

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

Step 0: Install UFW (if not already installed)

- >sudo apt update
- >sudo apt install ufw

Step 1: Enable UFW

- >sudo ufw enable

Step 2: View current rules

- >sudo ufw status verbose

```
(kali㉿kali)-[~]  
$ sudo ufw status verbose  
  
Status: active  
Logging: on (low)  
Default: deny (incoming), allow (outgoing), disabled (routed)  
New profiles: skip
```

Step 3: Block a specific port (e.g., Port 23 – Telnet)

- >sudo ufw deny 23

```
(kali㉿kali)-[~]  
$ sudo ufw deny 23  
  
Rule added  
Rule added (v6)
```

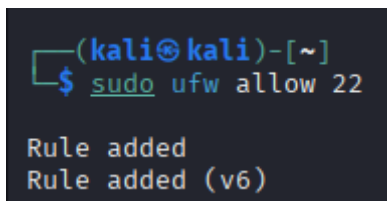
Step 4: Test the block rule

- >telnet localhost 23

```
(kali㉿kali)-[~]  
$ telnet localhost 23  
  
Trying ::1...  
Connection failed: Connection refused  
Trying 127.0.0.1...  
telnet: Unable to connect to remote host: Connection refused
```

Step 5: Allow SSH (port 22)

->sudo ufw allow 22



```
(kali㉿kali)-[~]  
$ sudo ufw allow 22  
  
Rule added  
Rule added (v6)
```

A terminal window with a dark background. The prompt is `(kali㉿kali)-[~]`. The user enters `$ sudo ufw allow 22`. The output shows two lines: `Rule added` and `Rule added (v6)`.

Step 6: Remove test block rule (cleanup)

->sudo ufw delete deny 23