# Sublist3r

# Installing Sublist3r

Unfortunately Sublist3r is not installed on Kali Linux by default so before we can start scanning some hosts we have to install the tool first. Fortunately the installation process is pretty straightforward and should not cause any trouble.

First open a terminal sessions and change the directory to the Desktop as following:

cd Desktop

The next step is to run the following command to clone the repository in a new directory:

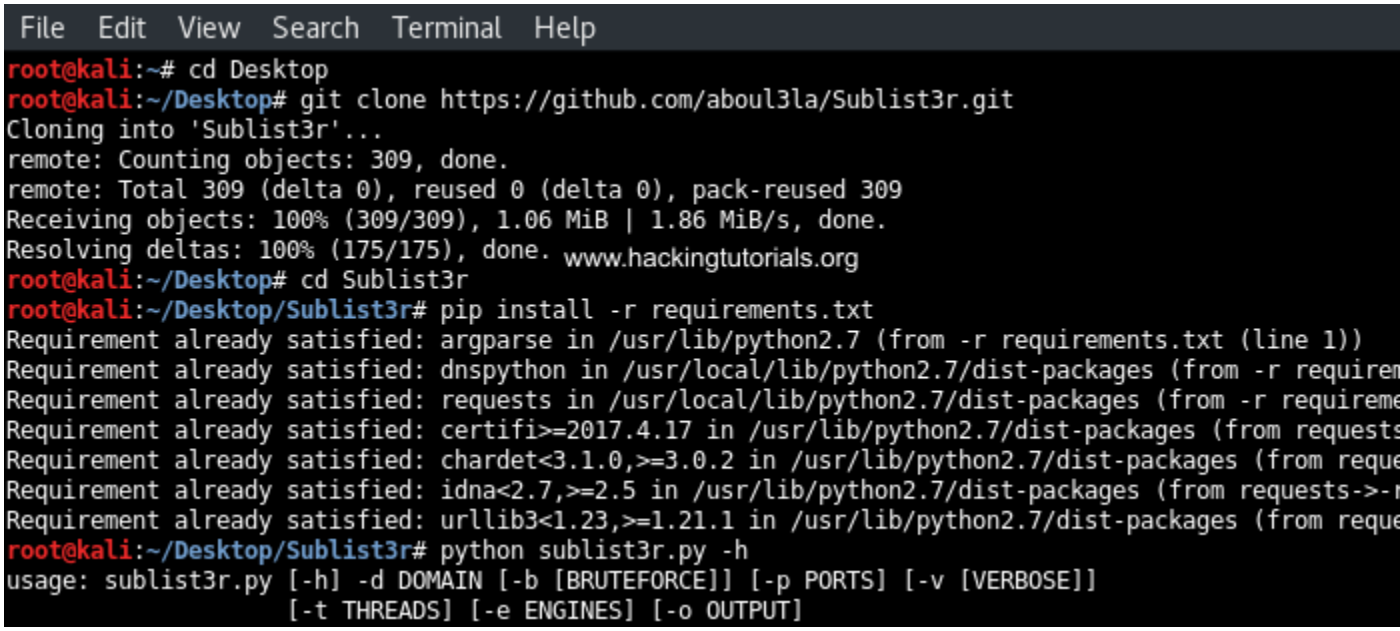
git clone https://github.com/aboul3la/Sublist3r.git

Change the directory to Sublist3r:

cd Sublist3r

And finally complete the installation by installing the required dependencies with the following command:

pip install -r requirements.txt




Installing Sublist3r

# Running Sublist3r

Let’s start with looking at the usage instructions. The usage instructions can be printed to the terminal by running Sublist3r with the -h option as following:

python sublist3r -h

```
File  Edit  View  Search  Terminal  Help
root@kali:~/Desktop/Sublist3r# python sublist3r.py -h
usage: sublist3r.py [-h] -d DOMAIN [-b [BRUTEFORCE]] [-p PORTS] [-v [VERBOSE]]
                    [-t THREADS] [-e ENGINES] [-o OUTPUT]

                      www.hackingtutorials.org
OPTIONS:
  -h, --help            show this help message and exit
  -d DOMAIN, --domain DOMAIN
                        Domain name to enumerate it's subdomains
  -b [BRUTEFORCE], --bruteforce [BRUTEFORCE]
                        Enable the subbrute bruteforce module
  -p PORTS, --ports PORTS
                        Scan the found subdomains against specified tcp ports
  -v [VERBOSE], --verbose [VERBOSE]
                        Enable Verbosity and display results in realtime
  -t THREADS, --threads THREADS
                        Number of threads to use for subbrute bruteforce
  -e ENGINES, --engines ENGINES
                        Specify a comma-separated list of search engines
  -o OUTPUT, --output OUTPUT
                        Save the results to text file

Example: python sublist3r.py -d google.com
root@kali:~/Desktop/Sublist3r#
```

Sublist3r usage instructions

Let’s run the example command that is printed at the bottom of the usage instructions. This command will run Sublist3r with the default options on the google.com domain:

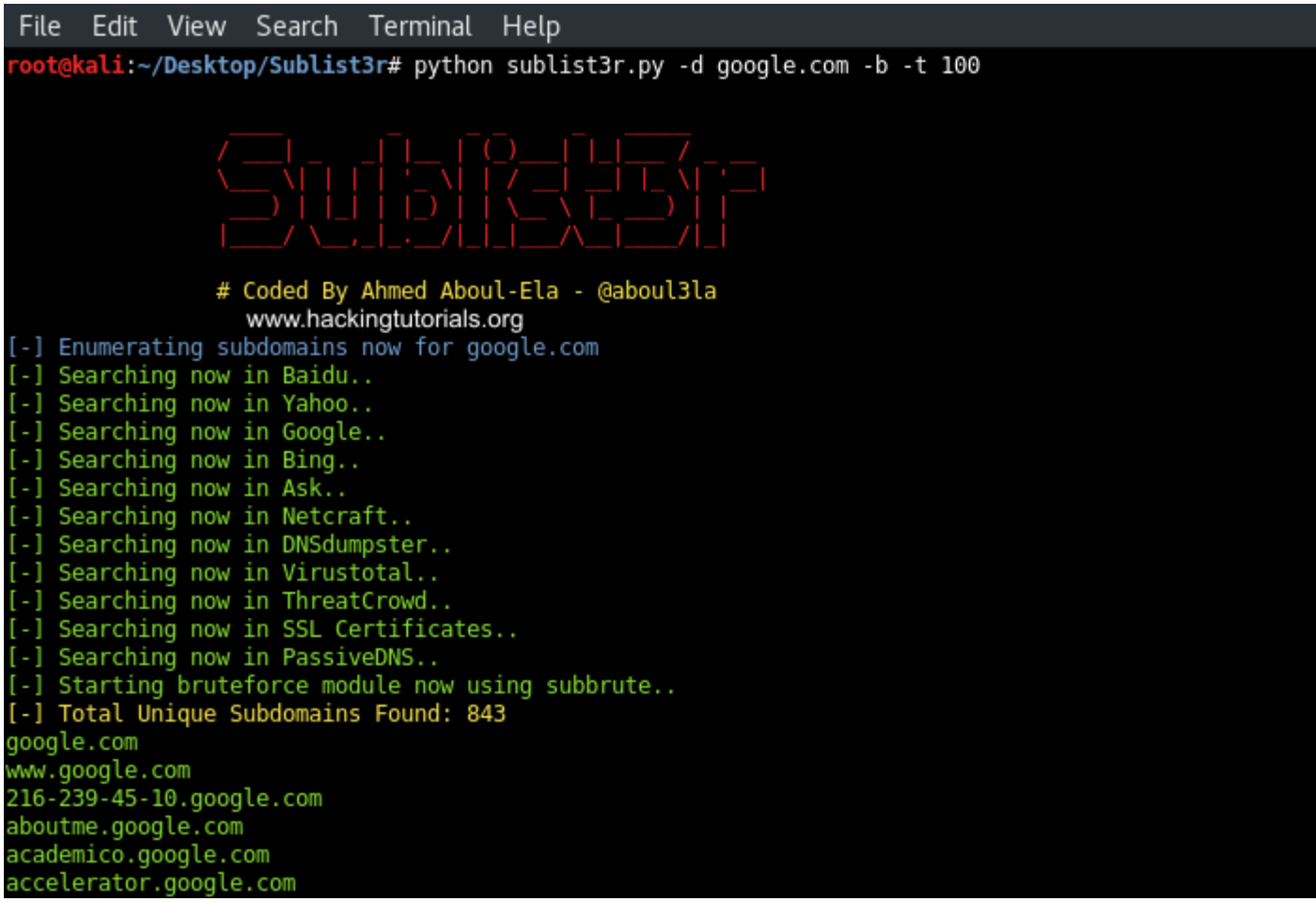
python sublist3r.py -d google.com


Sublist3r results

As we can see Sublist3r discovered 403 subdomains from Google, Bing, Yahoo and the other search engines. The found subdomains are then printed to the terminal.

So far we've only searched publicly available sources for sub domains for the given domain name. In the next step we will also activate Subbrute which uses a wordlist to brute force subdomains. The following command activates Subbrute with 100 threads:

python sublist3r.py -d google.com -b -t 100




Sublist3r and Subbrute results

As we can see Sublist3r and Subbrute found a total of 843 unique subdomains for the google.com domain.

To get the best results for subdomain discovery it is recommended to use a set of different tools. As different tools use different sources, techniques and wordlists to discover subdomains, combining the results of each tool will get you the best results. In this tutorial we've only covered Sublist3r (and Subbrute) but in future tutorials we will also look at some other tools such as recon-ng, Fierce and GoBuster and combine the results to a single list of unique subdomains.

# Links

Sublist3r: https://github.com/aboul3la/Sublist3r

Subbrute: https://github.com/TheRook/subbrute