Build and configure a firewall(UFW)

Name-Sarada Sankar Nayak

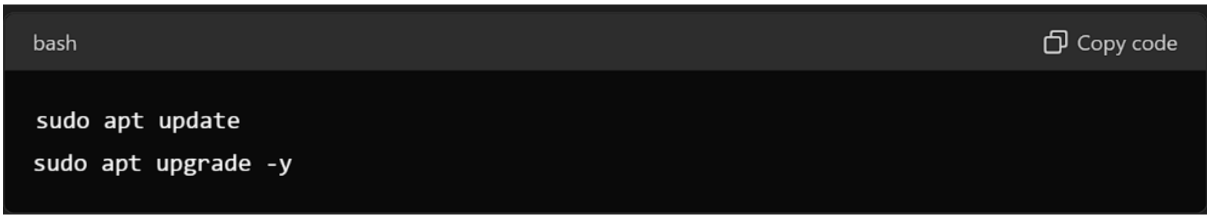
University-Vellore Institute of Technology,Chennai

Pre-requisites

- Basic knowledge of Linux commands
- An Ubuntu System
- Root or sudo Access

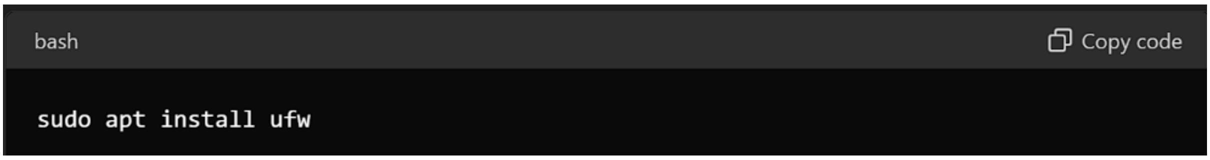
Procedures

Step-1)Ensure your System is up-to-date



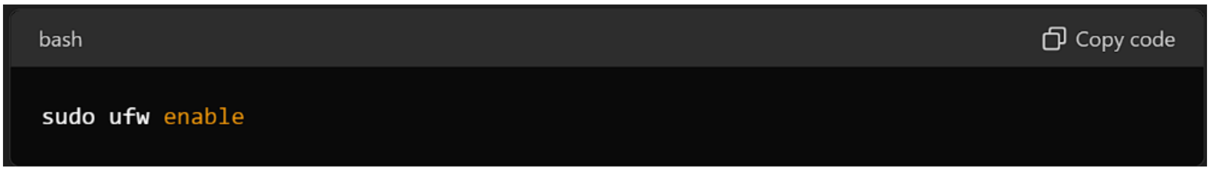
```bash
sudo apt update
sudo apt upgrade -y
```

Step-2)Install UFW



```bash
sudo apt install ufw
```

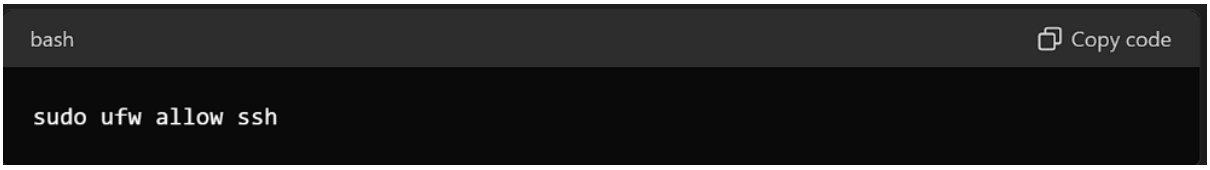
Step-3)Enable UFW



```bash
sudo ufw enable
```

Step-4)Allow SSH connections

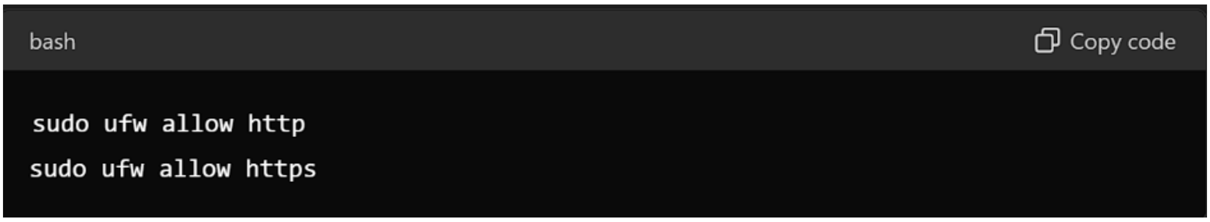
To prevent locking yourself out of the system,allow SSH connections



```
sudo ufw allow ssh
```

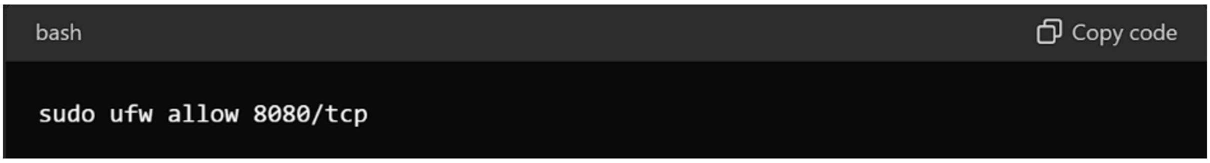
Step-5)Allow Specific Services and Ports

1)Allow HTTP and HTTPS Traffic:



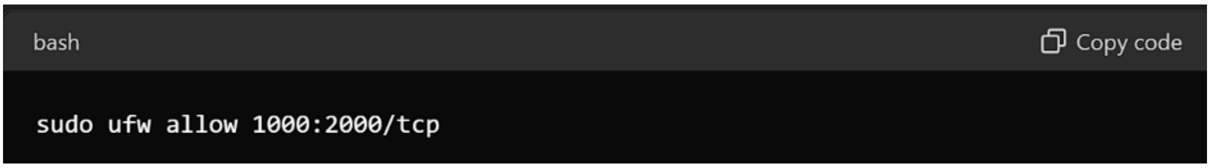
```
sudo ufw allow http
sudo ufw allow https
```

2)Allow other specific Ports:



```
sudo ufw allow 8080/tcp
```

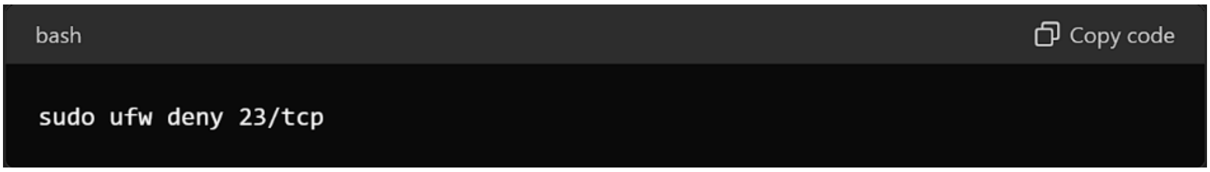
3)Allow range of Ports:



```
sudo ufw allow 1000:2000/tcp
```

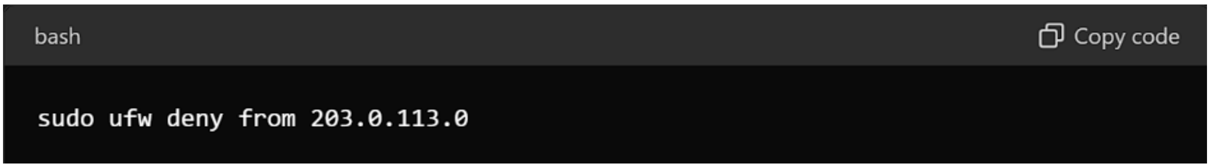
Step-6)Deny Specific services and ports:

1)Deny Specific port:



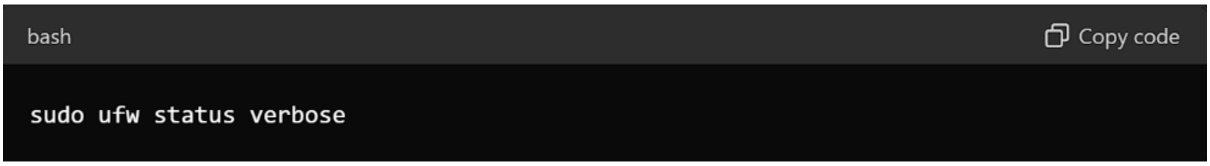
```bash
sudo ufw deny 23/tcp
```

2)Deny Specific IP address:



```bash
sudo ufw deny from 203.0.113.0
```

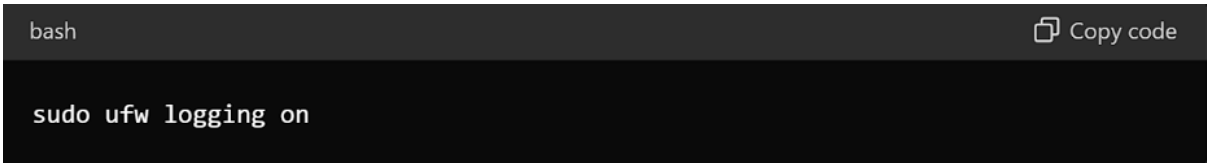
Step-7)To Check status of UFW and View current rules:



```bash
sudo ufw status verbose
```

Step-8)Adavnced UFW configuration:

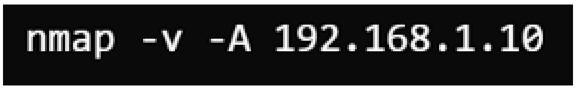
Enable logging in to monitor UFW activity



```bash
sudo ufw logging on
```

Step-9)Testing the firewall

Use “nmap” function from another OS to scan open ports on your firewall protected machine.(i.e I used Kali Linux OS for checking)



```
nmap -v -A 192.168.1.10
```

(Replace it with your actual Firewall IP address)