

```
root@kali: ~/Desktop/tools/Sublist3r# python sublist3r.py -d tesla.com
```

Sublist3r

Coded By Ahmed Aboul-Ela - @aboul3la

```
[*] Enumerating subdomains now for tesla.com
[*] Searching now in Baidu..
[*] Searching now in Yahoo..
[*] Searching now in Google..
[*] Searching now in Bing..
[*] Searching now in Ask..
[*] Searching now in Netcraft..
[*] Searching now in DNSdumpster..
[*] Searching now in Virustotal..
[*] Searching now in ThreatCrowd..
[*] Searching now in SSL Certificates..
[*] Searching now in PassiveDNS..
[!] Error: Google probably now...
[*] Finished now the Google...
[*] Total Unique Subdomains Found: 36
```

```
www.tesla.com
auth.tesla.com
autodiscover.tesla.com
blog.tesla.com
comparison.tesla.com
dev.tesla.com
eua-origin.tesla.com
forums.tesla.com
imap.tesla.com
ir.tesla.com
lyncdiscover.tesla.com
model3.tesla.com
my.tesla.com
naa-origin.tesla.com
nas-origin.tesla.com
new.tesla.com
new-dev.tesla.com
partners.tesla.com
pop.tesla.com
powerwall.tesla.com
resources.tesla.com
shop.tesla.com
```

Domain Discovery

Expanding your scope like a boss



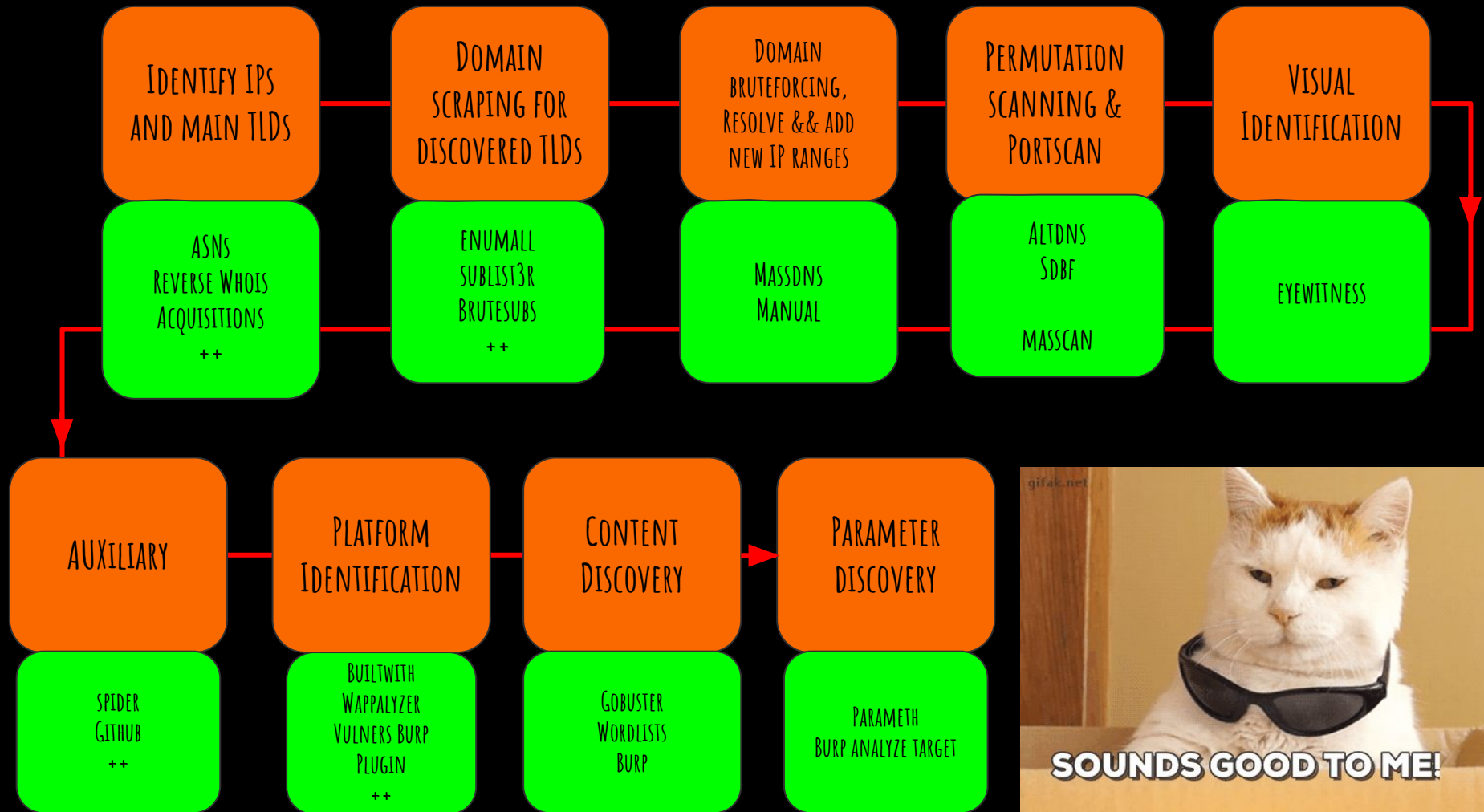
whoami

- ★ JASON HADDIX - @JHADDIX
- ★ HEAD OF TRUST AND SECURITY @BUGCROWD
- ★ 2014-2015 TOP HUNTER ON BUGCROWD (59 CURRENTLY)
- ★ FATHER, HACKER, BLOGGER, GAMER!



PLAYERUNKNOWN'S
BATTLEGROUNDS





★ AUTONOMOUS SYSTEM NUMBER - [HTTP://BGP.HE.NET](http://bgp.he.net)


HURRICANE ELECTRIC
 INTERNET SERVICES

Quick Links
[BGP Toolkit Home](#)
[BGP Prefix Report](#)
[BGP Peer Report](#)
[Exchange Report](#)
[Bogon Routes](#)
[World Report](#)
[Multi Origin Routes](#)
[DNS Report](#)
[Top Host Report](#)
[Internet Statistics](#)
[Looking Glass](#)
[Network Tools App](#)
[Free IPv6 Tunnel](#)
[IPv6 Certification](#)
[IPv6 Progress](#)
[Going Native](#)
[Contact Us](#)

Search Results

Result	Description
AS51602	AD Aerodrom 'Nikola Tesla' Beograd 
AS47988	Tesla stedna banka d.d. 
AS394161	Tesla Motors, Inc. 
91.208.233.0/24	Tesla stedna banka d.d. 
66.242.48.0/22	Toledo Tesla (C05787700)
209.133.79.0/24	Tesla Motors, Inc.
203.31.23.0/24	Tesla Engineering Group 
194.24.249.0/24	AD Aerodrom 'Nikola Tesla' Beograd 
194.24.248.0/24	AD Aerodrom 'Nikola Tesla' Beograd 
141.101.246.0/24	LLC "TESLA" 




Updated 28 Jul 2017 03:05 PST © 2017 Hurricane Electric.

AS394161 Tesla Motors, Inc.

[Tools](#)
[Home](#)
[Report](#)
[Report](#)
[s](#)

[AS Info](#)
[Graph v4](#)
[Prefixes v4](#)
[Peers v4](#)
[Whois](#)
[IRR](#)

Prefix	Description
209.133.79.0/24	Tesla Motors, Inc.

Rev whois



[HTTP://VIEWDNS.INFO/](http://viewdns.info/)



[HTTP://DOMAINBIGDATA.COM/](http://domainbigdata.com/)

DomainBigData

Search any domain, ip, registrant name / email



Names /

Tesla Motors

List of domain names registered by **Tesla Motors**

Domain Name	Create Date	Registrar
telsamotors.jp	2007-02-03	
teslalifestyle.com	2012-11-06	markmonitor.com
thetelalife.com	2012-07-02	markmonitor.com
teslamotors.com	2003-04-03	markmonitor.com
acecharging.com	2007-08-31	markmonitor.com
acechargingsystem.com	2007-08-31	markmonitor.com
poweredbyt.com	2010-06-28	markmonitor.com
service-ranger.com	2010-06-14	markmonitor.com
smilap.net	2015-03-07	markmonitor.com

viewdns.info/reversewhois/?q=tesla+motors



Viewdns.info

Tools

API

Research

Data

[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](#).

Registrant 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:

[Download The Full Report for \\$49](#)

Domain Name	Creation Date	Registrar
acecharging.com	2007-08-31	MARKMONITOR INC.
acecharging.org	2007-08-31	MARKMONITOR INC.
acechargingsystem.com	2007-08-31	MARKMONITOR INC.
acechargingsystem.org	2007-08-31	MARKMONITOR INC.
arrendadoratesla.co.uk	2014-07-18	MARKMONITOR INC. T/A MARKMONITOR INC. [TAG = MARKMONITOR]
backgrounddatasequencingfirm.com	2012-08-21	MARKMONITOR INC.
bancotesla.co.uk	2014-07-18	MARKMONITOR INC. T/A MARKMONITOR INC. [TAG = MARKMONITOR]
chinatesta.cn	2007-06-09	MARKMONITOR INC.
chinatesta.com.cn	2007-06-09	MARKMONITOR INC.
chinatesta.com	2007-06-09	MARKMONITOR INC.
chinatestamotors.cn	2007-06-09	MARKMONITOR INC.
chinatestamotors.com.cn	2007-06-09	MARKMONITOR INC.
chinatestamotors.com	2007-06-09	MARKMONITOR INC.

Acquisitions

★ CRUNCHBASE

★ PROTECTED BY
DISTIL BOT
PROTECTION

★ STAY TUNED

Secure <https://www.crunchbase.com/organization/tesla-motors/acquisitions>

Look up a specific company, person, investor, or event

Tesla

Overview Timeline Contributors



ADD TO LIST

Acquisitions (3)

UPDATE

Date	Acquired	Amount
Nov 8, 2016	Grohmann Engineering	Unknown
Jun 22, 2016	SolarCity	\$2.6B in Stock
May 8, 2015	Riviera Tool	Unknown

TOP CONTRIBUTORS

ADD TO THIS PROFILE

CONTRIBUTE

Sub Scraping



crt.sh
Google Certificate Transparency
OpenSSL SAN (Subject Alternative Name)

Sub Scraping

RECON-NG/ENUMALL	BOTH	SUBLIST3R
SSLTOOLS.COM API	GOOGLE (RECON-NG NOW HANDLES CAPTCHA)	BAIDU
HACKERTARGET.COM API	BING	ASK
SHODAN	CRT.SH	DNSDUMPSTER (SCANS.IO)
	THREATCROWD	VIRUSTOTAL
<u>ZOOMYEYE</u> (NOT CORE)	NETCRAFT	PTRARCHIVE.COM
<u>THREATCROWD REGGED BY EMAIL</u> (NOT CORE)		
<u>ZONE TRANSFER</u> (NOT CORE)		
<u>RISKIQ API</u> (NOT CORE)		
<u>CENSYS.IO</u> (NOT CORE)		

Scraping - Sublist3r

about3la / Sublist3r

Code

Issues 21

Pull requests 4

Projects

Fast subdomains enumeration tool for penetration testers



```
root@kali:~/Desktop/tools/Sublist3r# python sublist3r.py -d tesla.com
```

CTF



Home



tools



php-reverse-shell.php



Trash

```
root@kali:~/Desktop/tools/brutesubs# docker
```

Home
tools
php-reverse-shell.php
Trash

anshumanbh / brutesubs

Watch 9 Star 63 Fork 15

Code Issues 1 Pull requests 0 Projects 0 Wiki Insights

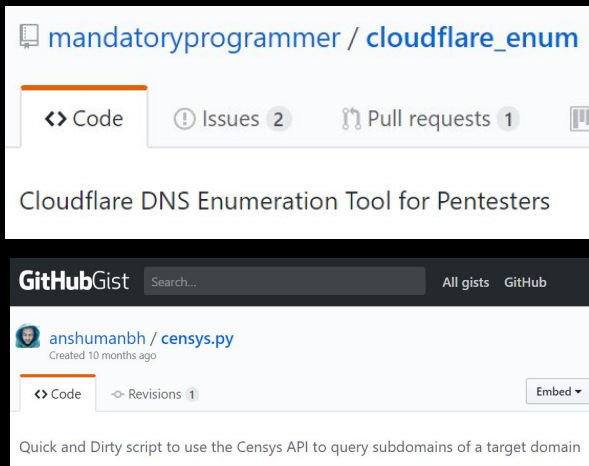
An automation framework for running multiple open sourced subdomain bruteforcing tools (in parallel) using your own wordlists via Docker Compose



SOME CONFIGURATION REQUIRED

- UPDATE DOCKER IMAGE WITH NON CORE RECON-NG MODULES
- .ENV FILE
- DISABLE BRUTEFORCE (SEE WHY NEXT...)

Sub Scraping (bespoke)



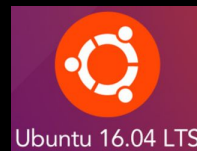
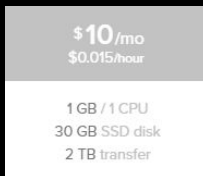
★ CLOUDFLARE
★ CENSYS.IO
★ HAVEN'T TESTED BUT LOVE
THE IDEAS

```
mandatory@mandatorys-box /t/cloudflare_enum> ./cloudflare_enum.py thehackerblog@yopmail.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: huey11.disney.com -> 192.195.66.12
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)

Tool	Time to run	Threads	Found
subbrute time ./subbrute.py -c 100 all.txt \$TARGET.com tee subbrute.output	errored	100	0
gobuster time gobuster -m dns -u \$TARGET.com -t 100 -w all.txt	21m15.857s	100	87
massdns time ./subbrute.py /root/work/bin/all.txt \$TARGET.com ./bin/massdns -r resolvers.txt -t A -a -o -w massdns_output.txt -	1m24.167	n/a	213
dns-parallel-prober time python dns-queue.py \$TARGET.com 100 \$TARGET_outputfile -i /root/work/bin/all.txt	42m2.868s	100	43
blacksheepwall time ./blacksheepwall_linux_amd64 -clean -dictionary /root/work/bin/all.txt -domain \$TARGET.com	256m9.385s	100	61



Sub Bruting

WITH MASSDNS, WHY NOT ALL OF THEM?

ALL.TXT

[HTTPS://GIST.GITHUB.COM/JHADDIX/86A06C5DC309D08580A018C66354A056](https://gist.github.com/jhaddix/86a06c5dc309d08580a018c66354a056)



 bluto_lots-of-spinach.txt	6/4/2017 9:42 PM	TXT File	1,946 KB
 deepmagic.com_top50kprefixes.txt	8/20/2015 2:58 PM	TXT File	592 KB
 deepmagic.com_top500prefixes.txt	8/20/2015 2:58 PM	TXT File	4 KB
 dns_raft-large-words-lowercase.txt	6/4/2017 9:56 PM	TXT File	920 KB
 dns_top_1000000_RobotsDissalowed.txt	6/4/2017 10:23 PM	TXT File	1,578 KB
 dnscan_subdomains.txt	7/31/2016 3:00 PM	TXT File	5 KB
 dnscan_subdomains-100.txt	7/31/2016 3:00 PM	TXT File	1 KB
 dnscan_subdomains-500.txt	7/31/2016 3:00 PM	TXT File	3 KB
 dnscan_subdomains-1000.txt	7/31/2016 3:00 PM	TXT File	6 KB
 dnscan_subdomains-10000.txt	7/31/2016 3:00 PM	TXT File	62 KB
 dnscan_subdomains-uk-500.txt	7/31/2016 3:00 PM	TXT File	4 KB
 dnscan_subdomains-uk-1000.txt	7/31/2016 3:00 PM	TXT File	7 KB
 dnscan_suffixes.txt	7/31/2016 3:00 PM	TXT File	36 KB
 dnscan_tlds.txt	7/31/2016 3:00 PM	TXT File	9 KB
 dnsenum_dns.txt	6/4/2017 9:24 PM	TXT File	15 KB
 dnspop_bitquark_20160227_subdomains_popular_1000.txt	3/10/2016 3:47 PM	TXT File	5 KB
 dnspop_bitquark_20160227_subdomains_popular_10000.txt	3/10/2016 3:47 PM	TXT File	92 KB
 dnspop_bitquark_20160227_subdomains_popular_100000.txt	3/10/2016 3:47 PM	TXT File	1,393 KB
 dnspop_bitquark_20160227_subdomains_popular_1000000.txt	3/10/2016 3:47 PM	TXT File	11,371 KB
 dnsrecon_meatasploit_standard_namelist.txt	5/19/2017 3:06 AM	TXT File	12 KB
 dnsrecon_subdomains-top1mil-5000.txt	1/16/2017 6:03 PM	TXT File	33 KB
 dnsrecon_subdomains-top1mil-20000.txt	1/16/2017 6:03 PM	TXT File	146 KB
 dnsrecon_subdomains-top1mil-110000.txt	1/16/2017 6:03 PM	TXT File	1,092 KB
 ethicalhack3r_subdomains.txt	6/4/2017 9:30 PM	TXT File	6 KB
 fierce_hostlist.txt	8/20/2015 2:58 PM	TXT File	15 KB
 hostilebruteforcer.txt	6/4/2017 9:32 PM	TXT File	22 KB
 knock_wordlist.txt	2/3/2017 5:01 AM	TXT File	12 KB
 master.txt	5/19/2017 3:31 AM	TXT File	2,149 KB
 nmap_vhosts-default.lst.txt	5/19/2017 3:08 AM	TXT File	1 KB
 recon-ng_hostnames.txt	5/19/2017 3:04 AM	TXT File	12 KB
 reverseraider_fast.list.txt	12/25/2008 2:07 AM	TXT File	1 KB
 reverseraider_services.list.txt	10/4/2008 10:07 AM	TXT File	4 KB
 reverseraider_word.list.txt	9/25/2008 5:21 PM	TXT File	728 KB
 sorted_knock_dnsrecon_fierce_recon-ng.txt	1/16/2017 6:03 PM	TXT File	904 KB
 subbrute_names.txt	2/12/2017 10:49 AM	TXT File	890 KB

Permutation Scanning

ALTDNS : [HTTPS://GITHUB.COM/INFOSEC-AU/ALTDNS](https://github.com/infosec-au/altdns)

```
➤ ~/altdns cat resolved_results
```

```
acs.t[REDACTED].com:acs-[REDACTED].us-west-2.elb.amazonaws.com.  
test.[REDACTED].com:ec2-[REDACTED] us-west-1.compute.amazonaws.com.  
apollo.[REDACTED].com:[REDACTED]  
enigma.[REDACTED].com:internal-[REDACTED].us-west-2.elb.amazonaws.com.  
am.[REDACTED].com:internal-[REDACTED].us-west-2.elb.amazonaws.com.  
cn.[REDACTED]:[REDACTED]05399.ap-northeast-1.elb.amazonaws.com.  
events.[REDACTED].com:events [REDACTED].s3-website-us-west-2.amazonaws.com.  
ava.[REDACTED].com:internal [REDACTED].us-west-2.elb.amazonaws.com.  
cdn.[REDACTED].com:internal-[REDACTED].us-west-2.elb.amazonaws.com.  
fantasy.[REDACTED].com:fantasy.[REDACTED]  
am.[REDACTED]:internal-[REDACTED].us-west-2.elb.amazonaws.com.  
dev.[REDACTED].com:ll-[REDACTED].com.  
test.[REDACTED].com:test.[REDACTED].cdn.cloudflare.net.  
livestats [REDACTED].com:livestats-[REDACTED].elb.amazonaws.com.
```

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](https://github.com/jfrancois/SDBF)

[HTTPS://WWW.FOO.BE/PAPERS/SDBF.PDF](https://www.foo.be/papers/sdbf.pdf)

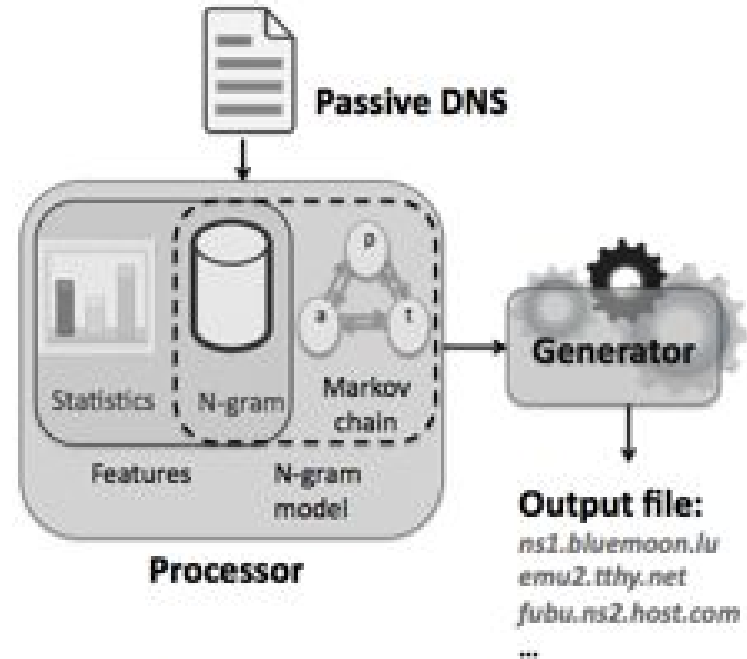


Fig. 1: Architecture of Smart DNS Brute-Forcer (SDBF)

Port Scanning

65536 UNVERIFIED HOSTS (A LARGE TARGETS ASN)

Tool	Time to run	Found
masscan masscan -p1,3-4,6-7,9,13,17,19-26,30,32-33,37,42-43,49,53,70,79-85,88-90,99-100,106,109-111,113,119,125,131,139,143-144,146,161,163,179,199,211-212,222,254-256,259,264,280,301,306,311,340,366,389,406-407,416-417,425,427,443-445,458,464-465,481,497,500,512-515,524,541,543-545,548,554-555,563,587,593,616-617,625,631,636,646,648,666-668,683,687,691,700,705,711,714,720,722,726,749,765,777,783,787,800-801,808,843,873,880,888,898,900-903,911-912,981,987,990,992-993,995,999-1002,1007,1009-1011,1021-1100,1102,1104-1108,1110-1114,1117,1119,1121-1124,1126,1130-1132,1137-1138,1141,1145,1147-1149,1151-1152,1154,1163-1166,1169,1174-1175,1183,1185-1187,1192,1198-1199,1201,1213,1216-1218,1233-1234,1236,1244,1247-1248,1259,1271-1272,1277,1287,1296,1300-1301,1309-1311,1322,1328,1334,1352,1417,1433-1434,1443,1455,1461,1494,1500-1501,1503,1521,1524,1533,1556,1580,1583,1594,1600,1641,1658,1666,1687-1688,1700,1717-1721,1723,1755,1761,1782-1783,1801,1805,1812,1839-1840,1862-1864,1875,1900,1914,1935,1947,1971-1972,1974,1984,1998-2010,2013,2020-2022,2030,2033-2035,2038,2040-2043,2045-2049,2065,2068,2099-2100,2103,2105,2107,2111,2119,2121,2126,2135,2144,2160-2161,2170,2179,2190-2191,2196,2200,2222,2251,2260,2288,2301,2323,2366,2381-2383,2393-2394,2399,2401,2492,2500,2522,2525,2557,2601-2602,2604-2605,2607-2608,2638,2701-2702,2710,2717-2718,2725,2800,2809,2811,2869,2875,2909-2910,2920,2967-2968,2998,3000-3001,3003,3005-3007,3011,3013,3017,3030-3031,3052,3071,3077,3128,3168,3211,3221,3260-3261,3268-3269,3283,3300-3301,3306,3322-3325,3333,3351,3367,3369-3372,3389-3390,3404,3476,3493,3517,3527,3546,3551,3580,3659,3689-3690,3703,3737,3766,3784,3800-3801,3809,3814,3826-3828,3851,3869,3871,3878,3880,3889,3905,3914,3918,3920,3945,3971,3986,3995,3998,4000-4006,4045,4111,4125-4127,4129,4224,4242,4279,4321,4343,4443-4446,4449,4550,4567,4662,4848,4899-4900,4998,5000-5004,5009,5030,5033,5050-5051,5054,5060-5061,5080,5087,5100-5102,5120,5190,5200,5214,5221-5222,5225-5226,5269,5280,5298,5357,5405,5414,5431-5432,5440,5500,5510,5544,5550,5555,5560,5566,5631,5633,5666,5678-5679,5718,5730,5800-5802,5810-5811,5815,5822,5825,5850,5859,5862,5877,5900-5904,5906-5907,5910-5911,5915,5922,5925,5950,5952,5959-5963,5987-5989,5998-6007,6009,6025,6059,6100-6101,6106,6112,6123,6129,6156,6346,6389,6502,6510,6543,6547,6565-6567,6580,6646,6666-6669,6689,6692,6699,6779,6788-6789,6792,6839,6881,6901,6969,7000-7002,7004,7007,7019,7025,7070,7100,7103,7106,7200-7201,7402,7435,7443,7496,7512,7625,7627,7676,7741,7777-7778,7800,7911,7920-7921,7937-7938,7999-8002,8007-8011,8021-8022,8031,8042,8045,8080-8090,8093,8099-8100,8180-8181,8192-8194,8200,8222,8254,8290-8292,8300,8333,8383,8400,8402,8443,8500,8600,8649,8651-8652,8654,8701,8800,8873,8888,8899,8994,9000-9003,9009-9011,9040,9050,9071,9080-9081,9090-9091,9099-9103,9110-9111,9200,9207,9220,9290,9415,9418,9485,9500,9502-9503,9535,9575,9593-9595,9618,9666,9876-9878,9898,9900,9917,9929,9943-9944,9968,9998-10004,10009-10010,10012,10024-10025,10082,10180,10215,10243,10566,10616-10617,10621,10626,10628-10629,10778,11110-11111,111967,12000,12174,12265,12345,13456,13722,13782-13783,14000,14238,14441-14442,15000,15002-15004,15660,15742,16000-16001,16012,16016,16018,16080,16113,16992-16993,17877,17988,18040,18101,18988,19101,19283,19315,19350,19780,19801,19842,20000,20005,20031,20221-20222,20828,21571,22939,23502,24444,24800,25734-25735,26214,27000,27352-27353,27355-27356,27715,28201,30000,30718,30951,31038,31337,32768-32785,33354,33899,34571-34573,35500,38292,40193,40911,41511,42510,44176,44442-44443,44501,45100,48080,49152-49161,49163,49165,49167,49175-49176,49400,49999-50003,50006,50300,50389,50500,50636,50800,51103,51493,52673,52822,52848,52869,54045,54328,55055-55056,55555,55600,56737-56738,57294,57797,58080,60020,60443,61532,61900,62078,63331,64623,64680,65000,65129,65389,280,4567,7001,8008,9080 -iL \$TARGET_LIST --max-rate 100000 -oG \$TARGET_OUTPUT	11m4.164s	196
nmap	∞	zzz

Visual Identification

```
root@kali:~/Desktop/tools/EyeWitness# python EyeWitness.py --prepend-https -f ../domain/tesla.com.lst --all-protocols --headless
```

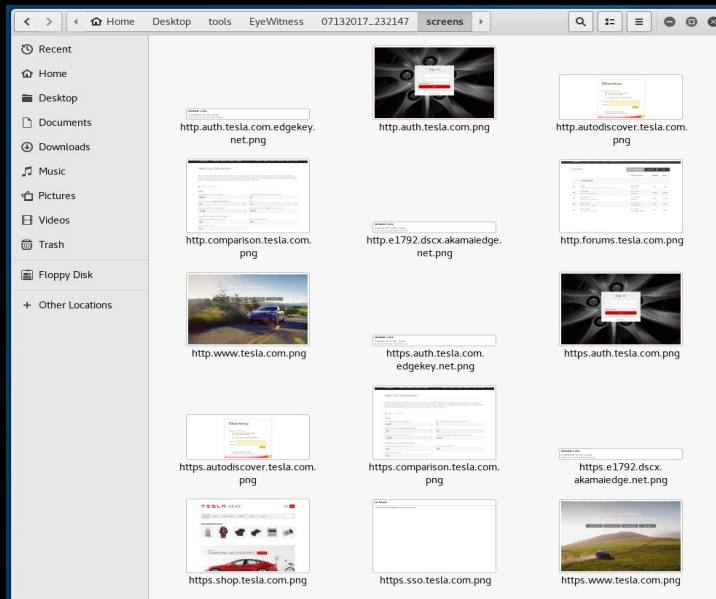


ChrisTruncer / EyeWitness

Watch 79 Star 700

Code Issues 4 Pull requests 2 Projects 0 Wiki Insights

EyeWitness is designed to take screenshots of websites, provide some server header info, and identify default credentials if possible. <https://www.christophertruncer.com/ey...>



- ★ 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

[HTTPS://GITHUB.COM/APPSECCO/BUGCROWD-LEVELUP-SUBDOMAIN-ENUMERATION/BLOB/MASTER/ESOTERIC_SUBDOMAIN_ENUMERATION_TECHNIQUES.PDF](https://github.com/appsecco/bugcrowd-levelup-subdomain-enumeration/blob/master/esoteric_subdomain_enumeration_techniques.pdf)

[HTTPS://WWW.YOUTUBE.COM/WATCH?V=1Kg0_537Eq8](https://www.youtube.com/watch?v=1Kg0_537Eq8)

Github Recon

- Environments (dev, stage, prod)
- Secret Keys (API_key, AWS_Secret, etc.)
- Internal credentials
- API endpoints
- Domain patterns

Auxiliary DEMO -BURP

Platform Identification and CVE searching



Retire.js

What you require you must also retire



Wappalyzer

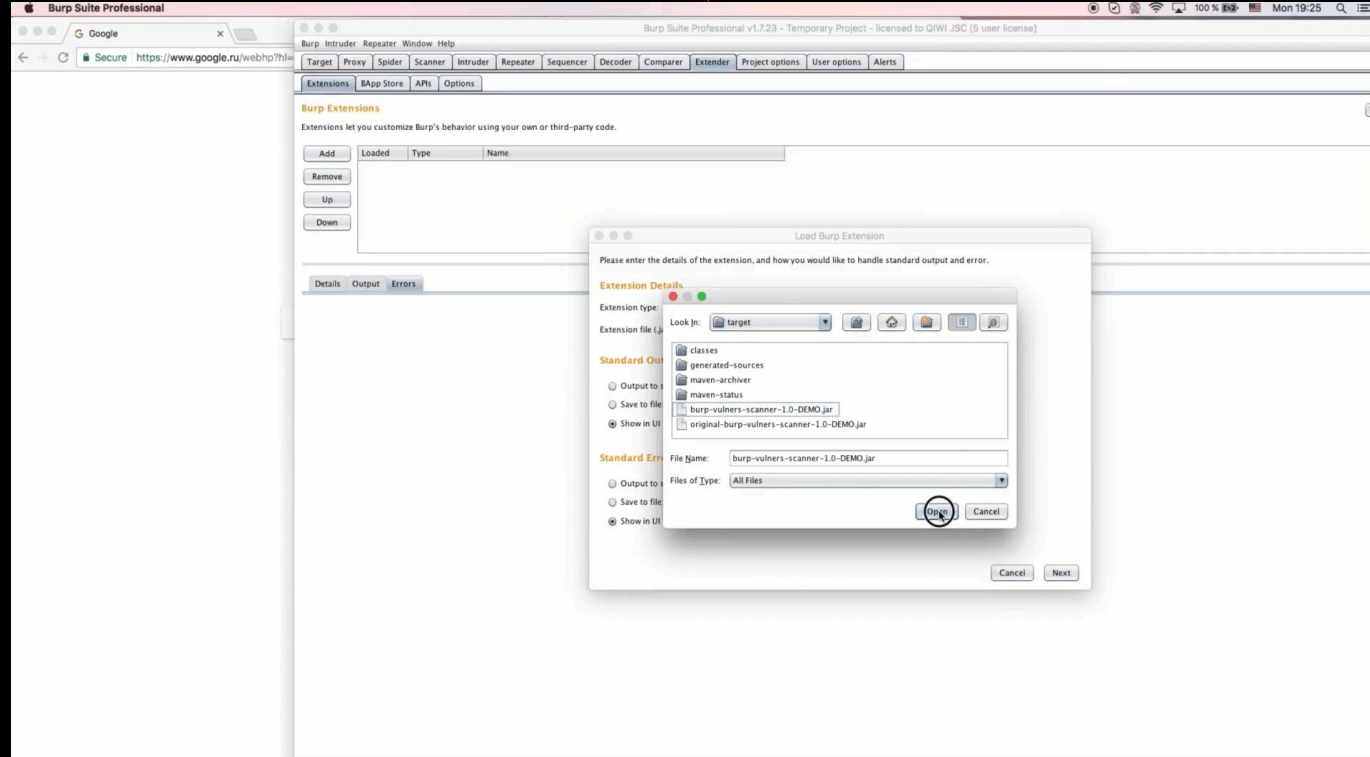
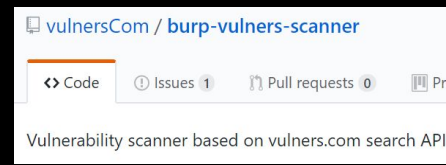


**built
With**



OpenGSE
Web Server

Java
Programming Language



Content Discovery / Directory Bruting

☒ SECLISTS / RAFT / DIGGER WORDLISTS

☒ PATATOR

☒ WPSCAN

☒ CMSMAP

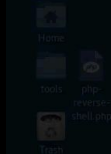
★ GOBUSTER

★ BURP CONTENT DISCOVERY

★ ROBOTS DISALLOWED

★ -_(ツ)_/-

```
root@kali:~/Desktop/tools/gobuster# wc -l ../secLists/Discovery/Web_Content/raft-large-words.txt
```



OJ / gobuster

<> Code ① Issues 11 ② Pull requests 4

Directory/file & DNS busting tool written in Go

go pentesting tool dns web

danielmiessler / RobotsDisallowed

<> Code ① Issues 1 ② Pull requests 0 ③ Projects 0 ④ Wiki Insights ▾

A harvest of the Disallowed directories from the robots.txt files of the world's top websites.

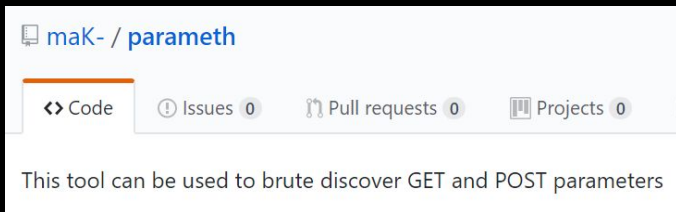
Parameter Bruting?



YEP! - UNTESTED BUT LOVE THE IDEA



CAN BE COMBINED WITH BACKSLASH SCANNERS TOP 2500 PARAMS



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

```
discobiscuits
```

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

```
=====
```

```
Establishing base figures...
```

```
GET: content-length-> 22 status-> 200
```

```
POST: content-length-> 22 status-> 200
```

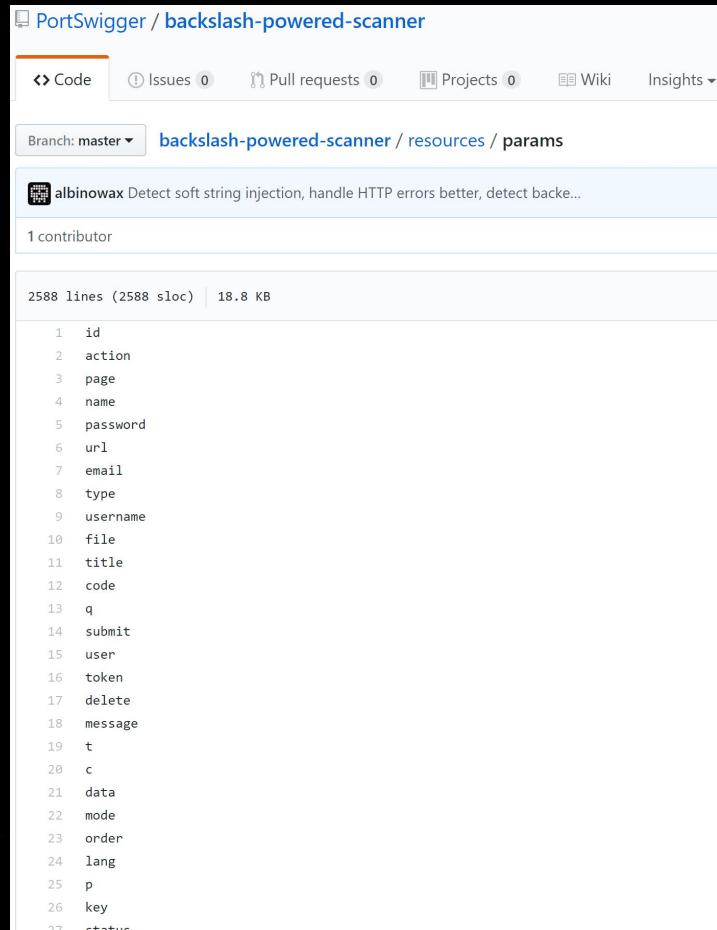
```
Scanning it like you own it...
```

```
GET(size): m | 22 ->36 ( https://makthepla.net/parameth/simpletest.php?m=discobiscuits )
```

```
POST(size): r | 22 ->42 ( https://makthepla.net/parameth/simpletest.php )
```

```
GET(status): redirect | 200->301 ( https://makthepla.net/parameth/simpletest.php?redirect=discobiscuits )
```

```
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

★ KUBEBOB:
○ A SECURITY TESTING SLACKBOT BUILT WITH A
KUBERNETES BACKEND ON THE GOOGLE CLOUD
PLATFORM

★ ASSETNOTE
★ DATASPLOIT & INTRIGUE

dvopsway / datasplit

Watch 1 Star 17 Fork 247

Code Pull requests 1 Projects 0 Wiki Insights

A tool to perform various OSINT techniques, aggregate all the raw data, visualise it on a dashboard, and facilitate alerting and monitoring on the data.

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.