Task 4 - Setup and Use a Firewall on Windows/Linux

Objective: Configure and test basic firewall rules to allow or block traffic.

Tools: Windows Firewall / UFW (Uncomplicated Firewall) on Linux.

1.Search for "Windows Defender Firewall with Advanced Security".

2. Select Inbound Rules in the left pane to view the list.

3.

1) Right-click Inbound Rules →New Rule…

2) Rule Type: Port → Next

3) Protocol: TCP →Specific local ports: 23 →Next

4) Action: Block the connection → Next

5) Profile: Check all three (Domain, Private, Public) →Next \

6) Name: TEST_BLOCK_TELNET_23 → Finish

4) Test Rule Test with telnet as described above.

5) Remove Block Rule Find the rule TEST_BLOCK_TELNET_23 in Inbound Rules, right-click, and select Delete.

2. Linux - Uncomplicated Firewall (UFW - Terminal Commands)

1)Open Firewall Tool

sudo ufw status

2) List Current Rules

sudo ufw status numbered

3) Add Block Rule (Port 23)

sudo ufw deny 23/tcp

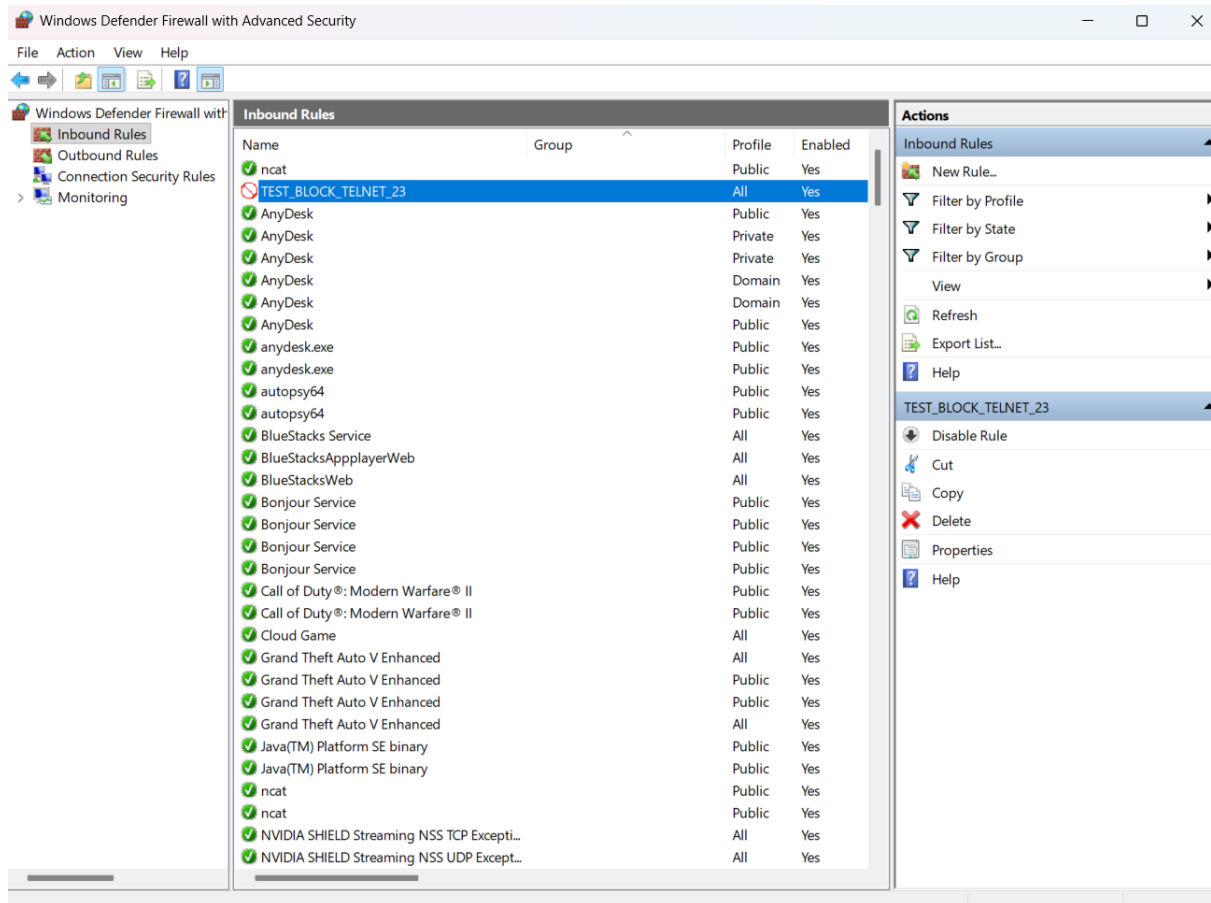4) Add SSH Rule (Port 22)

sudo ufw allow 22/tcp

5) Test Rule

From a remote machine, try connecting: telnet <IP> 23 (You should see a Connection refused or timeout).This confirms the rule is active.

6) Remove Block Rule

sudo ufw status numbered (find the number)

sudo ufw delete <RULE_NUMBER>

❖ Screenshots

```
┌──(root💀kali)-[/home/kali]
└─# ufw status
Status: active

To                        Action      From
--
80,443/tcp                ALLOW OUT   Anywhere
80,443/tcp (v6)           ALLOW OUT   Anywhere (v6)


┌──(root💀kali)-[/home/kali]
└─# ufw status numbered
Status: active

     To                   Action      From
     --
[ 1] 80,443/tcp           ALLOW OUT   Anywhere              (out)
[ 2] 80,443/tcp (v6)      ALLOW OUT   Anywhere (v6)         (out)
```

```
┌──(root💀kali)-[/home/kali]
└─# ufw allow 22/tcp
Rule added
Rule added (v6)

┌──(root💀kali)-[/home/kali]
└─# ufw status numbered
Status: active

     To                   Action      From
     --
[ 1] 80,443/tcp           ALLOW OUT   Anywhere              (out)
[ 2] 22/tcp               ALLOW IN    Anywhere
[ 3] 80,443/tcp (v6)      ALLOW OUT   Anywhere (v6)         (out)
[ 4] 22/tcp (v6)          ALLOW IN    Anywhere (v6)
```

```
┌──(root💀kali)-[/home/kali]
└─# ufw status numbered
Status: active

     To                   Action      From
     --
[ 1] 80,443/tcp           ALLOW OUT   Anywhere              (out)
[ 2] 22/tcp               ALLOW IN    Anywhere
[ 3] 80,443/tcp (v6)      ALLOW OUT   Anywhere (v6)         (out)


┌──(root💀kali)-[/home/kali]
└─# ufw delete 2
Deleting:
 allow 22/tcp
Proceed with operation (y|n)? y
Rule deleted
```