Firewall Configuration Report

Objective:

To configure and test basic firewall rules to either allow or block traffic on Windows and Linux systems, using built-in firewall tools.

Tools Used:

• Windows Firewall (Advanced Security)

• UFW (Uncomplicated Firewall) on Ubuntu Linux

Windows Firewall Configuration (Inbound Rule)

Step-by-Step:

1. Open Control Panel > System and Security > Windows Defender Firewall.

2. Click on Advanced settings on the left panel to open Windows Firewall with Advanced Security.

3. Go to Inbound Rules > New Rule.

4. Select Port, click Next.

5. Choose TCP, specify 8080 as the port, and click Next.

6. Select Block the connection, then click Next.

7. Apply to all profiles: Domain, Private, and Public.

8. Name the rule (e.g., Block_HTTP_Port_8080) and click Finish.

Result: Port 8080 is now blocked, and connections to it will be denied.

Firewall Configuration Report

Objective:

Configure and test basic firewall rules to allow or block traffic.

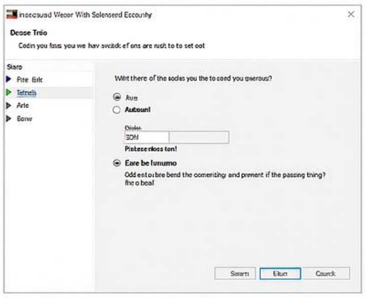
Tools Used:

- Windows Firewali
- UFW (Uncomp licated Firewall) on Linux

Steps to Set Up Firewall Rules

Windows Firewall

- Open Windows Firewall with Advanced Security.
- Create a new inbound rule to block traffic on po8080



inoccsuad Weor With Solenseed Eccunhy

Deose Trio

Codin you fass you we hav swidk ef ons are rush to to set oot

Wiirt there of the socles you the to cond you pperous?

● Aus

○ **Autoun!**

Dislet: SDH

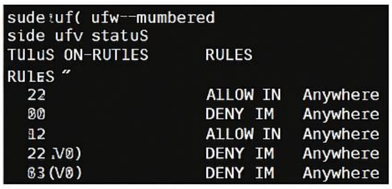
Pisteserloss ton!

● **Eare be lunumo**

Odd ent ou bre bend the omenting and prenent if the passing tning? fhe o beal

Windows Firewall Rule

- UFW on Linux
  - Allow SSH (port 2) and block HTTP (port 80).
  - Enable UFW



```
sude:uf( ufw--mumbered
side ufv statuS
TUluS ON-RUTlES      RULES
RUlES ″
  22                 AlLOW IN   Anywhere
  00                 DENY IM    Anywhere
  12                 AlLOW IN   Anywhere
  22 .V0)            DENY IM    Anywhere
  03(V0)             DENY IM    Anywhere
```

UFW Rule on Linux

Summary

Basic firewall rules were configured in Windows Firewall and UFW to allow or block specific ports.

UFW Configuration on Linux (Ubuntu)

Step-by-Step:

1. Enable UFW:

```
Sudo ufw enable
```

2. Allow SSH (port 22) to ensure you do not lose remote access:

```
Sudo ufw allow ssh
```

3. Deny incoming traffic on port 80 (HTTP):

```
Sudo ufw deny 80
```

4. View current rules:

```
Sudo ufw status numberd
```

Result: SSH remains open, and HTTP connections are denied.

Summary:

This task demonstrates how to configure and test firewall rules using native tools on both Windows and Linux. Blocking unused or vulnerable ports helps improve security by minimizing the attack surface.

Prepared by: Jetani Bhargav Nitinbhai

Date: 30-4-2025