TASK 4

Setup and Use a Firewall on Windows/Linux

MAY 30, 2025

PRADEEP U S
pradeep.ustd@gmail.com

Firewall Configuration with UFW on Kali Linux

To configure and test firewall rules using UFW on Kali Linux, including:

- Blocking and allowing specific ports
- Testing connectivity
- Reverting changes
- Understanding how firewalls filter traffic

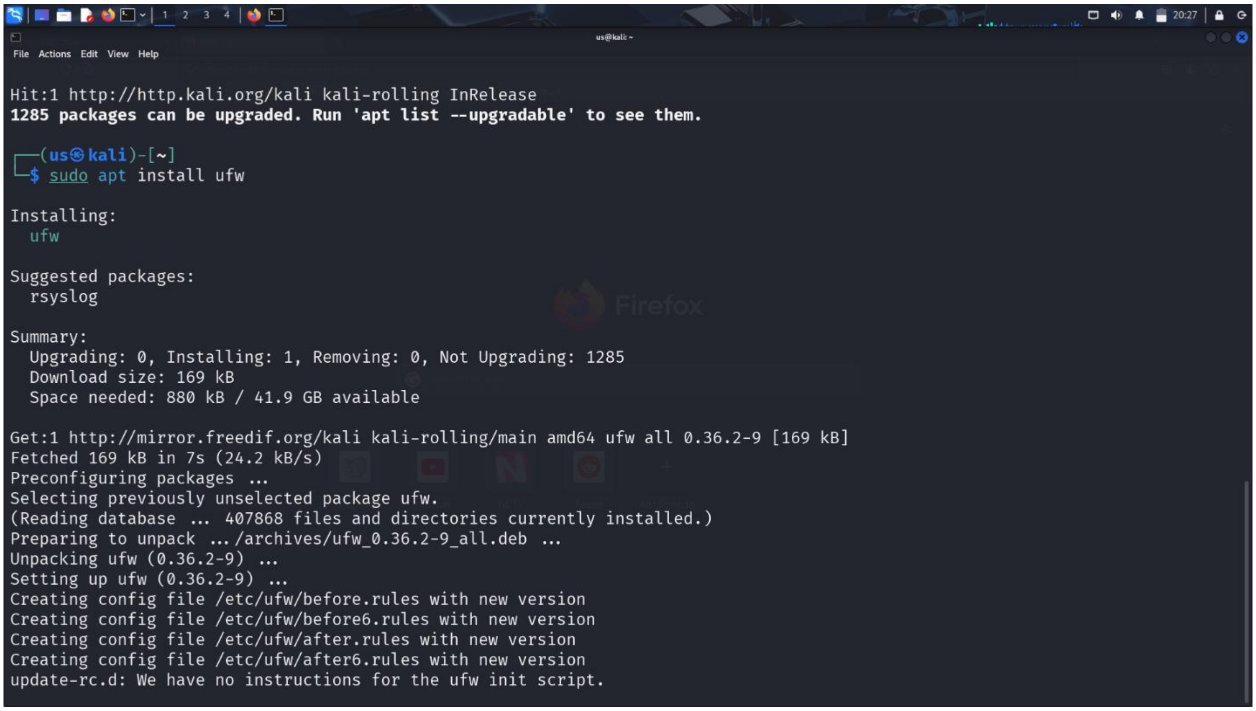
Environment

- OS: Kali Linux
- Firewall Tool: UFW
- Network Utility: Telnet

Steps

1) Installtion of UFW

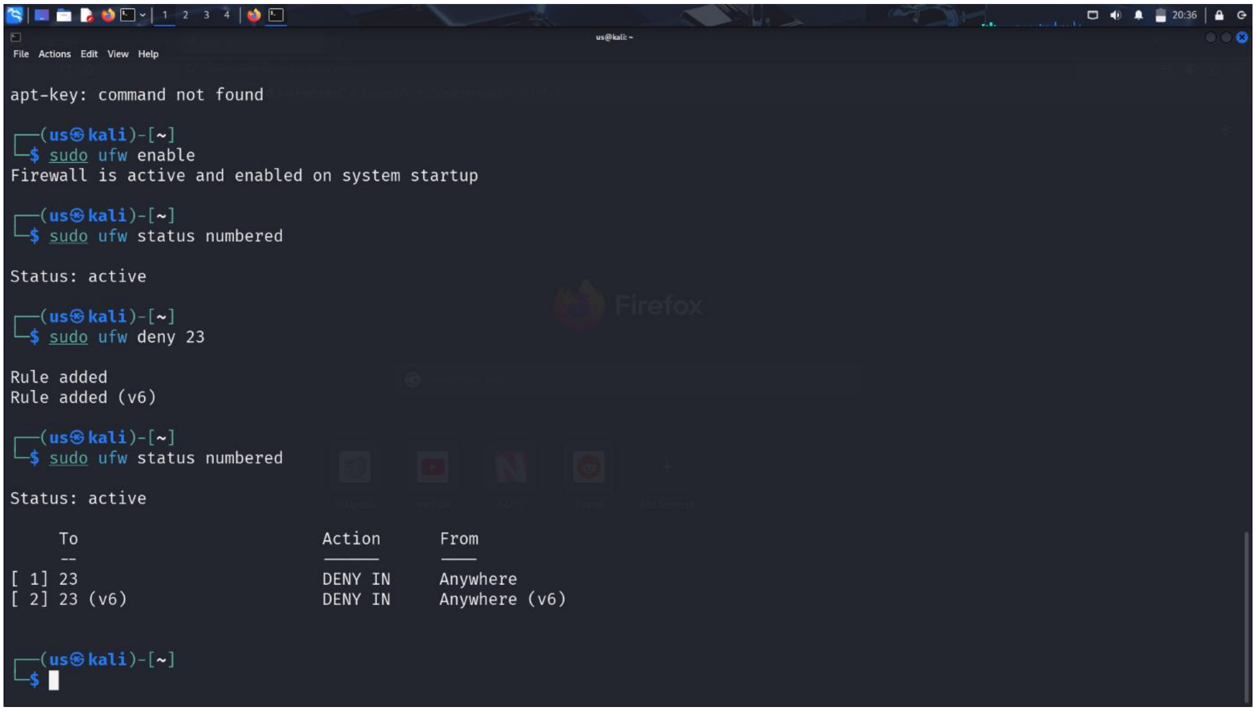
```
sudo apt install ufw
```



```
Hit:1 http://http.kali.org/kali kali-rolling InRelease
1285 packages can be upgraded. Run 'apt list --upgradable' to see them.

┌──(us㉿kali)-[~]
└─$ sudo apt install ufw

Installing:
  ufw

Suggested packages:
  rsyslog

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 1285
  Download size: 169 kB
  Space needed: 880 kB / 41.9 GB available

Get:1 http://mirror.freedif.org/kali kali-rolling/main amd64 ufw all 0.36.2-9 [169 kB]
Fetched 169 kB in 7s (24.2 kB/s)
Preconfiguring packages ...
Selecting previously unselected package ufw.
(Reading database ... 407868 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.
```

2) Enable UFW & Block Inbound Traffic on Port 23 (Telnet)

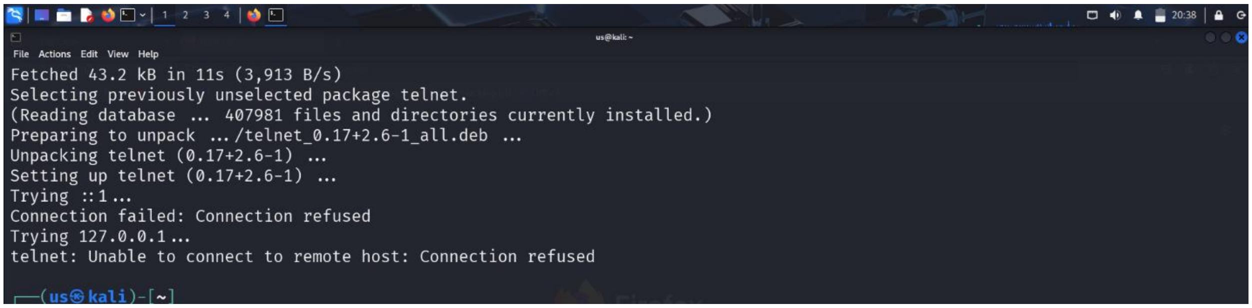
```
sudo ufw enable
sudo ufw deny 23
```



```
apt-key: command not found

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

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

Status: active

┌──(us㉿kali)-[~]
└─$ sudo ufw deny 23

Rule added
Rule added (v6)

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

Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 23                         DENY IN     Anywhere
[ 2] 23 (v6)                    DENY IN     Anywhere (v6)


┌──(us㉿kali)-[~]
└─$ 
```

3)Test the Block Rule

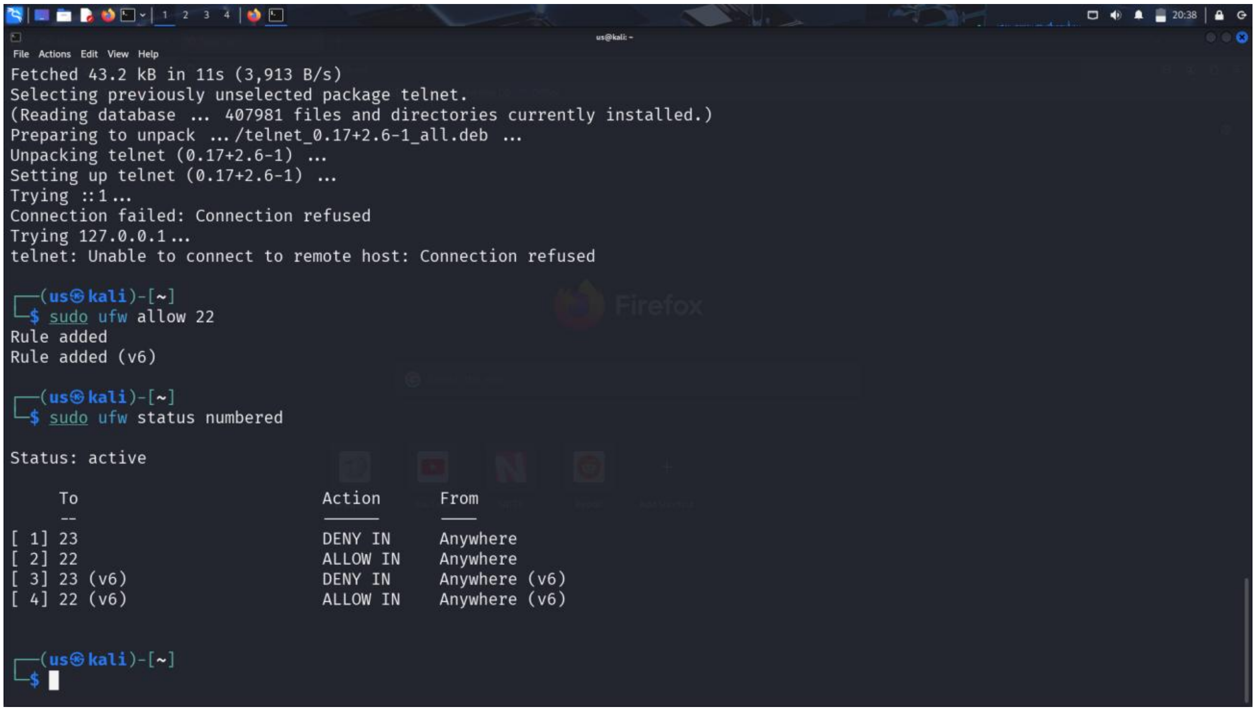
```
sudo apt install telnet

telnet localhost 23
```



```
Fetched 43.2 kB in 11s (3,913 B/s)
Selecting previously unselected package telnet.
(Reading database ... 407981 files and directories currently installed.)
Preparing to unpack .../telnet_0.17+2.6-1_all.deb ...
Unpacking telnet (0.17+2.6-1) ...
Setting up telnet (0.17+2.6-1) ...
Trying ::1...
Connection failed: Connection refused
Trying 127.0.0.1...
telnet: Unable to connect to remote host: Connection refused

┌──(us㉿kali)-[~]
```

4)Allow SSH (Port 22)

```
sudo ufw allow 22
```



```
Fetched 43.2 kB in 11s (3,913 B/s)
Selecting previously unselected package telnet.
(Reading database ... 407981 files and directories currently installed.)
Preparing to unpack .../telnet_0.17+2.6-1_all.deb ...
Unpacking telnet (0.17+2.6-1) ...
Setting up telnet (0.17+2.6-1) ...
Trying ::1...
Connection failed: Connection refused
Trying 127.0.0.1...
telnet: Unable to connect to remote host: Connection refused

┌──(us㉿kali)-[~]
└─$ sudo ufw allow 22
Rule added
Rule added (v6)

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

Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 23                         DENY IN     Anywhere
[ 2] 22                         ALLOW IN    Anywhere
[ 3] 23 (v6)                    DENY IN     Anywhere (v6)
[ 4] 22 (v6)                    ALLOW IN    Anywhere (v6)


┌──(us㉿kali)-[~]
└─$ 
```

How Firewalls Filter Traffic

Firewalls monitor network **traffic flow** and apply **rules** based on:

- Port numbers
- IP addresses
- Protocols (TCP/UDP)
- Traffic direction

Conclusion

We,

- Installed and enabled the firewall
- Blocked a vulnerable service (Telnet)
- Tested the block
- Allowed secure services (SSH)
- Reverted rules safely

This helps in minimizing attack surfaces and securing Linux systems.