Firewall Configuration Task Report

Task Overview

This report documents the completion of **Task 4: "Setup and Use a Firewall on Windows/Linux"** as part of the Cyber Security Internship program. The objective was to configure and test basic firewall rules to **allow or block network traffic** using either **Windows Firewall** or **UFW (Uncomplicated Firewall)** on Linux.

The task involved:

- **Listing existing firewall rules**
- **Blocking inbound traffic on a specific port (Port 23 - Telnet)**
- **Testing the blocked connection**
- **Allowing SSH (Port 22 - Linux only)**
- **Restoring the original firewall state**

This exercise helped in understanding **how firewalls filter traffic** and the importance of **secure network configurations**.

Tools Used

- **Operating System:** [Windows 10 / Ubuntu Linux]
- **Firewall Tool:**
  - **Windows:** Windows Defender Firewall with Advanced Security
  - **Linux:** UFW (Uncomplicated Firewall)

Steps Performed

1. Accessing Firewall Configuration

On Windows:

- Opened **Windows Defender Firewall** via:
  - **Control Panel → System and Security → Windows Defender Firewall**
  - Used **Advanced Settings** to configure inbound/outbound rules.

On Linux (UFW):

- Checked UFW status:

bash

Copy

Download

```
sudo ufw status
```

- Enabled UFW (if inactive):

bash

Copy

Download

```
sudo ufw enable
```

---

2. Listing Current Firewall Rules

On Windows:

- Ran the following command in **Command Prompt (Admin):**

cmd

Copy

Download

```
netsh advfirewall firewall show rule name=all
```

  - This displayed all existing inbound/outbound rules.

On Linux (UFW):

- Listed all active rules:

bash

Copy

Download

```
sudo ufw status verbose
```

  - Verified default policies (e.g., deny incoming, allow outgoing).

---

3. Blocking Inbound Traffic on Port 23 (Telnet)

On Windows:

- Created a new **Inbound Rule** to block **TCP Port 23**:
    1. Opened **Windows Defender Firewall with Advanced Security**.
    2. Navigated to **Inbound Rules** → **New Rule**.
    3. Selected **Port** → **TCP** → **Specific Ports: 23**.
    4. Chose **Block the connection** → Applied to **Domain, Private, Public**.
    5. Named the rule **"Block_Telnet_Port_23"**.

On Linux (UFW):

- Added a deny rule for **Port 23 (Telnet):**

bash

Copy

Download

```
sudo ufw deny 23/tcp
```

- Verified the rule was added:

bash

Copy

Download

```
sudo ufw status
```

---

4. Testing the Blocked Port (Telnet Connection Attempt)

- Installed **Telnet client** (if not available):
    - **Windows:**

cmd

Copy

Download

```
dism /online /Enable-Feature /FeatureName:TelnetClient
```

- - **Linux:**

bash

Copy

Download

```
sudo apt install telnet
```

- Attempted to connect to **localhost on Port 23**:

cmd

Copy

Download

```
telnet localhost 23
```

  - **Expected Result:** Connection timed out or "Connection refused."
  - **Verification:** Confirmed that the firewall successfully blocked Telnet traffic.

---

5. Allowing SSH (Port 22 - Linux Only)

On Linux (UFW):

- Added an **allow rule** for **SSH (Port 22):**

bash

Copy

Download

```
sudo ufw allow 22/tcp
```

- Verified SSH access:

bash

Copy

Download

```
ssh localhost
```

  - **Expected Result:** Successful SSH login (if SSH server is running).

---

6. Restoring Original Firewall State

On Windows:

- Deleted the **"Block_Telnet_Port_23"** rule from **Inbound Rules**.

On Linux (UFW):

- Removed the **deny rule for Port 23:**

bash

Copy

Download

```
sudo ufw delete deny 23/tcp
```

- Verified removal:

bash

Copy

Download

```
sudo ufw status
```

Key Learnings

- **Firewall Rule Management:** Learned how to **add, modify, and delete** firewall rules on both **Windows and Linux**.
- **Traffic Filtering:** Understood how firewalls **block/allows traffic** based on **ports and protocols**.
- **Security Best Practices:** Recognized why **blocking insecure services (like Telnet)** is crucial.
- **Testing & Verification:** Confirmed firewall effectiveness by **testing blocked/allowed connections**.

Conclusion

This task provided **hands-on experience** in **firewall configuration** and **network security**.
By **blocking Telnet (Port 23)** and **allowing SSH (Port 22)**, I understood how firewalls **protect systems from unauthorized access**. This exercise reinforced the importance of **proper firewall management** in cybersecurity.