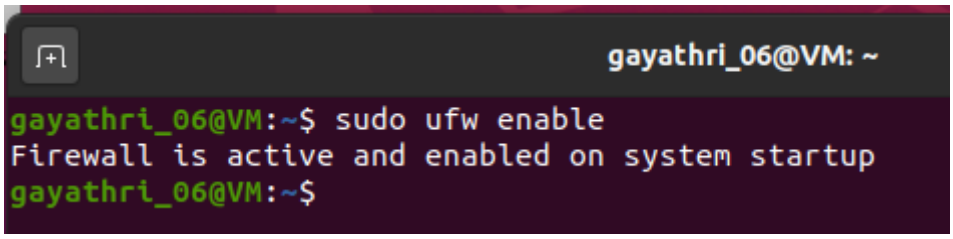
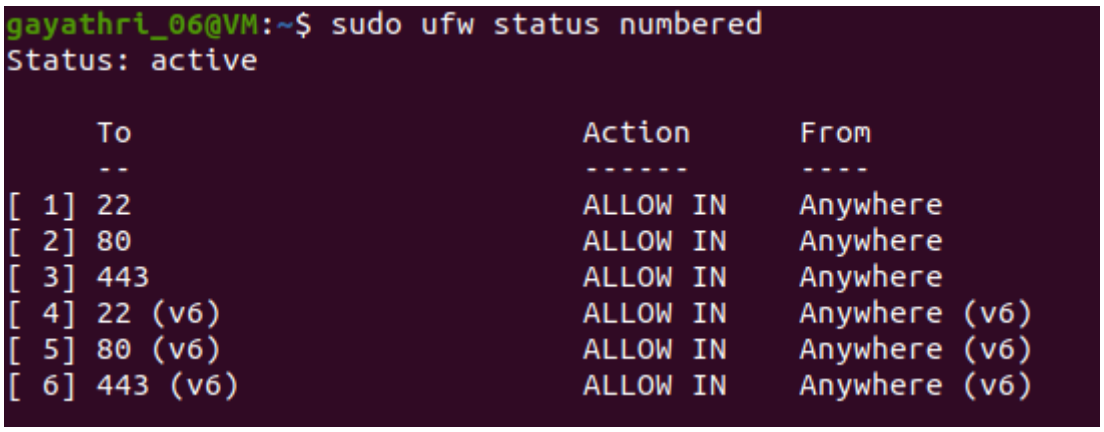
TASK 3: Setup and Use a Firewall on Windows/Linux

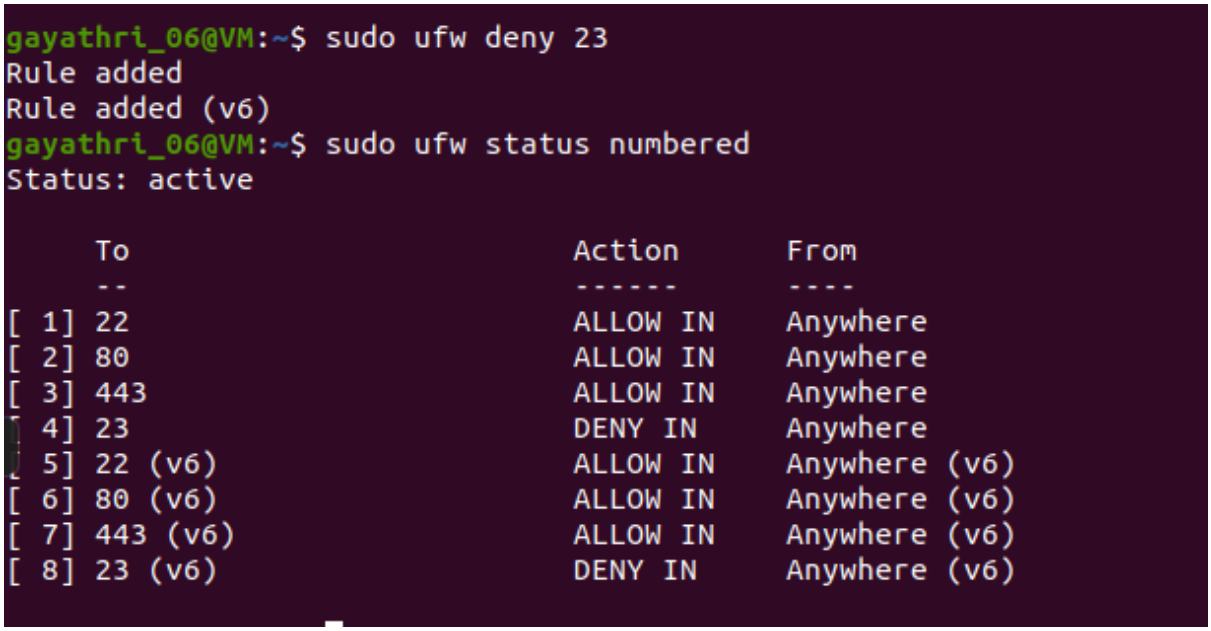
1.Open firewall configuration tool (Windows Firewall or terminal for UFW).



2.List current firewall rules.



3.Add a rule to block inbound traffic on a specific port (e.g., 23 for Telnet).



4.Test the rule by attempting to connect to that port locally or remotely.

```
gayathri_06@VM:~$ telnet localhost 23
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
VM login: gayathri_06
```

5.Add rule to allow SSH (port 22) if on Linux.

```
gayathri_06@VM:~$ sudo ufw allow 22
Skipping adding existing rule
Skipping adding existing rule (v6)
gayathri_06@VM:~$
```

6.Remove the test block rule to restore original state.

```
gayathri_06@VM:~$ sudo ufw delete 4
Deleting:
 deny 23
Proceed with operation (y|n)? y
Rule deleted
gayathri_06@VM:~$ sudo ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 22                         ALLOW IN    Anywhere
[ 2] 80                         ALLOW IN    Anywhere
[ 3] 443                        ALLOW IN    Anywhere
[ 4] 22 (v6)                    ALLOW IN    Anywhere (v6)
[ 5] 80 (v6)                    ALLOW IN    Anywhere (v6)
[ 6] 443 (v6)                   ALLOW IN    Anywhere (v6)
[ 7] 23 (v6)                    DENY IN     Anywhere (v6)
```

7.Document commands or GUI steps used.

8.Summarize how firewall filters traffic.

A firewall acts as a security gatekeeper by applying rules that allow or block traffic based on IP addresses, port numbers, and protocols. When a packet reaches a system, the firewall checks it against the list of rules in order. If a rule matches, the corresponding action (allow or deny) is applied. For UFW, the default behavior is to **deny all incoming** connections unless explicitly allowed, and to **allow all outgoing** connections. This ensures that only trusted services (like SSH or HTTP) are reachable from the outside, minimizing exposure to attacks while maintaining functionality for the user.