Domain Discovery
Expanding your scope like a boss
whoami

⭐ Jason Haddix - @jhaddix

⭐ Head of Trust and Security @Bugcrowd

⭐ 2014-2015 top hunter on Bugcrowd (59 currently)

⭐ Father, hacker, blogger, gamer!
### ASN’s

**Autonomous System Number** - http://bgp.he.net

---

**Search Results**

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AS851602</td>
<td>AD Aerodrom 'Nikola Tesla' Beograd</td>
</tr>
<tr>
<td>AS47988</td>
<td>Tesla stedna banka d.d.</td>
</tr>
<tr>
<td>AS394161</td>
<td>Tesla Motors, Inc.</td>
</tr>
<tr>
<td>91.208.233.0/24</td>
<td>Tesla stedna banka d.d.</td>
</tr>
<tr>
<td>66.242.48.0/22</td>
<td>Toledo Tesla (C05787700)</td>
</tr>
<tr>
<td>209.133.79.0/24</td>
<td>Tesla Motors, Inc.</td>
</tr>
<tr>
<td>203.31.21.0/24</td>
<td>Tesla Engineering Group</td>
</tr>
<tr>
<td>194.24.249.0/24</td>
<td>AD Aerodrom 'Nikola Tesla' Beograd</td>
</tr>
<tr>
<td>194.24.248.0/24</td>
<td>AD Aerodrom 'Nikola Tesla' Beograd</td>
</tr>
<tr>
<td>141.101.350.0/24</td>
<td>LLC &quot;TESLA&quot;</td>
</tr>
</tbody>
</table>

---

**Prefix**

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tesla Motors, Inc.</td>
</tr>
</tbody>
</table>

---

Updated: 20 July 2017 03:05 PDT © 2017 Hurricane Electric
**Rev whois**

**ViewDNS.info**

Tools > Reverse Whois Lookup

This free tool will allow you to find domain names owned by an individual person or company. Simply enter the email address or name of the person or company to find other domains registered using those same details. FAQ.

Register Name or Email Address:

Reverse Whois results for tesla motors

There are 824 domains that matched this search query. The first 500 of these are listed below:

- **Domain Name**  | **Creation Date**  | **Registrar**
- aoecharging.com    | 2007-08-31         | MARKMONITOR INC.
- aoecharging.org    | 2007-08-31         | MARKMONITOR INC.
- aoecharging.com    | 2007-08-31         | MARKMONITOR INC.
- aoecharging.org    | 2007-08-31         | MARKMONITOR INC.
- arrendadorsteela.co.uk | 2014-07-18    | MARKMONITOR INC. T/A MARKMONITOR INC. [TAG = MARKMONITOR]
- backgrounddatasetsequencingfirm.com | 2012-08-21 | MARKMONITOR INC.
- bancotesla.co.uk   | 2014-07-18         | MARKMONITOR INC. T/A MARKMONITOR INC. [TAG = MARKMONITOR]
- chinatesla.cn       | 2007-06-09         | MARKMONITOR INC.
- chinateslas.com.cn  | 2007-06-09         | MARKMONITOR INC.
- chinateslaf.com     | 2007-06-09         | MARKMONITOR INC.
- chinateslaf.com.cn  | 2007-06-09         | MARKMONITOR INC.
- chinateslaf.com.cn  | 2007-06-09         | MARKMONITOR INC.
- chinateslaf.com.cn  | 2007-06-09         | MARKMONITOR INC.
- chinateslaf.com.cn  | 2007-06-09         | MARKMONITOR INC.
<table>
<thead>
<tr>
<th>crt.sh</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Certificate Transparency</td>
</tr>
<tr>
<td>OpenSSL SAN (Subject Alternative Name)</td>
</tr>
</tbody>
</table>
## Sub Scraping

<table>
<thead>
<tr>
<th>RECON-NG/ENUMALL</th>
<th>BOTH</th>
<th>SUBLIST3R</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSLtools.com API</td>
<td>Google (Recon-ng now handles captcha)</td>
<td>Baidu</td>
</tr>
<tr>
<td>HackerTarget.com API</td>
<td>Bing</td>
<td>Ask</td>
</tr>
<tr>
<td>Shodan</td>
<td>Crt.sh</td>
<td>DNSDumpster (scans.io)</td>
</tr>
<tr>
<td></td>
<td>ThreatCrowd</td>
<td>Virustotal</td>
</tr>
<tr>
<td>Zoomeye (not core)</td>
<td>Netcraft</td>
<td>Ptrarchive.com</td>
</tr>
<tr>
<td>ThreatCrowd regged by email (not core)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Zone transfer (not core)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RiskIQ API (not core)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Censys.io (not core)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Scraping - Sublist3r

about3la / Sublist3r

- Code
- Issues 21
- Pull requests 4
- Projects

Fast subdomains enumeration tool for penetration testers
Some configuration required

- Update Docker image with non-core recon-ng modules
- .env file
- Disable Bruteforce (see why next...)
Sub Scraping (bespoke)

Cloudflare DNS Enumeration Tool for Pentesters

Quick and Dirty script to use the Censys API to query subdomains of a target domain

Cloudflare
Censys.io
Haven’t tested but love the ideas

```
mandatory@mandatory-box ~/cloudflare_enum> ./cloudflare_enum.py thehackerblog@opmail.com Testing1 disney.com
[ STATUS ] Logging in to Cloudflare...
[ SUCCESS ] Login was successful!
[ STATUS ] Adding domain to Cloudflare...
[ SUCCESS ] Querying Cloudflare DNS archives...
A: disney.com -> 199.181.132.249
A: api.disney.com -> 96.45.49.200
A: app.disney.com -> 208.218.3.17
A: apps.disney.com -> 199.181.132.250
A: archive.disney.com -> 198.105.199.57
A: archives.disney.com -> 199.181.132.250
A: data.disney.com -> 10.190.71.248
A: feeds.disney.com -> 198.105.197.192
A: home.disney.com -> 199.181.132.250
A: huey.disney.com -> 204.128.192.10
A: localhost.disney.com -> 127.0.0.1
A: louie.disney.com -> 204.128.192.30
A: mail2.disney.com -> 204.128.192.16
A: mail.disney.com -> 204.128.192.15
A: m.disney.com -> 199.181.132.250
A: mx1.disney.com -> 192.195.66.26
A: mx1.disney.com -> 204.128.192.17
A: mx2.disney.com -> 192.195.66.28
A: mx2.disney.com -> 204.128.192.36
A: services.disney.com -> 204.202.143.170
A: services.disney.com -> 204.202.143.171
A: webcache.disney.com -> 204.128.192.55
A: webcast.disney.com -> 207.177.177.41
A: www1.disney.com -> 199.181.132.250
A: www2.disney.com -> 199.181.132.250
CNAME: code.disney.com -> matterhorn.disney.com
```
Sub Bruting

1,136,964 LINE SUBDOMAIN DICTIONARY (ALL.TXT)

<table>
<thead>
<tr>
<th>Tool</th>
<th>Time to run</th>
<th>Threads</th>
<th>Found</th>
</tr>
</thead>
<tbody>
<tr>
<td>subbrute</td>
<td>errored</td>
<td>100</td>
<td>0</td>
</tr>
<tr>
<td>gobuster</td>
<td>21m15.857s</td>
<td>100</td>
<td>87</td>
</tr>
<tr>
<td>massdns</td>
<td>1m24.167</td>
<td>n/a</td>
<td>213</td>
</tr>
<tr>
<td>dns-parallel-prober</td>
<td>42m2.868s</td>
<td>100</td>
<td>43</td>
</tr>
<tr>
<td>blacksheepwall</td>
<td>256m9.385s</td>
<td>100</td>
<td>61</td>
</tr>
</tbody>
</table>

1,136,964 line subdomain dictionary (all.txt)
Sub Bruting

With MassDNS, why not all of them?

ALL.TXT

HTTPS://GIST.GITHUB.COM/JHADDIX/86A06C5DC309D08580A018C66354A056

A high-performance DNS stub resolver for bulk lookups
Permutation Scanning

Altdns: https://github.com/infosec-au/altdns
**Permutation Scanning**

**SDBF:** Smart DNS Brute-Forcer approach is based on techniques derived from natural language modeling and leverage Markov Chain Models in order to build the first DNS scanner (SDBF) that is leveraging both, training and advanced language modeling approaches.

https://github.com/jfrancois/SDBF

### Port Scanning

**65536 Unverified Hosts (a Large Targets ASN)**

<table>
<thead>
<tr>
<th>Tool</th>
<th>Time to run</th>
<th>Found</th>
</tr>
</thead>
<tbody>
<tr>
<td>masscan</td>
<td>11m4.164s</td>
<td>196</td>
</tr>
</tbody>
</table>

You can use a conf file for this!

| Nmap        | ∞                    | ZZZ    |

```bash
$TARGET_LIST --max-rate 100000 -oG $TARGET_OUTPUT
```
Visual Identification

Because of the nature of scraping and DNS redirects, some sites will be gone or the same.

Gotta get an idea of what is up and unique.

We also don't know what protocol these are on (HTTP vs HTTPS, ++).
Auxiliary

★ DNSSEC / NSEC / NSEC3 Walking
  ○ ldnsutils, nsec3walker, nsec3map

★ Github Recon
  ○ Search for goodies

★ Burp Suite Scope Filters
  ○ Simple and effective
  ○ Start with target, spider, scope down to keywords, repeat

★ Dorking: ads key, priv pol, tos, aws, s3

ESOTERIC SUB-DOMAIN ENUMERATION TECHNIQUES

BHARATH KUMAR
BUGCROWD LEVELUP | JULY 15TH 2017

iques.pdf

https://www.youtube.com/watch?v=1Kg0_53ZEq8
Auxiliary DEMO – BURP
Platform Identification and CVE searching

- **Retire.js**
  - What you require you must also retire

- **Wappalyzer**

- **built with**

- **OpenGSE**
  - Web Server
  - Java
    - Programming Language
Content Discovery / Directory Bruting

- Seclists / RAFT / Digger wordlists
- Patator
- WPScan
- CMSMap

- Gobuster
- Burp content discovery
- Robots disallowed
  "\_(ツ)_/"
Parameter Bruting?

★  YES! - Untested but love the idea
★
CAN BE COMBINED WITH BACKSLASH SCANNERS TOP 2500 PARAMS

maK- / parameth

This tool can be used to brute discover GET and POST parameters

```bash
parameth/mak#/ ./parameth.py -u https://makthepla.net/parameth/simpletest.php
```

parameth v1.0 - find parameters and craig rocks
Author: Ciaran McNally - https://makthepla.net

Establishing base figures...
GET: content-length-> 22 status-> 200
POST: content-length-> 22 status-> 200
Scanning it like you own it...
GET(size): m | 22 ->36 ( https://makthepla.net/parameth/simpletest.php?m=discobiscuits )
POST(size): r | 22 ->42 ( https://makthepla.net/parameth/simpletest.php )
parameth/mak#
Automation?

Somewhat
Best-in-breed tools/sites change, automation needs to support bespoke tooling

HODOR:
- A security testing Slackbot built with a Kubernetes backend on the Google Cloud Platform

Kubebot:
- A security testing Slackbot built with a Kubernetes backend on the Google Cloud Platform

Assetnote

Datasploit & intrigue

---

**Assetnote**

Note: The public version of assetnote is a proof-of-concept. Feel free to use it, but I provide no warranty or support for this project.

Assetnote notifies you of assets that have been found through scraping passive data stores. By using Pushover's push notification API, as soon as a new subdomain is found for an asset, a push notification is sent to your mobile phone (iOS/Android) with the data found.

For public release, I have included an example `manager` script for assetnote. This is Threatcrowd's public yet passive DNS data store. Assetnote can be extended very easily by writing scripts that interact with the `assetnote.db` SQLite database. The more scripts that have been made to scrape data sources, the more success one will have with this tool.

Assetnote was created mainly for bug bounties, to assist with finding bugs before others do. You get a push notification that a new subdomain has been put online, you're now probably one of the first people to know of this new asset. This means fewer duplicate findings and a higher success rate in finding security flaws in an organization.