UPES

UNIVERSITY OF TOMORROW

IT DATA SECURITY LAB FILE

Name- Dhairya Jain

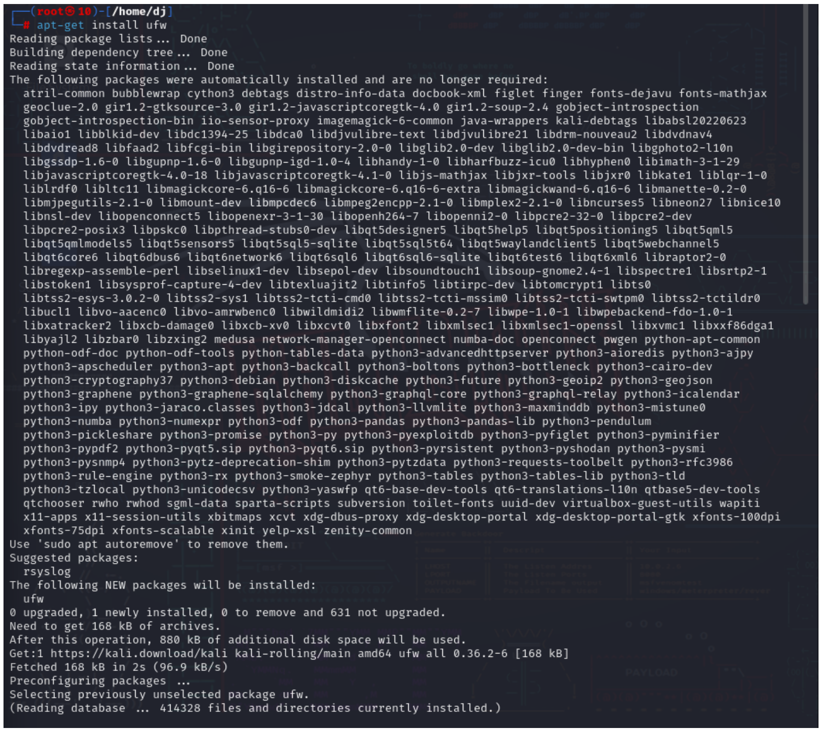
Sap ID- 500105432

Batch- CSF-B4

Experiment – 2

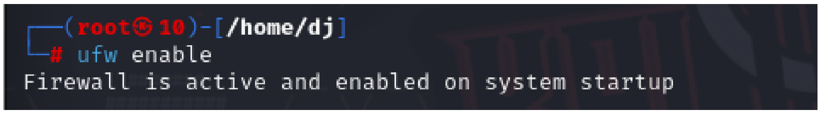
Aim- UFW (Uncomplicated Firewall)

- Installation



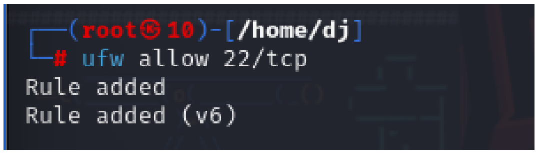
```
┌──(root㉿10)-[/home/dj]
└─# apt-get install ufw
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following packages were automatically installed and are no longer required:
  atril-common bubblewrap cython3 debtags distro-info-data docbook-xml figlet finger fonts-dejavu fonts-mathjax
  geoclue-2.0 gir1.2-gtksource-3.0 gir1.2-javascriptcoregtk-4.0 gir1.2-soup-2.4 gobject-introspection
  gobject-introspection-bin iio-sensor-proxy imagemagick-6-common java-wrappers kali-debtags libabsl20220623
  libaio1 libblkid-dev libdc1394-25 libdca0 libdjvulibre-text libdjvulibre21 libdrm-nouveau2 libdvdnav4
  libdvdread8 libfaad2 libfcgi-bin libgirepository-2.0-0 libglib2.0-dev libglib2.0-dev-bin libgphoto2-l10n
  libgssdp-1.6-0 libgupnp-1.6-0 libgupnp-igd-1.0-4 libhandy-1-0 libharfbuzz-icu0 libhyphen0 libimath-3-1-29
  libjavascriptcoregtk-4.0-18 libjavascriptcoregtk-4.1-0 libjs-mathjax libjxr-tools libjxr0 libkate1 liblqr-1-0
  liblrdf0 libltc11 libmagickcore-6.q16-6 libmagickcore-6.q16-6-extra libmagickwand-6.q16-6 libmanette-0.2-0
  libmjpegutils-2.1-0 libmount-dev libmpcdec6 libmpeg2encpp-2.1-0 libmplex2-2.1-0 libncurses5 libneon27 libnice10
  libnsl-dev libopenconnect5 libopenexr-3-1-30 libopenh264-7 libopenni2-0 libpcre2-32-0 libpcre2-dev
  libpcre2-posix3 libpskc0 libpthread-stubs0-dev libqt5designer5 libqt5help5 libqt5positioning5 libqt5qml5
  libqt5qmlmodels5 libqt5sensors5 libqt5sql5-sqlite libqt5sql5t64 libqt5waylandclient5 libqt5webchannel5
  libqt6core6 libqt6dbus6 libqt6network6 libqt6sql6 libqt6sql6-sqlite libqt6test6 libqt6xml6 libraptor2-0
  libregexp-assemble-perl libselinux1-dev libsepol-dev libsoundtouch1 libsoup-gnome2.4-1 libspectre1 libsrtp2-1
  libstoken1 libsysprof-capture-4-dev libtexluajit2 libtinfo5 libtirpc-dev libtomcrypt1 libts0
  libtss2-esys-3.0.2-0 libtss2-sys1 libtss2-tcti-cmd0 libtss2-tcti-mssim0 libtss2-tcti-swtpm0 libtss2-tctildr0
  libucl1 libvo-aacenc0 libvo-amrwbenc0 libwildmidi2 libwmflite-0.2-7 libwpe-1.0-1 libwpebackend-fdo-1.0-1
  libxatracker2 libxcb-damage0 libxcb-xv0 libxcvt0 libxfont2 libxmlsec1 libxmlsec1-openssl libxvmc1 libxxf86dga1
  libyajl2 libzbar0 libzxing2 medusa network-manager-openconnect numba-doc openconnect pwgen python-apt-common
  python-odf-doc python-odf-tools python-tables-data python3-advancedhttpserver python3-aioredis python3-ajpy
  python3-apscheduler python3-apt python3-backcall python3-boltons python3-bottleneck python3-cairo-dev
  python3-cryptography37 python3-debian python3-diskcache python3-future python3-geoip2 python3-geojson
  python3-graphene python3-graphene-sqlalchemy python3-graphql-core python3-graphql-relay python3-icalendar
  python3-ipy python3-jaraco.classes python3-jdcal python3-llvmlite python3-maxminddb python3-mistune0
  python3-numba python3-numexpr python3-odf python3-pandas python3-pandas-lib python3-pendulum
  python3-pickleshare python3-promise python3-py python3-pyexploitdb python3-pyfiglet python3-pyminifier
  python3-pypdf2 python3-pyqt5.sip python3-pyqt6.sip python3-pyrsistent python3-pyshodan python3-pysmi
  python3-pysnmp4 python3-pytz-deprecation-shim python3-pytzdata python3-requests-toolbelt python3-rfc3986
  python3-rule-engine python3-rx python3-smoke-zephyr python3-tables python3-tables-lib python3-tld
  python3-tzlocal python3-unicodecsv python3-yaswfp qt6-base-dev-tools qt6-translations-l10n qtbase5-dev-tools
  qtchooser rwho rwhod sgml-data sparta-scripts subversion toilet-fonts uuid-dev virtualbox-guest-utils wapiti
  x11-apps x11-session-utils xbitmaps xcvt xdg-dbus-proxy xdg-desktop-portal xdg-desktop-portal-gtk xfonts-100dpi
  xfonts-75dpi xfonts-scalable xinit yelp-xsl zenity-common
Use 'sudo apt autoremove' to remove them.
Suggested packages:
  rsyslog
The following NEW packages will be installed:
  ufw
0 upgraded, 1 newly installed, 0 to remove and 631 not upgraded.
Need to get 168 kB of archives.
After this operation, 880 kB of additional disk space will be used.
Get:1 https://kali.download/kali kali-rolling/main amd64 ufw all 0.36.2-6 [168 kB]
Fetched 168 kB in 2s (96.9 kB/s)
Preconfiguring packages ...
Selecting previously unselected package ufw.
(Reading database ... 414328 files and directories currently installed.)
```

- Basic Commands
- Enable UFW:



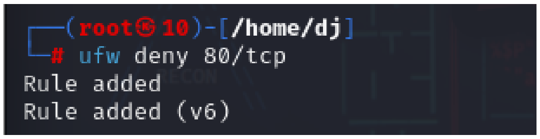
```
┌──(root㉿10)-[/home/dj]
└─# ufw enable
Firewall is active and enabled on system startup
```

- Allow specific port (e.g., SSH on port 22)



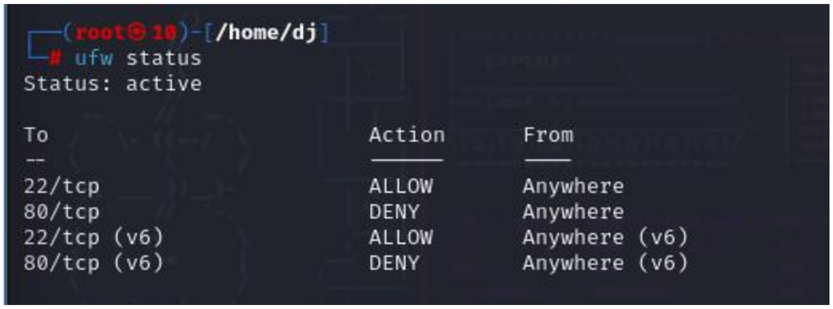
```
┌──(root㉿10)-[/home/dj]
└─# ufw allow 22/tcp
Rule added
Rule added (v6)
```

- Deny a specific port:



```
┌──(root㉿10)-[/home/dj]
└─# ufw deny 80/tcp
Rule added
Rule added (v6)
```

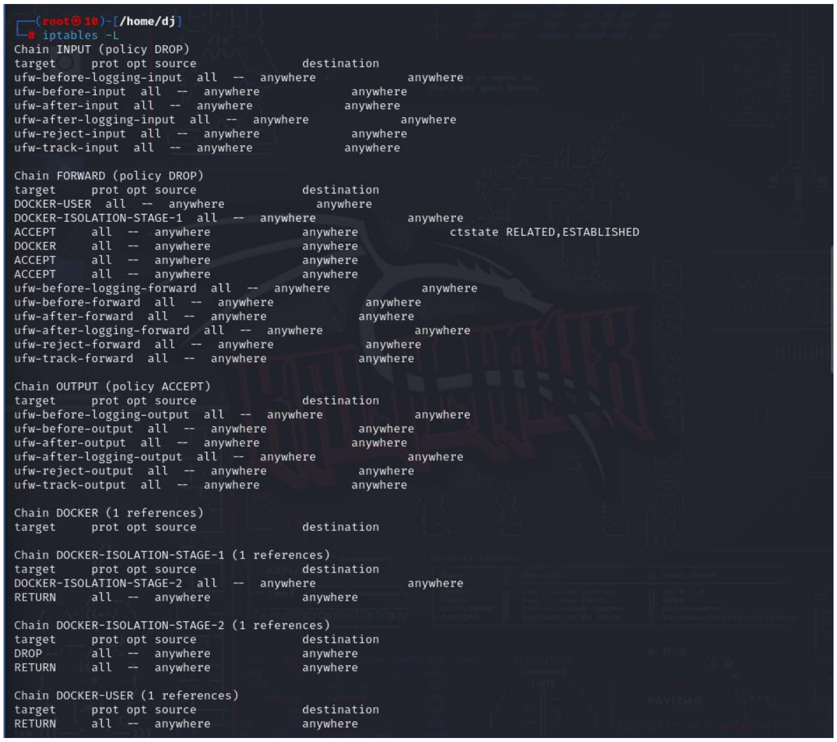
- Check status:



```
┌──(root㉿10)-[/home/dj]
└─# ufw status
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)
```

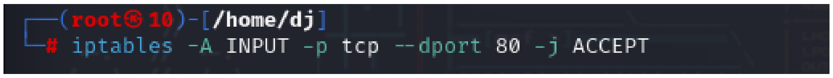
Iptables

- List current rules



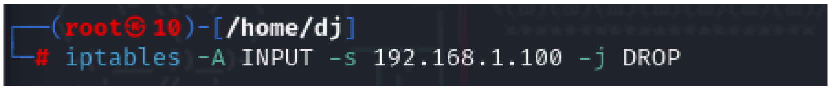
```
┌──(root㉿10)-[/home/dj]
└─# iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ufw-before-logging-input  all  --  anywhere             anywhere
ufw-before-input  all  --  anywhere             anywhere
ufw-after-input  all  --  anywhere             anywhere
ufw-after-logging-input  all  --  anywhere             anywhere
ufw-reject-input  all  --  anywhere             anywhere
ufw-track-input  all  --  anywhere             anywhere

Chain FORWARD (policy DROP)
target     prot opt source               destination
DOCKER-USER  all  --  anywhere             anywhere
DOCKER-ISOLATION-STAGE-1  all  --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere             ctstate RELATED,ESTABLISHED
DOCKER     all  --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere
ufw-before-logging-forward  all  --  anywhere             anywhere
ufw-before-forward  all  --  anywhere             anywhere
ufw-after-forward  all  --  anywhere             anywhere
ufw-after-logging-forward  all  --  anywhere             anywhere
ufw-reject-forward  all  --  anywhere             anywhere
ufw-track-forward  all  --  anywhere             anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ufw-before-logging-output  all  --  anywhere             anywhere
ufw-before-output  all  --  anywhere             anywhere
ufw-after-output  all  --  anywhere             anywhere
ufw-after-logging-output  all  --  anywhere             anywhere
ufw-reject-output  all  --  anywhere             anywhere
ufw-track-output  all  --  anywhere             anywhere

Chain DOCKER (1 references)
target     prot opt source               destination

Chain DOCKER-ISOLATION-STAGE-1 (1 references)
target     prot opt source               destination
DOCKER-ISOLATION-STAGE-2  all  --  anywhere             anywhere
RETURN     all  --  anywhere             anywhere

Chain DOCKER-ISOLATION-STAGE-2 (1 references)
target     prot opt source               destination
DROP       all  --  anywhere             anywhere
RETURN     all  --  anywhere             anywhere

Chain DOCKER-USER (1 references)
target     prot opt source               destination
RETURN     all  --  anywhere             anywhere
```

- Allow a specific port (e.g., HTTP on port 80):



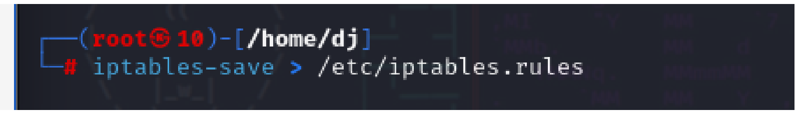
```
┌──(root㉿10)-[/home/dj]
└─# iptables -A INPUT -p tcp --dport 80 -j ACCEPT
```

- Block a specific IP address:



```
┌──(root㉿10)-[/home/dj]
└─# iptables -A INPUT -s 192.168.1.100 -j DROP
```

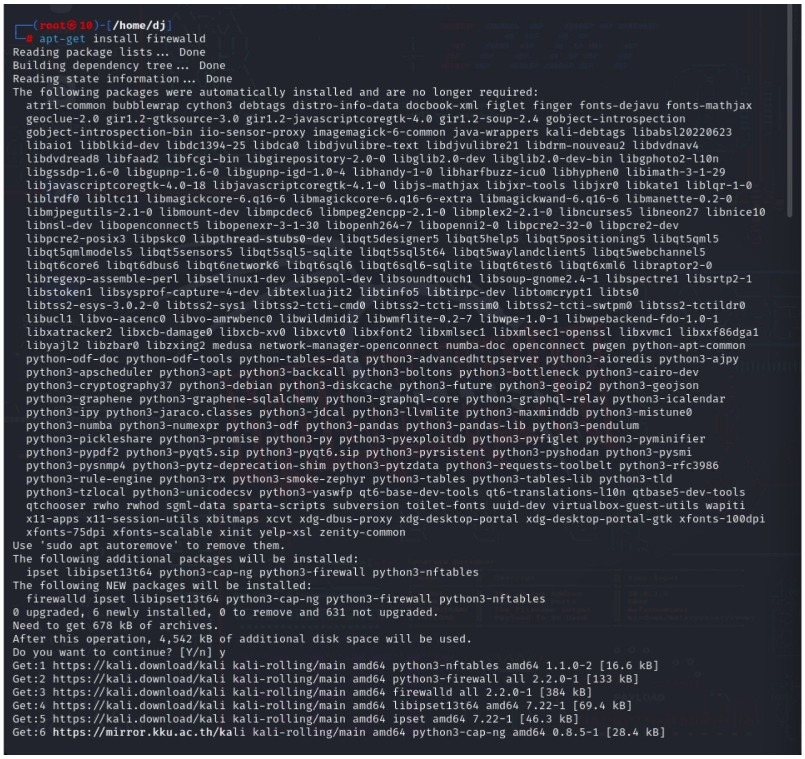
- Save rules:



```
┌──(root㉿10)-[/home/dj]
└─# iptables-save > /etc/iptables.rules
```

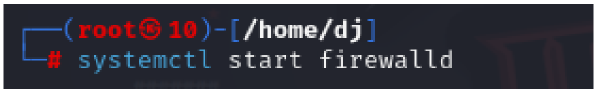
Firewalld

- Installation



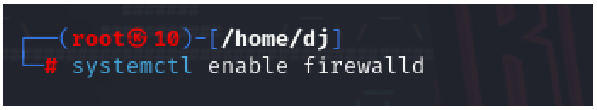
```
┌──(root㉿10)-[/home/dj]
└─# apt-get install firewalld
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following packages were automatically installed and are no longer required:
  atril-common bubblewrap cython3 debtags distro-info-data docbook-xml figlet finger fonts-dejavu fonts-mathjax
  geoclue-2.0 gir1.2-gtksource-3.0 gir1.2-javascriptcoregtk-4.0 gir1.2-soup-2.4 gobject-introspection
  gobject-introspection-bin iio-sensor-proxy imagemagick-6-common java-wrappers kali-debtags libabsl20220623
  libaio1 libblkid-dev libdc1394-25 libdca0 libdjvulibre-text libdjvulibre21 libdrm-nouveau2 libdvdnav4
  libdvdread8 libfaad2 libfcgi-bin libgirepository-2.0-0 libglib2.0-dev libglib2.0-dev-bin libgphoto2-l10n
  libgssdp-1.6-0 libgupnp-1.6-0 libgupnp-igd-1.0-4 libhandy-1-0 libharfbuzz-icu0 libhyphen0 libimath-3-1-29
  libjavascriptcoregtk-4.0-18 libjavascriptcoregtk-4.1-0 libjs-mathjax libjxr-tools libjxr0 libkate1 liblqr-1-0
  liblrdf0 libltc11 libmagickcore-6.q16-6 libmagickcore-6.q16-6-extra libmagickwand-6.q16-6 libmanette-0.2-0
  libmjpegutils-2.1-0 libmount-dev libmpcdec6 libmpeg2encpp-2.1-0 libmplex2-2.1-0 libncurses5 libneon27 libnice10
  libnsl-dev libopenconnect5 libopenexr-3-1-30 libopenh264-7 libopenni2-0 libpcre2-32-0 libpcre2-dev
  libpcre2-posix3 libpskc0 libpthread-stubs0-dev libqt5designer5 libqt5help5 libqt5positioning5 libqt5qml5
  libqt5qmlmodels5 libqt5sensors5 libqt5sql5-sqlite libqt5sql5t64 libqt5waylandclient5 libqt5webchannel5
  libqt6core6 libqt6dbus6 libqt6network6 libqt6sql6 libqt6sql6-sqlite libqt6test6 libqt6xml6 libraptor2-0
  libregexp-assemble-perl libselinux1-dev libsepol-dev libsoundtouch1 libsoup-gnome2.4-1 libspectre1 libsrtp2-1
  libstoken1 libsysprof-capture-4-dev libtexluajit2 libtinfo5 libtirpc-dev libtomcrypt1 libts0
  libtss2-esys-3.0.2-0 libtss2-sys1 libtss2-tcti-cmd0 libtss2-tcti-mssim0 libtss2-tcti-swtpm0 libtss2-tctildr0
  libucl1 libvo-aacenc0 libvo-amrwbenc0 libwildmidi2 libwmflite-0.2-7 libwpe-1.0-1 libwpebackend-fdo-1.0-1
  libxatracker2 libxcb-damage0 libxcb-xv0 libxcvt0 libxfont2 libxmlsec1 libxmlsec1-openssl libxvmc1 libxxf86dga1
  libyajl2 libzbar0 libzxing2 medusa network-manager-openconnect numba-doc openconnect pwgen python-apt-common
  python-odf-doc python-odf-tools python-tables-data python3-advancedhttpserver python3-aioredis python3-ajpy
  python3-apscheduler python3-apt python3-backcall python3-boltons python3-bottleneck python3-cairo-dev
  python3-cryptography37 python3-debian python3-diskcache python3-future python3-geoip2 python3-geojson
  python3-graphene python3-graphene-sqlalchemy python3-graphql-core python3-graphql-relay python3-icalendar
  python3-ipy python3-jaraco.classes python3-jdcal python3-llvmlite python3-maxminddb python3-mistune0
  python3-numba python3-numexpr python3-odf python3-pandas python3-pandas-lib python3-pendulum
  python3-pickleshare python3-promise python3-py python3-pyexploitdb python3-pyfiglet python3-pyminifier
  python3-pypdf2 python3-pyqt5.sip python3-pyqt6.sip python3-pyrsistent python3-pyshodan python3-pysmi
  python3-pysnmp4 python3-pytz-deprecation-shim python3-pytzdata python3-requests-toolbelt python3-rfc3986
  python3-rule-engine python3-rx python3-smoke-zephyr python3-tables python3-tables-lib python3-tld
  python3-tzlocal python3-unicodecsv python3-yaswfp qt6-base-dev-tools qt6-translations-l10n qtbase5-dev-tools
  qtchooser rwho rwhod sgml-data sparta-scripts subversion toilet-fonts uuid-dev virtualbox-guest-utils wapiti
  x11-apps x11-session-utils xbitmaps xcvt xdg-dbus-proxy xdg-desktop-portal xdg-desktop-portal-gtk xfonts-100dpi
  xfonts-75dpi xfonts-scalable xinit yelp-xsl zenity-common
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  ipset libipset13t64 python3-cap-ng python3-firewall python3-nftables
The following NEW packages will be installed:
  firewalld ipset libipset13t64 python3-cap-ng python3-firewall python3-nftables
0 upgraded, 6 newly installed, 0 to remove and 631 not upgraded.
Need to get 678 kB of archives.
After this operation, 4,542 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 https://kali.download/kali kali-rolling/main amd64 python3-nftables amd64 1.1.0-2 [16.6 kB]
Get:2 https://kali.download/kali kali-rolling/main amd64 python3-firewall all 2.2.0-1 [133 kB]
Get:3 https://kali.download/kali kali-rolling/main amd64 firewalld all 2.2.0-1 [384 kB]
Get:4 https://kali.download/kali kali-rolling/main amd64 libipset13t64 amd64 7.22-1 [69.4 kB]
Get:5 https://kali.download/kali kali-rolling/main amd64 ipset amd64 7.22-1 [46.3 kB]
Get:6 https://mirror.kku.ac.th/kali kali-rolling/main amd64 python3-cap-ng amd64 0.8.5-1 [28.4 kB]
```

- Basic Commands:
- Start Firewalld



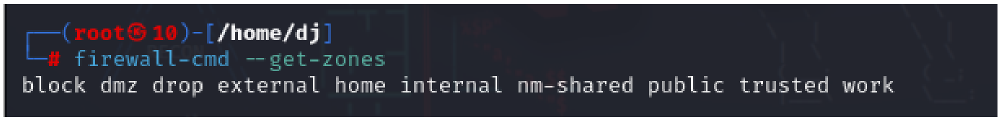
```
┌──(root㉿10)-[/home/dj]
└─# systemctl start firewalld
```

- Enable Firewalld on boot



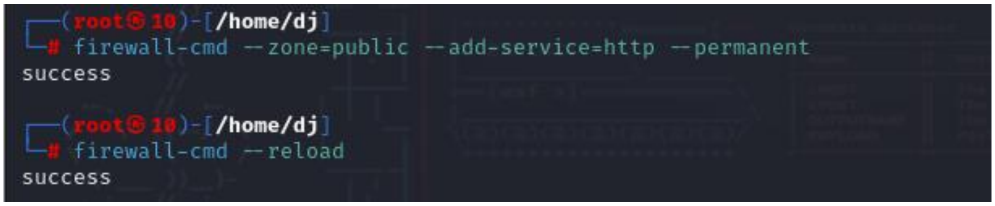
```
┌──(root㉿10)-[/home/dj]
└─# systemctl enable firewalld
```

- List all available zones



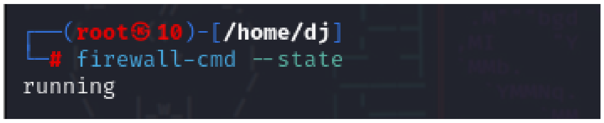
```
┌──(root㉿10)-[/home/dj]
└─# firewall-cmd --get-zones
block dmz drop external home internal nm-shared public trusted work
```

- Allow a service (e.g., HTTP) in the public zone



```
┌──(root㉿10)-[/home/dj]
└─# firewall-cmd --zone=public --add-service=http --permanent
success

┌──(root㉿10)-[/home/dj]
└─# firewall-cmd --reload
success
```

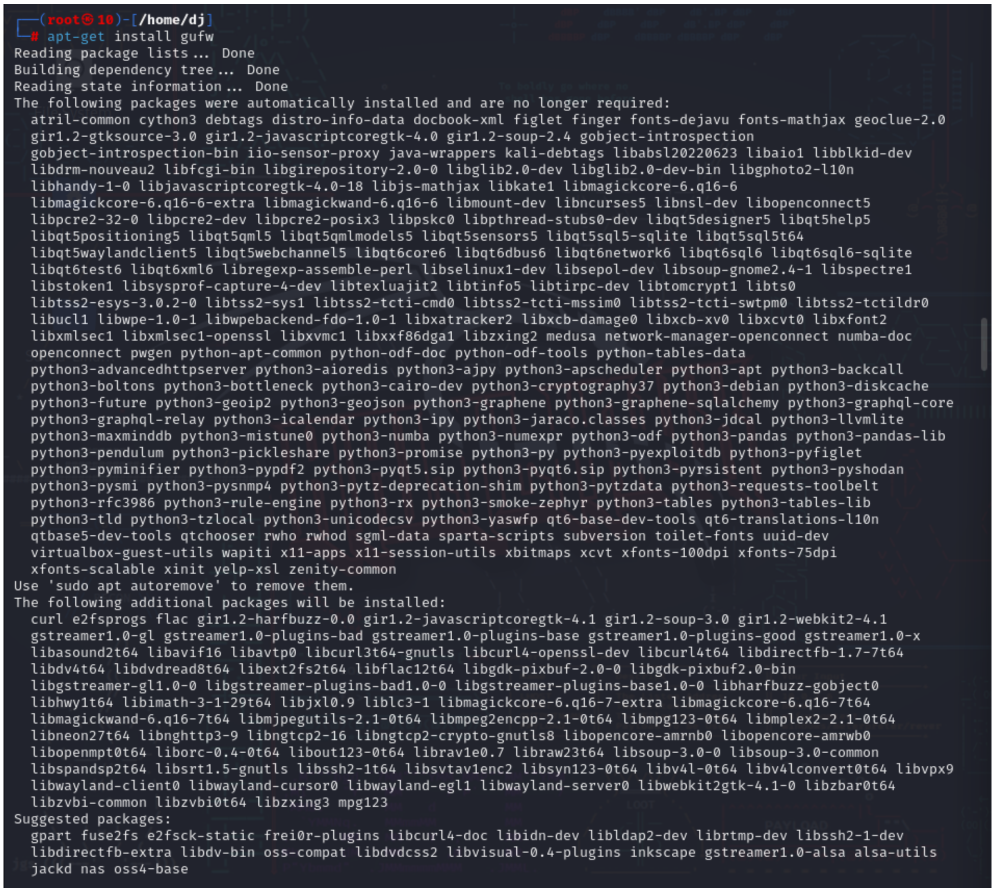
- Check the status of the firewall



```
┌──(root㉿10)-[/home/dj]
└─# firewall-cmd --state
running
```

GUFW (Graphical Interface for UFW)

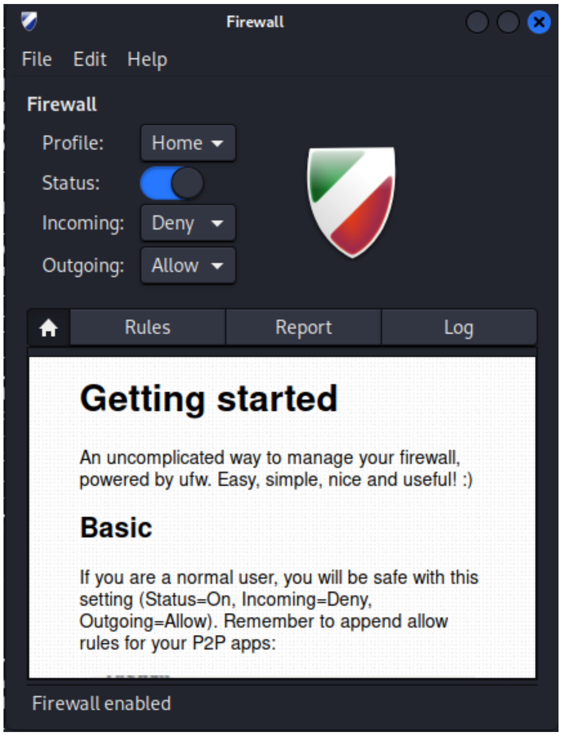
- Installation-



```
┌──(root㉿10)-[/home/dj]
└─# apt-get install gufw
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following packages were automatically installed and are no longer required:
  atril-common cython3 debtags distro-info-data docbook-xml figlet finger fonts-dejavu fonts-mathjax geoclue-2.0
  gir1.2-gtksource-3.0 gir1.2-javascriptcoregtk-4.0 gir1.2-soup-2.4 gobject-introspection
  gobject-introspection-bin iio-sensor-proxy java-wrappers kali-debtags libabsl20220623 libaio1 libblkid-dev
  libdrm-nouveau2 libfcgi-bin libgirepository-2.0-0 libglib2.0-dev libglib2.0-dev-bin libgphoto2-l10n
  libhandy-1-0 libjavascriptcoregtk-4.0-18 libjs-mathjax libkate1 libmagickcore-6.q16-6
  libmagickcore-6.q16-6-extra libmagickwand-6.q16-6 libmount-dev libncurses5 libnsl-dev libopenconnect5
  libpcre2-32-0 libpcre2-dev libpcre2-posix3 libpskc0 libpthread-stubs0-dev libqt5designer5 libqt5help5
  libqt5positioning5 libqt5qml5 libqt5qmlmodels5 libqt5sensors5 libqt5sql5-sqlite libqt5sql5t64
  libqt5waylandclient5 libqt5webchannel5 libqt6core6 libqt6dbus6 libqt6network6 libqt6sql6 libqt6sql6-sqlite
  libqt6test6 libqt6xml6 libregexp-assemble-perl libselinux1-dev libsepol-dev libsoup-gnome2.4-1 libspectre1
  libstoken1 libsysprof-capture-4-dev libtexluajit2 libtinfo5 libtirpc-dev libtomcrypt1 libts0
  libtss2-esys-3.0.2-0 libtss2-sys1 libtss2-tcti-cmd0 libtss2-tcti-mssim0 libtss2-tcti-swtpm0 libtss2-tctildr0
  libucl1 libwpe-1.0-1 libwpebackend-fdo-1.0-1 libxatracker2 libxcb-damage0 libxcb-xv0 libxcvt0 libxfont2
  libxmlsec1 libxmlsec1-openssl libxvmc1 libxxf86dga1 libzxing2 medusa network-manager-openconnect numba-doc
  openconnect pwgen python-apt-common python-odf-doc python-odf-tools python-tables-data
  python3-advancedhttpserver python3-aioredis python3-ajpy python3-apscheduler python3-apt python3-backcall
  python3-boltons python3-bottleneck python3-cairo-dev python3-cryptography37 python3-debian python3-diskcache
  python3-future python3-geoip2 python3-geojson python3-graphene python3-graphene-sqlalchemy python3-graphql-core
  python3-graphql-relay python3-icalendar python3-ipy python3-jaraco.classes python3-jdcal python3-llvmlite
  python3-maxminddb python3-mistune0 python3-numba python3-numexpr python3-odf python3-pandas python3-pandas-lib
  python3-pendulum python3-pickleshare python3-promise python3-py python3-pyexploitdb python3-pyfiglet
  python3-pyminifier python3-pypdf2 python3-pyqt5.sip python3-pyqt6.sip python3-pyrsistent python3-pyshodan
  python3-pysmi python3-pysnmp4 python3-pytz-deprecation-shim python3-pytzdata python3-requests-toolbelt
  python3-rfc3986 python3-rule-engine python3-rx python3-smoke-zephyr python3-tables python3-tables-lib
  python3-tld python3-tzlocal python3-unicodecsv python3-yaswfp qt6-base-dev-tools qt6-translations-l10n
  qtbase5-dev-tools qtchooser rwho rwhod sgml-data sparta-scripts subversion toilet-fonts uuid-dev
  virtualbox-guest-utils wapiti x11-apps x11-session-utils xbitmaps xcvt xfonts-100dpi xfonts-75dpi
  xfonts-scalable xinit yelp-xsl zenity-common
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  curl e2fsprogs flac gir1.2-harfbuzz-0.0 gir1.2-javascriptcoregtk-4.1 gir1.2-soup-3.0 gir1.2-webkit2-4.1
  gstreamer1.0-gl gstreamer1.0-plugins-bad gstreamer1.0-plugins-base gstreamer1.0-plugins-good gstreamer1.0-x
  libasound2t64 libavif16 libavtp0 libcurl3t64-gnutls libcurl4-openssl-dev libcurl4t64 libdirectfb-1.7-7t64
  libdv4t64 libdvdread8t64 libext2fs2t64 libflac12t64 libgdk-pixbuf-2.0-0 libgdk-pixbuf2.0-bin
  libgstreamer-gl1.0-0 libgstreamer-plugins-bad1.0-0 libgstreamer-plugins-base1.0-0 libharfbuzz-gobject0
  libhwy1t64 libimath-3-1-29t64 libjxl0.9 liblc3-1 libmagickcore-6.q16-7-extra libmagickcore-6.q16-7t64
  libmagickwand-6.q16-7t64 libmjpegutils-2.1-0t64 libmpeg2encpp-2.1-0t64 libmpg123-0t64 libmplex2-2.1-0t64
  libneon27t64 libnghttp3-9 libngtcp2-16 libngtcp2-crypto-gnutls8 libopencore-amrnb0 libopencore-amrwb0
  libopenmpt0t64 liborc-0.4-0t64 libout123-0t64 librav1e0.7 libraw23t64 libsoup-3.0-0 libsoup-3.0-common
  libspandsp2t64 libsrt1.5-gnutls libssh2-1t64 libsvtav1enc2 libsyn123-0t64 libv4l-0t64 libv4lconvert0t64 libvpx9
  libwayland-client0 libwayland-cursor0 libwayland-egl1 libwayland-server0 libwebkit2gtk-4.1-0 libzbar0t64
  libzvbi-common libzvbi0t64 libzxing3 mpg123
Suggested packages:
  gpart fuse2fs e2fsck-static frei0r-plugins libcurl4-doc libidn-dev libldap2-dev librtmp-dev libssh2-1-dev
  libdirectfb-extra libdv-bin oss-compat libdvdcss2 libvisual-0.4-plugins inkscape gstreamer1.0-alsa alsa-utils
  jackd nas oss4-base
```

- **Usage:**

After installation, you can launch GUFW from the applications menu and use its simple interface to enable/disable the firewall, allow/deny ports, and manage rules.



Firewall

Profile: Home

Status: On

Incoming: Deny

Outgoing: Allow

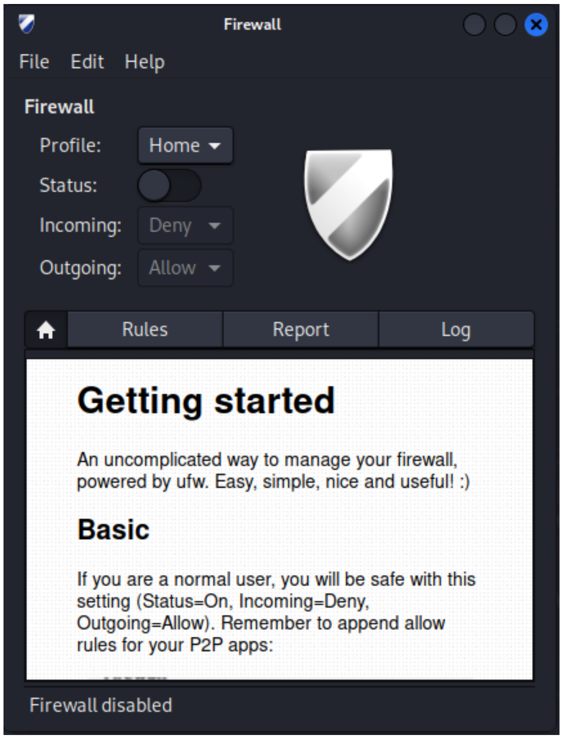
Getting started

An uncomplicated way to manage your firewall, powered by ufw. Easy, simple, nice and useful! :)

Basic

If you are a normal user, you will be safe with this setting (Status=On, Incoming=Deny, Outgoing=Allow). Remember to append allow rules for your P2P apps:

Firewall enabled



Firewall

Profile: Home

Status: Off

Incoming: Deny

Outgoing: Allow

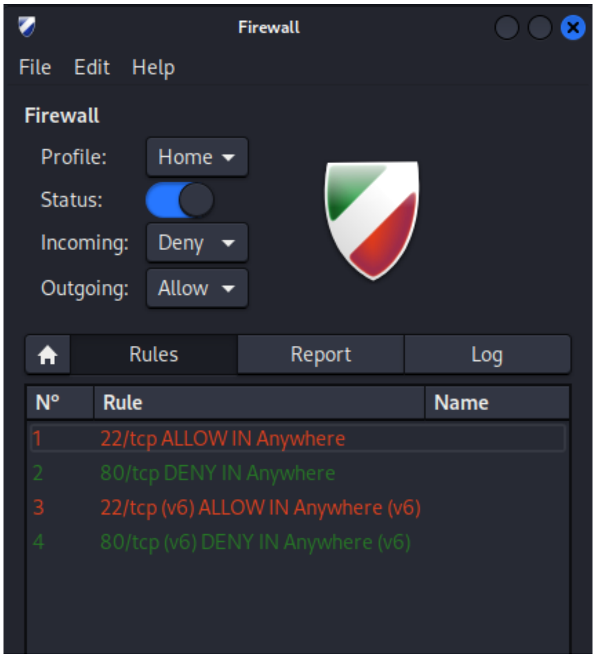
Getting started

An uncomplicated way to manage your firewall, powered by ufw. Easy, simple, nice and useful! :)

Basic

If you are a normal user, you will be safe with this setting (Status=On, Incoming=Deny, Outgoing=Allow). Remember to append allow rules for your P2P apps:

Firewall disabled



Firewall

Profile: Home

Status:

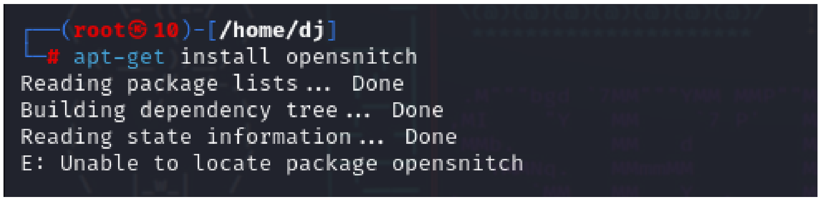
Incoming: Deny

Outgoing: Allow

N°	Rule	Name
1	22/tcp ALLOW IN Anywhere	
2	80/tcp DENY IN Anywhere	
3	22/tcp (v6) ALLOW IN Anywhere (v6)	
4	80/tcp (v6) DENY IN Anywhere (v6)	

OpenSnitch-

- Installation-

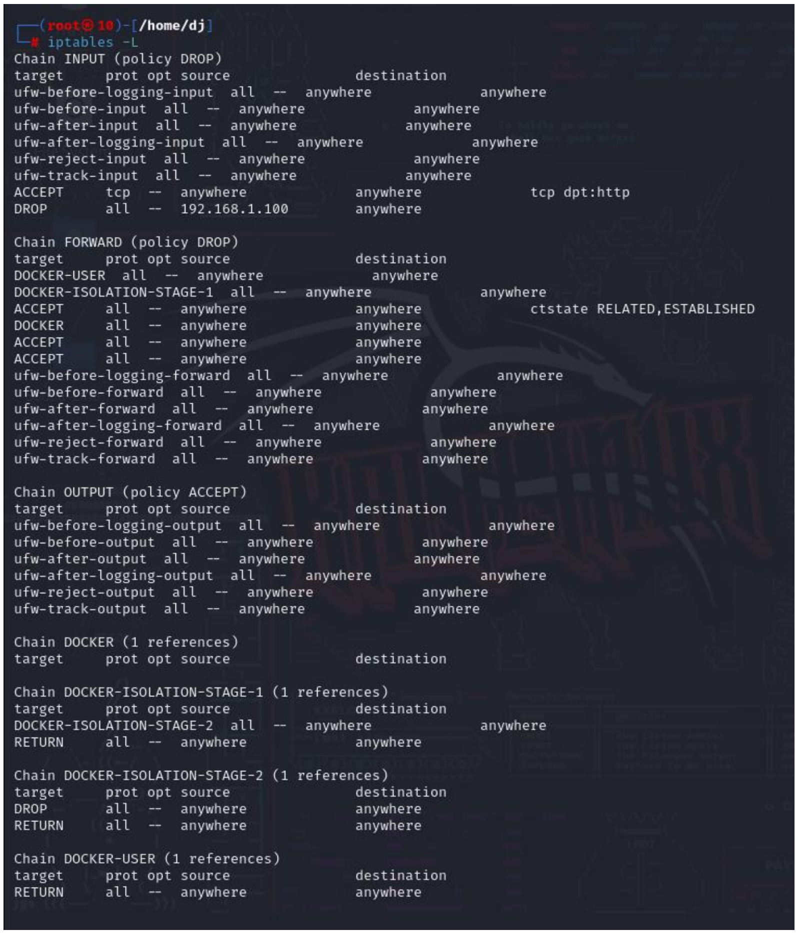


```
┌──(root㉿10)-[/home/dj]
└─# apt-get install opensnitch
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
E: Unable to locate package opensnitch
```

Firewall Configuration and Vulnerability Finding in Kali Linux

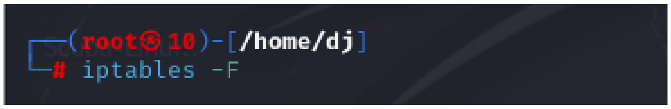
Firewall Configuration

- View current rules



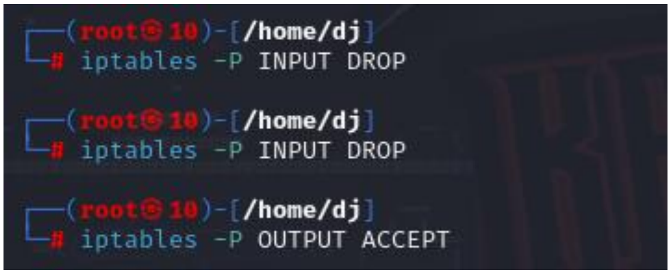
```
┌──(root㉿10)-[/home/dj]
└─# iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ufw-before-logging-input  all  --  anywhere             anywhere
ufw-before-input  all  --  anywhere             anywhere
ufw-after-input  all  --  anywhere             anywhere
ufw-after-logging-input  all  --  anywhere             anywhere
ufw-reject-input  all  --  anywhere             anywhere
ufw-track-input  all  --  anywhere             anywhere
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http
DROP       all  --  192.168.1.100        anywhere

Chain FORWARD (policy DROP)
target     prot opt source               destination
DOCKER-USER  all  --  anywhere             anywhere
DOCKER-ISOLATION-STAGE-1  all  --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere             ctstate RELATED,ESTABLISHED
DOCKER     all  --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere
ufw-before-logging-forward  all  --  anywhere             anywhere
ufw-before-forward  all  --  anywhere             anywhere
ufw-after-forward  all  --  anywhere             anywhere
ufw-after-logging-forward  all  --  anywhere             anywhere
ufw-reject-forward  all  --  anywhere             anywhere
ufw-track-forward  all  --  anywhere             anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ufw-before-logging-output  all  --  anywhere             anywhere
ufw-before-output  all  --  anywhere             anywhere
ufw-after-output  all  --  anywhere             anywhere
ufw-after-logging-output  all  --  anywhere             anywhere
ufw-reject-output  all  --  anywhere             anywhere
ufw-track-output  all  --  anywhere             anywhere

Chain DOCKER (1 references)
target     prot opt source               destination

Chain DOCKER-ISOLATION-STAGE-1 (1 references)
target     prot opt source               destination
DOCKER-ISOLATION-STAGE-2  all  --  anywhere             anywhere
RETURN     all  --  anywhere             anywhere

Chain DOCKER-ISOLATION-STAGE-2 (1 references)
target     prot opt source               destination
DROP       all  --  anywhere             anywhere
RETURN     all  --  anywhere             anywhere

Chain DOCKER-USER (1 references)
target     prot opt source               destination
RETURN     all  --  anywhere             anywhere
```

- Flush existing rules



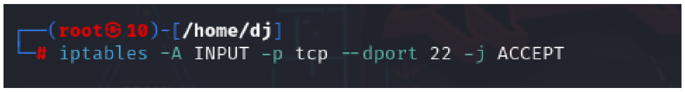
```
┌──(root㉿10)-[/home/dj]
└─# iptables -F
```

- Set default policies



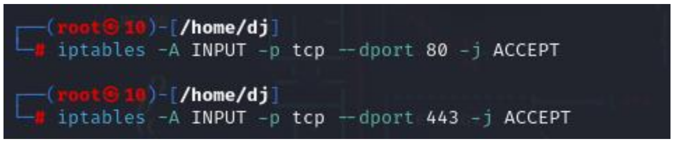
```
┌──(root㉿10)-[/home/dj]
└─# iptables -P INPUT DROP

┌──(root㉿10)-[/home/dj]
└─# iptables -P INPUT DROP

┌──(root㉿10)-[/home/dj]
└─# iptables -P OUTPUT ACCEPT
```

- Allow ssh access



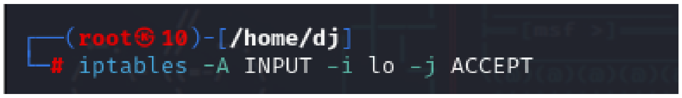
```
┌──(root㉿10)-[/home/dj]
└─# iptables -A INPUT -p tcp --dport 22 -j ACCEPT
```

- Allow traffic on specific port



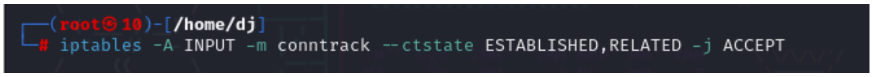
```
┌──(root㉿10)-[/home/dj]
└─# iptables -A INPUT -p tcp --dport 80 -j ACCEPT

┌──(root㉿10)-[/home/dj]
└─# iptables -A INPUT -p tcp --dport 443 -j ACCEPT
```

- Allow traffic from localhost



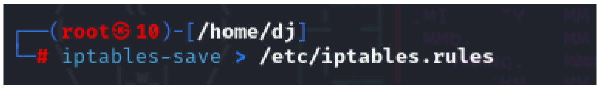
```
┌──(root㉿10)-[/home/dj]
└─# iptables -A INPUT -i lo -j ACCEPT
```

- Allow established connection



```
┌──(root㉿10)-[/home/dj]
└─# iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
```

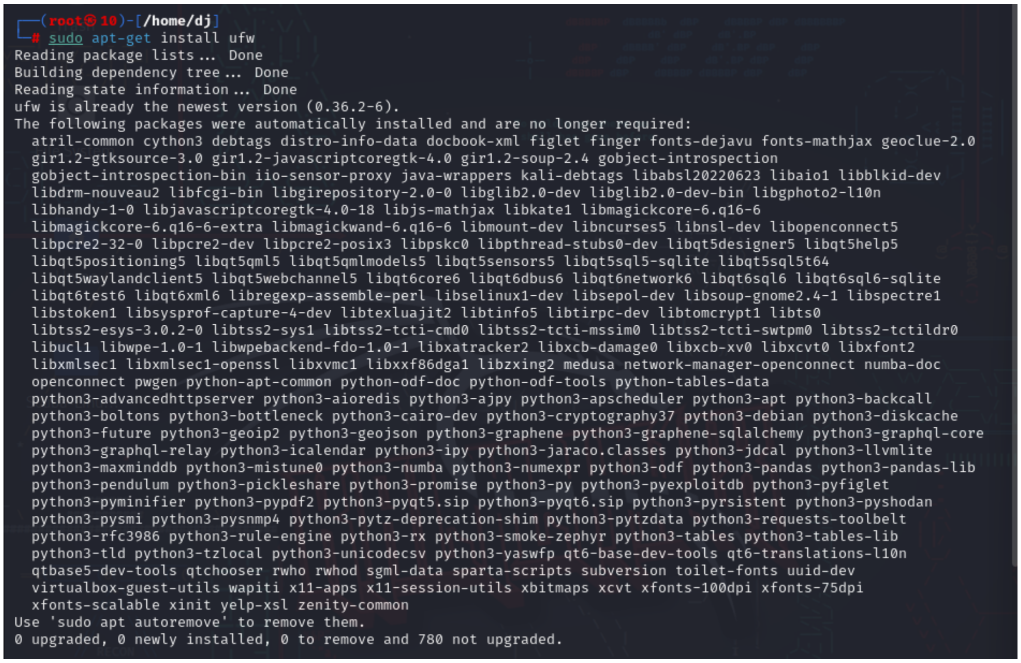
- Save the rules



```
┌──(root㉿10)-[/home/dj]
└─# iptables-save > /etc/iptables.rules
```

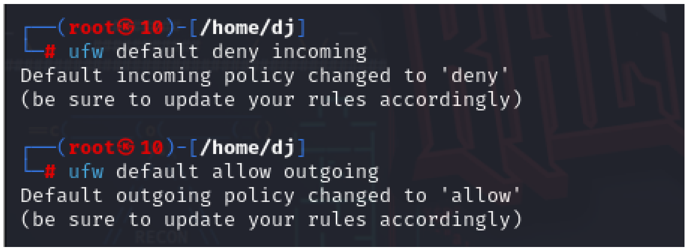
Configuring the Firewall with UFW

- Install UFW



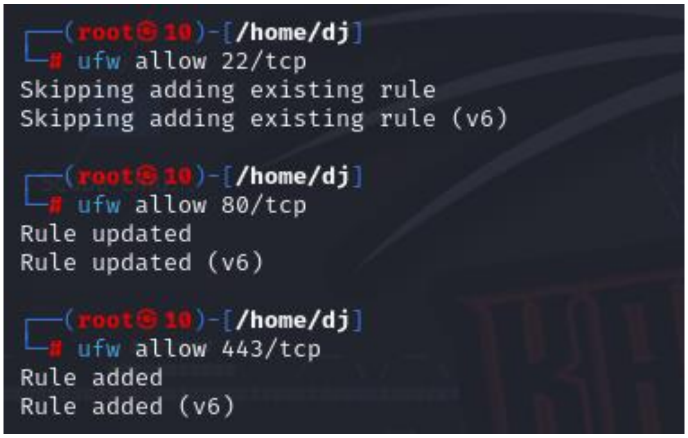
```
┌──(root㉿10)-[/home/dj]
└─# sudo apt-get install ufw
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
ufw is already the newest version (0.36.2-6).
The following packages were automatically installed and are no longer required:
  atril-common cython3 debtags distro-info-data docbook-xml figlet finger fonts-dejavu fonts-mathjax geoclue-2.0
  gir1.2-gtksource-3.0 gir1.2-javascriptcoregtk-4.0 gir1.2-soup-2.4 gobject-introspection
  gobject-introspection-bin iio-sensor-proxy java-wrappers kali-debtags libabsl20220623 libaio1 libblkid-dev
  libdrm-nouveau2 libfcgi-bin libgirepository-2.0-0 libglib2.0-dev libglib2.0-dev-bin libgphoto2-l10n
  libhandy-1-0 libjavascriptcoregtk-4.0-18 libjs-mathjax libkate1 libmagickcore-6.q16-6
  libmagickcore-6.q16-6-extra libmagickwand-6.q16-6 libmount-dev libncurses5 libnsl-dev libopenconnect5
  libpcre2-32-0 libpcre2-dev libpcre2-posix3 libpskc0 libpthread-stubs0-dev libqt5designer5 libqt5help5
  libqt5positioning5 libqt5qml5 libqt5qmlmodels5 libqt5sensors5 libqt5sql5-sqlite libqt5sql5t64
  libqt5waylandclient5 libqt5webchannel5 libqt6core6 libqt6dbus6 libqt6network6 libqt6sql6 libqt6sql6-sqlite
  libqt6test6 libqt6xml6 libregexp-assemble-perl libselinux1-dev libsepol-dev libsoup-gnome2.4-1 libspectre1
  libstoken1 libsysprof-capture-4-dev libtexluajit2 libtinfo5 libtirpc-dev libtomcrypt1 libts0
  libtss2-esys-3.0.2-0 libtss2-sys1 libtss2-tcti-cmd0 libtss2-tcti-mssim0 libtss2-tcti-swtpm0 libtss2-tctildr0
  libucl1 libwpe-1.0-1 libwpebackend-fdo-1.0-1 libxatracker2 libxcb-damage0 libxcb-xv0 libxcvt0 libxfont2
  libxmlsec1 libxmlsec1-openssl libxvmc1 libxxf86dga1 libzxing2 medusa network-manager-openconnect numba-doc
  openconnect pwgen python-apt-common python-odf-doc python-odf-tools python-tables-data
  python3-advancedhttpserver python3-aioredis python3-ajpy python3-apscheduler python3-apt python3-backcall
  python3-boltons python3-bottleneck python3-cairo-dev python3-cryptography37 python3-debian python3-diskcache
  python3-future python3-geoip2 python3-geojson python3-graphene python3-graphene-sqlalchemy python3-graphql-core
  python3-graphql-relay python3-icalendar python3-ipy python3-jaraco.classes python3-jdcal python3-llvmlite
  python3-maxminddb python3-mistune0 python3-numba python3-numexpr python3-odf python3-pandas python3-pandas-lib
  python3-pendulum python3-pickleshare python3-promise python3-py python3-pyexploitdb python3-pyfiglet
  python3-pyminifier python3-pypdf2 python3-pyqt5.sip python3-pyqt6.sip python3-pyrsistent python3-pyshodan
  python3-pysmi python3-pysnmp4 python3-pytz-deprecation-shim python3-pytzdata python3-requests-toolbelt
  python3-rfc3986 python3-rule-engine python3-rx python3-smoke-zephyr python3-tables python3-tables-lib
  python3-tld python3-tzlocal python3-unicodecsv python3-yaswfp qt6-base-dev-tools qt6-translations-l10n
  qtbase5-dev-tools qtchooser rwho rwhod sgml-data sparta-scripts subversion toilet-fonts uuid-dev
  virtualbox-guest-utils wapiti x11-apps x11-session-utils xbitmaps xcvt xfonts-100dpi xfonts-75dpi
  xfonts-scalable xinit yelp-xsl zenity-common
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 780 not upgraded.
```

- Set default policies



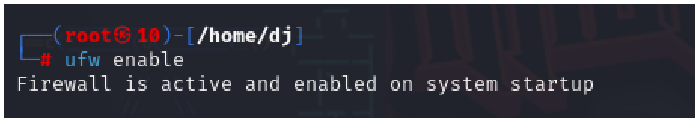
```
┌──(root㉿10)-[/home/dj]
└─# ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)

┌──(root㉿10)-[/home/dj]
└─# ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)
```

- Allow specific ports



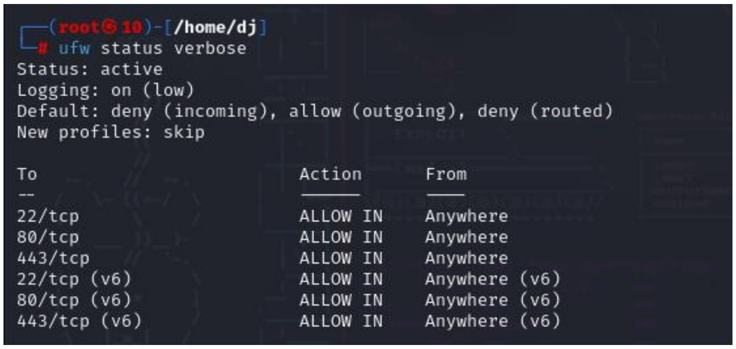
```
┌──(root㉿10)-[/home/dj]
└─# ufw allow 22/tcp
Skipping adding existing rule
Skipping adding existing rule (v6)

┌──(root㉿10)-[/home/dj]
└─# ufw allow 80/tcp
Rule updated
Rule updated (v6)

┌──(root㉿10)-[/home/dj]
└─# ufw allow 443/tcp
Rule added
Rule added (v6)
```

- Enable UFW



```
┌──(root㉿10)-[/home/dj]
└─# ufw enable
Firewall is active and enabled on system startup
```

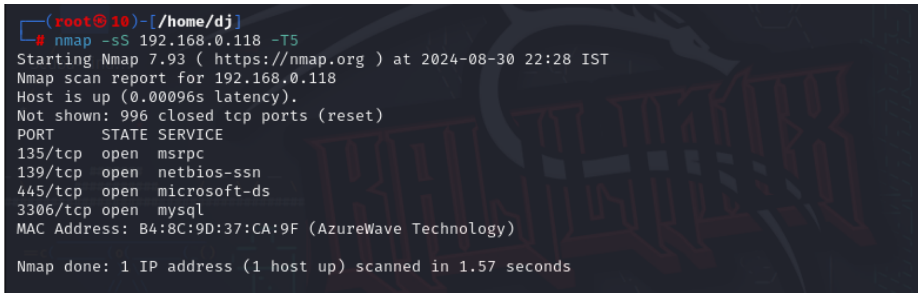
- Check UFW status



```
┌──(root㉿10)-[/home/dj]
└─# ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), deny (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW IN    Anywhere
80/tcp                     ALLOW IN    Anywhere
443/tcp                    ALLOW IN    Anywhere
22/tcp (v6)                ALLOW IN    Anywhere (v6)
80/tcp (v6)                ALLOW IN    Anywhere (v6)
443/tcp (v6)               ALLOW IN    Anywhere (v6)
```

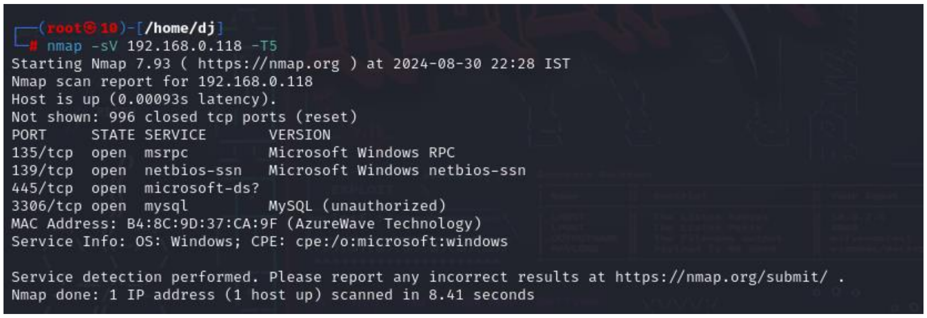
Vulnerability finding

- Basic host scan



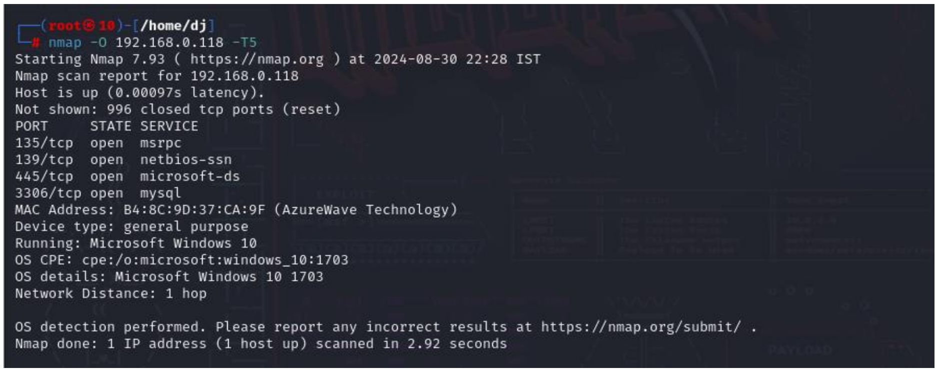
```
┌──(root㉿10)-[/home/dj]
└─# nmap -sS 192.168.0.118 -T5
Starting Nmap 7.93 ( https://nmap.org ) at 2024-08-30 22:28 IST
Nmap scan report for 192.168.0.118
Host is up (0.00096s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql
MAC Address: B4:8C:9D:37:CA:9F (AzureWave Technology)

Nmap done: 1 IP address (1 host up) scanned in 1.57 seconds
```

- Version detection



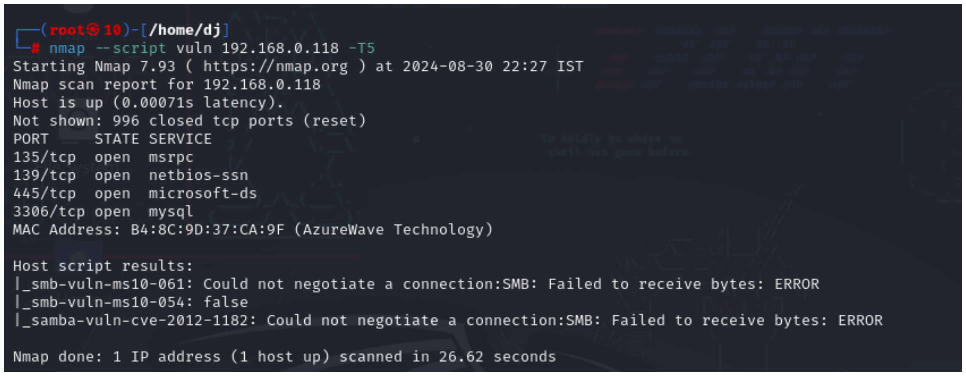
```
┌──(root㉿10)-[/home/dj]
└─# nmap -sV 192.168.0.118 -T5
Starting Nmap 7.93 ( https://nmap.org ) at 2024-08-30 22:28 IST
Nmap scan report for 192.168.0.118
Host is up (0.00093s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
3306/tcp open  mysql         MySQL (unauthorized)
MAC Address: B4:8C:9D:37:CA:9F (AzureWave Technology)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.41 seconds
```

- Operating system detection



```
┌──(root㉿10)-[/home/dj]
└─# nmap -O 192.168.0.118 -T5
Starting Nmap 7.93 ( https://nmap.org ) at 2024-08-30 22:28 IST
Nmap scan report for 192.168.0.118
Host is up (0.00097s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql
MAC Address: B4:8C:9D:37:CA:9F (AzureWave Technology)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10:1703
OS details: Microsoft Windows 10 1703
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.92 seconds
```

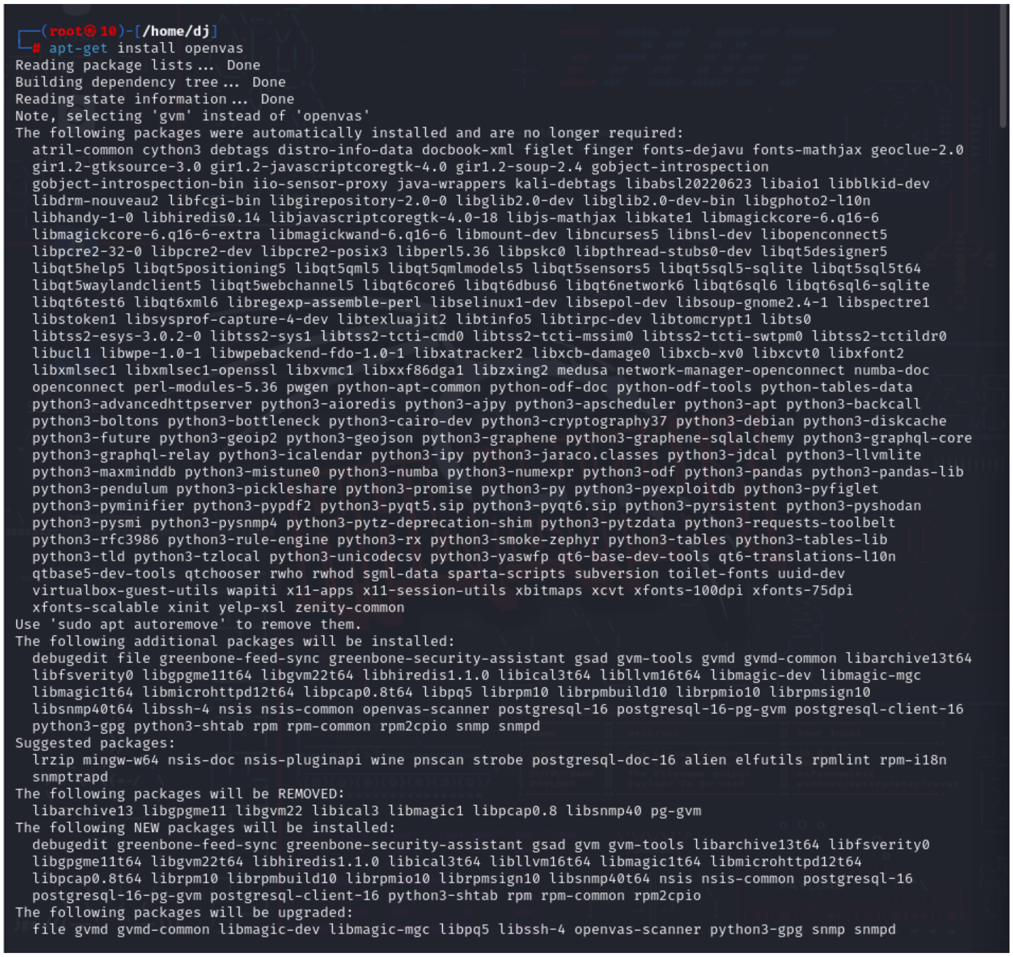
- Vulnerability script



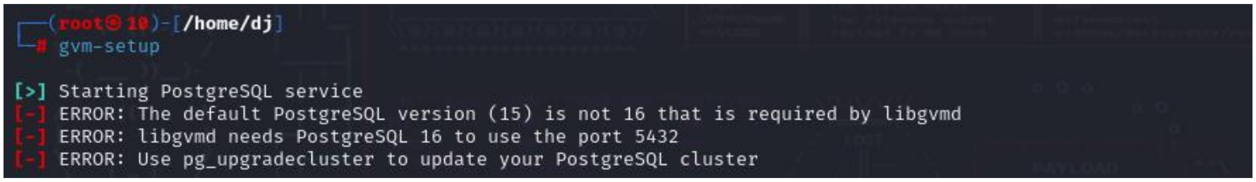
```
┌──(root㉿10)-[/home/dj]
└─# nmap --script vuln 192.168.0.118 -T5
Starting Nmap 7.93 ( https://nmap.org ) at 2024-08-30 22:27 IST
Nmap scan report for 192.168.0.118
Host is up (0.00071s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql
MAC Address: B4:8C:9D:37:CA:9F (AzureWave Technology)

Host script results:
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
|_smb-vuln-ms10-054: false
|_samba-vuln-cve-2012-1182: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR

Nmap done: 1 IP address (1 host up) scanned in 26.62 seconds
```

Vulnerability Scanning with OpenVAS

- Install and setup OpenVAS



```
┌──(root㉿10)-[/home/dj]
└─# apt-get install openvas
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
Note, selecting 'gvm' instead of 'openvas'
The following packages were automatically installed and are no longer required:
  atril-common cython3 debtags distro-info-data docbook-xml figlet finger fonts-dejavu fonts-mathjax geoclue-2.0
  gir1.2-gtksource-3.0 gir1.2-javascriptcoregtk-4.0 gir1.2-soup-2.4 gobject-introspection
  gobject-introspection-bin iio-sensor-proxy java-wrappers kali-debtags libabsl20220623 libaio1 libblkid-dev
  libdrm-nouveau2 libfcgi-bin libgirepository-2.0-0 libglib2.0-dev libglib2.0-dev-bin libgphoto2-l10n
  libhandy-1-0 libhiredis0.14 libjavascriptcoregtk-4.0-18 libjs-mathjax libkate1 libmagickcore-6.q16-6
  libmagickcore-6.q16-6-extra libmagickwand-6.q16-6 libmount-dev libncurses5 libnsl-dev libopenconnect5
  libpcre2-32-0 libpcre2-dev libpcre2-posix3 libperl5.36 libpskc0 libpthread-stubs0-dev libqt5designer5
  libqt5help5 libqt5positioning5 libqt5qml5 libqt5qmlmodels5 libqt5sensors5 libqt5sql5-sqlite libqt5sql5t64
  libqt5waylandclient5 libqt5webchannel5 libqt6core6 libqt6dbus6 libqt6network6 libqt6sql6 libqt6sql6-sqlite
  libqt6test6 libqt6xml6 libregexp-assemble-perl libselinux1-dev libsepol-dev libsoup-gnome2.4-1 libspectre1
  libstoken1 libsysprof-capture-4-dev libtexluajit2 libtinfo5 libtirpc-dev libtomcrypt1 libts0
  libtss2-esys-3.0.2-0 libtss2-sys1 libtss2-tcti-cmd0 libtss2-tcti-mssim0 libtss2-tcti-swtpm0 libtss2-tctildr0
  libucl1 libwpe-1.0-1 libwpebackend-fdo-1.0-1 libxatracker2 libxcb-damage0 libxcb-xv0 libxcvt0 libxfont2
  libxmlsec1 libxmlsec1-openssl libxvmc1 libxxf86dga1 libzxing2 medusa network-manager-openconnect numba-doc
  openconnect perl-modules-5.36 pwgen python-apt-common python-odf-doc python-odf-tools python-tables-data
  python3-advancedhttpserver python3-aioredis python3-ajpy python3-apscheduler python3-apt python3-backcall
  python3-boltons python3-bottleneck python3-cairo-dev python3-cryptography37 python3-debian python3-diskcache
  python3-future python3-geoip2 python3-geojson python3-graphene python3-graphene-sqlalchemy python3-graphql-core
  python3-graphql-relay python3-icalendar python3-ipy python3-jaraco.classes python3-jdcal python3-llvmlite
  python3-maxminddb python3-mistune0 python3-numba python3-numexpr python3-odf python3-pandas python3-pandas-lib
  python3-pendulum python3-pickleshare python3-promise python3-py python3-pyexploitdb python3-pyfiglet
  python3-pyminifier python3-pypdf2 python3-pyqt5.sip python3-pyqt6.sip python3-pyrsistent python3-pyshodan
  python3-pysmi python3-pysnmp4 python3-pytz-deprecation-shim python3-pytzdata python3-requests-toolbelt
  python3-rfc3986 python3-rule-engine python3-rx python3-smoke-zephyr python3-tables python3-tables-lib
  python3-tld python3-tzlocal python3-unicodecsv python3-yaswfp qt6-base-dev-tools qt6-translations-l10n
  qtbase5-dev-tools qtchooser rwho rwhod sgml-data sparta-scripts subversion toilet-fonts uuid-dev
  virtualbox-guest-utils wapiti x11-apps x11-session-utils xbitmaps xcvt xfonts-100dpi xfonts-75dpi
  xfonts-scalable xinit yelp-xsl zenity-common
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  debugedit file greenbone-feed-sync greenbone-security-assistant gsad gvm-tools gvmd gvmd-common libarchive13t64
  libfsverity0 libgpgme11t64 libgvm22t64 libhiredis1.1.0 libical3t64 libllvm16t64 libmagic-dev libmagic-mgc
  libmagic1t64 libmicrohttpd12t64 libpcap0.8t64 libpq5 librpm10 librpmbuild10 librpmio10 librpmsign10
  libsnmp40t64 libssh-4 nsis nsis-common openvas-scanner postgresql-16 postgresql-16-pg-gvm postgresql-client-16
  python3-gpg python3-shtab rpm rpm-common rpm2cpio snmp snmpd
Suggested packages:
  lrzip mingw-w64 nsis-doc nsis-pluginapi wine pnscan strobe postgresql-doc-16 alien elfutils rpmlint rpm-i18n
  snmptrapd
The following packages will be REMOVED:
  libarchive13 libgpgme11 libgvm22 libical3 libmagic1 libpcap0.8 libsnmp40 pg-gvm
The following NEW packages will be installed:
  debugedit greenbone-feed-sync greenbone-security-assistant gsad gvm gvm-tools libarchive13t64 libfsverity0
  libgpgme11t64 libgvm22t64 libhiredis1.1.0 libical3t64 libllvm16t64 libmagic1t64 libmicrohttpd12t64
  libpcap0.8t64 librpm10 librpmbuild10 librpmio10 librpmsign10 libsnmp40t64 nsis nsis-common postgresql-16
  postgresql-16-pg-gvm postgresql-client-16 python3-shtab rpm rpm-common rpm2cpio
The following packages will be upgraded:
  file gvmd gvmd-common libmagic-dev libmagic-mgc libpq5 libssh-4 openvas-scanner python3-gpg snmp snmpd
```



```
┌──(root㉿10)-[/home/dj]
└─# gvm-setup

[>] Starting PostgreSQL service
[-] ERROR: The default PostgreSQL version (15) is not 16 that is required by libgvmd
[-] ERROR: libgvmd needs PostgreSQL 16 to use the port 5432
[-] ERROR: Use pg_upgradecluster to update your PostgreSQL cluster
```