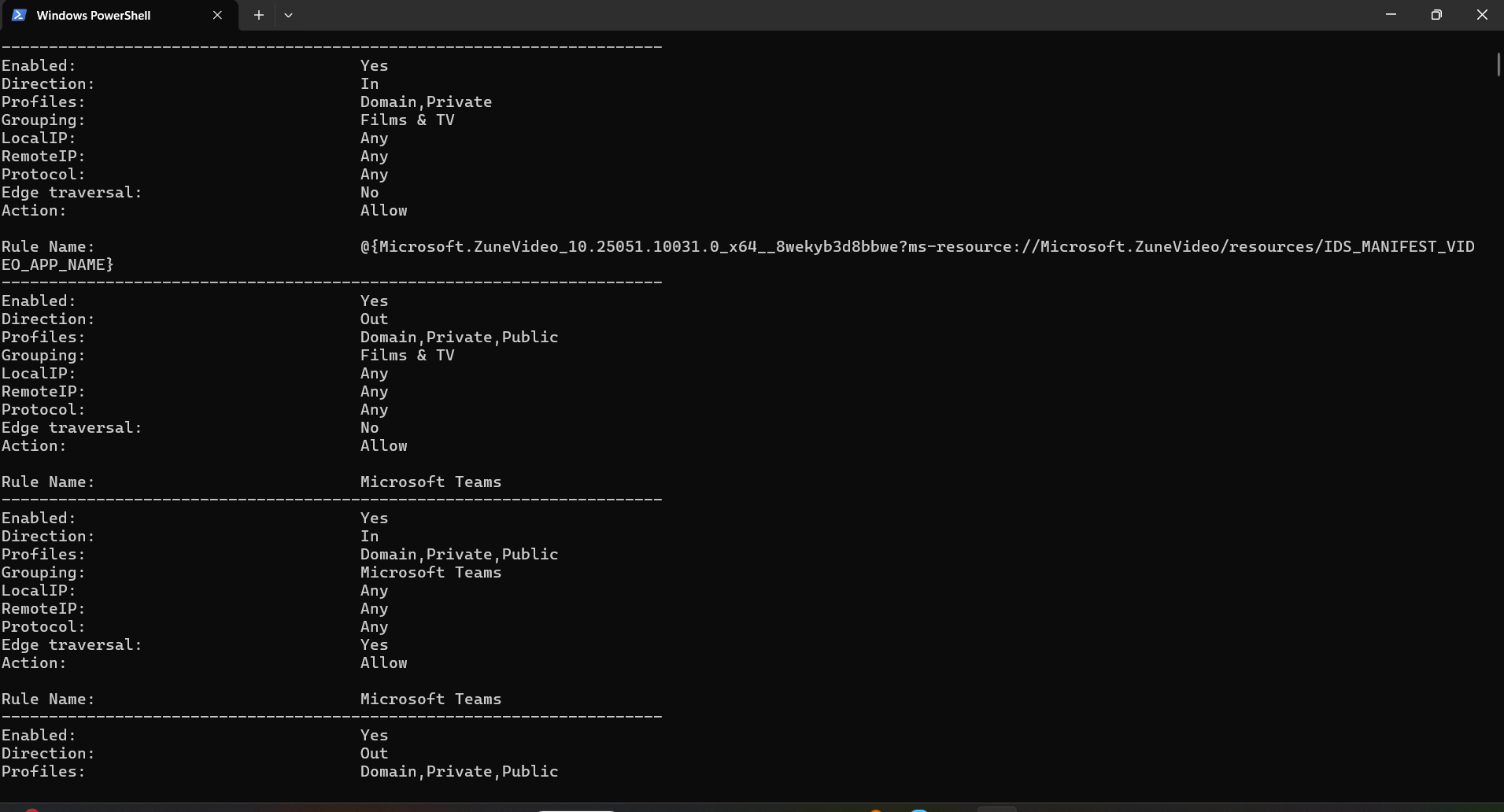
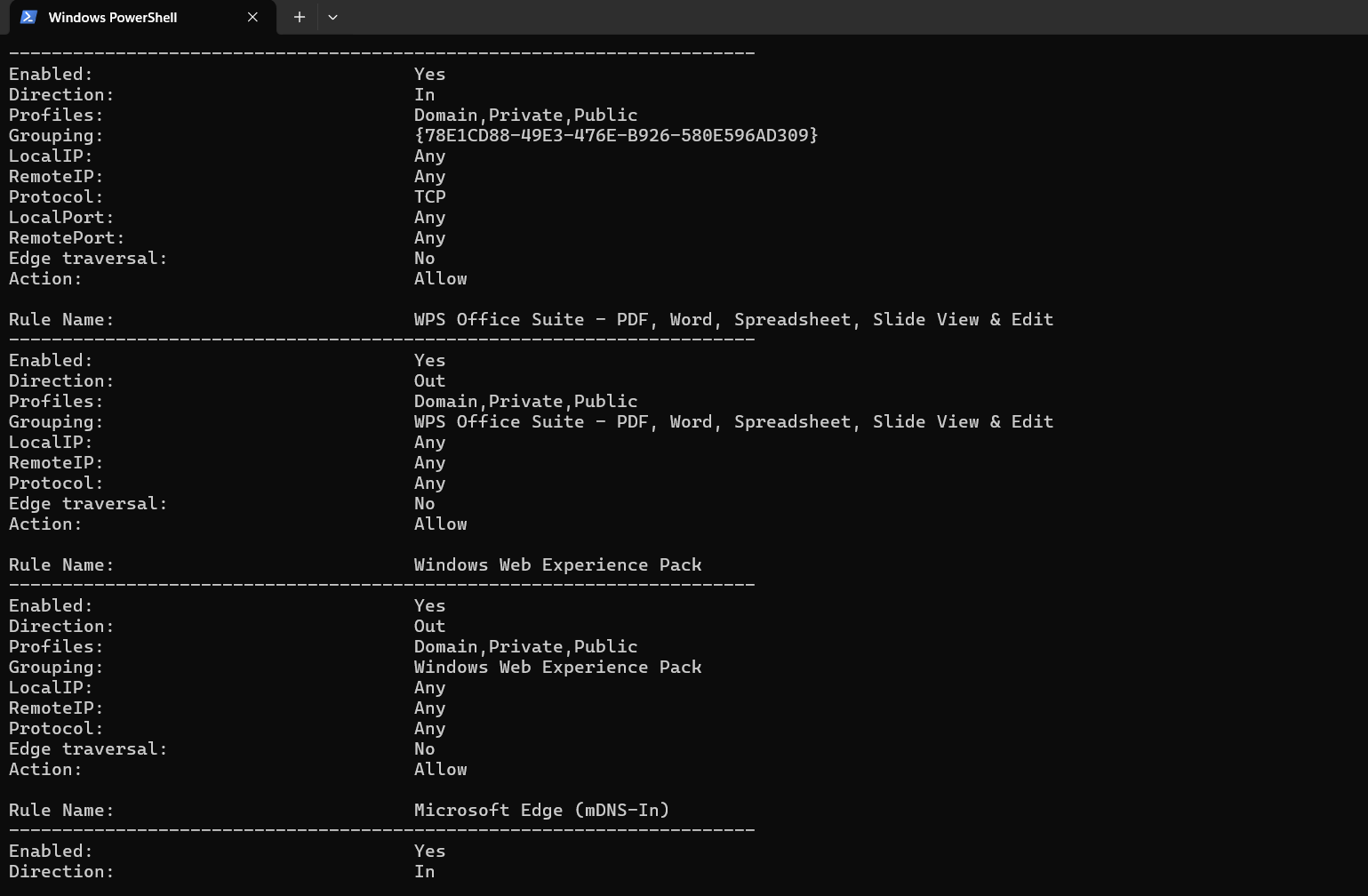
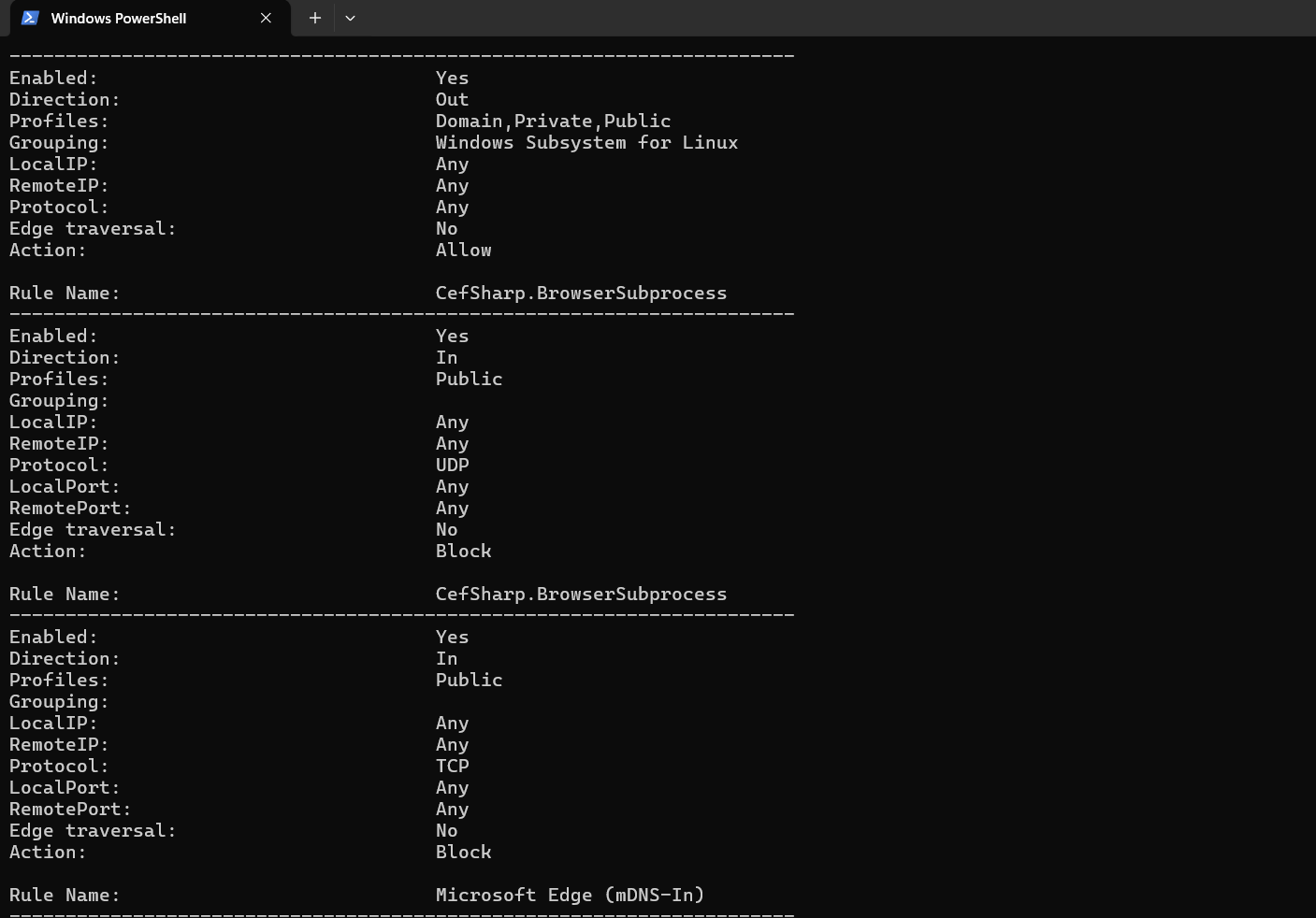
**TASK- 4**

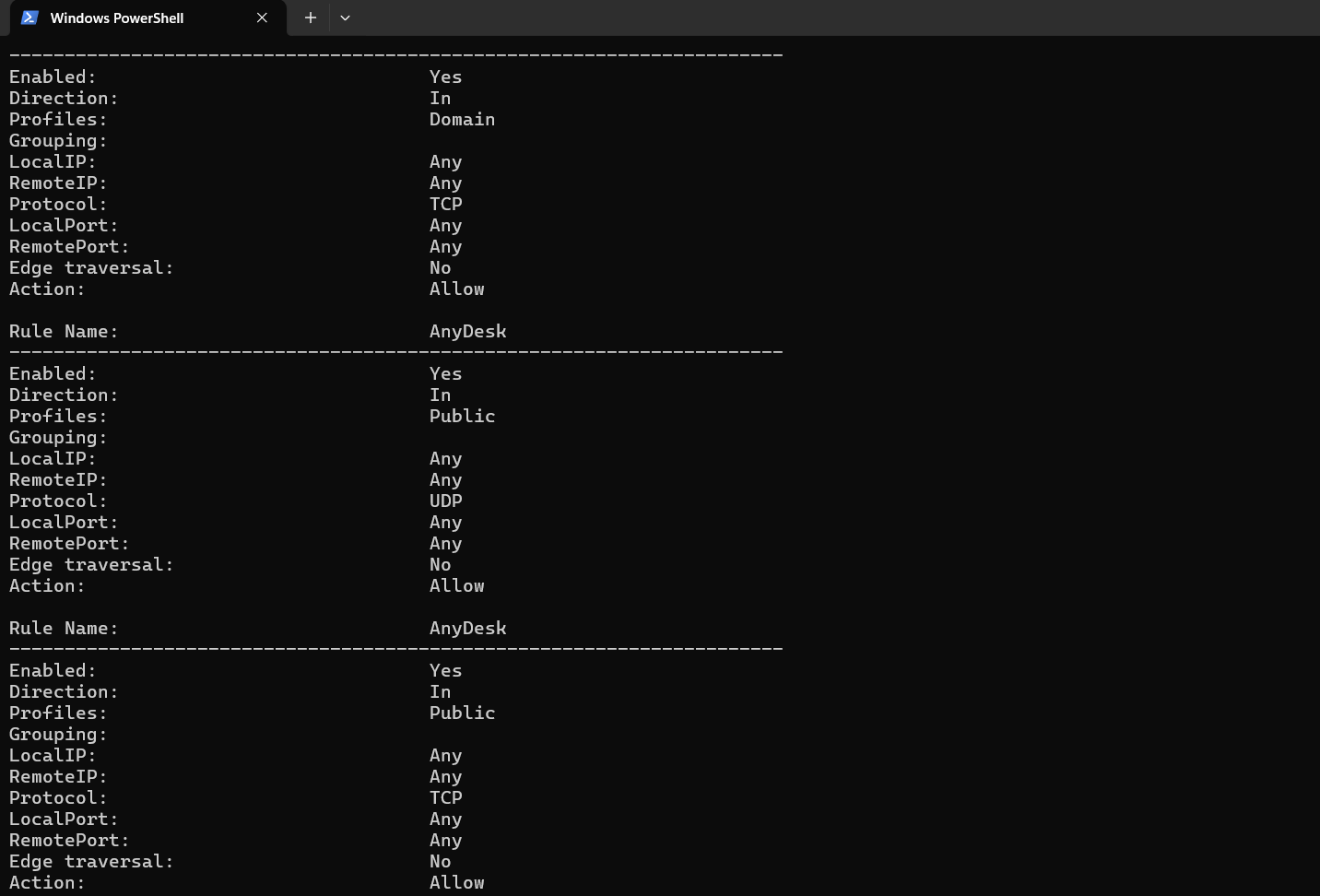
1. Current firewall rules:

Command: netsh advfirewall firewall show rule name=all







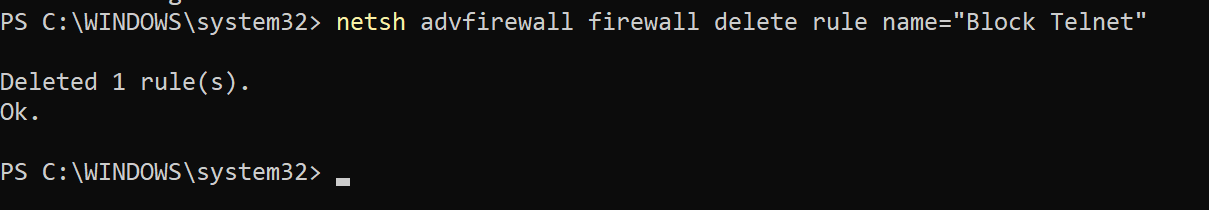


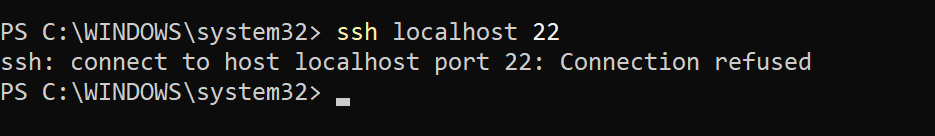
2. Blocking the port 23- TELNET

Command: netsh advfirewall firewall add rule name="Block Telnet" dir=in action=block protocol=TCP localport=23



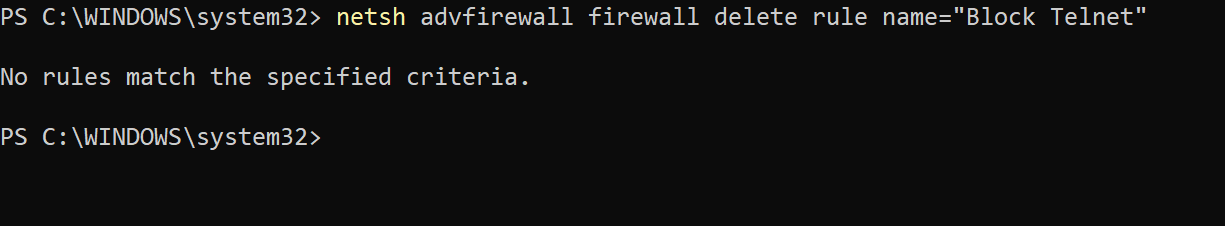
3. Blocking the port 22- SSH

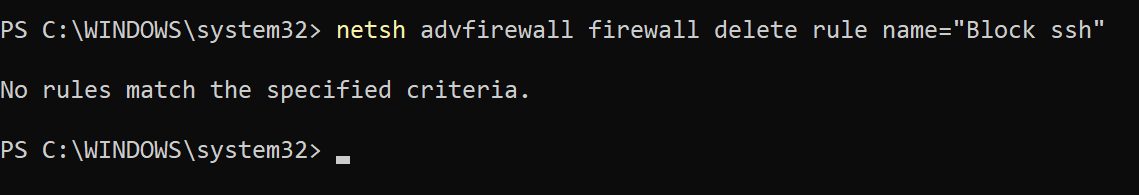




4. Removing the test block rules.

netsh advfirewall firewall delete rule name="Block Telnet"





Windows Firewall evaluates inbound and outbound rules against each network profile (Domain, Private, Public). It filters traffic based on:

– Application

– Port Number

– Protocol (TCP/UDP)

– Traffic Direction (Inbound/Outbound)

– IP Addresses

Each packet is matched against the rules. If no rule matches, the default behaviour applies (usually block inbound, allow outbound).