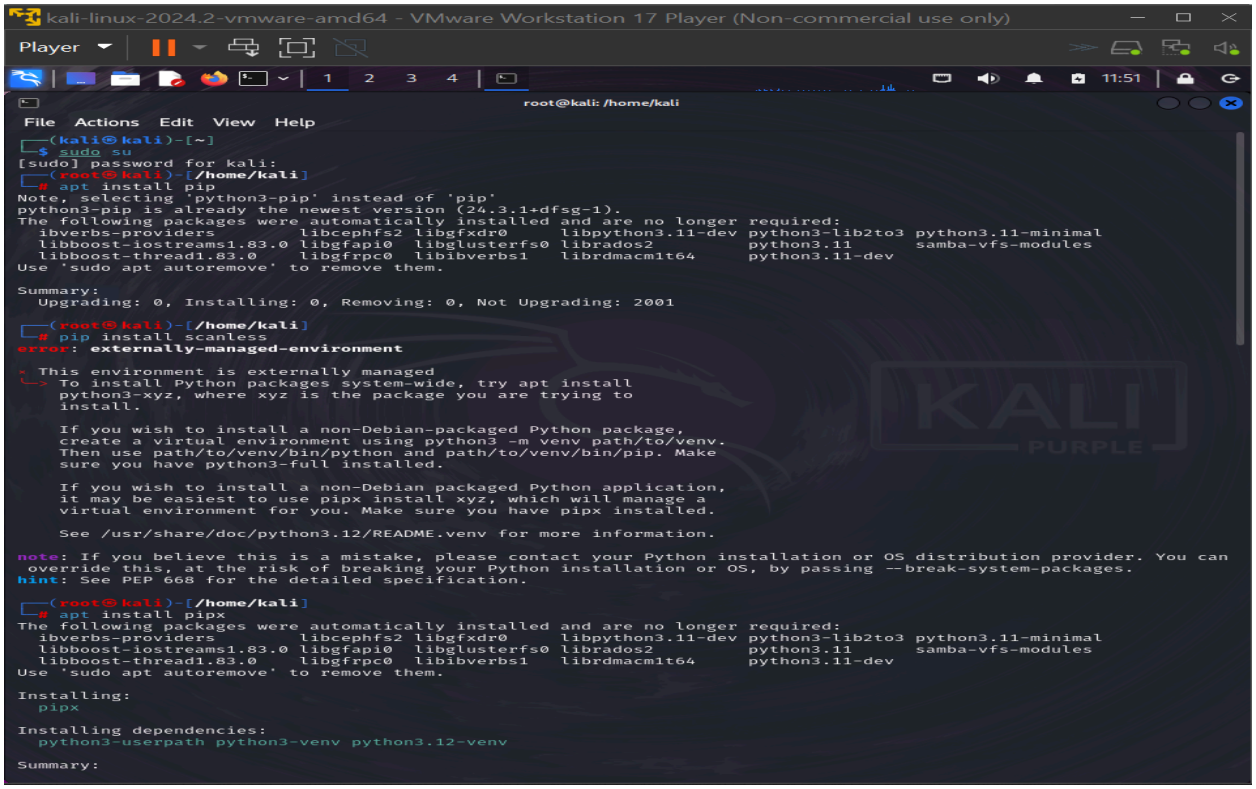
SCANLESS FOR EASY ANONYMOUS PORT SCANNING

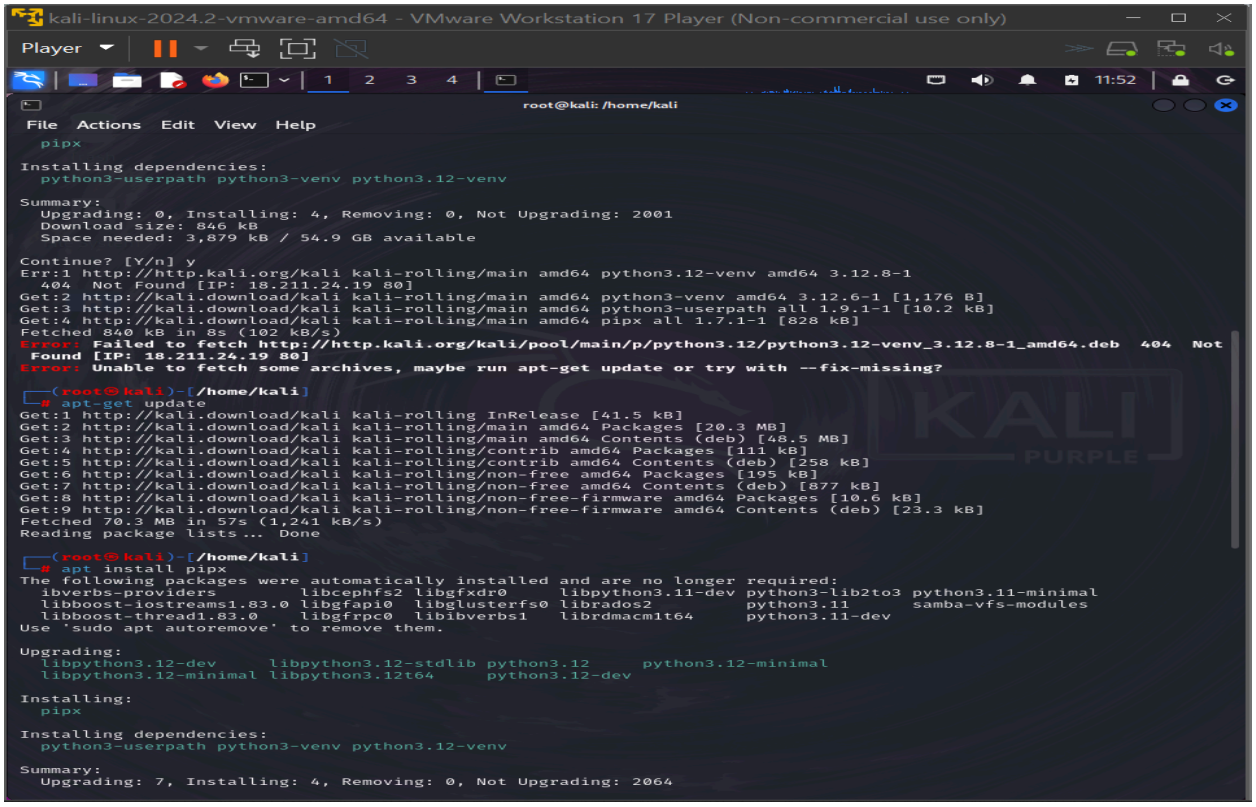
Tools: KALI LINUX
Site : Scanme.org

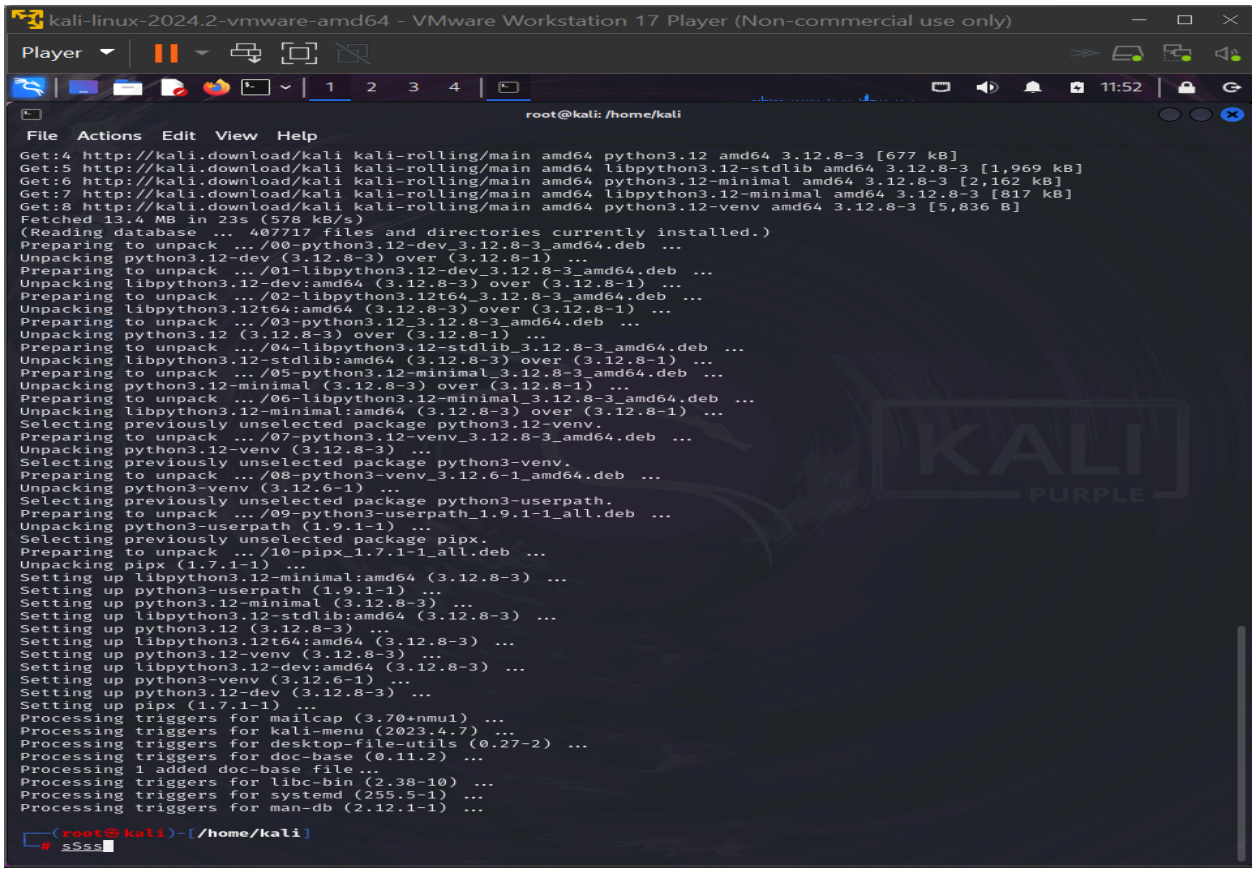
Scanless is a script which makes use of online scanners to allow you to scan a target anonymously. It provides a number of scanners which you can use to scan your target. The different scanners will prioritise different ports, making it worthwhile to run a number of scans using the different tools.

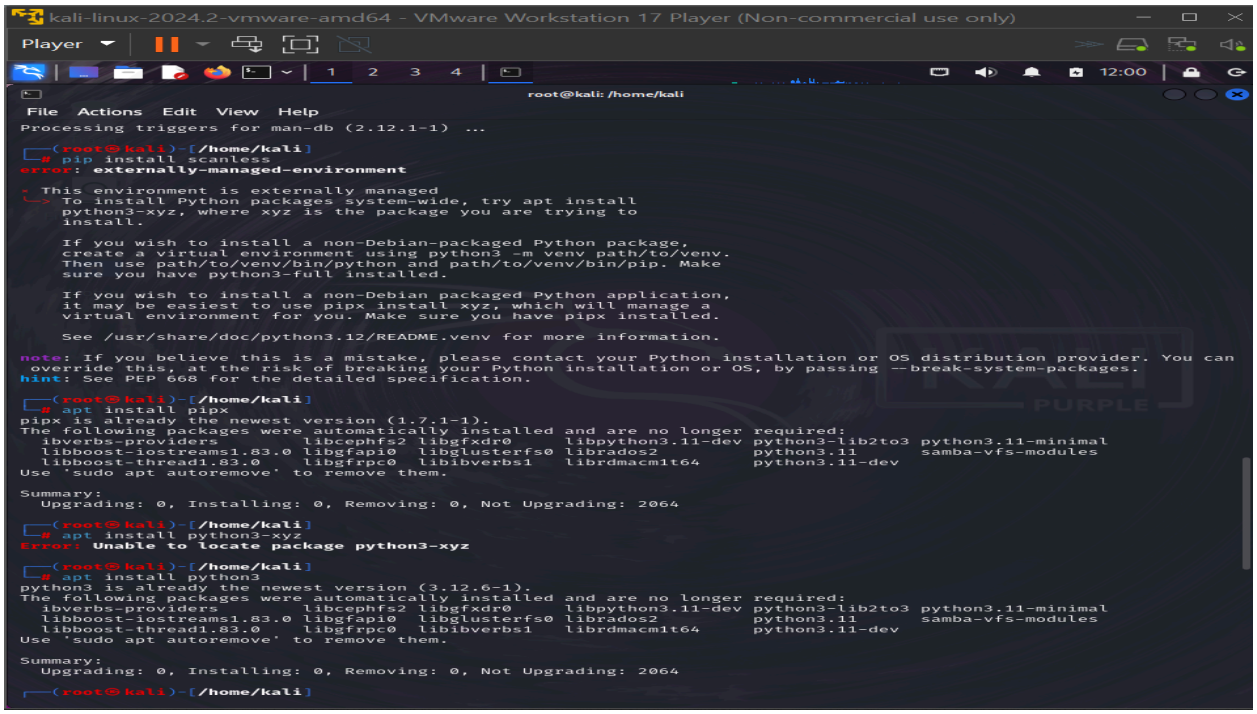
We will need a tool called pip to download this tool. You may already have it installed, but if not, use the following command to install it: sudo su –

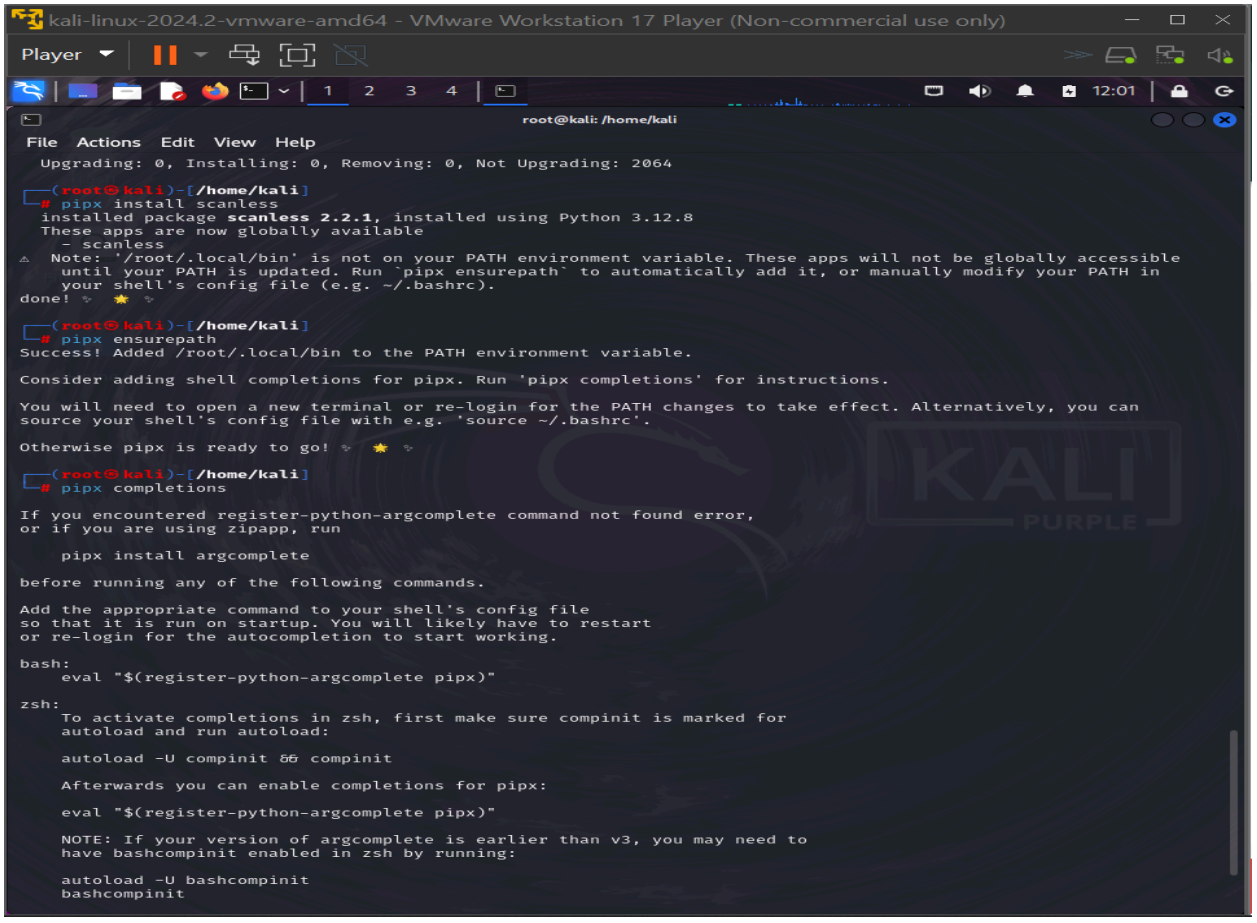
Input from the task :




kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
11:52
root@kali: /home/kali
File Actions Edit View Help
pipx
Installing dependencies:
python3-userpath python3-venv python3.12-venv
Summary:
Upgrading: 0, Installing: 4, Removing: 0, Not Upgrading: 2001
Download size: 846 kB
Space needed: 3,879 kB / 54.9 GB available
Continue? [Y/n] y
Err:1 http://http.kali.org/kali kali-rolling/main amd64 python3.12-venv amd64 3.12.8-1
404 Not Found [IP: 18.211.24.19 80]
Get:2 http://kali.download/kali kali-rolling/main amd64 python3-venv amd64 3.12.6-1 [1,176 B]
Get:3 http://kali.download/kali kali-rolling/main amd64 python3-userpath all 1.9.1-1 [10.2 kB]
Get:4 http://kali.download/kali kali-rolling/main amd64 pipx all 1.7.1-1 [828 kB]
Fetched 840 kB in 8s (102 kB/s)
Error: Failed to fetch http://http.kali.org/kali/pool/main/p/python3.12/python3.12-venv_3.12.8-1_amd64.deb 404 Not Found [IP: 18.211.24.19 80]
Error: Unable to fetch some archives, maybe run apt-get update or try with --fix-missing?
┌──(root㉿kali)-[/home/kali]
└─# apt-get update
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [20.3 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [48.5 MB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [111 kB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [258 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [195 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [877 kB]
Get:8 http://kali.download/kali kali-rolling/non-free-firmware amd64 Packages [10.6 kB]
Get:9 http://kali.download/kali kali-rolling/non-free-firmware amd64 Contents (deb) [23.3 kB]
Fetched 70.3 MB in 57s (1,241 kB/s)
Reading package lists... Done
┌──(root㉿kali)-[/home/kali]
└─# apt install pipx
The following packages were automatically installed and are no longer required:
ibverbs-providers libcephfs2 libgfxdr0 libpython3.11-dev python3-lib2to3 python3.11-minimal
libboost-iostreams1.83.0 libgfapi0 libglusterfs0 librados2 python3.11 samba-vfs-modules
libboost-thread1.83.0 libgfrpc0 libibverbs1 librdmacm1t64 python3.11-dev
Use 'sudo apt autoremove' to remove them.
Upgrading:
libpython3.12-dev libpython3.12-stdlib python3.12 python3.12-minimal
libpython3.12-minimal libpython3.12t64 python3.12-dev
Installing:
pipx
Installing dependencies:
python3-userpath python3-venv python3.12-venv
Summary:
Upgrading: 7, Installing: 4, Removing: 0, Not Upgrading: 2064


kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
11:52
root@kali: /home/kali
File Actions Edit View Help
Get:4 http://kali.download/kali kali-rolling/main amd64 python3.12 amd64 3.12.8-3 [677 kB]
Get:5 http://kali.download/kali kali-rolling/main amd64 libpython3.12-stdlib amd64 3.12.8-3 [1,969 kB]
Get:6 http://kali.download/kali kali-rolling/main amd64 python3.12-minimal amd64 3.12.8-3 [2,162 kB]
Get:7 http://kali.download/kali kali-rolling/main amd64 libpython3.12-minimal amd64 3.12.8-3 [817 kB]
Get:8 http://kali.download/kali kali-rolling/main amd64 python3.12-venv amd64 3.12.8-3 [5,836 B]
Fetched 13.4 MB in 23s (578 kB/s)
(Reading database ... 407717 files and directories currently installed.)
Preparing to unpack .../00-python3.12-dev_3.12.8-3_amd64.deb ...
Unpacking python3.12-dev (3.12.8-3) over (3.12.8-1) ...
Preparing to unpack .../01-libpython3.12-dev_3.12.8-3_amd64.deb ...
Unpacking libpython3.12-dev:amd64 (3.12.8-3) over (3.12.8-1) ...
Preparing to unpack .../02-libpython3.12t64_3.12.8-3_amd64.deb ...
Unpacking libpython3.12t64:amd64 (3.12.8-3) over (3.12.8-1) ...
Preparing to unpack .../03-python3.12_3.12.8-3_amd64.deb ...
Unpacking python3.12 (3.12.8-3) over (3.12.8-1) ...
Preparing to unpack .../04-libpython3.12-stdlib_3.12.8-3_amd64.deb ...
Unpacking libpython3.12-stdlib:amd64 (3.12.8-3) over (3.12.8-1) ...
Preparing to unpack .../05-python3.12-minimal_3.12.8-3_amd64.deb ...
Unpacking python3.12-minimal (3.12.8-3) over (3.12.8-1) ...
Preparing to unpack .../06-libpython3.12-minimal_3.12.8-3_amd64.deb ...
Unpacking libpython3.12-minimal:amd64 (3.12.8-3) over (3.12.8-1) ...
Selecting previously unselected package python3.12-venv.
Preparing to unpack .../07-python3.12-venv_3.12.8-3_amd64.deb ...
Unpacking python3.12-venv (3.12.8-3) ...
Selecting previously unselected package python3-venv.
Preparing to unpack .../08-python3-venv_3.12.6-1_amd64.deb ...
Unpacking python3-venv (3.12.6-1) ...
Selecting previously unselected package python3-userpath.
Preparing to unpack .../09-python3-userpath_1.9.1-1_all.deb ...
Unpacking python3-userpath (1.9.1-1) ...
Selecting previously unselected package pipx.
Preparing to unpack .../10-pipx_1.7.1-1_all.deb ...
Unpacking pipx (1.7.1-1) ...
Setting up libpython3.12-minimal:amd64 (3.12.8-3) ...
Setting up python3-userpath (1.9.1-1) ...
Setting up python3.12-minimal (3.12.8-3) ...
Setting up libpython3.12-stdlib:amd64 (3.12.8-3) ...
Setting up python3.12 (3.12.8-3) ...
Setting up libpython3.12t64:amd64 (3.12.8-3) ...
Setting up python3.12-venv (3.12.8-3) ...
Setting up libpython3.12-dev:amd64 (3.12.8-3) ...
Setting up python3-venv (3.12.6-1) ...
Setting up python3.12-dev (3.12.8-3) ...
Setting up pipx (1.7.1-1) ...
Processing triggers for mailcap (3.70+nmu1) ...
Processing triggers for kali-menu (2023.4.7) ...
Processing triggers for desktop-file-utils (0.27-2) ...
Processing triggers for doc-base (0.11.2) ...
Processing 1 added doc-base file...
Processing triggers for libc-bin (2.38-10) ...
Processing triggers for systemd (255.5-1) ...
Processing triggers for man-db (2.12.1-1) ...
┌──(root㉿kali)-[/home/kali]
└─# sSss


kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
12:00
root@kali: /home/kali
File Actions Edit View Help
Processing triggers for man-db (2.12.1-1) ...
┌──(root㉿kali)-[/home/kali]
└─# pip install scanless
error: externally-managed-environment
× This environment is externally managed
╰─> To install Python packages system-wide, try apt install
python3-xyz, where xyz is the package you are trying to
install.
If you wish to install a non-Debian-packaged Python package,
create a virtual environment using python3 -m venv path/to/venv.
Then use path/to/venv/bin/python and path/to/venv/bin/pip. Make
sure you have python3-full installed.
If you wish to install a non-Debian packaged Python application,
it may be easiest to use pipx install xyz, which will manage a
virtual environment for you. Make sure you have pipx installed.
See /usr/share/doc/python3.12/README.venv for more information.
note: If you believe this is a mistake, please contact your Python installation or OS distribution provider. You can
override this, at the risk of breaking your Python installation or OS, by passing --break-system-packages.
hint: See PEP 668 for the detailed specification.
┌──(root㉿kali)-[/home/kali]
└─# apt install pipx
pipx is already the newest version (1.7.1-1).
The following packages were automatically installed and are no longer required:
libverbs-providers libcephfs2 libgfxdr0 libpython3.11-dev python3-lib2to3 python3.11-minimal
libboost-iostreams1.83.0 libgfapi0 libglusterfs0 libradosd2 python3.11 samba-vfs-modules
libboost-thread1.83.0 libgfrpc0 libibverbs1 librdmacm1t64 python3.11-dev
Use 'sudo apt autoremove' to remove them.
Summary:
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 2064
┌──(root㉿kali)-[/home/kali]
└─# apt install python3-xyz
Error: Unable to locate package python3-xyz
┌──(root㉿kali)-[/home/kali]
└─# apt install python3
python3 is already the newest version (3.12.6-1).
The following packages were automatically installed and are no longer required:
libverbs-providers libcephfs2 libgfxdr0 libpython3.11-dev python3-lib2to3 python3.11-minimal
libboost-iostreams1.83.0 libgfapi0 libglusterfs0 libradosd2 python3.11 samba-vfs-modules
libboost-thread1.83.0 libgfrpc0 libibverbs1 librdmacm1t64 python3.11-dev
Use 'sudo apt autoremove' to remove them.
Summary:
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 2064
┌──(root㉿kali)-[/home/kali]


kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
12:01
root@kali: /home/kali
File Actions Edit View Help
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 2064
┌──(root㉿kali)-[/home/kali]
└─# pipx install scanless
installed package scanless 2.2.1, installed using Python 3.12.8
These apps are now globally available
- scanless
⚠ Note: '/root/.local/bin' is not on your PATH environment variable. These apps will not be globally accessible
until your PATH is updated. Run `pipx ensurepath` to automatically add it, or manually modify your PATH in
your shell's config file (e.g. ~/.bashrc).
done!
┌──(root㉿kali)-[/home/kali]
└─# pipx ensurepath
Success! Added /root/.local/bin to the PATH environment variable.
Consider adding shell completions for pipx. Run 'pipx completions' for instructions.
You will need to open a new terminal or re-login for the PATH changes to take effect. Alternatively, you can
source your shell's config file with e.g. 'source ~/.bashrc'.
Otherwise pipx is ready to go!
┌──(root㉿kali)-[/home/kali]
└─# pipx completions
If you encountered register-python-argcomplete command not found error,
or if you are using zipapp, run
pipx install argcomplete
before running any of the following commands.
Add the appropriate command to your shell's config file
so that it is run on startup. You will likely have to restart
or re-login for the autocompletion to start working.
bash:
eval "$(register-python-argcomplete pipx)"
zsh:
To activate completions in zsh, first make sure compinit is marked for
autoload and run autoload:
autoload -U compinit && compinit
Afterwards you can enable completions for pipx:
eval "$(register-python-argcomplete pipx)"
NOTE: If your version of argcomplete is earlier than v3, you may need to
have bashcompinit enabled in zsh by running:
autoload -U bashcompinit
bashcompinit


```
┌──(root㉿kali)-[/home/kali]
└─# scanless -t scanme.nmap.org -s ipfingerprints
Running scanless v2.2.1 ...

ipfingerprints:
Host is up (0.15s latency).
Not shown: 484 closed ports
PORT    STATE    SERVICE
22/tcp  open     ssh
80/tcp  filtered http
111/tcp filtered rpcbind
135/tcp filtered msrpc
136/tcp filtered profile
137/tcp filtered netbios-ns
138/tcp filtered netbios-dgm
139/tcp filtered netbios-ssn
445/tcp filtered microsoft-ds
Aggressive OS guesses: Linux 2.6.32 - 3.13 (96%), Linux 2.6.22 - 2.6.36 (94%), Linux 3.10
(94%), Linux 3.10 - 4.2 (94%), Linux 2.6.32 (94%), Linux 3.2 - 4.6 (94%), Linux 2.6.32 - 3.10
(93%), HP P2000 G3 NAS device (93%), Linux 2.6.18 (93%), Linux 3.16 - 4.6 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 15 hops

┌──(root㉿kali)-[/home/kali]
└─# scanless -t jumia.com -s ipfingerprints
Running scanless v2.2.1 ...

ipfingerprints:
Host is up (0.0071s latency).
Not shown: 491 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
Aggressive OS guesses: Crestron XPanel control system (91%), ASUS RT-N56U WAP (Linux 3.4)
(89%), Linux 3.1 (89%), Linux 3.16 (89%), Linux 3.2 (89%), AXIS 210A or 211 Network Camera
(Linux 2.6.17) (88%), HP P2000 G3 NAS device (88%), Android 4.1 - 6.0 (Linux 3.4 or 3.10)
(87%), Android 5.0 - 5.1 (87%), Android 5.0 - 6.0 (Linux 3.10) (87%)
No exact OS matches for host (test conditions non-ideal).

┌──(root㉿kali)-[/home/kali]
└─#
```

Here we will be using a tool called scanless to anonymously scan ports.

To use Scanless anonymously for port scanning, you'll need to install a few tools and follow these steps:

Install pip: First, ensure that `pip` is installed. If it's not, use the following commands:

```
sudo su -
```

```
apt-get update
```

```
apt install pip
```

If `pip` is not available, you can try installing `pipx`:

```
apt install pipx
```

Install Scanless: Once `pipx` is installed, use it to install Scanless:

```
pipx install scanless
```

Ensure Environment Setup: After installation, run the following commands to ensure that everything is set up correctly:

```
pipx ensurepath
```

```
pipx completions
```

Restart Terminal: Close the terminal completely and open a new one. Enter root permissions if necessary.

Check Scanless Help: To see the available options for Scanless, run:

```
scanless -h
```

List Available Scanners: To view the types of scans that Scanless can perform, run:

```
scanless -l
```

Run a Scan: Once you know which scanner you want to use, you can scan a target by using the following command format:

```
scanless -t [Target IP or Hostname] -s [Scanner Name]
```

This will allow you to conduct anonymous port scans using Scanless.