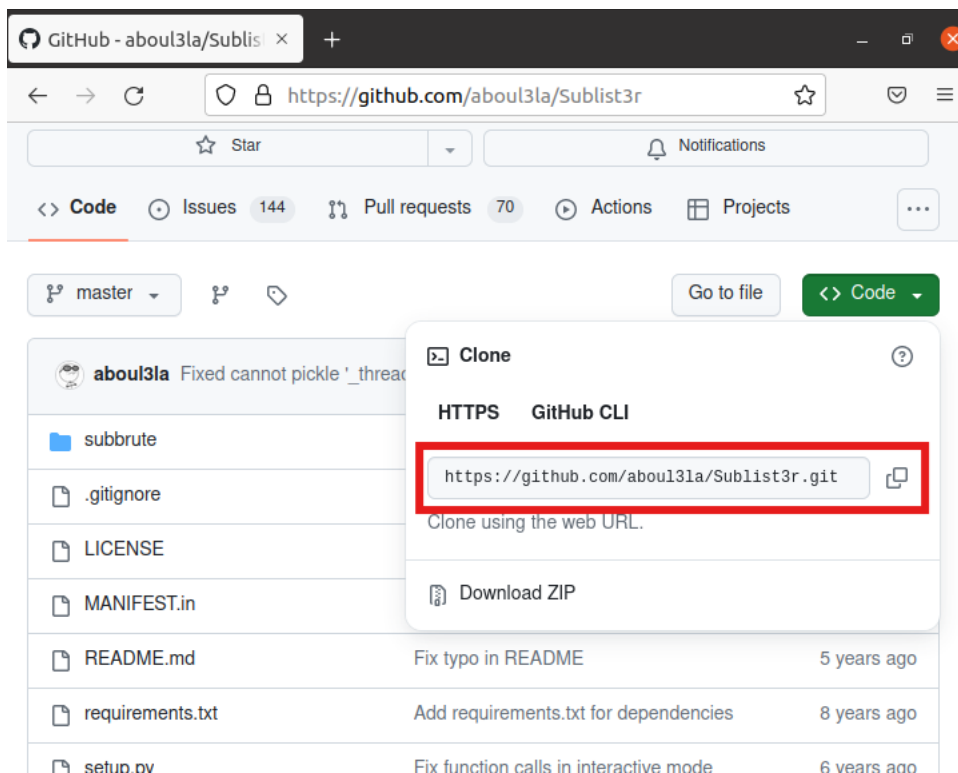


Sublist3r

Sublister is a tool designed in python and uses OSINT in order to enumerate subdomains of websites. It helps pen-testers in collecting and gathering subdomains for a domain which is their target. In order to fetch the accurate results, sublilster uses many search engines like Google, Yahoo, etc. and even tools like Netcraft, Virustotal, etc.

Steps to Install and run the Sublist3r:-

1. Firstly, in order to clone the sublistr3 tool go to its official github page.



2. Now use git clone command to your desired directory in order to clone the tool.

```
(root@kali)-[/home/kali/Sublist3r]
# git clone https://github.com/about3la/Sublist3r.git
Cloning into 'Sublist3r' ...
remote: Enumerating objects: 383, done.
remote: Total 383 (delta 0), reused 0 (delta 0), pack-reused 383
Receiving objects: 100% (383/383), 1.12 MiB | 324.00 KiB/s, done.
Resolving deltas: 100% (213/213), done.

(root@kali)-[/home/kali/Sublist3r]
#
```

3. After that go to Sublist3r directory where you have clone it.

```
(root@kali)-[/home/kali]
# ls
Desktop  Documents  Downloads  Music  Pictures  Public  Sublist3r  Templates  Videos

(root@kali)-[/home/kali]
# cd Sublist3r

(root@kali)-[/home/kali/Sublist3r]
#
```

4. Now we have to install the requirements to do so use pip command as show below.

```
(root@kali)-[/home/kali/Sublist3r]
# pip install -r requirements.txt
Collecting argparse (from -r requirements.txt (line 1))
  Using cached argparse-1.4.0-py2.py3-none-any.whl.metadata (2.8 kB)
Requirement already satisfied: dnspython in /usr/lib/python3/dist-packages (from -r requirements.txt (line 2))
Requirement already satisfied: requests in /usr/lib/python3/dist-packages (from -r requirements.txt (line 3))
Using cached argparse-1.4.0-py2.py3-none-any.whl (23 kB)
Installing collected packages: argparse
Successfully installed argparse-1.4.0
WARNING: Running pip as the 'root' user can result in broken permissions and conflicting behaviour with the sys
https://pip.pypa.io/warnings/venv
```

5. Now we must install the requests using pip command.

```
(root@kali)-[/home/kali/Sublist3r]
# sudo pip install requests
Requirement already satisfied: requests in /usr/lib/python3/dist-packages (2.31.0)
WARNING: Running pip as the 'root' user can result in broken permissions and conflicting behaviour with the system package manager. It is recommended to use a virtual environment instead: https://pip.pypa.io/warnings/venv
```

6. Now we have to install the dnspython using pip command.

```
(root@kali)-[/home/kali/Sublist3r]
# sudo pip install dnspython
Requirement already satisfied: dnspython in /usr/lib/python3/dist-packages (2.4.2)
WARNING: Running pip as the 'root' user can result in broken permissions and conflicting behaviour with the system package manager. It is recommended to use a virtual environment instead: https://pip.pypa.io/warnings/venv
```

7. After that install argparse using pip.

```
(root@kali)-[/home/kali/Sublist3r]
# sudo pip install argparse
Collecting argparse
  Using cached argparse-1.4.0-py2.py3-none-any.whl.metadata (2.8 kB)
Using cached argparse-1.4.0-py2.py3-none-any.whl (23 kB)
Installing collected packages: argparse
Successfully installed argparse-1.4.0
WARNING: Running pip as the 'root' user can result in broken permissions and conflicting behaviour with the system package manager. It is recommended to use a virtual environment instead: https://pip.pypa.io/warnings/venv
```

8. To run the tool use ./sublist3r.py.

```
(root@kali)-[/home/kali/Sublist3r]
# ./sublist3r.py

What are Folding Lists in Scala?
How to define a list item in HTML?
How to find SubString in Python?

# Coded By Ahmed Aboul-Ela - @aboul3la

Usage: python3 ./sublist3r.py [Options] use -h for help
Error: the following arguments are required: -d/--domain
```

9. Now we can use it. I have use -d flag to find out the sub domains.

```
(root@kali)-[/home/kali/Sublist3r]
# python sublist3r.py -d reddit.com

Share Your Experience SUBLIST3R
# Coded By Ahmed Aboul-Ela - @aboul3la

Python theHarvester - How to use it?
[-] Enumerating subdomains now for reddit.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
[-] Total Unique Subdomains Found: 16
addons.reddit.com
ads-api.reddit.com
alb.reddit.com
amp.reddit.com
h.reddit.com
www.h.reddit.com
m.reddit.com
www.m.reddit.com
pay.reddit.com
pixel.reddit.com
tls-test-1.reddit.com
www.tls-test-1.reddit.com
tls-test-2.reddit.com

Example:
To list the subdomains of a domain enter the following command in Linux and replace "kali.org" with the domain of your interest.

python3 /usr/bin/sublist3r.py -d kali.org -v

Where -d stands for domain listing and -v will verbose the output and tell from where it is getting the subdomains.

# python3 /usr/bin/sublist3r.py -d kali.org -v
```