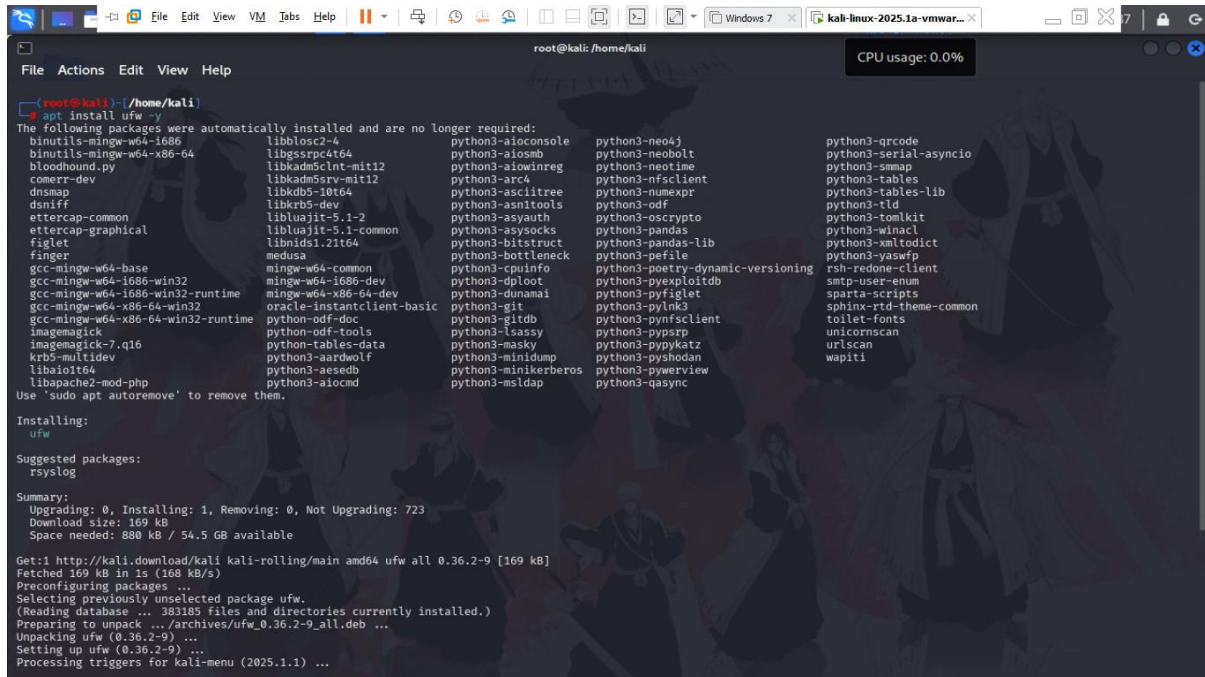


In this demonstration, we'll be setting up firewall rules in Kali Linux, set rules and test them,

1. Setting Up UFW(Uncomplicated Firewall)

Command: apt install ufw -y



```
root@kali: /home/kali
File Actions Edit View Help
CPU usage: 0.0%

(root@kali) ~/home/kali
$ apt install ufw -y
The following packages were automatically installed and are no longer required:
binutils-mingw-w64-i686 libblosc2-4 python3-aioconsole python3-neo4j python3-qrcode
binutils-mingw-w64-x86_64 libblosc2-4 python3-aioconsole python3-neobolt python3-serial-asyncio
bloodhound.py libblosc2-4 python3-aioconsole python3-neotime python3-smmmap
comerr-dev libblosc2-4 python3-aioconsole python3-nfsclient python3-tables
dnsmasq libblosc2-4 python3-aioconsole python3-numexpr python3-tables-lib
dsntiff libblosc2-4 python3-aioconsole python3-odf python3-tld python3-tomlkit
ettercap-common libblosc2-4 python3-aioconsole python3-oscrypto python3-winacl
ettercap-graphical libblosc2-4 python3-aioconsole python3-pandas python3-winact
figlet libblosc2-4 python3-aioconsole python3-pandas-lib python3-xmldict
finger libblosc2-4 python3-aioconsole python3-pefile python3-yaswfp
gcc-mingw-w64-base libblosc2-4 python3-aioconsole python3-poetry-dynamic-versioning python3-yaswfp
gcc-mingw-w64-i686-win32 libblosc2-4 python3-aioconsole python3-pyexploitdb smtp-user-enum
gcc-mingw-w64-i686-win32-runtime libblosc2-4 python3-aioconsole python3-pyfiglet sparta-scripts
gcc-mingw-w64-x86_64-win32 libblosc2-4 python3-aioconsole python3-pylnk3 sphinx-rtd-theme-common
gcc-mingw-w64-x86_64-win32-runtime libblosc2-4 python3-aioconsole python3-pynfsclient toilet-fonts
imagemagick libblosc2-4 python3-aioconsole python3-pysrp unicornsans
imagemagick-7.q16 libblosc2-4 python3-aioconsole python3-pysocks urlscan
krb5-multidev libblosc2-4 python3-aioconsole python3-pyssh python3-wapiti
libaio1t64 libblosc2-4 python3-aioconsole python3-pyssh python3-wapiti
libapache2-mod-php libblosc2-4 python3-aioconsole python3-pyssh python3-wapiti
libapache2-mod-php libblosc2-4 python3-aioconsole python3-pyssh python3-wapiti
Use 'sudo apt autoremove' to remove them.

Installing:
ufw

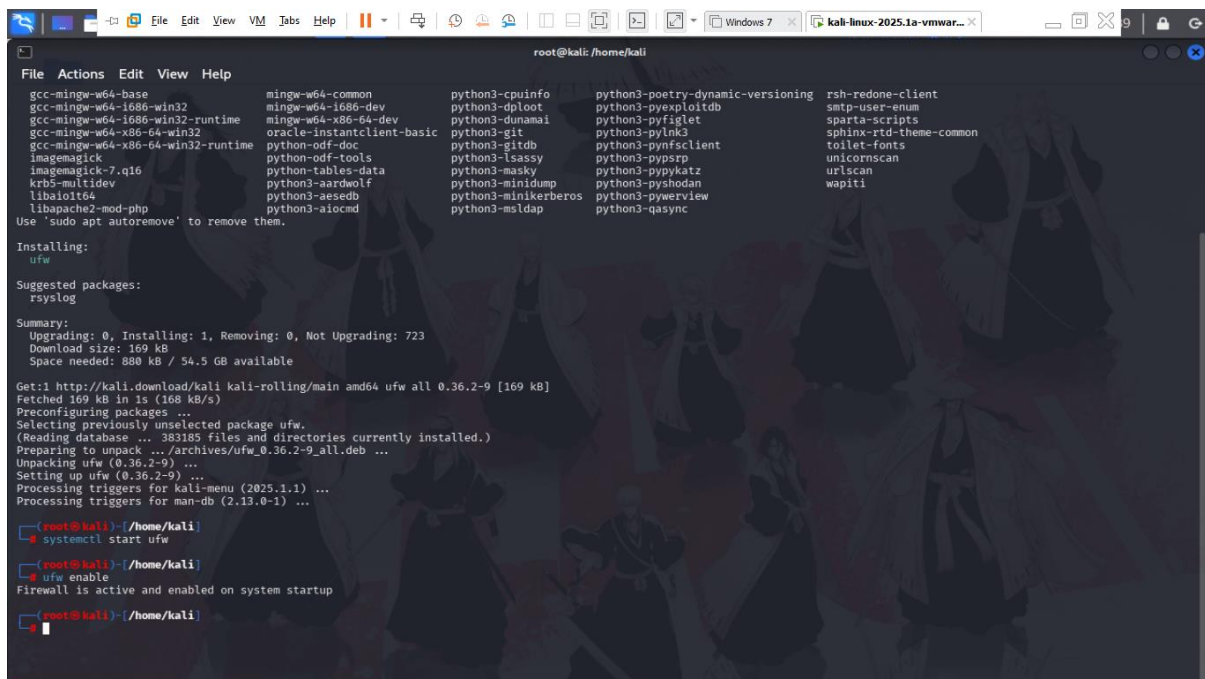
Suggested packages:
rsyslog

Summary:
Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 723
Download size: 169 kB
Space needed: 880 kB / 54.5 GB available

Get:1 http://kali.download/kali kali-rolling/main amd64 ufw all 0.36.2-9 [169 kB]
Fetched 169 kB in 1s (168 kB/s)
Preconfiguring packages ...
Selecting previously unselected package ufw.
(Reading database ... 383185 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) ...
Processing triggers for kali-menu (2025.1.1) ...
```

1.1 starting the service

Command : systemctl start ufw & ufw enable



```
root@kali: /home/kali
File Actions Edit View Help

gcc-mingw-w64-base minGW-w64-common python3-cpuinfo python3-poetry-dynamic-versioning rsh-redone-client
gcc-mingw-w64-i686-win32 minGW-w64-i686-dev python3-dploit python3-pyexploitdb smtp-user-enum
gcc-mingw-w64-i686-win32-runtime minGW-w64-x86_64-dev python3-dunamai python3-pyfiglet sparta-scripts
gcc-mingw-w64-x86_64-win32 oracle-instantclient-basic python3-git python3-pylnk3 sphinx-rtd-theme-common
gcc-mingw-w64-x86_64-win32-runtime python-odf-doc python3-gitdb python3-pynfsclient toilet-fonts
imagemagick python-odf-tools python3-lsassy python3-pysrp unicornsans
imagemagick-7.q16 python-tables-data python3-masky python3-pysocks urlscan
krb5-multidev python3-aardwolf python3-minidump python3-pyssh python3-wapiti
libaio1t64 python3-aesdb python3-minikerberos python3-pyssh python3-wapiti
libapache2-mod-php python3-aioconsole python3-msldap python3-qasync

Use 'sudo apt autoremove' to remove them.

Installing:
ufw

Suggested packages:
rsyslog

Summary:
Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 723
Download size: 169 kB
Space needed: 880 kB / 54.5 GB available

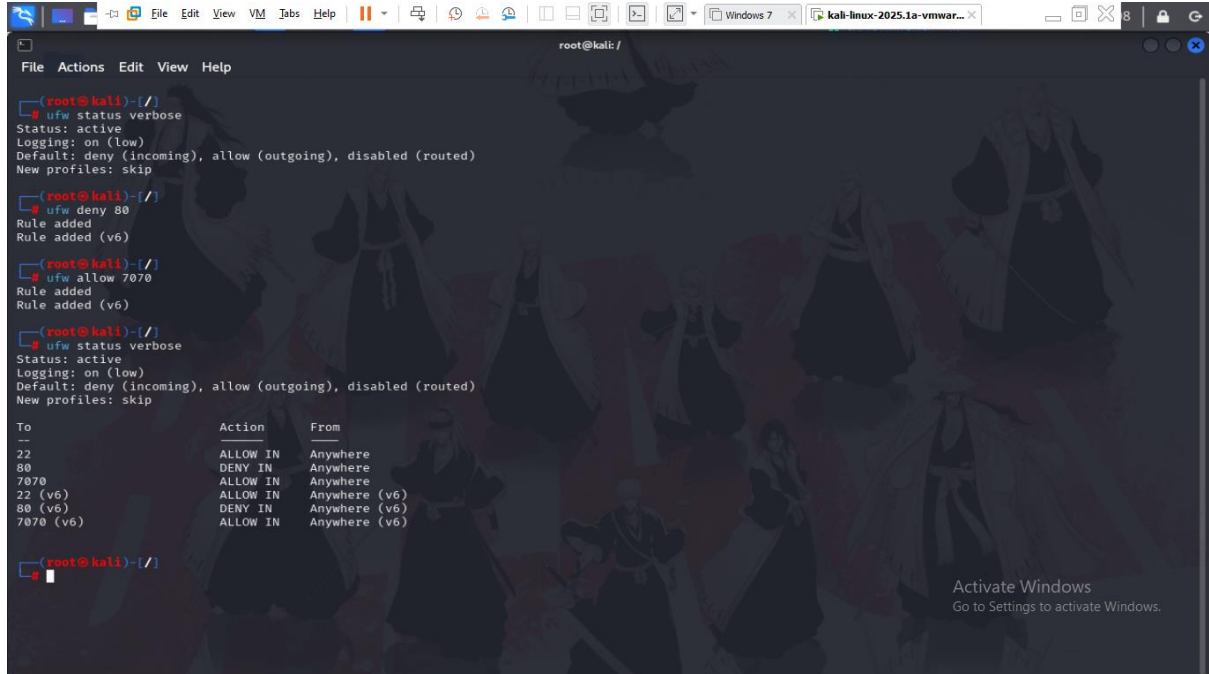
Get:1 http://kali.download/kali kali-rolling/main amd64 ufw all 0.36.2-9 [169 kB]
Fetched 169 kB in 1s (168 kB/s)
Preconfiguring packages ...
Selecting previously unselected package ufw.
(Reading database ... 383185 files and directories currently installed.)
Preparing to unpack .../archives/ufw_0.36.2-9_all.deb ...
Unpacking ufw (0.36.2-9) ...
Setting up ufw (0.36.2-9) ...
Processing triggers for kali-menu (2025.1.1) ...
Processing triggers for man-db (2.13.0-1) ...

(root@kali) ~/home/kali
$ systemctl start ufw
$ ufw enable
Firewall is active and enabled on system startup

(root@kali) ~/home/kali
```

2. Listing current firewall rules

- Here few rules have been set up just to demonstrate what rules have been implemented.



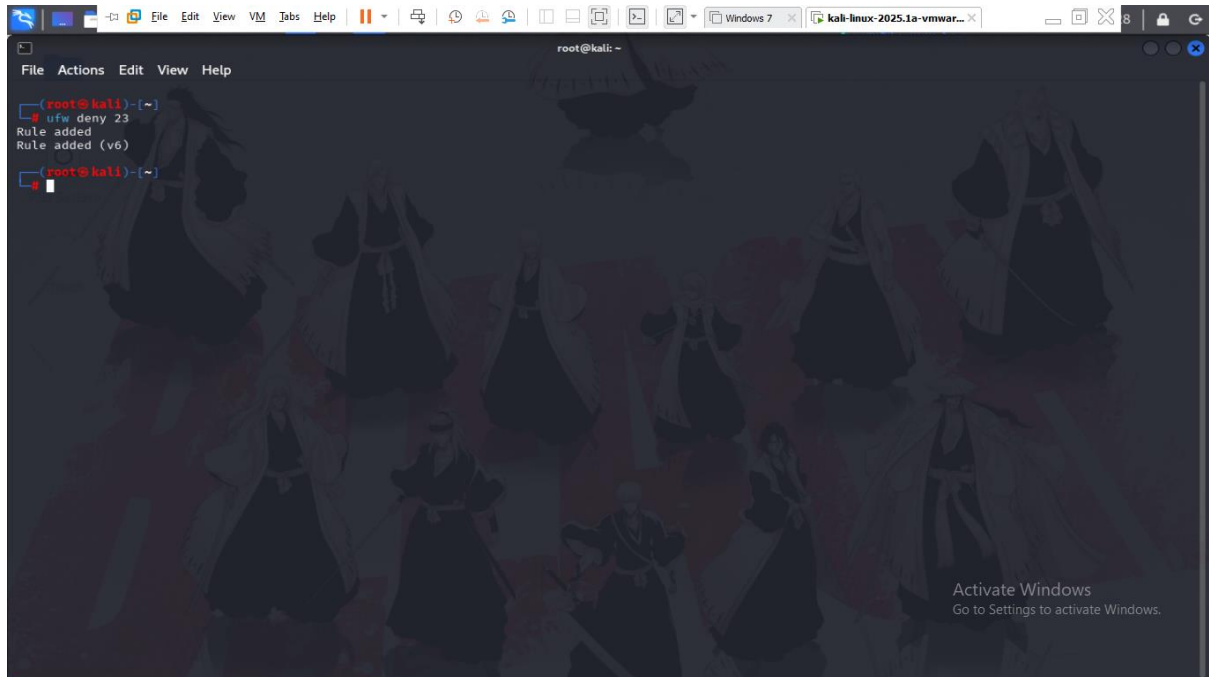
The screenshot shows a Kali Linux terminal window with the following content:

```
root@kali: /  
File Actions Edit View Help  
  
(root@kali)-[/]  
└─$ ufw status verbose  
Status: active  
Logging: on (low)  
Default: deny (incoming), allow (outgoing), disabled (routed)  
New profiles: skip  
  
(root@kali)-[/]  
└─$ ufw deny 80  
Rule added  
Rule added (v6)  
  
(root@kali)-[/]  
└─$ ufw allow 7070  
Rule added  
Rule added (v6)  
  
(root@kali)-[/]  
└─$ ufw status verbose  
Status: active  
Logging: on (low)  
Default: deny (incoming), allow (outgoing), disabled (routed)  
New profiles: skip  
  
To Action From  
--  
22 ALLOW IN Anywhere  
80 DENY IN Anywhere  
7070 ALLOW IN Anywhere  
22 (v6) ALLOW IN Anywhere (v6)  
80 (v6) DENY IN Anywhere (v6)  
7070 (v6) ALLOW IN Anywhere (v6)  
  
(root@kali)-[/]  
└─$
```

An "Activate Windows" watermark is visible in the bottom right corner of the terminal window.

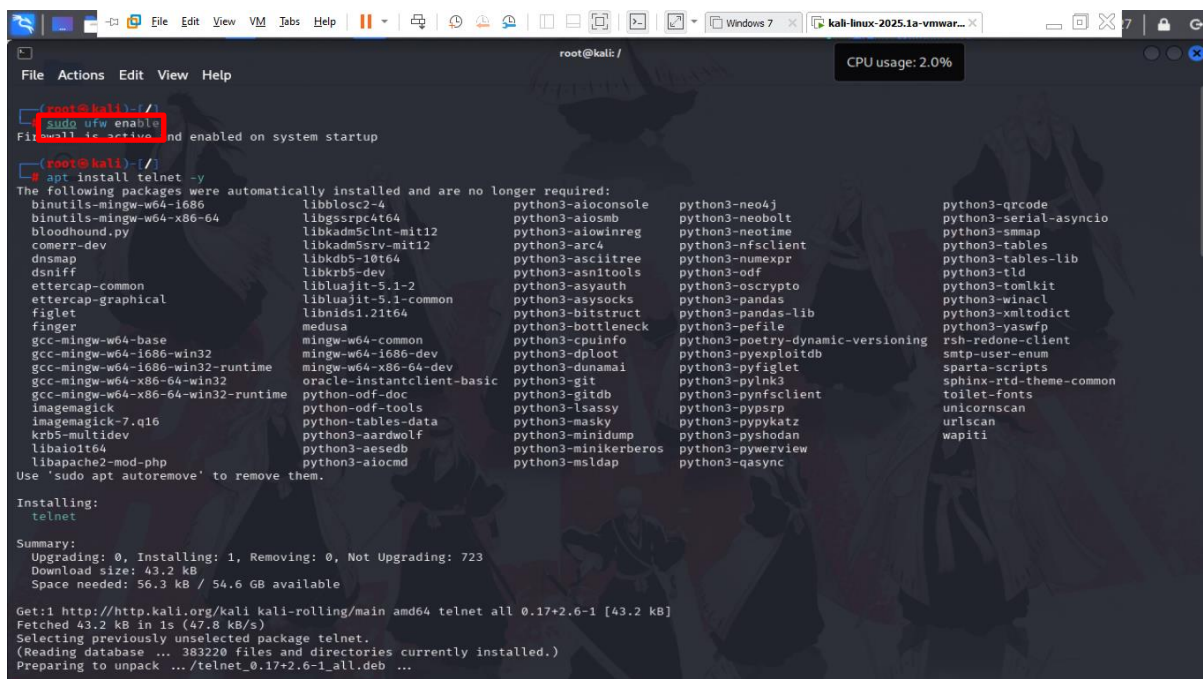
3. Blocking rule (blocking port 23)

- Command used : `ufw deny 23`



4. Testing the Deny firewall rule (Deny 23)

- Command used : -
 - Sudo ufw enable
 - Apt install telnet -y
 - Ufw deny 23
 - apt install xinetd telnetd -y
 - telnet localhost 23
 - Nano /etc/inetd.conf
 - Systemctl restart xinetd



```
root@kali: /  
File Actions Edit View Help CPU usage: 2.0%  
root@kali: /  
# sudo ufw enable  
Firewall is active and enabled on system startup  
root@kali: /  
# apt install telnet -y  
The following packages were automatically installed and are no longer required:  
binutils-mingw-w64-i686 libblosc2-4 python3-aioclient python3-neo4j python3-qrcode  
binutils-mingw-w64-x86_64 libgssrpc4t64 python3-aiohttp python3-neobolt python3-serial-asyncio  
bloodhound.py libkadm5clnt-mit12 python3-aiohttp python3-neotime python3-smmmap  
comerr-dev libkadm5srv-mit12 python3-arc4 python3-nfsclient python3-tables  
dnsmap libkdb5-10t64 python3-asciitree python3-numexpr python3-tables-lib  
dsiff libkdb5-dev python3-asn1tools python3-odf python3-tld  
ettercap-common liblua5.1-2 python3-asyauth python3-oscrypt python3-tomlkit  
ettercap-graphical liblua5.1-common python3-asysocks python3-pandas python3-winacl  
figlet libnids1.2t64 python3-bitstruct python3-pandas-lib python3-xmltodict  
finger medusa python3-bottleneck python3-pefile python3-yaswfp  
gcc-mingw-w64-base mingw-w64-common python3-cpuinfo python3-poetry-dynamic-versioning rsh-redone-client  
gcc-mingw-w64-i686-win32 mingw-w64-i686-dev python3-dploit python3-pyexploitdb smtp-user-enum  
gcc-mingw-w64-i686-win32-runtime oracle-instantclient-basic python3-dunamai python3-pyfiglet sparta-scripts  
gcc-mingw-w64-x86_64-win32 python-odf-doc python3-git python3-pylnk3 sphinx-rtd-theme-common  
gcc-mingw-w64-x86_64-win32-runtime python-odf-tools python3-github python3-pynfsclient toilet-fonts  
imagemagick python-tables-data python3-lsassy python3-pyppkatz unicornscan  
krb5-multidev python3-aardwolf python3-masky python3-pyshodan urlscan  
libaio1t64 python3-aesedb python3-minidump python3-pyshodan wapiti  
libapache2-mod-php python3-aiohttp python3-msldap python3-qasync  
Use 'sudo apt autoremove' to remove them.  
Installing:  
telnet  
Summary:  
Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 723  
Download size: 43.2 kB  
Space needed: 56.3 kB / 54.6 GB available  
Get:1 http://http.kali.org/kali kali-rolling/main amd64 telnet all 0.17+2.6-1 [43.2 kB]  
Fetched 43.2 kB in 1s (47.8 kB/s)  
Selecting previously unselected package telnet.  
(Reading database ... 383220 files and directories currently installed.)  
Preparing to unpack .../telnet_0.17+2.6-1_all.deb ...
```

```
File Actions Edit View Help
root@kali: /
CPU usage: 1.0%

Fetches 43.2 kB in 1s (47.8 kB/s)
Selecting previously unselected package telnet.
(Reading database ... 383220 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) ...

ufw deny 23
Rule added (v6)

telnet localhost 23
Trying 127.0.0.1...
telnet: Unable to connect to remote host: Connection refused

(root@kali)~$ apt install xinetd telnetd -y
The following packages were automatically installed and are no longer required:
binutils-mingw-w64-i686 libblosc2-4 python3-aiocmd python3-neo4j python3-qrcode
binutils-mingw-w64-x86_64 libbssrpc4t64 python3-aiosmb python3-neobolt python3-serial-asyncio
bloodhound.py libkadm5clnt-mit12 python3-aiowinreg python3-neotime python3-smmmap
comerr-dev libkadm5srv-mit12 python3-arc4 python3-nfsclient python3-tables
dnsmap libkdb5-10t64 python3-asciitree python3-numexpr python3-tables-lib
dsniff libkrb5-dev python3-asn1tools python3-odf python3-tld
ettercap-common liblua5.1-2 python3-asysocks python3-odf python3-tomlkit
ettercap-graphical figlet libnids1.21t64 python3-bitstruct python3-oscrypto python3-tomlkit
finger medusa python3-bottleneck python3-pandas python3-winacl
gcc-mingw-w64-base mingw-w64-common python3-cpuinfo python3-pandas-lib python3-xmltodict
gcc-mingw-w64-i686-win32 mingw-w64-i686-dev python3-dploit python3-pefile python3-xaswfp
gcc-mingw-w64-i686-win32-runtime mingw-w64-x86_64-dev python3-dunamai python3-pyfiglet python3-xaswfp
gcc-mingw-w64-x86_64-win32 oracle-instantclient-basic python3-git python3-pyfiglet python3-smtp-user-enum
gcc-mingw-w64-x86_64-win32-runtime python-odf-doc python3-github python3-pynfsclient python3-sphinx-rtd-theme-common
imagemagick python-odf-tools python3-lsassy python3-pyppkatz python3-toilet-fonts
imagemagick-7.q16 python-tables-data python3-masky python3-pyssh python3-unicornscan
krb5-multidev python3-aardwolf python3-minidump python3-pyshodan python3-uriscan
libaio1t64 python3-aesedb python3-minikerberos python3-pyssh python3-wapiti
libapache2-mod-php python3-aiohttp python3-msldap python3-qasync python3-wapiti

Use 'sudo apt autoremove' to remove them.
```

```
File Actions Edit View Help
root@kali: /

telnet localhost 23
Trying ::1...
Connection failed: Connection refused
Trying 127.0.0.1...
telnet: Unable to connect to remote host: Connection refused

(root@kali)~$ apt install xinetd telnetd -y
The following packages were automatically installed and are no longer required:
binutils-mingw-w64-i686 libblosc2-4 python3-aiocmd python3-neo4j python3-qrcode
binutils-mingw-w64-x86_64 libbssrpc4t64 python3-aiosmb python3-neobolt python3-serial-asyncio
bloodhound.py libkadm5clnt-mit12 python3-aiowinreg python3-neotime python3-smmmap
comerr-dev libkadm5srv-mit12 python3-arc4 python3-nfsclient python3-tables
dnsmap libkdb5-10t64 python3-asciitree python3-numexpr python3-tables-lib
dsniff libkrb5-dev python3-asn1tools python3-odf python3-tld
ettercap-common liblua5.1-2 python3-asysocks python3-odf python3-tomlkit
ettercap-graphical figlet libnids1.21t64 python3-bitstruct python3-oscrypto python3-tomlkit
finger medusa python3-bottleneck python3-pandas python3-winacl
gcc-mingw-w64-base mingw-w64-common python3-cpuinfo python3-pandas-lib python3-xmltodict
gcc-mingw-w64-i686-win32 mingw-w64-i686-dev python3-dploit python3-pefile python3-xaswfp
gcc-mingw-w64-i686-win32-runtime mingw-w64-x86_64-dev python3-dunamai python3-pyfiglet python3-smtp-user-enum
gcc-mingw-w64-x86_64-win32 oracle-instantclient-basic python3-git python3-pyfiglet python3-sphinx-rtd-theme-common
gcc-mingw-w64-x86_64-win32-runtime python-odf-doc python3-github python3-pynfsclient python3-toilet-fonts
imagemagick python-odf-tools python3-lsassy python3-masky python3-pyssh python3-unicornscan
imagemagick-7.q16 python-tables-data python3-minidump python3-pyshodan python3-uriscan
krb5-multidev python3-aardwolf python3-minikerberos python3-pyssh python3-wapiti
libaio1t64 python3-aesedb python3-msldap python3-qasync python3-wapiti
libapache2-mod-php python3-aiohttp python3-msldap python3-qasync python3-wapiti

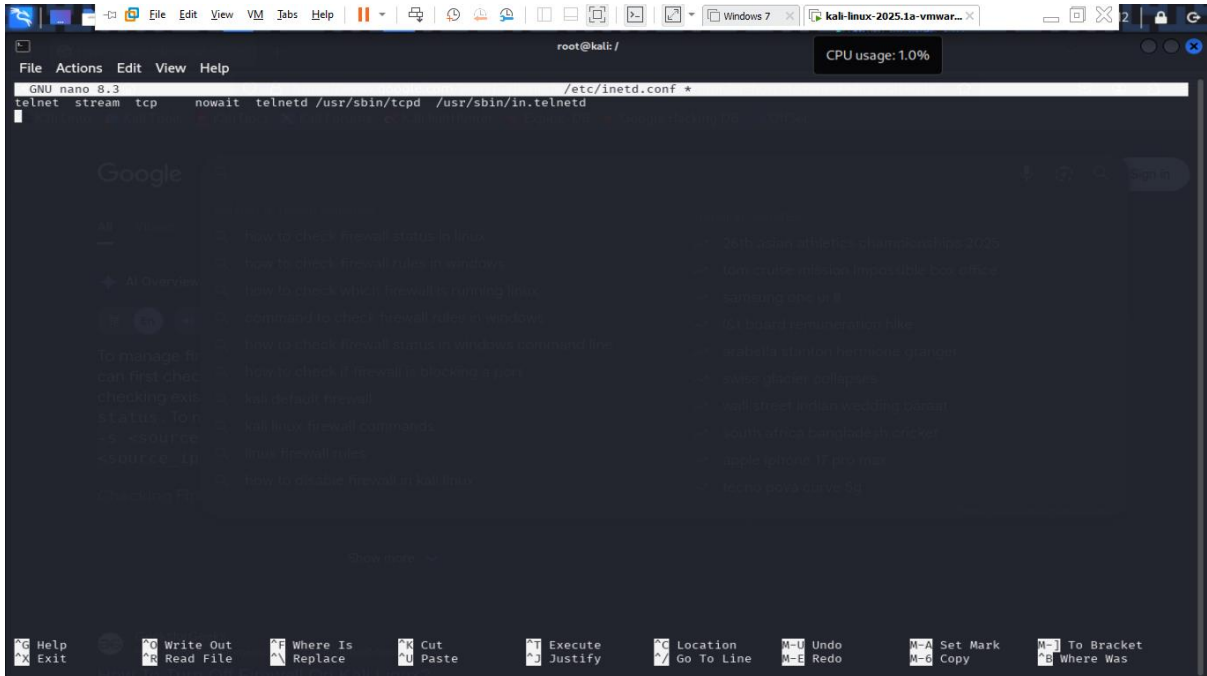
Use 'sudo apt autoremove' to remove them.

Installing:
telnetd xinetd

Installing dependencies:
inetutils-telnetd

Summary:
Upgrading: 0, Installing: 3, Removing: 0, Not Upgrading: 723
Download size: 273 kB
Space needed: 604 kB / 54.6 GB available
```

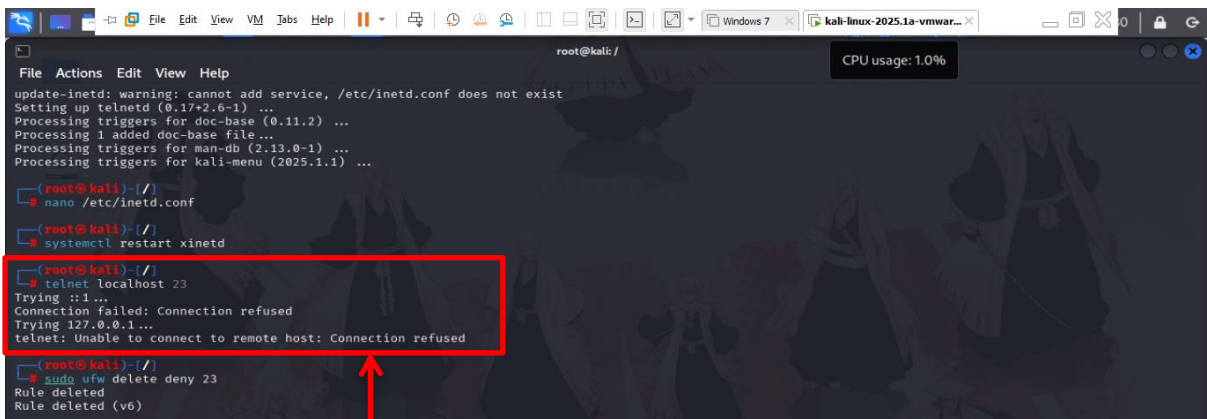

- This is the configuration file of telnetd (here the text file has been edited to incorporate proper application of services). This command is an instruction that listens for incoming connections and launches appropriate services.



The screenshot shows a terminal window with the nano text editor open at the file `/etc/inetd.conf`. The file content is as follows:

```
telnet stream tcp nowait telnetd /usr/sbin/tcpd /usr/sbin/in.telnetd
```

The terminal window title is `root@kali: /` and the status bar shows `CPU usage: 1.0%`. The nano editor interface includes a menu bar (File, Actions, Edit, View, Help) and a bottom status bar with various shortcuts.



The screenshot shows a terminal window with the following commands and output:

```
update-inetd: warning: cannot add service, /etc/inetd.conf does not exist
Setting up telnetd (0.17+2.6-1) ...
Processing triggers for doc-base (0.11.2) ...
Processing 1 added doc-base file ...
Processing triggers for man-db (2.13.0-1) ...
Processing triggers for kali-menu (2025.1.1) ...

(root@kali)-[/]
└─$ nano /etc/inetd.conf
(root@kali)-[/]
└─$ systemctl restart xinetd
(root@kali)-[/]
└─$ telnet localhost 23
Trying ::1...
Connection failed: Connection refused
Trying 127.0.0.1...
telnet: Unable to connect to remote host: Connection refused
(root@kali)-[/]
└─$ sudo ufw delete deny 23
Rule deleted
Rule deleted (v6)
```

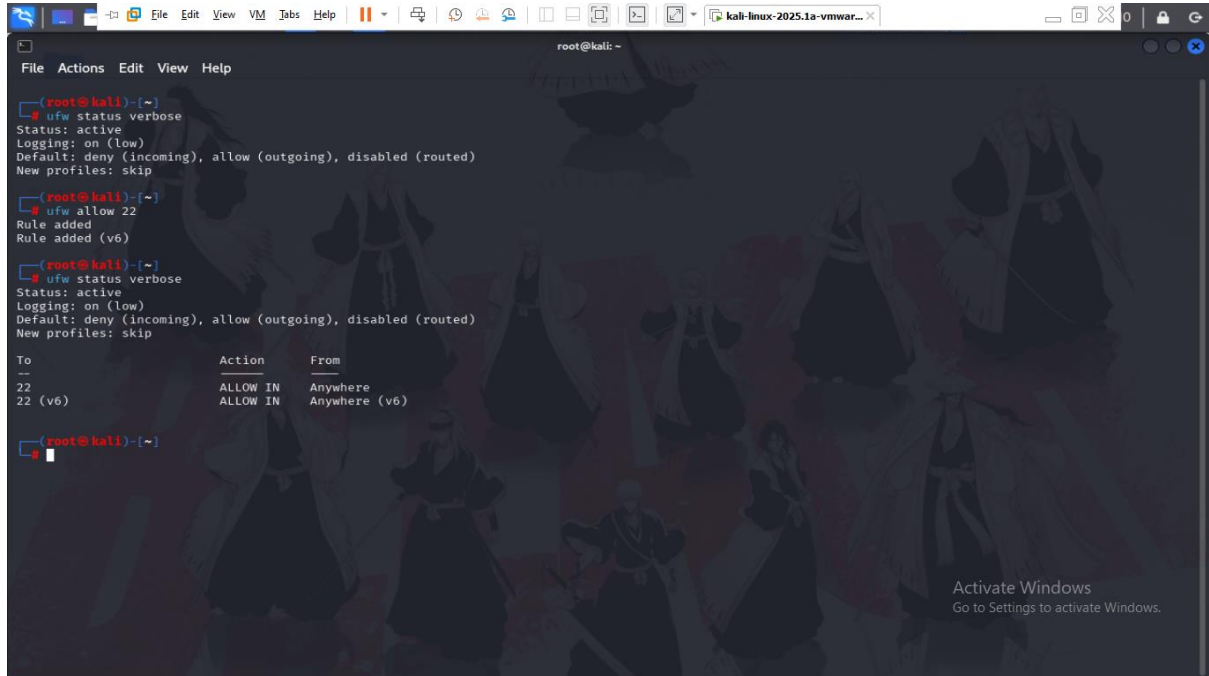
A red box highlights the output of the `telnet localhost 23` command, and a red arrow points from this box to a text box on the right.

Here, “connection refused” indicates that the connection has not been established and connection to port has been denied

5. Adding rule to allow SSH (Port 22)

Command used : `ufw status verbose`

`Ufw allow 22`



The screenshot shows a terminal window titled 'root@kali: ~' with a menu bar (File, Actions, Edit, View, Help). The terminal output is as follows:

```
(root@kali)~# ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

(root@kali)~# ufw allow 22
Rule added
Rule added (v6)

(root@kali)~# ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip
```

To	Action	From
22	ALLOW IN	Anywhere
22 (v6)	ALLOW IN	Anywhere (v6)

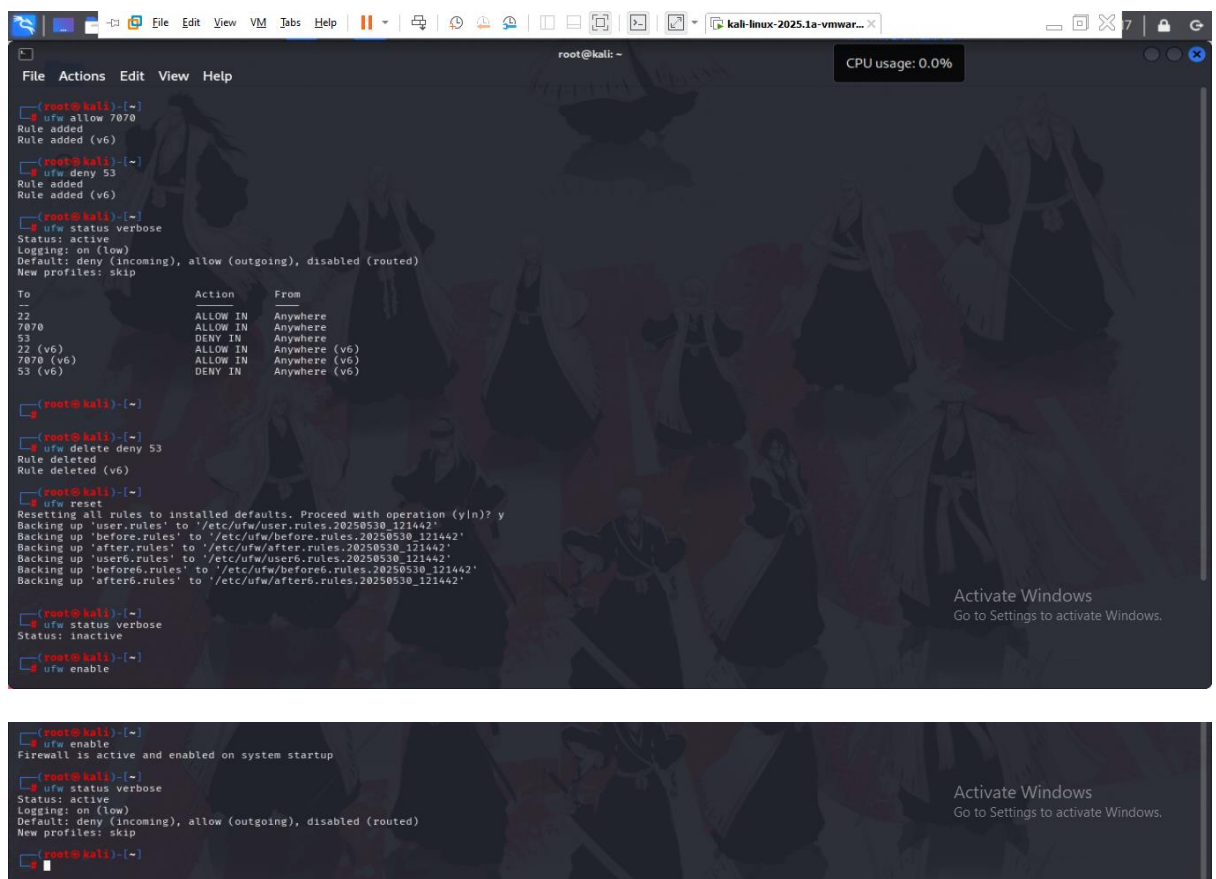
At the bottom of the terminal, there is an 'Activate Windows' watermark and a message: 'Go to Settings to activate Windows.'

6. Removing the test block rule at restoring to original state

- First a rule is established in order to restore it to its original state, for reference, we set up 2 rules here “Allow 7070” & “Deny 53”

Command used :

- Ufw status verbose
- Ufw allow 7070
- Ufw deny 53
- Ufw delete deny 53
- Ufw reset
- Ufw enable



```
(root@kali)~# ufw allow 7070
Rule added
Rule added (v6)

(root@kali)~# ufw deny 53
Rule added
Rule added (v6)

(root@kali)~# ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To Action From
--
22 ALLOW IN Anywhere
7070 ALLOW IN Anywhere
53 DENY IN Anywhere
22 (v6) ALLOW IN Anywhere (v6)
7070 (v6) ALLOW IN Anywhere (v6)
53 (v6) DENY IN Anywhere (v6)

(root@kali)~# ufw delete deny 53
Rule deleted
Rule deleted (v6)

(root@kali)~# ufw reset
Resetting all rules to installed defaults. Proceed with operation (y/n)? y
Backing up 'user.rules' to '/etc/ufw/user.rules.20250530_121442'
Backing up 'before.rules' to '/etc/ufw/before.rules.20250530_121442'
Backing up 'after.rules' to '/etc/ufw/after.rules.20250530_121442'
Backing up 'user6.rules' to '/etc/ufw/user6.rules.20250530_121442'
Backing up 'before6.rules' to '/etc/ufw/before6.rules.20250530_121442'
Backing up 'after6.rules' to '/etc/ufw/after6.rules.20250530_121442'

(root@kali)~# ufw status verbose
Status: inactive

(root@kali)~# ufw enable
Firewall is active and enabled on system startup

(root@kali)~# ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

(root@kali)~#
```

- Here “ufw reset” and then “ufw enable” is used to bring ufw to it’s original state of no rules applied

7. Documenting commands used

- apt install ufw -y
- systemctl start ufw & ufw enable
- ufw deny 23
- Sudo ufw enable
- Apt install telnet -y
- Ufw deny 23
- apt install xinetd telnetd -y
- telnet localhost 23
- Nano /etc/inetd.conf
- Systemctl restart xinetd
- ufw status verbose
- Ufw allow 22
- Ufw status verbose
- Ufw allow 7070
- Ufw deny 53
- Ufw delete deny 53
- Ufw reset
- Ufw enable

8. Summarizing how firewall filters traffic

- Acts as a gatekeeper – Checks every incoming/outgoing network packet against defined rules.
- Enabled UFW– Turned the firewall on to start filtering traffic.
- Viewed current rules – Saw which ports were already allowed or blocked.
- Blocked port 23 (Telnet) – Added a rule to deny insecure Telnet traffic.
- Tested the block** – Used `telnet` to confirm the connection was refused.
- Allowed port 22 (SSH) – Ensured essential traffic (SSH) was not interrupted.
- Removed the block– Cleaned up the test rule after verifying it worked.
- Conclusion – Firewalls follow set rules to allow safe traffic and block risky ones, giving control over how the system connects to the network.