Firewall Configuration and Testing on Linux using UFW

Objective:
To configure and test basic firewall rules using UFW (Uncomplicated Firewall) to allow or block specific traffic, particularly SSH (port 22) and Telnet (port 23).

System Configuration and Tool Used

- **Operating System:** Ubuntu/Linux (Debian-based)
- **Firewall Tool:** UFW (Uncomplicated Firewall)
- **Terminal Access:** Required for command-line operations
- **Testing Tool:** telnet for verifying port accessibility

Steps, Commands, and Observations

✅ **1. Update Package List**

Command:

bash

sudo apt update

Purpose:
Ensures the latest package info is available for installing UFW.

✅ **2. Install UFW**

Command:

bash

sudo apt install ufw

Purpose:
Installs the Uncomplicated Firewall tool if it's not already installed.

✅ **3. Allow SSH Traffic (Port 22)**

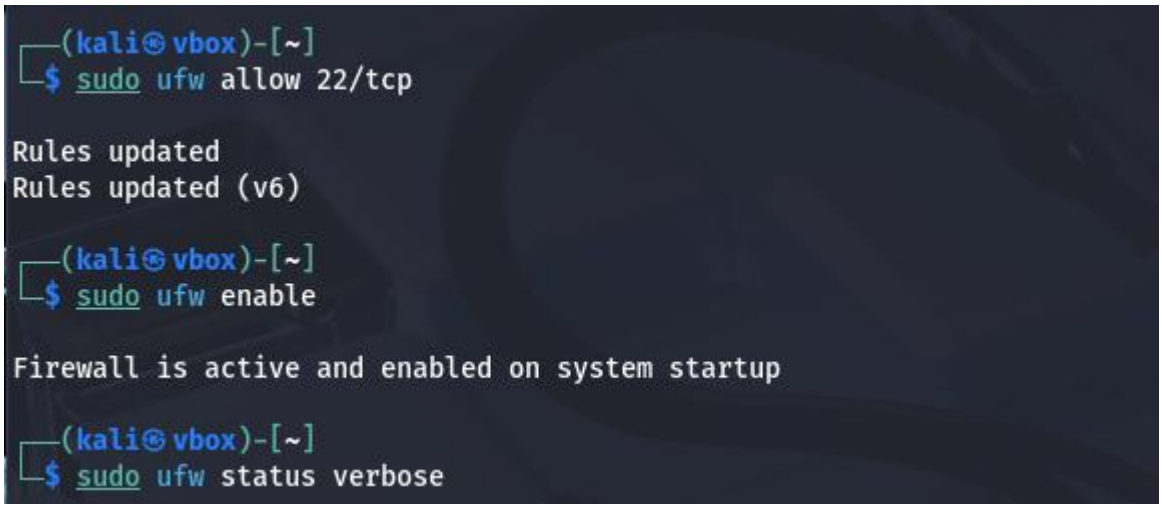
Command:

bash

sudo ufw allow 22/tcp

Purpose:
Allows SSH access to avoid being locked out of the system, especially useful for remote servers.

Screenshot 3: Output confirming SSH rule addition



✅ **4. Enable UFW**

Command:

bash

sudo ufw enable

Expected Output:

pgsql

CopyEdit

Command may disrupt existing ssh connections. Proceed with operation (y|n)? y

Firewall is active and enabled on system startup

Screenshot 4: Output showing UFW is enabled

✅ 5. View Current Firewall Rules

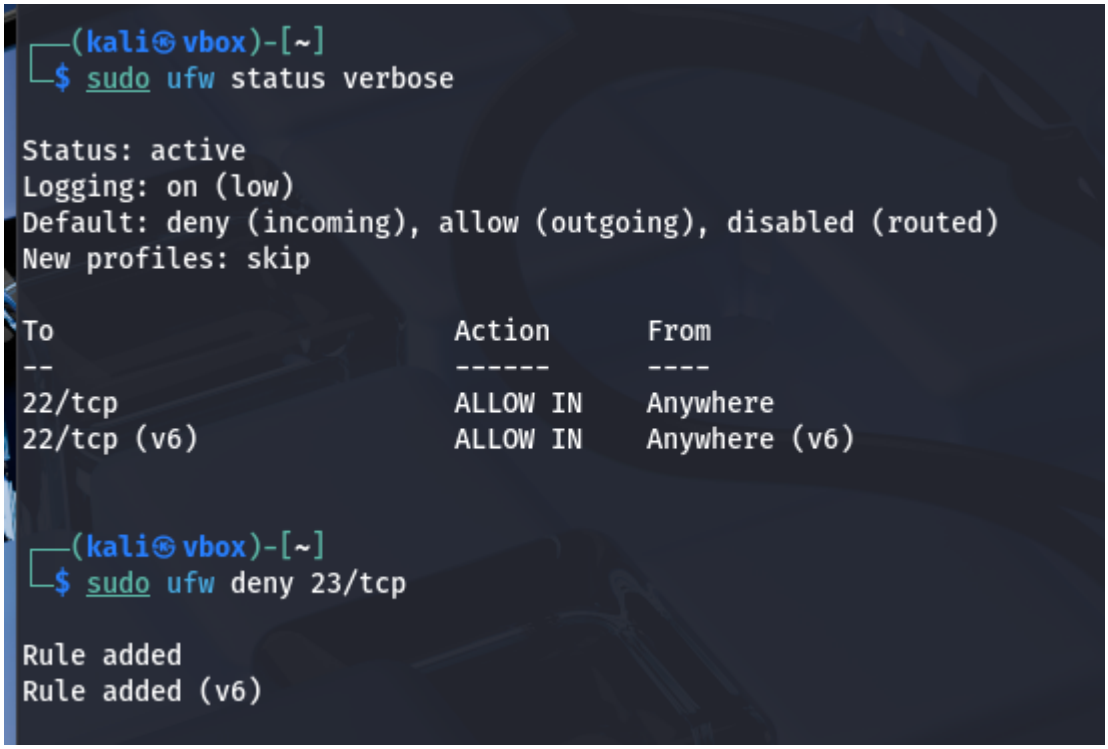
Command:

bash

sudo ufw status verbose

Purpose:
Displays currently active firewall rules in detail.

Screenshot 5: Output showing active rules



✅ 6. Block Telnet (Port 23)

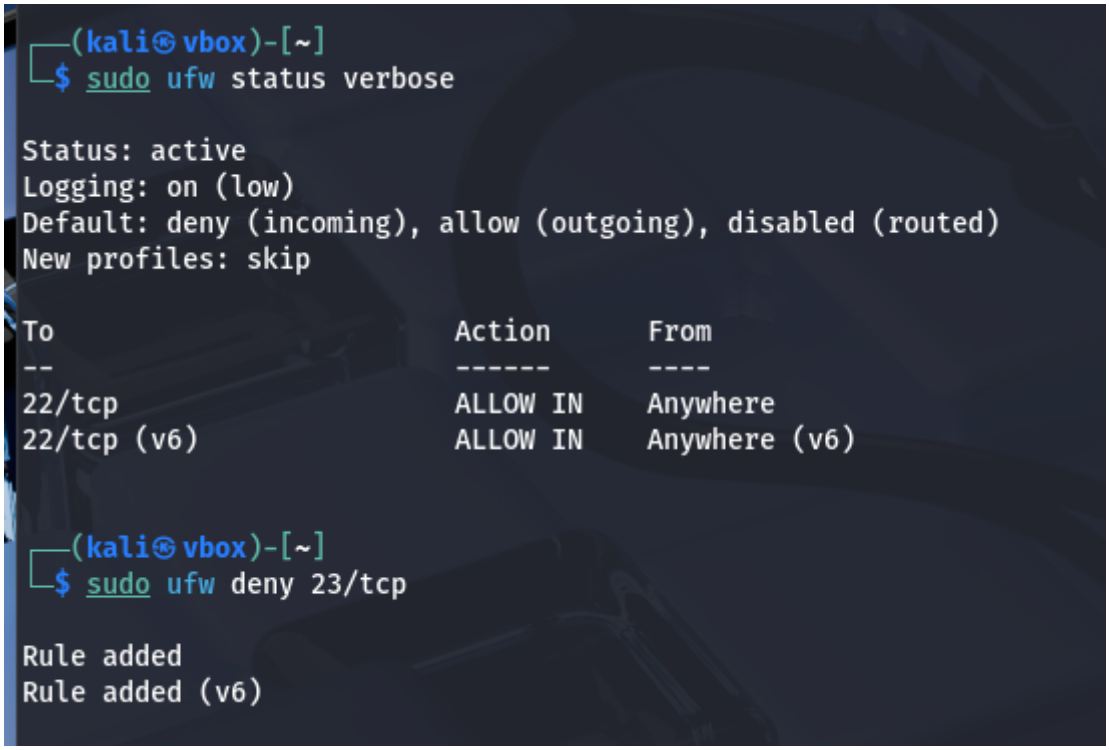
Command:

bash

sudo ufw deny 23/tcp

Purpose:
Adds a rule to block any inbound Telnet traffic, demonstrating how to filter traffic on a specific port.

Screenshot 6: Output confirming rule denial for port 23



✅ **7. Test Rule with Telnet**

Command:

bash

telnet localhost 23

Expected Output:

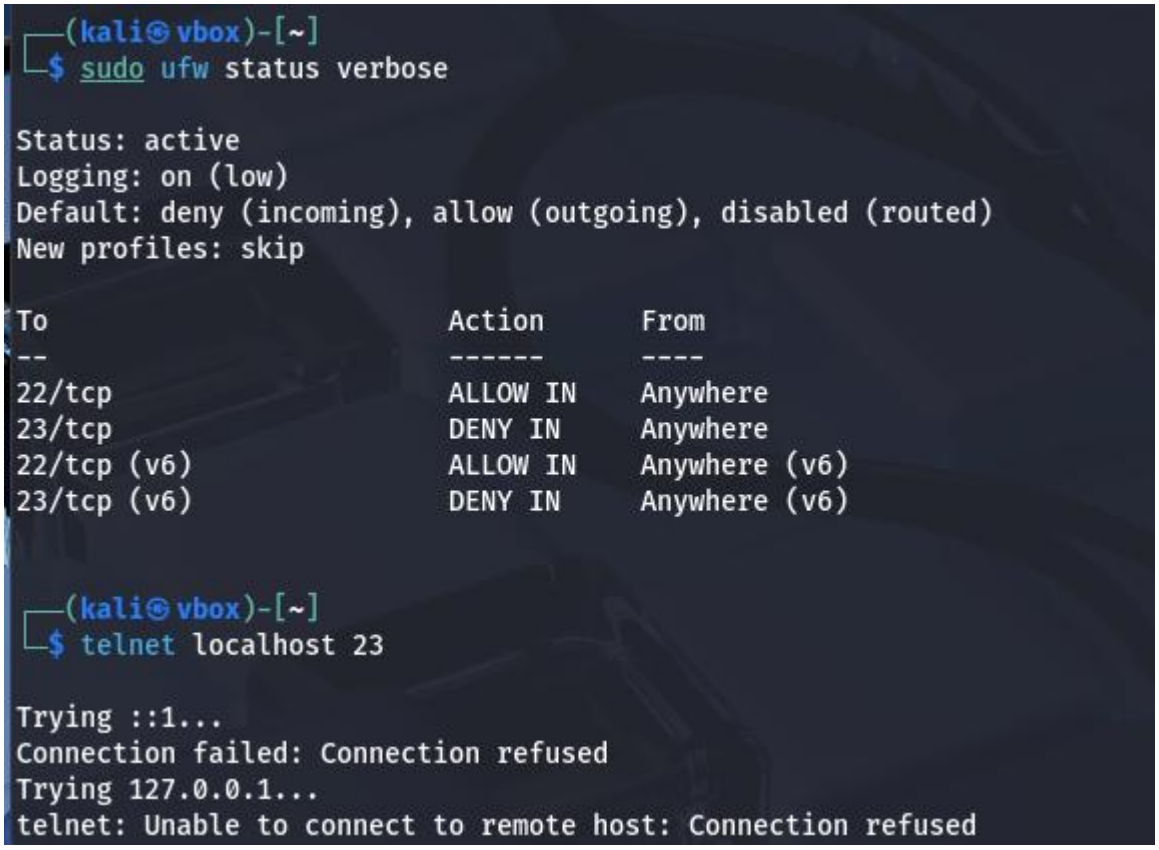
vbnet

Trying 127.0.0.1...

telnet: Unable to connect to remote host: Connection refused

Purpose:
To test and verify that port 23 is successfully blocked.

Screenshot 7: Output of Telnet failure due to firewall block



✅ **8. (Re)Allow SSH Access (Optional)**

Command:

bash

sudo ufw allow 22/tcp

Purpose:
Ensures SSH remains allowed for accessibility.

📸 **Screenshot 8:** Output confirming SSH rule addition (optional)

✅ **9. Remove the Block Rule on Port 23**

Command:

bash

sudo ufw delete deny 23/tcp

Expected Output:

mathematica

Rule deleted

Rule deleted (v6)

Purpose:
Cleans up test rules and restores the firewall to its previous state.

Summary of Firewall Behavior

- **UFW** is a simplified firewall tool for Linux, making rule management intuitive.
- **Rules added** via simple commands like allow and deny affect the system's inbound traffic.
- **SSH (port 22)** was allowed to maintain remote access.
- **Telnet (port 23)** was denied, and testing via telnet confirmed it was blocked.
- **Deleted the deny rule** to maintain a clean firewall configuration post-testing.
- The **UFW rules are persistent** across reboots unless manually changed.

✅ **Conclusion**

Through this task, we have successfully configured a basic firewall, tested traffic filtering, and learned how to manage inbound connections using UFW on a Linux system. This basic approach can be extended to enforce strong network security policies on both servers and desktops.