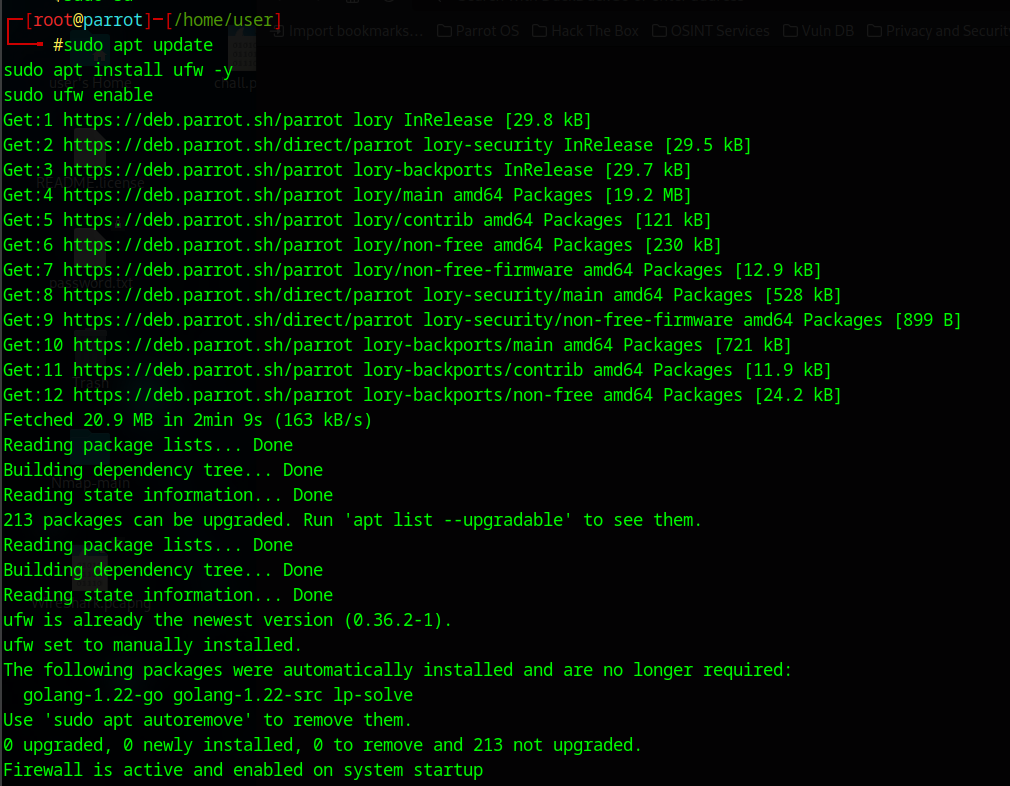
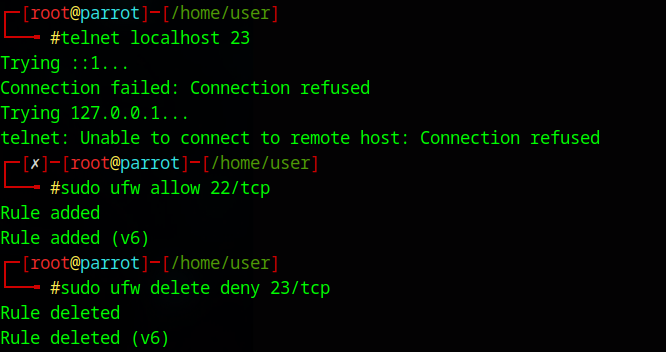
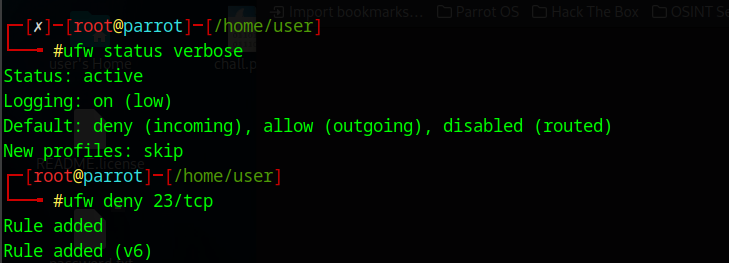
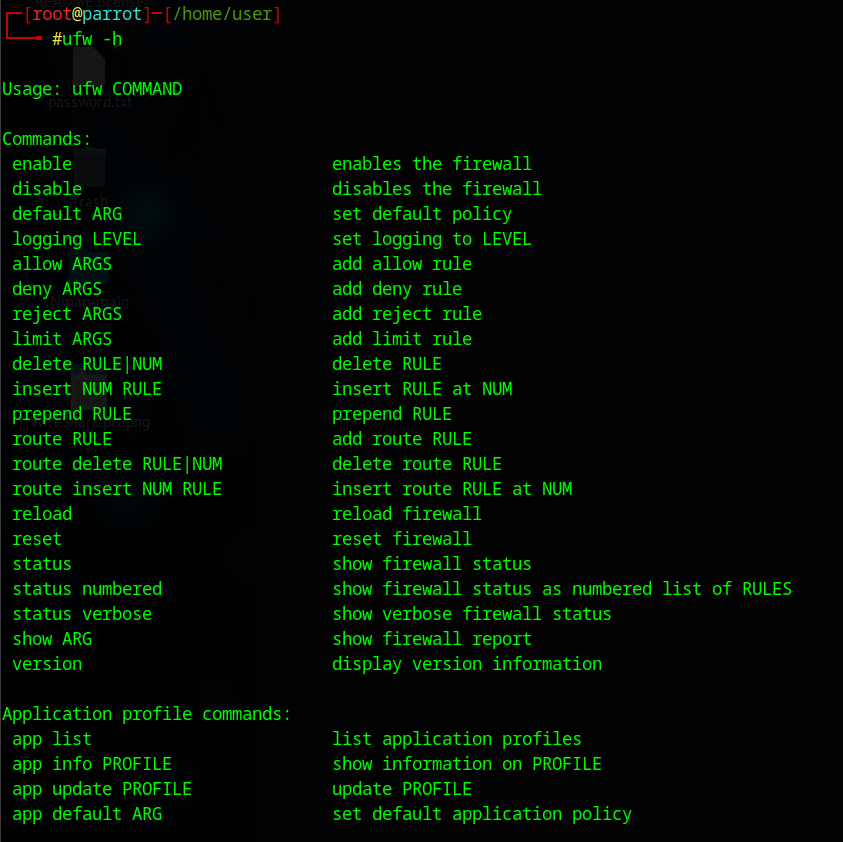
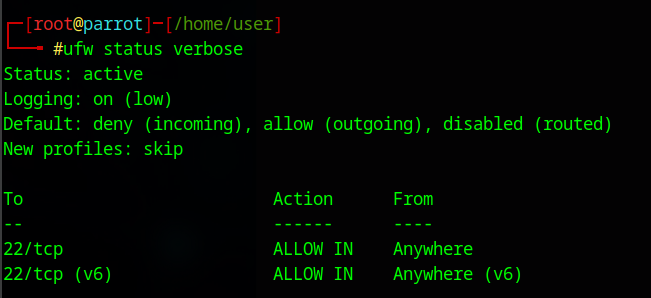
**TASK 4**

**Firewall Report**







**Document Commands Used**

**command history for the report:**

sudo apt install ufw -y

sudo ufw enable

sudo ufw status verbose

sudo ufw -h

sudo ufw deny 23/tcp

sudo telnet localhost 23

sudo ufw allow 22/tcp

sudo ufw delete deny 23/tcp

**Summary:**

A firewall acts as a security barrier between your system (or network) and the outside world. It filters incoming and outgoing network traffic based on a set of rules.

How It Works:

1. Traffic Inspection: Every data packet that tries to enter or leave your system is checked by the firewall.

2. Rule Matching: The firewall compares the packet against predefined rules (e.g., allow or deny traffic on specific ports or IPs).

3. Decision:

If it matches an allow rule, it's let through.

If it matches a deny rule, it's blocked.

If it doesn't match any rule, the default policy is applied (usually deny for incoming traffic).

Rule Criteria Can Include:

•Port numbers (e.g., block port 23 for Telnet)

•IP addresses (e.g., block traffic from a malicious IP)

•Protocols (TCP, UDP, ICMP)

•Direction (inbound vs. outbound)

Example:

•sudo ufw deny 23

→ Blocks all incoming connections to port 23 (Telnet).

•sudo ufw allow 22

→ Allows incoming SSH connections.