Sublist3r
Cyber Intel | Sublist3r | 22/09/2023

Executive Summary

This report presents an overview of Sublist3r, a versatile open-source reconnaissance tool designed for subdomain enumeration. Sublist3r aids security professionals, penetration testers, and researchers in the discovery of subdomains associated with a target domain.

Index

1. Introduction

Sublist3r is a command-line tool that facilitates subdomain enumeration by querying various search engines and DNS databases. Its primary purpose is to identify subdomains related to a specific target domain. This information is valuable in security assessments, as it can help identify potential entry points and security vulnerabilities.

2.Tool Details

Key Features

- **Subdomain Enumeration**: Sublist3r queries multiple search engines and DNS databases to discover subdomains associated with a target domain.
- **Custom Wordlists**: Users can provide custom wordlists to enhance the accuracy of subdomain discovery.
- **Output Formats**: Sublist3r generates output in various formats, including plain text and CSV, making it adaptable to different analysis tools.

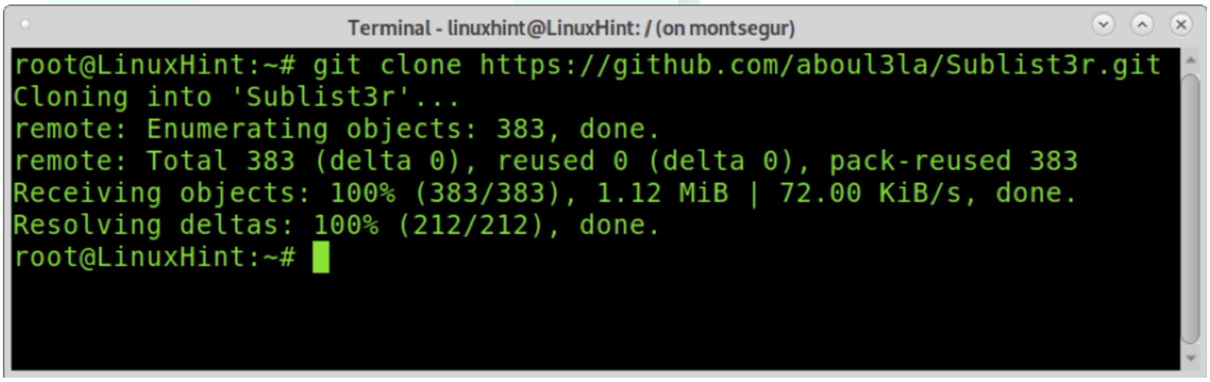
Warnings

- Scanning with **Virus Total** will not work due to the requests getting blocked.
- Installation with **apt** causes a lot of errors, refrain from using it and instead install from the GitHub repository.

3.Installation

Step 1. Clone the git repo

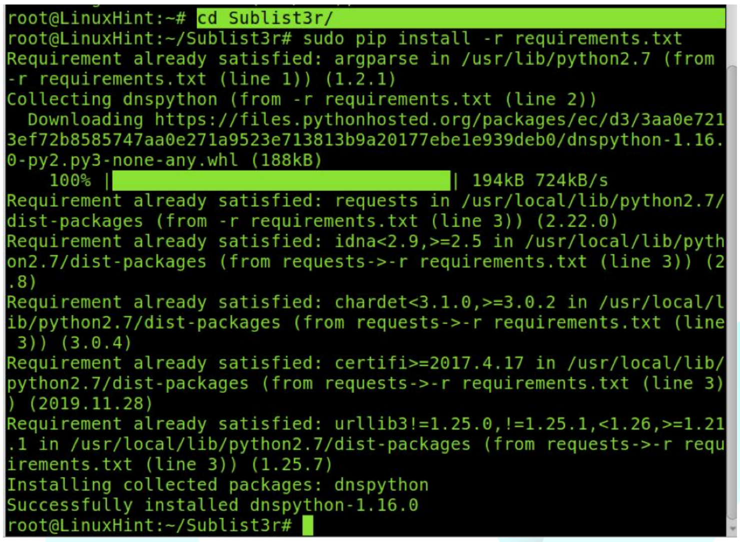
```
git clone https://github.com/aboul3la/Sublist3r.git
```



```
root@LinuxHint:~# git clone https://github.com/aboul3la/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 | 72.00 KiB/s, done.
Resolving deltas: 100% (212/212), done.
root@LinuxHint:~#
```

Step 2. Navigate to folder & install the requirements

```
cd Sublist3r/
sudo pip install –r requirements.txt
```

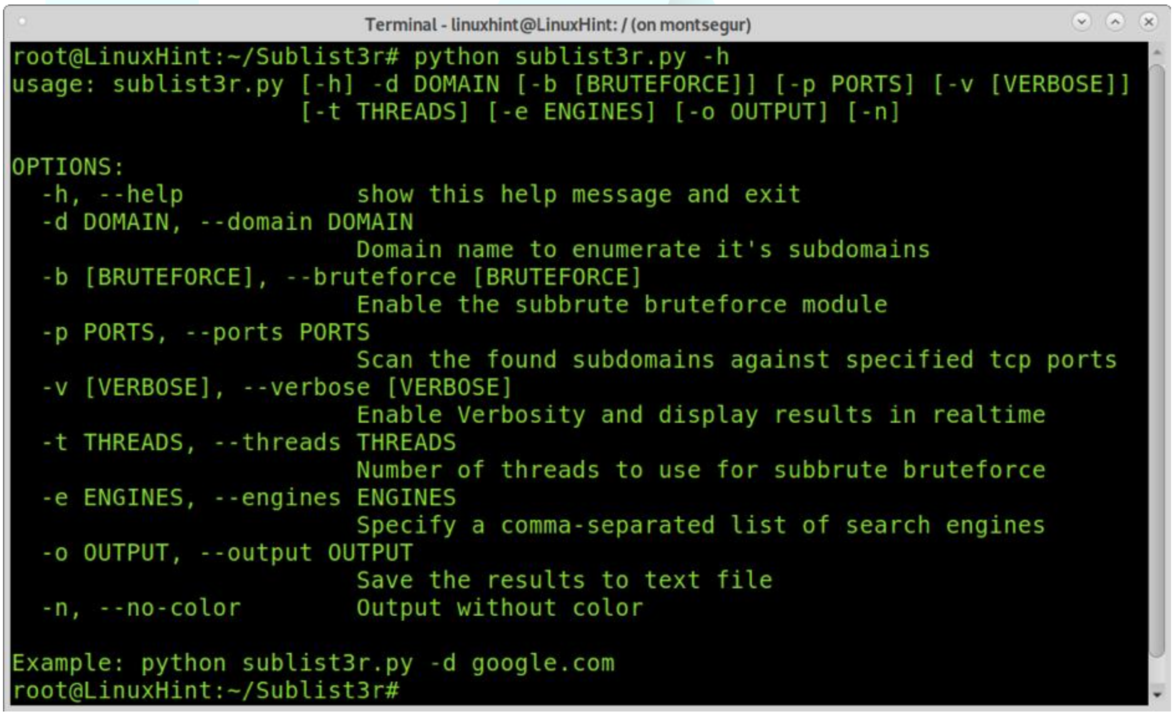


```
root@LinuxHint:~# cd Sublist3r/
root@LinuxHint:~/Sublist3r# sudo pip install -r requirements.txt
Requirement already satisfied: argparse in /usr/lib/python2.7 (from
-r requirements.txt (line 1)) (1.2.1)
Collecting dnspython (from -r requirements.txt (line 2))
  Downloading https://files.pythonhosted.org/packages/ec/d3/3aa0e721
3ef72b8585747aa0e271a9523e713813b9a20177ebe1e939deb0/dnspython-1.16.
0-py2.py3-none-any.whl (188kB)
    100% |████████████████████████████████| 194kB 724kB/s
Requirement already satisfied: requests in /usr/local/lib/python2.7/
dist-packages (from -r requirements.txt (line 3)) (2.22.0)
Requirement already satisfied: idna<2.9,>=2.5 in /usr/local/lib/pyth
on2.7/dist-packages (from requests->-r requirements.txt (line 3)) (2
.8)
Requirement already satisfied: chardet<3.1.0,>=3.0.2 in /usr/local/l
ib/python2.7/dist-packages (from requests->-r requirements.txt (line
 3)) (3.0.4)
Requirement already satisfied: certifi>=2017.4.17 in /usr/local/lib/
python2.7/dist-packages (from requests->-r requirements.txt (line 3)
) (2019.11.28)
Requirement already satisfied: urllib3!=1.25.0,!=1.25.1,<1.26,>=1.21
.1 in /usr/local/lib/python2.7/dist-packages (from requests->-r requ
irements.txt (line 3)) (1.25.7)
Installing collected packages: dnspython
Successfully installed dnspython-1.16.0
root@LinuxHint:~/Sublist3r# █
```

4. Execution

To run the tool

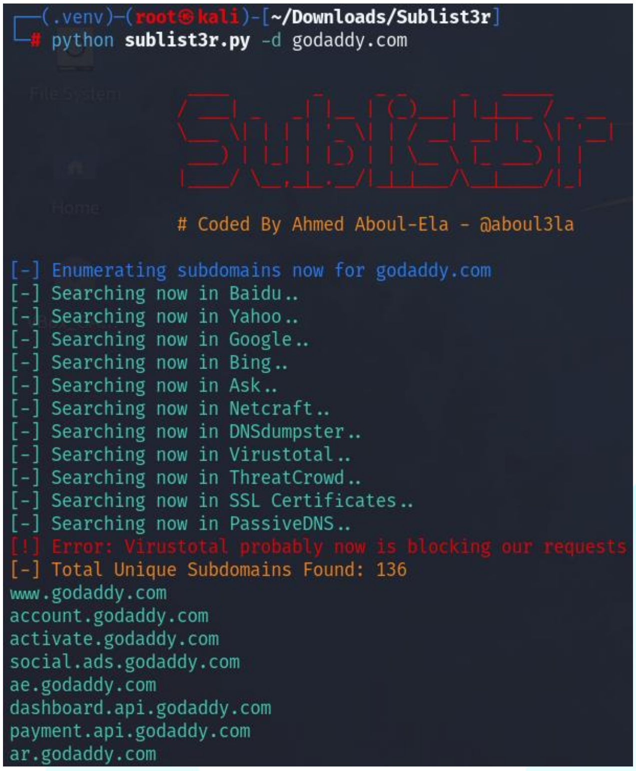
```
python sublist3r.py -h
```



```
root@LinuxHint:~/Sublist3r# python 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

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

Use Case 1. Search subdomains

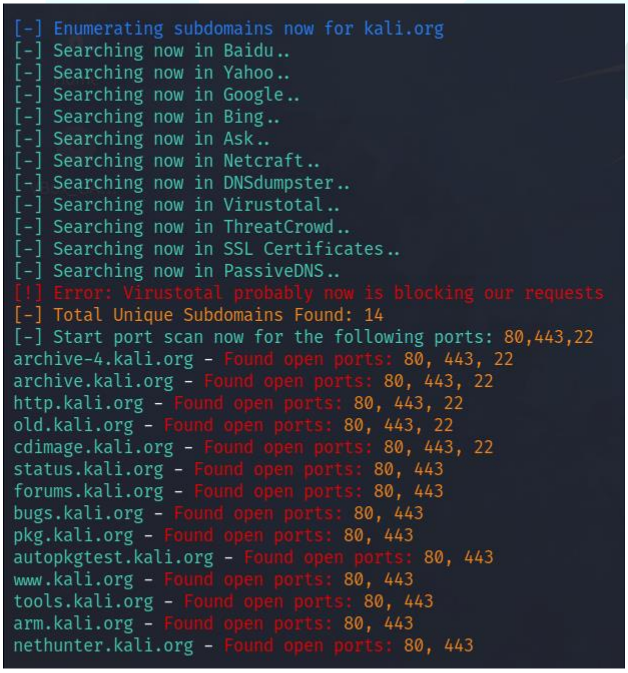
```
python sublist3r.py -d godaddy.com
```



```
┌──(.venv)─(root㉿kali)-[~/Downloads/Sublist3r]
└─# python sublist3r.py -d godaddy.com

                  # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for godaddy.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: 136
www.godaddy.com
account.godaddy.com
activate.godaddy.com
social.ads.godaddy.com
ae.godaddy.com
dashboard.api.godaddy.com
payment.api.godaddy.com
ar.godaddy.com
```

Use Case 2. Specify TCP Ports to be scanned for the subdomain

```
python sublist3r.py -d kali.org -p 80,443,22
```

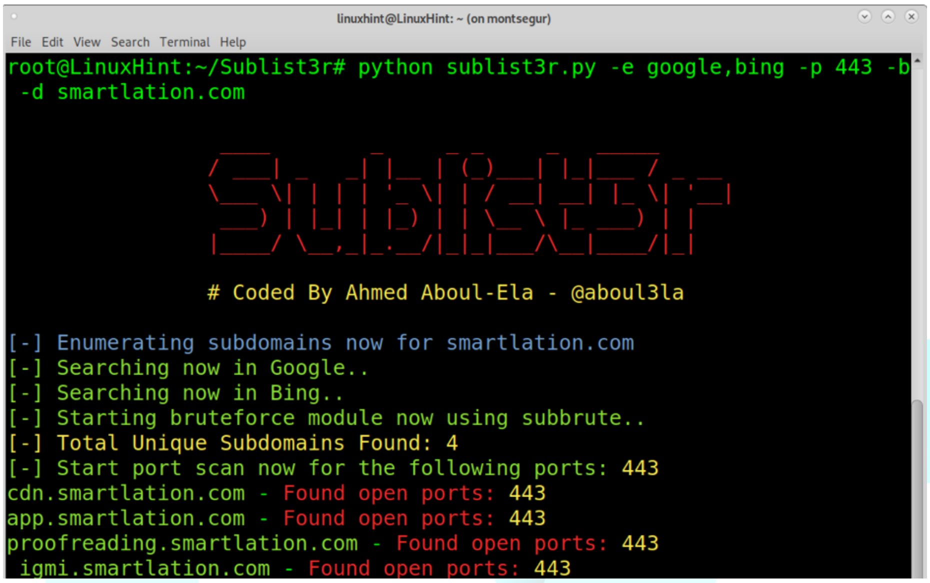


```
[-] Enumerating subdomains now for kali.org
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
[-] Total Unique Subdomains Found: 14
[-] Start port scan now for the following ports: 80,443,22
archive-4.kali.org - Found open ports: 80, 443, 22
archive.kali.org - Found open ports: 80, 443, 22
http.kali.org - Found open ports: 80, 443, 22
old.kali.org - Found open ports: 80, 443, 22
cdimage.kali.org - Found open ports: 80, 443, 22
status.kali.org - Found open ports: 80, 443
forums.kali.org - Found open ports: 80, 443
bugs.kali.org - Found open ports: 80, 443
pkg.kali.org - Found open ports: 80, 443
autopkgtest.kali.org - Found open ports: 80, 443
www.kali.org - Found open ports: 80, 443
tools.kali.org - Found open ports: 80, 443
arm.kali.org - Found open ports: 80, 443
nethunter.kali.org - Found open ports: 80, 443
```

Use Case 3: Specify the search engine to use along with brute forcing

The subdomain dictionary is called **names.txt** and contains 101,010 subdomains.

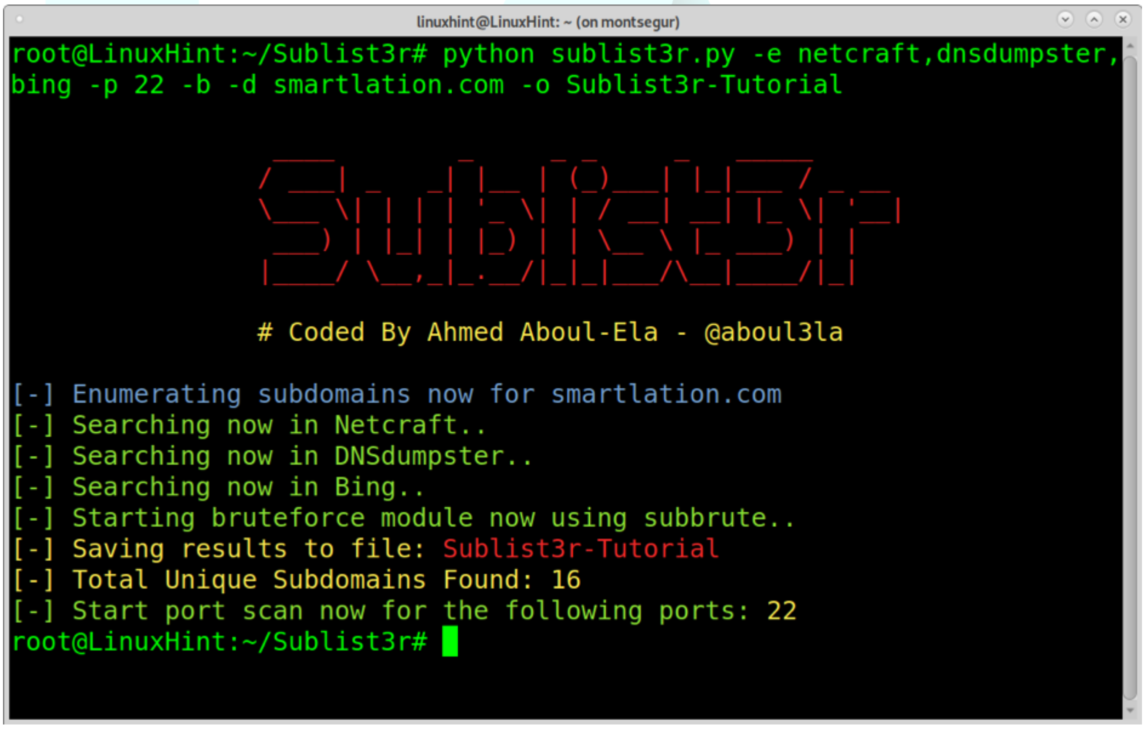
```
python sublist3r.py -e google,bing  -b -d smartlation.com
```


linuxhint@LinuxHint: ~ (on montsegur)
File Edit View Search Terminal Help

```
root@LinuxHint:~/Sublist3r# python sublist3r.py -e google,bing -p 443 -b
 -d smartlation.com

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

                # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for smartlation.com
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Starting bruteforce module now using subbrute..
[-] Total Unique Subdomains Found: 4
[-] Start port scan now for the following ports: 443
cdn.smartlation.com - Found open ports: 443
app.smartlation.com - Found open ports: 443
proofreading.smartlation.com - Found open ports: 443
 igmi.smartlation.com - Found open ports: 443
```

Use Case 4: Output results to a file

```
python sublist3r.py -e netcraft,dnsdumpster,bing -p 22 -b -d
smartlation.com -o Sublist3r-Tutorial
```



```
root@LinuxHint:~/Sublist3r# python sublist3r.py -e netcraft,dnsdumpster,
bing -p 22 -b -d smartlation.com -o Sublist3r-Tutorial

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

                # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for smartlation.com
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Bing..
[-] Starting bruteforce module now using subbrute..
[-] Saving results to file: Sublist3r-Tutorial
[-] Total Unique Subdomains Found: 16
[-] Start port scan now for the following ports: 22
root@LinuxHint:~/Sublist3r# 
```

5. Scope and Limitations

- Sublist3r's effectiveness depends on the availability and accessibility of search engines and DNS databases. Some sources may impose query rate limits.

- False positives and outdated subdomains may be included in the results, requiring manual verification.

- Sublist3r is a command-line tool, which may not be as user-friendly for individuals unfamiliar with command-line interfaces.

6. Conclusion

Sublist3r is a valuable addition to the toolkit of security professionals and researchers involved in domain discovery and reconnaissance. Its ability to efficiently identify subdomains associated with a target domain enhances the overall security assessment process. Sublist3r's flexibility and support for custom wordlists make it a versatile choice for subdomain enumeration tasks.

7. References

Sublist3r for Enumerate Subdomains (linuxhint.com)

OpenAI. (2023). *ChatGPT* (August 3 Version) [Large language model].

https://chat.openai.com