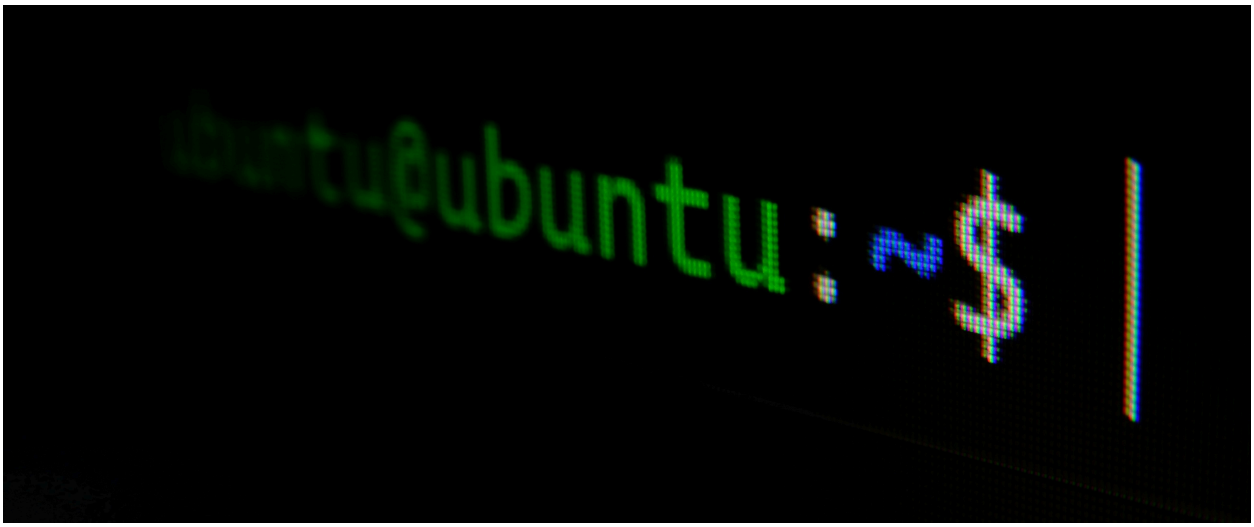


CHAPTER 4 - SOFTWARE

More often than not you would require installing software, utilities, dependencies to aid in your cybersecurity defensive architecture or investigating files, examining autopsy reports or memory dump scans etc. You would also find yourself as you move onwards on the journey the need and availability of ***Software Packages -*** group of files, a library of sorts that includes dependencies required to carry out a task or achieve an output. All the files and dependencies are included in the software package as separate files , often along a script, allowing software or dependency execution relatively simpler.

▼ [4.1] APT [Advanced Packaging Tool]

apt command or ***Advanced Packaging Tool*** is the default software manager in Debian-based Linux distros, such as Kali.

apt command's primary command is: '**apt-get',** it is used to download and or update/upgrade existing software or newer software packages.

To check whether the package required to install already exists on your system you could do so using:

```
apt-cache search keyword
```

example:

```
┌──(jynx㉿kali)-[~]
└─$ apt-cache search snort
fwsnort - Snort-to-iptables rule translator
golang-github-jasonish-go-idsrules-dev - Go IDS rule parser
libdaq-dev - Data Acquisition library for packet I/O - development files
libdaq2 - Data Acquisition library for packet I/O - shared library
libdaq3 - Data Acquisition library for packet I/O - shared library
libdaq3-dev - Data Acquisition library for packet I/O - development files
oinkmaster - Snort rules manager
psad - Port Scan Attack Detector
sagan-rules - Real-time System & Event Log Monitoring System [rules]
snort - flexible Network Intrusion Detection System
snort-common - flexible Network Intrusion Detection System - common files
snort-common-libraries - flexible Network Intrusion Detection System - libraries
snort-common-libraries-dbgsym - debug symbols for snort-common-libraries
snort-dbgsym - debug symbols for snort
snort-doc - flexible Network Intrusion Detection System - documentation
snort-rules-default - flexible Network Intrusion Detection System - ruleset
suricata - Next Generation Intrusion Detection and Prevention Tool

┌──(jynx㉿kali)-[~]
└─$
```

There are many results, because there are many dependencies with the word ‘snort’, try python3 and you would see a lot more than these.

INSTALLING a Software;

```
apt-get install packagename
```

example:

```
┌──(jynx㉿kali)-[~]
└─$ sudo apt-get install snort
[sudo] password for jynx:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
snort is already the newest version (3.1.82.0-0kali1+b1).
0 upgraded, 0 newly installed, 0 to remove and 307 not upgraded.

┌──(jynx㉿kali)-[~]
└─$
```

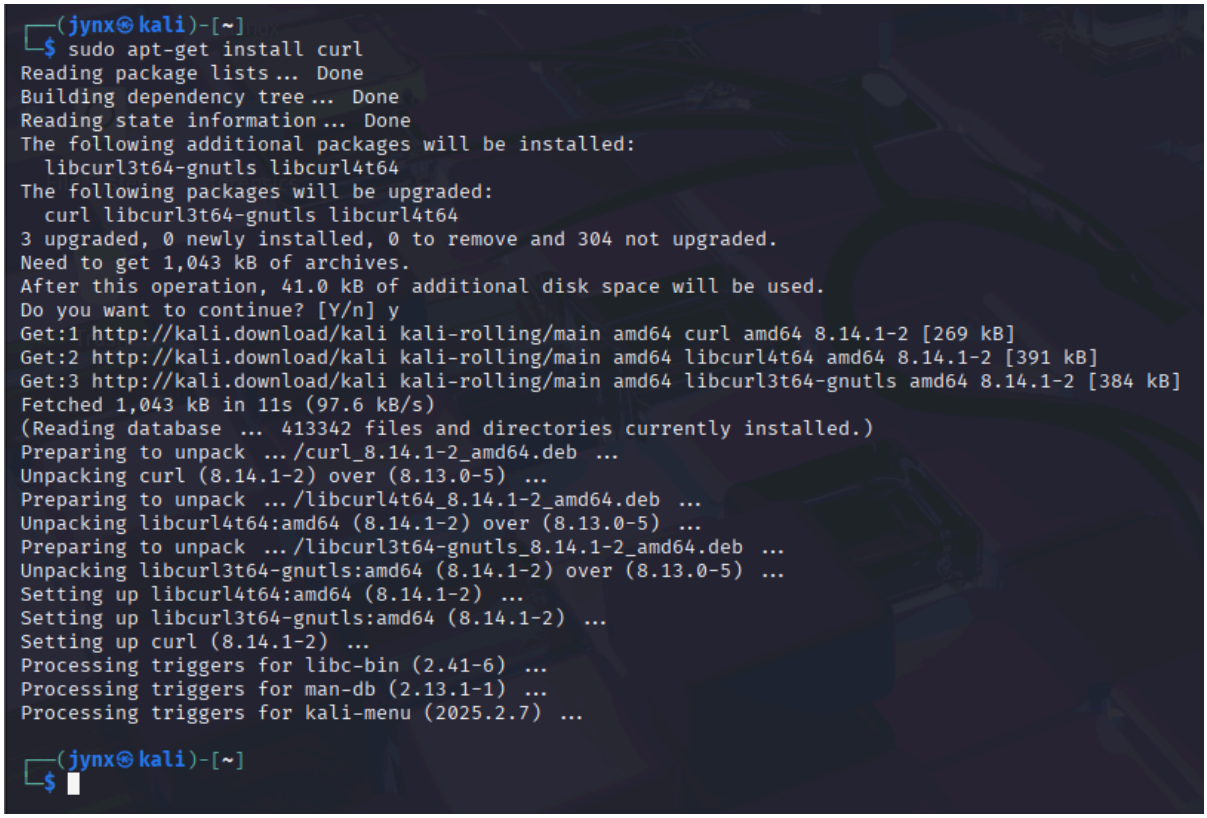
sudo - is used for root privileges since, my system doesn't allow installing packages for unauthorized users/groups.

I already had snort installed, thus in the last line it reads:

'0 upgraded, 0 newly installed, 0 to remove and 307 not upgraded.'

You would see different output, depending on the system it might also ask for whether you really want to install the package [Y/n]; answer with Y/y- as in YES and n/N- as in NO.

example:



REMOVING a Software [Uninstalling];

To remove a software just like with installing, using apt-get but now instead of *'install'* use *'remove'* option.

```
apt-get remove keyword
```

example:

```
┌──(jynx㉿kali)-[~]
└─$ sudo apt-get remove curl
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following packages were automatically installed and are no longer required:
  base58 binutils-mingw-w64-i686 binutils-mingw-w64-x86-64 debugedit dnsmap dsniff ettercap-common
  ettercap-graphical faraday-agent-dispatcher figlet finger gcc-mingw-w64-base gcc-mingw-w64-i686-win32
  gcc-mingw-w64-i686-win32-runtime gcc-mingw-w64-x86-64-win32 gcc-mingw-w64-x86-64-win32-runtime gir1.2-vte-2.91
  greenbone-feed-sync gvmd gvmd-common imagemagick imagemagick-7.q16 libaio1t64 libapache2-mod-php libblosc2-4
  libdlt2 libfsverity0 liblzf1 libmosquitto1 libnids1.21t64 librpmbuild10 librpmsign10 libtbb12 libtbbbind-2-5
  libtbbmalloc2 medusa mingw-w64-common mingw-w64-i686-dev mingw-w64-x86-64-dev mosquitto notus-scanner nsis
  nsis-common numba-doc openvas-scanner oracle-instantclient-basic ospd-openvas pgcli postgresql python-odf-doc
  python-odf-tools python-tables-data python3-alembic python3-amqp python3-apispec python3-apispec-webframeworks
  python3-autobahn python3-base58 python3-billiard python3-bleach python3-bottle python3-bottleneck python3-cbor
  python3-celery python3-cli-helpers python3-click-didyoumean python3-click-repl python3-cmd2 python3-configobj
  python3-cpuinfo python3-croniter python3-cvss python3-defusedxml python3-django python3-ecdsa
  python3-elastic-transport python3-elasticsearch python3-ephem python3-faraday-agent-parameters-types
  python3-faraday-plugins python3-feedparser python3-filedepot python3-filteralchemy python3-flask-celery-helper
  python3-flask-classful python3-flask-kvsession python3-flask-limiter python3-flask-login python3-flask-mail
  python3-flask-principal python3-flask-sqlalchemy python3-flaskext.wtf python3-flatbuffers python3-gevent
  python3-gevent-websocket python3-git python3-gitdb python3-gnupg python3-gvm python3-html2text python3-hupper
  python3-kombu python3-llvmlite python3-log-symbols python3-marshmallow python3-marshmallow-sqlalchemy
  python3-memcache python3-mnemonic python3-nplusone python3-numba python3-numexpr python3-odf python3-ordered-set
  python3-paho-mqtt python3-pandas python3-pandas-lib python3-pefile python3-pgspecial python3-plaster
  python3-plaster-pastedeploy python3-png python3-psycogreen python3-psycopg python3-psycopg-c python3-py-sneakers
  python3-pyexploitdb python3-pyfiglet python3-pyotp python3-pyqrcode python3-pyramid python3-pyshodan
  python3-qasync python3-qrcode python3-serial-asyncio python3-sgmllib3k python3-sh python3-shtab
  python3-simple-rest-client python3-simplekv python3-slugify python3-smmap python3-snappy python3-spinners
  python3-sqlalchemy-schemadisplay python3-sqlparse python3-standard-imghdr python3-status
```

Yet again, you would be asked for whether you really want to un-install the package [Y/n]; answer with Y/y- as in YES and n/N- as in NO [Same way we did as for installation].

The *'remove'* command will not and does not remove the configuration files by default, essentially allowing you to install the package again without having to reinstall all the configuration files again, to remove the configuration files as well, you can use the *'purge'* option with **apt-get** command.

```
apt-get purge keyword
```

example:

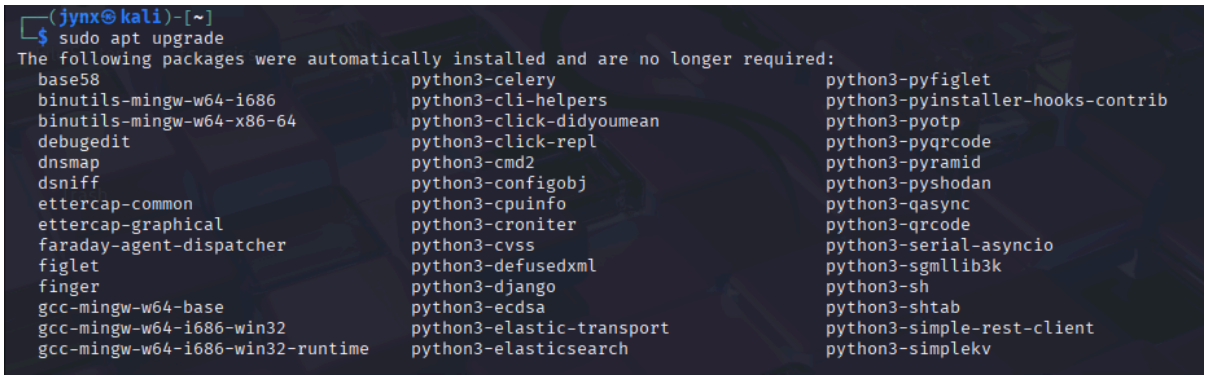
```
┌──(jynx㉿kali)-[~]
└─$ sudo apt-get purge curl
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following packages were automatically installed and are no longer required:
  base58 binutils-mingw-w64-i686 binutils-mingw-w64-x86-64 debugedit dnsmap dsniff ettercap-common
  ettercap-graphical faraday-agent-dispatcher figlet finger gcc-mingw-w64-base gcc-mingw-w64-i686-win32
  gcc-mingw-w64-i686-win32-runtime gcc-mingw-w64-x86-64-win32 gcc-mingw-w64-x86-64-win32-runtime gir1.2-vte-2.91
  greenbone-feed-sync gvmd gvmd-common imagemagick imagemagick-7.q16 libaio1t64 libapache2-mod-php libblosc2-4
  libdlt2 libfsverity0 liblzf1 libmosquitto1 libnids1.21t64 librpmbuild10 librpmsign10 libtbb12 libtbbbind-2-5
  libtbbmalloc2 medusa mingw-w64-common mingw-w64-i686-dev mingw-w64-x86-64-dev mosquitto notus-scanner nsis
  nsis-common numba-doc openvas-scanner oracle-instantclient-basic ospd-openvas pgcli postgresql python-odf-doc
  python-odf-tools python-tables-data python3-alembic python3-amqp python3-apispec python3-apispec-webframeworks
  python3-autobahn python3-base58 python3-billiard python3-bleach python3-bottle python3-bottleneck python3-cbor
  python3-celery python3-cli-helpers python3-click-didyoumean python3-click-repl python3-cmd2 python3-configobj
  python3-cpuinfo python3-croniter python3-cvss python3-defusedxml python3-django python3-ecdsa
```

▼ [4.2] Upgrading Dependencies

To upgrade existing packages or installations on your system, use '**apt**' command with *'upgrade'* option.

```
sudo apt upgrade
```

example:



→ It upgrades/updates all the packages, software and dependencies on your Kali system.

Other options to try [UPDATES/UPGRADES]:

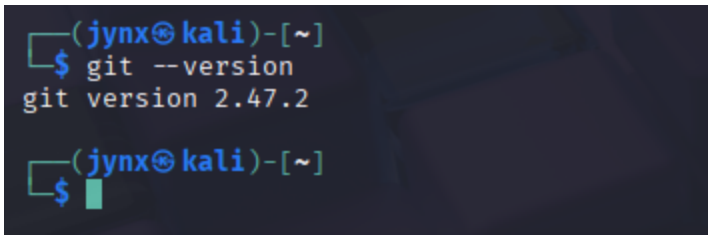
```
# Update package lists
sudo apt update

# Upgrade all installed packages
sudo apt upgrade

# For a more comprehensive upgrade (handles dependencies better)
sudo apt full-upgrade

# Clean up unnecessary packages
sudo apt autoremove
sudo apt autoclean
```

▼ [4.3] Using GitHub (GIT)

Sometimes software that aren't yet community recognized or cater to niche creators/subjects would not be available on the open-source repositories in such a case, it might be available on GitHub, once you find your relevant GitHub repository for the particular package or dependency, clone it to your local Kali system using:
1. Check if you have installed git:

```
git --version
```

example:



If not, follow the instructions below:

```
# Install git
sudo apt update
sudo apt install git

# Clone the repository
git clone https://github.com/username/repository-name.git

# Navigate to the cloned directory
cd repository-name



#OPTIONAL:
# Check for installation instructions
cat README.md
cat INSTALL.md
```

```
# Common installation methods:
# For Python projects:
pip install -r requirements.txt
python setup.py install

# For projects with Makefile:
make
sudo make install

# For projects with install script:
chmod +x install.sh
./install.sh
```