BUILDING AND CONFIGURING A FIREWALL

Table of Contents

1. INTRODUCTION **2**
2. **PROJECT OVERVIEW** **2**
3. PREREQUISITES **2**
4. PROJECT SETUP **2**
4.1. Initial Sever Setup 2
4.2. Installing UFW 3
5. FIREWALL CONFIGURATION **3**
5.1. Enabling UFW 3
5.2. Allowing and denying services 3
5.3. To check the status of firewall 4
5.4. Deleting any service in the firewall 5
6. FIREWALL TESTING **6**
6.1. Installing NMAP 6
6.2. Look for IP Address 6
6.3. Test the firewall 7

1. INTRODUCTION

This documentation provides a comprehensive guide to building and configuring a firewall on an Ubuntu system. Firewalls are crucial for securing servers and personal computers by controlling incoming and outgoing network traffic. It acts as a barrier between a trusted internal network and untrusted external networks. Firewalls can be configured to allow or deny traffic based on factors like IP addresses, port numbers, or protocols.

2. PROJECT OVERVIEW

The goal of this project is to set up a firewall on Ubuntu using UFW. The process involves installing UFW, configuring basic and advanced rules, and testing to ensure the firewall functions as expected.

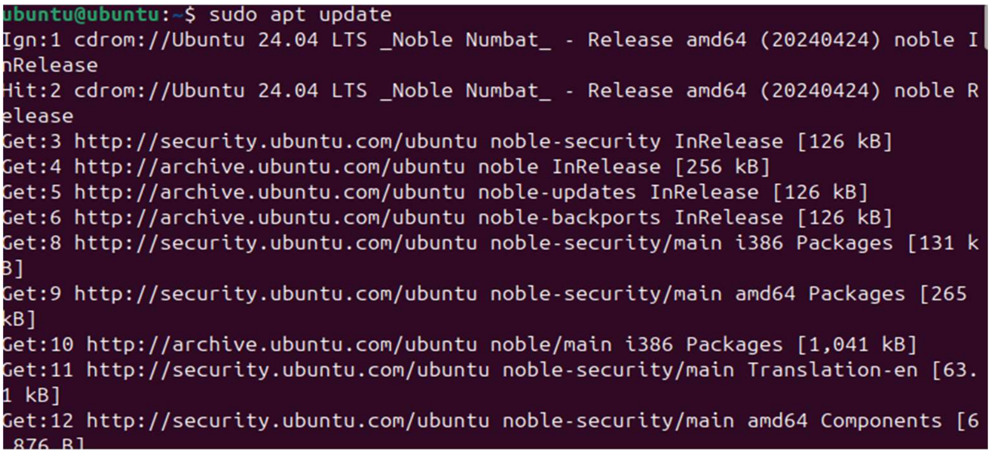
3. PREREQUISITES

- ✓ An Ubuntu system (version 24.04 has been used here).
- ✓ Administrative access to the Ubuntu system (sudo privileges).
- ✓ Basic knowledge of command-line operations in Linux.

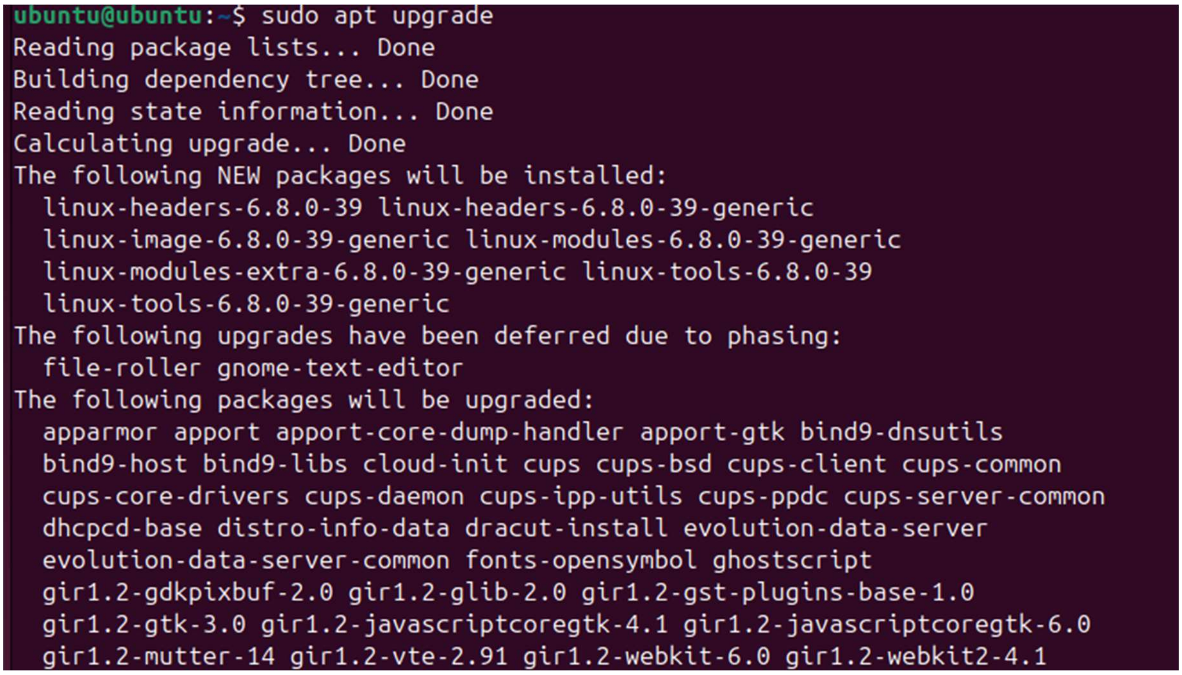
4. PROJECT SETUP

4.1 Initial Server Setup

Before building and configuring the firewall, we need to ensure that our Ubuntu server is up to date.



```
ubuntu@ubuntu:~$ sudo apt update
Ign:1 cdrom://Ubuntu 24.04 LTS _Noble Numbat_ - Release amd64 (20240424) noble I
nRelease
Hit:2 cdrom://Ubuntu 24.04 LTS _Noble Numbat_ - Release amd64 (20240424) noble R
elease
Get:3 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Get:4 http://archive.ubuntu.com/ubuntu noble InRelease [256 kB]
Get:5 http://archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:6 http://archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Get:8 http://security.ubuntu.com/ubuntu noble-security/main i386 Packages [131 k
B]
Get:9 http://security.ubuntu.com/ubuntu noble-security/main amd64 Packages [265
kB]
Get:10 http://archive.ubuntu.com/ubuntu noble/main i386 Packages [1,041 kB]
Get:11 http://security.ubuntu.com/ubuntu noble-security/main Translation-en [63.
1 kB]
Get:12 http://security.ubuntu.com/ubuntu noble-security/main amd64 Components [6
 876 B]
```



```
ubuntu@ubuntu:~$ sudo apt upgrade
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following NEW packages will be installed:
  linux-headers-6.8.0-39 linux-headers-6.8.0-39-generic
  linux-image-6.8.0-39-generic linux-modules-6.8.0-39-generic
  linux-modules-extra-6.8.0-39-generic linux-tools-6.8.0-39
  linux-tools-6.8.0-39-generic
The following upgrades have been deferred due to phasing:
  file-roller gnome-text-editor
The following packages will be upgraded:
  apparmor apport apport-core-dump-handler apport-gtk bind9-dnsutils
  bind9-host bind9-libs cloud-init cups cups-bsd cups-client cups-common
  cups-core-drivers cups-daemon cups-ipp-utils cups-ppdc cups-server-common
  dhcpcd-base distro-info-data dracut-install evolution-data-server
  evolution-data-server-common fonts-opensymbol ghostscript
  gir1.2-gdkpixbuf-2.0 gir1.2-glib-2.0 gir1.2-gst-plugins-base-1.0
  gir1.2-gtk-3.0 gir1.2-javascriptcoregtk-4.1 gir1.2-javascriptcoregtk-6.0
  gir1.2-mutter-14 gir1.2-vte-2.91 gir1.2-webkit-6.0 gir1.2-webkit2-4.1
```

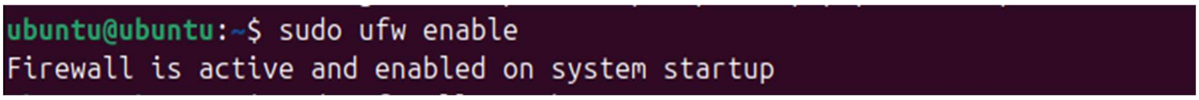
4.2 Installing UFW

UFW is installed by default on Ubuntu.

5. FIREWALL CONFIGURATION

5.1 Enabling UFW

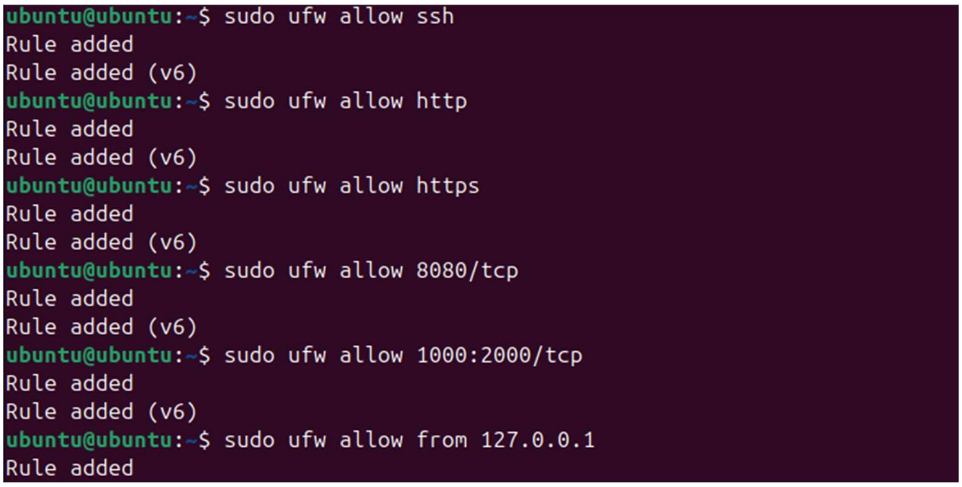
Now we will enable the UFW by the following command:



```
ubuntu@ubuntu:~$ sudo ufw enable
Firewall is active and enabled on system startup
```

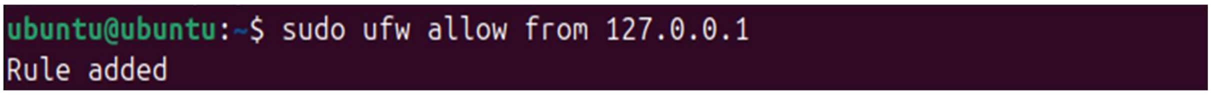
5.2 Allowing and Denying Services

Here we will either allow or deny services using UFW commands:
We have allowed services like SSH, HTTP, HTTPS, TCP port 8080 and TCP ports that range from 1000 to 2000.



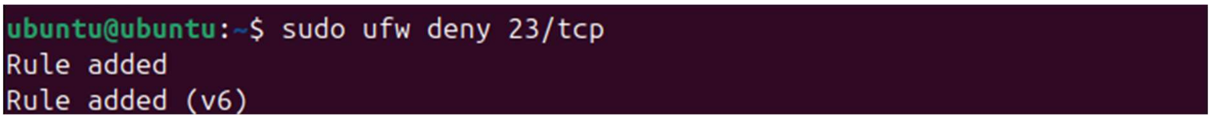
```
ubuntu@ubuntu:~$ sudo ufw allow ssh
Rule added
Rule added (v6)
ubuntu@ubuntu:~$ sudo ufw allow http
Rule added
Rule added (v6)
ubuntu@ubuntu:~$ sudo ufw allow https
Rule added
Rule added (v6)
ubuntu@ubuntu:~$ sudo ufw allow 8080/tcp
Rule added
Rule added (v6)
ubuntu@ubuntu:~$ sudo ufw allow 1000:2000/tcp
Rule added
Rule added (v6)
ubuntu@ubuntu:~$ sudo ufw allow from 127.0.0.1
Rule added
```

Here we have also allowed the IP address of the local computer.



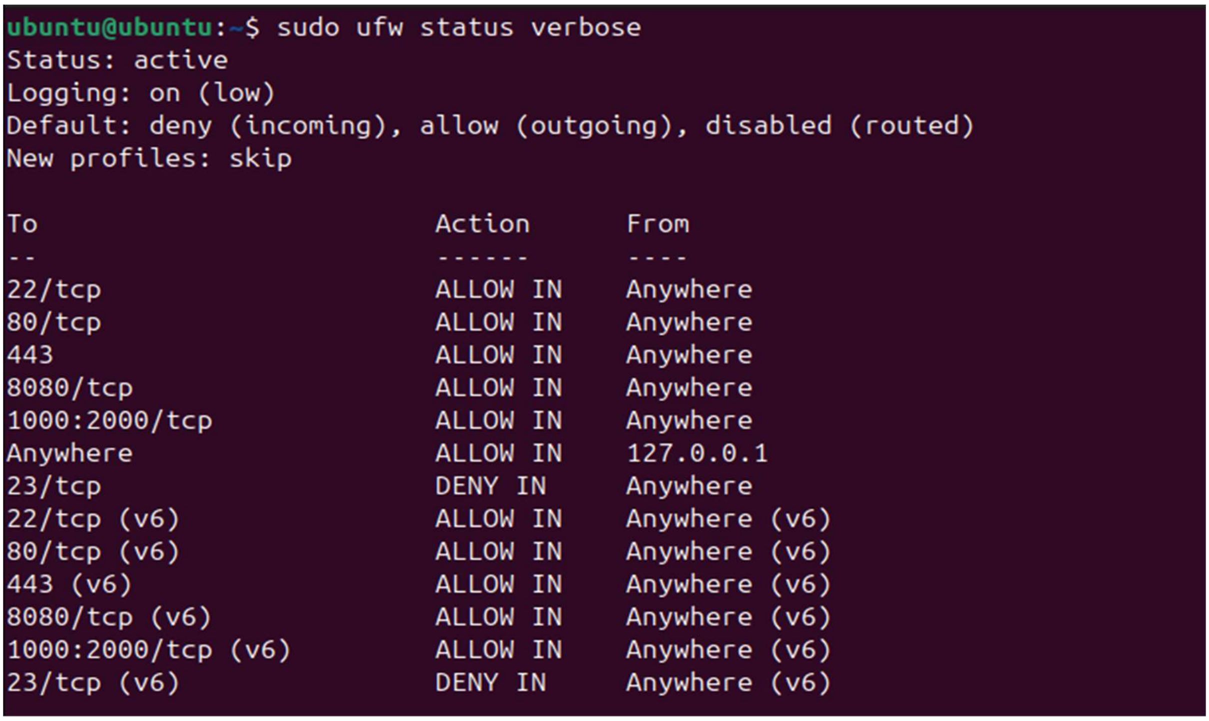
```
ubuntu@ubuntu:~$ sudo ufw allow from 127.0.0.1
Rule added
```

Here we have denied some services like TCP port 23.



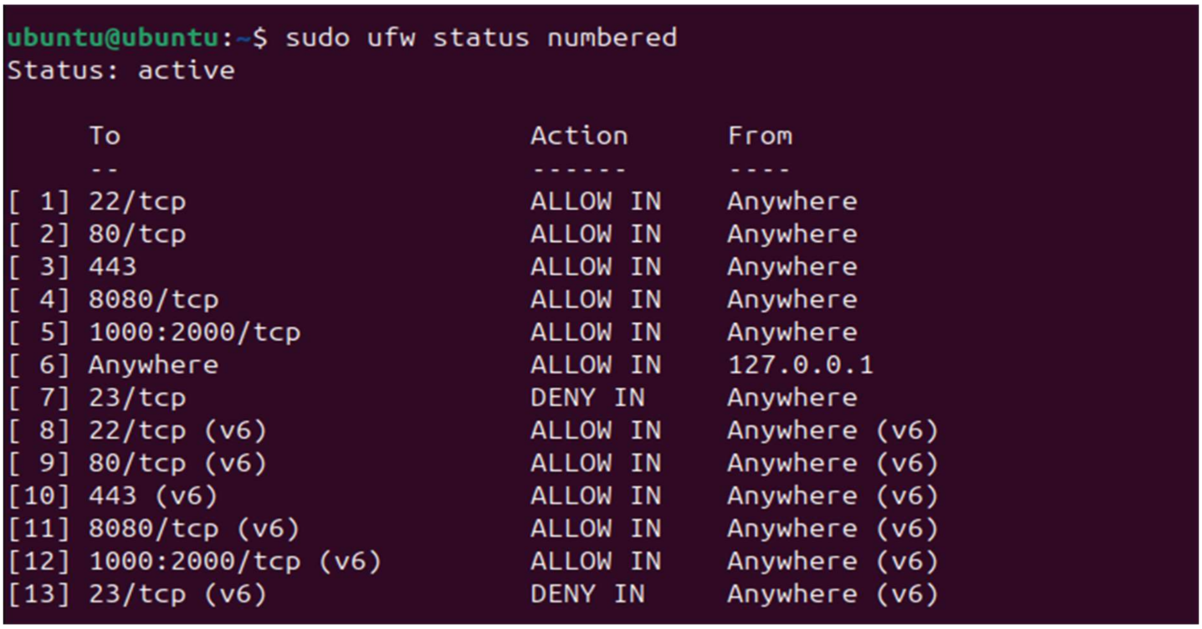
```
ubuntu@ubuntu:~$ sudo ufw deny 23/tcp
Rule added
Rule added (v6)
```

5.3 To check the status of the firewall



```
ubuntu@ubuntu:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW IN    Anywhere
80/tcp                     ALLOW IN    Anywhere
443                        ALLOW IN    Anywhere
8080/tcp                   ALLOW IN    Anywhere
1000:2000/tcp              ALLOW IN    Anywhere
Anywhere                   ALLOW IN    127.0.0.1
23/tcp                     DENY IN     Anywhere
22/tcp (v6)                ALLOW IN    Anywhere (v6)
80/tcp (v6)                ALLOW IN    Anywhere (v6)
443 (v6)                   ALLOW IN    Anywhere (v6)
8080/tcp (v6)              ALLOW IN    Anywhere (v6)
1000:2000/tcp (v6)         ALLOW IN    Anywhere (v6)
23/tcp (v6)                DENY IN     Anywhere (v6)
```

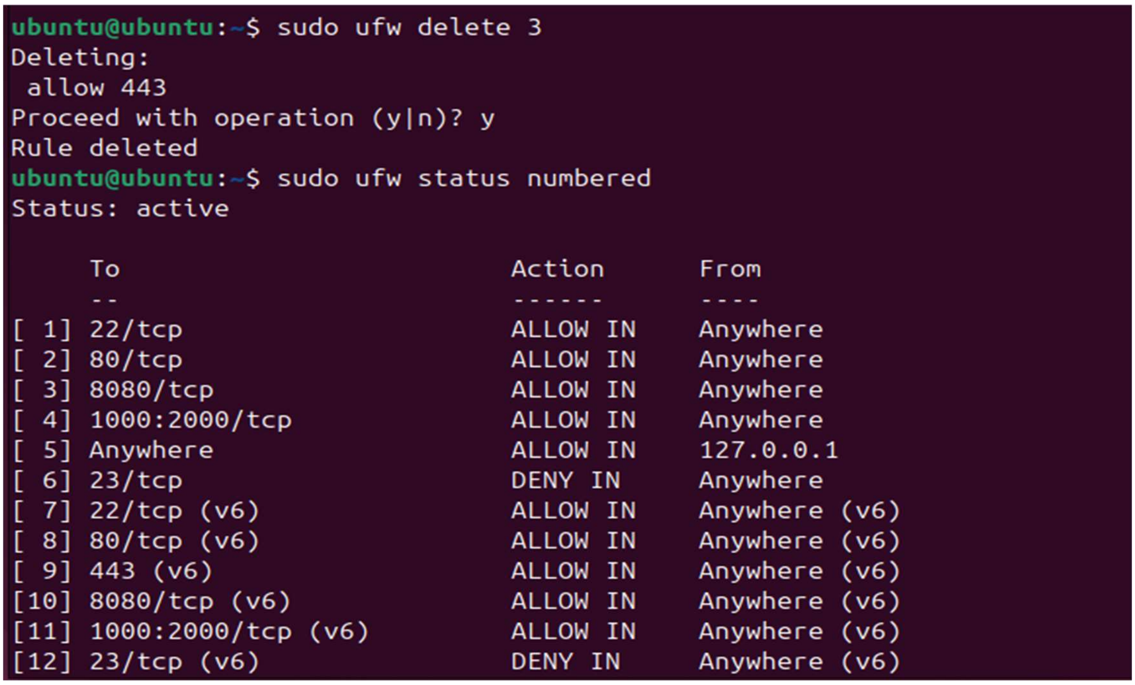
If we want to check the status in the numbered format, then we can use the following command:



```
ubuntu@ubuntu:~$ sudo ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 22/tcp                     ALLOW IN    Anywhere
[ 2] 80/tcp                     ALLOW IN    Anywhere
[ 3] 443                        ALLOW IN    Anywhere
[ 4] 8080/tcp                   ALLOW IN    Anywhere
[ 5] 1000:2000/tcp              ALLOW IN    Anywhere
[ 6] Anywhere                   ALLOW IN    127.0.0.1
[ 7] 23/tcp                     DENY IN     Anywhere
[ 8] 22/tcp (v6)                ALLOW IN    Anywhere (v6)
[ 9] 80/tcp (v6)                ALLOW IN    Anywhere (v6)
[10] 443 (v6)                   ALLOW IN    Anywhere (v6)
[11] 8080/tcp (v6)              ALLOW IN    Anywhere (v6)
[12] 1000:2000/tcp (v6)         ALLOW IN    Anywhere (v6)
[13] 23/tcp (v6)                DENY IN     Anywhere (v6)
```

5.4 Deleting any service in the firewall

We can delete any service in the firewall if we want.



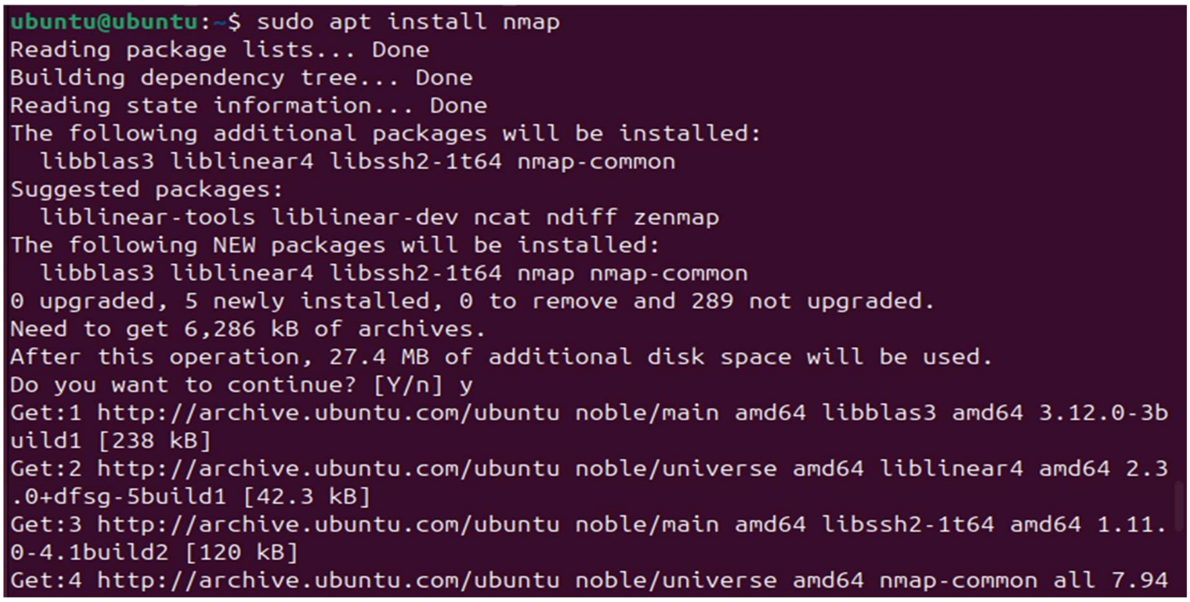
```
ubuntu@ubuntu:~$ sudo ufw delete 3
Deleting:
 allow 443
Proceed with operation (y|n)? y
Rule deleted
ubuntu@ubuntu:~$ sudo ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 22/tcp                     ALLOW IN    Anywhere
[ 2] 80/tcp                     ALLOW IN    Anywhere
[ 3] 8080/tcp                   ALLOW IN    Anywhere
[ 4] 1000:2000/tcp              ALLOW IN    Anywhere
[ 5] Anywhere                   ALLOW IN    127.0.0.1
[ 6] 23/tcp                     DENY IN     Anywhere
[ 7] 22/tcp (v6)                ALLOW IN    Anywhere (v6)
[ 8] 80/tcp (v6)                ALLOW IN    Anywhere (v6)
[ 9] 443 (v6)                   ALLOW IN    Anywhere (v6)
[10] 8080/tcp (v6)              ALLOW IN    Anywhere (v6)
[11] 1000:2000/tcp (v6)         ALLOW IN    Anywhere (v6)
[12] 23/tcp (v6)                DENY IN     Anywhere (v6)
```

6. FIREWALL TESTING

Testing the firewall rules is crucial to ensure they are functioning as expected.

6.1 Installing NMAP

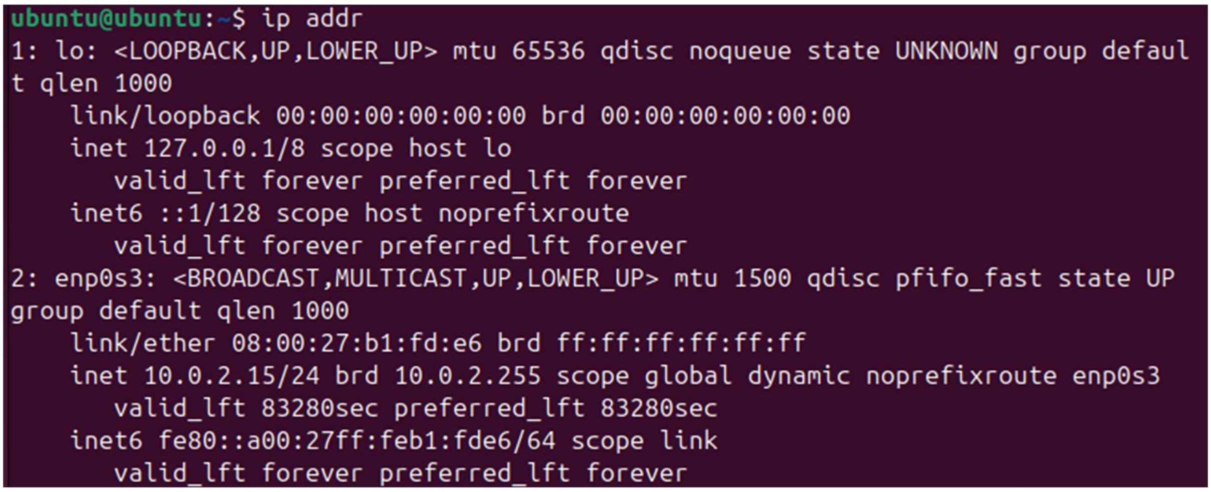
For testing the firewall, first, we must install a tool called NMAP which is used to scan IP addresses and ports in a network and to detect installed applications.



```
ubuntu@ubuntu:~$ sudo apt install nmap
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libblas3 liblinear4 libssh2-1t64 nmap-common
Suggested packages:
  liblinear-tools liblinear-dev ncat ndiff zenmap
The following NEW packages will be installed:
  libblas3 liblinear4 libssh2-1t64 nmap nmap-common
0 upgraded, 5 newly installed, 0 to remove and 289 not upgraded.
Need to get 6,286 kB of archives.
After this operation, 27.4 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://archive.ubuntu.com/ubuntu noble/main amd64 libblas3 amd64 3.12.0-3b
uild1 [238 kB]
Get:2 http://archive.ubuntu.com/ubuntu noble/universe amd64 liblinear4 amd64 2.3
.0+dfsg-5build1 [42.3 kB]
Get:3 http://archive.ubuntu.com/ubuntu noble/main amd64 libssh2-1t64 amd64 1.11.
0-4.1build2 [120 kB]
Get:4 http://archive.ubuntu.com/ubuntu noble/universe amd64 nmap-common all 7.94
```

6.2 Look for IP Addresses

Next, we have to look for IP addresses present on our server.



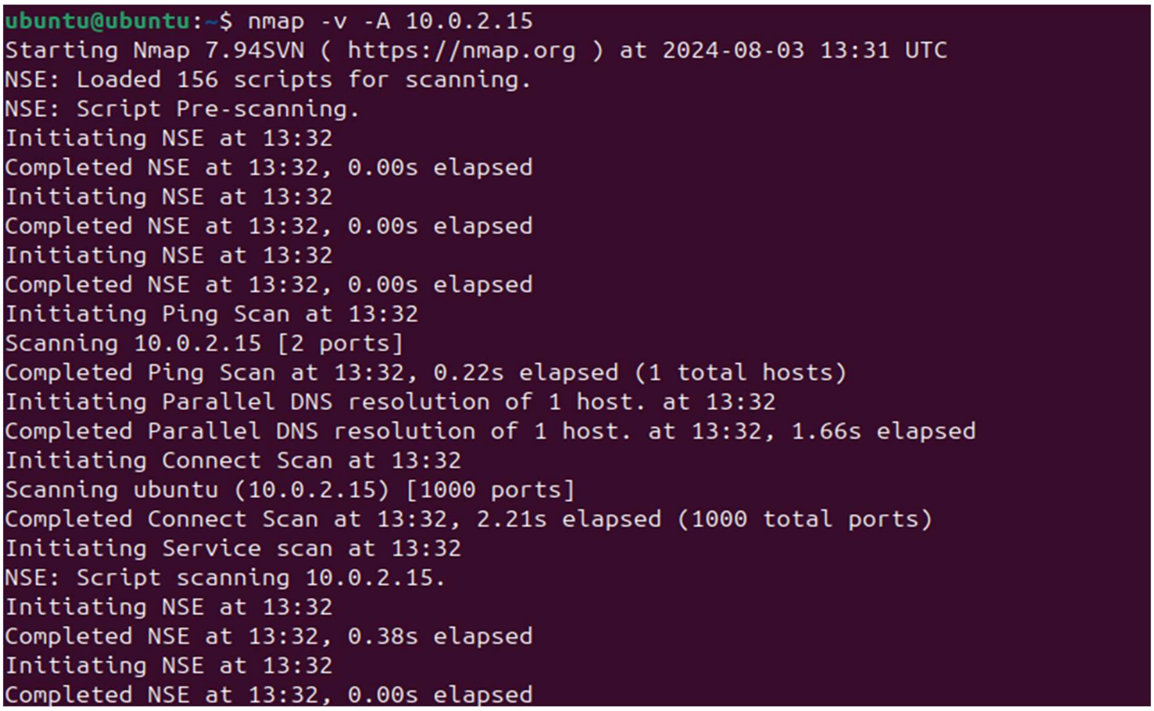
```
ubuntu@ubuntu:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
group default qlen 1000
    link/ether 08:00:27:b1:fd:e6 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
       valid_lft 83280sec preferred_lft 83280sec
    inet6 fe80::a00:27ff:feb1:fde6/64 scope link
       valid_lft forever preferred_lft forever
```

Here, the first address is 127.0.0.1 which is the IP address of the local host.

The second address is 10.0.2.15 which is the IP address of the firewall which we had created.

6.3 Test the firewall

Next, we have to scan our firewall to test specific port access.



```
ubuntu@ubuntu:~$ nmap -v -A 10.0.2.15
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-03 13:31 UTC
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 13:32
Completed NSE at 13:32, 0.00s elapsed
Initiating NSE at 13:32
Completed NSE at 13:32, 0.00s elapsed
Initiating NSE at 13:32
Completed NSE at 13:32, 0.00s elapsed
Initiating Ping Scan at 13:32
Scanning 10.0.2.15 [2 ports]
Completed Ping Scan at 13:32, 0.22s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:32
Completed Parallel DNS resolution of 1 host. at 13:32, 1.66s elapsed
Initiating Connect Scan at 13:32
Scanning ubuntu (10.0.2.15) [1000 ports]
Completed Connect Scan at 13:32, 2.21s elapsed (1000 total ports)
Initiating Service scan at 13:32
NSE: Script scanning 10.0.2.15.
Initiating NSE at 13:32
Completed NSE at 13:32, 0.38s elapsed
Initiating NSE at 13:32
Completed NSE at 13:32, 0.00s elapsed
```