STEP 1: Windows Defender Firewall with Advanced Security ON YOUR PC.

A screenshot of a computer

AI-generated content may be incorrect.

STEP 2:NOW CHECK THE INBOUND AND OUTBOUND RULES

AFTER CLICKING ON THE INBOUND RULES COME FRONT OF MY PC THAT WHAT IS ENABLED WHICH PROTOCOL IS RUNNING IN MY PC

STEP 3:AFTER APPLYING **Inbound Rules** → **New Rule**.

Choose **Port** → **TCP** → enter **23**.

Select **Block the connection** → apply to all profiles → name it **Block**

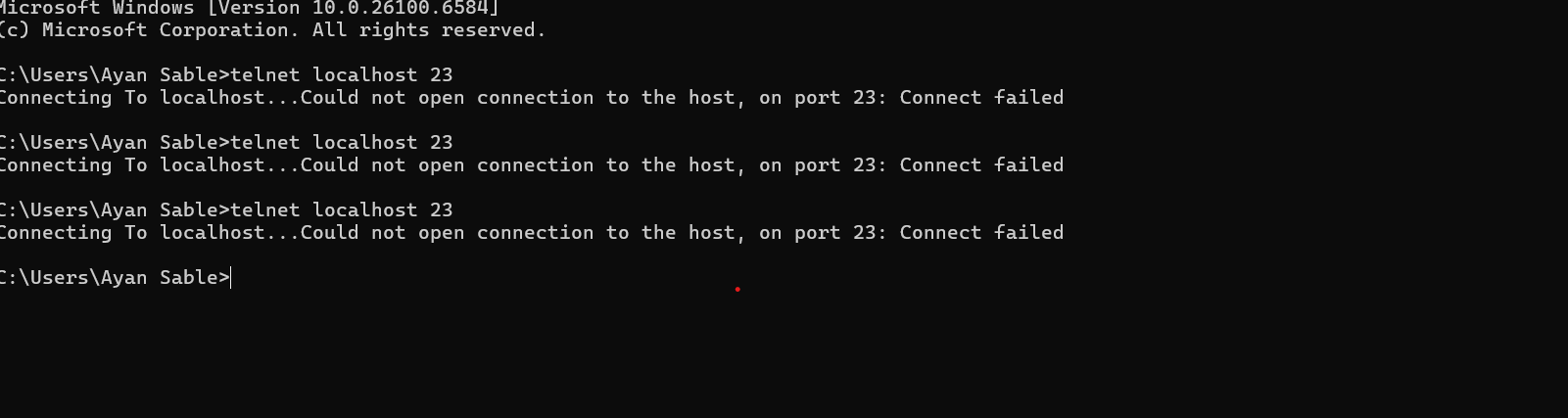
**Telnet Port 23**.output:

A screen shot of a computer

AI-generated content may be incorrect.ITS CONNECTION FAILS MEANS WE HAVE SUCCESSFULLY DONE

STEP 4:NOW DO ITS NORMAL

STEP 5: NOW FOR OUTBOUND TRAFFIC SAME PROCEDURE THEN BLOCK THE TELNET PORT AND PING IN COMMAND PROMPT



ITS SHOW THAT THE CONNECTION IS BLOCK FOR OUTBOUND TRAFFIC

STEP 6:NOW TO FOR SSH INBOUND RULE FIREWALL

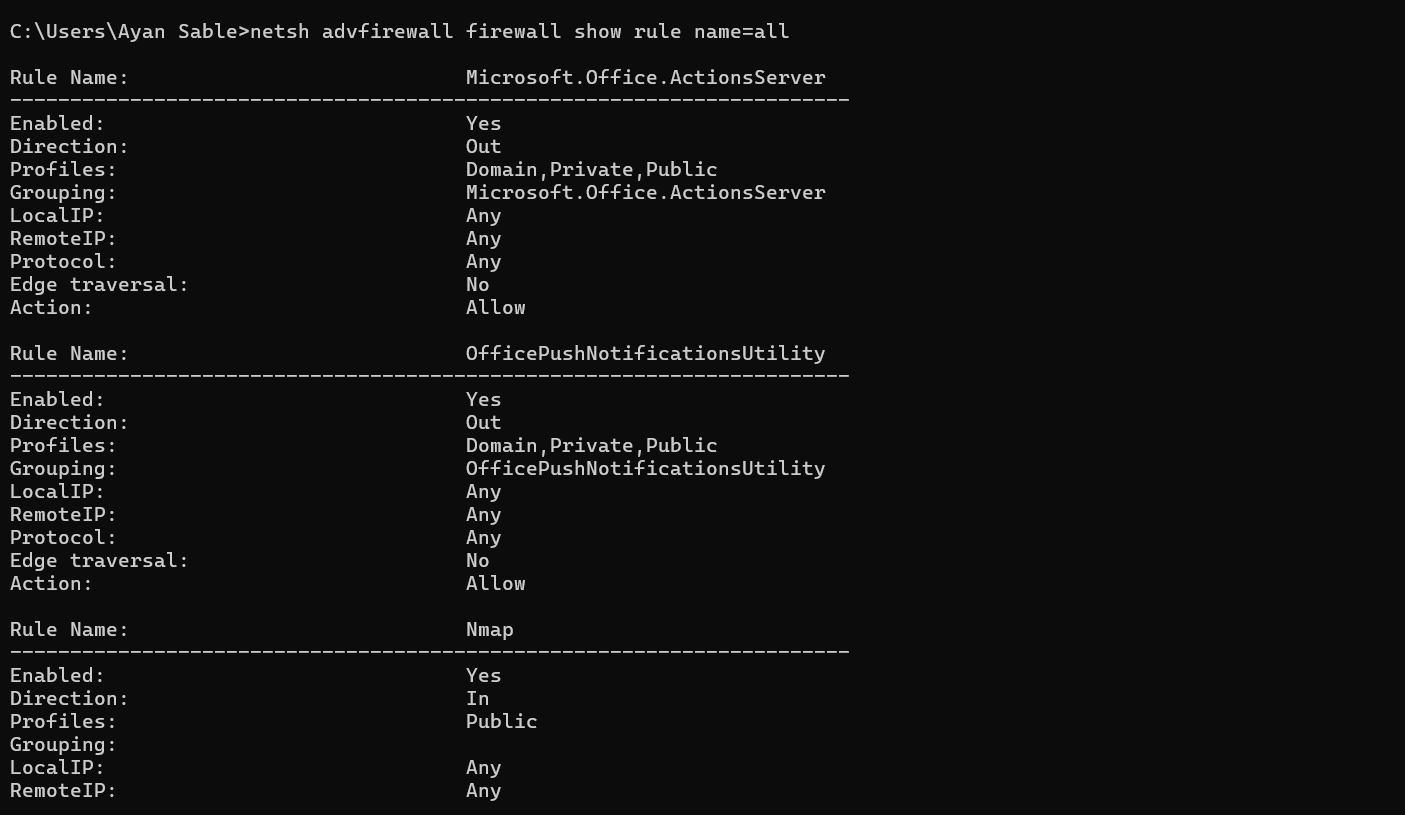
SAME STEP GO INBOUND BLOCK PORT SSH

A screen shot of a computer

AI-generated content may be incorrect.

ITS WILL THAT THE CONNECTION IS REFUSED FOR SSH PORT

STEP 7:FIREWALL RULES (netsh advfirewall firewall show rule name=all)



STEP 8:HOW TO RESTORE ORIGINAL

Disable or remove the rule:

Remove-NetFirewallRule -DisplayName "Rule Name"

##HOW FIREWALL FILTERS

Inspects inbound/outbound traffic based on rules (port, protocol, direction, action).

Stateful firewall: Tracks connection states.

Stateless firewall: Checks each packet independently.

Protects against unauthorized access, insecure protocols, and malware.