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.

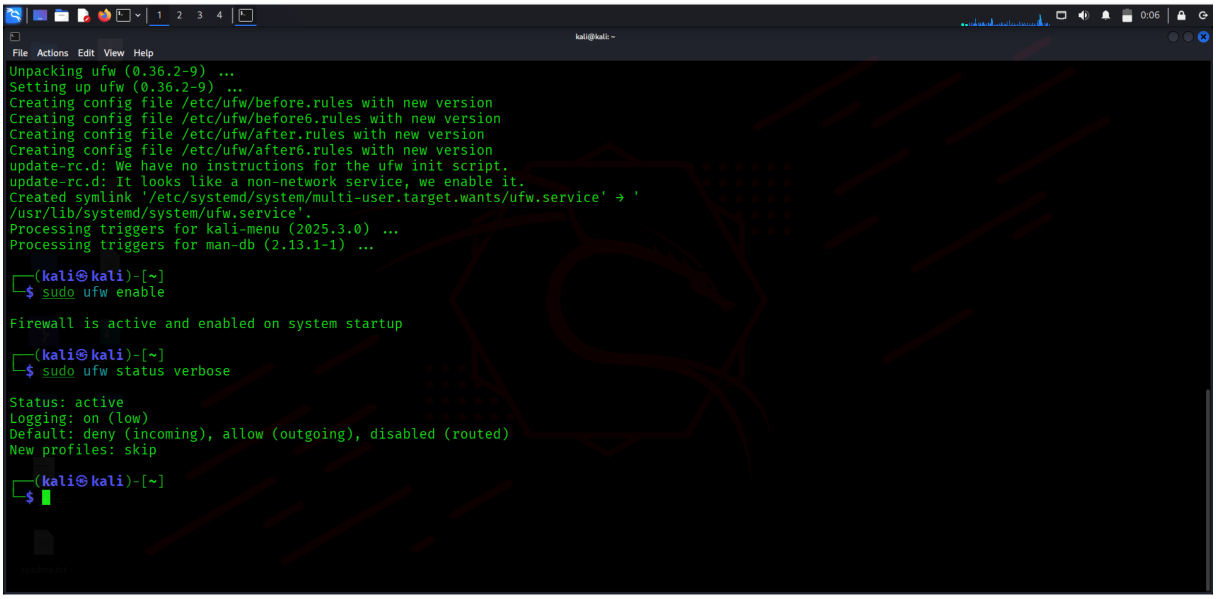
Steps & Screenshots

1. Enable UFW:

sudo apt install ufw -y

sudo ufw enable

sudo ufw status verbose



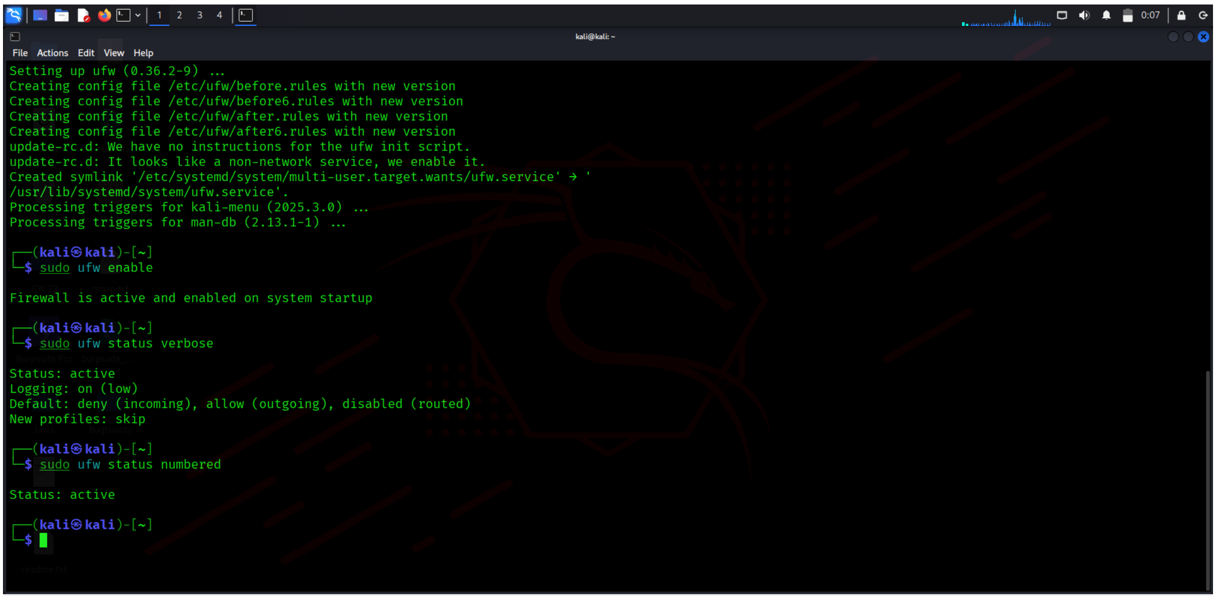
```
Unpacking ufw (0.36.2-9) ...
Setting up ufw (0.36.2-9) ...
Creating config file /etc/ufw/before.rules with new version
Creating config file /etc/ufw/before6.rules with new version
Creating config file /etc/ufw/after.rules with new version
Creating config file /etc/ufw/after6.rules with new version
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)



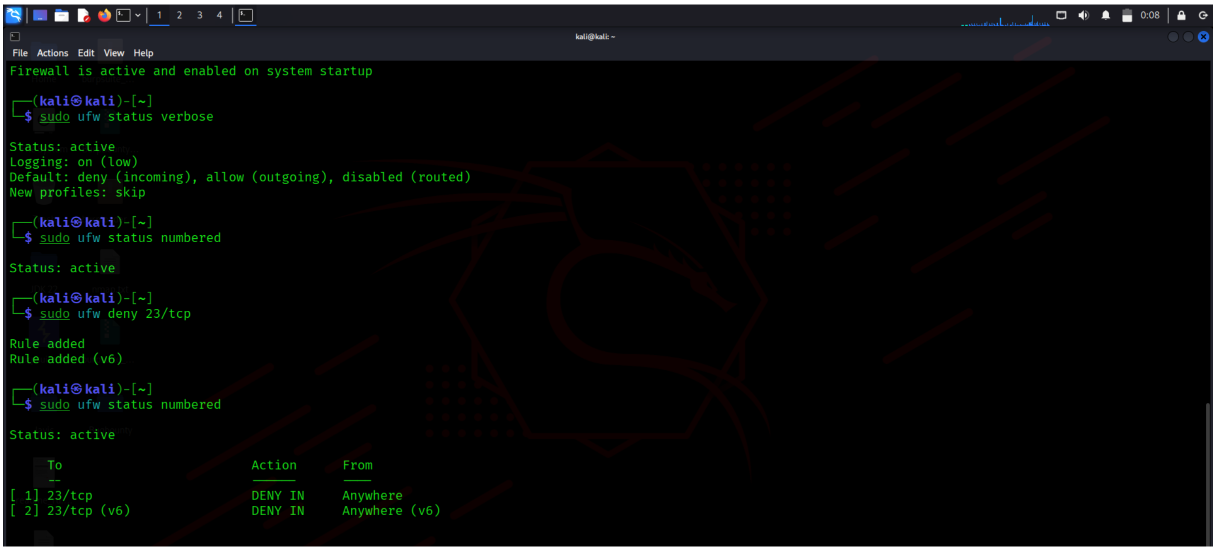
```
Setting up ufw (0.36.2-9) ...
Creating config file /etc/ufw/before.rules with new version
Creating config file /etc/ufw/before6.rules with new version
Creating config file /etc/ufw/after.rules with new version
Creating config file /etc/ufw/after6.rules with new version
update-rc.d: We have no instructions 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



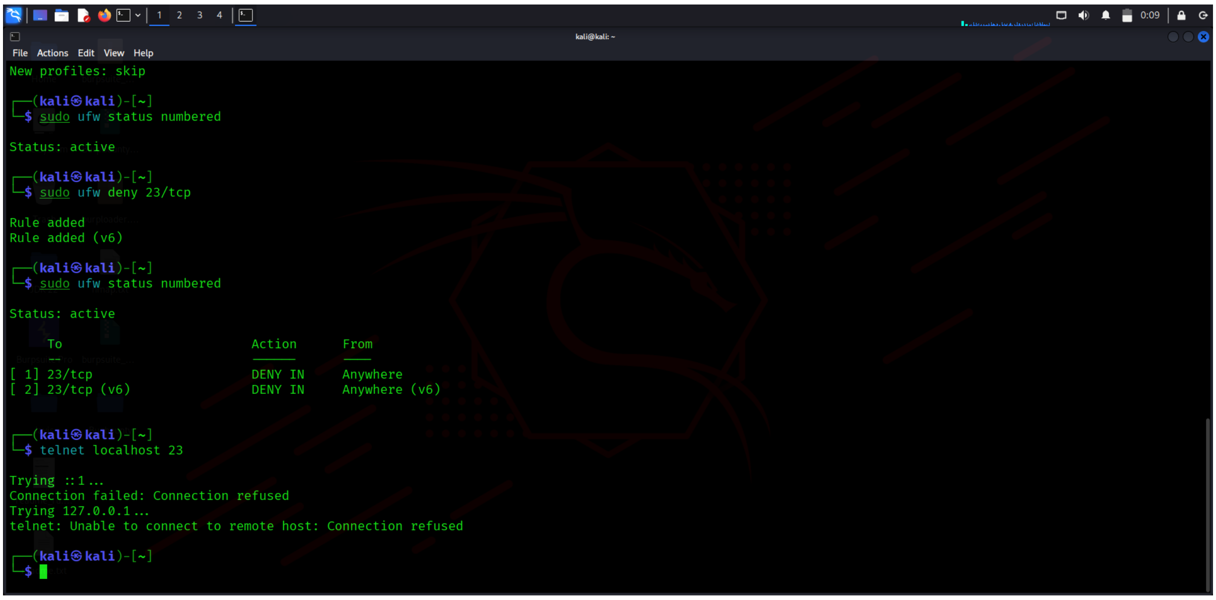
```
Firewall is active and enabled on system startup

┌──(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)
```

Screenshot 3: Rules showing DENY 23/tcp.

4. Test the Rule:

telnet localhost 23

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



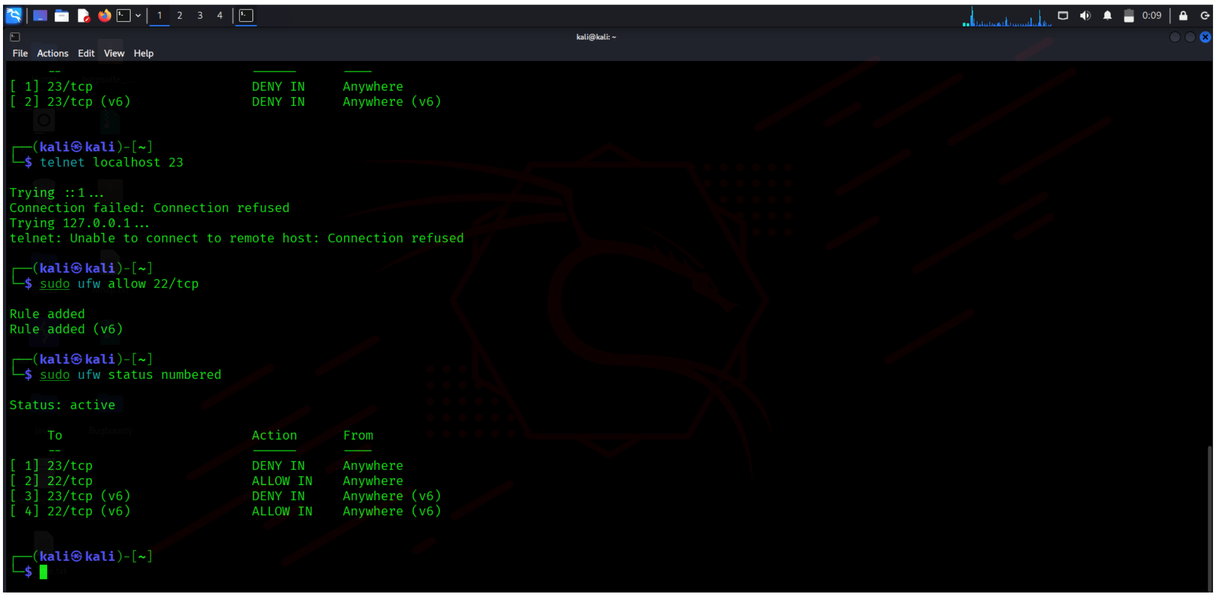
```
New profiles: skip

┌──(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)-[~]
└─$ 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



```
     --                         ------      ----
[ 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)-[~]
└─$ 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] 22/tcp                     ALLOW IN    Anywhere
[ 3] 23/tcp (v6)                DENY IN     Anywhere (v6)
[ 4] 22/tcp (v6)                ALLOW IN    Anywhere (v6)


┌──(kali㉿kali)-[~]
└─$ 
```

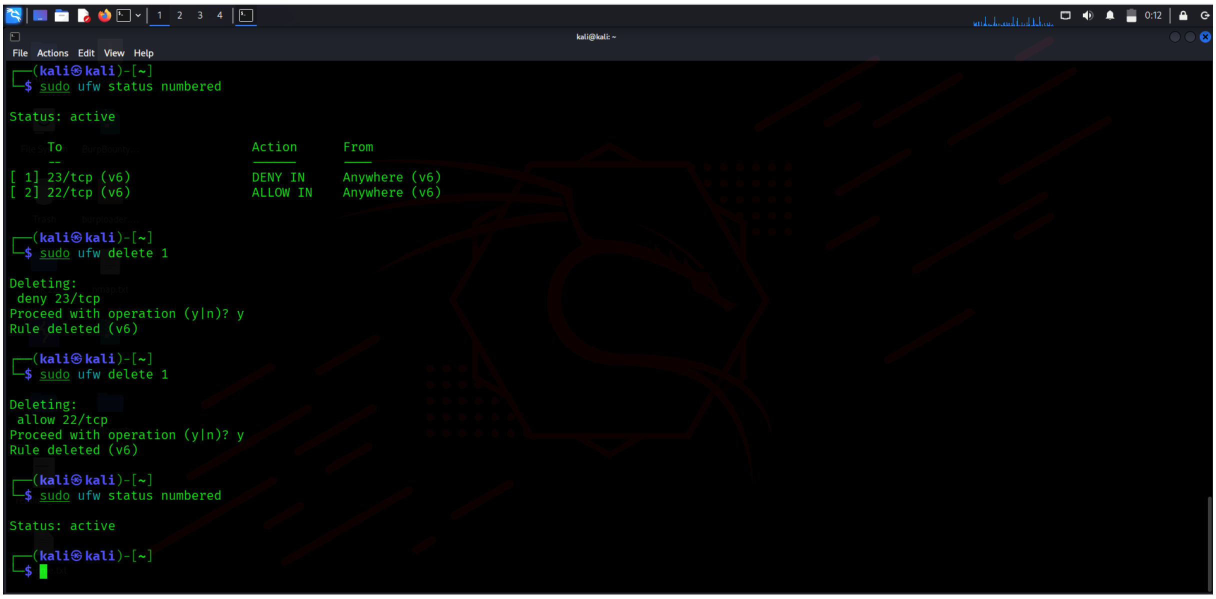
Screenshot 5: Rules showing ALLOW 22/tcp.

6. Remove the Block Rule:

sudo ufw delete <rule_number>

sudo ufw status numbered

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



```
┌──(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.