# GitHub - TheRook/subbrute: A DNS meta-query spider that enumerates DNS records, and subdomains.

By brooksbf

Archived: 2026-04-05 14:36:41 UTC

## subdomain-bruteforcer (SubBrute)

SubBrute is a community driven project with the goal of creating the fastest, and most accurate subdomain enumeration tool. Some of the magic behind SubBrute is that it uses open resolvers as a kind of proxy to circumvent DNS rate-limiting (https://www.us-cert.gov/ncas/alerts/TA13-088A). This design also provides a layer of anonymity, as SubBrute does not send traffic directly to the target's name servers.

## Whats new in v2.1?

Better stablity. Better support for testing cloudflare domains.

Thank you for the bug posts!

## Whats new in v1.2.1?

The big news in this version is that SubBrute is now a recursive DNS-spider, and also a library, more on this later. SubBrute should be easy to use, so the interface should be intuitive (like nmap!), if you would like the interface to change, let us know. In this version we are opening up SubBrute's fast DNS resolution pipeline for any DNS record type. Additionally, SubBrute now has a feature to detect subdomains were their resolution is intentionally blocked, which sometimes happens when a subdomain is intended for for use on an internal network.

- SubBrute is now a DNS spider that recursively crawls enumerated DNS records. This feature boosted *.google.com from 123 to 162 subdomains. (Always enabled)
- --type enumerate an arbitrary record type (AAAA, CNAME, SOA, TXT, MX...)
- -s can now read subdomains from result files.
- New useage - The subdomains enumerated from previous scans can now be used as input to enumerate other DNS records. The following commands demonstrate this new functionality:

```
./subbrute.py google.com -o google.names
        ...162 subdomains found...

./subbrute.py -s google.names google.com --type TXT
        google.com,"v=spf1 include:_spf.google.com ip4:216.73.93.70/31 ip4:216.73.93.72/31 ~all"
        adwords.google.com,"v=spf1 redirect=google.com"
        ...
```

```
./subbrute.py -s google.names google.com --type CNAME
        blog.google.com,www.blogger.com,blogger.l.google.com
        groups.google.com,groups.l.google.com
        ...
```

- SubBrute is now a subdomain enumeration library with a python interface: subbrute.run() Do you want to use SubBrute in your python projects? Consider the following:

```
import subbrute

for d in subbrute.run("google.com"):
        print d
```

Feedback welcome.

## Whats new in v1.1?

This version merges pull requests from the community; changes from JordanMilne, KxCode and rc0r is in this release. In SubBrute 1.1 we fixed bugs, improved accuracy, and efficiency. As requested, this project is now GPLv3.

Accuracy and better wildcard detection:

- A new filter that can pickup geolocation aware wildcards.
- Filter misbehaving nameservers

Faster:

- More than 2,000 high quality nameservers were added to resolvers.txt, these servers will resolve multiple queries in under 1 sec.
- Nameservers are verified when they are needed. A seperate thread is responsible creating a feed of nameservers, and corresponding wildcard blacklist.

New output:

- -a will list all addresses associated with a subdomain.
- -v debug output, to help developers/hackers debug subbrute.
- -o output results to file.

## More Information

names.txt contains 101,010 subdomains. subs_small.txt was stolen from fierce2 which contains 1896 subdomains. If you find more subdomains to add, open a bug report or pull request and I'll be happy to add them.

No install required for Windows, just cd into the 'windows' folder:

- subbrute.exe google.com

Easy to install: You just need http://www.dnspython.org/ and python2.7 or python3. This tool should work under any operating system: bsd, osx, windows, linux...

(On a side note giving a makefile root always bothers me, it would be a great way to install a backdoor...)

Under Ubuntu/Debian all you need is:

- sudo apt-get install python-dnspython

On other operating systems you may have to install dnspython manually:

http://www.dnspython.org/

Easy to use:

- ./subbrute.py google.com

Tests multiple domains:

- ./subbrute.py google.com gmail.com blogger.com

or a newline delimited list of domains:

- ./subbrute.py -t list.txt

Also keep in mind that subdomains can have subdomains (example: _xmpp-server._tcp.gmail.com):

- ./subbrute.py gmail.com > gmail.out
- ./subbrute.py -t gmail.out

Cheers!

---