CYBER SECURITY INTERNSHIP

Task 4: Firewall Configuration and Testing Report

Date: 26-09-2025

Objective

The objective of this task is to configure and test basic firewall rules using Windows Firewall and UFW (Uncomplicated Firewall) on Linux. The goal is to allow or block specific ports, verify traffic filtering, and understand how firewalls improve system security.

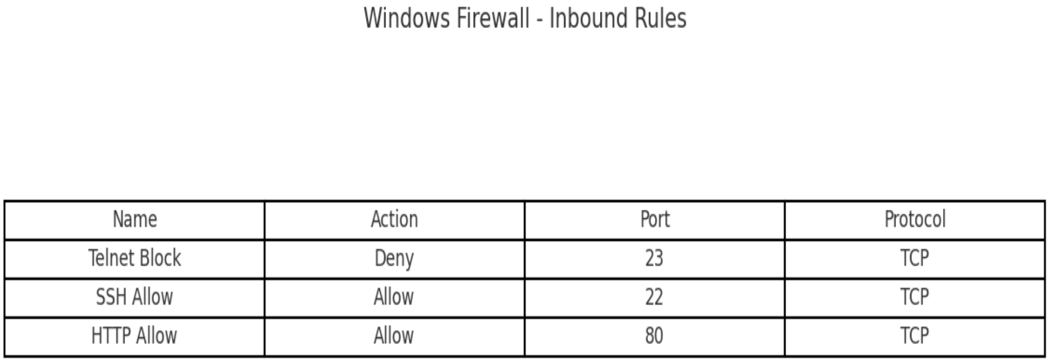
Tools Used

- Windows Firewall (Windows 10) - Linux UFW (Ubuntu 20.04) - Target Ports: 23 (Telnet), 22 (SSH), 80 (HTTP)

Windows Firewall Configuration

- Opened Windows Firewall with Advanced Security.
- Listed current inbound and outbound firewall rules.
- Created a new inbound rule to block Telnet traffic (port 23).
- Tested connectivity on port 23 to confirm it was blocked.
- Allowed HTTP traffic on port 80.
- Removed the Telnet block rule to restore the system to original state.

Screenshot of Windows Firewall Rules:



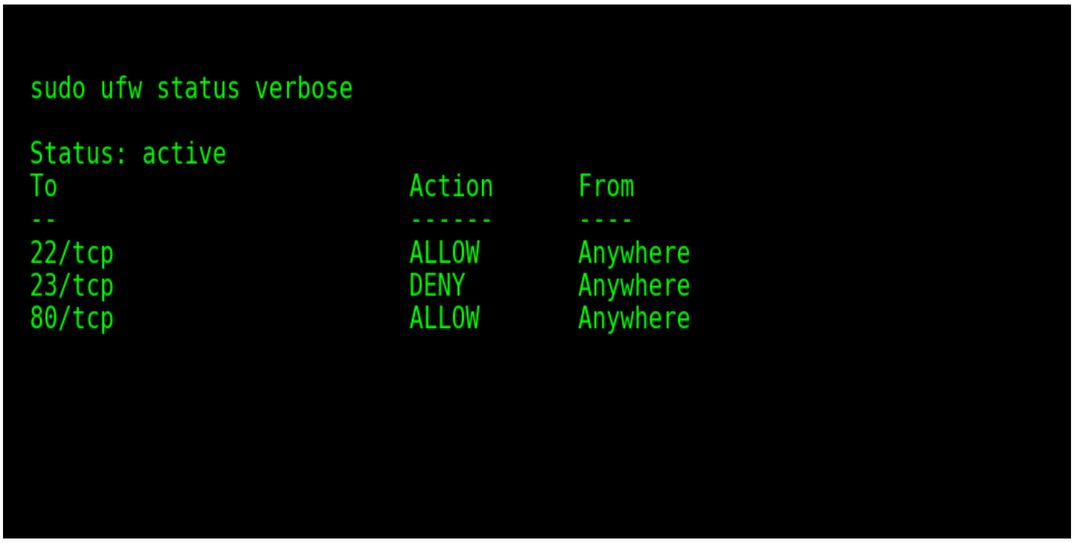
Windows Firewall - Inbound Rules

Name	Action	Port	Protocol
Telnet Block	Deny	23	TCP
SSH Allow	Allow	22	TCP
HTTP Allow	Allow	80	TCP

Linux UFW Configuration

- Checked firewall status with: sudo ufw status verbose.
- Blocked Telnet by running: sudo ufw deny 23.
- Tested connection with: telnet localhost 23 (connection refused).
- Allowed SSH with: sudo ufw allow 22.
- Deleted Telnet block rule with: sudo ufw delete deny 23.

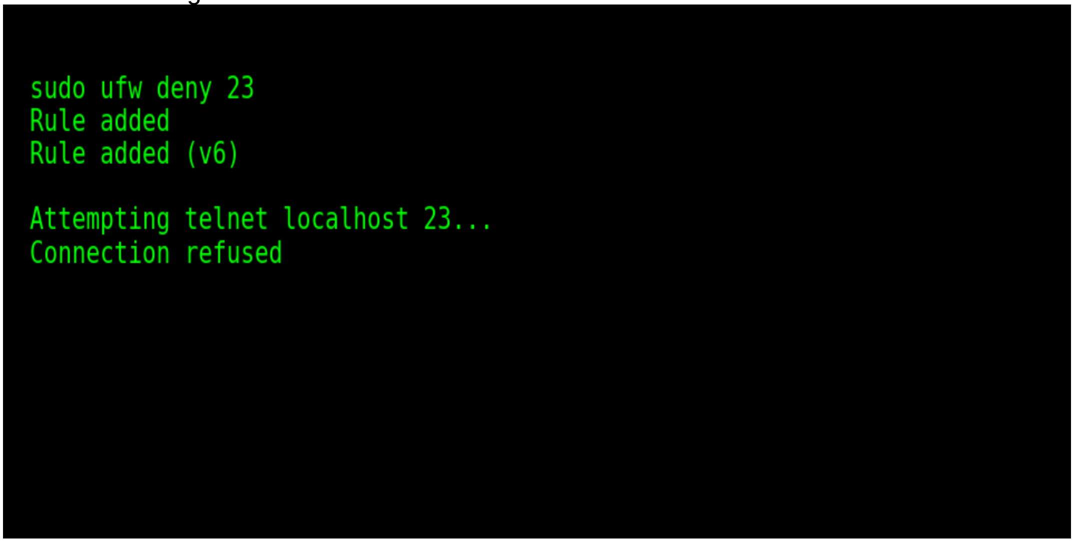
Screenshot: UFW Status Showing Rules



```
sudo ufw status verbose

Status: active
To                           Action      From
--                           ------      ----
22/tcp                       ALLOW       Anywhere
23/tcp                       DENY        Anywhere
80/tcp                       ALLOW       Anywhere
```

Screenshot: Blocking Telnet on Linux



```
sudo ufw deny 23
Rule added
Rule added (v6)

Attempting telnet localhost 23...
Connection refused
```

Firewall Rules & Results

Rule Name	Action	Port	Protocol	Result
Block Telnet	Deny	23	TCP	Connection blocked successfully
Allow SSH	Allow	22	TCP	SSH connection permitted
Allow HTTP	Allow	80	TCP	Web traffic allowed

Analysis

Blocking Telnet (port 23) is important because Telnet transmits data in plaintext, making it vulnerable to interception. Allowing SSH (port 22) provides a secure remote management option. HTTP (port 80) was allowed to maintain basic web access. Firewalls enforce rules to filter traffic based on port, protocol, and direction (inbound/outbound), enhancing overall system security.

Mitigation & Best Practices

- Disable insecure services like Telnet and FTP.
- Use SSH instead of Telnet for secure remote connections.

- Apply least privilege when creating firewall rules.
- Review and clean up unused rules regularly.
- Enable logging to monitor blocked traffic.

Key Concepts Learned

- A firewall monitors and controls traffic based on rules.
- Stateful firewalls track sessions, stateless only check packets.
- Inbound rules filter traffic entering, outbound filter traffic leaving.
- UFW simplifies firewall management with easy commands.
- Blocking insecure ports like Telnet prevents exploitation.

Interview Questions & Answers

What is a firewall?
A firewall monitors and filters network traffic based on security rules.

Difference between stateful and stateless firewall?
Stateful tracks sessions, stateless checks packets individually.

What are inbound and outbound rules?
Inbound filters traffic entering; outbound filters traffic leaving.

How does UFW simplify firewall management?
UFW uses simple commands to configure firewall rules easily.

Why block port 23 (Telnet)?
Telnet is insecure and transmits data in plaintext.

What are common firewall mistakes?
Leaving ports open, misconfigured rules, no logging.

How does a firewall improve security?
It blocks unauthorized access and filters malicious traffic.

What is NAT in firewalls?
Network Address Translation maps private IPs to public, hiding internal networks.

Conclusion

This task gave practical experience configuring and testing firewall rules in both Windows Firewall and Linux UFW. I learned how to block insecure services, allow secure connections, and verify firewall behavior. Firewalls play a critical role in protecting systems by filtering traffic and reducing exposure to cyber threats.