Firewall Configuration Report

System: [Windows 10 / Ubuntu 22.04]
Tool Used: [Windows Firewall / UFW]
Date: [Insert Date]

Steps Performed:

1. Checked firewall status.
2. Added a rule to block inbound traffic on port 23 (Telnet).
3. Tested the rule by attempting to connect to the blocked port.
4. Added a rule to allow SSH on port 22.
5. Verified firewall rules were applied.
6. Removed the test block rule to restore original state.

Commands Used (Linux UFW):

```
sudo ufw status
sudo ufw deny 23/tcp
sudo ufw allow 22/tcp
sudo ufw status numbered
sudo ufw delete deny 23/tcp
```

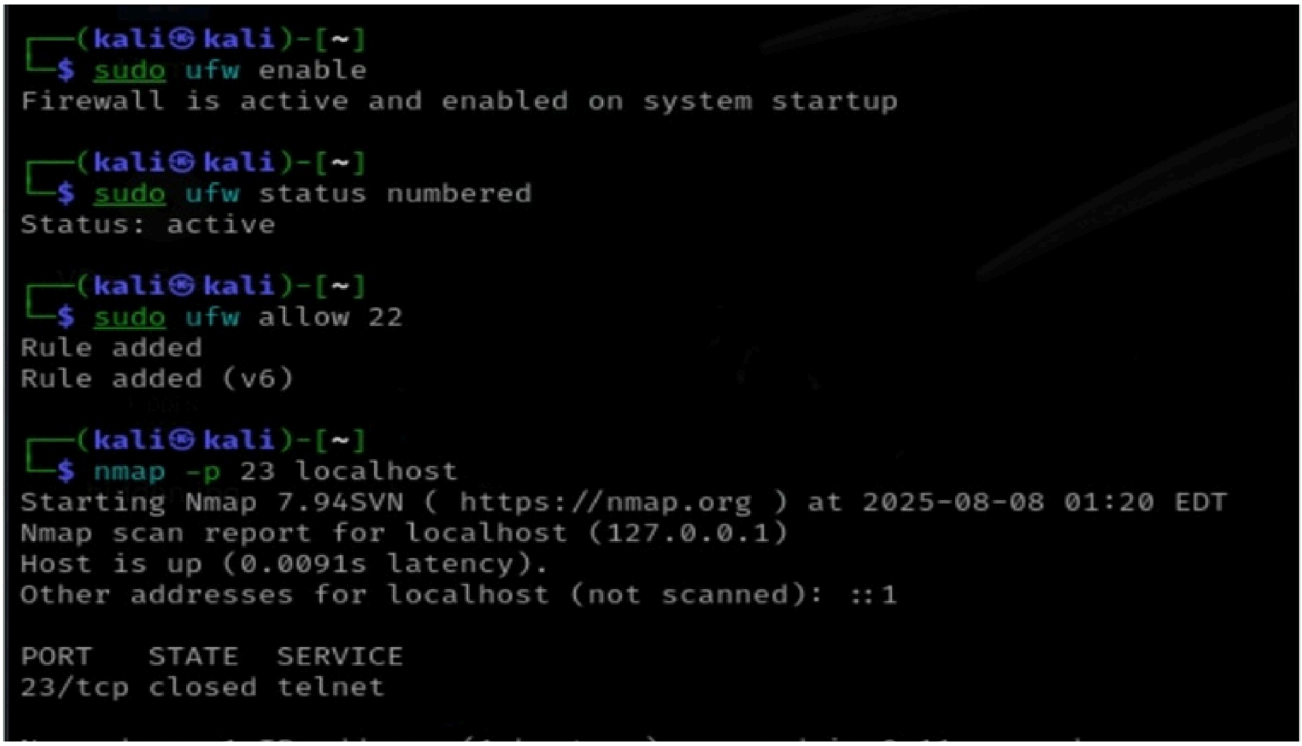
Firewall Traffic Filtering Summary:

Firewalls monitor and control network traffic based on rules. Inbound rules block unwanted external connections, while outbound rules prevent unauthorized data exfiltration. Rules can filter traffic by IP, port, protocol, or application. Blocking unused ports helps reduce the attack surface.

Firewall Rules Summary:

Rule Block	Action	Port	Protocol
Telnet Allow	Deny	23	TCP
SSH	Allow	22	TCP

Terminal Output Screenshot:



```
┌──(kali㉿kali)-[~]
└─$ sudo ufw enable
Firewall is active and enabled on system startup

┌──(kali㉿kali)-[~]
└─$ sudo ufw status numbered
Status: active

┌──(kali㉿kali)-[~]
└─$ sudo ufw allow 22
Rule added
Rule added (v6)

┌──(kali㉿kali)-[~]
└─$ nmap -p 23 localhost
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-08 01:20 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0091s latency).
Other addresses for localhost (not scanned): ::1

PORT   STATE  SERVICE
23/tcp closed telnet
```