Subdomain enumeration cheat sheet

Certificate Transparency logs - search engines

https://crt.sh/

https://censys.io/

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'

```
$ 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

Zone walking - NSEC

$ ldns-walk @<nameserver> <domain>

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

Installing ldns utilities

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

Zone transfer

$ dig AXFR @<nameserver> <domain>

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

Zone walking - NSEC3 - nsec3walker

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

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

Installing nsec3walker on Ubuntu 16.04:

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

appsecco.com

Bharath
@yamakira_