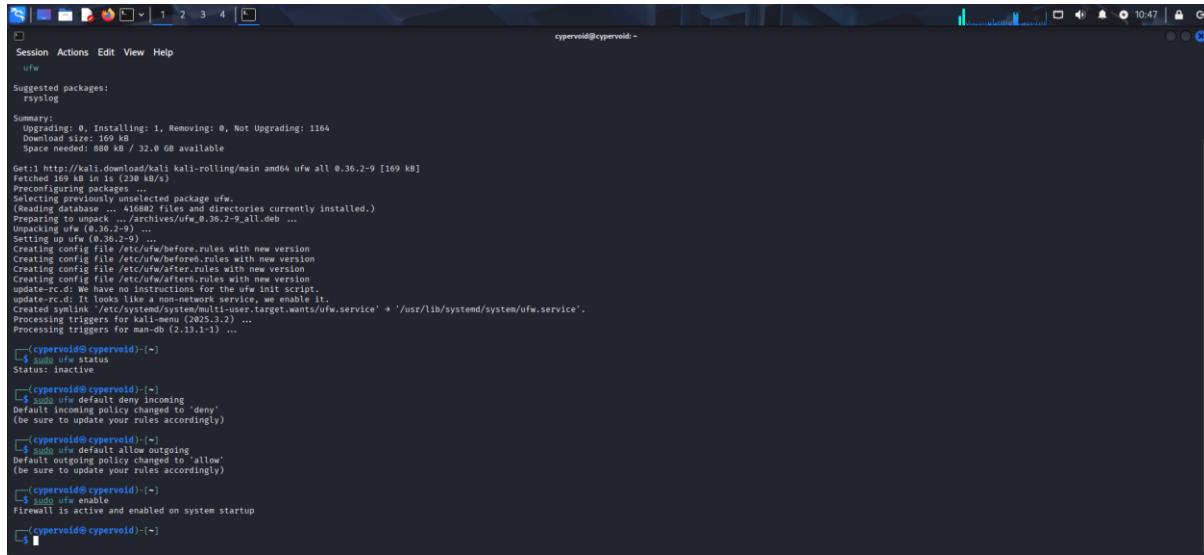


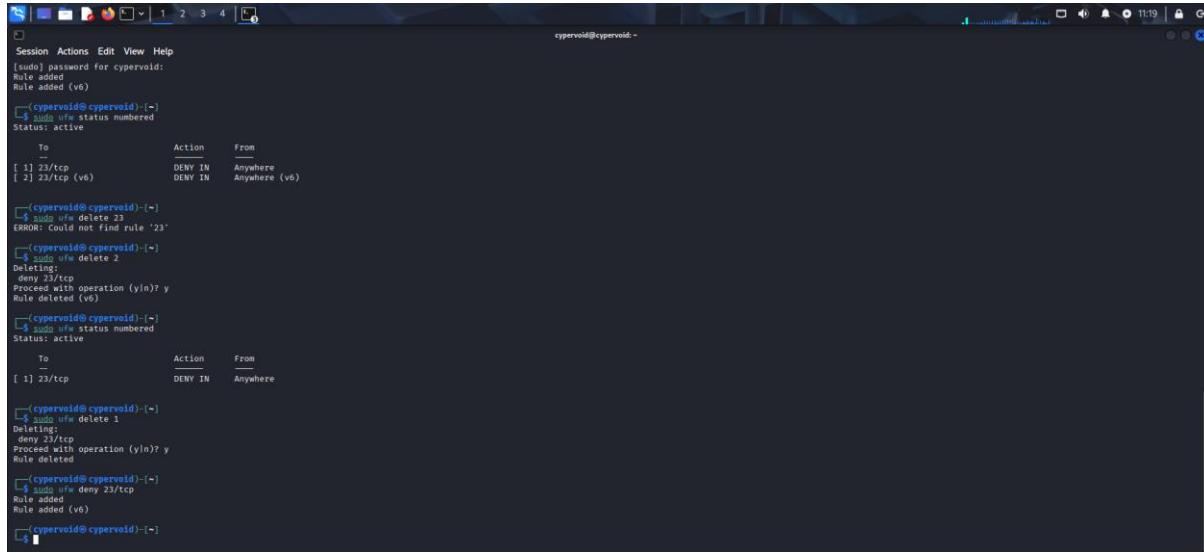
This exercise demonstrates how to use UFW (Uncomplicated Firewall) on Kali Linux to manage and filter network traffic. It shows blocking and allowing specific ports using UFW and testing connectivity with ncat, highlighting the 'Silent Drop' behavior when a port is denied.

Analyst: Manju Varma M



```
Session Actions Edit View Help
ufw
Suggested packages:
rsyslog
Summary:
Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 1164
Download size: 169 kB
Space needed: 888 kB / 32.0 GB available
Get:1 http://kali.download/kali kali-rolling/main amd64 ufw all 0.36.2-9 [169 kB]
Fetched 169 kB in 0s (230 kB/s)
Preconfiguring packages...
Selecting previously unselected package ufw.
(Reading database ... 416882 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/after.rules' with new version
Creating config file '/etc/ufw/afters.rules' with new version
Creating config file '/etc/ufw/allowed' with new version
update-rc.d: warning: default start/stop in /etc/init.d/ufw ignored.
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 (2.025.3-2) ...
Processing triggers for man-db (2.17.3-1) ...
(cybervoid@cybervoid) ~
$ ufw status
Status: active
(cybervoid@cybervoid) ~
$ sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
(cybervoid@cybervoid) ~
$ sudo ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)
(cybervoid@cybervoid) ~
$ sudo ufw enable
Firewall is active and enabled on system startup
(cybervoid@cybervoid) ~
```

Fig 1. Enabling the Firewall



```
Session Actions Edit View Help
[sudo] password for cybervoid:
Rule added
Rule added (v6)
(cybervoid@cybervoid) ~
$ ufw status numbered
Status: active
To          Action      From
[ 1] 23/tcp    DENY IN    Anywhere
[ 2] 23/tcp (v6) DENY IN    Anywhere (v6)

(cybervoid@cybervoid) ~
$ sudo ufw delete 23
ERROR: Could not find rule '23'
(cybervoid@cybervoid) ~
$ sudo ufw delete 2
Deleting:
deny 23/tcp
Proceed with operation (y/n)? y
Rule deleted (v6)

(cybervoid@cybervoid) ~
$ ufw status numbered
Status: active
To          Action      From
[ 1] 23/tcp    DENY IN    Anywhere

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

(cybervoid@cybervoid) ~
$ sudo ufw deny 23/tcp
Rule added
Rule added (v6)

(cybervoid@cybervoid) ~
```

Fig 2. Blocking 23/TCP and Allowing 22/TCP

The screenshot shows two terminal windows side-by-side. Both windows are titled 'cypervoid@cypervoid:~'.

Left Terminal:

```
(cypervoid@cypervoid) ~]$ nc -l -p 23
(UNKNOWN) [127.0.0.1] 23 (telnet) : Connection refused
```

Right Terminal:

```
(cypervoid@cypervoid) ~]$ nc 127.0.0.1 23
ncat: Connection refused.
```

Fig 3. No Communication After Blocked

The screenshot shows two terminal windows side-by-side. Both windows are titled 'cypervoid@cypervoid:~'.

Left Terminal:

```
(cypervoid@cypervoid) ~]$ nc -l -p 23
(cypervoid@cypervoid) ~]$ nc 127.0.0.1 23
hi
how are u doing
``
```

Right Terminal:

```
(cypervoid@cypervoid) ~]$ nc -l -p 23
(cypervoid@cypervoid) ~]$ nc 127.0.0.1 23
hi
how are u doing
``
```

Fig 4. Communication After Restoring The Firewall

Doing This Was Pretty Fun and It was Easy to Understand how firewall Works as well...