CodeNinja a.k.a. Aakash Choudhary

Home About Vulnerability Newsletter Welcome to my website

Bug-Hunting-Day-6

Apr 1, 2019

So, Here is my Day 6 Sumary of my Bug Hunting Track

Day 6 -> Analyzing of Tools and note their documents/usage/guide here

1. Sublist3r ->

https://github.com/aboul3la/Sublist3r

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.

Good Last Updated : 6 Months Ago

Examples

- To list all the basic options and switches use -h switch:

```
python sublist3r.py -h
```

- To enumerate subdomains of specific domain:

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

- To enumerate subdomains of specific domain and show only subdomains which have open ports 80 and 443 :

```
python sublist3r.py -d example.com -p 80,443
```

- 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
```

What Suits to me?

- python3 sublist3r.py -d target_website.com –ports 80,443 -b -t 50 -o ~/Desktop/bounty/Projects/target_site_name/Output/sublist3r_full_with80,443.txt
- python3 sublist3r.py -d target_website.com –ports 80,443 -b -t 50 -e dnsdumpster,yahoo -o ~/Desktop/bounty/Projects/target_site_name/Output/sublist3r_with_dnsdumpster_yahoo_80,443.txt

Engines List =>

- baidu,
- yahoo,
- google,
- bing,
- ask,
- netcraft,
- dnsdumpster,
- virustotal,
- threatcrowd,
- ssl,
- passivedns

---

1. Amass

https://github.com/OWASP/Amass

- **DNS:** Basic enumeration, Brute forcing (upon request), Reverse DNS sweeping, Subdomain name alterations/permutations, Zone transfers (upon request)
- **Scraping:** Ask, Baidu, Bing, CommonCrawl, DNSDB, DNSDumpster, DNSTable, Dogpile, Exalead, FindSubdomains, Google, IPv4Info, Netcraft, PTRArchive, Riddler, SiteDossier, ThreatCrowd, VirusTotal, Yahoo
- **Certificates:** Active pulls (upon request), Censys, CertDB, CertSpotter, Crtsh, Entrust
- **APIs:** BinaryEdge, BufferOver, CIRCL, HackerTarget, PassiveTotal, Robtex, SecurityTrails, Shodan, Twitter, Umbrella, URLScan
- **Web Archives:** ArchiveIt, ArchiveToday, Arquivo, LoCArchive, OpenUKArchive, UKGovArchive, Wayback

---

Basic Usage

1. amass -d
2. amass -src -ip -brute -min-for-recursive 3 -d
3. amass -src -ip -brute -min-for-recursive 3 -d ,,

We will need a config file to use your API keys with Amass Ok, I have many API Keys, lets see how many keys it needing in **amass_config.ini** file

- ** censys **
- ** certdb**
- ** Shodan**

Well there is more.

Flags Interesting for me ->

- -active [Enable active Recon Method]
- -brute [Bruteforce]
- -d [Domain]
- -do [Write all the data operations to a JSON file]
- -ip [Print IP addresses with the discovered names]
- -json [All discoveries written as individual JSON objects]
- -passive [A purely passive mode of execution]
- -oA [Output to all available file formats with prefix]
- -w [Wordlist]

Speedy Work -> -noalts -norecursive -passive

Awesome Resource : https://miloserdov.org/?p=2309 https://moretip.com/amass-in-depth-subdomain-enumeration/

Dictionaries to brute-force subdomains

I have all of these following wordlists in /opt/wordlists Directory

- all.txt
- asnlist.txt
- bitquark_subdomains_top100K.txt
- deepmagic.com_top500prefixes.txt
- deepmagic.com_top50kprefixes.txt
- fierce_hostlist.txt
- jhaddix_all.txt
- namelist.txt
- nameservers.txt
- sorted_knock_dnsrecon_fierce_recon-ng.txt
- subdomains.lst
- subdomains-top1mil-110000.txt
- subdomains-top1mil-20000.txt
- subdomains-top1mil-5000.txt
- user_agents.txt

Commands for mine Interest ->

1. amass -d -v -b -ip -w -noalts -passive -whois -o ~/Desktop/bounty/Projects/target-name/Output/amass-result-passive-whois.txt
2. amass -d -v -ip -b -w -o ~/Desktop/bounty/Projects/target-name/Output/amass-result.txt
3. amass -active -d web -p 80,443,8080 -oA ~/Desktop/bounty/Projects/target-name/Output/amass-with-port-result

1. Knockpy

https://github.com/guelfoweb/knock

It is designed to scan for **DNS zone transfer** and to try to bypass the **wildcard DNS record** automatically if it is enabled. Now knockpy supports queries to VirusTotal subdomains, you can setting the API_KEY within the config.json file.

Great, So, this needing API Key of Virustotal

#Commands

1. knockpy domain.com [Internal wordlist]
2. knockpy domain.com -w wordlist.txt [External Wordlist]
3. knockpy -r domain.com [or IP] [Resolve domain name and get response header]
4. knockpy -c domain.com [Save in CSV]
5. knockpy -j domain.com [Export in JSON]

---

1. Domained Multi Tool Subdomain Enumeration

https://github.com/cakinney/domained

Domained is a multi tool subdomain enumeration tool that uses several subdomain enumeration tools and wordlists to create a unique list of subdomains that are passed to EyeWitness for reporting.

Command Examples ->

1. domained.py -d example.com [Sublist3r (+subbrute), enumall, Knock, Amass, and SubFinder]
2. domained.py -d example.com -b -p –vpn[with seclist subdomain list bruteforcing (massdns, subbrute, Sublist3r, Amass, enumall, and SubFinder), adds ports 8443/8080 and checks if on VPN]
3. domained.py -d example.com -b –bruteall [with large-all.txt bruteforcing (massdns, subbrute, Sublist3r, Amass, enumall and SubFinder)]
4. domained.py -d example.com –quick [only Amass and SubFinder]
5. domained.py -d example.com –noeyewitness [No eyewitness]
6. domained.py -d example.com –active [Eyewitness Active Scan]

I will wait more to use this tool

---

1. Aquatone

https://github.com/michenriksen/aquatone

Aquatone is a tool for visual inspection of websites across a large amount of hosts and is convenient for quickly gaining an overview of HTTP-based attack surface.

Useful Commands

There are many commands but following one is for my interest

-

cat hosts.txt	aquatone -out ~/Desktop/bounty/Projects/target-name/Output/aquatone-result -ports 80,443,8080 -threads 20

Or we can use -small,large,medium,xlarge for ports options

- **small**: 80, 443
- **medium**: 80, 443, 8000, 8080, 8443 (same as default)
- **large**: 80, 81, 443, 591, 2082, 2087, 2095, 2096, 3000, 8000, 8001, 8008, 8080, 8083, 8443, 8834, 8888
- **xlarge**: 80, 81, 300, 443, 591, 593, 832, 981, 1010, 1311, 2082, 2087, 2095, 2096, 2480, 3000, 3128, 3333, 4243, 4567, 4711, 4712, 4993, 5000, 5104, 5108, 5800, 6543, 7000, 7396, 7474, 8000, 8001, 8008, 8014, 8042, 8069, 8080, 8081, 8088, 8090, 8091, 8118, 8123, 8172, 8222, 8243, 8280, 8281, 8333, 8443, 8500, 8834, 8880, 8888, 8983, 9000, 9043, 9060, 9080, 9090, 9091, 9200, 9443, 9800, 9981, 12443, 16080, 18091, 18092, 20720, 28017

Api keys :-> .keys.yml

```
shodan: %APIKEY%
passivetotal_key: %EMAIL%
passivetotal_secret: %SECRET%
censys_id: %ID%
censys_secret: %SECRET%
riddler_username: %EMAIL%
riddler_password: %ACCOUNT PASSWORD%
virustotal: %APIKEY%
```

Output

When Aquatone is done processing the target hosts, it has created a bunch of files and folders in the current directory:

- **aquatone_report.html**: An HTML report to open in a browser that displays all the collected screenshots and response headers clustered by similarity.
- **aquatone_urls.txt**: A file containing all responsive URLs. Useful for feeding into other tools.
- **headers/**: A folder with files containing raw response headers from processed targets
- **html/**: A folder with files containing the raw response bodies from processed targets. If you are processing a large amount of hosts, and don't need this for further analysis, you can disable this with the `-save-body=false` flag to save some disk space.
- **screenshots/**: A folder with PNG screenshots of the processed targets

1. Subffinder

https://github.com/subfinder/subfinder

using passive online sources successor to sublist3r project

API keys -> /.config/subfinder/config.json

```
PassivetotalUsername
PassivetotalKey
SecurityTrailsKey
RiddlerEmail
RiddlerPassword
CensysUsername
CensysSecret
ShodanAPIKey
```

Useful Commands

1. ./subfinder -d freelancer.com -oD ~/Desktop/bounty/Projects/target-name/Output/subfinder-output.txt/.json -b -w wordlist.txt -t 100 -v
2. ./subfinder -d freelancer.com -oD ~/Desktop/bounty/Projects/target-name/Output/subfinder-output.txt/.json -b -w wordlist.txt -t 100 -nW -oT [For Aquatone] -v