# Build and Configure a Firewall

## Aim:

Set up and configure a firewall on you Linux System

## Required:

- Basic Concepts of Linux.
- A Linux OS system (It can be a virtual a root system).

## Guide:

You should be a ROOT user to perform this

## Procedure:

- Here we will use the tool called 'UFW' stands for uncomplicated Firewall which is a front-end interface for managing the iptables firewall used in Linux Systems.
- UFW simplifies the process of configuring a firewall

---

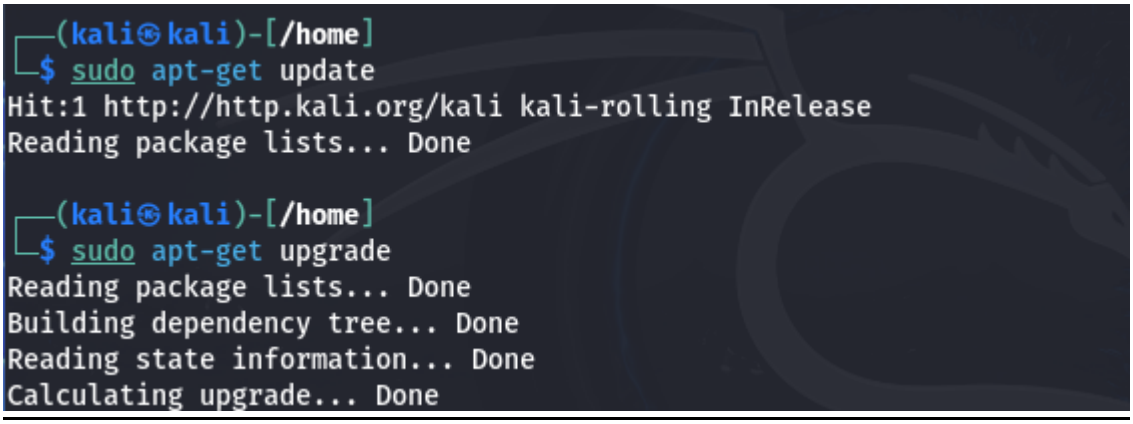
## Steps:

### 1. Update you Linux system

Command-

**sudo apt-get update**

**sudo apt-get upgrade**

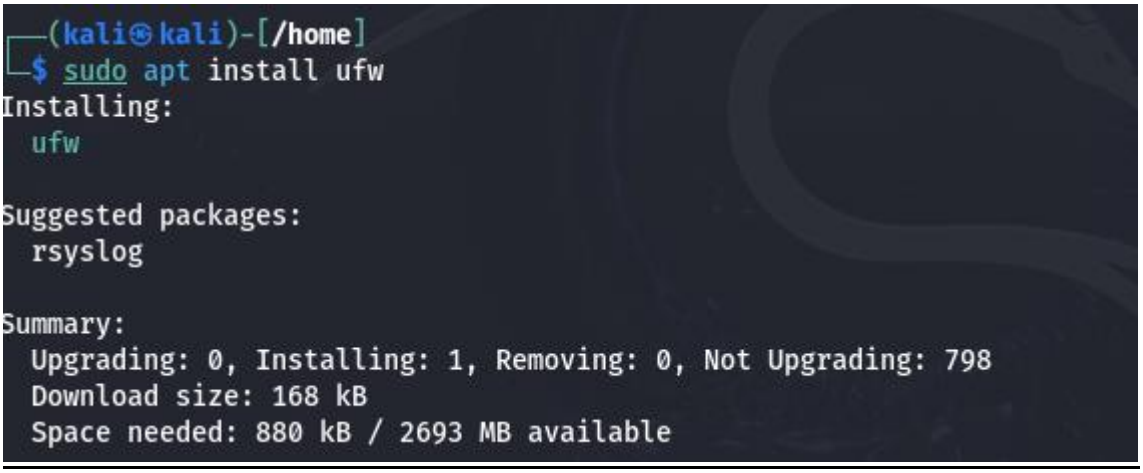



## 2. Install UFW

UFW can be present in your ubuntu system, but u can install it in your system

Command-

**sudo apt install ufw**




## 3. Enable UFW

By default, UFW is disabled so we enable it by

Command-

**sudo ufw enable**

```
┌──(kali㉿kali)-[/home]
└─$ sudo ufw enable
Firewall is active and enabled on system startup
```

Now u have UFW enabled with which u can configure the Firewall

## 4. Allow SSH connections

Allowing SSH through the firewall by

Command-

**sudo ufw allow ssh**

or you can do it by specifying port

Command-

**sudo ufw allow 22/tcp**

enables you to securely log in to your system remotely which can be essential for managing servers or accessing systems without physical access.

```
┌──(kali㉿kali)-[/home]
└─$ sudo ufw allow 22/tcp
[sudo] password for kali:
Rule added
Rule added (v6)
```

The setting up of UFW is Complete.

- Using UFW we call Allow some specific services and deny some specific services
- There are two ways to achieve this
    - Specifying port name
    - Specifying port number

---

# Allowing Specific Services

1. Allowing a service (HTTP and HTTPS)

We can achieve this by using

Command-

**sudo ufw allow http**
**sudo ufw allow 80/tcp**

for http and for https u can go for

Command-

**sudo ufw allow https**
**sudo ufw allow 443/tcp**


2. Allowing specific ports

We can allow some specific ports by specifying the port number

Command-

**Sudo ufw allow 8080/tcp**

```
┌──(kali㉿kali)-[~]
└─$ sudo ufw allow 8080/tcp
Rule added
Rule added (v6)
```

3. Allow range of ports

We can allow some range of ports by specifying the range like

Command-

**Sudo ufw allow 1000:2000/tcp**

```
┌──(kali㉿kali)-[~]
└─$ sudo ufw allow 1000:2000/tcp
Rule added
Rule added (v6)
```

**4.** Allow specific ipaddress

Using ufw we can allow connection form specific ipaddress like for example(192.168.1.4)

Command-

**Sudo ufw allow from 192.168.1.4**

```
┌──(kali㉿kali)-[~]
└─$ sudo ufw allow from 192.168.1.4
Rule added
```

**5.** Allow specific subnets

We can allow connection from specific subnets for example(192.168.1.4/24)

Command-

Sudo ufw allow 192.168.1.4/24


---

# Denying specific service

By default, UFW deny the coming connection except for the one which u allow. You can explicitly deny services

1. **Deny a specific port**

   You can deny a specific port by using the command

Command-

Sudo ufw deny 23/tcp


2. **Deny a specific ipaddress**

   You can deny a connection from ipaddress

Command-

Sudo ufw deny from 203.0.113.0

## To know the rules of ufw

Command-

**sudo ufw status**

```
┌──(kali㉿kali)-[~]
└─$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW       Anywhere
80/tcp                     ALLOW       Anywhere
443/tcp                    ALLOW       Anywhere
8080/tcp                   ALLOW       Anywhere
Anywhere                   ALLOW       192.168.1.4
Anywhere                   ALLOW       192.168.1.0/24
1000:2000/tcp              ALLOW       Anywhere
23/tcp                     DENY        Anywhere
Anywhere                   DENY        203.0.113.0
22/tcp (v6)                ALLOW       Anywhere (v6)
80/tcp (v6)                ALLOW       Anywhere (v6)
443/tcp (v6)               ALLOW       Anywhere (v6)
8080/tcp (v6)              ALLOW       Anywhere (v6)
1000:2000/tcp (v6)         ALLOW       Anywhere (v6)
23/tcp (v6)                DENY        Anywhere (v6)
```

Let's say there is a scenario where you want to delete a rule that u found in the status command. You can do it in two ways by specifying number of the rule or specifying the name of the rule

Command-

**sudo ufw delete 4**

**sudo ufw delete 23/tcp**


---

## Testing the Firewall

The testing of firewall is done by checking open ports and checking the connections of denied ports

Command-

**namp -v -a 192.168.1.30**

---

## Checking connections:

Checking connections with the denied services ensure the firewall is working as expected

---

## Conclusion:

we have successfully configured a firewall on our systems using UFW.

---