CSS 600: Independent Study

Sublist3r

Sublist3r is a Python tool that uses OSINT to enumerate website subdomains. It assists penetration testers and bug hunters in collecting and gathering subdomains for the domain being targeted.

Prerequisite's:

Python 3 – For running Sublist3r tool, a python3 needs to be present prior to installing requirements

Installation:

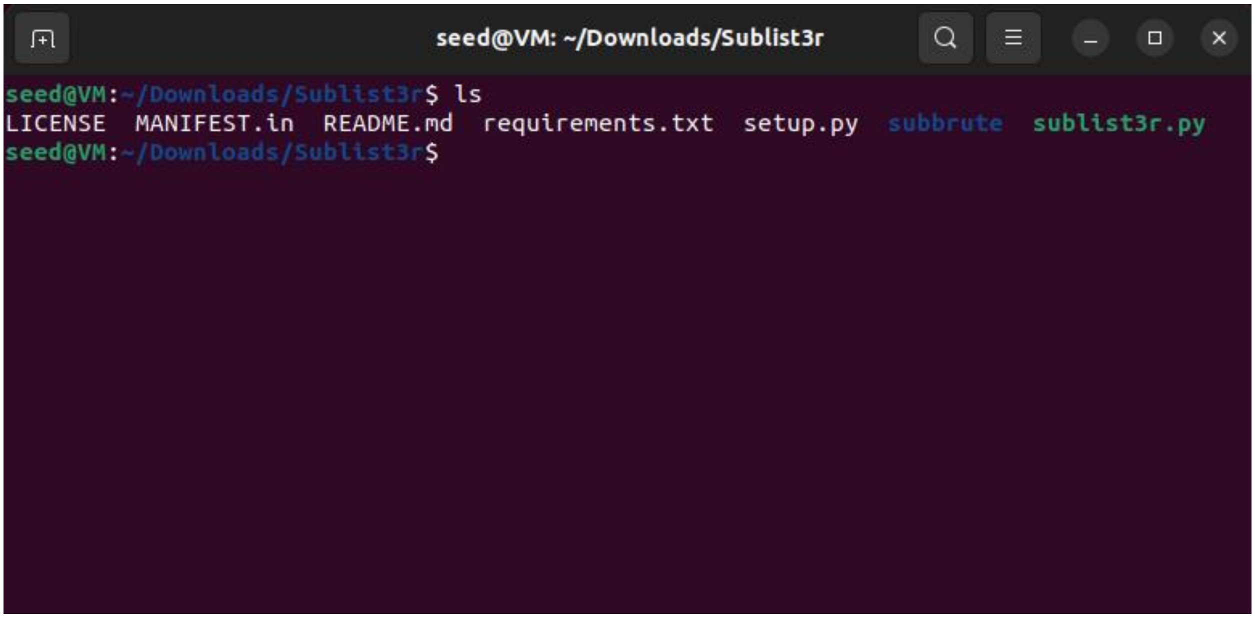
For demonstration, Ubuntu 20.04 Linux distribution is used throughout this guide

- Python 3 - sudo apt install -y python3-pip

After installing appropriate Python version, next step is to install Sublist3r tool, which can be downloaded from below address:

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

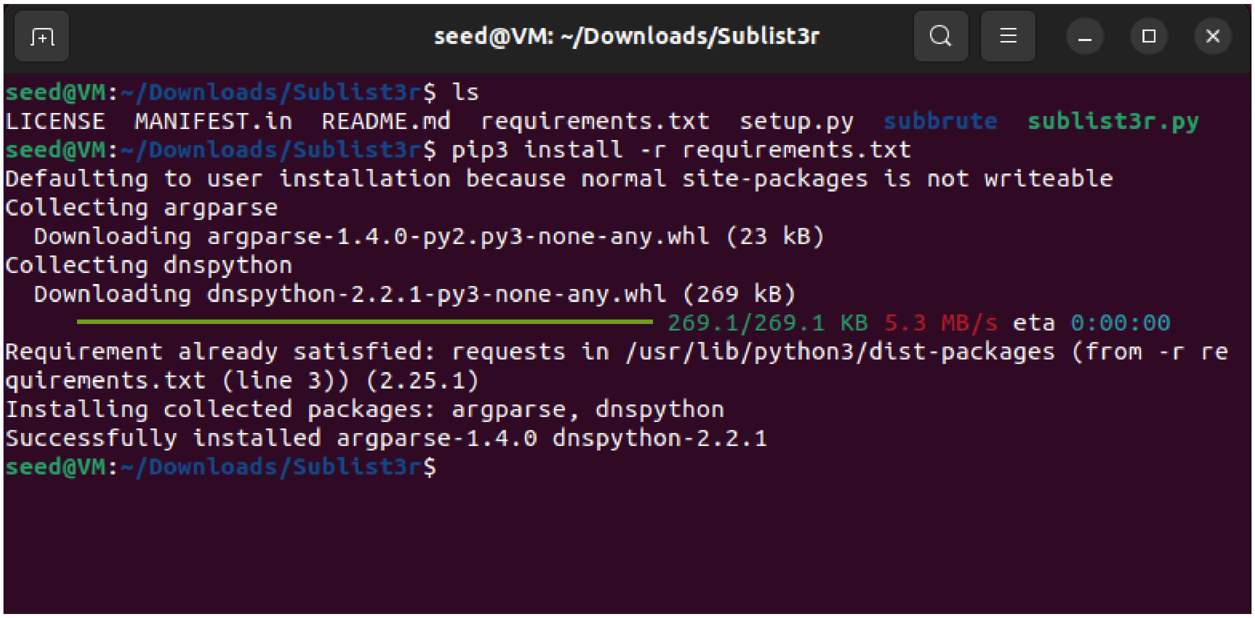
After downloading the tool, next step is to traverse to the downloaded directory as shown in below example:



```
seed@VM:~/Downloads/Sublist3r$ ls
LICENSE  MANIFEST.in  README.md  requirements.txt  setup.py  subbrute  sublist3r.py
seed@VM:~/Downloads/Sublist3r$
```

Then the next step is to install the requirements for running the tool which can be done using below command:

- pip3 install -r requirements.txt



```
seed@VM:~/Downloads/Sublist3r$ ls
LICENSE  MANIFEST.in  README.md  requirements.txt  setup.py  subbrute  sublist3r.py
seed@VM:~/Downloads/Sublist3r$ pip3 install -r requirements.txt
Defaulting to user installation because normal site-packages is not writeable
Collecting argparse
  Downloading argparse-1.4.0-py2.py3-none-any.whl (23 kB)
Collecting dnspython
  Downloading dnspython-2.2.1-py3-none-any.whl (269 kB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 269.1/269.1 KB 5.3 MB/s eta 0:00:00
Requirement already satisfied: requests in /usr/lib/python3/dist-packages (from -r re
quirements.txt (line 3)) (2.25.1)
Installing collected packages: argparse, dnspython
Successfully installed argparse-1.4.0 dnspython-2.2.1
seed@VM:~/Downloads/Sublist3r$
```

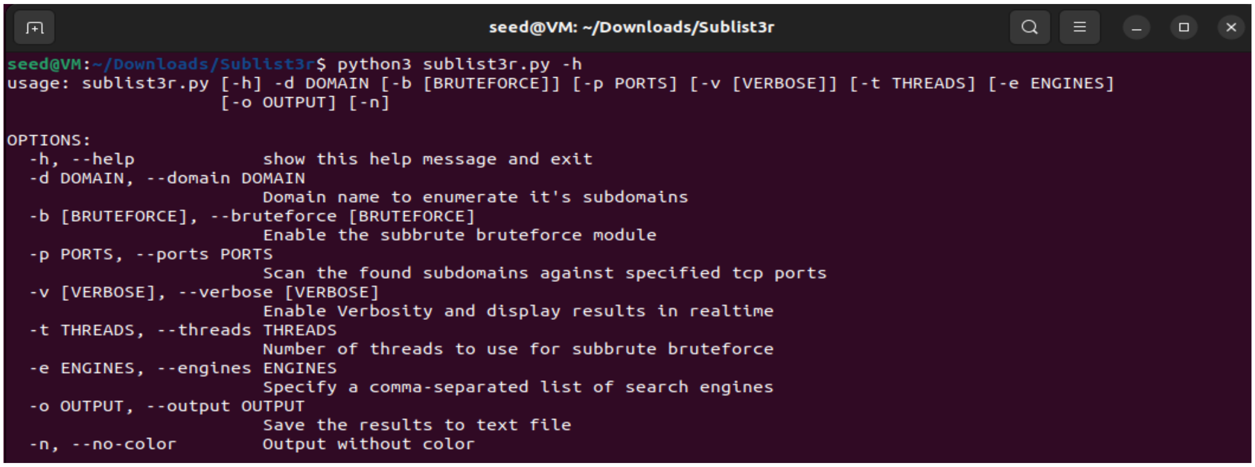
Execution:

After installing the required packages as shown in above screenshot, the tool can be executed using following command

- python3 sublist3r.py

The manual for identifying the appropriate usage of switches within the tool can be found using following command

- python3 sublist3r.py -h

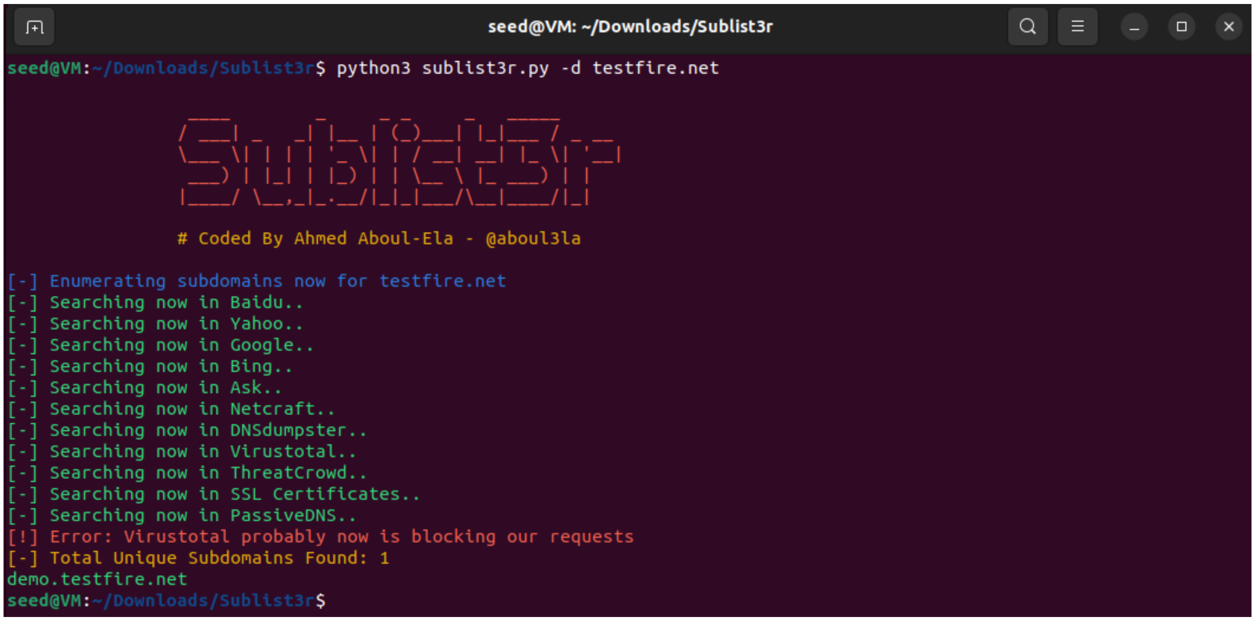


```
seed@VM:~/Downloads/Sublist3r$ python3 sublist3r.py -h
usage: sublist3r.py [-h] -d DOMAIN [-b [BRUTEFORCE]] [-p PORTS] [-v [VERBOSE]] [-t THREADS] [-e ENGINES]
                    [-o OUTPUT] [-n]

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
  -n, --no-color        Output without color
```

For testing purpose, following demo vulnerable website is used and below command can be run against it to identify the subdomains

- python3 sublist3r.py -d testfire.net



```
seed@VM:~/Downloads/Sublist3r$ python3 sublist3r.py -d testfire.net

                 ____        _     _ _     _   _____
                / ___| _   _| |__ | (_)___| |_|___ / _ __
                \___ \| | | | '_ \| | / __| __| |_ \| '__|
                 ___) | |_| | |_) | | \__ \ |_ ___) | |
                |____/ \__,_|_.__/|_|_|___/\__|____/|_|

                # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for testfire.net
[-] 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: 1
demo.testfire.net
seed@VM:~/Downloads/Sublist3r$
```

As seen from the result, this tool is very helpful in initial reconnaissance activities for scanning subdomains within target scope domains which can be utilized for identifying various web application vulnerabilities.