CYBER SECURITY INTERNSHIP

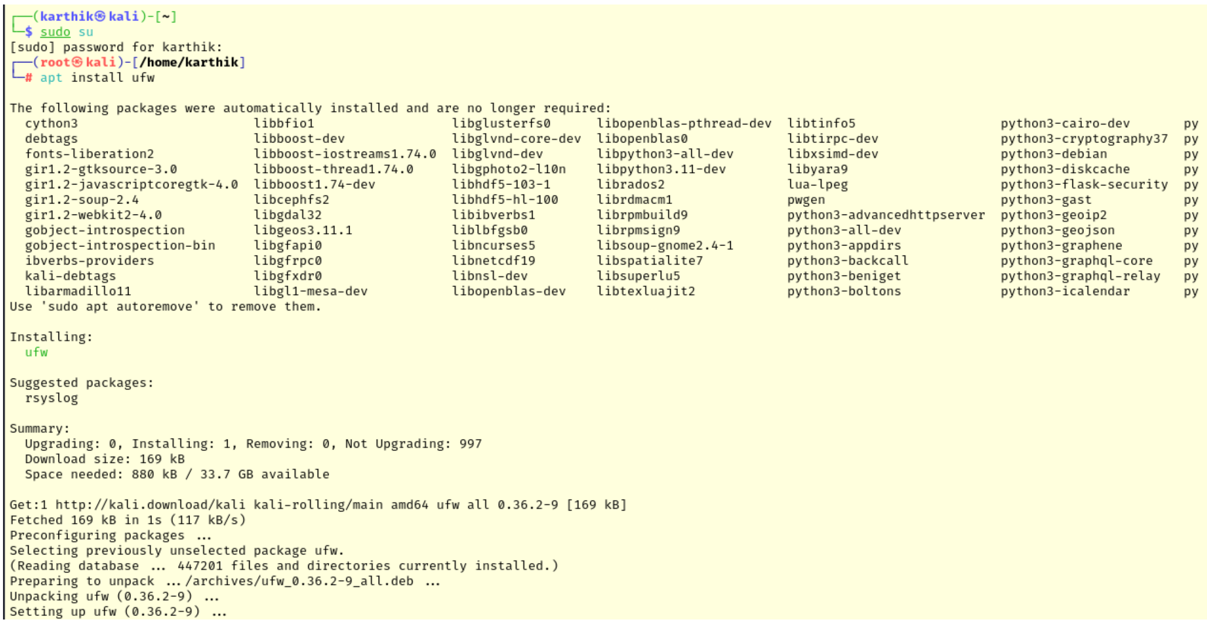
Task 3: Setup and Use a Firewall on Linux

Objective: Configure and test basic firewall rules to allow or block traffic

Tools: UFW (Uncomplicated Firewall) on Linux

Open a terminal window and enter:

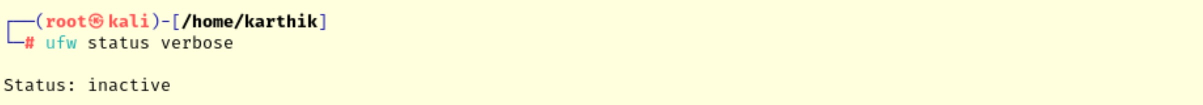
- UFW should be installed. Install it with: **sudo apt install ufw**



```
┌──(karthik㉿kali)-[~]
└─$ sudo su
[sudo] password for karthik:
┌──(root㉿kali)-[/home/karthik]
└─# apt install ufw

The following packages were automatically installed and are no longer required:
  cython3                      libbfio1                 libglusterfs0     libopenblas-pthread-dev  libtinfo5                  python3-cairo-dev       py
  debtags                      libboost-dev             libglvnd-core-dev libopenblas0             libtirpc-dev               python3-cryptography37  py
  fonts-liberation2            libboost-iostreams1.74.0 libglvnd-dev      libpython3-all-dev       libxsimd-dev               python3-debian          py
  gir1.2-gtksource-3.0         libboost-thread1.74.0    libgphoto2-l10n   libpython3.11-dev        libyara9                   python3-diskcache       py
  gir1.2-javascriptcoregtk-4.0 libboost1.74-dev         libhdf5-103-1     librados2                lua-lpeg                   python3-flask-security  py
  gir1.2-soup-2.4              libcephfs2               libhdf5-hl-100    librdmacm1               pwgen                      python3-gast            py
  gir1.2-webkit2-4.0           libgdal32                libibverbs1       librpmbuild9             python3-advancedhttpserver python3-geoip2          py
  gobject-introspection        libgeos3.11.1            liblbfgsb0        librpmsign9              python3-all-dev            python3-geojson         py
  gobject-introspection-bin    libgfapi0                libncurses5       libsoup-gnome2.4-1       python3-appdirs            python3-graphene        py
  ibverbs-providers            libgfrpc0                libnetcdf19       libspatialite7           python3-backcall           python3-graphql-core    py
  kali-debtags                 libgfxdr0                libnsl-dev        libsuperlu5              python3-beniget            python3-graphql-relay   py
  libarmadillo11               libgl1-mesa-dev          libopenblas-dev   libtexluajit2            python3-boltons            python3-icalendar       py
Use 'sudo apt autoremove' to remove them.

Installing:
  ufw

Suggested packages:
  rsyslog

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 997
  Download size: 169 kB
  Space needed: 880 kB / 33.7 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 (117 kB/s)
Preconfiguring packages ...
Selecting previously unselected package ufw.
(Reading database ... 447201 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) ...
```

1.Open the firewall configuration tool (UFW via Terminal):

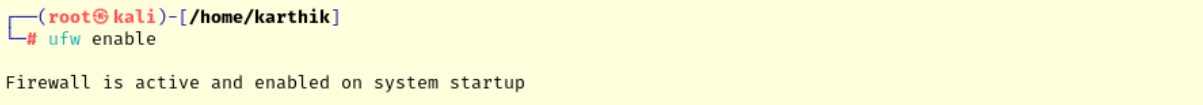
Open a root terminal: **Enter ufw status verbose**



```
┌──(root㉿kali)-[/home/karthik]
└─# ufw status verbose

Status: inactive
```

This checks if UFW is enabled and shows its current status.

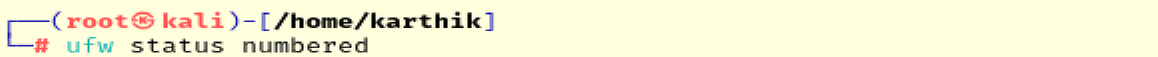
To enable UFW (if not already enabled): **use ufw enable**



```
┌──(root㉿kali)-[/home/karthik]
└─# ufw enable

Firewall is active and enabled on system startup
```

2. List current firewall rules:

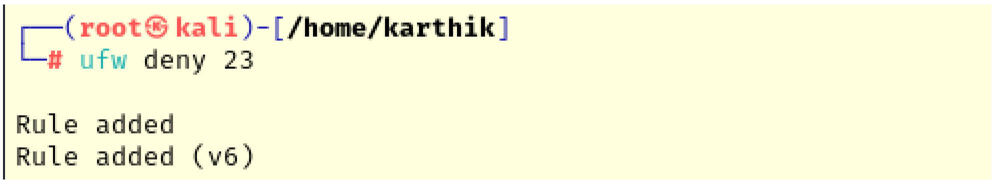
To list all current rules: **ufw status numbered**



```
┌──(root㉿kali)-[/home/karthik]
└─# ufw status numbered
```

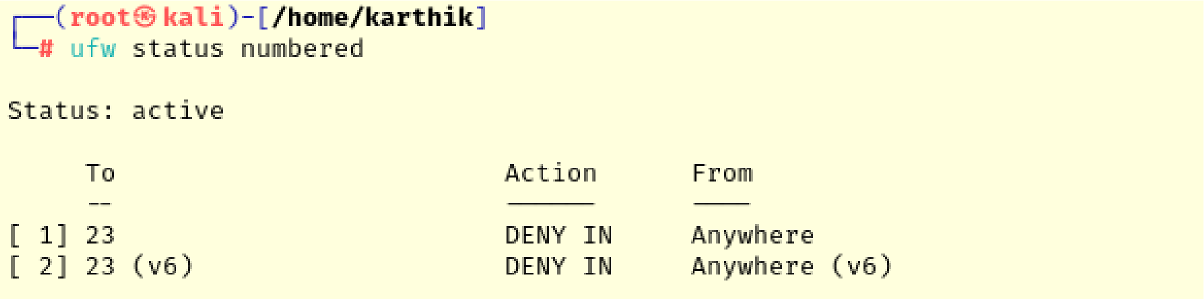
3.Add a rule to block inbound traffic on a specific port (e.g. 23 for Telnet).

To block inbound traffic on port 23, use: **ufw deny 23**



```
┌──(root㉿kali)-[/home/karthik]
└─# ufw deny 23

Rule added
Rule added (v6)
```

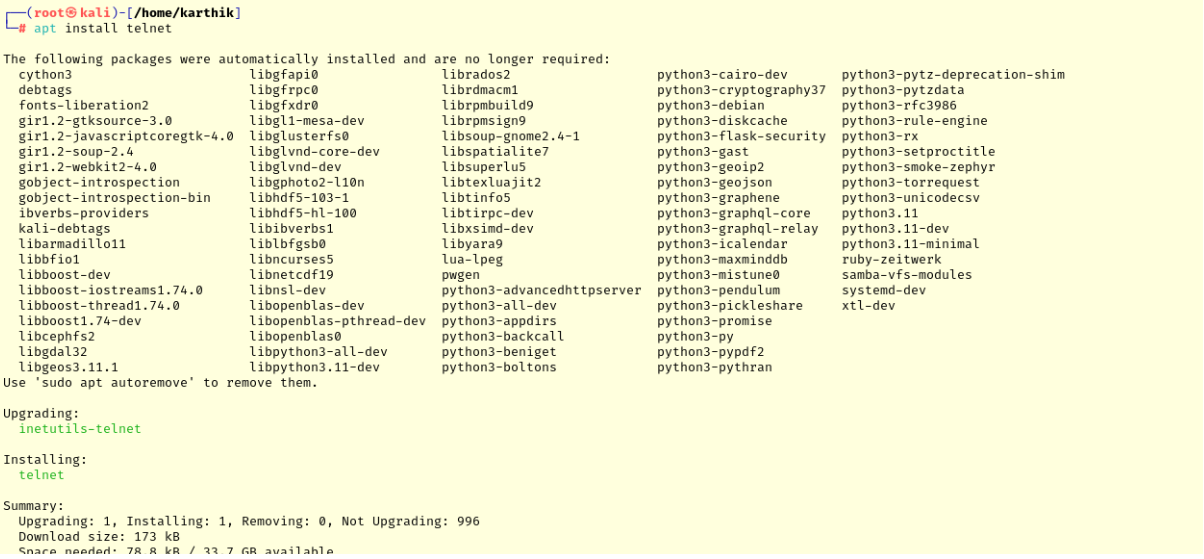
You can verify the rule was added: **ufw status number**



```
┌──(root㉿kali)-[/home/karthik]
└─# ufw status numbered

Status: active

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

4. Test the rule by attempting to connect to that port locally

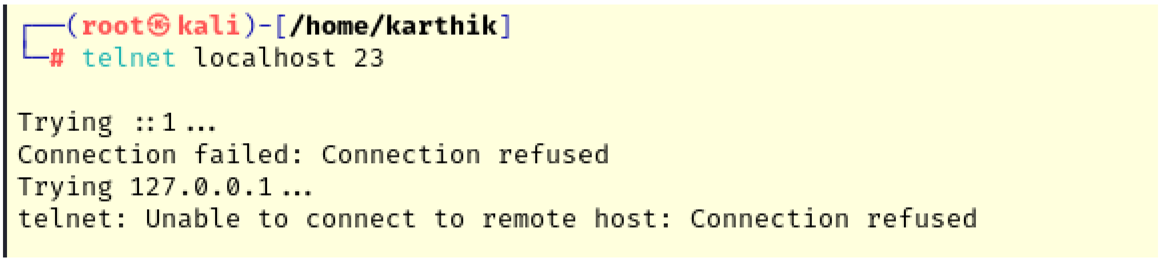
Install telnet (if not already): **apt install telnet**



```
┌──(root㉿kali)-[/home/karthik]
└─# apt install telnet

The following packages were automatically installed and are no longer required:
  cython3                       libgfapi0                librados2                   python3-cairo-dev       python3-pytz-deprecation-shim
  debtags                       libgfrpc0                librdmacm1                  python3-cryptography37  python3-pytzdata
  fonts-liberation2             libgfxdr0                librpmbuild9                python3-debian          python3-rfc3986
  gir1.2-gtksource-3.0          libgl1-mesa-dev          librpmsign9                 python3-diskcache       python3-rule-engine
  gir1.2-javascriptcoregtk-4.0  libglusterfs0            libsoup-gnome2.4-1          python3-flask-security  python3-rx
  gir1.2-soup-2.4               libglvnd-core-dev        libspatialite7              python3-gast            python3-setproctitle
  gir1.2-webkit2-4.0            libglvnd-dev             libsuperlu5                 python3-geoip2          python3-smoke-zephyr
  gobject-introspection         libgphoto2-l10n          libtexluajit2               python3-geojson         python3-torrequest
  gobject-introspection-bin     libhdf5-103-1            libtinfo5                   python3-graphene        python3-unicodecsv
  ibverbs-providers             libhdf5-hl-100           libtirpc-dev                python3-graphql-core    python3.11
  kali-debtags                  libibverbs1              libxsimd-dev                python3-graphql-relay   python3.11-dev
  libarmadillo11                liblbfgsb0               libyara9                    python3-icalendar       python3.11-minimal
  libbfio1                      libncurses5              lua-lpeg                    python3-maxminddb       ruby-zeitwerk
  libboost-dev                  libnetcdf19              pwgen                       python3-mistune0        samba-vfs-modules
  libboost-iostreams1.74.0      libnsl-dev               python3-advancedhttpserver  python3-pendulum        systemd-dev
  libboost-thread1.74.0         libopenblas-dev          python3-all-dev             python3-pickleshare     xtl-dev
  libboost1.74-dev              libopenblas-pthread-dev  python3-appdirs             python3-promise
  libcephfs2                    libopenblas0             python3-backcall            python3-py
  libgdal32                     libpython3-all-dev       python3-beniget             python3-pypdf2
  libgeos3.11.1                 libpython3.11-dev        python3-boltons             python3-pythran
Use 'sudo apt autoremove' to remove them.

Upgrading:
  inetutils-telnet

Installing:
  telnet

Summary:
  Upgrading: 1, Installing: 1, Removing: 0, Not Upgrading: 996
  Download size: 173 kB
  Space needed: 78.8 kB / 33.7 GB available
```

Then test: **telnet localhost 23**

Expected result: **Connection refused** or **Connection timed out**.

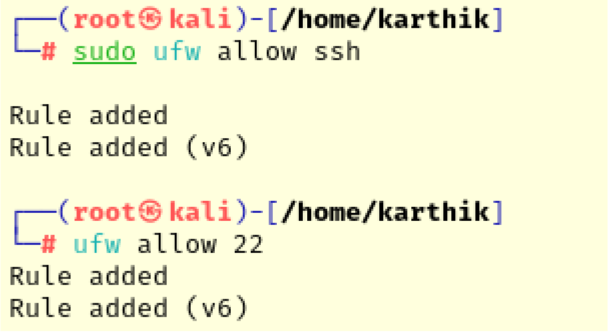


```
┌──(root㉿kali)-[/home/karthik]
└─# telnet localhost 23

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

5. Add rule to allow SSH (port 22)

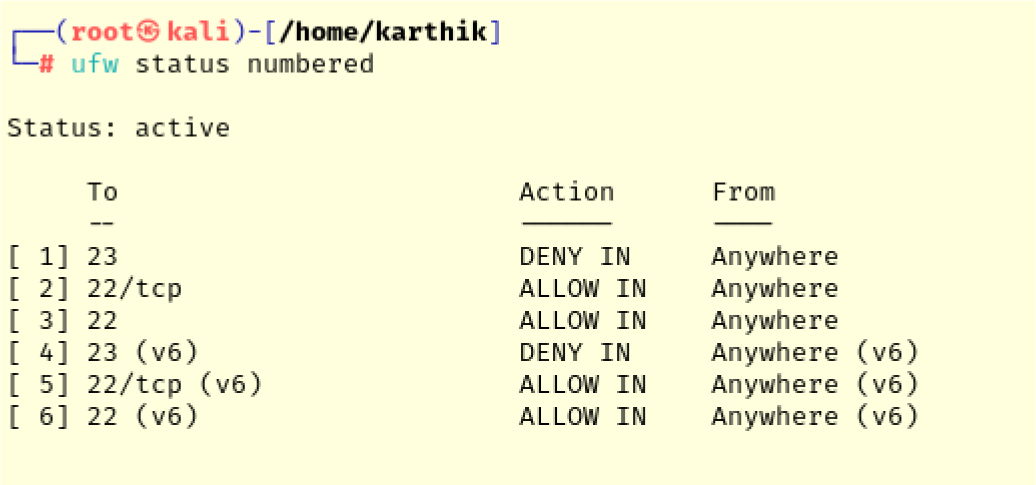
Allow SSH so you don't lock yourself out: **ufw allow ssh**

Or specifically: **ufw allow 22**



```
┌──(root㉿kali)-[/home/karthik]
└─# sudo ufw allow ssh

Rule added
Rule added (v6)

┌──(root㉿kali)-[/home/karthik]
└─# ufw allow 22
Rule added
Rule added (v6)
```

Always confirm: **ufw status numbered**



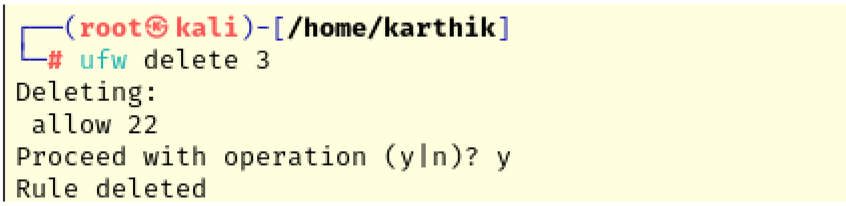
```
┌──(root㉿kali)-[/home/karthik]
└─# ufw status numbered

Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 23                         DENY IN     Anywhere
[ 2] 22/tcp                     ALLOW IN    Anywhere
[ 3] 22                         ALLOW IN    Anywhere
[ 4] 23 (v6)                    DENY IN     Anywhere (v6)
[ 5] 22/tcp (v6)                ALLOW IN    Anywhere (v6)
[ 6] 22 (v6)                    ALLOW IN    Anywhere (v6)
```

6. Remove the test block rule to restore original state

First, list rules: **ufw status numbered**

Find the number of the deny 23 rule, then delete: **ufw delete [rule-number]**

For example: **ufw delete 3**



```
┌──(root㉿kali)-[/home/karthik]
└─# ufw delete 3
Deleting:
 allow 22
Proceed with operation (y|n)? y
Rule deleted
```

A **firewall filters traffic** by applying rules to **incoming and outgoing network packets**. It uses:

- **Allow/deny rules** to permit or block specific IP addresses, ports, and protocols.
- **Default policies** (deny all or allow all) for traffic not explicitly matched by a rule.
- **Stateful inspection**, meaning it tracks active connections and allows return traffic for approved outgoing connections.

UFW simplifies this by letting users define human-readable rules, while the system translates them into underlying iptables/net filter configurations.