Dns Recon Cheatsheet

DNS BruteForcing

DNS Wordlists

Description	URL
Top 1000	https://github.com/bitquark/dnspop/tree/master/results
Top 10000	https://github.com/bitquark/dnspop/tree/master/results
Top 100000	https://github.com/bitquark/dnspop/tree/master/results
Top 1000000	https://github.com/bitquark/dnspop/tree/master/results
Various Others	https://github.com/danielmiessler/SecLists/tree/master/Discovery/DNS

DNSRecon

```
$ dnsrecon -d <domain> -D <dir/wordlist> -t brt
```

Output Formats

- –xml
- –json
- –csv
- –db # SQLite file

NMap

```
$ nmap --script dns-brute --script-args dns-brute.domain=<domain>,dns-br
```

Fierce

```
$ fierce -dns <domain> -wordlist <dir/wordlist>
```

DNS Lookups

Types

Type	Description

Type	Description
ANY	Any type
A	A type record
AXFR	Zone Transfer
CNAME	Canonical Name
IXFR	Incremental Zone Transfer
MX	Mail Exchange
NS	Name Server
SOA	State of Authority
TXT	Text

Standard Lookup

Dig

```
$ dig <domain>
```

DNSRecon

```
$ dnsrecon -t std -d <domain>
```

Only return IP address

```
$ dig <domain> +short
```

Use specific NS

```
$ dig @<name server> <domain>
```

Reverse DNS lookup

```
$ dig -x <ip> +short
```

Reverse IP lookup for range

```
$ dnsrecon -t rvs -i 192.168.1.1,192.168.1.254
```

Query specific type

```
$ dig -t <type> <domain> <other options>
```

DNS Zone Transfer

Dig

```
$ dig -t axfr <domain>
```

DNSRecon

```
$ dnsrecon -d <domain> -t axfr
```

NSLookup (Windows)

```
$ nslookup
> set type=any
> ls -d <domain>
```

Free site tools

Domain	Description	API

Domain	Description	API
https://www.virustotal.com	Database of malware samples. Can search my file, sum, or other characteristics (ip/domain)	Yes
https://www.dnsdumpster.com	DNS recon using open source data. Gives graphs / maps of IP address locations as well	No
https://crt.sh/?q=%25bitrot.sh	Certificate search. Can tie in domains based on common certs	No
https://censys.io	scans.io driven data. Can look up domains, certificates, etc	Yes
http://searchdns.netcraft.com	Web based domain search tool	No
https://www.shodan.io	Shodan open net scanner.	Yes
https://reverse.report	Another scans.io based site with global reverse DNS records.	No

NEXT POST →

0 Comments https://bitrot.sh 1 Login

♡ Recommend Share Sort by Best

Start the discussion…

LOG IN WITH

OR SIGN UP WITH DISQUS ?

Name

Be the first to comment.

Subscribe Add Disqus to your site Disqus' Privacy Policy DISQUS

Bit Rot • 2018 • Bit Rot

Hugo v0.30.2 powered • Theme by Beautiful Jekyll adapted to Beautiful Hugo