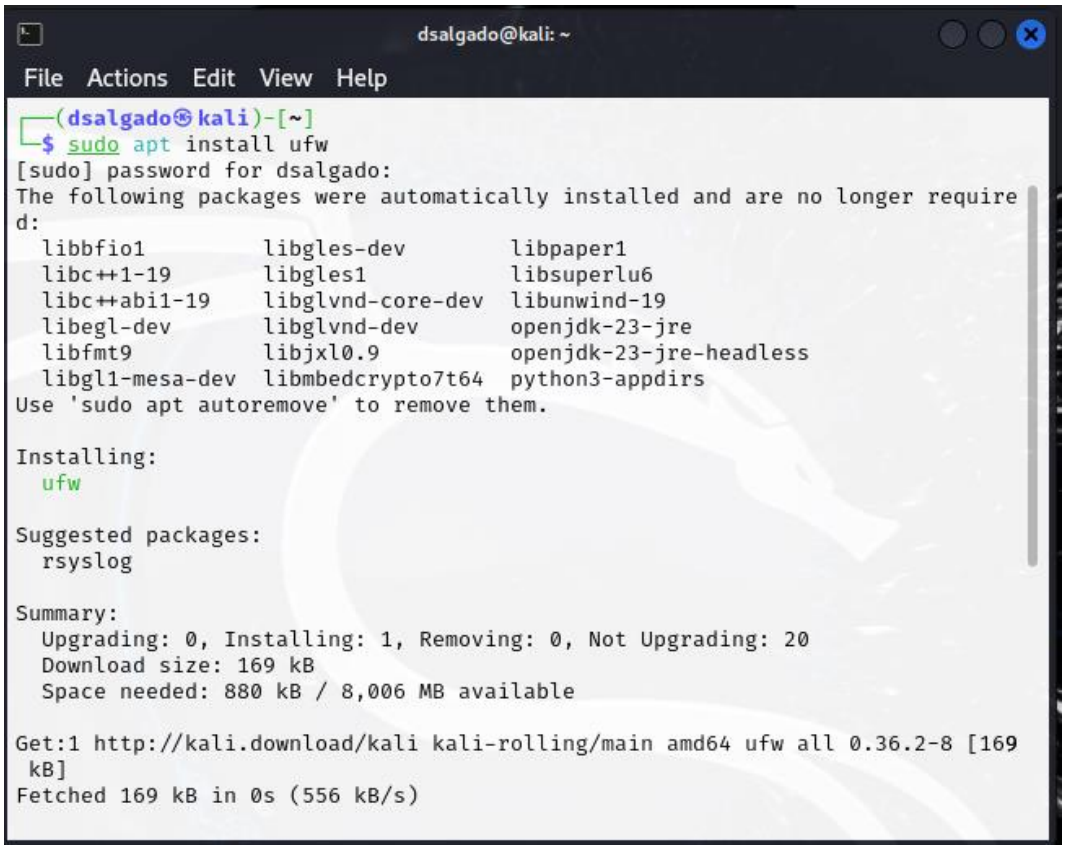
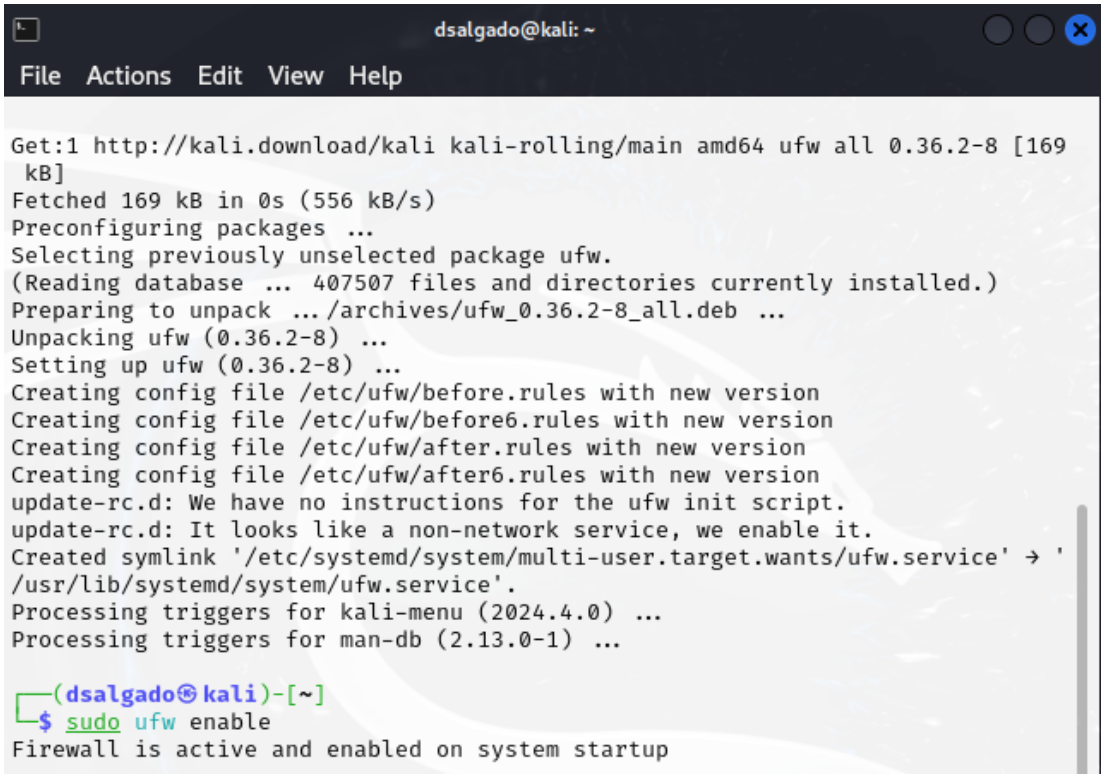
Build and Configure a Firewall

Step 1: Install UFW (Uncomplicated Firewall)



2: Enable UFW (By default it comes disabled)



3: Allow SSH connections

```
┌──(dsalgado㉿kali)-[~]
└─$ sudo ufw allow ssh
Rule added
Rule added (v6)
```

4: Allow service of HTTP and HTTPS

```
┌──(dsalgado㉿kali)-[~]
└─$ sudo ufw allow http
Rule added
Rule added (v6)

┌──(dsalgado㉿kali)-[~]
└─$ sudo ufw allow https
Rule added
Rule added (v6)
```

5: Allow traffic only through port 8080

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

6: Allow traffic to a certain range of ports

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

7: Allow a specific IP address (For example, 192.168.1.100)

```
┌──(dsalgado㉿kali)-[~]
└─$ sudo ufw allow from 192.168.1.100
Rule added
```

8: Allow specific subnets

```
┌──(dsalgado㉿kali)-[~]
└─$ sudo ufw allow from 192.168.1.0/24
Rule added
```

Now instead of allowing I will be denying different things

9: Deny a specific port

```
┌──(dsalgado㉿kali)-[~]
└─$ sudo ufw deny 23/tcp
Rule added
Rule added (v6)
```

10: Deny a specific IP address

```
┌──(dsalgado㉿kali)-[~]
└─$ sudo ufw deny from 203.0.113.0
Rule added
```

11: View UFW status and rules

```
┌──(dsalgado㉿kali)-[~]
└─$ 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    192.168.1.100
Anywhere                   ALLOW IN    192.168.1.0/24
23/tcp                     DENY IN     Anywhere
Anywhere                   DENY IN     203.0.113.0
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)
```

12: If I want to delete and specific rule, I can number the rules by

```
┌──(dsalgado㉿kali)-[~]
└─$ 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    192.168.1.100
[ 7] Anywhere                   ALLOW IN    192.168.1.0/24
[ 8] 23/tcp                     DENY IN     Anywhere
[ 9] Anywhere                   DENY IN     203.0.113.0
[10] 22/tcp (v6)                ALLOW IN    Anywhere (v6)
[11] 80/tcp (v6)                ALLOW IN    Anywhere (v6)
[12] 443 (v6)                   ALLOW IN    Anywhere (v6)
[13] 8080/tcp (v6)              ALLOW IN    Anywhere (v6)
[14] 1000:2000/tcp (v6)         ALLOW IN    Anywhere (v6)
[15] 23/tcp (v6)                DENY IN     Anywhere (v6)
```

And then for example, I can erase rule #5 by

```
┌──(dsalgado㉿kali)-[~]
└─$ sudo ufw delete 5
Deleting:
 allow 1000:2000/tcp
Proceed with operation (y|n)? y
Rule deleted
```

13: I can have advanced configurations to my firewall like for example logging by

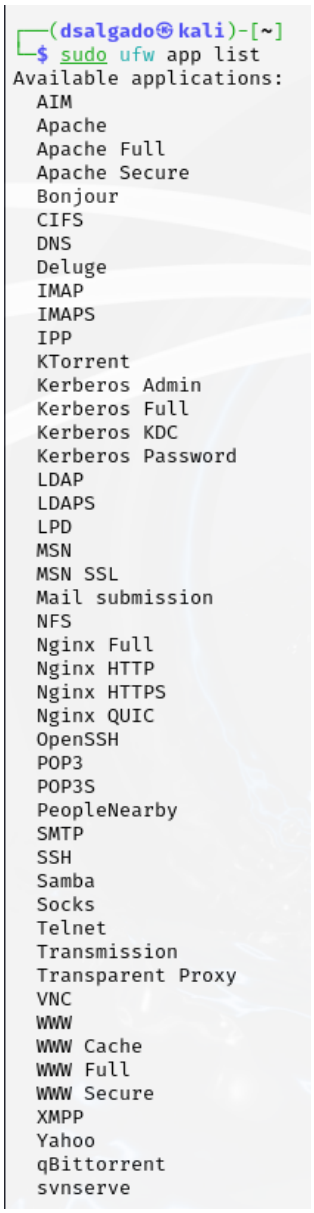
```
┌──(dsalgado㉿kali)-[~]
└─$ sudo ufw logging on
Logging enabled
```

14: I can set default policies too by

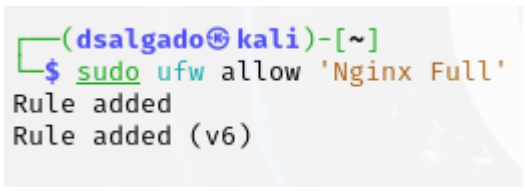
```
┌──(dsalgado㉿kali)-[~]
└─$ sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)

┌──(dsalgado㉿kali)-[~]
└─$ sudo ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)
```

15: I can also check specific applications by



And allow just one, for example by



Conclusion: I have successfully set up and configured a firewall using UFW. This setup will help me protect my network from unauthorized access and potential threats.