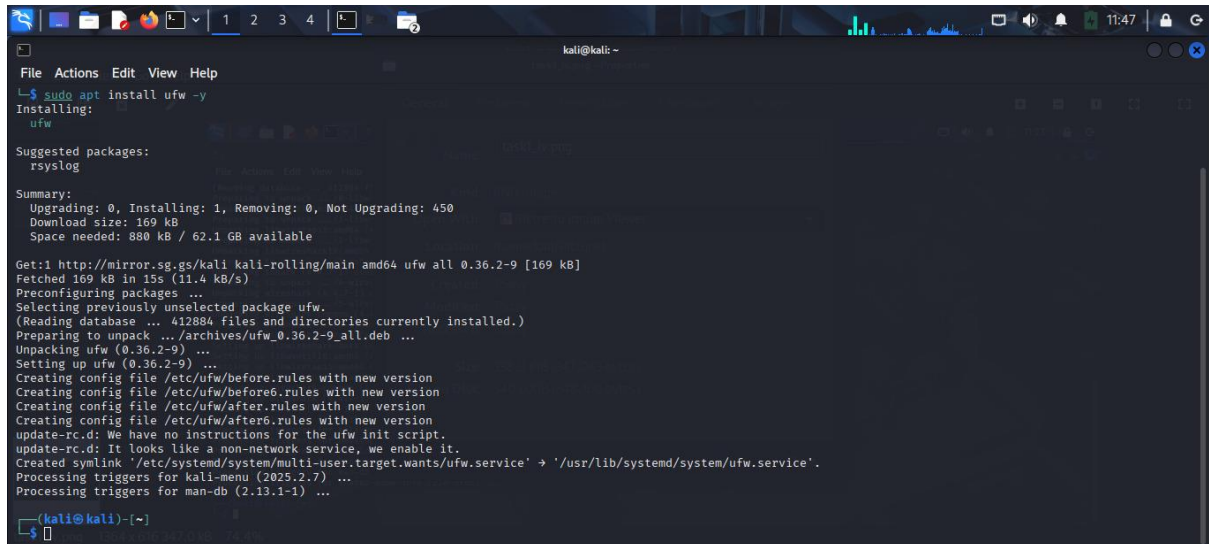


Task 4

Task 4. Setup and use a firewall on windows/linux

Step 1: Install and enable UFW

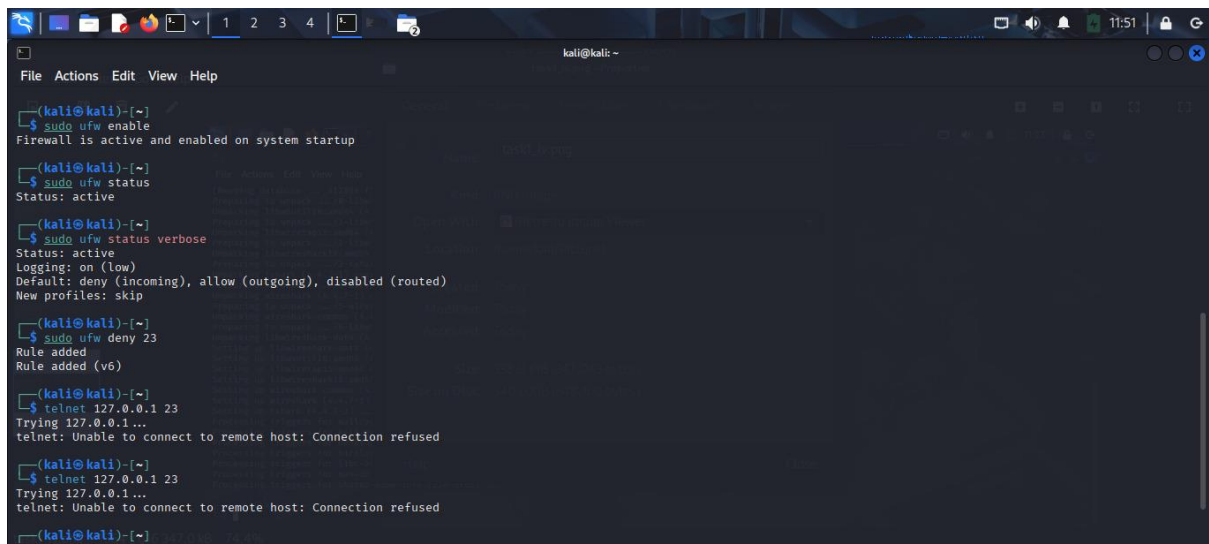


```
kali@kali: ~  
File Actions Edit View Help  
~$ sudo apt install ufw -y  
Installing:  
ufw  
  
Suggested packages:  
rsyslog  
  
Summary:  
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 450  
  Download size: 169 kB  
  Space needed: 880 kB / 62.1 GB available  
  
Get:1 http://mirror.sg.gs/kali kali-rolling/main amd64 ufw all 0.36.2-9 [169 kB]  
Fetched 169 kB in 15s (11.4 kB/s)  
Preconfiguring packages ...  
Selecting previously unselected package ufw.  
(Reading database ... 412884 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 (2025.2-7) ...  
Processing triggers for man-db (2.13.1-1) ...  
  
kali@kali:~$
```

Step 2: List current firewall rules

Step 3: Add rule to block inbound traffic on port 23

Step 4: Test the rule



```
(kali@kali)-[~]  
$ sudo ufw enable  
Firewall is active and enabled on system startup  
  
(kali@kali)-[~]  
$ sudo ufw status  
Status: active  
  
(kali@kali)-[~]  
$ sudo ufw status verbose  
Status: active  
Logging: on (low)  
Default: deny (incoming), allow (outgoing), disabled (routed)  
New profiles: skip  
  
(kali@kali)-[~]  
$ sudo ufw deny 23  
Rule added  
Rule added (v6)  
  
(kali@kali)-[~]  
$ telnet 127.0.0.1 23  
Trying 127.0.0.1...  
telnet: Unable to connect to remote host: Connection refused  
  
(kali@kali)-[~]  
$ telnet 127.0.0.1 23  
Trying 127.0.0.1...  
telnet: Unable to connect to remote host: Connection refused  
  
(kali@kali)-[~]
```

Step 5: Remove the telnet block rule

```
(kali@kali)~$ telnet 127.0.0.1 23
Trying 127.0.0.1...
telnet: Unable to connect to remote host: Connection refused

(kali@kali)~$ sudo ufw delete deny 23
Rule deleted
Rule deleted (v6)

(kali@kali)~$
```

Summary:

A firewall filters traffic by allowing or blocking data packets based on predefined rules.

It can control traffic based on IP address, port number, or protocol.

In this test, UFW blocked Telnet (port 23) and allowed SSH (port 22).