[Date:07-04-2023]

Report by Pankaj Jarial on

subdoamin finder tools

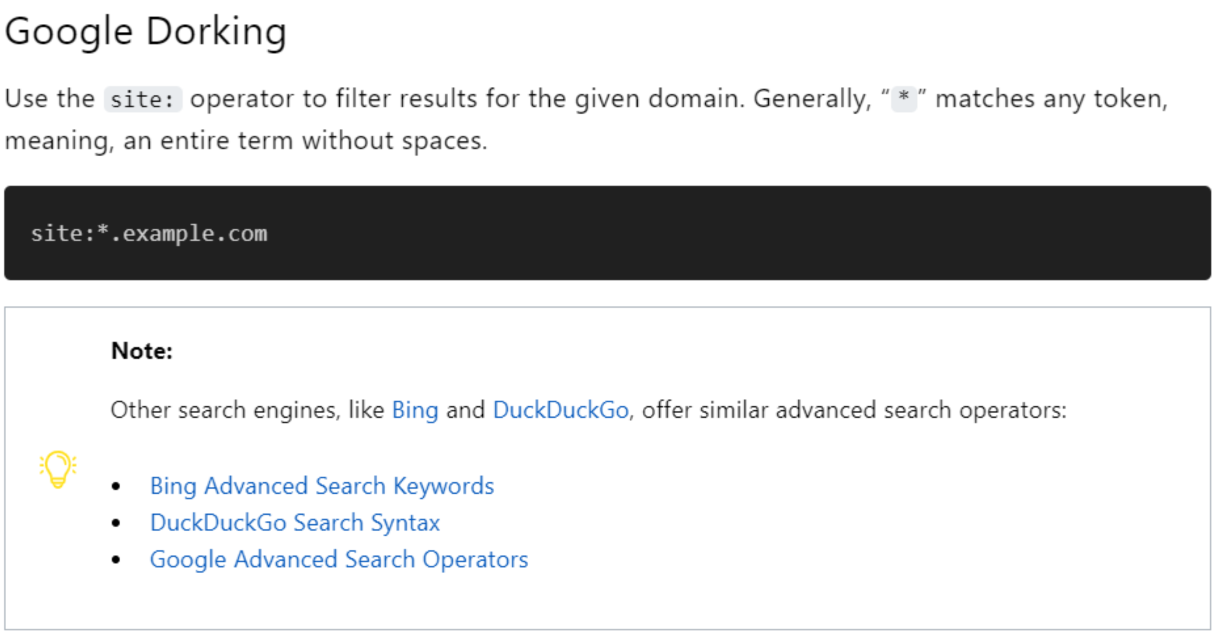
What is mean by Subdomain Finder?

1. A subdomain finder is a tool used to find the subdomains of a given domain.

2. Subdomains are created when a second-level domain is added to a top-level domain. For example, the subdomain "www" is a subdomain of the domain "example.com". A subdomain can be created for any purpose, and there is no limit to the number of subdomains that can be created for a single domain.

3. Subdomain Finder scans the DNS records and supplementary databases to analyze the domain's hierarchy. Our subdomain scanner checks: DNS records (NS, MX, TXT, AXFR) DNS enumeration.

Side from any tool be can simply search on internet by just Google search-hacking Google Dorking



Google Dorking

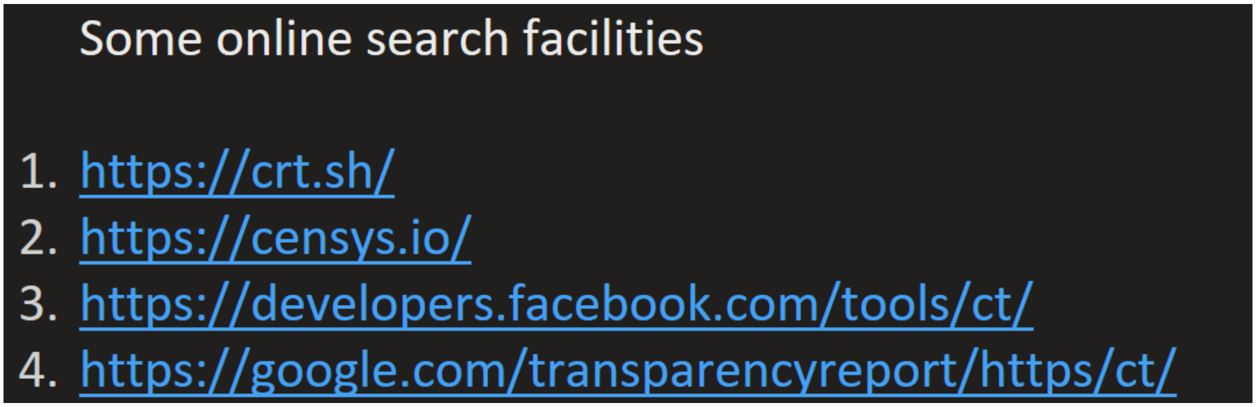
Use the `site:` operator to filter results for the given domain. Generally, "`*`" matches any token, meaning, an entire term without spaces.

```
site:*.example.com
```

Note:

Other search engines, like Bing and DuckDuckGo, offer similar advanced search operators:

- Bing Advanced Search Keywords
- DuckDuckGo Search Syntax
- Google Advanced Search Operators

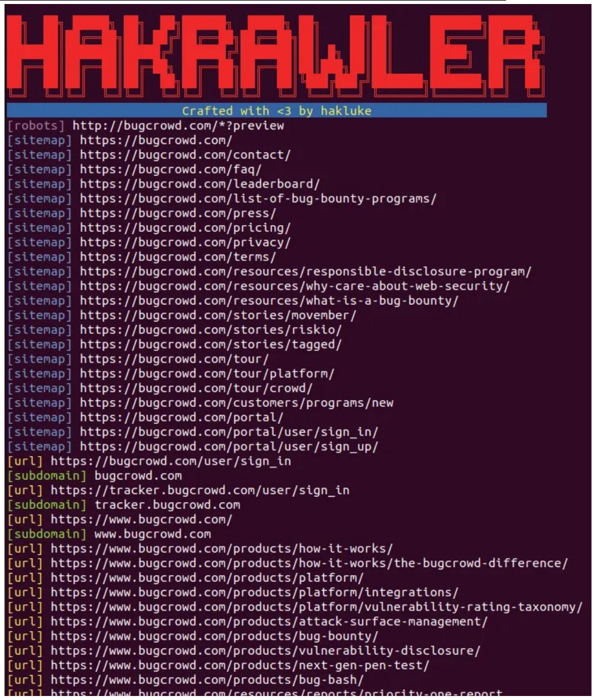


Some online search facilities

1. https://crt.sh/
2. https://censys.io/
3. https://developers.facebook.com/tools/ct/
4. https://google.com/transparencyreport/https/ct/

And there are also some tools which helps us to find subdomain as much as possible, without much scrolling and clicking like Google Dorking

1. Hakrawler



```
HAKRAWLER
Crafted with <3 by hakluke
[robots] http://bugcrowd.com/*?preview
[sitemap] https://bugcrowd.com/
[sitemap] https://bugcrowd.com/contact/
[sitemap] https://bugcrowd.com/faq/
[sitemap] https://bugcrowd.com/leaderboard/
[sitemap] https://bugcrowd.com/list-of-bug-bounty-programs/
[sitemap] https://bugcrowd.com/press/
[sitemap] https://bugcrowd.com/pricing/
[sitemap] https://bugcrowd.com/privacy/
[sitemap] https://bugcrowd.com/terms/
[sitemap] https://bugcrowd.com/resources/responsible-disclosure-program/
[sitemap] https://bugcrowd.com/resources/why-care-about-web-security/
[sitemap] https://bugcrowd.com/resources/what-is-a-bug-bounty/
[sitemap] https://bugcrowd.com/stories/movember/
[sitemap] https://bugcrowd.com/stories/riskio/
[sitemap] https://bugcrowd.com/stories/tagged/
[sitemap] https://bugcrowd.com/tour/
[sitemap] https://bugcrowd.com/tour/platform/
[sitemap] https://bugcrowd.com/tour/crowd/
[sitemap] https://bugcrowd.com/customers/programs/new
[sitemap] https://bugcrowd.com/portal/
[sitemap] https://bugcrowd.com/portal/user/sign_in/
[sitemap] https://bugcrowd.com/portal/user/sign_up/
[url] https://bugcrowd.com/user/sign_in
[subdomain] bugcrowd.com
[url] https://tracker.bugcrowd.com/user/sign_in
[subdomain] tracker.bugcrowd.com
[url] https://www.bugcrowd.com/
[subdomain] www.bugcrowd.com
[url] https://www.bugcrowd.com/products/how-it-works/
[url] https://www.bugcrowd.com/products/how-it-works/the-bugcrowd-difference/
[url] https://www.bugcrowd.com/products/platform/
[url] https://www.bugcrowd.com/products/platform/integrations/
[url] https://www.bugcrowd.com/products/platform/vulnerability-rating-taxonomy/
[url] https://www.bugcrowd.com/products/attack-surface-management/
[url] https://www.bugcrowd.com/products/bug-bounty/
[url] https://www.bugcrowd.com/products/vulnerability-disclosure/
[url] https://www.bugcrowd.com/products/next-gen-pen-test/
[url] https://www.bugcrowd.com/products/bug-bash/
[url] https://www.bugcrowd.com/resources/reports/priority-one-report
```

The URLs are extracted by spidering the application, querying wayback machine, parsing robots.txt files and parsing sitemap.xml files.

The tool also collects any subdomains it finds along the way. As far as I know, this subdomain enumeration method is not currently used by any other popular subdomain enumeration tools, so it may help to uncover some additional targets.

Features

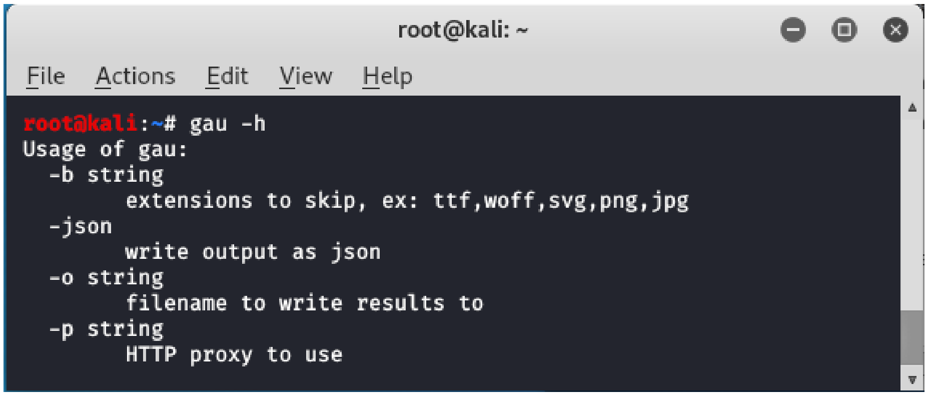
•Easily chainable with other tools (accepts hostnames from stdin, dumps plain URLs to stdout using the -plain tag)
•Collects URLs by crawling each page the application, following links
•Collects URLs from wayback machine
•Collects URLs from robots.txt
•Collects URLs from sitemap.xml
•Discovers new domains and subdomains belonging to the target as it finds them during the crawling process
•Written in Golang
•Variable scope can be set to narrow down or expand results

•Can export results into files containing raw HTTP requests, which may be parsed by other tools such as SQLMap.

2. Getallurls (gau)

Gau tool is written in go language you must have go language installed into your Kali

Linux in order to use this tool. This tool comes with an awesome user interface. getallurls (gau) fetches known URLs from AlienVault's Open Threat Exchange, the Wayback Machine, Common Crawl, and URLScan for any given domain. Inspired by Tomnomnom's waybackurls.

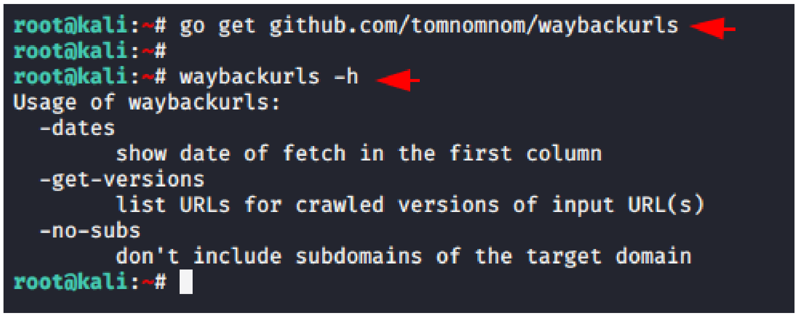


```
root@kali:~# gau -h
Usage of gau:
  -b string
        extensions to skip, ex: ttf,woff,svg,png,jpg
  -json
        write output as json
  -o string
        filename to write results to
  -p string
        HTTP proxy to use
```

3. Waybackurls

Waybackurls is a Golang language-based tool, so you need to have a Golang environment on your system.

Waybackurls is also a Golang based script or tool used for crawling domains on stdin, fetch known URLs from Wayback Machines, also known as Archives for *.targetdomain and output them stdout.

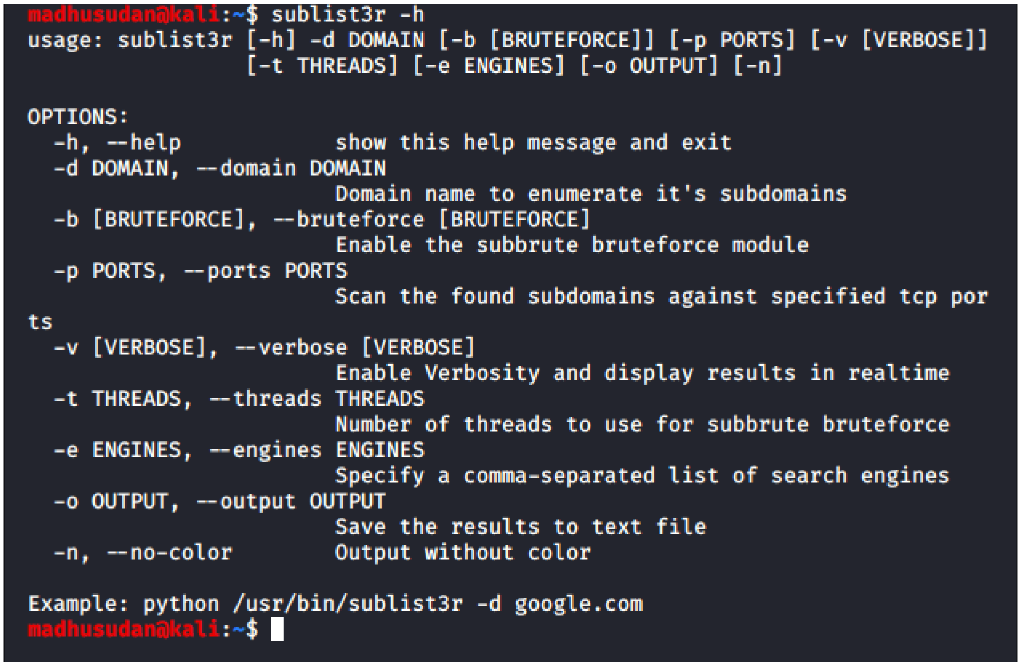


```
root@kali:~# go get github.com/tomnomnom/waybackurls
root@kali:~#
root@kali:~# waybackurls -h
Usage of waybackurls:
  -dates
        show date of fetch in the first column
  -get-versions
        list URLs for crawled versions of input URL(s)
  -no-subs
        don't include subdomains of the target domain
root@kali:~#
```

4. sublist3r

Sublist3r is a python tool designed to enumerate subdomains of websites using OSINT. It helps penetration testers and bug hunters collect and gather subdomains for the domain they are targeting. Sublist3r enumerates subdomains using many search engines such as Google, Yahoo, Bing, Baidu and Ask. Sublist3r also enumerates subdomains using Netcraft, Virustotal, ThreatCrowd, DNSdumpster and ReverseDNS.

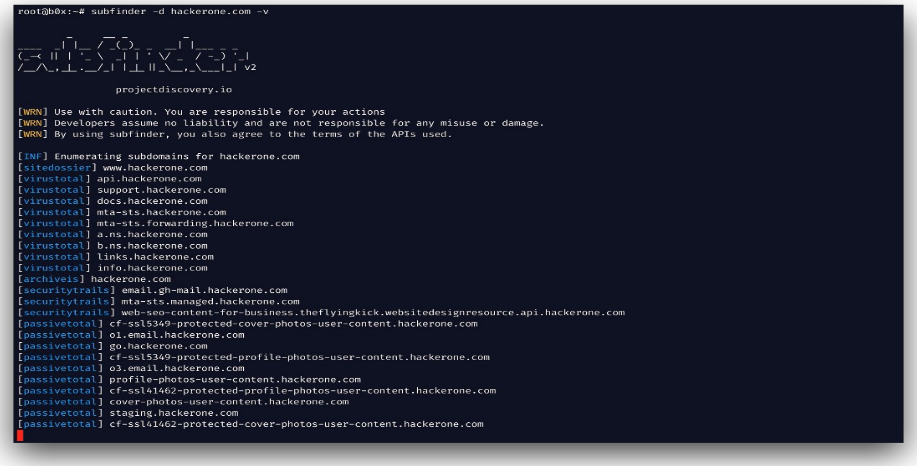
subbrute was integrated with Sublist3r to increase the possibility of finding more subdomains using bruteforce with an improved wordlist. The credit goes to TheRook who is the author of subbrute.



```
madhusudan@kali:~$ sublist3r -h
usage: sublist3r [-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 por
ts
  -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 /usr/bin/sublist3r -d google.com
madhusudan@kali:~$ █
```

5. subfinder

subfinder is a subdomain discovery tool that returns valid subdomains for websites, using passive online sources. It has a simple, modular architecture and is optimized for speed. subfinder is built for doing one thing only - passive subdomain enumeration, and it does that very well.We have made it to comply with all the used passive source licenses and usage restrictions. The passive model guarantees speed and stealthiness that can be leveraged by both penetration testers and bug bounty hunters alike.



```
root@b0x:~# subfinder -d hackerone.com -v

               _     __ _         _
____    _| |__  / _(_)_ _   __| |___ _ _
(_-< || | '_ \  _| | ' \/ _  / -_) '_|
/__/\_,_|_.__/_| |_|_||_\__,_\___|_| v2

                projectdiscovery.io

[WRN] Use with caution. You are responsible for your actions
[WRN] Developers assume no liability and are not responsible for any misuse or damage.
[WRN] By using subfinder, you also agree to the terms of the APIs used.

[INF] Enumerating subdomains for hackerone.com
[sitedossier] www.hackerone.com
[virustotal] api.hackerone.com
[virustotal] support.hackerone.com
[virustotal] docs.hackerone.com
[virustotal] mta-sts.hackerone.com
[virustotal] mta-sts.forwarding.hackerone.com
[virustotal] a.ns.hackerone.com
[virustotal] b.ns.hackerone.com
[virustotal] links.hackerone.com
[virustotal] info.hackerone.com
[archiveis] hackerone.com
[securitytrails] email.gh-mail.hackerone.com
[securitytrails] mta-sts.managed.hackerone.com
[securitytrails] web-seo-content-for-business.theflyingkick.websitedesignresource.api.hackerone.com
[passivetotal] cf-ssl5349-protected-cover-photos-user-content.hackerone.com
[passivetotal] o1.email.hackerone.com
[passivetotal] go.hackerone.com
[passivetotal] cf-ssl5349-protected-profile-photos-user-content.hackerone.com
[passivetotal] o3.email.hackerone.com
[passivetotal] profile-photos-user-content.hackerone.com
[passivetotal] cf-ssl41462-protected-profile-photos-user-content.hackerone.com
[passivetotal] cover-photos-user-content.hackerone.com
[passivetotal] staging.hackerone.com
[passivetotal] cf-ssl41462-protected-cover-photos-user-content.hackerone.com
```

Features

•Fast and powerful resolution and wildcard elimination modules

•Curated passive sources to maximize results

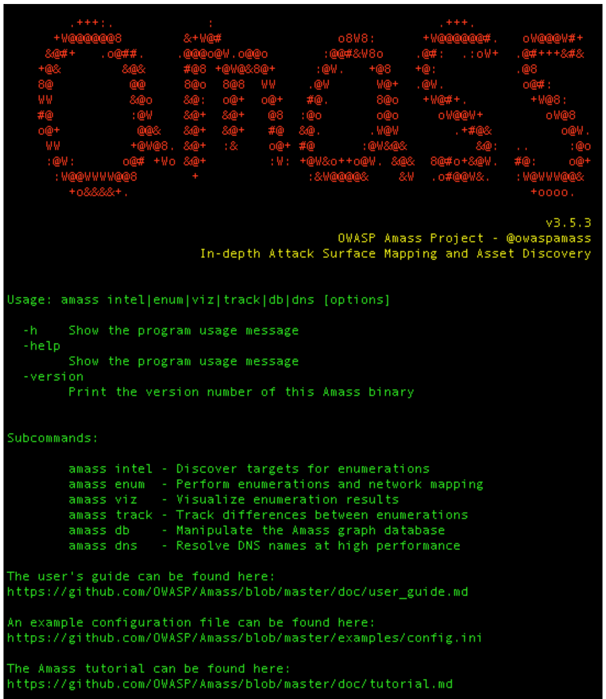
•Multiple output formats supported (JSON, file, stdout)

•Optimized for speed and lightweight on resources

•STDIN/OUT support enables easy integration into workflows

6. OWASP /AMAAS

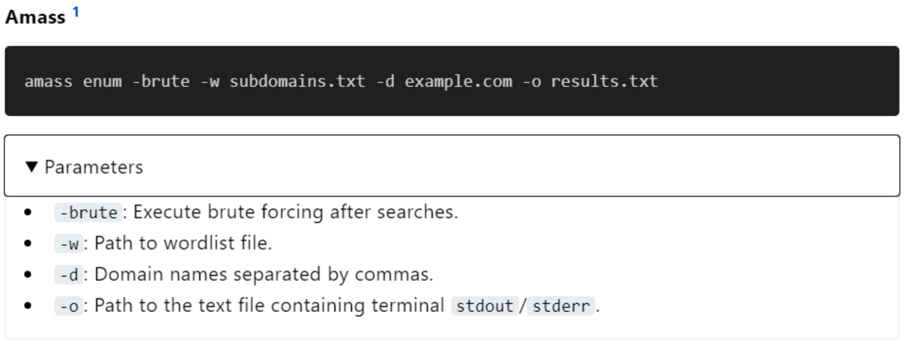
Amass is an open source network mapping and attack surface discovery tool that uses information gathering and other techniques such as active reconnaissance and external asset discovery to scrap all the available data. In order to accomplish this, it uses its own internal machinery and it also integrates smoothly with different external services to increase its results, efficiency and power



```
                                                          v3.5.3
                                OWASP Amass Project - @owaspamass
                In-depth Attack Surface Mapping and Asset Discovery


Usage: amass intel|enum|viz|track|db|dns [options]

  -h    Show the program usage message
  -help
        Show the program usage message
  -version
        Print the version number of this Amass binary


Subcommands:

        amass intel - Discover targets for enumerations
        amass enum  - Perform enumerations and network mapping
        amass viz   - Visualize enumeration results
        amass track - Track differences between enumerations
        amass db    - Manipulate the Amass graph database
        amass dns   - Resolve DNS names at high performance

The user's guide can be found here:
https://github.com/OWASP/Amass/blob/master/doc/user_guide.md

An example configuration file can be found here:
https://github.com/OWASP/Amass/blob/master/examples/config.ini

The Amass tutorial can be found here:
https://github.com/OWASP/Amass/blob/master/doc/tutorial.md
```

¶Scraping unpublished subdomains

Sometimes subdomains won’t show up. They can be a bit inactive, and when queried, their activity goes far below the radar. So how do we get them? Meet subdomain brute forcing. This technique allows us to bring in our custom wordlist and try it against the configured domain name, in an attempt to find or discover unseen subdomains.



Amass [1]

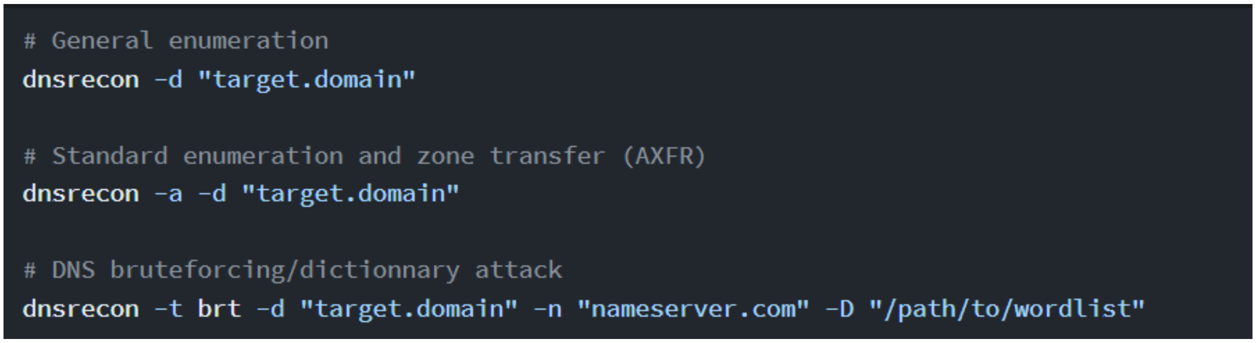
```
amass enum -brute -w subdomains.txt -d example.com -o results.txt
```

▼ Parameters

- `-brute`: Execute brute forcing after searches.
- `-w`: Path to wordlist file.
- `-d`: Domain names separated by commas.
- `-o`: Path to the text file containing terminal `stdout` / `stderr`.

7. DNSRecon

DNSRecon is a Python port of a Ruby script that I wrote to learn the language and about DNS in early 2007. This time I wanted to learn about Python and extend the functionality of the original tool and in the process re-learn how DNS works and how could it be used in the process of a security assessment and network troubleshooting.



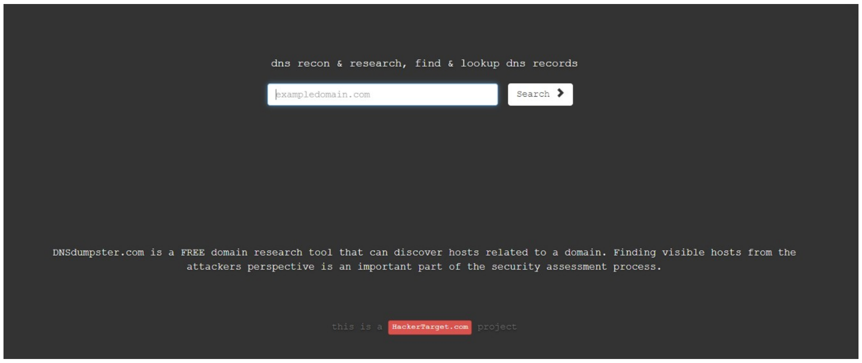
```
# General enumeration
dnsrecon -d "target.domain"

# Standard enumeration and zone transfer (AXFR)
dnsrecon -a -d "target.domain"

# DNS bruteforcing/dictionnary attack
dnsrecon -t brt -d "target.domain" -n "nameserver.com" -D "/path/to/wordlist"
```

8. DNSDumpster

A tool to perform DNS reconnaissance on target networks. The results include a variety of information that are useful for users performing network reconnaissance. Some of the information return include

- Host subdomains
- Different dns informat(MX, A record)
- Geo information
- Email

also appears with search engine

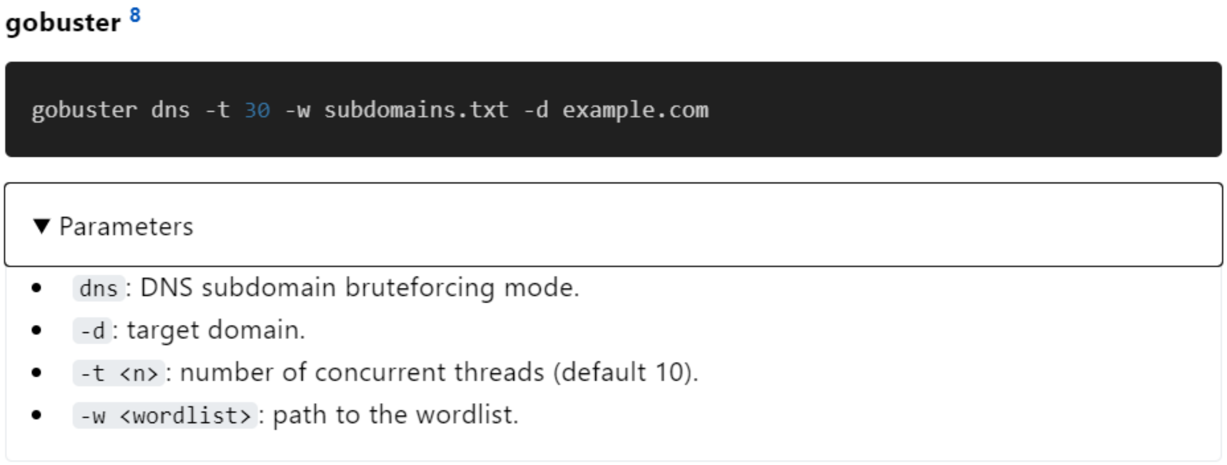


dns recon & research, find & lookup dns records

DNSdumpster.com is a FREE domain research tool that can discover hosts related to a domain. Finding visible hosts from the attackers perspective is an important part of the security assessment process.

this is a HackerTarget.com project

9. gobuster



gobuster[8]

```
gobuster dns -t 30 -w subdomains.txt -d example.com
```

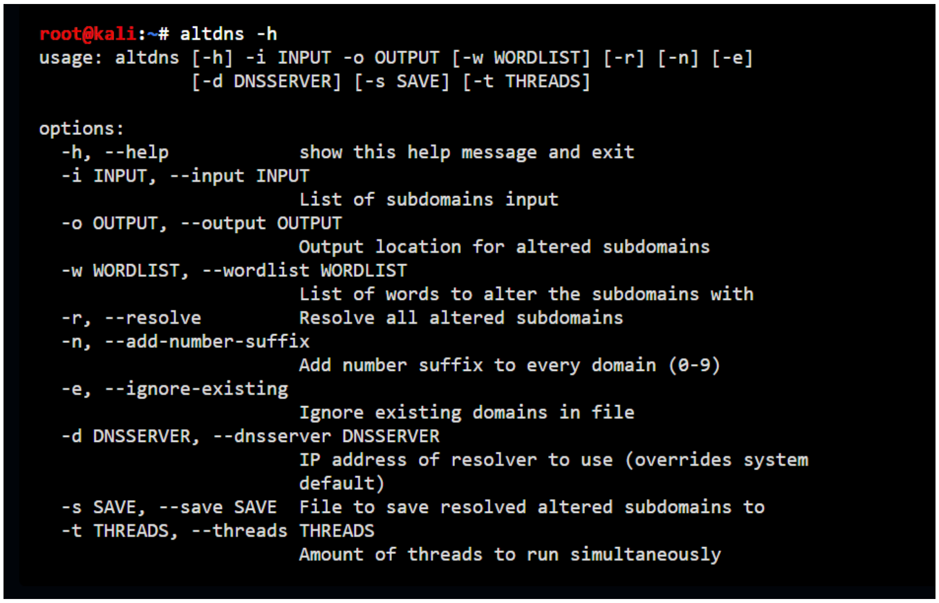
▼ Parameters

- `dns`: DNS subdomain bruteforcing mode.
- `-d`: target domain.
- `-t <n>`: number of concurrent threads (default 10).
- `-w <wordlist>`: path to the wordlist.

10. AltDNS

This package contains a DNS recon tool that allows for the discovery of subdomains that conform to patterns. Altdns takes in words that could be present in subdomains under a domain (such as test, dev, staging) as well as takes in a list of subdomains that you know of.

From these two lists that are provided as input to altdns, the tool then generates a massive output of “altered” or “mutated” potential subdomains that could be present. It saves this output so that it can then be used by your favourite DNS bruteforcing tool.



```
root@kali:~# altdns -h
usage: altdns [-h] -i INPUT -o OUTPUT [-w WORDLIST] [-r] [-n] [-e]
              [-d DNSSERVER] [-s SAVE] [-t THREADS]

options:
  -h, --help            show this help message and exit
  -i INPUT, --input INPUT
                        List of subdomains input
  -o OUTPUT, --output OUTPUT
                        Output location for altered subdomains
  -w WORDLIST, --wordlist WORDLIST
                        List of words to alter the subdomains with
  -r, --resolve         Resolve all altered subdomains
  -n, --add-number-suffix
                        Add number suffix to every domain (0-9)
  -e, --ignore-existing
                        Ignore existing domains in file
  -d DNSSERVER, --dnsserver DNSSERVER
                        IP address of resolver to use (overrides system
                        default)
  -s SAVE, --save SAVE  File to save resolved altered subdomains to
  -t THREADS, --threads THREADS
                        Amount of threads to run simultaneously
```