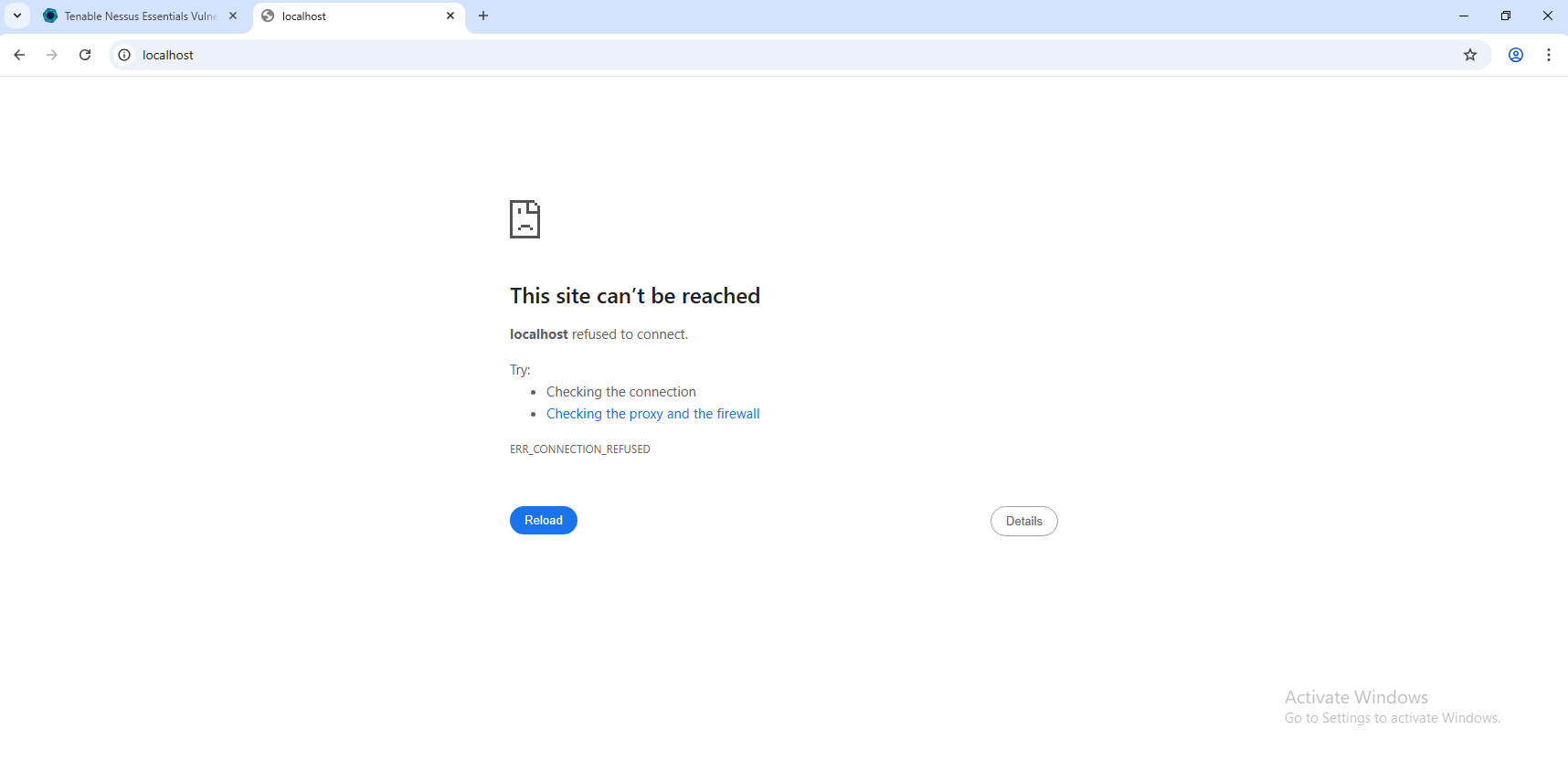
**Task 4 : Setup and Use a Firewall on Windows/Linux**

**Steps Performed:**

1. **Opened Windows Defender Firewall with Advanced Security**
   * Accessed via wf.msc command from Run dialog.
2. **Listed Current Rules:**
   * Viewed existing inbound and outbound rules through the GUI.
3. **Blocked Port 80 (HTTP):**
   * Created a new **Inbound Rule**:
     + Protocol: **TCP**
     + Port: **80**
     + Action: **Block the connection**
     + Applied to: Domain, Private, Public
     + Named: “Block Port 80”
4. **Tested the Rule:**
   * Tried accessing http://localhost in browser — connection failed, confirming the block.
   * Also used telnet localhost 80 — connection was refused.



1. **Verified via Command Line:**

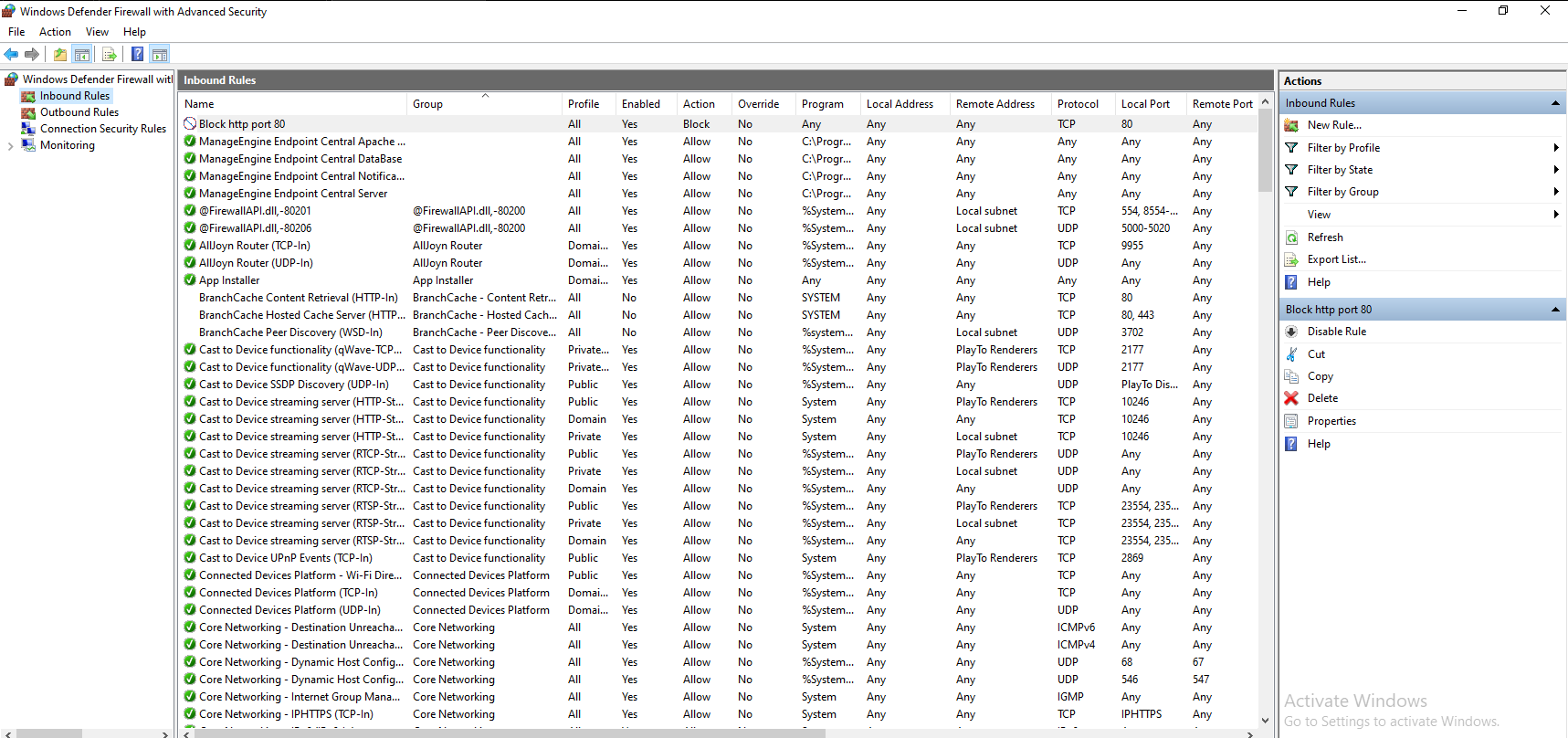
netstat -ano | findstr :80

Confirmed no service was listening on port 80.

* + Checked process using:

tasklist | findstr <PID>

1. **Removed Rule to Restore Normal Function:**
   * Deleted the “Block Port 80” rule from the firewall GUI.

**Part 2: Linux Firewall (UFW) Configuration**

**Steps Performed:**

1. **Checked Firewall Status:**

sudo ufw status

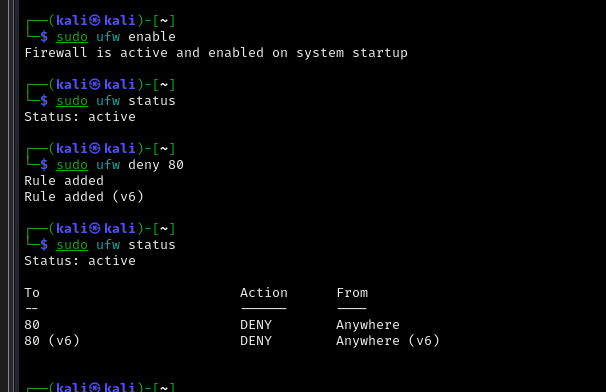
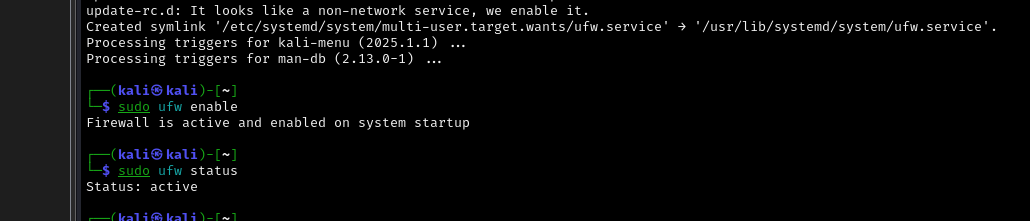
1. **Blocked Port 80:**

sudo ufw deny 80

1. **Verified the Rule:**
   * Used:

sudo ufw status

Output confirmed port 80 was denied.



1. **Tested Port Access:**
   * Started a Python HTTP server:

sudo python3 -m http.server 80

* + In browser: http://localhost failed to load, confirming block.

1. **Checked Running Services on Port 80:**

sudo lsof -i :80

* + Showed the Python process using port 80.

sudo ufw delete deny 80