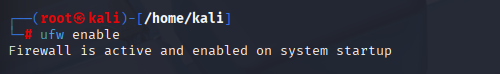
**Installing UFW**

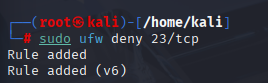


**Enabling ufw**

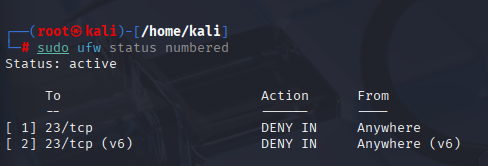




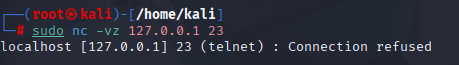
**Denying Telnet**



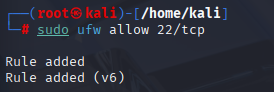
**Status**



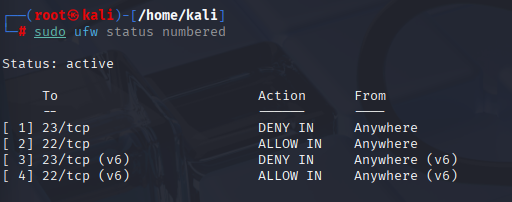
**Connection Attempt**



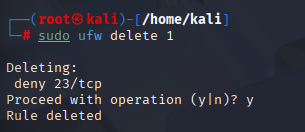
**Allowing ssh**

****

**Status**



**Deleting Rule 1**



**Understanding ufw working:**

* **UFW (Uncomplicated Firewall)** is a front-end for Linux’s underlying **iptables** or **nftables**.
* It provides a **simple command-line interface** to manage firewall rules without needing to write complex iptables commands.
* UFW works by applying rules to **network packets**:
  + It checks the **port** (e.g., 22 for SSH, 80 for HTTP).
  + It checks the **direction** (incoming or outgoing).
  + It checks the **action** (allow, deny, reject, limit).
* Rules are applied in order, and packets are either **allowed** or **blocked** based on these rules.
* When you add rules with ufw allow or ufw deny, UFW updates the iptables/nftables backend to enforce them.
* UFW can also manage IPv6 traffic if enabled in its config.