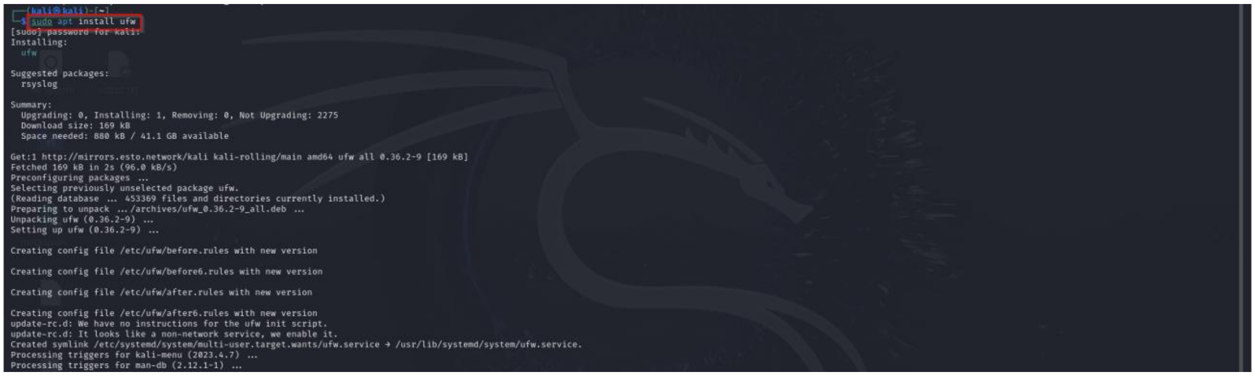
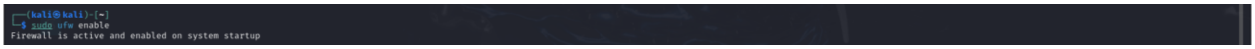
Task 4: Setup and Use a Firewall on Windows/Linux

Objective: Basic firewall management skills and understanding of network traffic filtering

- Step 1: **Linux (UFW):**
- Open a terminal.
- Make sure UFW is installed: sudo apt install ufw
- Enable if not already: sudo ufw enable



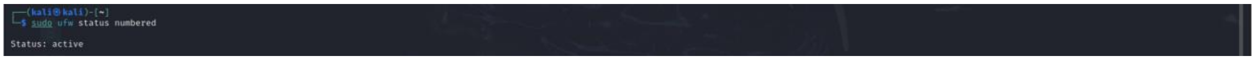
```
┌──(kali㉿kali)-[~]
└─$ sudo apt install ufw
[sudo] password for kali:
Installing:
  ufw

Suggested packages:
  rsyslog

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 2275
  Download size: 169 kB
  Space needed: 880 kB / 41.1 GB available

Get:1 http://mirrors.esto.network/kali kali-rolling/main amd64 ufw all 0.36.2-9 [169 kB]
Fetched 169 kB in 2s (96.0 kB/s)
Preconfiguring packages ...
Selecting previously unselected package ufw.
(Reading database ... 453369 files and directories currently installed.)
Preparing to unpack .../archives/ufw_0.36.2-9_all.deb ...
Unpacking ufw (0.36.2-9) ...
Setting up ufw (0.36.2-9) ...

Creating config file /etc/ufw/before.rules with new version

Creating config file /etc/ufw/before6.rules with new version

Creating config file /etc/ufw/after.rules with new version

Creating config file /etc/ufw/after6.rules with new version
update-rc.d: We have no instructions for the ufw init script.
update-rc.d: It looks like a non-network service, we enable it.
Created symlink /etc/systemd/system/multi-user.target.wants/ufw.service → /usr/lib/systemd/system/ufw.service.
Processing triggers for kali-menu (2023.4.7) ...
Processing triggers for man-db (2.12.1-1) ...
```



```
┌──(kali㉿kali)-[~]
└─$ sudo ufw enable
Firewall is active and enabled on system startup
```

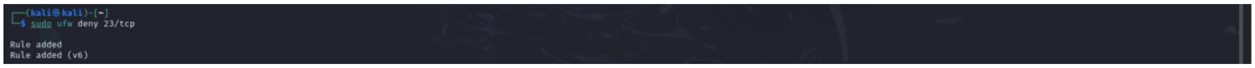
- Step 2: List Current Firewall Rules

Command: sudo ufw status numbered



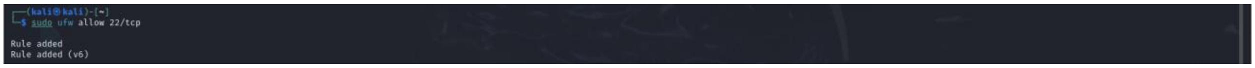
```
┌──(kali㉿kali)-[~]
└─$ sudo ufw status numbered

Status: active
```

- Step 3: Add a Rule to Block Inbound Traffic on a Specific Port (e.g., 23 – Telnet-+)



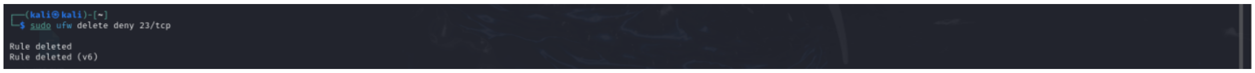
```
┌──(kali㉿kali)-[~]
└─$ sudo ufw deny 23/tcp

Rule added
Rule added (v6)
```

- Step 4: Add Rule to Allow SSH (Port 22) if on Linux



```
┌──(kali㉿kali)-[~]
└─$ sudo ufw allow 22/tcp

Rule added
Rule added (v6)
```

- Step 5: Remove the Test Block Rule to Restore Original State



```
┌──(kali㉿kali)-[~]
└─$ sudo ufw delete deny 23/tcp

Rule deleted
Rule deleted (v6)
```

- Step 6: **Summarize How Firewall Filters Traffic**
- A firewall acts as a **traffic filter** between your system/network and external networks.
- It uses **rules** to decide whether to **allow**, **deny**, or **block** packets based on **source/destination IP**, **port number**, **protocol (TCP/UDP)**, and **direction** (inbound/outbound).
- This helps prevent unauthorized access and limits exposure to attacks.