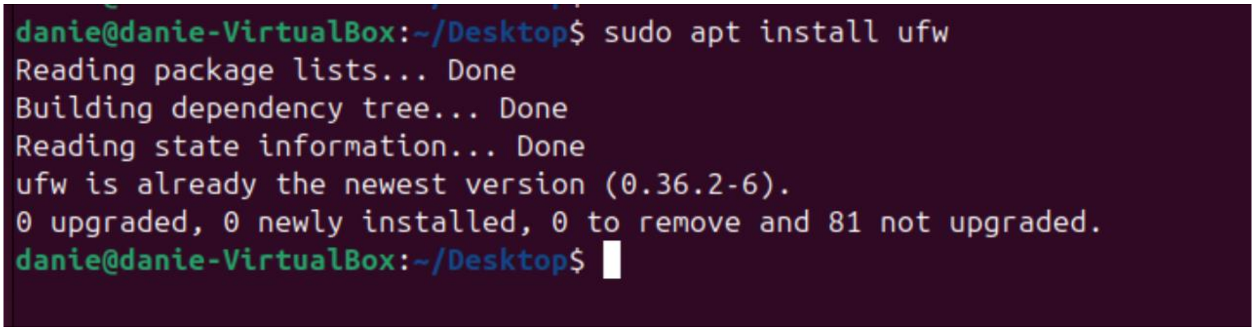
Project: Building and configuring a Firewall.

Requirements: Ubuntu Virtual Machine and Kali Linux VM.

Setting up Uncomplicated Firewall.

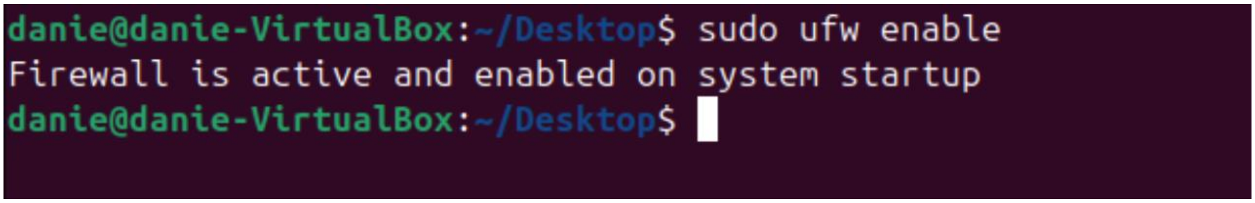
1. Updated Ubuntu and Kali Linux Systems

2. Installed Uncomplicated fire wall (UFW).



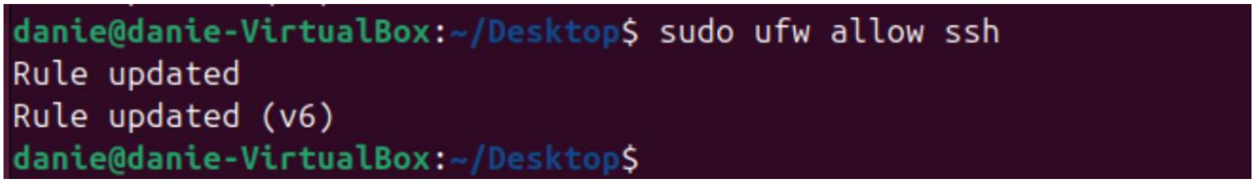
```
danie@danie-VirtualBox:~/Desktop$ sudo apt install ufw
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
ufw is already the newest version (0.36.2-6).
0 upgraded, 0 newly installed, 0 to remove and 81 not upgraded.
danie@danie-VirtualBox:~/Desktop$ 
```

3. Enabled UFW

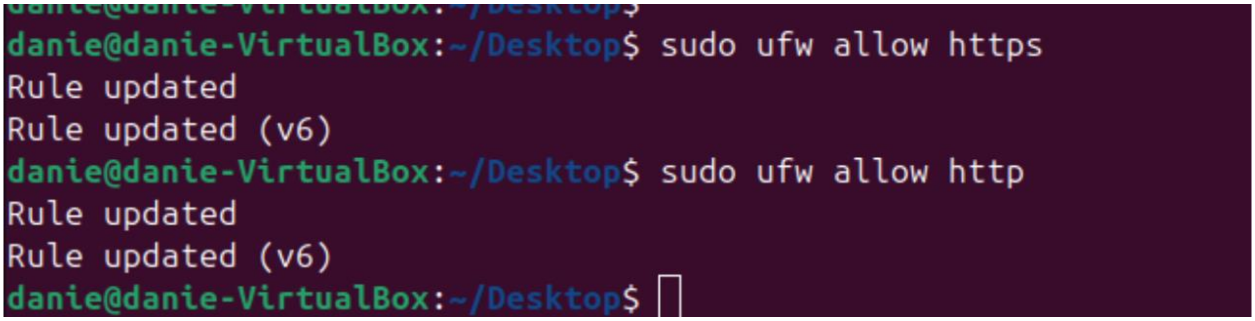


```
danie@danie-VirtualBox:~/Desktop$ sudo ufw enable
Firewall is active and enabled on system startup
danie@danie-VirtualBox:~/Desktop$ 
```

4. Allowed SSH connections and specific service ports.

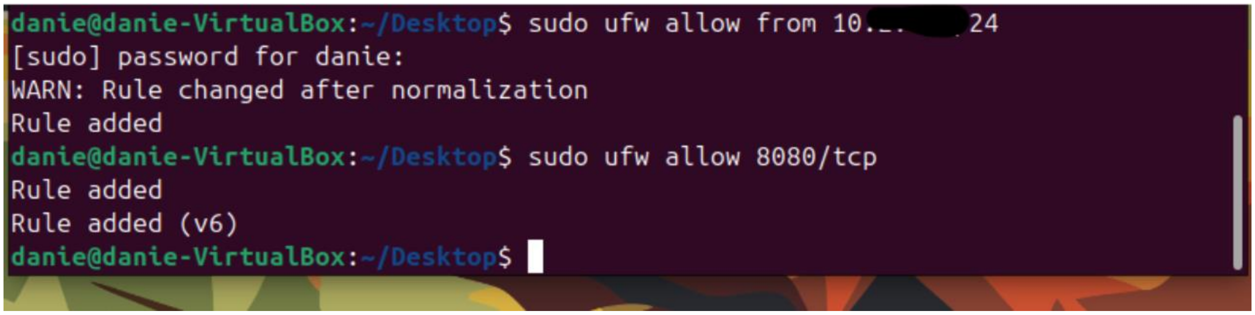


```
danie@danie-VirtualBox:~/Desktop$ sudo ufw allow ssh
Rule updated
Rule updated (v6)
danie@danie-VirtualBox:~/Desktop$
```



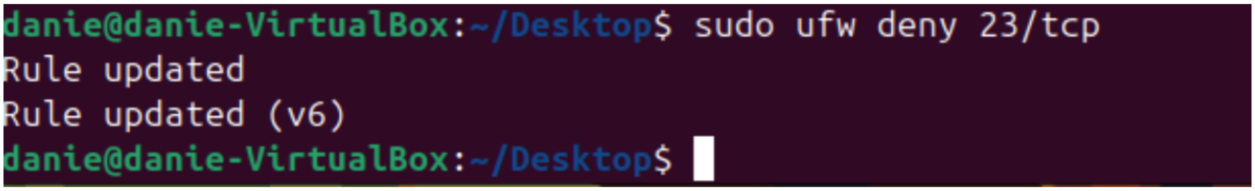
```
danie@danie-VirtualBox:~/Desktop$
danie@danie-VirtualBox:~/Desktop$ sudo ufw allow https
Rule updated
Rule updated (v6)
danie@danie-VirtualBox:~/Desktop$ sudo ufw allow http
Rule updated
Rule updated (v6)
danie@danie-VirtualBox:~/Desktop$ 
```

5. Allowing specific IP address and Port ranges.



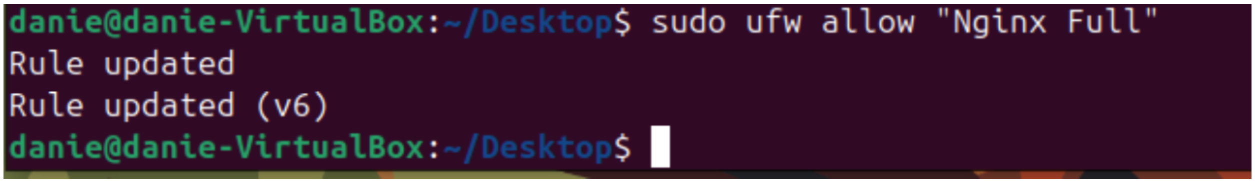
```
danie@danie-VirtualBox:~/Desktop$ sudo ufw allow from 10.[redacted]24
[sudo] password for danie:
WARN: Rule changed after normalization
Rule added
danie@danie-VirtualBox:~/Desktop$ sudo ufw allow 8080/tcp
Rule added
Rule added (v6)
danie@danie-VirtualBox:~/Desktop$
```

6. Denying Ports.



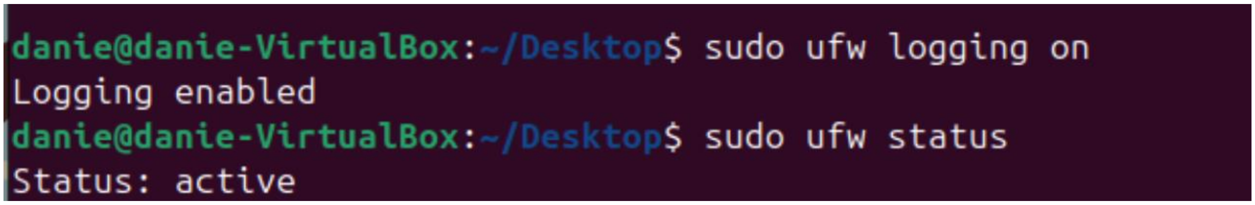
```
danie@danie-VirtualBox:~/Desktop$ sudo ufw deny 23/tcp
Rule updated
Rule updated (v6)
danie@danie-VirtualBox:~/Desktop$
```

7. Allowing specific Applications.



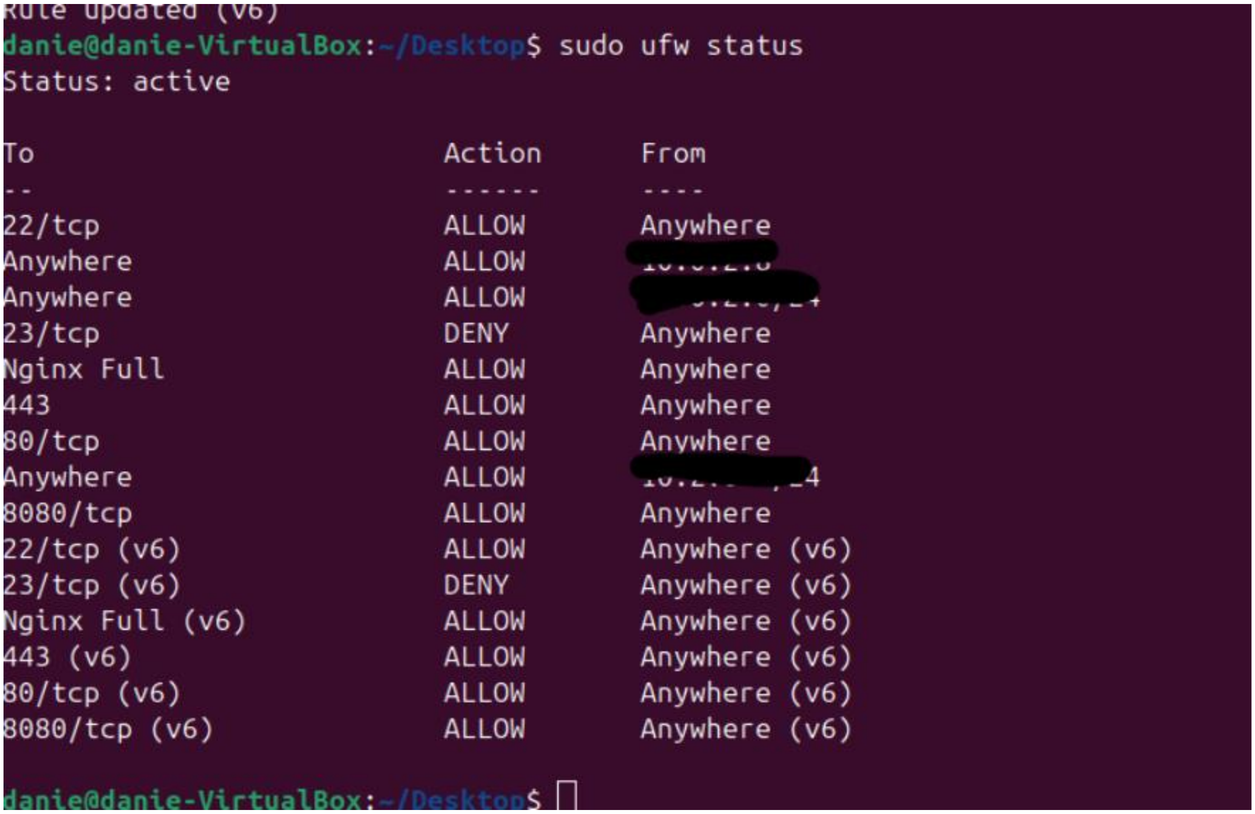
```
danie@danie-VirtualBox:~/Desktop$ sudo ufw allow "Nginx Full"
Rule updated
Rule updated (v6)
danie@danie-VirtualBox:~/Desktop$
```

8.Enabling Logging



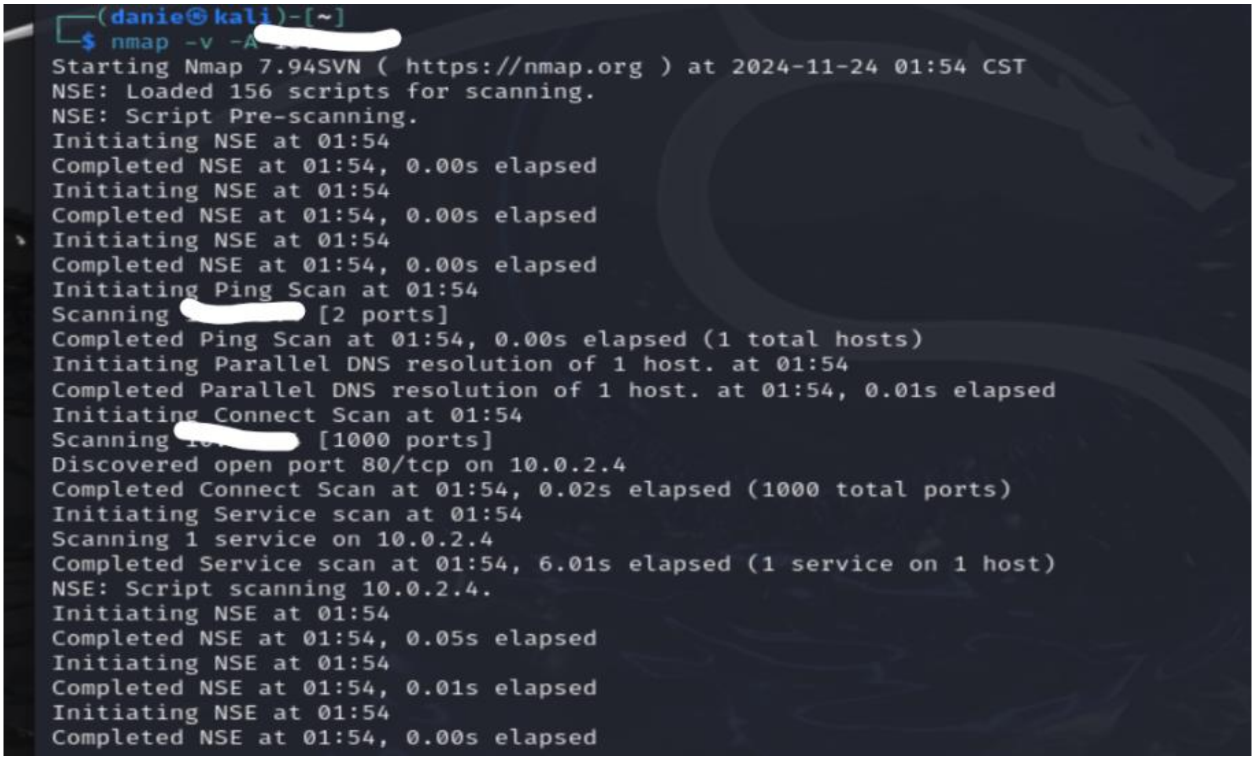
```
danie@danie-VirtualBox:~/Desktop$ sudo ufw logging on
Logging enabled
danie@danie-VirtualBox:~/Desktop$ sudo ufw status
Status: active
```

9. Firewall status.

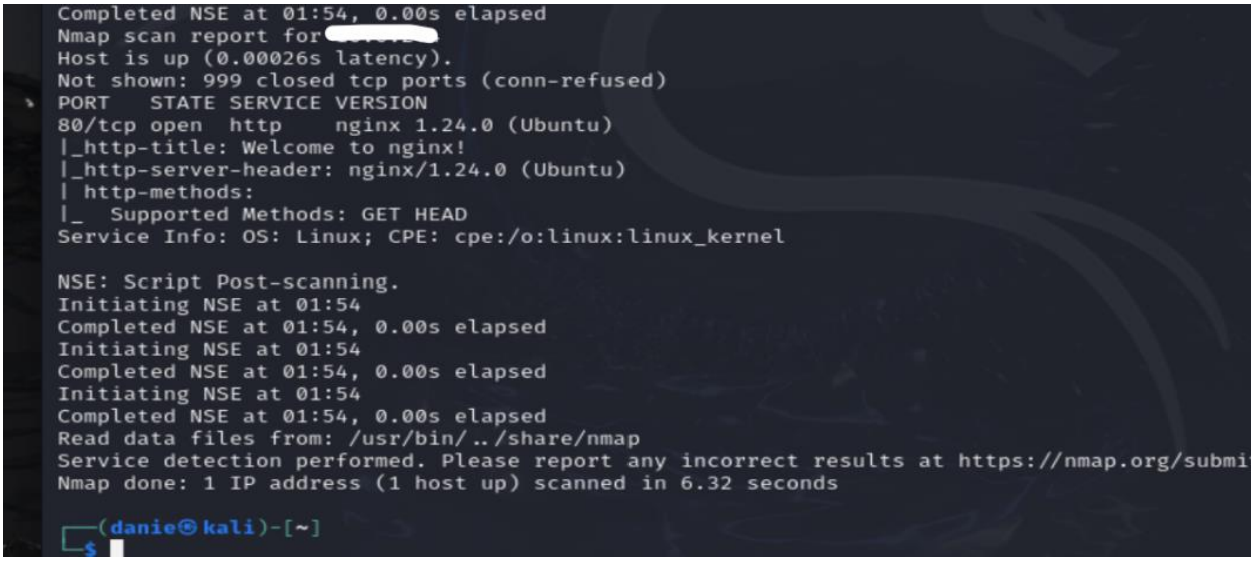


```
Rule updated (v6)
danie@danie-VirtualBox:~/Desktop$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW       Anywhere
Anywhere                   ALLOW       [redacted]
Anywhere                   ALLOW       [redacted]
23/tcp                     DENY        Anywhere
Nginx Full                 ALLOW       Anywhere
443                        ALLOW       Anywhere
80/tcp                     ALLOW       Anywhere
Anywhere                   ALLOW       [redacted]
8080/tcp                   ALLOW       Anywhere
22/tcp (v6)                ALLOW       Anywhere (v6)
23/tcp (v6)                DENY        Anywhere (v6)
Nginx Full (v6)            ALLOW       Anywhere (v6)
443 (v6)                   ALLOW       Anywhere (v6)
80/tcp (v6)                ALLOW       Anywhere (v6)
8080/tcp (v6)              ALLOW       Anywhere (v6)

danie@danie-VirtualBox:~/Desktop$ 
```

10. Testing Firewall using Nmap on Kali machine to check for open ports.



```
┌──(danie㉿kali)-[~]
└─$ nmap -v -A [redacted]
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-24 01:54 CST
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 01:54
Completed NSE at 01:54, 0.00s elapsed
Initiating NSE at 01:54
Completed NSE at 01:54, 0.00s elapsed
Initiating NSE at 01:54
Completed NSE at 01:54, 0.00s elapsed
Initiating Ping Scan at 01:54
Scanning [redacted] [2 ports]
Completed Ping Scan at 01:54, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 01:54
Completed Parallel DNS resolution of 1 host. at 01:54, 0.01s elapsed
Initiating Connect Scan at 01:54
Scanning [redacted] [1000 ports]
Discovered open port 80/tcp on 10.0.2.4
Completed Connect Scan at 01:54, 0.02s elapsed (1000 total ports)
Initiating Service scan at 01:54
Scanning 1 service on 10.0.2.4
Completed Service scan at 01:54, 6.01s elapsed (1 service on 1 host)
NSE: Script scanning 10.0.2.4.
Initiating NSE at 01:54
Completed NSE at 01:54, 0.05s elapsed
Initiating NSE at 01:54
Completed NSE at 01:54, 0.01s elapsed
Initiating NSE at 01:54
Completed NSE at 01:54, 0.00s elapsed
```



```
Completed NSE at 01:54, 0.00s elapsed
Nmap scan report for [redacted]
Host is up (0.00026s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
80/tcp open  http    nginx 1.24.0 (Ubuntu)
|_http-title: Welcome to nginx!
|_http-server-header: nginx/1.24.0 (Ubuntu)
| http-methods:
|_  Supported Methods: GET HEAD
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
Initiating NSE at 01:54
Completed NSE at 01:54, 0.00s elapsed
Initiating NSE at 01:54
Completed NSE at 01:54, 0.00s elapsed
Initiating NSE at 01:54
Completed NSE at 01:54, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submi
Nmap done: 1 IP address (1 host up) scanned in 6.32 seconds

┌──(danie㉿kali)-[~]
└─$ 
```

Created a fire wall with configured rules and monitored logging.