Cheatography

subdomain-enumeration Cheat Sheet

by driver_ via cheatography.com/39507/cs/12288/

Certificate Transparency logs - search engines

https://crt.sh/

Certificate Transparency logs - search engines (cont)

https://censys.io/

By **driver_**

cheatography.com/driver/

Not published yet.

Last updated 14th July, 2017.

Certificate Transparency logs - search engines (cont)

https://google.com/transparencyreport/https/ct/

Extracting sub-domains from Rapid7 FDNS dataset

$ zcat <dataset_name> | jq -r 'if (.name | test("\\.example\\.com$")) then .name else empty end'

Extracting sub-domains from Rapid7 FDNS dataset (cont)

```
$ zcat 20170204-fdns.json.gz | jq -r 'if (.name | test("\\.example\\.com$")) then .name else empty end'
```

Rapid7 · Forward DNS dataset
https://scans.io/study/sonar.fdns_v2

By **driver_**
cheatography.com/driver/

Not published yet.
Last updated 14th July, 2017.

Zone walking - NSEC

$ ldns-walk @<nameserver> <domain>

Zone walking - NSEC (cont)

```
$ ldns-walk @ns1.insecuredns.com
insecuredns.com
```

Installing ldns utilities

```
$ sudo apt-get install ldnsutils #
On Ubuntu/Debian
$ yum install ldns # On
Redhat/CentOS
```

By **driver_**
cheatography.com/driver/

Not published yet.
Last updated 14th July, 2017.

Cheatography

subdomain-enumeration Cheat Sheet

by driver_ via cheatography.com/39507/cs/12288/

Zone transfer

$ dig AXFR @<nameserver> <domain>

Zone transfer (cont)

```
$ dig AXFR @ns1.insecuredns.com
insecuredns.com
```


By **driver_**

cheatography.com/driver/

Not published yet.

Last updated 14th July, 2017.

Cheatography

subdomain-enumeration Cheat Sheet

by driver_ via cheatography.com/39507/cs/12288/

Zone walking - NSEC3 - nsec3walker

```
$ ./collect insecuredns.com >
insecuredns.com.collect
```

Zone walking - NSEC3 - nsec3walker (cont)

```
$ ./unhash <
insecuredns.com.collect >
insecuredns.com.unhash
```

Installing nsec3walker on Ubuntu 16.04:

```
$ wget
https://dnscurve.org/nsec3walker-20
101223.tar.gz`
$ tar -xzf
nsec3walker-20101223.tar.gz
$ cd nsec3walker-20101223
$ make
```

Calculating NSEC3 hash for a domain

$ ldns-nsec3-hash -t <iterations> -s <salt> <domain>

By **driver_**
cheatography.com/driver/

Not published yet.
Last updated 14th July, 2017.

Calculating NSEC3 hash for a domain (cont)

```
$ ldns-nsec3-hash -t 10 -s 1A2B3C4D5E6F
myzone.example.com
```

By **driver_**
cheatography.com/driver/

Not published yet.
Last updated 14th July, 2017.