

Passive Reconnaissance and OSINT

Martin Stanek

2024

Table of Contents

Introduction

Searching information – IP addresses, domains, names, e-mails, technology, . . .

Slovak specifics

Reconnaissance

- reconnaissance – techniques for gathering information about target
- usually the first step in penetration testing or adversarial activities
- reconnaissance supports planning of subsequent techniques
- information of interest:
 - domains, domain names, IP ranges and addresses, ports, technology stack, vulnerabilities, organizational structure, e-mails, usernames, people and their roles, credentials, physical assets, etc.
- passive reconnaissance
 - publicly available information and services, OSINT (e.g. DNS, CT logs, search engines)
- active reconnaissance
 - interaction with target (e.g. enumeration and scanning networks/hosts, webapp scanning, e-mail)

Passive reconnaissance

- positives:
 - target is not notified about reconnaissance activities
 - most information publicly available – usually no permission required
- negatives:
 - imprecise results, possibly outdated information
 - some information cannot be obtained or verified passively

OSINT defined in Sect. 931 of Public Law 109-163, Department of Defense Strategy for Open-source Intelligence (2006):

Open-source intelligence (OSINT) is intelligence that is produced from publicly available information and is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement.

- OSINT is used in various contexts:
 - military intelligence, law enforcement, business, journalism, personal, etc.

- OSINT for cybersecurity (reconnaissance/information gathering)
- closely related but not equal to passive reconnaissance
 - active OSINT (download info from the webpage, validate DNS records, etc.)
 - closed sources for passive reconnaissance

General methodology for OSINT

1. Start with known data
2. Set specific goals (what data you want to get)
3. Repeat:
 - Gather data using tools
 - Analyze the data
4. Validate the result
5. Document your steps and results

- OSINT – *publicly available information*
- Don't get carried away
- Personal data and GDPR
- Trestný zákon 300/2005 Z.z. v znení neskorších predpisov:
 - § 374 Neoprávnené nakladanie s osobnými údajmi
 - § 247 Neoprávnený prístup do počítačového systému
 - § 247a Neoprávnený zásah do počítačového systému
 - § 247b Neoprávnený zásah do počítačového údajja
 - § 247c Neoprávnené zachytávanie počítačových údajov

Resources and tools

- publicly available information
 - usually free resources and tools to harvest data
 - paid services for some resources (e.g. for more detailed data, bulk queries, API access)
- various collections of (free) tools and resources
 - [OSINT Framework](#), [OSINT Techniques](#), [OSINT Dojo](#), ...
- stay up-to-date
 - obsolete and abandoned tools, API changes
 - out-dated or vanished web resources
 - check for new techniques and resources

IP addresses, domains, names

- Goals:
 - IP ranges and addresses
 - domains registered by the company
 - domain names
- Sources:
 - Whois (RIPE, DNS)
 - DNS queries
 - Certificate Transparency logs (crt.sh)
 - web search engines – Google, Bing

IP addresses and ranges

- IP Address blocks
 - RIPE (Réseaux IP Européens)
 - ARIN (American Registry for Internet Numbers), etc.
- RIPE Whois database
 - additional info: names, phones, e-mails, etc.
 - reverse searches (based on e-mails, names)
 - [web interface](#), CLI (`whois`), or RESTful API

RIPE Whois example (uniba.sk)

- query RIPE with IP address of www.uniba.sk (see unfiltered result for more information):

```
$ whois 158.195.6.138 | grep -E '(inetnum|organisation|...)'
inetnum:          158.195.0.0 - 158.195.255.255
admin-c:          U054-RIPE
organisation:     ORG-CUIB1-RIPE
phone:            +421 2 59244986
phone:            +421 2 59244 944
admin-c:          PK8515-RIPE
route:            158.195.0.0/17
```

- additional data: whois U054-RIPE and similar queries
- full text search using web interface; example: search for @uniba.sk

- registrars maintain records for domain registration
- Whois and GDPR
 - (most) registrars remove registrant names and contact information from Whois records
 - still some non-personal info can be found, e.g. phone, e-mail
- easy to search
 - some TLD registrars provide web interface, web services
 - command-line tools (`whois <domain>`)
- reverse Whois (web service)
 - find all domains that share something in common (e-mail, company, etc.)
- validate info – old, incorrect, etc.

Whois example (uniba.sk)

Searching in WHOIS.SK-NIC.SK

Search for .sk or org.sk domain:

Domain information

```
Názov domény:      uniba.sk
Dátum vytvorenia:  2003-09-17
Platná do:         2031-09-17
Posledná aktivita: 2023-08-31
Stav domény:      ok
Menný server:     dns1.uniba.sk
Menný server:     dns3.uniba.sk
Menný server:     dns2.uniba.sk
Menný server:     dns4.uniba.sk

Držiteľ domény:   UNIV-0027
Corporation:
Názov:            Univerzita Komenského v Bratislave
Organizácia:     Univerzita Komenského v Bratislave
IČO:              00397865
Telefón:         +421.259244948
Email:           hostmaster@uniba.sk
Ulica:           Šafárikovo námestie 6
Obec:            Bratislava
PSČ:             81499
Kód štátu:       SK
Dátum vytvorenia: 2017-09-01
Posledná aktivita: 2024-03-01

Registrátor domény: UNIV-0027
Názov:            Univerzita Komenského v Bratislave
Organizácia:     Univerzita Komenského v Bratislave
IČO:              00397865
Telefón:         +421.259244948
Email:           hostmaster@uniba.sk
```

- validate names gathered elsewhere
- usual stuff: MX, NS, TXT records
- reverse DNS search for an IP range (PTR records)
- semi-active approach
 - someone has to talk to target's DNS servers
 - open DNS resolvers, Google (8.8.8.8, 8.8.4.4), Cloudflare (1.1.1.1, 1.0.0.1), etc.

Certificate Transparency logs

- publicly available records of certificates
- goal of CT logs: protect users and domain owners
 - difficult/impossible for a CA to issue a certificate for a domain without being visible
 - open auditing and monitoring system
- OSINT: source of domain names (CN, SAN)
- web interface: crt.sh (not the only one)

crt.sh example (uniba.sk)

crt.sh ID	Logged At ↑	Not Before	Not After	Common Name	
12264536436	2024-03-03	2024-03-03	2024-06-01	sluzby.fmph.uniba.sk	sluzby.fmph.uniba.sk
12264536201	2024-03-03	2024-03-03	2024-06-01	sluzby.fmph.uniba.sk	sluzby.fmph.uniba.sk
12264534248	2024-03-03	2024-03-03	2024-06-01	sluzby.fmph.uniba.sk	sluzby.fmph.uniba.sk
12264533153	2024-03-03	2024-03-03	2024-06-01	sluzby.fmph.uniba.sk	sluzby.fmph.uniba.sk
12235269957	2024-03-01	2024-03-01	2024-05-30	oversi.uniba.sk	oversi.uniba.sk
12235272059	2024-03-01	2024-03-01	2024-05-30	zamvpn.uniba.sk	zamvpn.uniba.sk
12235265209	2024-03-01	2024-03-01	2024-05-30	zamvpn.uniba.sk	zamvpn.uniba.sk
12235265198	2024-03-01	2024-03-01	2024-05-30	oversi.uniba.sk	oversi.uniba.sk
12226162742	2024-02-29	2024-02-29	2025-02-28	radius.uniba.sk	radius2.uniba.sk radius3.uniba.sk radius.uniba.sk
12226162726	2024-02-29	2024-02-29	2025-02-28	radius.uniba.sk	radius2.uniba.sk radius3.uniba.sk radius.uniba.sk
12216009886	2024-02-28	2024-02-28	2024-05-28	cray.dbp.fmph.uniba.sk	cray.dbp.fmph.uniba.sk cray.upc.uniba.sk
12216002969	2024-02-28	2024-02-28	2024-05-28	cray.dbp.fmph.uniba.sk	cray.dbp.fmph.uniba.sk cray.upc.uniba.sk
12211007367	2024-02-27	2024-02-27	2024-05-27	ctrl.seclab.dcs.fmph.uniba.sk	ctrl.seclab.dcs.fmph.uniba.sk x10.ctrl.seclab.dcs.fmph.uniba.sk x11.ctrl.seclab.dcs.fmph.uniba.sk x12.ctrl.seclab.dcs.fmph.uniba.sk x13.ctrl.seclab.dcs.fmph.uniba.sk

DNS queries (2)

- zone transfer (works rarely)

```
$ dig @8.8.8.8 dns1.uniba.sk +short
```

```
158.195.4.3
```

```
$ dig @158.195.4.3 AXFR uniba.sk +short
```

```
; Transfer failed.
```

- brute-forcing domain names
 - guesses are easy to validate
 - dictionary words (various top-X subdomains lists exist)
- DNSSEC
 - NSEC walking (non-existence leaks domain names)
 - NSEC3 zone enumeration (hash for dictionary attacks)

Web search engines, services, and tools

- Web engines scrapping
 - Google, Bing: `site:uniba.sk -www.uniba.sk -known_domain ...`
- Other services, examples:
 - [VirusTotal](#) (search for domain), [Hacker Target DNS & IP Tools](#)
 - [DNSdumpster](#): search for domain, [Network Discovery Process](#)
 - Shodan
- automate the enumeration with tools
 - usually aggregate results from multiple sources
 - optionally perform brute-forcing
 - often have other OSINT capabilities (beyond DNS reconnaissance)
 - DNS focused tools: OWASP Amass, DNSRecon, etc.

Tools with a broader scope

- automation of data collection
 - various data types
 - many data sources (the most useful are paid)
- theHarvester (IP, names, e-mails)
- Recon-ng
- Maltego
- Spiderfoot

- harvesting/scrapping web for e-mail addresses
 - shady business practice
- starting point for targeting people
 - phishing, social engineering, leaked credentials
- Hunter (hunter.io, PyHunter wrapper, etc.)
- Google – “site:domain.xx intext:@domain.xx”
- Bing – “site:domain.xx inbody:@domain.xx”



Breaches

- breaches as a source of valuable information
 - e-mails, passwords, etc.
- collection 1.4 billion cleartext passwords and e-mails (2017)
 - other leaks/collections in 2021 and 2024
 - password history for some account
 - filter using target domain
 - better password guessing
- [HaveIBeenPwned](#)
 - checking e-mail address in publicized data breaches

What's running there?

- virtual hosts: single IP for multiple (separate) web applications
 - usually DNS names in CT logs
 - DNS records pointing to a single IP
 - brute force (active technique)
- search engines: Shodan, Censys
 - banners, ports, certificates, etc.
- probing is active reconnaissance
- semi-active approach for web applications
 - Wappalyzer, WhatRuns and others (often browser extension)
 - (active recon) WhatWeb CLI

WhatRuns (uniba.sk)

What runs uniba.sk?  

CMS

 TYPO3 CMS 4.7

 Mousewheel JS

Video

 YouTube

Web Framework

 Bootstrap

Programming Language

 PHP

CDN

 CloudFlare

Analytics

 Google Analytics UA

Font Script

 Font Awesome

 Google Font API

Web Server

 Apache 2.2.22

Operating System

 Debian

Javascript Frameworks

 jQuery 1.11.1

 whatruns

- search engine for Internet-connected devices
 - servers, printers, webcams, control systems, etc.
- Shodan
 - scans Internet regularly
 - indexes banners, certificates, ports, etc.
- Examples (filters require an account):
 - `port:22 hostname:"uniba.sk"` (136 results)
 - `IIS hostname:"uniba.sk"` (14 results, some old versions, Censys: more results)
- command line interface available
- use API to automating searches
- other tools use Shodan (using an API key, e.g. recon-ng)

Shodan example (www.dcs.fmph.uniba.sk)

158.195.87.156



// LAST SEEN: 2024-03-03

General Information

Hostnames	dcf.fmph.uniba.sk www.dcf.fmph.uniba.sk
Domains	UNIBA.SK
Country	Slovakia
City	Bratislava
Organization	Comenius University Bratislava
ISP	Zdruzenie pouzivatelov Slovenskej akademickej datovej siete
ASN	AS2607

Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

Open Ports

80 443

// 80 / TCP

914256635 | 2024-03-01T05:49:37.060429

Apache httpd 1.3.41

```
HTTP/1.1 200 OK
Date: Fri, 01 Mar 2024 05:49:36 GMT
Server: Apache/1.3.41 (Unix) mod_ssl/2.8.31 OpenSSL/0.9.71 PHP/4.3.11
Last-Modified: Tue, 13 Apr 2004 16:31:30 GMT
ETag: "26a002-f0-407c15e2"
Accept-Ranges: bytes
Content-Length: 240
Content-Type: text/html
```

// 443 / TCP

914256635 | 2024-03-03T23:44:47.307032

Apache httpd 1.3.41

```
HTTP/1.1 200 OK
Date: Sun, 03 Mar 2024 23:44:47 GMT
Server: Apache/1.3.41 (Unix) mod_ssl/2.8.31 OpenSSL/0.9.71 PHP/4.3.11
Last-Modified: Tue, 13 Apr 2004 16:31:30 GMT
```

Censys example (www.dcs.fmph.uniba.sk)

158.195.87.156

As of: Mar 06, 2024 5:51pm UTC | Latest

[Summary](#) [History](#) [WHOIS](#) [Explore](#)

Basic Information

Reverse DNS www.dcs.fmph.uniba.sk

Forward DNS dcs.fmph.uniba.sk, wwwtmp.dcs.fmph.uniba.sk, www.dcs.fmph.uniba.sk

Routing 158.195.0.0/17 via [SANET Slovak Academic Network, SK \(AS2607\)](#)

Services (2) [80/HTTP](#), [443/HTTP](#)

HTTP 80/TCP

03/06/2024 02:34 UTC

Software

[VIEW ALL DATA](#)

[GO](#)

[mod_ssl 2.8.31](#)

[OpenSSL 0.9.7l](#)

[Apache HTTPD 1.3.41](#)

[PHP 4.3.11](#)

- using Google to find useful information (security relevant)
 - operators: OR, AND, -, *, site, intext, intitle, filetype/ext, etc.
- Google Hacking Database ([GHDB](#))
- Examples:
 - `filetype:cfg "radius" (pass|passwd|password)`
 - `intitle:"index of" "tomcat-users.xml"`
 - `inurl:"cgi-bin" "No password set!" "There is no password set on this router."`
 - `intext:"INTERNAL USE ONLY" ext:doc OR ext:pdf OR ext:xls OR ext:xlsx`
- other search engines can be used as well

- archives: Archive.org
- social networks
 - business (e.g. LinkedIn) and personal
 - online communities
- metadata and other information in documents
 - Office, PDF, SVG, etc.
 - use search engines to find document
 - FOCA, metagoofil + ExifTool

- knowing local environment can help
- specific resources not available globally
 - public administration and their services
 - publication of data required by laws
- few examples for Slovak republic (SK)

SK: Central register of contracts

- The Freedom of Information Act
(Zákon č. 211/2000 Z. z. o slobodnom prístupe k informáciám)
 - some contracts must be published
- Central register of contracts (Centrálny register zmlúv – CRZ)
 - [web page](#) with search/filter
 - some entities must publish here
- Other subject must publish contracts as well
 - municipalities, NBS, etc.
 - often available on their own web sites
 - some contracts are indexed by search engines

SK: Contracts and orders – examples

- Industrial property office of the Slovak Republic
 - contract: 59/2020
 - IT components (OS, SAN, network devices, firewalls, virtualization platform etc.)
 - network topology
- Financial Directorate of the Slovak Republic
 - contract: Z202012343_Z
 - AntiSpam, AntiVirus, Advanced Malware Protection, centralized management
 - email security appliance

- certified systems for electronic procurement
- sometimes more information than contract
- precedes an implementation

Examples:

- Ministry of Foreign and European Affairs of the Slovak Republic
 - EU journal ref. no.: 2020/S 124-303196
 - network firewalls, network protection in selected remote locations
 - integration with central management Palo Alto Networks Panorama
- Statistical Office of the SR
 - EU journal ref. no.: 2020/S 141-346994
 - telecommunication and network services for LAN/WAN
 - network topology, network devices, etc.

- complete list of domains is available for SK zone
 - `sk-nic.sk/subory/domains.txt`
 - domain, registrar, registrant, status, NS records, expiration date
 - not a common practice for other TLDs
- usage
 - check for typosquatting (other services for global checking)
 - find all domains with common registrant, registrars, or name servers

- details obtained in a job description
 - hard to hide if you want to narrow down candidates
- Application specialist (for a bank):
 - Máš skúsenosť s administráciou Microsoft Windows platformy?
 - Máš skúsenosti s prácou s MSSQL prípadne ORACLE databázou? Stačí byť začiatočník.
 - Windows Server prostredie je nevyhnutnosť, no UNIX bude len a len výhodou.
 - IIS, Apache, Vmware a mnoho ďalších sú komponenty, s ktorými pracujeme.
 - Ak poznáš Sharepoint platformu, je to super. Či už online alebo onpremise.
- System engineer for network infrastructure (another bank):
 - Administrácia komponentov sieťovej a bezpečnostnej infraštruktúry Cisco, F5 load balancer (datacentra, budovy ústredia, pobočky, bankomaty, pripojenia do externých organizácii)
 - Administrácia monitorovacieho nástroja Hewllet Packard Network Node Manager

Using OSINT for finding missing people

- interesting application of OSINT
- Trace Labs (www.tracelabs.org)
 - nonprofit organization
 - collecting OSINT on missing persons
 - CTF events
 - interesting scoring system
 - strict rules of engagement

Choose an organization in a public sector. Perform a basic OSINT research, **without** directly or indirectly interacting with its IT infrastructure. Use suitable tools and document your findings.

1. *What information can be obtained from Whois and DNS?*
2. *Find domain names, IP addresses of Internet-connected systems.*
3. *Explore and compare Shodan and Censys results for the domain.*
4. *Find technologies that are used in the organization.*

1. Michael Bazzell, *OSINT Techniques: Resources for Uncovering Online Information*, 10th Edition, 2023
2. Javier Pastor-Galindo et al., *The Not Yet Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends*, IEEE Access, 2020.
DOI:10.1109/ACCESS.2020.2965257
3. Tools and resources collections (many other exist):
 - [OSINT Framework](#)
 - [OSINT Techniques – Tools](#)
 - [OSINT Dojo – Resources](#)