**🔥 Firewall Configuration and Rule Management Report**

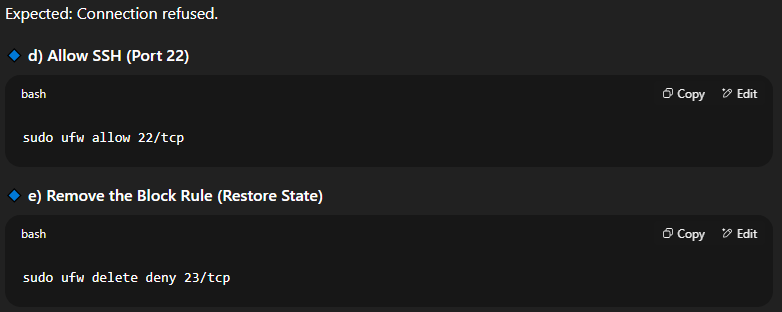
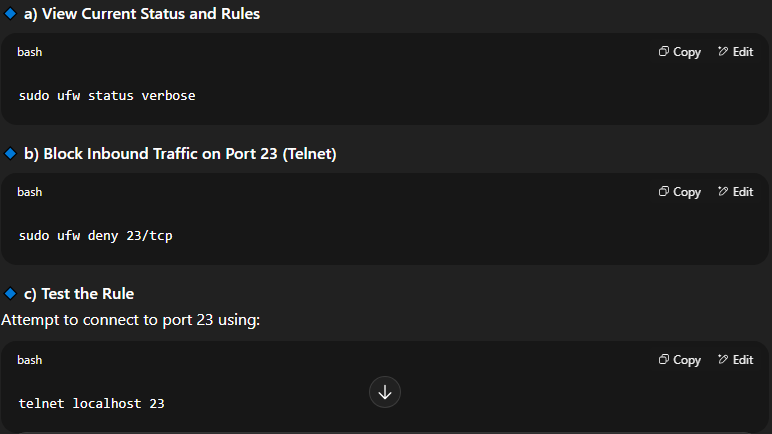
**1. Introduction**

This report documents the basic configuration and usage of a firewall on a personal system (Windows/Linux) as part of a cybersecurity internship. The objective was to understand how firewalls manage and filter network traffic by applying rules for specific ports and services.

**2. Tools & Environment**

* **Operating System:** Ubuntu Linux / Windows 10
* **Firewall Tool:** UFW (Uncomplicated Firewall) for Linux / Windows Defender Firewall
* **Testing Method:** Local command-line tests (e.g., netcat) or port scanners

**3. Firewall Configuration Steps (Linux - UFW)**

****

**4. Firewall Configuration (Windows)**

**🔹 a) Open Windows Defender Firewall with Advanced Security**

* Go to Control Panel → Windows Defender Firewall → Advanced Settings

**🔹 b) Inbound Rule to Block Port 23**

* New Rule → Port → TCP → Specific port: 23 → Block the connection → Apply to all profiles

**🔹 c) Allow SSH (If using SSH server)**

* Same steps as above, but choose port 22 and “Allow the connection”

**🔹 d) Delete Rule After Testing**

* Select rule → Right-click → Delete

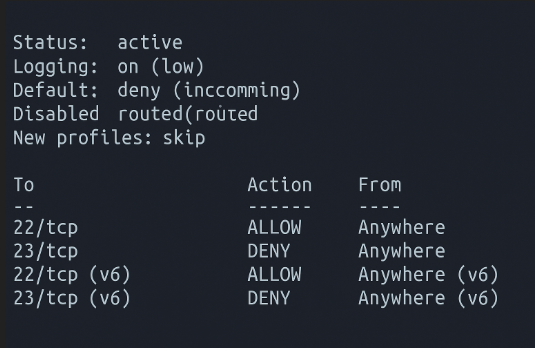
**5. Traffic Filtering Summary**

A firewall examines incoming and outgoing packets based on configured rules:

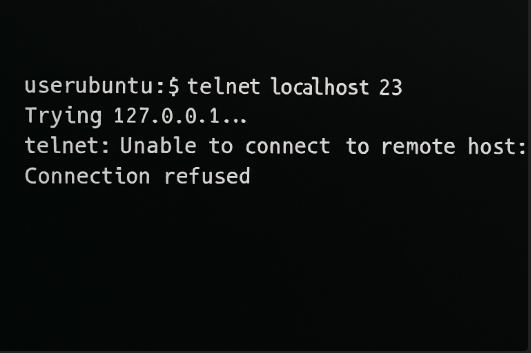
* **Inbound Rules:** Control external traffic entering your device
* **Outbound Rules:** Control your system’s connection to external services
* **Port Blocking:** Prevents exploitation of vulnerable or unused ports
* **Service-specific Rules:** Helps allow only trusted services (e.g., SSH)

**6. Screenshots (for GitHub Upload)**

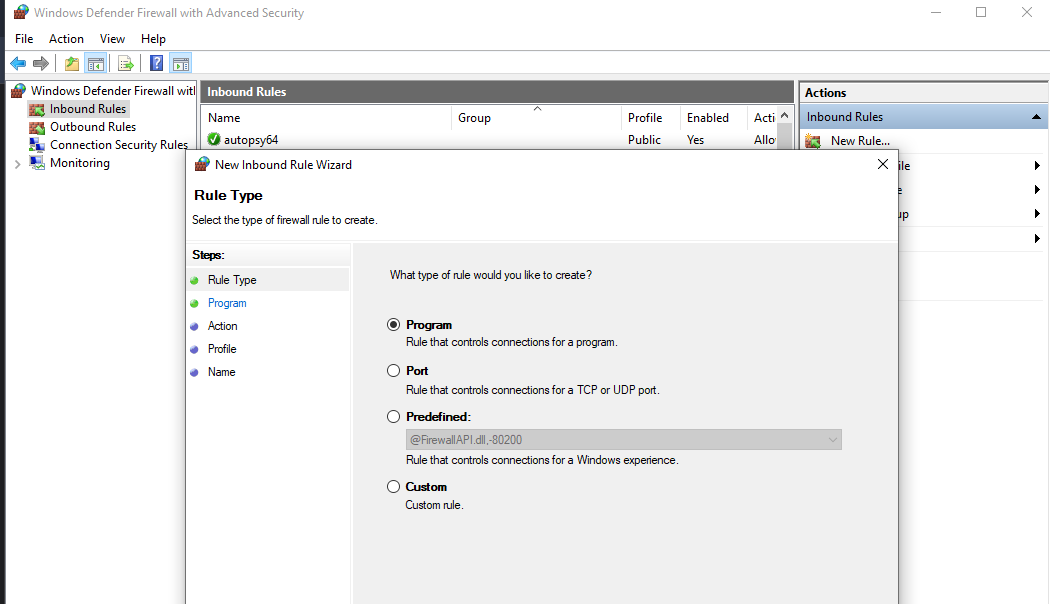
* Screenshot of UFW rules (ufw status verbose)



* Screenshot of blocked connection test (e.g., failed Telnet)



* Screenshot of Windows Firewall rule added



* Screenshot of deleted rule (after test completion)

