Pentesting0x

Subfinder

START

By: sudobyter

aliwaleedhum

What's subfinder?

Subfinder, a powerful open-source tool used for subdomain enumeration, which is crucial for cybersecurity assessments, penetration testing, and bug bounty hunting.

Subfinder هي أداة مفتوحة المصدر قوية تُستخدم لتعداد النطاقات الفرعية، وهي حاسمة لتقييمات الأمن السيبراني، اختبار الاختراق، وصيد المكافآت الأمنية.

How to install subfinder?

- GO

```
$_ > go install -v
github.com/projectdiscovery/subfinder/v2/cmd
/subfinder@latest
```

How to configure subfinder?

- Configure the tool

```
$_> vim ~/.config/subfinder/config.yaml
```

How to configure subfinder?

- Configure the tool

```
# subfinder config file
# generated by https://github.com/projectdiscovery/goflags

# domains to find subdomains for
#domain: []

# file containing list of domains for subdomain discovery
#list:

# specific sources to use for discovery (-s crtsh,github). use -ls to display all available sources
#sources: []

# use only sources that can handle subdomains recursively (e.g. subdomain.domain.tld vs domain.tld)
#recursive: false

# use all sources for enumeration (slow)
#all: false

# sources to exclude from enumeration (-es alienvault,zoomeyeapi)
#exclude-sources: []

# subdomain or list of subdomain to match (file or comma separated)
#match: []

#  subdomain or list of subdomain to filter (file or comma separated)
#filter: []

# maximum number of http requests to send per second (global)
#rate-limit: 0

# maximum number of http requests to send per second four providers in key=value format (-rls hacke
#rate-limits: ["github=30/m", "fullhunt=60/m", "robtex=18446744073709551615/ms", "securitytrails=1/
/m", "whoisxmlapi=50/s"]

# number of concurrent goroutines for resolving (-active only)
#t: 10

# update subfinder to latest version
#update: false

# disable automatic subfinder update check
#disable-update-check: false
```

~/.config/subfinder/config.yaml

How to configure subfinder?

- Configure providers

```
$_> vim
~/.config/subfinder/provider-config.yaml
```

How to configure subfinder?

- Insert API keys between brackets

```
#evigil: []
binaryedge: []
bufferover: []
builtwith: []
c99: []
censys: []
certspotter: []
chaos: []
chinaz: []
dnsdb: []
dnsrepo: []
facebook: []
fofa: []
fullhunt: []
github: []
hunter: []
intelx: []
leakix: []
netlas: []
passivetotal: []
quake: []
redhuntlabs: []
robtex: []
securitytrails: []
shodan: []
threatbook: []
virustotal: []
whoisxmlapi: []
zoomeyeapi: []
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~/.config/subfinder/provider-config.yaml
```

Free of cost api's?

- binaryedge
- censys
- certspotter
- chaos
- dnsdb
- github
- intelx
- passivetotal
- robtex

Free of cost api's?

- securitytrails
- shodan
- spyse
- urlscan
- virustotal
- zoomeye

Examples of using subfinder?

- Simple Subdomain Discovery

```
$_ > subfinder -d example.com
```

- Output control

```
$_ > subdfider -d example.com -o output.txt
```

Examples of using subfinder?

- Json OUTPUT

```
$_ > subfinder -d example.com -o output.json -oJ
```

- Using specific Sources

```
$_ > subfinder -d example.com -sources shodan,censys
```

Examples of using subfinder?

- Excluding sources

```
$_ > subfinder -d example.com -exclude-sources archiveis,alienvault
```

- Using API keys for enhanced searching

```
$_ > subfinder -d example.com -all
```

Examples of using subfinder?

- Recursive subdomain discovery

```
$_ > subfinder -d example.com -recursive
```

- Using with a list of domains

```
$_ > subfinder -dL domains.txt -o results.txt
```

Examples of using subfinder?

- Integrating with HTTPX

```
$_ > subfinder -d example.com | httpx
```

- Setting rate limits

```
$_ > subfinder -d example.com -rate-limit 100
```

Examples of using subfinder?

- Random agent selection

```
$_ > subfinder -d example.com -random-agent
```

- Increase concurrency

```
$_ > subfinder -d example.com -t 50
```

Examples of using subfinder?

- Running in Verbose mode

```
$_ > subfinder -d example.com -v
```

- Using docker

```
$_ > docker run -it projectdiscovery/subfinder -d example.com
```

Examples of using subfinder?

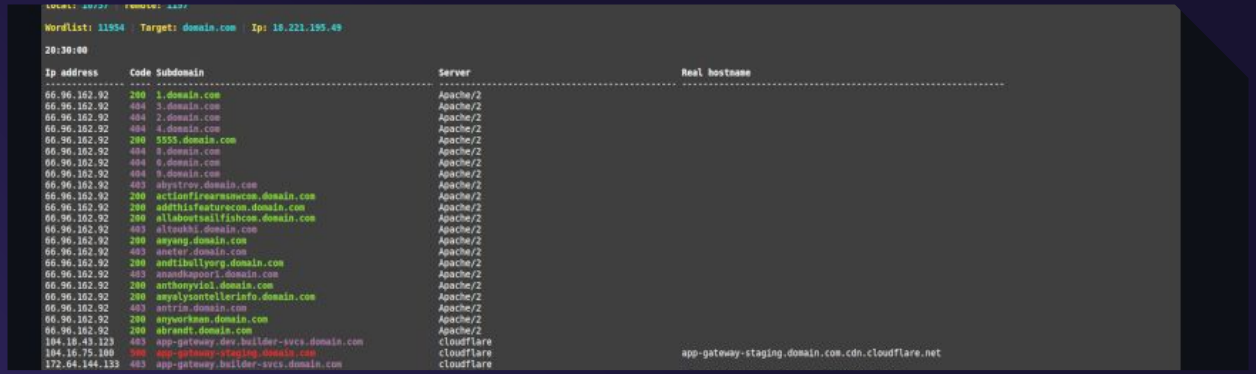
- Subdomain discovery with Resolvers

```
$_ > subfinder -d example.com -r 8.8.8.8,1.1.1.1
```

Github Subfinder

URL

https://github.com/projectdiscovery/subfinder



aliwaleedhum

Y0U C4N
F1ND M3 @T

https://aliwaleed.xyz

sudobyter@gmail.com