Internship: Cyber Security Internship

Name: Adil Firoz

Date: 29 January 2026

Operating System: Ubuntu Linux

Tool Used: UFW

Objective

The objective of this task was to configure and manage a host-based firewall using **UFW** on Ubuntu. The task involved allowing and denying specific ports, blocking an IP address, verifying network connectivity, and enabling firewall logging.

Step-by-Step Implementation

Step 1: Install and Enable UFW

Initially, the ufw command was not found, indicating that UFW was not installed. After installation, UFW was enabled successfully.

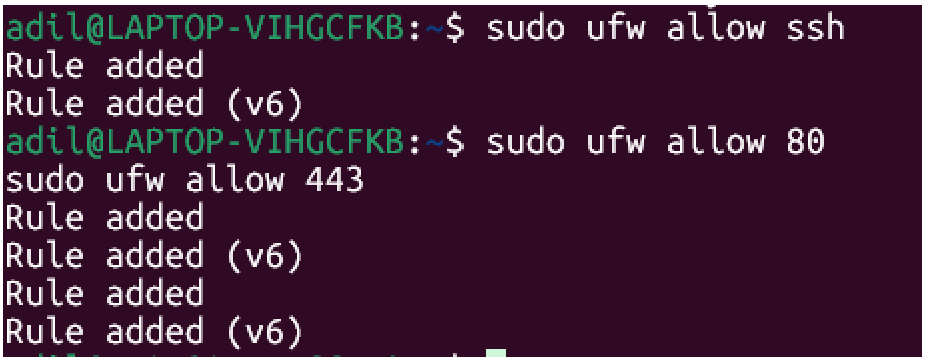
Step 2: Allow Required Services

The following essential services were allowed through the firewall:

- SSH (Port 22)
- HTTP (Port 80)
- HTTPS (Port 443)

Commands used:

Screenshot 2: Allow rules for SSH, HTTP, and HTTPS



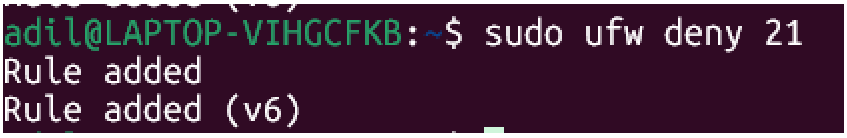
```
adil@LAPTOP-VIHGCFKB:~$ sudo ufw allow ssh
Rule added
Rule added (v6)
adil@LAPTOP-VIHGCFKB:~$ sudo ufw allow 80
sudo ufw allow 443
Rule added
Rule added (v6)
Rule added
Rule added (v6)
```

Step 3: Deny Insecure Services

To improve security, FTP (Port 21) was blocked:

sudo ufw deny 21

Screenshot 3: Deny rule for port 21



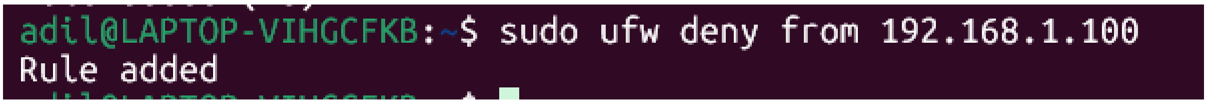
```
adil@LAPTOP-VIHGCFKB:~$ sudo ufw deny 21
Rule added
Rule added (v6)
```

Step 4: Block a Specific IP Address

A specific IP address was blocked to simulate access restriction:

sudo ufw deny from 192.168.1.100

Screenshot 4: IP-based deny rule



```
adil@LAPTOP-VIHGCFKB:~$ sudo ufw deny from 192.168.1.100
Rule added
```

Step 5: Verify Firewall Rules

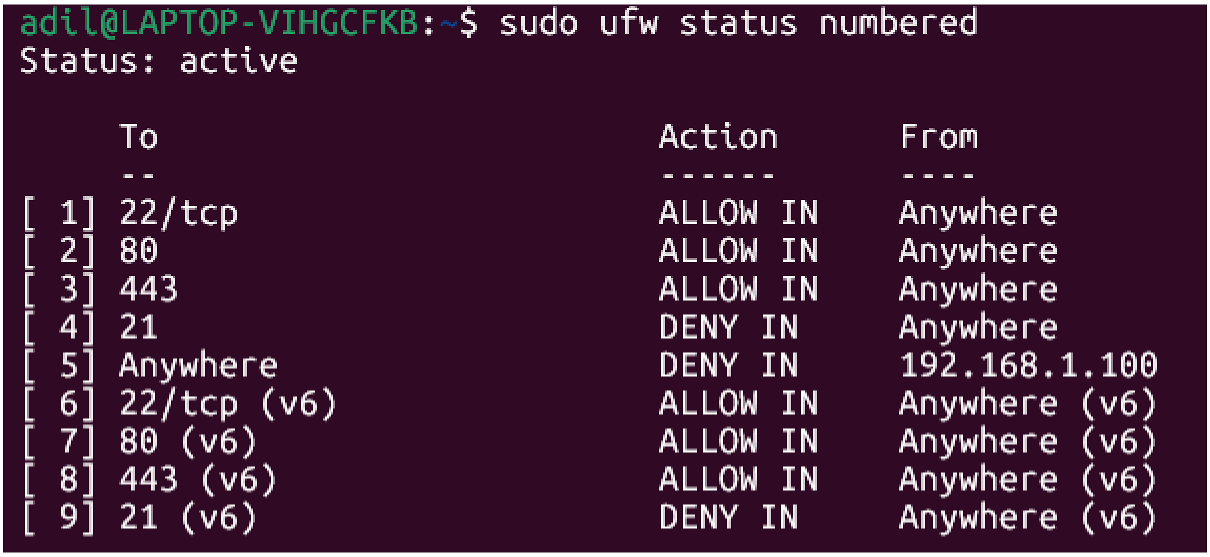
All configured rules were verified using:

sudo ufw status numbered

The output confirmed:

- Allowed ports: 22, 80, 443
- Denied port: 21
- Blocked IP: 192.168.1.100
- IPv6 rules applied automatically

Screenshot 5: UFW status numbered output



```
adil@LAPTOP-VIHGCFKB:~$ sudo ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 22/tcp                     ALLOW IN    Anywhere
[ 2] 80                         ALLOW IN    Anywhere
[ 3] 443                        ALLOW IN    Anywhere
[ 4] 21                         DENY IN     Anywhere
[ 5] Anywhere                   DENY IN     192.168.1.100
[ 6] 22/tcp (v6)                ALLOW IN    Anywhere (v6)
[ 7] 80 (v6)                    ALLOW IN    Anywhere (v6)
[ 8] 443 (v6)                   ALLOW IN    Anywhere (v6)
[ 9] 21 (v6)                    DENY IN     Anywhere (v6)
```

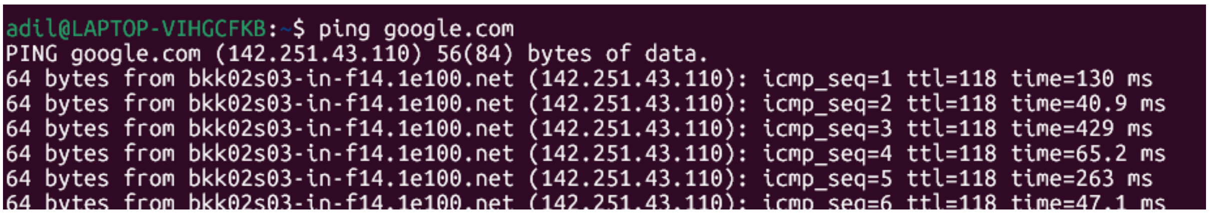
Step 6: Network Connectivity Test

Internet connectivity was tested using:

ping google.com

The successful replies confirmed that firewall rules did not block outbound traffic.

Screenshot 6: Successful ping test



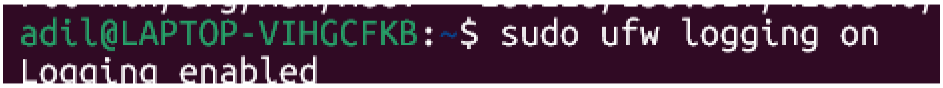
```
adil@LAPTOP-VIHGCFKB:~$ ping google.com
PING google.com (142.251.43.110) 56(84) bytes of data.
64 bytes from bkk02s03-in-f14.1e100.net (142.251.43.110): icmp_seq=1 ttl=118 time=130 ms
64 bytes from bkk02s03-in-f14.1e100.net (142.251.43.110): icmp_seq=2 ttl=118 time=40.9 ms
64 bytes from bkk02s03-in-f14.1e100.net (142.251.43.110): icmp_seq=3 ttl=118 time=429 ms
64 bytes from bkk02s03-in-f14.1e100.net (142.251.43.110): icmp_seq=4 ttl=118 time=65.2 ms
64 bytes from bkk02s03-in-f14.1e100.net (142.251.43.110): icmp_seq=5 ttl=118 time=263 ms
64 bytes from bkk02s03-in-f14.1e100.net (142.251.43.110): icmp_seq=6 ttl=118 time=47.1 ms
```

Step 7: Enable Firewall Logging

Firewall logging was enabled to track allowed and denied traffic:

sudo ufw logging on

Screenshot 7: UFW logging enabled



```
adil@LAPTOP-VIHGCFKB:~$ sudo ufw logging on
Logging enabled
```

Result

The firewall was successfully configured using UFW. Essential services were allowed, insecure services were blocked, a specific IP address was denied, and logging was enabled. Network connectivity remained intact, confirming correct firewall behavior.

Conclusion

This task demonstrated practical firewall management using UFW on Ubuntu. Proper firewall configuration is critical for system security, and UFW provides a simple yet effective way to control network traffic and reduce attack surfaces.