SCSP
SEASONED CYBER SECURITY PROFESSIONALS

Subdomain Enumeration Cheat Sheet

Follow us @ scspcommunity

Using Subbrute

```
$ python subbrute.py domain.example.com
```

Using KnockPy

```
$ knockpy domain.com -w subdomains-list.txt
```

Using Google Dorks

```
$ 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

```
$ python sublist3r.py -b –v -d example.com –o results.txt
```

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 results.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 Nmap

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

Using Aquatone

```
# 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

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

Using MassDNS

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