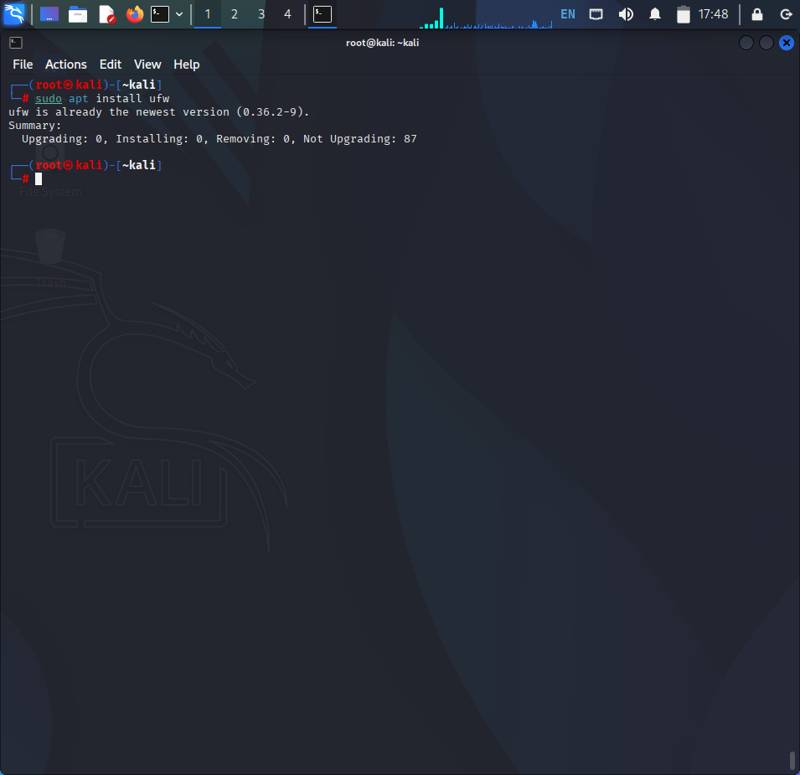
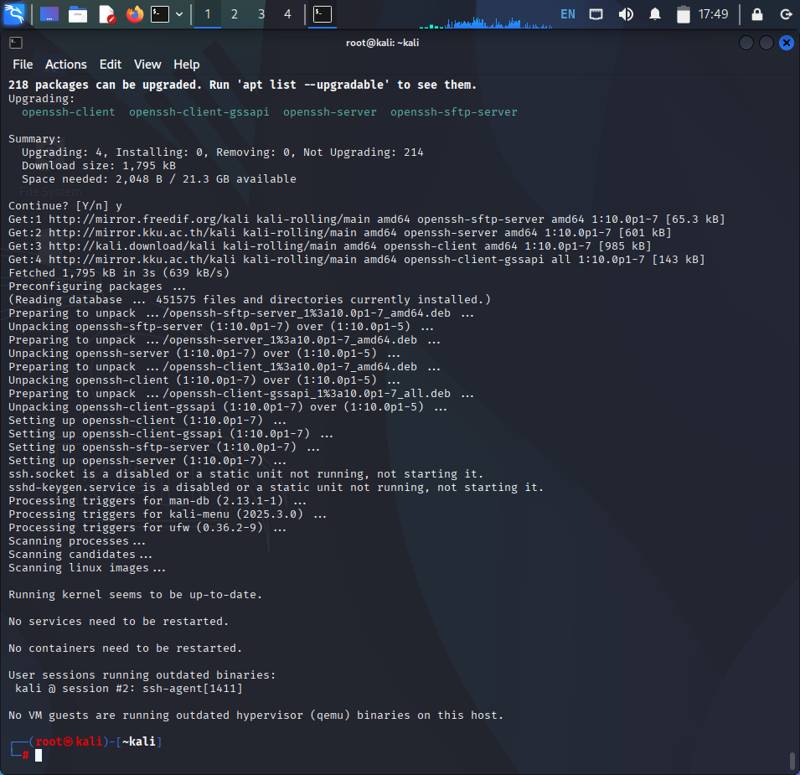
## Installing UFW Firewall:



Description: This screenshot shows the step 'Installing UFW Firewall' in the process of configuring the firewall and managing SSH connections using UFW in Linux.

Command: apt install ufw

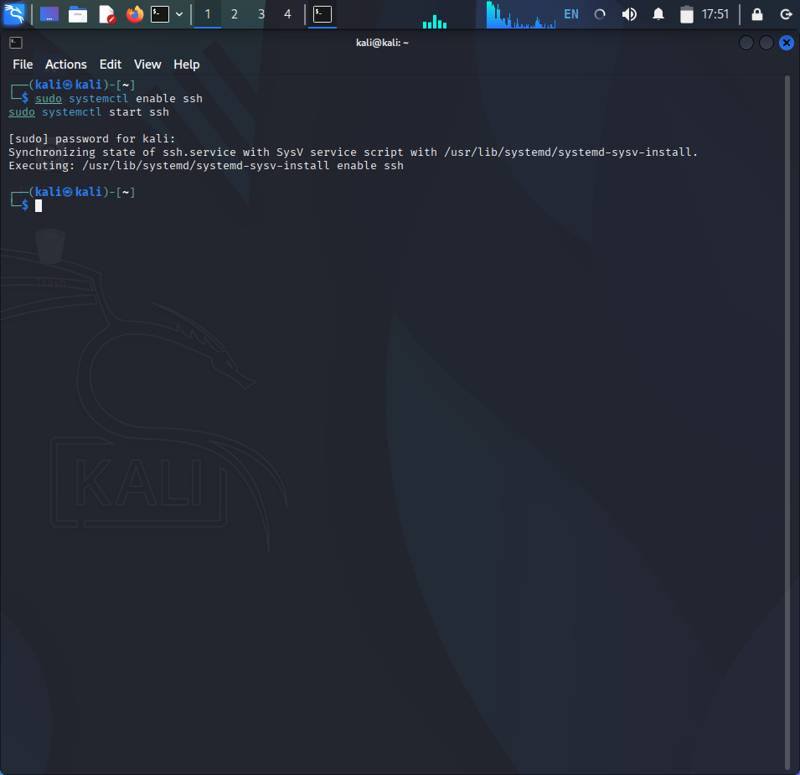
## Checking UFW Status Before Configuration:



Description: Installation if ssh-server in kali linux to enable and disable service for firewall

Command: sudo apt install openssh-server

## Allowing SSH Connections (Port 22):

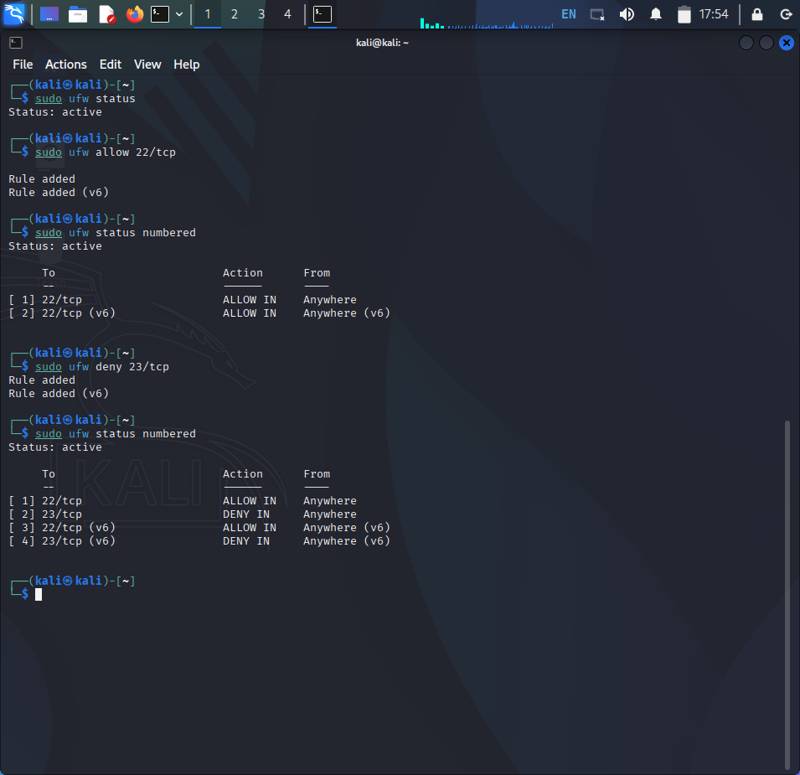


Description: This screenshot shows the step 'Allowing SSH Connections (Port 22)' in the process of configuring the firewall and managing SSH connections using UFW in Linux.

Command: sudo systemctl enable ssh

Sudo systemctl start ssh

## Blocking SSH Connections (Port 22):



Description: This screenshot shows the step 'Blocking SSH Connections (Port 22)' in the process of configuring the firewall and managing SSH connections using UFW in Linux.

Command:

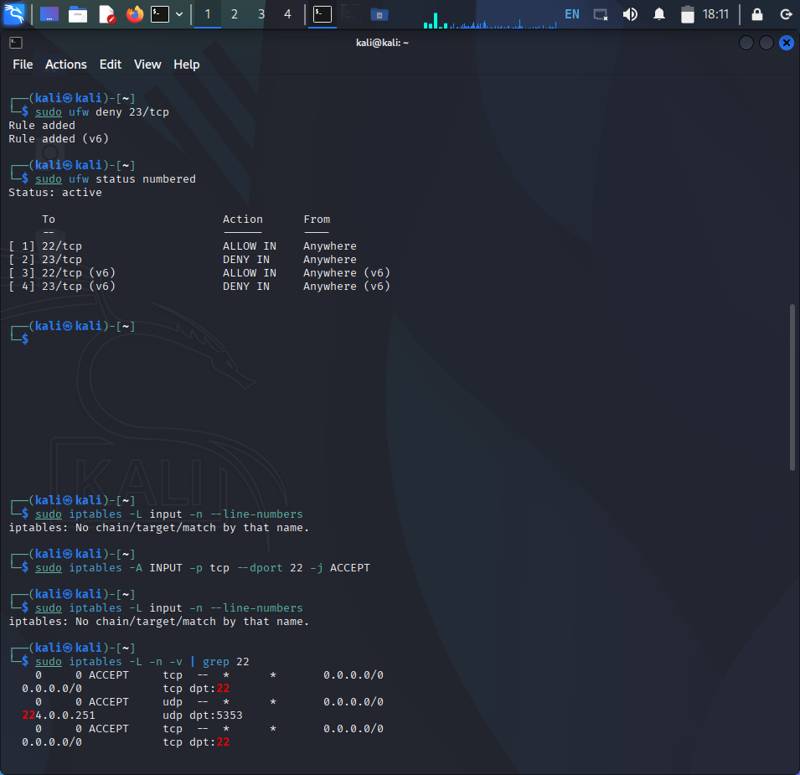
1. sudo ufw status -------- checking ufw status

2. sudo ufw enable -------- enabling ufw

3. sudo ufw allow 22/tcp ------ adding rule to firewall

4. sudo ufw status numbered ------ checking rule is added or not

## Verifying Firewall Rules:

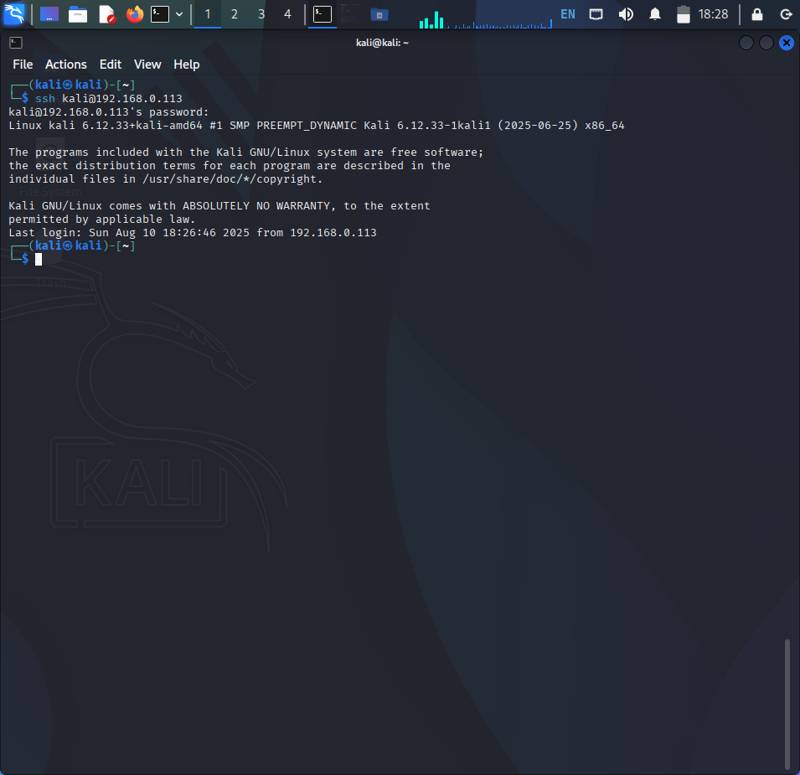


Description: In this screenshot adding iptables to access all ipaddress or specific address

Command:1. sudo iptables –A INPUT –p tcp –dport 22 –j ACCEPT --- ----- -- ACCEPTING CONNECTION

2. Sudo iptables –L –n –v | grep 22 --------- ----- --- checking status port22 is added or not

## Testing SSH Access After Blocking:

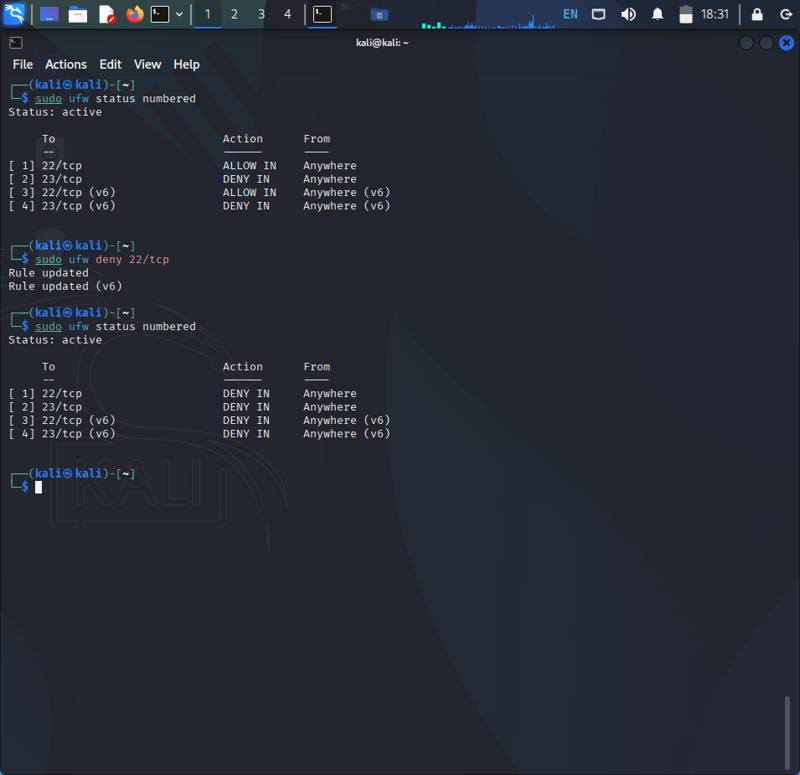


Description: This screenshot shows the step 'Testing SSH Access After allowing ' in the process of configuring the firewall and managing SSH connections using UFW in Linux.

Command:

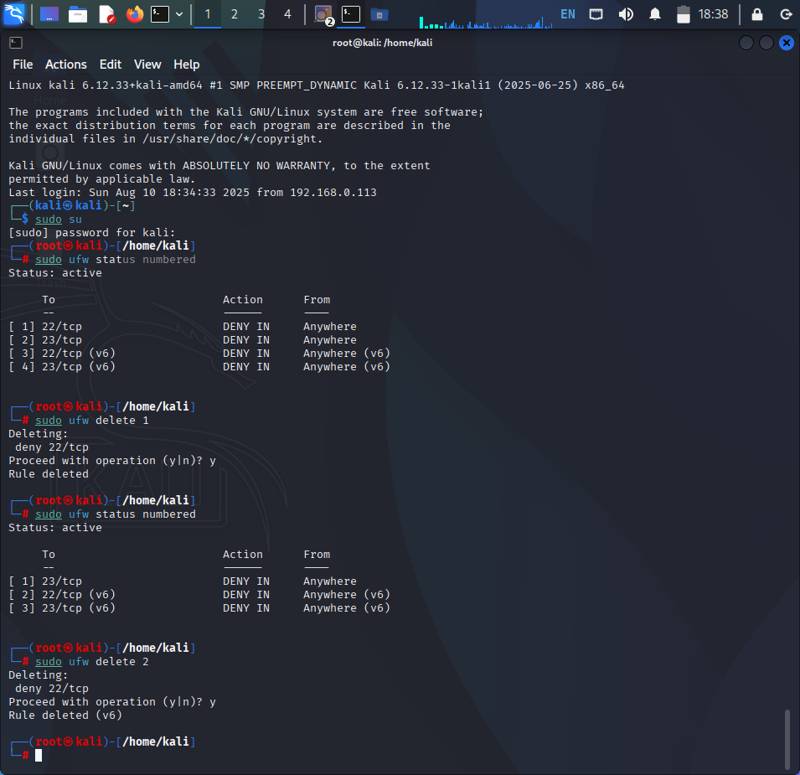
Ssh username@<ipaddress>

## Testing SSH Access After Allowing:

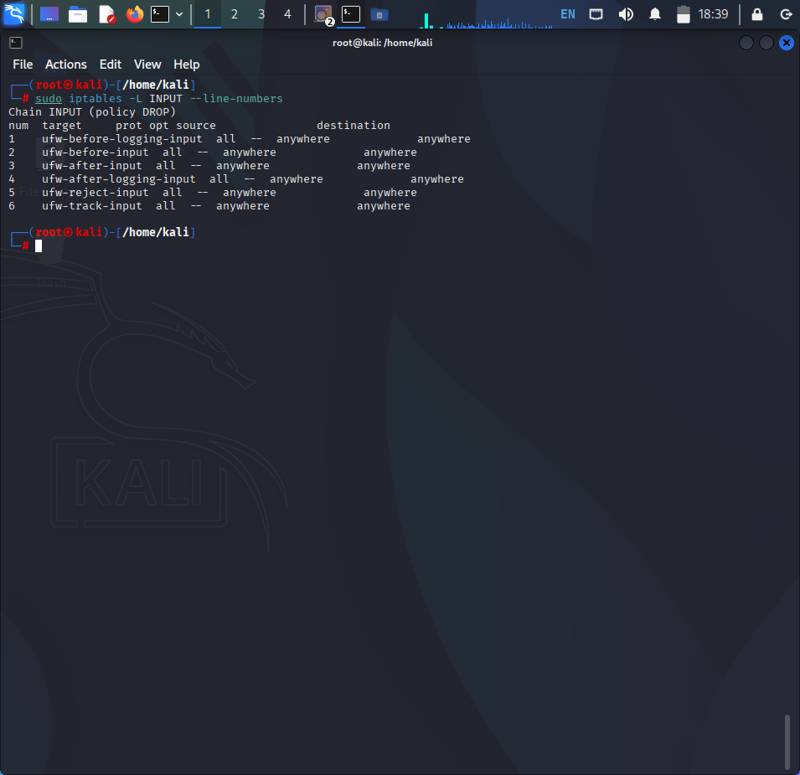


Description: This screenshot shows the step 'Testing SSH Access After deny' in the process of configuring the firewall and managing SSH connections using UFW in Linux.

Command: sudo ufw deny 22/tcp or sudo ufw delete <id>



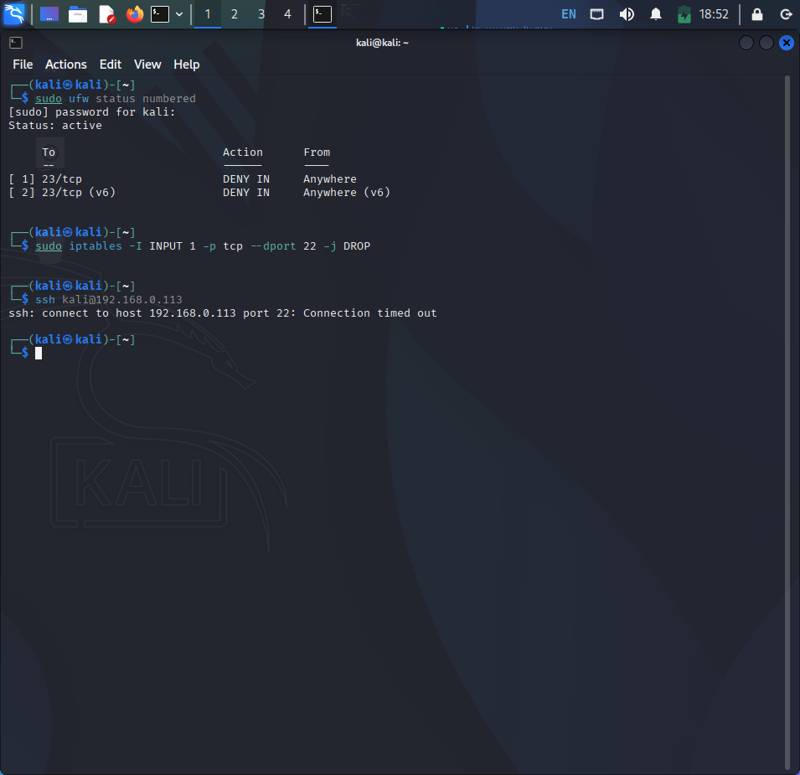
## Reloading Firewall Rules



Description: This screenshot shows the step 'Reloading Firewall Rules' in the process of configuring the firewall and managing SSH connections using UFW in Linux.

Command: sudo iptables –L INPUT --line-numbers

## Checking Final UFW Configuration:



Description: This screenshot shows how to delete iptable from iptables.

Command: 1. sudo iptables –L INPUT 1 –p tcp –-dport 22 –j drop

2. ssh username@<ipaddress> -- --- checking connection is blocked either not.