**Sublist3r**

Sublist3r is a popular open-source tool used in cybersecurity and penetration testing. It's designed to enumerate subdomains of websites using various techniques.

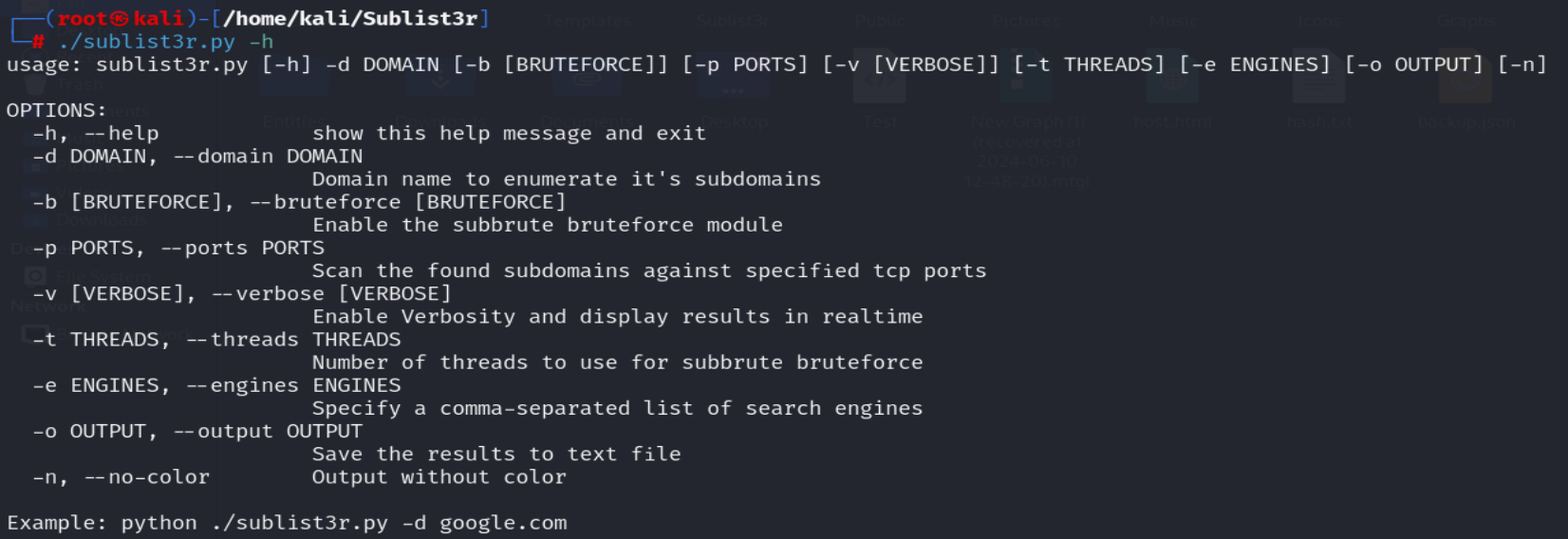
Here's a brief overview:

1. Purpose: Sublist3r helps security professionals and ethical hackers discover subdomains associated with a target domain.
2. Functionality: It uses search engines, DNS records, and other sources to find and list subdomains.
3. Key features:
   * Multithreaded subdomain enumeration
   * Supports multiple search engines
   * Can use Netcraft, Virustotal, ThreatCrowd, DNSdumpster, and ReverseDNS
4. Usage: Typically used in the reconnaissance phase of security assessments or penetration tests.
5. Language: Written in Python
6. Availability: Open-source and freely available on GitHub

We can perform these :

Key Options:

* -d: Specify the target domain
* -t: Number of threads (default is 40)
* -o: Save results to a text file
* -v: Verbose mode
* -p: Scan specific ports
* -e: Specify search engines to use

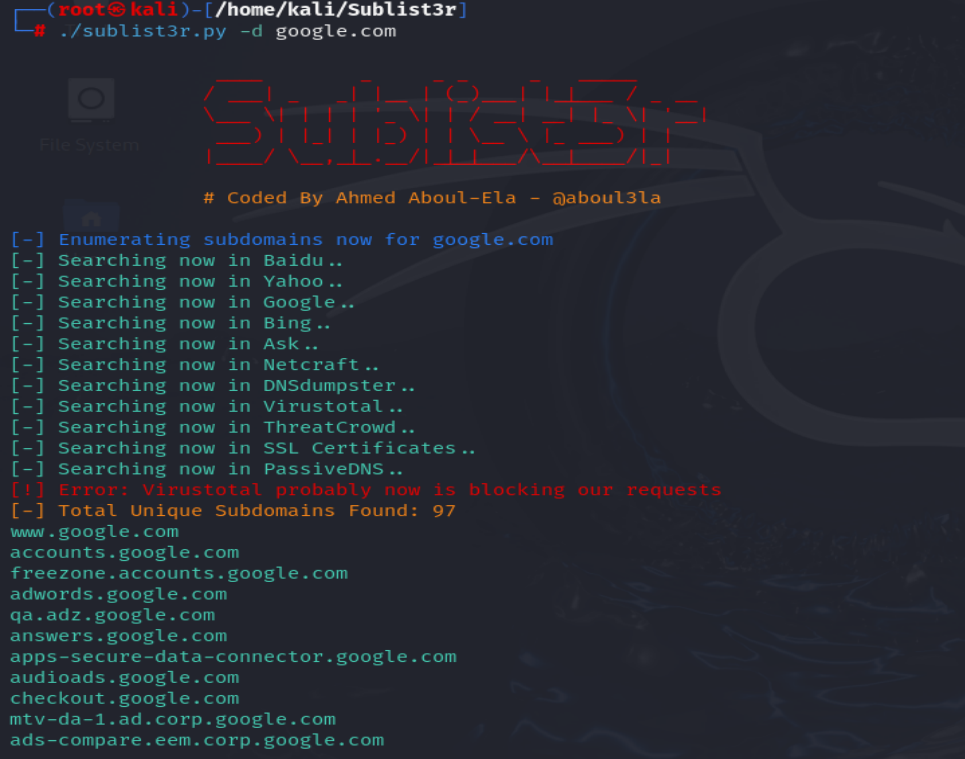
****

* Specify the domain: -d <url>

Command: ./sublist3r.py -d google.com

* Specify the search engine: -e <engine name>

Command: ./sublist3r.py -d google.com -e bing

****

* Specify the port : -p <port number>

****

This way, we can use sublist3r and enumerate subdomains.