Elevate Labs – Cyber Security Internship

NAME:Srinivas Atta

Task 4: Setup and Use a Firewall on Windows/Linux

By: Ministry of MSME, Govt. of India

Objective

Configure and test basic firewall rules to allow or block specific network traffic, and gain practical skills in traffic filtering.

Tools Required

- Windows Firewall (built-in)
- UFW (Uncomplicated Firewall) on Linux

Execution Steps / Guide

1. Open firewall configuration tool
    - On Windows: Open "Windows Defender Firewall with Advanced Security" from Control Panel.
    - On Linux: Open terminal and ensure UFW is installed (`sudo apt install ufw`).
2. List current firewall rules
    - Windows: Use GUI or run `netsh advfirewall firewall show rule name=all` in command prompt.
    - Linux: Run `sudo ufw status numbered`.
3. Add a rule to block inbound traffic on a specific port
    - Example: Block Telnet port 23.
        - Windows: Create a new inbound rule → select TCP port 23 → block connection.
        - Linux: `sudo ufw deny 23`.
4. Test the block rule
    - Attempt to connect to that port locally or remotely to confirm it's blocked.

5. Add a rule to allow SSH (Linux only)
   - Command: `sudo ufw allow 22`.
6. Remove the test block rule
   - Windows: Delete the created inbound rule.
   - Linux: `sudo ufw delete deny 23`.
7. Document all commands or GUI steps used
   - Take screenshots of the firewall settings before and after applying rules.
8. Summarize how firewall filters traffic
   - Note that it accepts or drops packets based on rules defined for ports, IPs, and protocols.

Findings / Results

- Successfully blocked incoming connections on port 23 (Telnet).
- Verified the block by attempting a connection and observing it fail.
- Allowed port 22 (SSH) on Linux to enable secure remote login.
- Removed test block rule and restored original firewall state.

Evidence: (Insert screenshots here)

- Screenshot 1: Initial firewall rules
- Screenshot 2: Block rule applied
- Screenshot 3: Test connection results
- Screenshot 4: Rules after removing the block

Security Analysis

Blocking unused or insecure ports like Telnet (Port 23) reduces the attack surface. Allowing only trusted and encrypted services (like SSH) maintains accessibility without compromising security. Misconfigured rules or overly permissive settings can make systems vulnerable.

Recommendations

- Always keep Telnet disabled; use SSH for remote access.
- Periodically review firewall rules to ensure only required ports are open.
- Combine firewall protection with intrusion detection/prevention systems for layered security.
- Document all firewall changes for audit and troubleshooting purposes.

Outcome

- Learned to configure firewall rules for both Windows and Linux.
- Practiced blocking insecure services and allowing critical secure ones.
- Understood how firewalls control traffic flow and help secure a system.

Key Concepts

- Firewall rule configuration
- Network traffic filtering
- Ports and protocols
- UFW basics
- Windows Firewall advanced settings