Setup and Use a Firewall on Windows/Linux

Objective

To configure and test basic firewall rules to allow or block network traffic using **Windows Firewall** or **UFW (Uncomplicated Firewall)** on Linux.

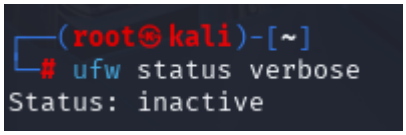
Tools Used

- **Operating System:** Kali Linux
- **Firewall Tool:** UFW
- **Terminal**

Steps Performed

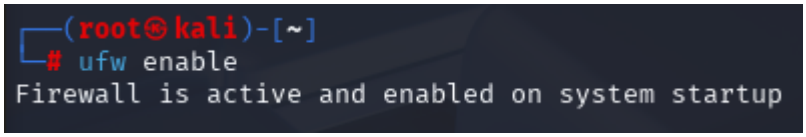
1. Checked Firewall Status

Command used (for Linux): sudo ufw status



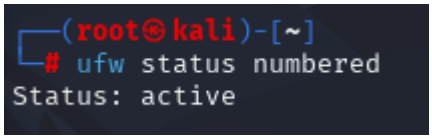
2. Enabled the Firewall

Command: sudo ufw enable



3. Listed Current Firewall Rules

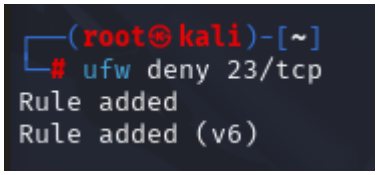
Command: sudo ufw status numbered



4. Added Rule to Block a Specific Port (e.g., 23 - Telnet)

Command:

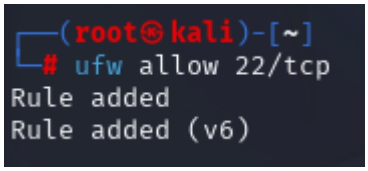
sudo ufw deny 23



Test Performed:
Attempted to connect to port 23 using telnet localhost 23 (or any similar method)
✅ Connection was blocked as expected.

5. Allowed SSH (Port 22)

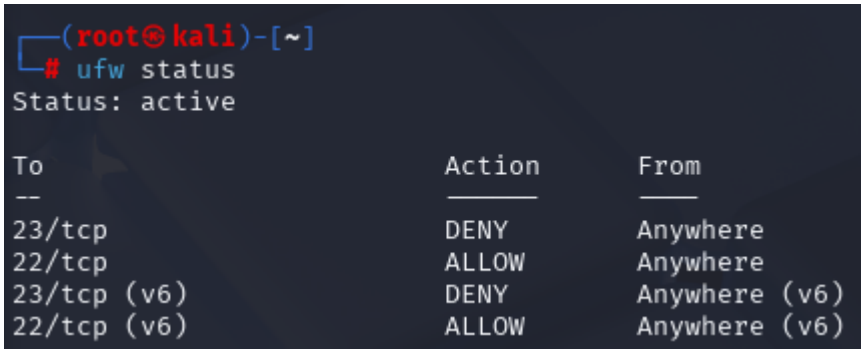
Command: sudo ufw allow 22



Test: Verified SSH connection — it worked successfully.

6. Verified Final Firewall Configuration

Command: sudo ufw status



Summary / Explanation

- **Firewall Function:**
  A firewall filters incoming and outgoing network traffic based on defined security rules. It helps block unauthorized access while permitting legitimate communication.
- **In this task:**
  - I learned how to enable and manage firewall rules.
  - Verified blocking/allowing specific ports.
  - Observed how firewall rules directly control network connections.

Conclusion

The firewall was successfully configured and tested.
Blocking and allowing specific ports demonstrated how traffic filtering works effectively. The system's security posture improved by restricting unnecessary open ports.