuring a higher level of privacy.
4. **Secure Data Transmission**: VPN use protocols like IPsec and SSL/TLS to create encrypted tunnels for data transmission, ensures information remains confidential and unchanged during transit.

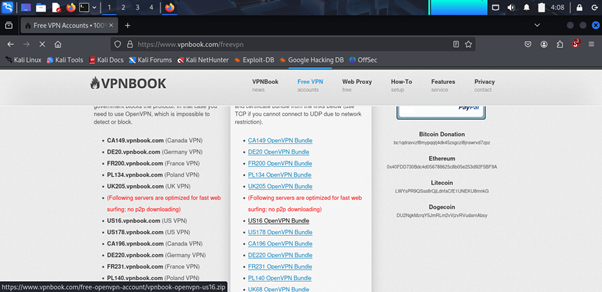
2. Install and configure a VPN client on your system

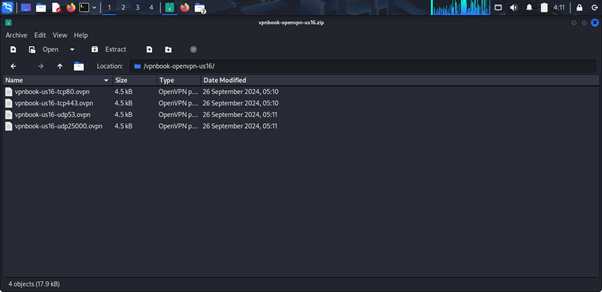
To install OpenVPN in kali, use **sudo apt install openvpn** and press enter

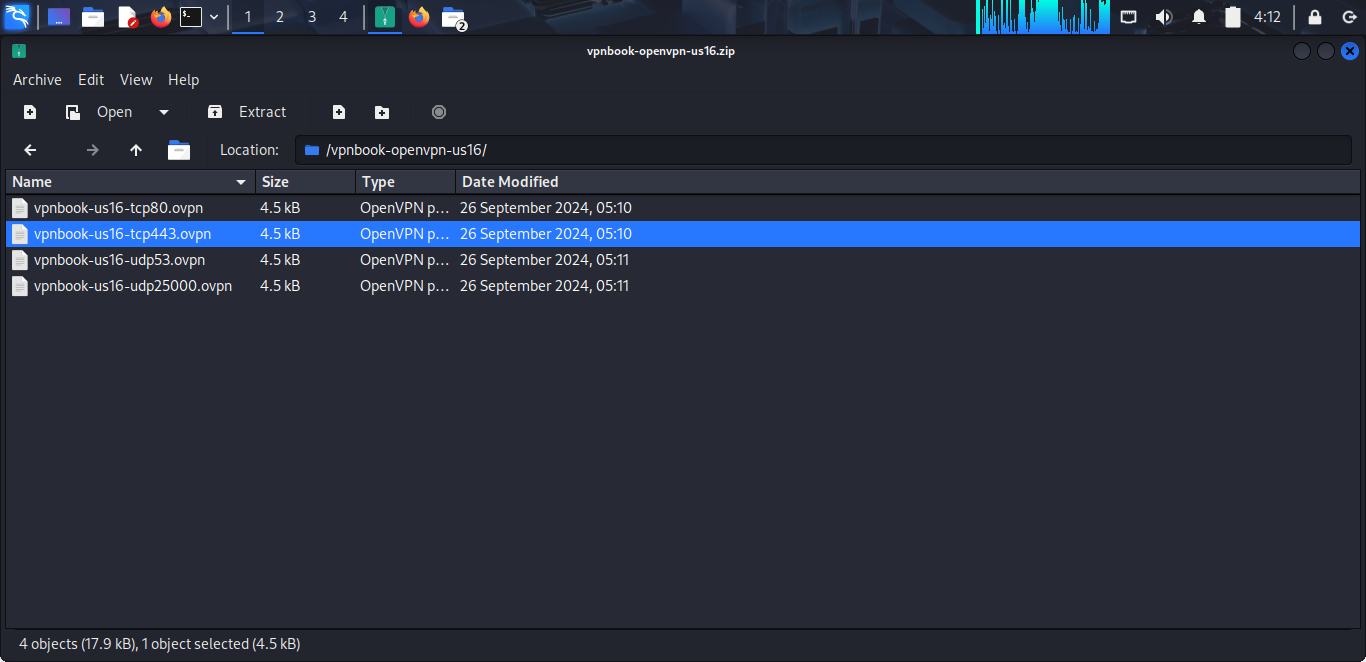


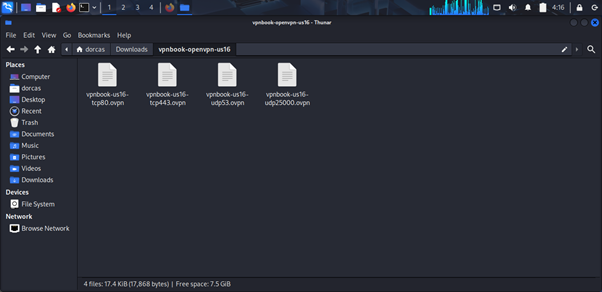
Open a browser and type in vpnbook.com

Scroll down and click on OpenVPN, download the US 16 OpenVPN Bundle server, open the download file. Right click on the file to extract.



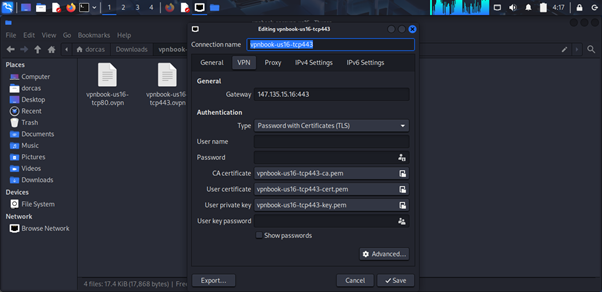


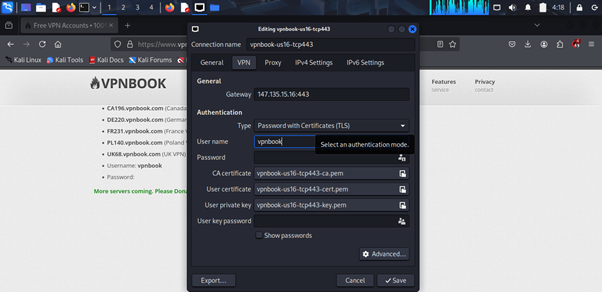




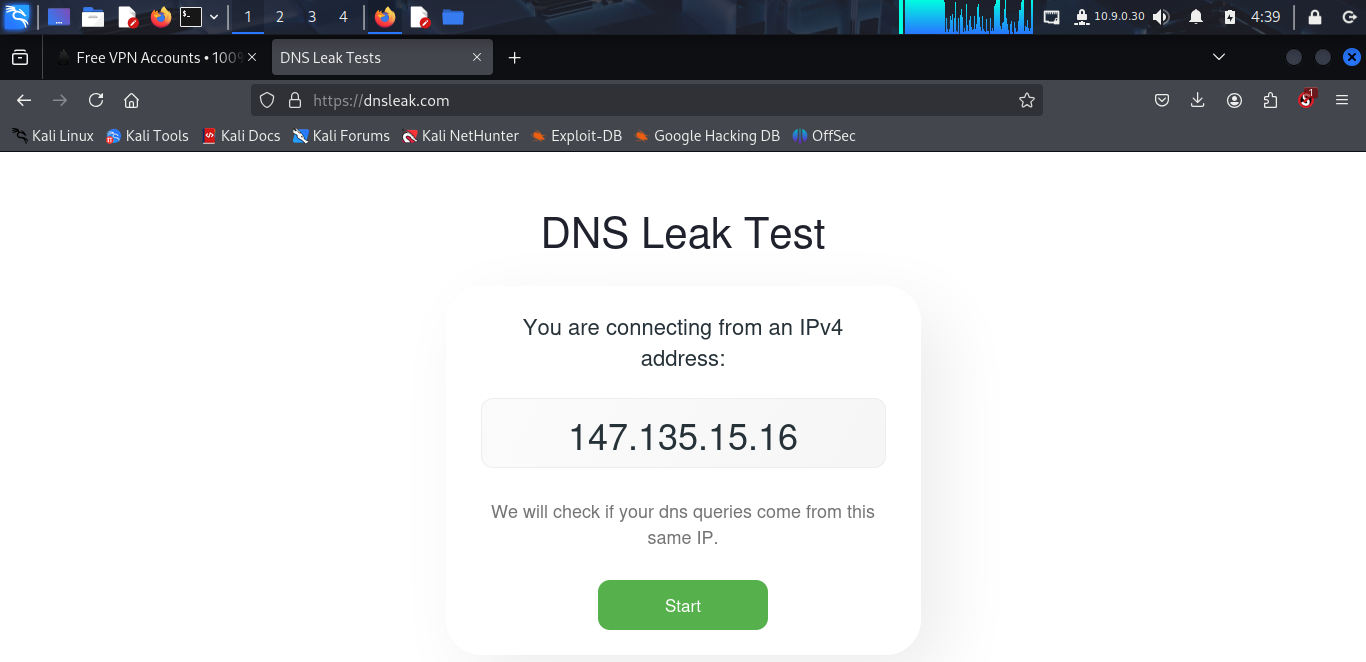
Click on the network connections to add VPN extracted, VPN connections, Add a VPN connection. Click on import a saved VPN configuration and create.

Go to Download and click on vpnbook-us1tcp 443 and open. Insert the username and password from vpnbook.com website. Click VPN Connections to confirm the configuration is setup.





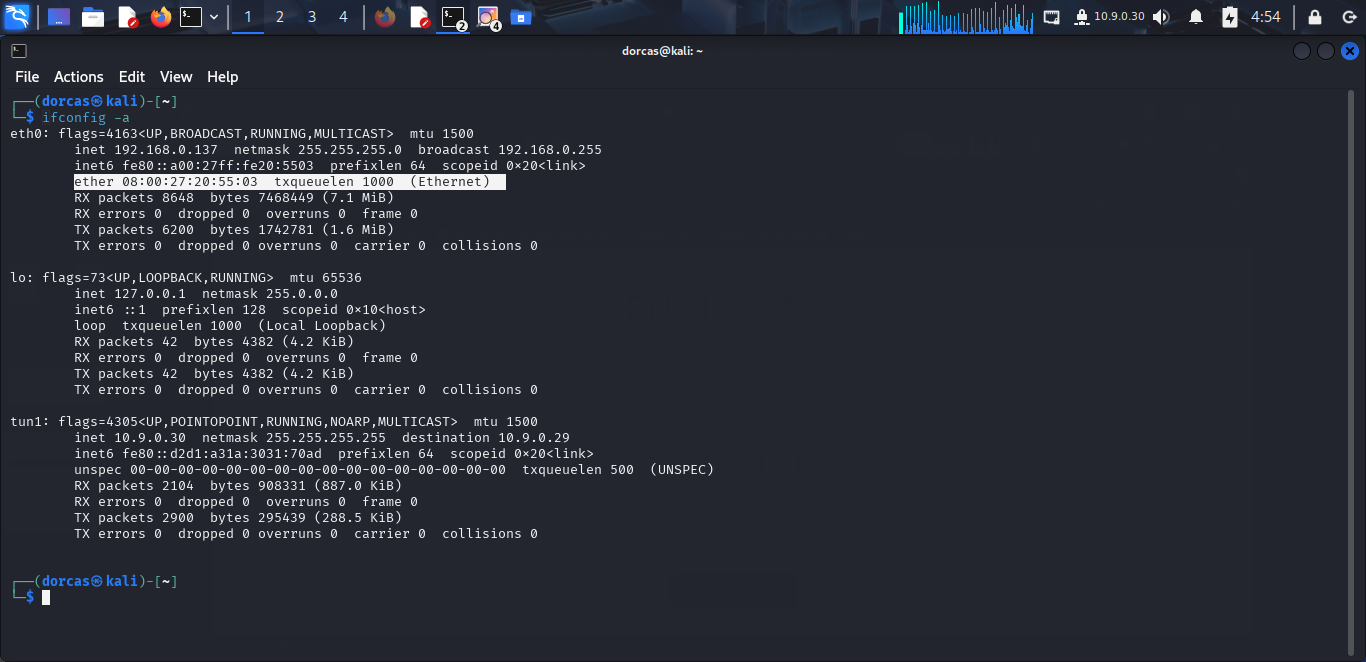
3. Test the VPN connection by connecting to a public VPN server and verifying your new IP address.



## Part 2: MAC Address Practice

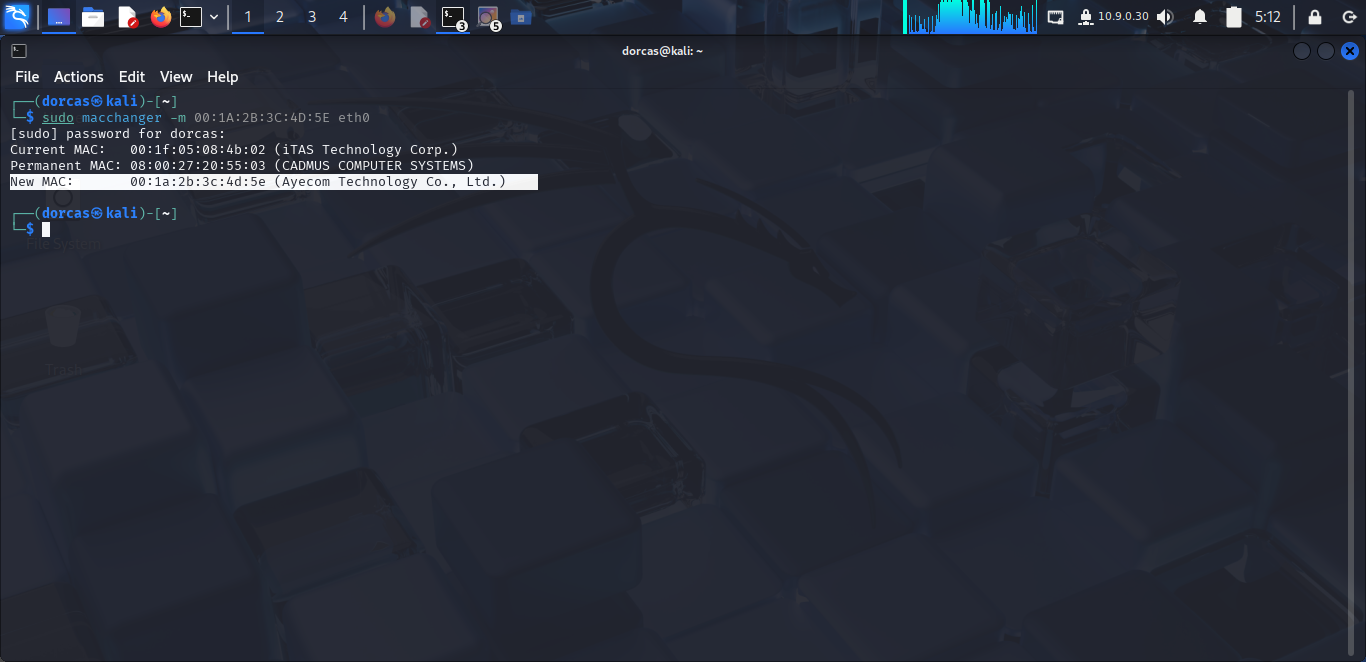
1. Find the current MAC address of your system.

Ether 08:00:27:20:20:55:03 is the MAC address



2. Change the MAC address of your network interface to the following: 00:1A:2B:3C:4D:5E.

To change mac address type **sudo macchanger –m 00:1A:2B:3C:4D:5E eth0**



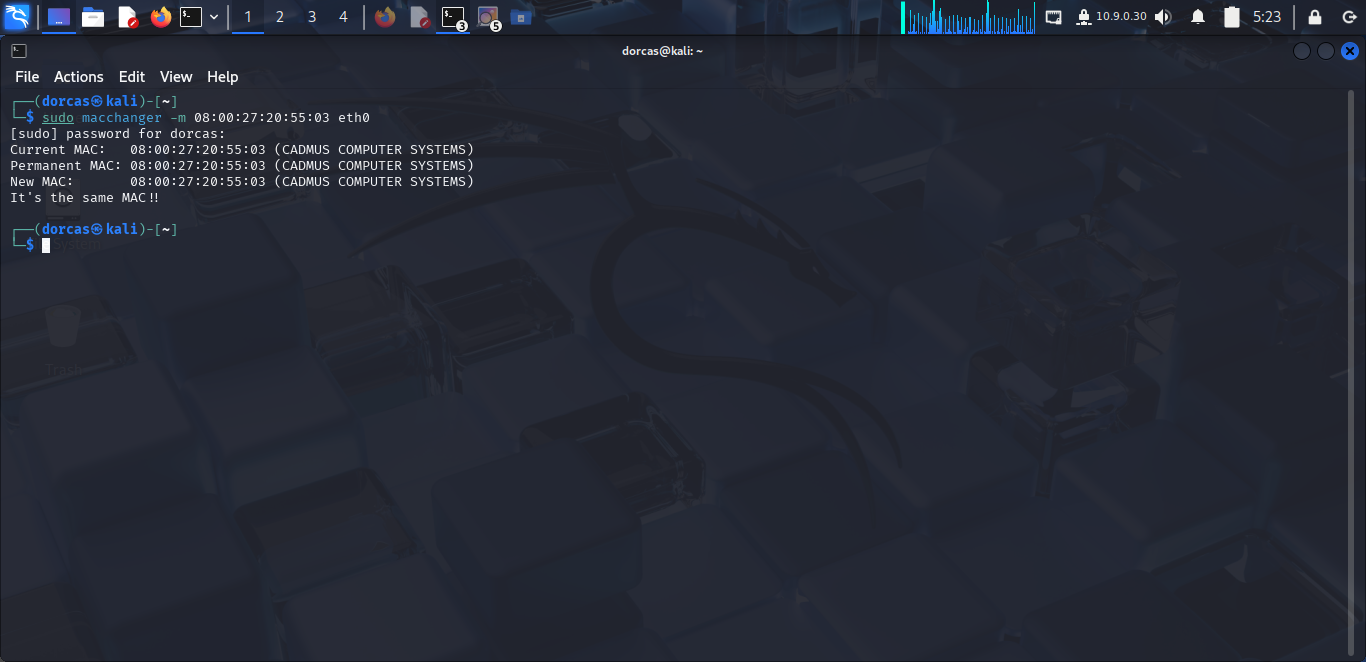
3. Verify the new MAC address to confirm the change.

MAC Address changed.



4. Revert to your original MAC address and document the process, including both MAC addresses.

To revert MAC address to its original form. Insert **sudo macchanger –m 08:00:27:20:55:03 eth0**



MAC address changed to the original form.



## Part 3: UNIX User Password Management

1. List all the users on the system and identify their password status.

Most users are not logged in.

To list all the users on the system and their password status input **lslogins**





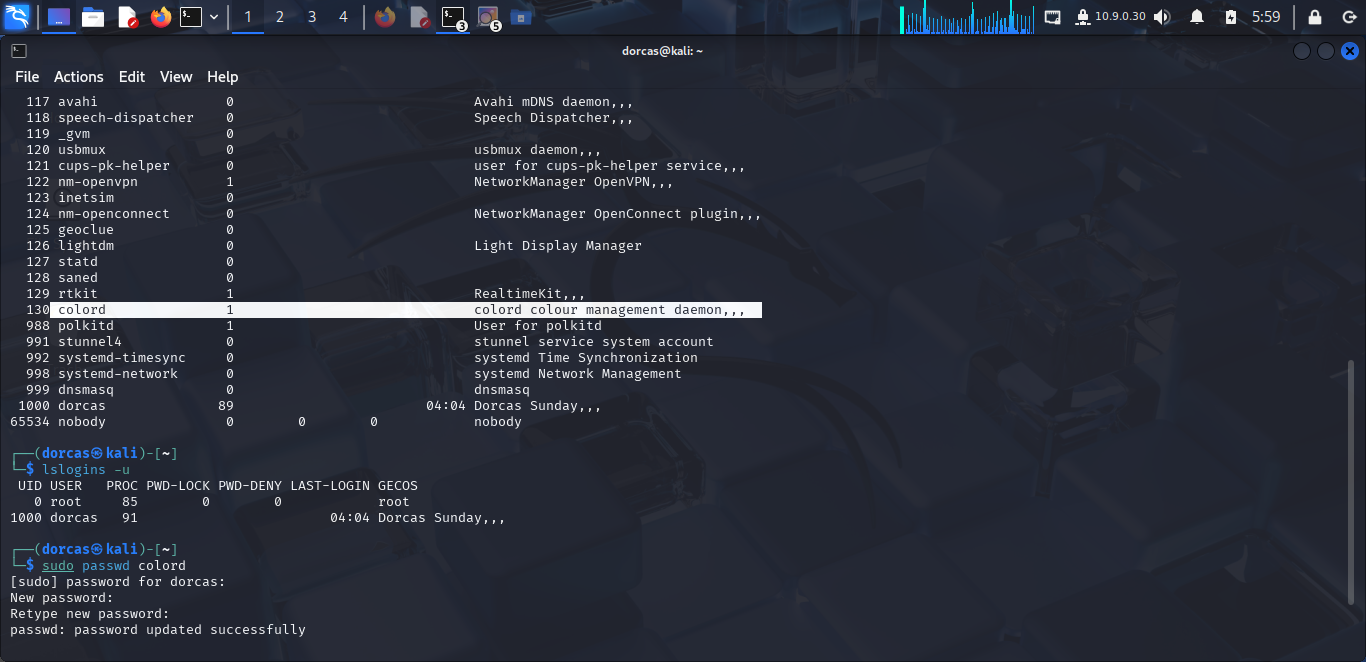
2. Check if any users have empty passwords.

User 107 tcpdump, 108 miredo, 109\_rpc, 110 redis 111 mosquito 112 redsocks, 113 sshd, etc do not have a password



3. Change the password for an existing user.

To change an existing user password type in **sudo passwd colord** andpress enter



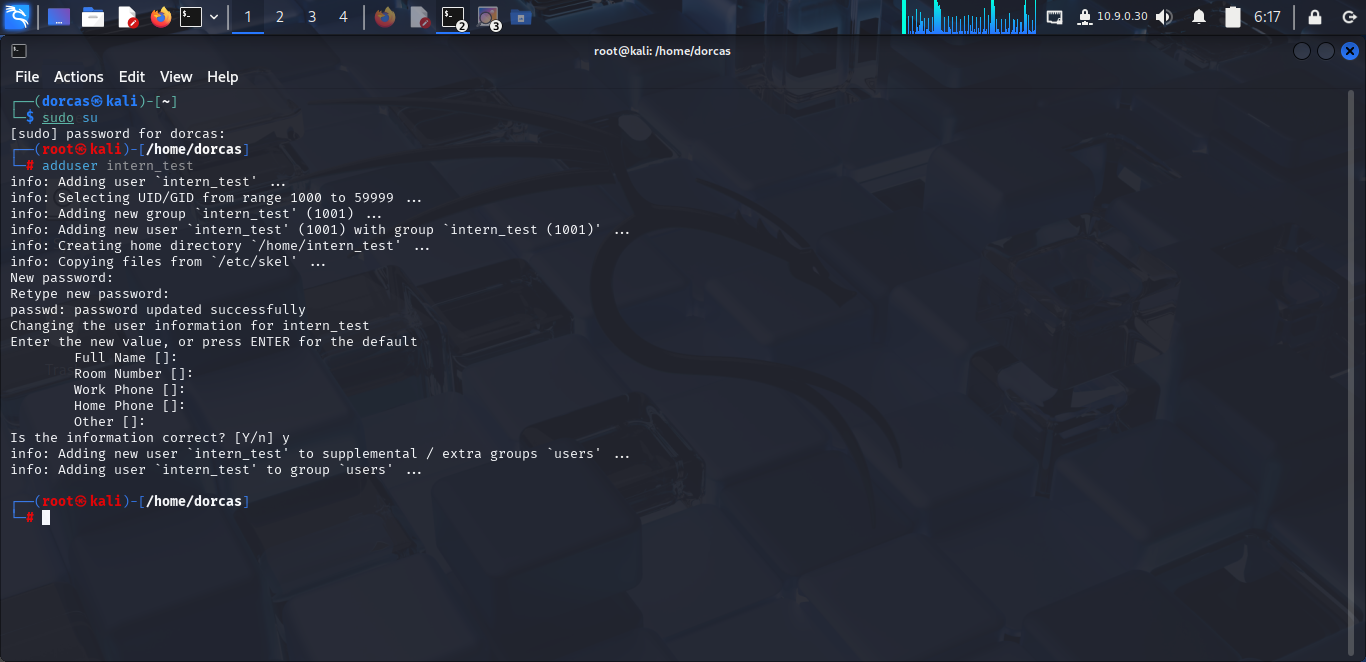
4. Create a new user with the username **'intern\_test'** and assign them a secure password.

To create a new user account for ‘**intern\_test’** the following command prompt was used.

**sudo su**

**Adduser intern\_test**

A secure password was assigned.



5. Disable a specific user account without deleting it.

**sudo passwd –l intern\_test** command was used to disable the user and **sudo passwd –u** **intern\_test** to unlock the user without deleting the user account.

