

# Task 2: Basic Firewall Configuration with UFW

## INSTALL UFW:

To install **UFW (Uncomplicated Firewall)** on a Linux system, first update your package list using the command `sudo apt update`. Then install UFW by running `sudo apt install ufw -y`. Before turning it on, it's important to allow SSH connections (especially if you are connected remotely) using `sudo ufw allow ssh`. After that, enable the firewall with `sudo ufw enable`. You can then verify its status with `sudo ufw status verbose` or check the version using `ufw version`. This setup ensures that UFW is properly installed, running, and configured with safe access to your system via SSH.

```
hack@kali: ~
$ sudo apt install ufw -y
The following packages were automatically installed and are no longer required:
binutils-mingw-w64-i686      imagemagick      libwscale6
binutils-mingw-w64-x86_64    imagemagick-7.q16 libudfread0
bloodhound.py                krb5-multidev    libxml2
comerr-dev                  libaio1t64       medusa
dnsmasq                      libapache2-mod-php mingw-w64-i686-dev
dsniff                       libavformat59    mingw-w64-x86_64-dev
ettercap-common              libbluray2       oracle-instantclient-basic
ettercap-graphical           libgssrpc4t64    python3-aardwolf
figlet                       libkadm5clnt-mit12 python3-aesedb
finger                       libkdb5-10t64    python3-alocmd
gcc-mingw-w64-base           libkrb5-dev      python3-alocmb
gcc-mingw-w64-i686-win32     libnids1.21t64   python3-aiowinreg
gcc-mingw-w64-x86_64-win32   libsm2-6         python3-arc4
gcc-mingw-w64-x86_64-win32-runtime libssh-gcrypt-4  python3-asciitree
python3-asn1tools            python3-asyaauth python3-oscrypto
python3-asysocks             python3-pefile    python3-unicrypto
python3-bitstruct            python3-pyexploitdb python3-winact
python3-dploit               python3-pyfiglet  python3-xmltodict
python3-git                  python3-pylnk3    python3-yaswfp
python3-gitdb                python3-pynfsclient rsh-radone-client
python3-lsassy               python3-pypsrp    simplescreenrecorder-lib
python3-masky                python3-pysshodan smtp-user-enum
python3-minidump             python3-pysshodan sparta-scripts
python3-minikerberos         python3-qasync    toilet-fonts
python3-msldap               python3-qrcode    unicornscan
python3-neo4j                python3-serial-asyncio urlscan
python3-neobolt              python3-smap      wapi1
python3-neotime              python3-tld

Installing:
ufw

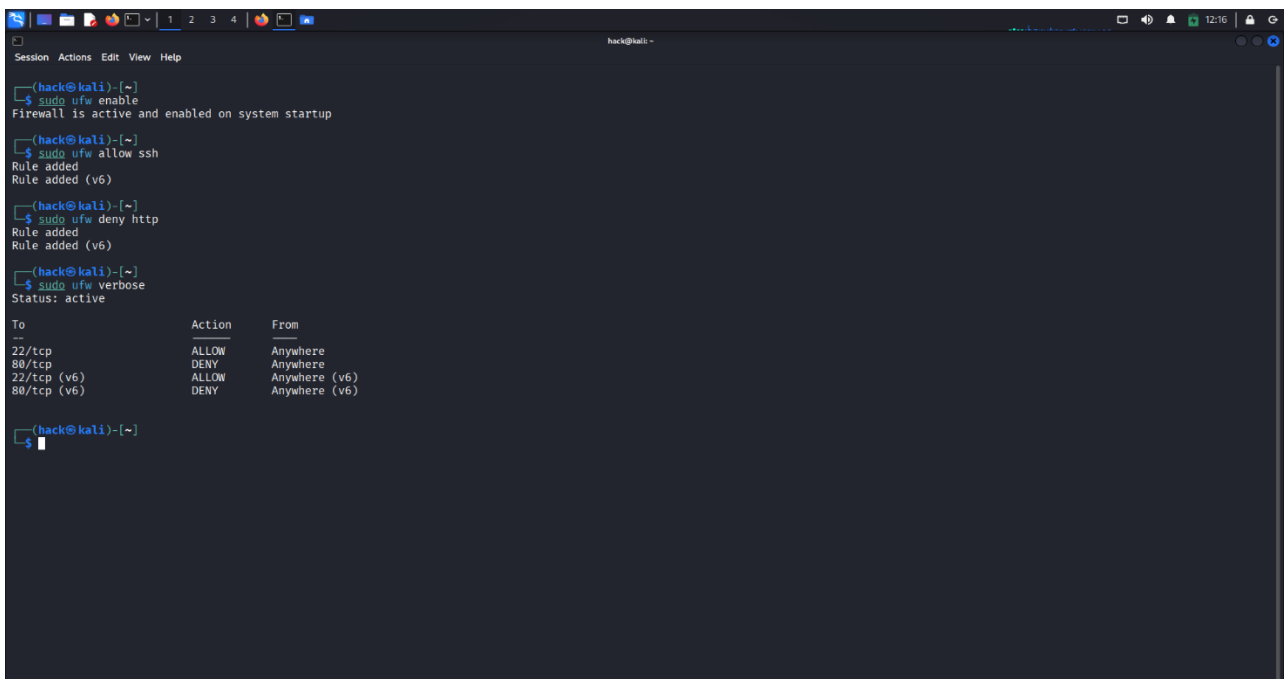
Suggested packages:
rsyslog

Summary:
Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 376
Download size: 169 kB
Space needed: 880 kB / 38.6 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 (180 kB/s)
Preconfiguring packages ...
Selecting previously unselected package ufw.
(Reading database ... 397884 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 (2025.4.1) ...
Processing triggers for man-db (2.13.1-1) ...
```

## SETTING UP UFW:

After installing UFW, you can begin configuring your firewall rules to control network traffic. Start by allowing essential services such as SSH using `sudo ufw allow ssh` to ensure remote access remains available. You can then deny or allow other ports based on your security needs — for example, `sudo ufw deny http` to block web traffic. Once your rules are set, enable the firewall with `sudo ufw enable` and verify the configuration using `sudo ufw status verbose`. This ensures that your system is protected and only trusted connections are allowed.



```
(hack@kali)~$ sudo ufw enable
Firewall is active and enabled on system startup

(hack@kali)~$ sudo ufw allow ssh
Rule added
Rule added (v6)

(hack@kali)~$ sudo ufw deny http
Rule added
Rule added (v6)

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

To Action From
--
22/tcp ALLOW Anywhere
80/tcp DENY Anywhere
22/tcp (v6) ALLOW Anywhere (v6)
80/tcp (v6) DENY Anywhere (v6)

(hack@kali)~$
```