

**HARSH GUPTA**

## **ELEVATE LABS TASK -4**

**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. Deliverables: Screenshot/configuration file showing firewall rules applied.**

### **TASK Linux (Using UFW)**

#### **Steps:**

1. **Open Terminal & Check Status:**

```
(kali㉿kali)-[~]  
$ sudo ufw status verbose # List rules (default: inactive)  
Status: inactive
```

2. **Enable UFW & Allow SSH First:**

```
(kali㉿kali)-[~]  
$ sudo ufw allow 22  
Rules updated  
Rules updated (v6)  
  
(kali㉿kali)-[~]  
$ sudo ufw enable  
Firewall is active and enabled on system startup
```

3. **Block Port 23 (Telnet):**

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

4. **Test the Rule:**

- **Locally:**

```
(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
```

5. **Remove Test Rule:**

```
(kali㉿kali)-[~]  
$ sudo ufw delete deny 23  
Rule deleted  
Rule deleted (v6)  
  
(kali㉿kali)-[~]  
$ sudo ufw reload  
Firewall reloaded
```

## 6. Documentation:

- Enabled UFW: ``sudo ufw enable``
- Allowed SSH: ``sudo ufw allow 22``
- Blocked Telnet: ``sudo ufw deny 23``
- Tested: ``telnet localhost 23``
- Deleted rule: ``sudo ufw delete deny 23``

---

## Summary: How Firewalls Filter Traffic

Firewalls act as gatekeepers between your device and networks:

### 1. Rules-Based Filtering:

- **Allow/Deny:** Explicit rules permit/block traffic based on ports, IPs, or protocols.
- **Direction:** Controls inbound (ingress) or outbound (egress) traffic.

### 2. Stateful Inspection:

- Tracks active connections (e.g., allows reply traffic for an established SSH session).

### 3. Default Policies:

- Linux UFW: Default deny (incoming) / allow (outgoing).
- Windows: Default rules permit common services (e.g., DHCP).

This exercise demonstrated core firewall management:

- Creating/removing rules to control traffic.
- Testing rules to validate security policies.
- Understanding stateful filtering fundamentals.

**Key Takeaway:** Firewalls enforce least-privilege access—block everything by default, allow only essential services.

