Subdomains Enumeration

Summary

- Enumerate all subdomains
    - Subbrute
    - KnockPy
    - GoogleDorks
    - EyeWitness
    - Sublist3r
    - Subfinder
    - Findomain
    - Aquatone (Ruby and Go versions)
    - AltDNS
    - MassDNS
    - Nmap
- Subdomain take over
    - tko-subs
    - HostileSubBruteForcer
    - SubOver

Enumerate all subdomains (only if the scope is *.domain.ext)

Using Subbrute

```
git clone https://github.com/TheRook/subbrute
python subbrute.py domain.example.com
```

Using KnockPy with Daniel Miessler’s SecLists for subdomain "/Discover/DNS"

```
git clone https://github.com/guelfoweb/knock
git clone https://github.com/danielmiessler/SecLists.git
knockpy domain.com -w subdomains-top1mil-110000.txt
```

Using EyeWitness and Nmap scans from the KnockPy and enumall scans

```
git clone https://github.com/ChrisTruncer/EyeWitness.git
./setup/setup.sh
./EyeWitness.py -f filename -t optionaltimeout --open (Optional)
./EyeWitness -f urls.txt --web
./EyeWitness -x urls.xml -t 8 --headless
./EyeWitness -f rdp.txt --rdp
```

Using Google Dorks and Google Transparency Report

You need to include subdomains ;) https://www.google.com/transparencyreport/https/ct/?hl=en-US#domain=[DOMAIN]g&incl_exp=true&incl_sub=true

```
site:*.domain.com -www
site:domain.com filetype:pdf
site:domain.com inurl:'&'
site:domain.com inurl:login,register,upload,logout,redirect,redir,goto,admin
site:domain.com ext:php,asp,aspx,jsp,jspa,txt,swf
site:*.*.domain.com
```

Using Sublist3r

```
To enumerate subdomains of specific domain and show the results in realtime:
python sublist3r.py -v -d example.com

To enumerate subdomains and enable the bruteforce module:
python sublist3r.py -b -d example.com

To enumerate subdomains and use specific engines such Google, Yahoo and Virustotal
engines
python sublist3r.py -e google,yahoo,virustotal -d example.com

python sublist3r.py -b -d example.com
```

Using Subfinder

```
go get github.com/subfinder/subfinder
./Subfinder/subfinder --set-config
PassivetotalUsername='USERNAME',PassivetotalKey='KEY'
./Subfinder/subfinder --set-config RiddlerEmail="EMAIL",RiddlerPassword="PASSWORD"
./Subfinder/subfinder --set-config CensysUsername="USERNAME",CensysSecret="SECRET"
./Subfinder/subfinder --set-config SecurityTrailsKey='KEY'
./Subfinder/subfinder -d example.com -o /tmp/results_subfinder.txt
```

Using Findomain

```
$ wget https://github.com/Edu4rdSHL/findomain/releases/latest/download/findomain-
linux
$ chmod +x findomain-linux
$ findomain_spyse_token="YourAccessToken"
$ findomain_virustotal_token="YourAccessToken"
$ findomain_fb_token="YourAccessToken"
$ ./findomain-linux -t example.com -o
```

Using Aquatone - old version (Ruby)

```
gem install aquatone
```

```
Discover subdomains : results in ~/aquatone/example.com/hosts.txt
aquatone-discover --domain example.com
aquatone-discover --domain example.com --threads 25
aquatone-discover --domain example.com --sleep 5 --jitter 30
aquatone-discover --set-key shodan o1hyw8pv59vSVjrZU3Qaz6ZQqgM91ihQ

Active scans : results in ~/aquatone/example.com/urls.txt
aquatone-scan --domain example.com
aquatone-scan --domain example.com --ports 80,443,3000,8080
aquatone-scan --domain example.com --ports large
aquatone-scan --domain example.com --threads 25

Final results
aquatone-gather --domain example.com
```

Alternatively, you can use the Docker image provided by txt3rob.

```
https://hub.docker.com/r/txt3rob/aquatone-docker/
docker pull txt3rob/aquatone-docker
docker run -it txt3rob/aquatone-docker aq example.com
```

Using Aquatone - new version (Go)

```
# Subfinder version
./Subfinder/subfinder -d $1 -r 8.8.8.8,1.1.1.1 -nW -o /tmp/subresult$1
cat /tmp/subresult$1 | ./Aquatone/aquatone -ports large -out /tmp/aquatone$1

# Amass version
./Amass/amass -active -brute -o /tmp/hosts.txt -d $1
cat /tmp/hosts.txt | ./Aquatone/aquatone -ports large -out /tmp/aquatone$1
```

Using AltDNS

It's recommended to use massdns in order to resolve the result of `AltDNS`

```
WORDLIST_PERMUTATION="./Altdns/words.txt"
python2.7 ./Altdns/altdns.py -i /tmp/inputdomains.txt -o /tmp/out.txt -w
$WORDLIST_PERMUTATION
```

Alternatively you can use goaltdns

Using MassDNS

```
DNS_RESOLVERS="./resolvers.txt"
cat /tmp/results_subfinder.txt | massdns -r $DNS_RESOLVERS -t A -o S -w
/tmp/results_subfinder_resolved.txt
```

Using Nmap

```
nmap -sn --script hostmap-crtsh host_to_scan.tld
```

Subdomain take over

Check Can I take over xyz by EdOverflow for a list of services and how to claim (sub)domains with dangling DNS records.

Using tko-subs

```
go get github.com/anshumanbh/tko-subs
./bin/tko-subs -domains=./lists/domains_tkos.txt -data=./lists/providers-data.csv
```

Using HostileSubBruteForcer

```
git clone https://github.com/nahamsec/HostileSubBruteforcer
chmod +x sub_brute.rb
./sub_brute.rb
```

Using SubOver

```
go get github.com/Ice3man543/SubOver
./SubOver -l subdomains.txt
```

References

- Subdomain Takeover: Proof Creation for Bug Bounties - Patrik Hudak
- Subdomain Takeover: Basics - Patrik Hudak