

# OSINT

## Content

---

- [Content](#)
- [Metadata concept](#)
- [Tools](#)
  - [Awesomeness](#)
  - [popular online resources](#)
  - [OSINT multifunctional tools / frameworks](#)
    - [scanning tools](#)
  - [Subdomain / ip / e-mail harvesting / enumerate / etc. \(concrete tools\)](#)
    - [network recon](#)
    - [subdomain recon](#)
    - [e-mail harvesting](#)

Google Custom Search



- [crafting metadata](#)
- [analyzing metadata](#)
- [Tricks](#)

- [Other approaches](#)
- [Resources](#)

---

### ***OSINT***

open-source intelligence ([OSINT - wikipedia](#))

#### [The Pyramid of Pain](#)

[Knowlesys](#) - OSINT realization - looks like resource which describes osint in general

#### ***Internet is based on:***

1. Hierarchy of DNS names (tree hierarchy)
  2. RIPE databases - exists 5 regions (Europe, Central Asia; North America; Asia, Pacific; Latin America, Caribbean; Africa) each region has its own ip-address pools and each region gives sub-pools to other instances (company or provider or country or ...)
  3. Set of autonomous systems - AS. (these has no hierarchy)
  4. SSL certificate chains
-

- **computer name**, where file was created/changed
- when? the file was created/changed - **date/time**
- where? the file was located - **path disclosure**
- e-mail addresses
- ip-addresses
- dns-names and subdomains

Most popular assests searched for compromisation:

- an unpatched server connected to the Internet
- an individual

---

## Tools

---

## Awesomeness

---

- [OSINT Framework](#) - awesome **collection of** various **tools** for **OSINT (Open Source Intelligence)**



- [003random/003Recon](#) - some tools to automate recon
- *recon.sh - this tool is a framework for storing reconnaissance information.*

- [www.robtex.com](#) - very-fast recon / beautiful
- [www.threatcrowd.org](#)
- [www.visualsitemapper.com](#) - a free service that can quickly show an interactive visual map of your site

## popular online resources

- [shodan.io](#) ([shodan REST api documentation](#) ([shodan python documentation \(release 1, 08 Dec 2017\).pdf](#)) [shodan developer \(official Python library for Shodan \(github\)\)](#))  
[shodan query keys](#)
- [censys.io](#) - search engine enables researchers to ask questions about the hosts and networks that compose the Internet ([scans.io](#) - internet-wide scan data repository - the censys project publishes daily snapshots of data found by these guys)
- [ipinfo.io](#) - get geolocation, ASN, and hostname information for an IP address, company name and domain for the company that's actually using the IP address, ... (free for the first 1,000 requests per day)
- [publicwww](#) - find any alphanumeric snippet, signature or keyword in the web pages HTML, JS and CSS code
- [nerdydata.com](#) - quality leads from all over the web

Google Custom Search



bing, virustotal, ...)

```
python sublist3r.py -d example.com -passive
```

```
python sublist3r.py -b -v -d example.com -active
```

- o [subfinder](#) (*passive*) - a subdomain discovery tool that discovers valid subdomains for websites  
better use docker

- o [censys-subdomain-finder](#) (*passive*) - enumeration using the crt logs (crt.sh)

```
python censys_subdomain_finder.py --censys-api-id [API_ID] --censys-api-secret [API_SECRET] example.com
```

[censys-enumeration](#) (*passive*) - a script to extract subdomains/emails for a given domain using SSL/TLS certificates dataset on Censys (json output)

```
python censys_enumeration.py --verbose --subdomains --emails domains.txt
```

- o [amass](#) (*passive with dns or active*) - in-depth subdomain enumeration

purely passive: `... -nodns ...`

passive: `amass -v -ip -min-for-recursive 3 -log ~/amass.log -d example.com ,`

has active methods: `-active -brute`

- o [knockpy](#) (*active*) - subdomain scan

```
knockpy example.com
```

- o [enumall.py](#) (*passive + bruteforce*) - automation of recon-ng subdomain discovery

```
./enumall.py example.com
```

```
./enumall.py -a example.com
```

Not all available technics are used by these tools, e.g. you can check specific technics from *subdomain enumerate* category (e.g. CSP analysis for subdomain search)

```
aquatone-discover --domain example.com --threads 25 - subdomain enumeration
```

```
aquatone-scan --domain example.com --ports large - enumeration common ports, used for web-services
```

```
aquatone-gather --domain example.com - retrieve and save HTTP response headers and make screenshots
```

```
aquatone-takeover --domain example.com - check subdomain-takeover situations
```

- [datasploit](#) (passive + active) - osint + active scans = HTML report

```
datasploit -d example.com
```

- **fast analysis**

- [domain\\_analyzer](#) - search all info about domain

- [domain-profiler](#) - a tool that uses information from whois, DNS, SSL, ASN, ...

- *lazyrecon (active) - sublist3r and certspotter + screenshots + grab response header + nmap + dirsearch = generate HTML report*

- [theHarvester](#) (passive + active) - e-mail, subdomain and people names harvester

```
python theHarvester.py -b all -d example.com
```

- [DMitry](#) (active + port scan) - gather as much information as possible about a host. Base functionality is able to gather possible subdomains, email addresses, uptime information, tcp port scan, whois lookups, ...

```
dmitry -i -w -n -s -e example.com
```

with port scan: `dmitry -i -w -n -s -e -p -b -t 2 example.com`

- web-spidering:



- [blacksheepwall](#) (based on *CommonCrawl* - grep the internet)

```
blacksheepwall -cmn-crawl CC-MAIN-2018-13-index -domain sberbank.ru
```

- making screenshots:

- [webscreenshot](#)
- [lazyspot](#)

- online services:

- IP, reverse IP, whois, NS, MX, PRT - history analysis, ...
  - [viewdns.info](#) - reverse IP lookup, whois, ip history, smap lookup, ...
  - [community.riskiq.com](#) ((alias: [passivetotal.com](#))) - with registration and limited amount of queries (10 requests everyday for free), however **VERY GOOD** resource
  - [reverse.domainlex.com](#) - reverse IP, NS, MX, whois
  - <http://ptrarchive.com/> - PTR - over 166 billion reverse DNS entries from 2008 to the present
- search whois history, etc.:
  - [www.recipdonor.com](#) (can search websites on single ip address, can search through history of whois)  
[RDS history](#), [several sites on single IP](#), [RDS subdomain](#)

Google Custom Search



- [ipvoid.com](#) - IP address tools online
- [pentest-tools.com](#) - google hacking, find subdomains, find vhosts, metadata extractor, icmp ping, whois lookup

- ***intrigue.io*** - [official site](#), [github](#)
- ***spiderfoot*** – open source intelligence automation tool for process of gathering intelligence about a given target, which may be an IP address, domain name, hostname or network subnet
- ***recon-ng (kali linux)*** - good (and huge) tool for various reconnaissance vectors  
[usage sample](#)
- Google dorks: `site:example.com -site:dev.example.com` - search for subdomains, excluding those we already know about (bing, yandex, ***github*** etc.) ([ghdb.html](#))
- [archive.org](#)
- check list of merges and acquisitions (e.g. [List of mergers and acquisitions](#))
- *maltego - to me it looks more like a toy*

## scanning tools

- [subresolve](#) - resolve and quickly portscan a list of sub-domains





## network recon

- search for other sites on **virtual hosting**:
  - [VHostScan](#)
  - *my-ip-neighbors.com - under maintenance for one week (in fact for a year already)*
- **whois, ASN, etc.**
  - `whois` (console utility) (never pass the domain name as the parameter, pass *domain name's IP-address*), etc.  
`whois -h whois.cymru.com " -v 8.8.8.8" - using cymru.com get AS of an IP address`  
`whois -h whois.radb.net -- '-i origin AS35995' | grep -Eo "([0-9.]{4}){4}/[0-9]{4}" - sing radb.net get ip-subnets of AS`
  - [whois.domaintools.com](#), [reverseip.domaintools.com](#), ...
  - [www.skvotte.ru](#)
- search **ip-addresses** and **ip-address pools**
  - [2ip.ru/whois](#)
  - [nic.ru/whois](#)
  - ASN lookup
    - [bgp.he.net](#) - hurricane electric internet services

Google Custom Search



- [www.arin.net](http://www.arin.net) (North America)
- [wq.apnic.net](http://wq.apnic.net) (Asia, Pacific)
- [lacnic.net](http://lacnic.net) (Latin America, Caribbean)
- [www.afrinic.net](http://www.afrinic.net) (Africa)

○ `curl -s http://download.maxmind.com/download/geoip/database/asnum/GeoIPASNum2.zip | gunzip | cut -d"," -f3 | sed 's/"//g' | sort -u | grep -i twitter` (MaxMind geo-ip base)

### • reverse ip lookup

- `dig -x 8.8.8.8`
- `host 8.8.8.8`
- [yougetsignal.com](http://yougetsignal.com)

## subdomain recon

Categorial/concrete tools/attacks:

- [CloudFail](#) - utilize misconfigured DNS and old database records to find hidden IP's behind the CloudFlare network

```
python cloudfail.py --target rublacklist.net
```

## subdomain enumerate

- [searchdns.netcraft.com](http://searchdns.netcraft.com)

- [domains-from-csp](#) - a script to extract domain names from Content Security Policy(CSP) headers

```
python csp_parser.py -r http://example.com
```

Everything beneath can be done faster if you will use frameworks and other complex tools

- **Subject Alternative Name (SAN)** - X509 extension to provide different names of the subject (subdomains) in one certificate  
Even if there is non-resolvable subdomain, probably admins use the same certificate for intranet connections.

- [crt.sh](#) example: `https://crt.sh/?q=%25.example.com`

- [crt search bash script](#)

- [transparencyreport.google.com](#)

- [certspotter.com/api](#)

- [certdb.com](#)

- [censys.io](#) example: `https://censys.io/certificates?q=.example.com`

- [certificate transparency monitor \(facebook\)](#)

- **Forward DNS**

- [Rapid7 - Forward DNS \(FDNS ANY\)](#) lists (120 Gb) - [how it works](#) - list is not full

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

- [dnsdumpster.com](#) (also contains historical data about dns) (online tool)



- o `fierce -dns zonetransfer.me`
- o `dnsrecon -a -d zonetransfer.me`

- [NSEC walking attack](#) - enumerates DNSSEC-signed zones

[Take your DNSSEC with a grain of salt](#)

- o `apt-get install ldnsutils`
  - `ldns-stroll @ns1.insecuredns.com insecuredns.com`
  - `ldns-walk @ns1.insecuredns.com insecuredns.com`
- o [nsec3map](#) – DNSSEC Zone Enumerator – позволяет перебрать содержимое всей доменной зоны и найти поддомены, если на dns сервере работает dnssec (<https://github.com/anonion0/nsec3map>)
- o [nsec3walker](#)
- o `nmap -sSU -p 53 --script dns-nsec-enum --script-args dns-nsec-enum.domains=example.com <target>`  
`nmap -sSU -p 53 --script dns-nsec3-enum --script-args dns-nsec-enum.domains=example.com <target>`

### subdomain bruteforce

Comparison of subdomain bruteforce tools: [massdns](#), [gobuster](#), [dns-paraller-prober](#), [blacksheepwall](#), [subbrute](#) (pic)

[SecLists](#) - check bruteforce lists

[compiled GIANT subdomain wordlist](#) (march 2018)

- [massdns](#)



- [dnsrecon](#)  

```
dnsrecon -d example.com -D /usr/share/wordlists/dnsmap.txt -t std --xml dnsrecon.xml
```

```
dnsrecon.py -n ns1.example.com -d example.com -D subdomains-top1mil-5000.txt -t brt
```
- ```
nmap --script dns-brute --script-args dns-brute.domain=domain.com,dns-brute.threads=6,dns-brute.hostlist=./sub1000000.lst
```
- [SDBF](#) - smart DNS bruteforcer ([paper](#))
- [DNSenum](#)
- [gobuster](#) - tool for URL and DNS bruteforce
- manually check existence of `dev.example.com` , `beta.example.com` , `db.example.com` , `admin.example.com` , ...

## e-mail harvesting

- [SimplyEmail](#)
- Google Chrome extentions:
  - [Email finder](#)
  - [Email finder](#) (automatically opens queries to yandex,google,rambler, ... and searches for emails ++ automatic Google Dorks)
  - [Email Extractor](#) - extract emails from visited pages
  - [hunter.io](#)
  - [emailhunter](#) - extract emails from visited pages

## AWS buckets search

Technique works through bruteforcing bucket names and searching for public buckets.

- [bucket\\_finder](#)
- [lazys3](#)
- [slurp](#) - removed after microsoft purchased github - Wierd!
- [s3-buckets-finder](#)

---

## Social engineering / phishing

[The social engineering framework](#) - a searchable information resource for people wishing to learn more about the psychological, physical and historical aspects of social engineering.

Social engineering questions: who? (clients/employees), purpose? (awareness assessment, checking Incident Response Center, get confidential information, ...), intruder model (insider/outsider), when? (at night, at the end of working day, ...)

- [SET](#) - the Social-Engineer Toolkit

[Pierce Phish](#) - other phishing framework (looks young)

- [evilginx2](#) - standalone man-in-the-middle attack framework used for phishing login credentials along with session cookies, allowing to bypass 2-factor authentication.  
[evilginx 2 - next generation of phishing 2FA tokens](#)
- [spoofoxb.com](#) - spoof e-mails, messangers, ...
- For spam delivery:
  - [dnsbl.info](#) - database of blacklisted ip-addresses
  - [mailgun.com](#) - *"powerful APIs that enable you to send, receive and track email effortlessly (10,000 emails free every month)"*
  - [sendpulse.com](#) - *"maximizing open rates automatically with Artificial Intelligence, Hyper-personalization, Predictive analysis for email, SMS, Web Push, SMTP"*
- [mail-tester.com](#) - first send your email, then check your score

### protection methods:

search for phishing sites: [altdns](#) - generates permutations, alterations and mutations of subdomains and then resolves them

- configure domain (example.com TXT record "v=spf1 +a +mx -all"), mail-servers, spam-filters, sandboxes, etc.
- monitor anomalies
- employee training
- carry socio-technical testing



## Metadata

### crafting metadata

- [FOCA \(Fingerprinting Organizations with Collected Archives\)](#) - search for company's documents (through google, yandex, bing, rambler, etc.) and afterwards exports and consolidate metadata (*FOCA not maintained anymore, but still brilliant*)
- [Belati](#) - the traditional swiss army knife for OSINT (FOCA's good/better alternative)
- [metagoofil](#) - extracting metadata from public documents found by google  
`metagoofil -d example.com -t pdf -l 100 -n 25 -o example -f example.com.html` - scan for documents from a domain (-d example.org) which are PDF files (-t pdf), searching 100 results (-l 100), download 25 files (-n 25), saving the downloads to a directory (-o example) and saving the output to a file (-f example.com.html)
- [snitch](#) - automate information gathering process for specified domain
- Google dorks: `site:example.com filetype:pdf` ([ghdb.html](#))
- *More tools on github:* [search for dorks in github](#)
- **grep the internet:** [commoncrawl](#) (get the latest date and start)  
data can be downloaded or can be searched online or you can use command-line tool  
(march 2018: [databases](#), [online search](#))

`exiftool -jk` - tool for extracting metadata from files





- [analysing metadata](#)

## Tricks

- email headers may contain ip-addresses from internal companie's infrastructure

---

## Other approaches

- Lookup [github.com](#), [bitbucket.org](#) and other open control version systems for client's backups, configs, dev code, etc.  
[GitMiner](#) - tool for advanced mining for content on Github

---

## Resources

- [The Art of Subdomain Enumeration](#)
- [Metadata: a hacker's best friend](#)

# Information Security / *PENTEST*

## / *OSINT*



Google Custom Search



[\\_tools\\_](#) [Android-security](#) [concepts](#) [concrete\\_protocols](#) [Cryptography](#)  
[GNSS\(GPS\)](#) [GSM](#) [osint-personal](#) [OSINT](#) [Personal-sec](#) [Reverse](#)  
[SQLi](#) [WiFi](#) [Windows](#) [XXE](#)

Information Security

Information Security  
[phonexicum @ yandex.ru](#)

 [phonexicum](#)  
 [phonexicum](#)

I created this site in a burst of information security studying to organize my mind and create some kind of cheatsheet.