Installing a Firewall with UFW(Uncomplicated Firewall)

Requirement

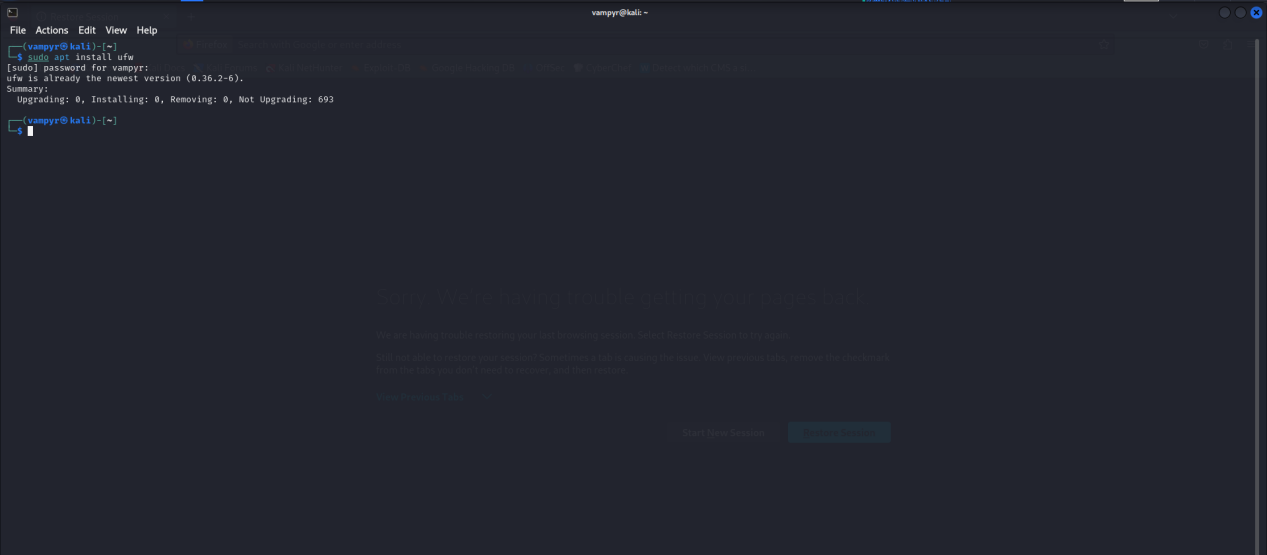
Linux system.

UFW

Step 1

- Install UFW with aptitude manager

sudo apt-get install ufw



- Check the status of ufw to know if its running

Sudo ufw status

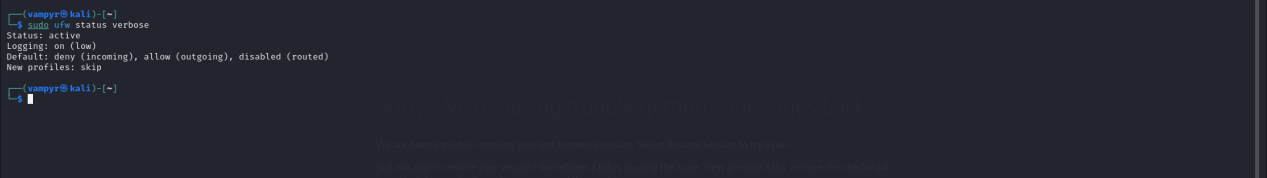
Step 2

I Enabled the firewall with command -

sudo ufw enable

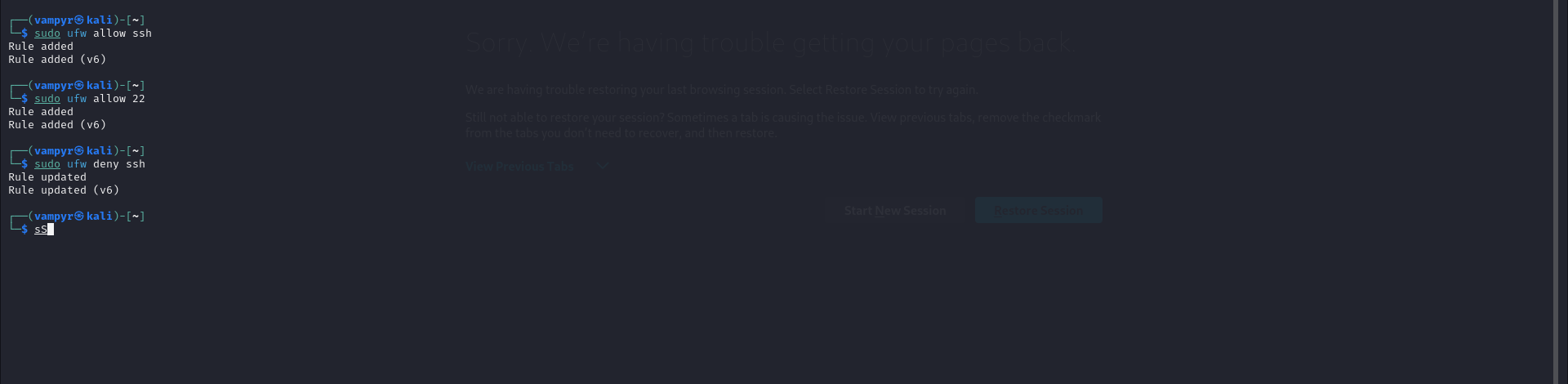
You can check the default connection status with

Sudo ufw status verbose



Step 3

You can use sudo ufw allow ssh or sudo ufw allow 22 to allow all incoming ssh or sudo ufw deny ssh to deny all incoming ssh connections connection now that the firewall is running



You can deny http or telnet connection which are not secure by using the same command

Sudo ufw deny http or sudo ufw deny telnet

This will deny all telnet or http connection to your server



You can check the status of all the ports that you have allowed or denied with

Sudo ufw status verbose



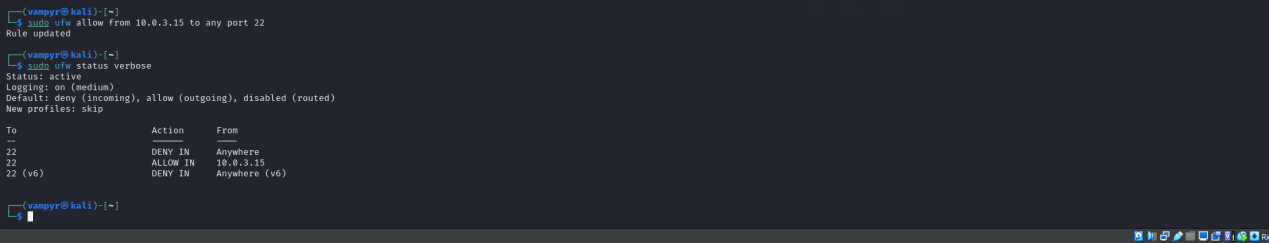
Say you want to allow ssh connections from your systems but deny for outsider so that attackers cannot ssh your server

You can use:

Sudo ufw allow from “your ip” to any port 22

You can do this for any protocol

I’ll be building a tool that automatically sets up the firewall and allows ports you want while disabling the unneccesary connections using bash soon so watchout for that



You can also allow your only your subnet to connect by adding your subnet

Sudo ufw allow from “subnet” to any port 22



Although it is not advisable because you only want specific ip addresses to be able to sconnect to your network

You can also delete rules from your list by first checking the rule number with

Sudo ufw status numbered

And the deleting the rule number with

Sudo ufw delete “number”



that’s it, Firewall has be set up and configured, with this knowledge I can configure a firewall for networks and servers to keep attackers out of your system