**Block or Disable SSH Access**

--------------------- On **IPtables Firewall** ---------------------

# iptables -I INPUT -s 192.168.1.100 -p tcp --dport ssh -j REJECT

# iptables -I INPUT -s 192.168.1.0/24 -p tcp --dport ssh -j REJECT

--------------------- On **FirewallD** ---------------------

# firewall-cmd --direct --add-rule ipv4 filter INPUT 1 -m tcp --source 192.168.1.100 -p tcp --dport 22 -j REJECT

# firewall-cmd --direct --add-rule ipv4 filter INPUT 1 -m tcp --source 192.168.1.100/24 -p tcp --dport 22 -j REJECT

To take new rules into effect, you need to use the following command.

# service iptables save [On IPtables Firewall]

# firewall-cmd --reload [On FirewallD]

Now, try to **SSH** the server from the blocked host. Please be mindful that here **192.168.1.150** is the blocked host.

# ssh 192.168.1.150

You should see the following message.

ssh: connect to host 192.168.1.150 port 22: Connection refused

**To block port 80 (HTTP server)**

# /sbin/iptables -A INPUT -p tcp --destination-port 80 -j DROP

# /sbin/service iptables save