Task 10: Firewall Configuration & Testing

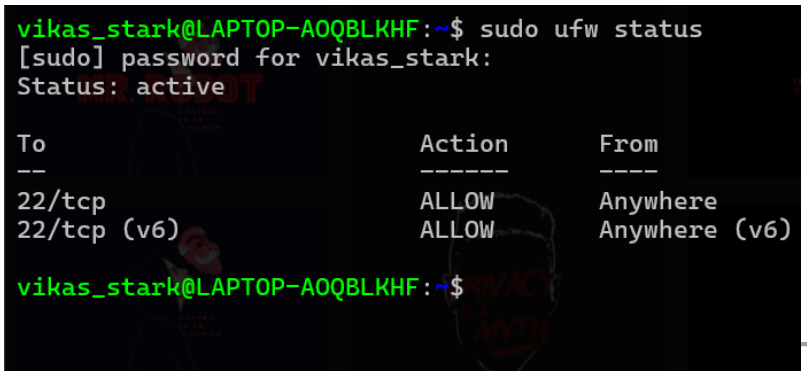
System Used

- OS: WSL (Ubuntu / Kali)
- Firewall Tool: UFW (Uncomplicated Firewall)

Step 1: Check Firewall Status

Open terminal and check whether firewall is installed and its current status.

sudo ufw status



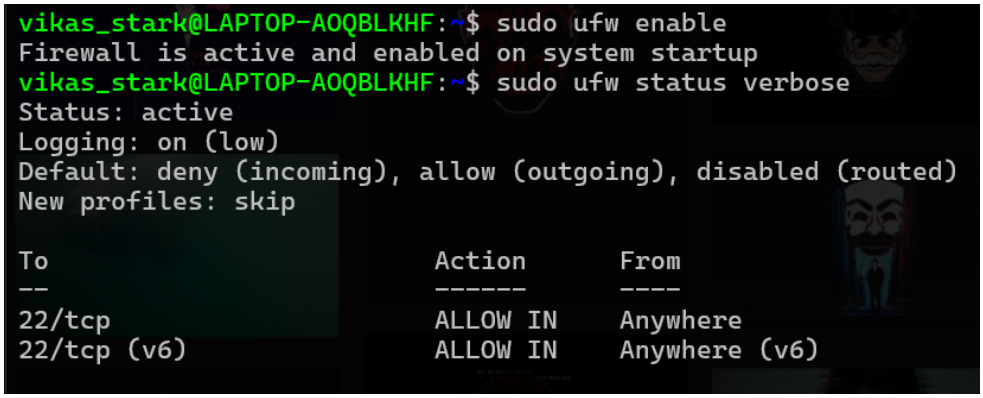
Step 2: Enable Firewall

Enable the firewall to start filtering traffic.

sudo ufw enable

Verify status again:

sudo ufw status verbose



Step 3: Allow Required Ports

Allow only necessary services.

Allow SSH (Port 22)

sudo ufw allow 22

Allow HTTP (Port 80)

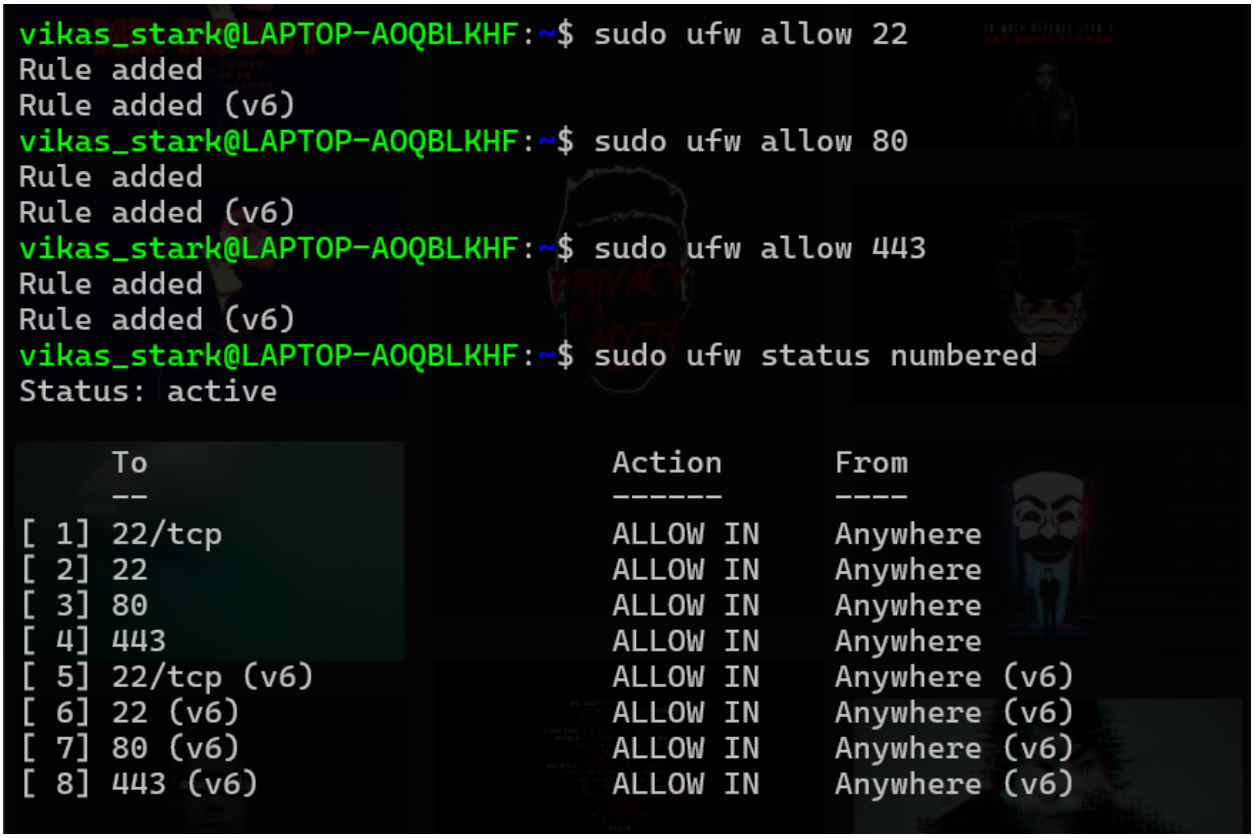
sudo ufw allow 80

Allow HTTPS (Port 443)

sudo ufw allow 443

Check rules:

sudo ufw status numbered



Step 4: Deny Unused / Risky Ports

Block a port that is not required (example: Port 23 – Telnet).

sudo ufw deny 23

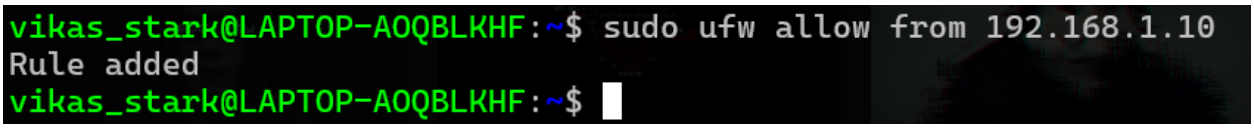
Step 5: Configure Inbound & Outbound Rules

Block Outbound Traffic on a Port (Example)

sudo ufw deny out 25

Allow Inbound Traffic from Specific IP (Optional)

sudo ufw allow from 192.168.1.10



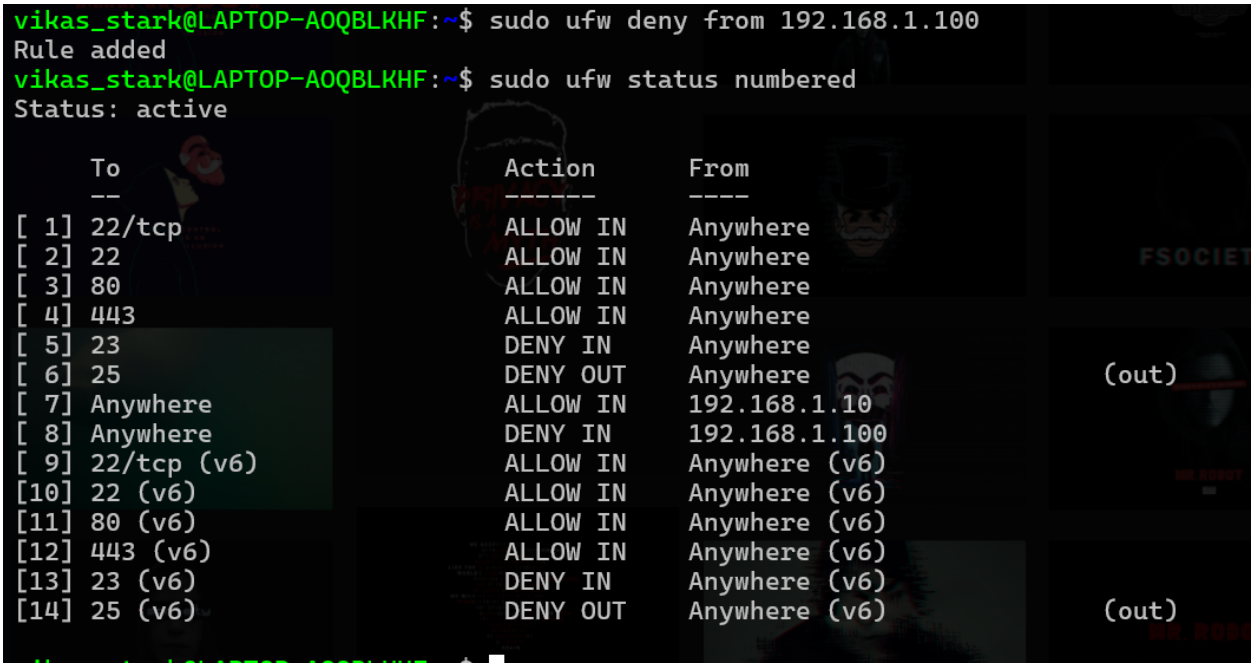
Step 6: Block a Malicious IP Address

Block a known malicious IP (example IP used for testing).

sudo ufw deny from 192.168.1.100

Verify:

sudo ufw status numbered



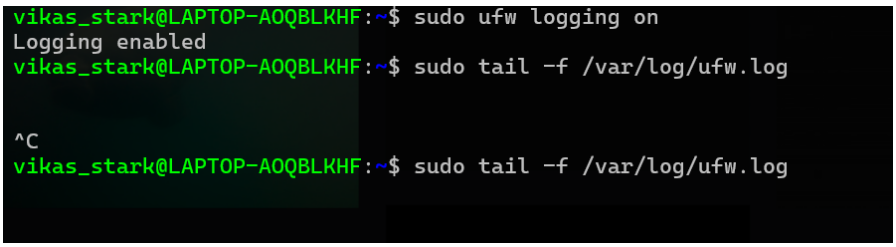
Step 7: Enable Firewall Logging

Enable logging to monitor traffic.

sudo ufw logging on

Check logs:

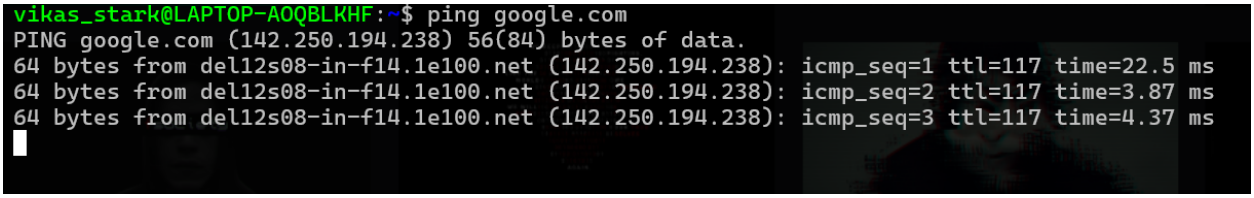
sudo tail -f /var/log/ufw.log



Step 8: Test Firewall Rules

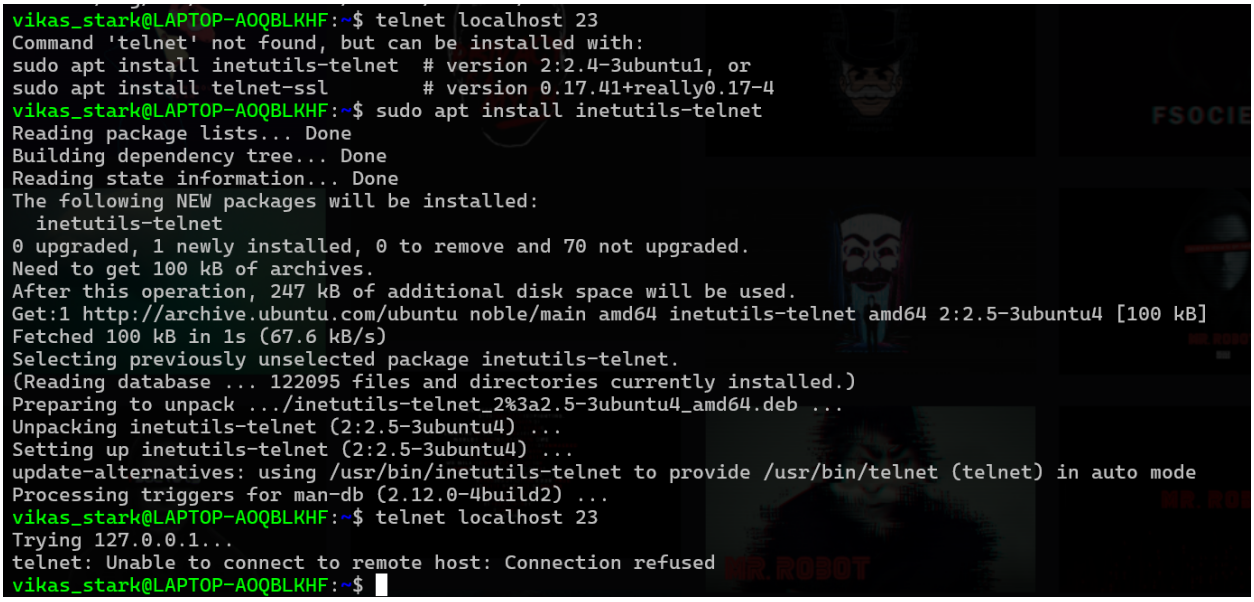
Test Allowed Port

ping google.com



Test Blocked Port

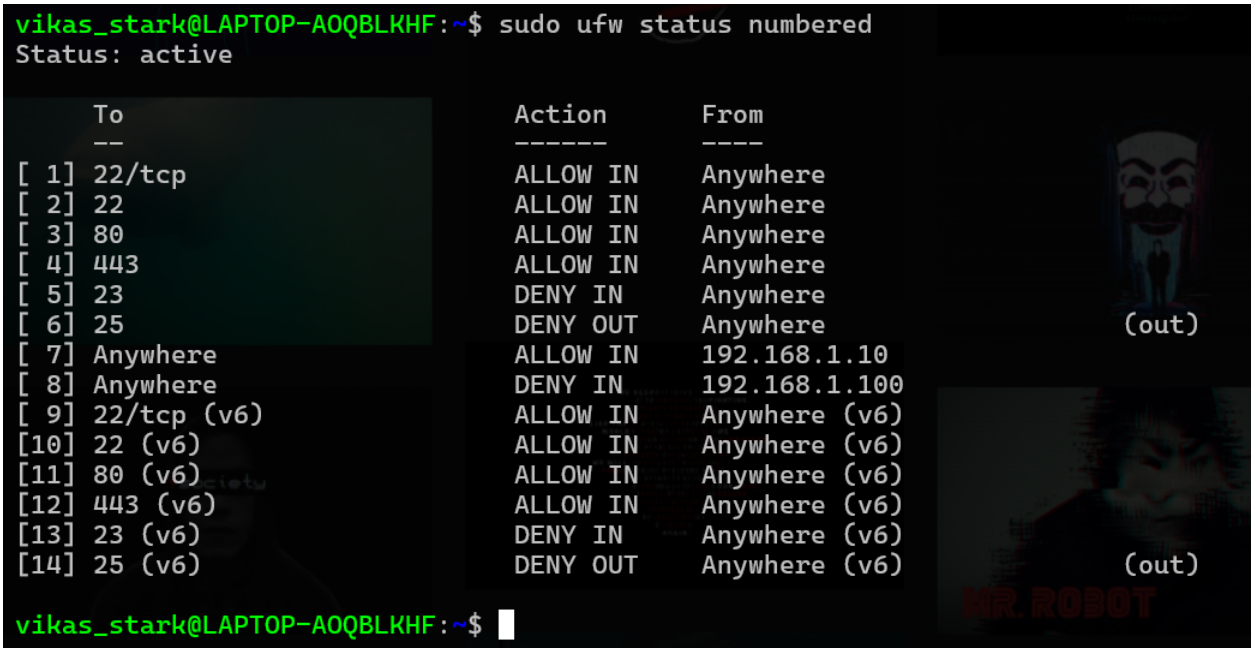
telnet localhost 23



Step 9: Document Firewall Rules

List rules with numbering:

sudo ufw status numbered



Step 10: Analyze Impact

- Unauthorized ports blocked
- Only required services accessible
- Malicious IP denied
- Logs help monitor suspicious traffic

Final Outcome

✓ Firewall successfully configured
✓ Ports allowed and denied correctly
✓ Malicious IP blocked
✓ Connectivity tested and verified
✓ Firewall management skills achieved