Firewall Configuration Report – UFW (Uncomplicated Firewall) on Parrot OS

👤 User: karzz@karzz-thin15b12ucx

🖥 OS: Parrot OS

📅 Date: 8th August 2025

# 🔧 Objective:

Configure the UFW firewall to:  
- Enable firewall service  
- Allow SSH (port 22)  
- Block Telnet (port 23)  
- List and verify all current rules  
- Understand traffic filtering with UFW

# 🧭 Steps Performed:

## Enable Firewall

Command:  
sudo ufw enable

Note: Firewall is now active and starts on boot.

## Allow SSH (Port 22)

Command:  
sudo ufw allow 22

Note: SSH traffic is allowed to enable remote administration.

## Deny Telnet (Port 23)

Command:  
sudo ufw deny 23

Note: Blocks insecure Telnet service from being accessed.

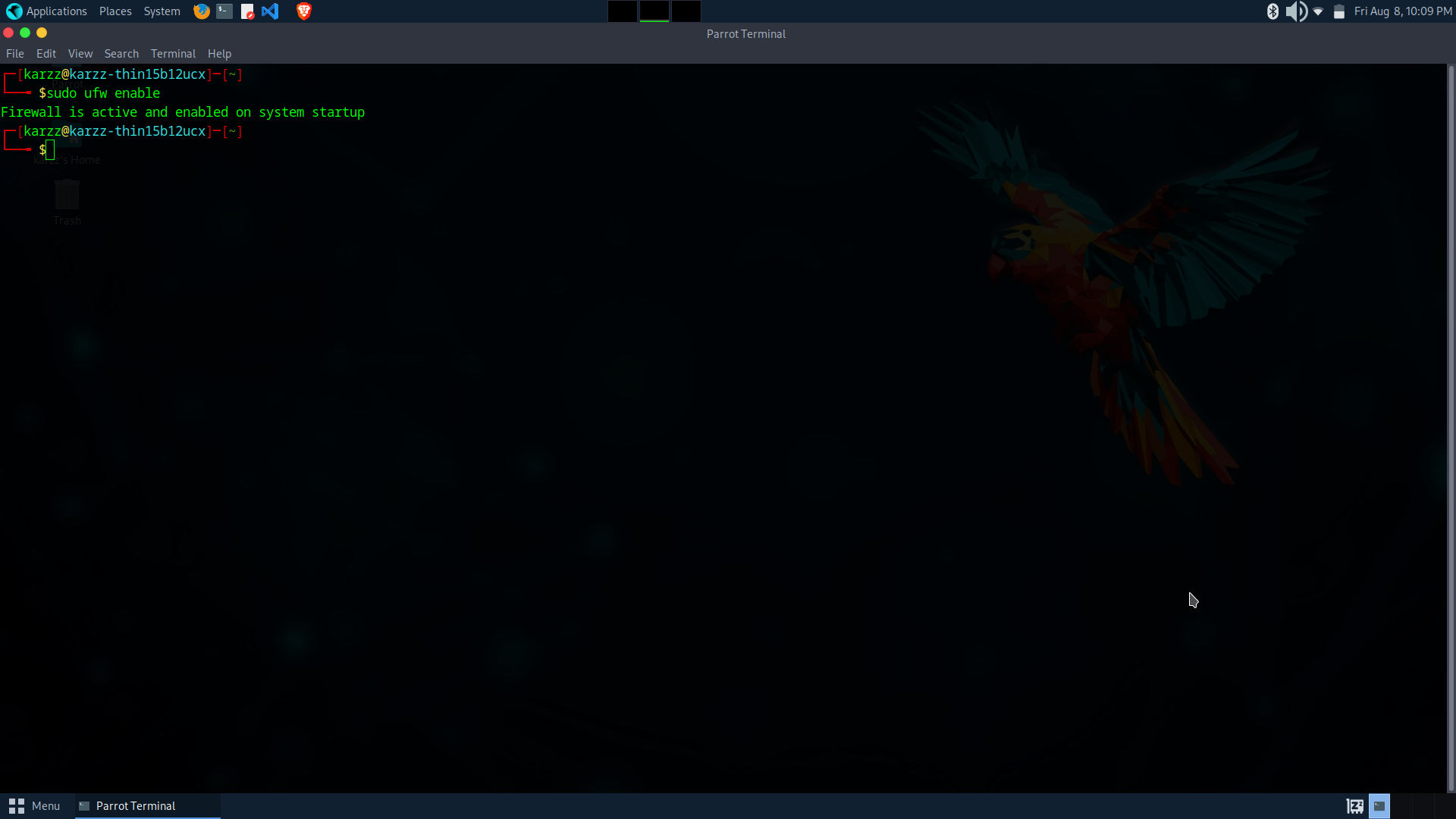
## List Rules (Numbered)

Command:  
sudo ufw status numbered

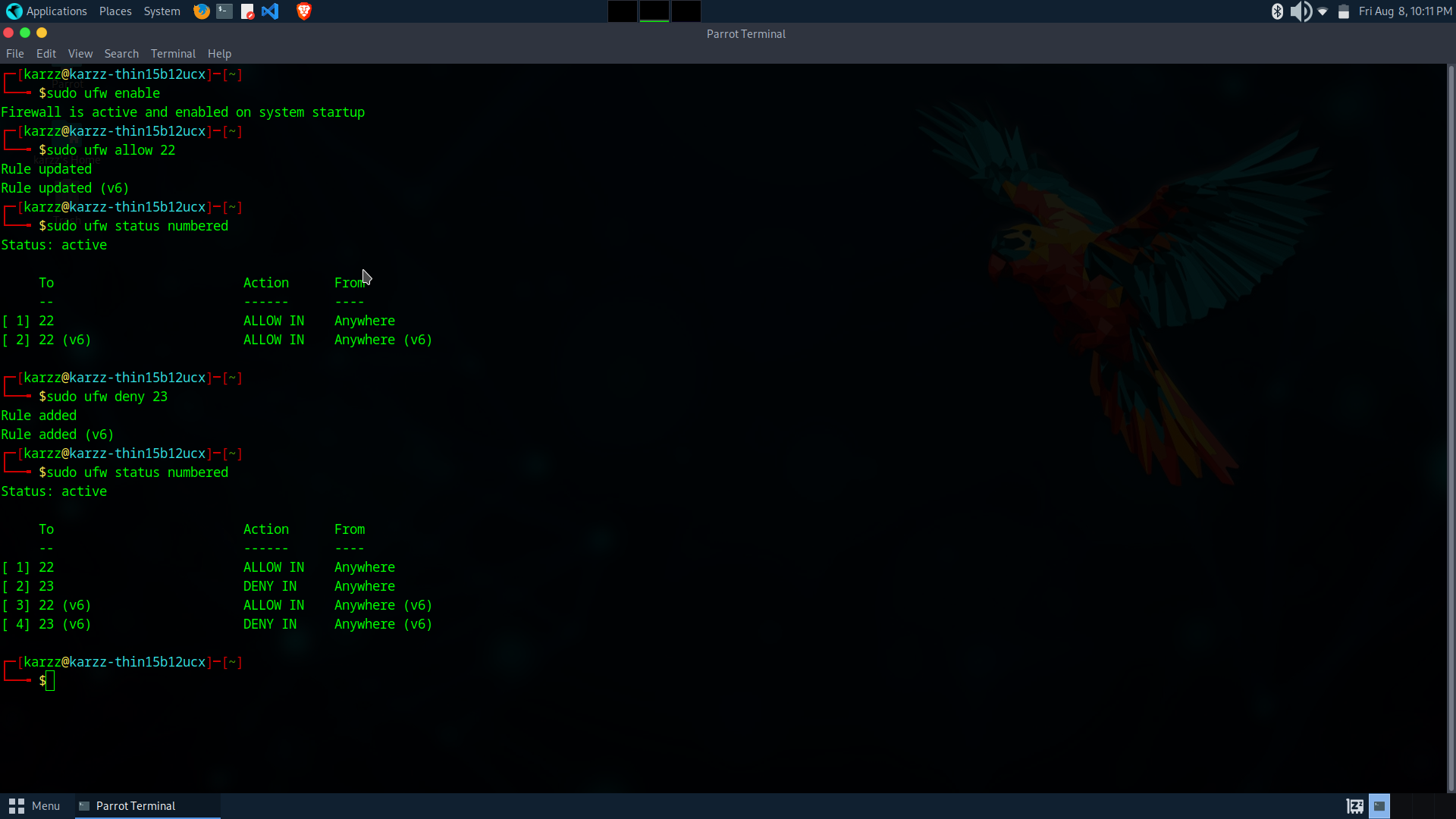
Note: Displays current firewall rules with indexing.

# 📸 Screenshots

UFW Enabled



Rules Applied



# 🧪 Testing (Optional but Recommended)

- Try connecting to port 22 (`ssh localhost`) – should work.  
- Try connecting to port 23 (`telnet localhost 23`) – should be blocked.

# ✅ Summary: How UFW Filters Traffic

UFW (Uncomplicated Firewall) simplifies firewall rule management for Linux. It works as a front-end for iptables and allows:  
- Defining rules per port and IP address.  
- ALLOW: Grants access to a service/port.  
- DENY: Blocks access to a service/port.  
- STATUS: Lists active rules for review.

# 📎 Notes

- Always ensure port 22 is allowed before enabling UFW on remote systems to prevent lockout.  
- Telnet is an insecure protocol and should be blocked or avoided in favor of SSH.