# Task 4 – Configure and Use a Firewall on Windows

Tools Used: Windows Defender Firewall, Command Prompt

## Objective:

The objective of this task was to explore and test basic firewall rules to manage network traffic by allowing or blocking specific ports.

## Activities Performed:

1. Initial Firewall Review:  
 Accessed Windows Defender Firewall through the Control Panel. Also checked firewall settings on a Linux test machine.

2. Blocking a Specific Port (Telnet – Port 23):  
 Navigated to Inbound Rules → Created a new rule to block TCP port 23.

3. Allowing SSH (Port 22):  
 On Linux, enabled SSH access to allow secure remote logins using the command:  
 sudo ufw allow 22/tcp  
 Verified connectivity by running ssh user@<IP> from another system, which connected successfully.

4. Testing Firewall Rules:  
 Attempted to access blocked ports both locally and remotely — all access attempts to blocked ports were unsuccessful.

5. Removing the Test Block Rule:  
 Deleted the inbound Telnet block rule to restore default settings.