

Task 4: Setup and Use a Firewall on Linux (UFW)

Objective

Configure and test basic firewall rules to allow or block traffic.

Tools

UFW (Uncomplicated Firewall) on Kali Linux.

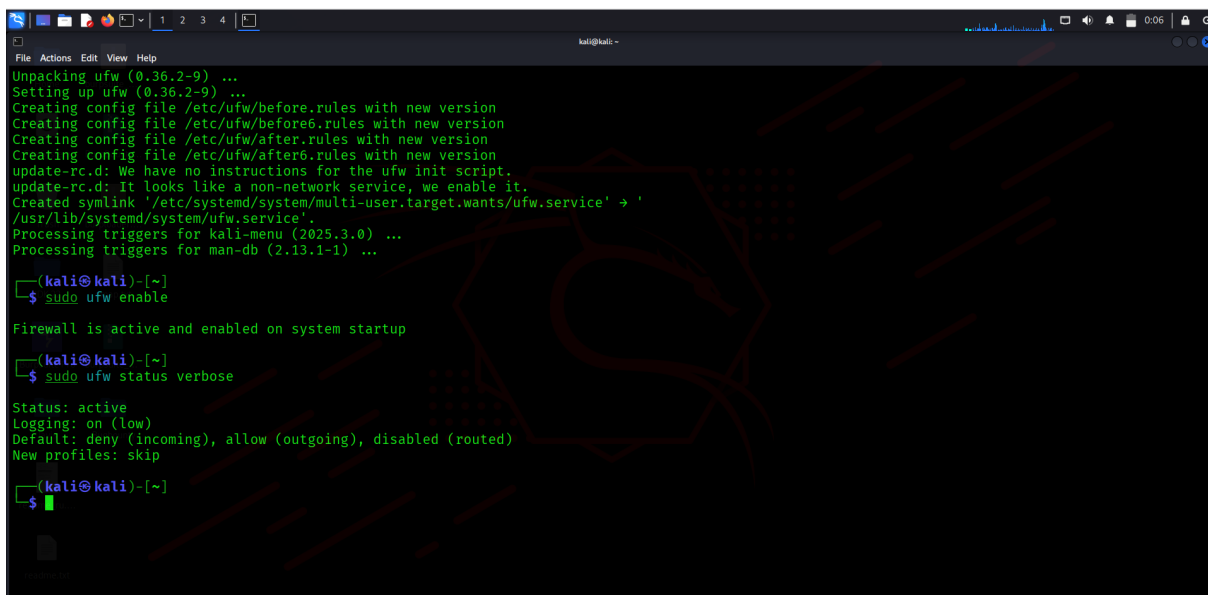
Steps & Screenshots

1. Enable UFW:

```
sudo apt install ufw -y
```

```
sudo ufw enable
```

```
sudo ufw status verbose
```

A screenshot of a Kali Linux terminal window. The terminal shows the output of the command 'sudo apt install ufw -y', which includes messages about unpacking ufw (0.36.2-9), setting it up, and creating configuration files. It also shows the output of 'sudo ufw enable', which states 'Firewall is active and enabled on system startup'. Finally, it shows the output of 'sudo ufw status verbose', which displays the status as 'active', logging as 'on (low)', default as 'deny (incoming), allow (outgoing), disabled (routed)', and new profiles as 'skip'. The terminal window has a dark background with a red dragon logo in the background.

```
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 (2025.3.0) ...
Processing triggers for man-db (2.13.1-1) ...

(kali@kali)-[~]
$ sudo ufw enable

Firewall is active and enabled on system startup

(kali@kali)-[~]
$ sudo ufw status verbose

Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

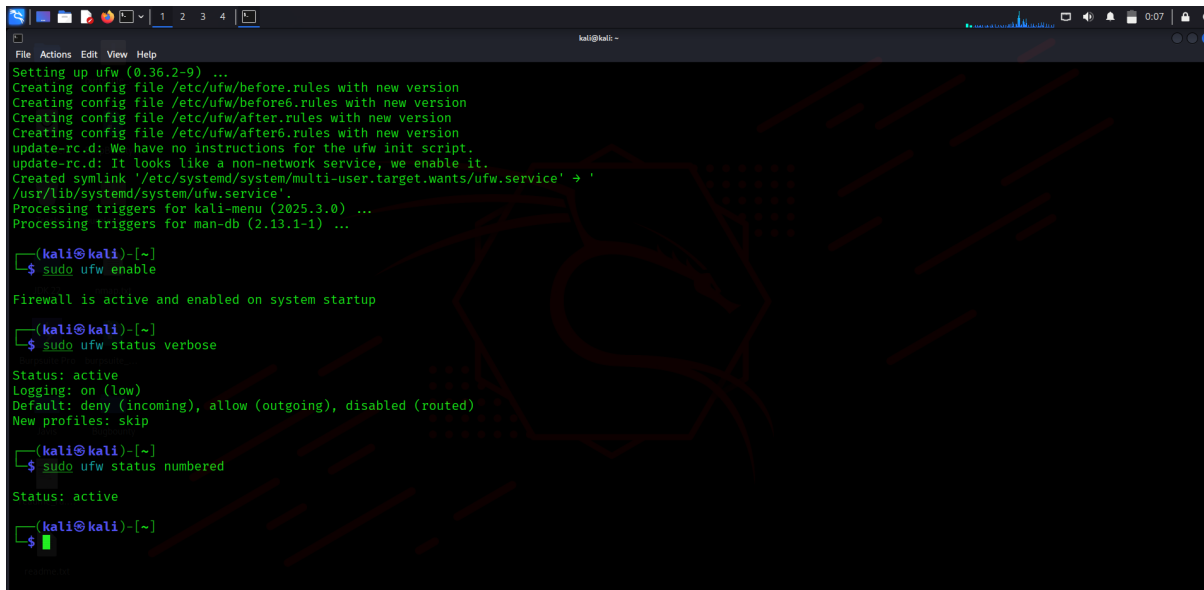
(kali@kali)-[~]
$
```

Screenshot 1: UFW enabled and showing status.

2. List Current Rules:

```
sudo ufw status numbered
```

Task 4: Setup and Use a Firewall on Linux (UFW)

A terminal window on a Kali Linux system showing the setup of UFW. The terminal output includes messages about creating config files, enabling the service, and checking its status. The status is active, with logging on (low) and default deny for incoming traffic.

```
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 (2025.3.0) ...
Processing triggers for man-db (2.13.1-1) ...

(kali@kali)~$ sudo ufw enable

Firewall is active and enabled on system startup

(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 status numbered

Status: active

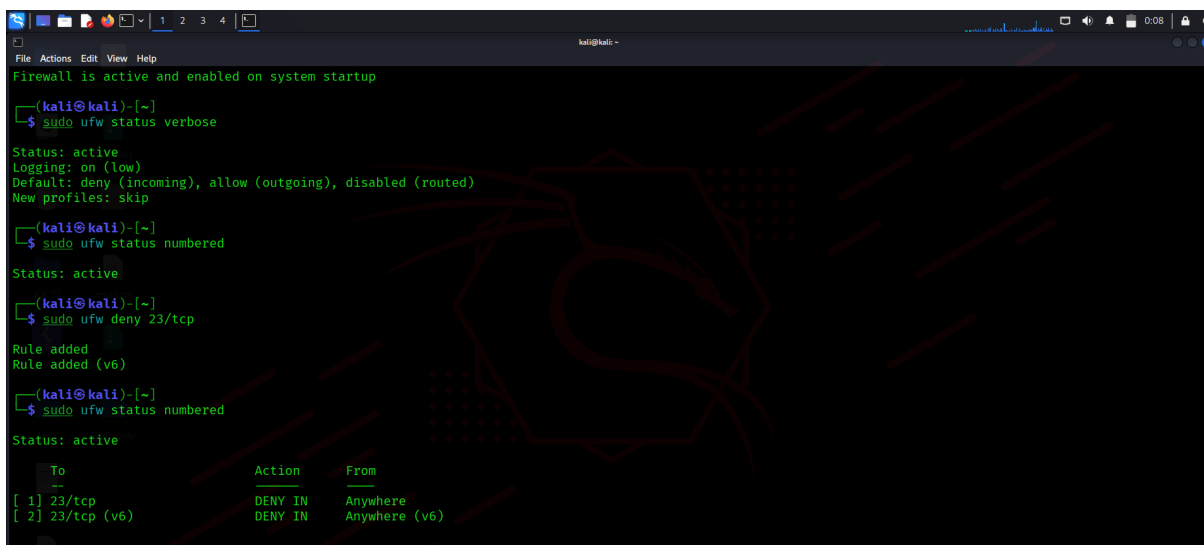
(kali@kali)~$
```

Screenshot 2: List of existing firewall rules.

3. Block Inbound Traffic on Port 23 (Telnet):

```
sudo ufw deny 23/tcp
```

```
sudo ufw status numbered
```

A terminal window on a Kali Linux system showing the addition of a deny rule for port 23/tcp. The terminal output shows the rule being added and the updated status, which now includes the new rule in the numbered list.

```
Firewall is active and enabled on system startup

(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 status numbered

Status: active

(kali@kali)~$ sudo ufw deny 23/tcp

Rule added
Rule added (v6)

(kali@kali)~$ sudo ufw status numbered

Status: active

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

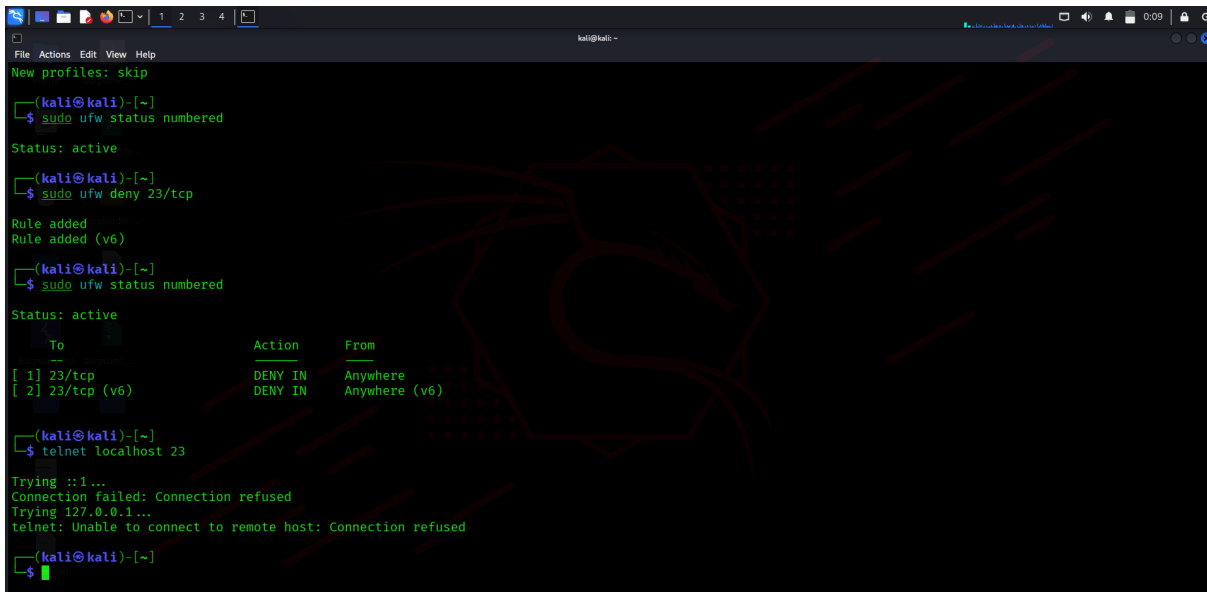
(kali@kali)~$
```

Screenshot 3: Rules showing DENY 23/tcp.

4. Test the Rule:

```
telnet localhost 23
```

Task 4: Setup and Use a Firewall on Linux (UFW)

A terminal window on a Kali Linux system. The user runs 'sudo ufw status numbered', which shows the firewall is active with two rules: rule 1 denies 23/tcp and rule 2 denies 23/tcp (v6). The user then runs 'telnet localhost 23', which fails with 'Connection refused'.

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

Status: active
(kali㉿kali)-[~]
$ sudo ufw deny 23/tcp

Rule added
Rule added (v6)
(kali㉿kali)-[~]
$ sudo ufw status numbered

Status: active
    To Action From
    --
[ 1] 23/tcp DENY IN Anywhere
[ 2] 23/tcp (v6) DENY IN Anywhere (v6)
(kali㉿kali)-[~]
$ telnet localhost 23

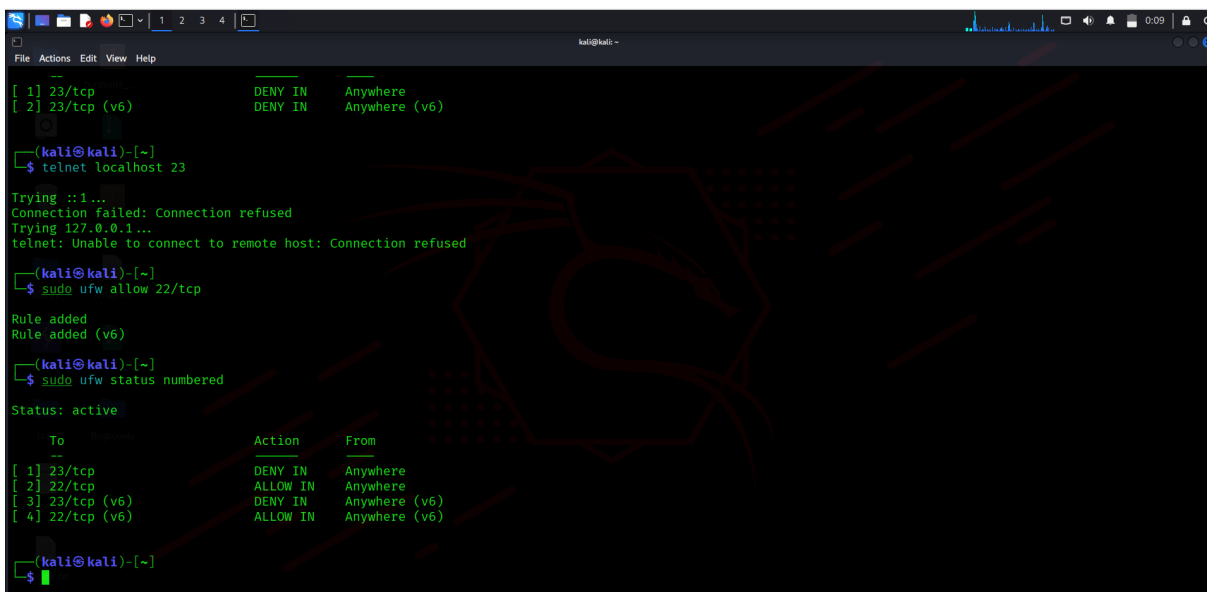
Trying ::1...
Connection failed: Connection refused
Trying 127.0.0.1...
telnet: Unable to connect to remote host: Connection refused
(kali㉿kali)-[~]
$
```

Screenshot 4: Telnet connection attempt failing.

5. Allow SSH (Port 22):

```
sudo ufw allow 22/tcp
```

```
sudo ufw status numbered
```

A terminal window on a Kali Linux system. The user runs 'sudo ufw allow 22/tcp', which adds rule 3 allowing 22/tcp. The user then runs 'sudo ufw status numbered', which shows four rules: rule 1 denies 23/tcp, rule 2 denies 23/tcp (v6), rule 3 allows 22/tcp, and rule 4 allows 22/tcp (v6).

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

Rule added
Rule added (v6)
(kali㉿kali)-[~]
$ sudo ufw status numbered

Status: active
    To Action From
    --
[ 1] 23/tcp DENY IN Anywhere
[ 2] 23/tcp (v6) DENY IN Anywhere (v6)
[ 3] 22/tcp ALLOW IN Anywhere
[ 4] 22/tcp (v6) ALLOW IN Anywhere (v6)
(kali㉿kali)-[~]
$
```

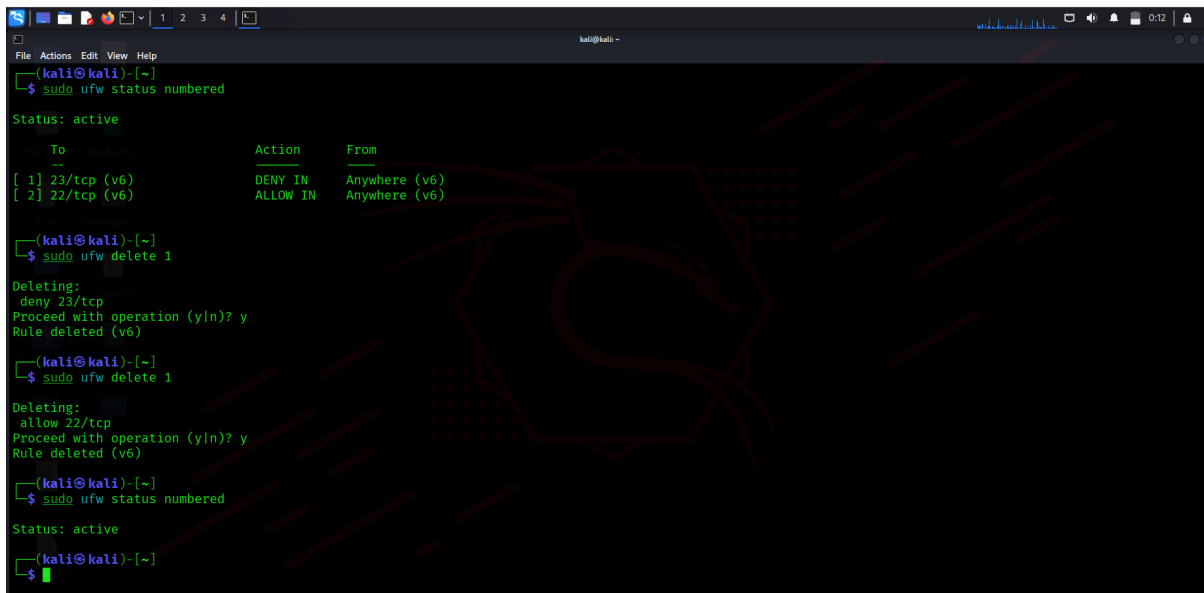
Screenshot 5: Rules showing ALLOW 22/tcp.

6. Remove the Block Rule:

```
sudo ufw delete <rule_number>
```

```
sudo ufw status numbered
```

Task 4: Setup and Use a Firewall on Linux (UFW)

A terminal window on a Kali Linux system showing the configuration of UFW. The user runs 'sudo ufw status numbered' which shows two rules: rule 1 denying port 23/tcp and rule 2 allowing port 22/tcp. Then, the user runs 'sudo ufw delete 1' to remove the first rule, followed by 'sudo ufw delete 1' again to remove the second rule. Finally, 'sudo ufw status numbered' is run again, showing that UFW is active but no rules are listed.

```
(kali@kali)~$ sudo ufw status numbered
Status: active

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

(kali@kali)~$ sudo ufw delete 1
Deleting:
deny 23/tcp
Proceed with operation (y/n)? y
Rule deleted (v6)

(kali@kali)~$ sudo ufw delete 1
Deleting:
allow 22/tcp
Proceed with operation (y/n)? y
Rule deleted (v6)

(kali@kali)~$ sudo ufw status numbered
Status: active

(kali@kali)~$
```

Screenshot 6: Rules list after removing Telnet block.

Summary

UFW is a user-friendly firewall management tool for Linux. It works by controlling incoming and outgoing traffic based on predefined rules. In this task, we:

- Enabled UFW and viewed current rules.
- Added a rule to block port 23 (Telnet).
- Tested the rule to confirm traffic was blocked.
- Allowed SSH access on port 22.
- Removed the Telnet block rule to restore the original state.