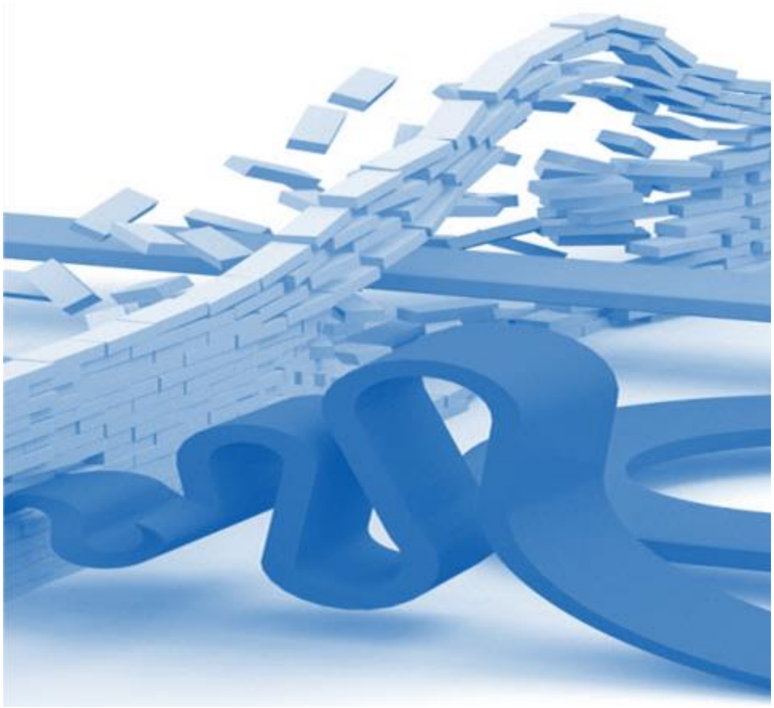
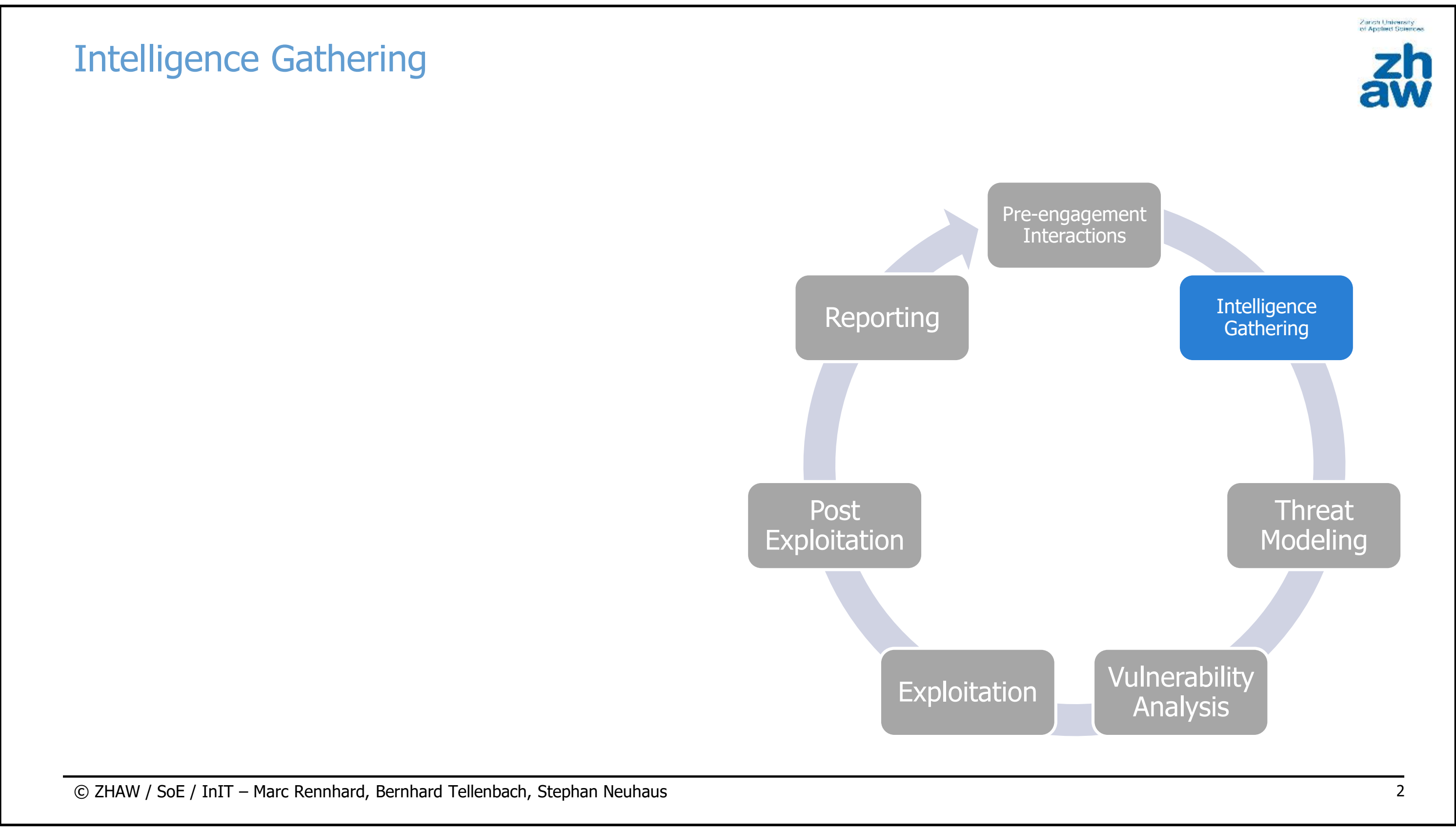


PENETRATION TESTING (PART II)

Prof. Dr. Bernhard Tellenbach



Intelligence Gathering

Pre-engagement Interactions

Intelligence Gathering

Threat Modeling

Vulnerability Analysis

Exploitation

Post Exploitation

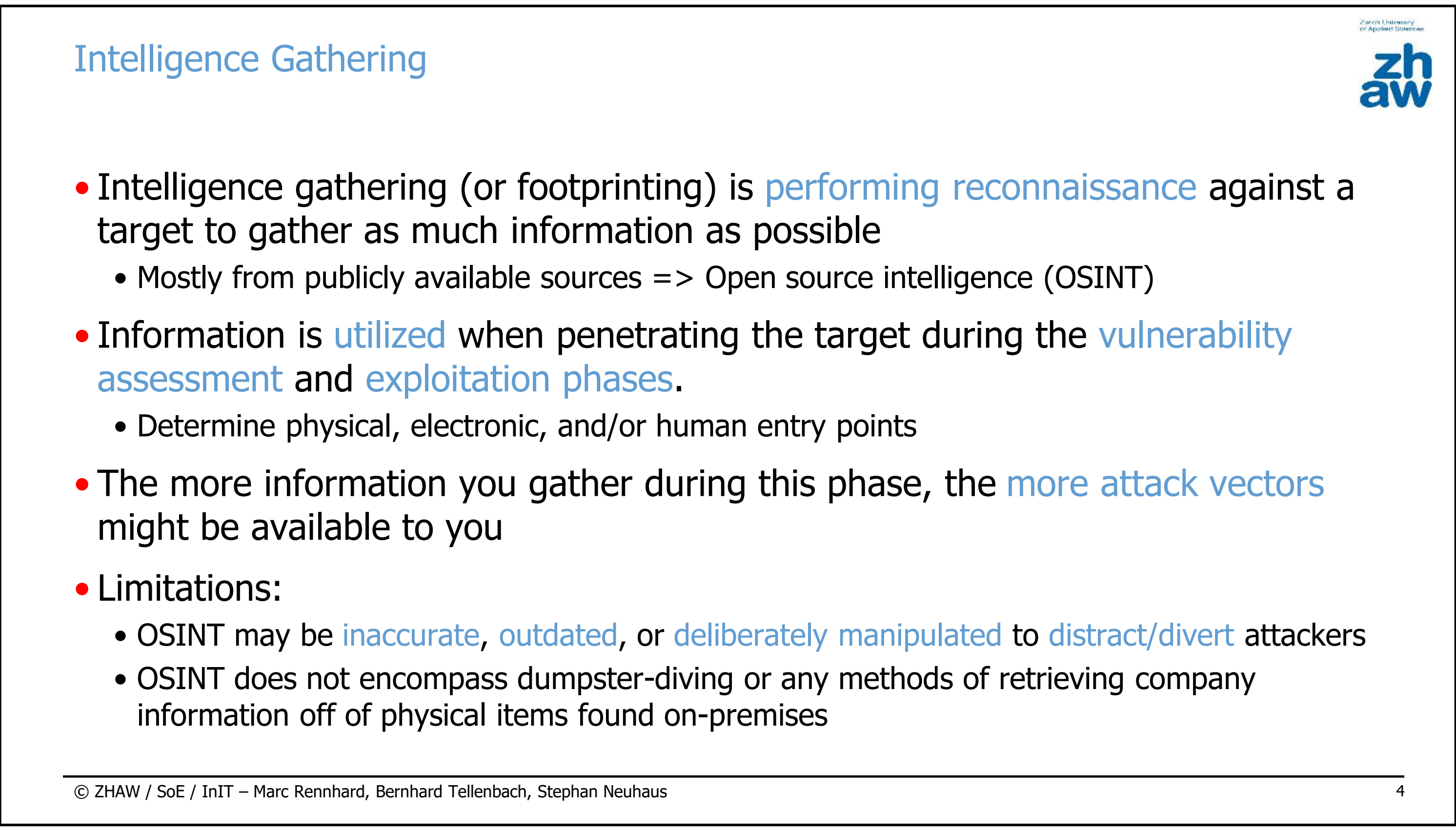
Reporting

Phases borrowed from PTES:

- **Pre-engagement interactions:** Initial communication and reasoning behind a penetration test
- **Intelligence gathering and threat modeling:** Get a better understanding of the tested organization
- **Vulnerability research, exploitation:** Identify vulnerabilities and demonstrate proof-of-concept or “real” exploits
- **Post exploitation:** Determine the value of the compromised target, maintain control and gain further access to other resources
- **Reporting:** Captures the entire process in a manner that makes sense to the customer and provides the most value to it

Goals

- You know selected methods and tools used during the intelligence gathering phase and know what information the tools can deliver
- You can make use of these methods and tools to collect different kinds of information
- You can judge whether a tool is passive, semi-passive or active and for what level of intelligence gathering (1, 2 or 3) it can be used



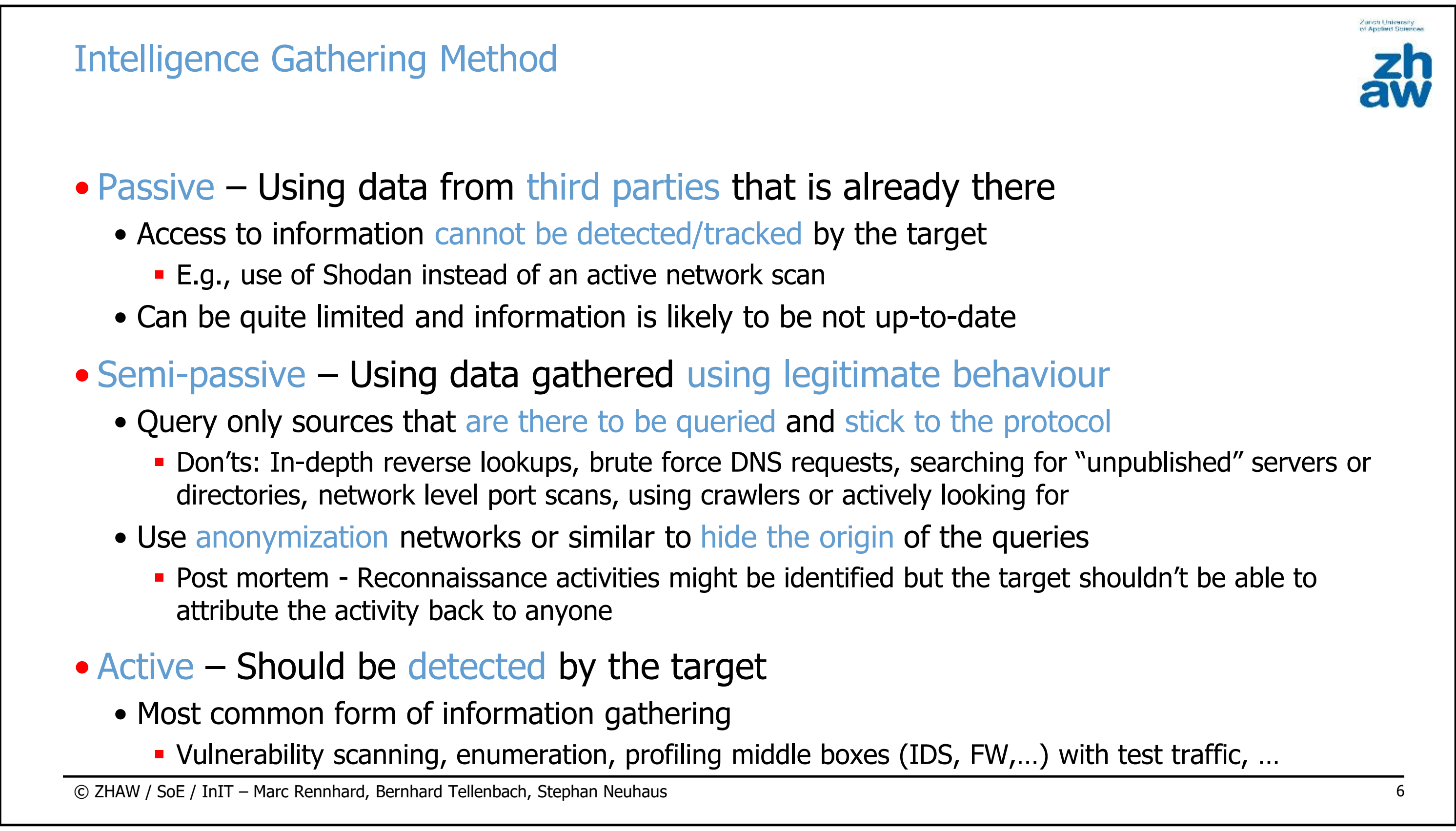
Intelligence Gathering

- Intelligence gathering (or footprinting) is performing reconnaissance against a target to gather as much information as possible
  - Mostly from publicly available sources => Open source intelligence (OSINT)
- Information is utilized when penetrating the target during the vulnerability assessment and exploitation phases.
  - Determine physical, electronic, and/or human entry points
- The more information you gather during this phase, the more attack vectors might be available to you
- Limitations:
  - OSINT may be inaccurate, outdated, or deliberately manipulated to distract/divert attackers
  - OSINT does not encompass dumpster-diving or any methods of retrieving company information off of physical items found on-premises

Open Source Intelligence (OSINT) helps to determine various entry points into an organization. These entry points can be physical, electronic, and/or human. Many companies fail to take into account what information about themselves they place in public and how this information can be used by a determined attacker. On top of that, many employees fail to take into account what information they place about themselves in public and how that information can be used to attack them or their employer.

Intelligence Gathering Levels

- The level clarifies the expected output and activities within certain real-world constraints such as time, effort, access to information, etc.
  - Level 1 – "Compliance driven‟
    - Information can be collected almost entirely by automated tools
  - Level 2 – "Best practice‟
    - Mix of automated tools and some manual analysis
    - A good understanding of the business, including information such as physical location, business relationships, organization chart, etc.
  - Level 3 – "State Sponsored‟
    - Automated tools and hours of in-depth and thorough manual analysis
    - Cultivating relationships on social networks, profiling of all key personalities of the company, in-depth study of systems and technologies they use, …
    - Most advanced, full-scope (red team)



Intelligence Gathering Method

- Passive – Using data from third parties that is already there
  - Access to information cannot be detected/tracked by the target
    - E.g., use of Shodan instead of an active network scan
  - Can be quite limited and information is likely to be not up-to-date
- Semi-passive – Using data gathered using legitimate behaviour
  - Query only sources that are there to be queried and stick to the protocol
    - Don'ts: In-depth reverse lookups, brute force DNS requests, searching for "unpublished" servers or directories, network level port scans, using crawlers or actively looking for
  - Use anonymization networks or similar to hide the origin of the queries
    - Post mortem - Reconnaissance activities might be identified but the target shouldn't be able to attribute the activity back to anyone
- Active – Should be detected by the target
  - Most common form of information gathering
    - Vulnerability scanning, enumeration, profiling middle boxes (IDS, FW,…) with test traffic, …

Shodan is a search engine that lets the user find specific types of computers (routers, servers, etc.) connected to the internet using a variety of filters. Some have also described it as a search engine of service banners, which are meta-data the server sends back to the client. This can be information about the server software, what options the service supports, a welcome message or anything else that the client can find out before interacting with the server.

Shodan collects data mostly on web servers (HTTP, port 80), as well as FTP (port 21), SSH (port 22) Telnet (port 23), SNMP (port 161), SIP (port 5060), and Real Time Streaming Protocol (RTSP, port 554). The latter can be used to access webcams and their video stream.

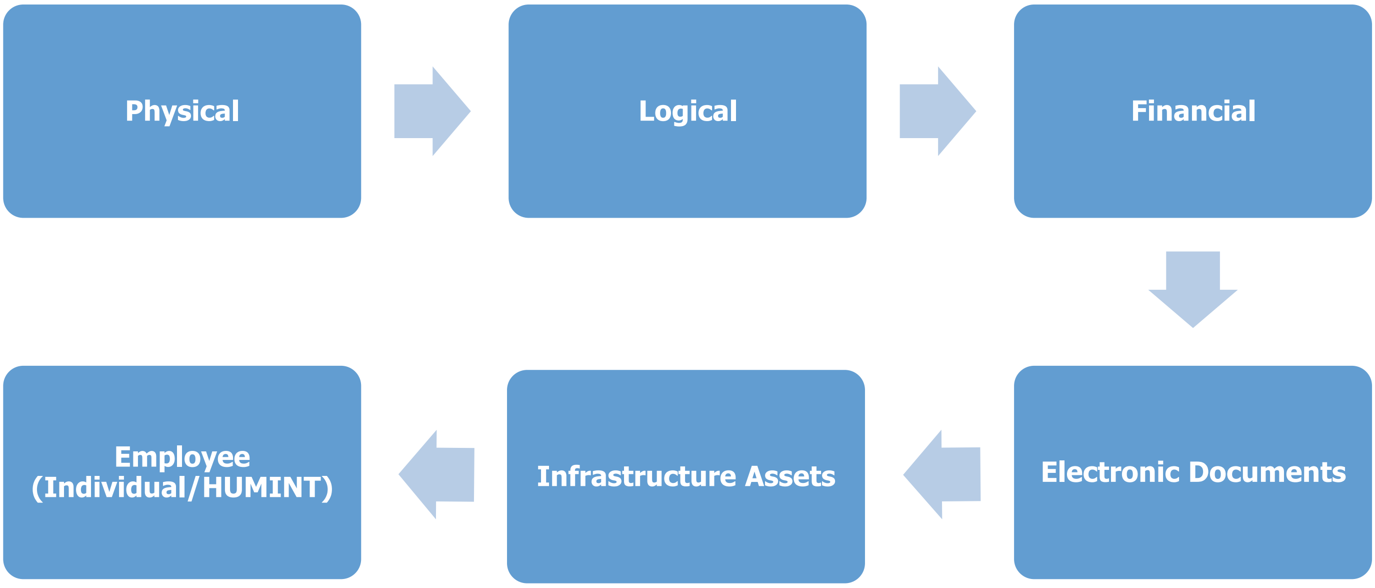
In May 2013, CNN Money released an article [1] detailing how SHODAN can be used to find dangerous systems on the Internet, including traffic light controls. They show screenshots of those systems, which provided the warning banner "DEATH MAY OCCUR !!!" upon connecting.

In January 2015, Shodan was discussed in a CSO Online article [2] addressing its pros and cons. According to one opinion, presented in the article as that of *Hagai Bar-El*, Shodan actually gives the public a good service, although it highlights vulnerable devices. This perspective is also described in one of his essays.

[1] Goldman, David (May 2, 2013). "Shodan finds the Internet's most dangerous spots". CNN Money. Retrieved 2016-03-13.

[2] "Shodan makes us all more secure". Retrieved 2016-03-13.

Intelligence to Gather



Physical

Logical

Financial

Electronic Documents

Infrastructure Assets

Employee (Individual/HUMINT)

Examples of pieces of information for the different categories.

The examples are also labelled with the information gathering level at which the information could eventually be gathered.

Physical:

- Locations (L1): Full address(es), ownership, time zones in which the target sites are located
- Relationships (L1): Shared office space, business partners, customers,…

Logical:

- Market Vertical (L1): Which industry the target resides in. i.e. financial, defense, agriculture, government, etc
- Meetings (L2/L3): Meeting Minutes published? Meetings open to public?
- Job openings (L1/L2): By viewing a list of job openings at an organization

Financial:

- Reporting (L1/L2): The targets financial reporting will depend heavily on the location of the organization. Reporting may also be made through the organizations head office and not for each branch office.

Electronic Documents:

- Document Metadata (L1/L2): Metadata or meta-content provides information about the data/document in scope. It can have information such as author/creator name, time and date, standards used/referred, location in a computer network (printer/folder/directory path/etc. info), geo-tag etc. For an image its' metadata can contain color, depth, resolution, camera make/type and even the co-ordinates and location information.
- Marketing Communications (L1/L2): Current marketing communications contain design

components (Colors, Fonts, Graphics etc..) which are for the most part used internally as well. Additional contact information including external marketing organizations.

Infrastructure Assets:

- Network blocks owned (L1): Network Blocks owned by the organization can be passively obtained from performing whois searches.
- Technologies used (L1/L2): OSINT searches through support forums, mailing lists and other resources can gather information of technologies used at the target.
- Remote access (L1/L2): Obtaining information on how employees and/or clients connect into the target for remote access provides a potential point of ingress.

Employees:

- Internet Presence: Email Address (L1), personal handles/nicknames (L1), personal domain names (L1/L2)
- Social Network Profile (L2/L3): Metadata leakage (e.g., from photos), tone and frequency of conversations,…
- History (L2/L3): Court records, political profile, sports/hobbies, professional licenses and degrees, …

Source (with more details/examples): http://www.pentest-standard.org/index.php/Intelligence_Gathering

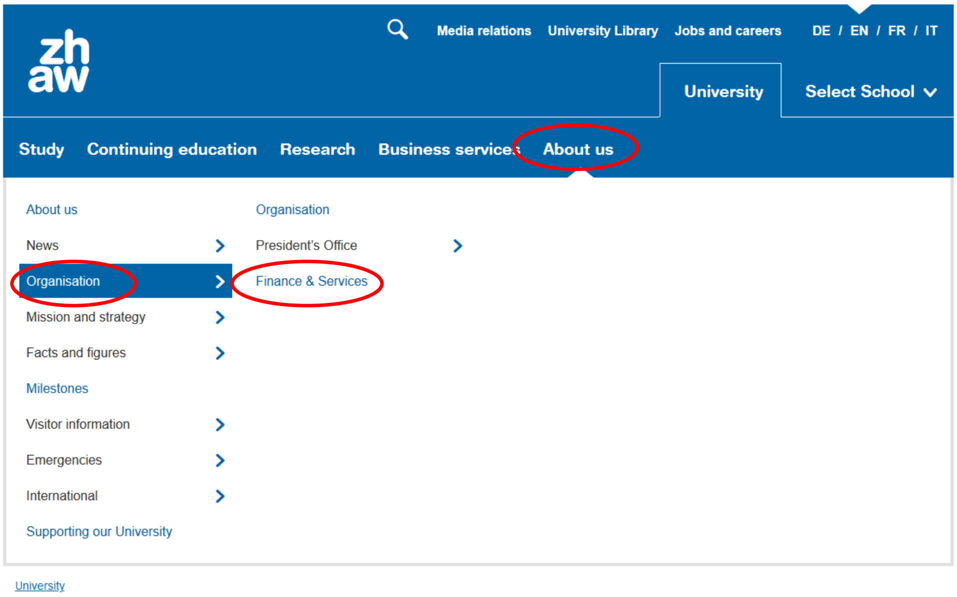
Task

- Target: The Zurich University of Applied Sciences (URL: www.zhaw.ch)
- Collect some information about the ZHAW that might be of use for a pentest
  - Physical - Locations, buildings, addresses, floor plans, locking system,…
  - Logical - Important people, business partners, clients, products, meetings, events social connections,…
  - Infrastructure Assets - Domains, IP addresses, servers, defences, …
  - Electronic documents
    - E.g., metadata analysis to identify usernames, software used, authors,…
    - Get corporate design components to craft phishing campaigns
  - Employee / Individuals (HUMINT)
    - Involves direct interaction – physical (e.g. observation) or verbal
- In practice, the focus would be much narrower

Zurich University of Applied Sciences

Browsing the Target's Website

Browsing the Target's Website (1)



Media relations University Library Jobs and careers DE / EN / FR / IT

University Select School

Study Continuing education Research Business services About us

About us

News

Organisation

Mission and strategy

Facts and figures

Milestones

Visitor information

Emergencies

International

Supporting our University

Organisation

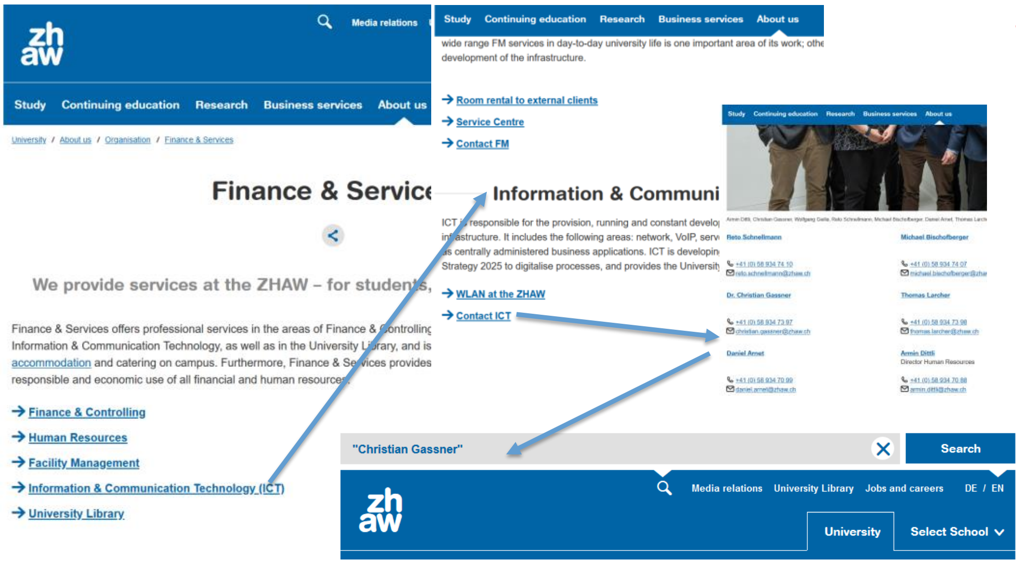
President's Office

Finance & Services

University

- The company website itself can provide lots of interesting information, especially with respect to contact persons and their roles

Browsing the Target’s Website (2)



University / About us / Organisation / Finance & Services

Finance & Servic

We provide services at the ZHAW – for students,

Finance & Services offers professional services in the areas of Finance & Controlling
Information & Communication Technology, as well as in the University Library, and is
accommodation and catering on campus. Furthermore, Finance & Services provides
responsible and economic use of all financial and human resources.

- → Finance & Controlling
- → Human Resources
- → Facility Management
- → Information & Communication Technology (ICT)
- → University Library

wide range FM services in day-to-day university life is one important area of its work; othe
development of the infrastructure.

- → Room rental to external clients
- → Service Centre
- → Contact FM

Information & Communi

ICT is responsible for the provision, running and constant develo
infrastructure. It includes the following areas: network, VoIP, serv
as centrally administered business applications. ICT is developin
Strategy 2025 to digitalise processes, and provides the University

- → WLAN at the ZHAW
- → Contact ICT

Armin Dittli, Christian Gassner, Wolfgang Gallia, Reto Schnellmann, Michael Bischofberger, Daniel Arnet, Thomas Larch

Reto Schnellmann
+41 (0) 58 934 74 10
reto.schnellmann@zhaw.ch

Michael Bischofberger
+41 (0) 58 934 74 07
michael.bischofberger@zhaw

Dr. Christian Gassner
+41 (0) 58 934 73 97
christian.gassner@zhaw.ch

Thomas Larcher
+41 (0) 58 934 73 98
thomas.larcher@zhaw.ch

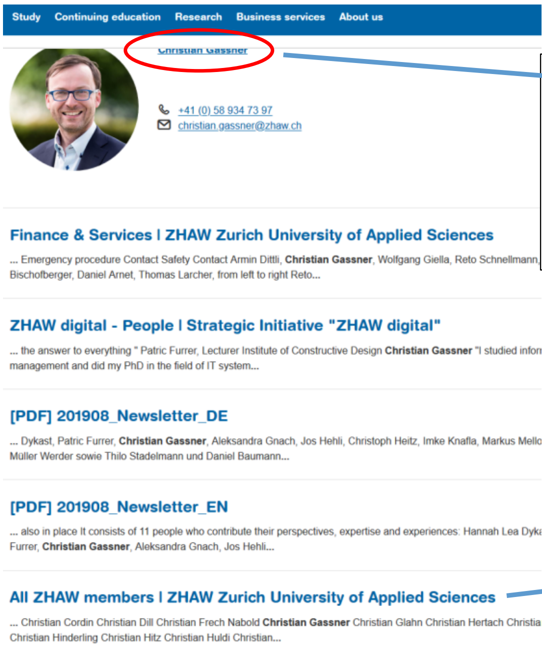
Daniel Arnet
+41 (0) 58 934 70 99
daniel.arnet@zhaw.ch

Armin Dittli
Director Human Resources
+41 (0) 58 934 70 88
armin.dittli@zhaw.ch

"Christian Gassner"

- If you identified some potentially interesting employees, look for search functions and enter the contact information of this person

Browsing the Target's Website (2)



Study Continuing education Research Business services About us

Christian Gassner

+41 (0) 58 934 73 97
christian.gassner@zhaw.ch

Finance & Services | ZHAW Zurich University of Applied Sciences

... Emergency procedure Contact Safety Contact Armin Dittli, **Christian Gassner**, Wolfgang Giella, Reto Schnellmann, Bischofberger, Daniel Arnet, Thomas Larcher, from left to right Reto...

ZHAW digital - People | Strategic Initiative "ZHAW digital"

... the answer to everything " Patric Furrer, Lecturer Institute of Constructive Design **Christian Gassner** "I studied infor management and did my PhD in the field of IT system...

[PDF] 201908_Newsletter_DE

... Dykast, Patric Furrer, **Christian Gassner**, Aleksandra Gnach, Jos Hehli, Christoph Heitz, Imke Knafla, Markus Mello Müller Werder sowie Thilo Stadelmann und Daniel Baumann...

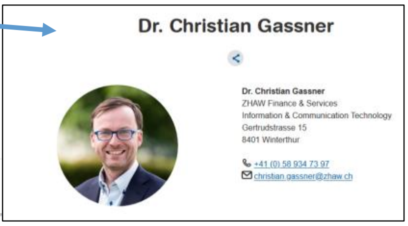
[PDF] 201908_Newsletter_EN

... also in place It consists of 11 people who contribute their perspectives, expertise and experiences: Hannah Lea Dyka Furrer, **Christian Gassner**, Aleksandra Gnach, Jos Hehli...

All ZHAW members | ZHAW Zurich University of Applied Sciences

... Christian Cordin Christian Dill Christian Frech Nabold **Christian Gassner** Christian Glahn Christian Hertach Christia Christian Hinderling Christian Hitz Christian Huldi Christian...

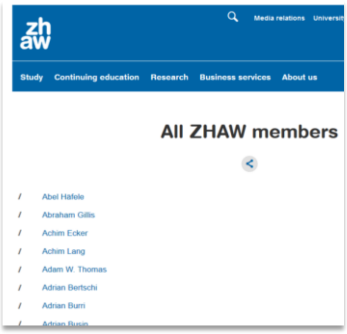
Profile Page



Dr. Christian Gassner

Dr. Christian Gassner
ZHAW Finance & Services
Information & Communication Technology
Gertrudstrasse 15
8401 Winterthur

+41 (0) 58 934 73 97
christian.gassner@zhaw.ch



Media relations Universit

Study Continuing education Research Business services About us

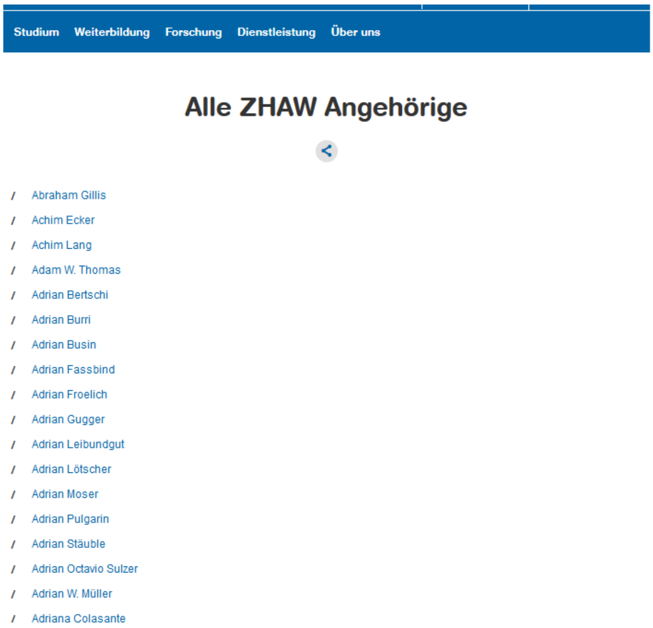
All ZHAW members

- Abel Häfele
- Abraham Gillis
- Achim Ecker
- Achim Lang
- Adam W. Thomas
- Adrian Bertschi
- Adrian Burri
- Adrian Busin

- So we have found additional information:
  - Christian Gassner has a leading position in ICT
  - We know his phone number and e-mail address
  - Valuable for social engineering attacks!

Browsing the Target's Website (3)

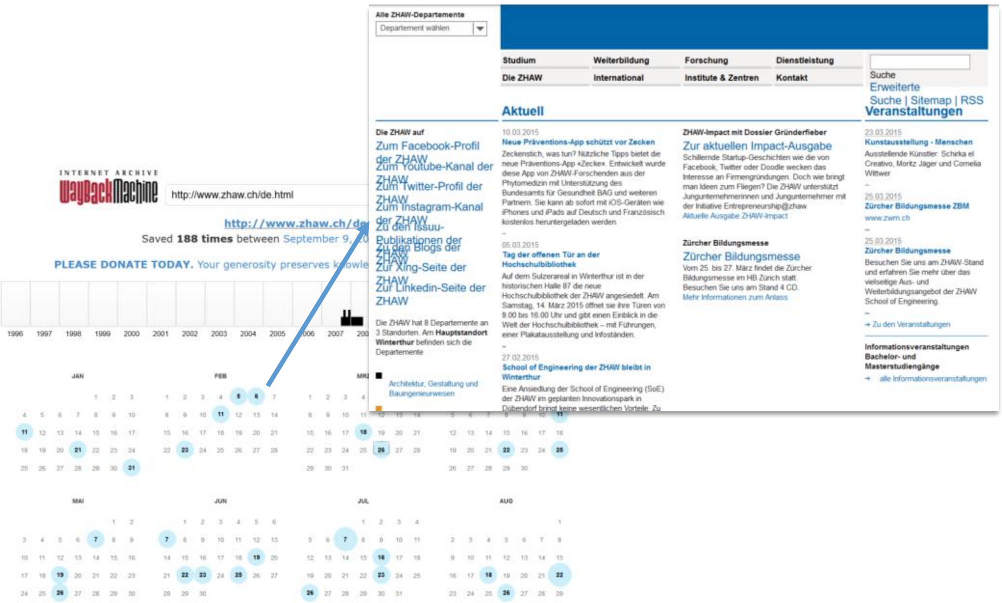
- What do you see on the page on the right?
- Discuss: Should this information be published or not? Why?



Alle ZHAW Angehörige

- Abraham Gillis
- Achim Ecker
- Achim Lang
- Adam W. Thomas
- Adrian Bertschi
- Adrian Burri
- Adrian Busin
- Adrian Fassbind
- Adrian Froelich
- Adrian Gugger
- Adrian Leibundgut
- Adrian Lötscher
- Adrian Moser
- Adrian Pulgarin
- Adrian Stäuble
- Adrian Octavio Sulzer
- Adrian W. Müller
- Adriana Colasante

Browsing the Target's Website (4)



INTERNET ARCHIVE WayBackMachine http://www.zhaw.ch/de.html

http://www.zhaw.ch/de

Saved **188 times** between September 9, 20

PLEASE DONATE TODAY. Your generosity preserves knowle

Alle ZHAW-Departemente

Departement wählen

Studium | Weiterbildung | Forschung | Dienstleistung
Die ZHAW | International | Institute & Zentren | Kontakt

Suche
Erweiterte Suche | Sitemap | RSS

Aktuell

Die ZHAW auf

Zum Facebook-Profil der ZHAW
Zum Youtube-Kanal der ZHAW
Zum Twitter-Profil der ZHAW
Zum Instagram-Kanal der ZHAW
Zu den Issuu-Publikationen der ZHAW
Zu den Blogs der ZHAW
Zur Xing-Seite der ZHAW
Zur Linkedin-Seite der ZHAW

Die ZHAW hat 8 Departemente an 3 Standorten. Am **Hauptstandort Winterthur** befinden sich die Departemente

■ Architektur, Gestaltung und Bauingenieurwesen

10.03.2015
Neue Präventions-App schützt vor Zecken
Zeckenstich, was tun? Nützliche Tipps bietet die neue Präventions-App «Zecke». Entwickelt wurde diese App von ZHAW-Forschenden aus der Phytomedizin mit Unterstützung des Bundesamts für Gesundheit BAG und weiteren Partnern. Sie kann ab sofort mit iOS-Geräten wie iPhones und iPads auf Deutsch und Französisch kostenlos heruntergeladen werden.

–

05.03.2015
Tag der offenen Tür an der Hochschulbibliothek
Auf dem Sulzerareal in Winterthur ist in der historischen Halle 87 die neue Hochschulbibliothek der ZHAW angesiedelt. Am Samstag, 14. März 2015 öffnet sie ihre Türen von 9.00 bis 16.00 Uhr und gibt einen Einblick in die Welt der Hochschulbibliothek – mit Führungen, einer Plakatausstellung und Infoständen.

–

27.02.2015
School of Engineering der ZHAW bleibt in Winterthur
Eine Ansiedlung der School of Engineering (SoE) der ZHAW im geplanten Innovationspark in Dübendorf bringt keine wesentlichen Vorteile. Zu

ZHAW-Impact mit Dossier Gründerfieber
Zur aktuellen Impact-Ausgabe
Schillernde Startup-Geschichten wie die von Facebook, Twitter oder Doodle wecken das Interesse an Firmengründungen. Doch wie bringt man Ideen zum Fliegen? Die ZHAW unterstützt Jungunternehmerinnen und Jungunternehmer mit der Initiative Entrepreneurship@zhaw.
Aktuelle Ausgabe ZHAW-Impact

Zürcher Bildungsmesse
Zürcher Bildungsmesse
Vom 25. bis 27. März findet die Zürcher Bildungsmesse im HB Zürich statt. Besuchen Sie uns am Stand 4 CD.
Mehr Informationen zum Anlass

Veranstaltungen

23.03.2015
Kunstausstellung - Menschen
Ausstellende Künstler: Schirka el Creativo, Moritz Jäger und Cornelia Wittwer

–

25.03.2015
Zürcher Bildungsmesse ZBM
www.zwm.ch

–

25.03.2015
Zürcher Bildungsmesse
Besuchen Sie uns am ZHAW-Stand und erfahren Sie mehr über das vielseitige Aus- und Weiterbildungsangebot der ZHAW School of Engineering.

–

→ Zu den Veranstaltungen

Informationsveranstaltungen Bachelor- und Masterstudiengänge
→ alle Informationsveranstaltungen

- Search for content from the past and/or in a passive way
  - Caches of search engines: `http://webcache.googleusercontent.com/search?q=cache:<URL>`
  - Use the wayback machine to search for information that has been removed from the web
  - Use Mementoweb to search multiple (Web) Archives

Memento is a United States *National Digital Information Infrastructure and Preservation Program* (NDIIPP)–funded project aimed at making Web-archived content more readily discoverable.

The project is being led by the Los Alamos National Laboratory and Old Dominion University. Rather than expecting people to know about the growing number of Web archives, and to guess which archive might hold an older version of the resource they're looking for, Memento proposes to make archived content discoverable via the original URL that the searcher already knew about. Essentially, Memento is an attempt to permit users to view any web page as it looked on a given date in the past.

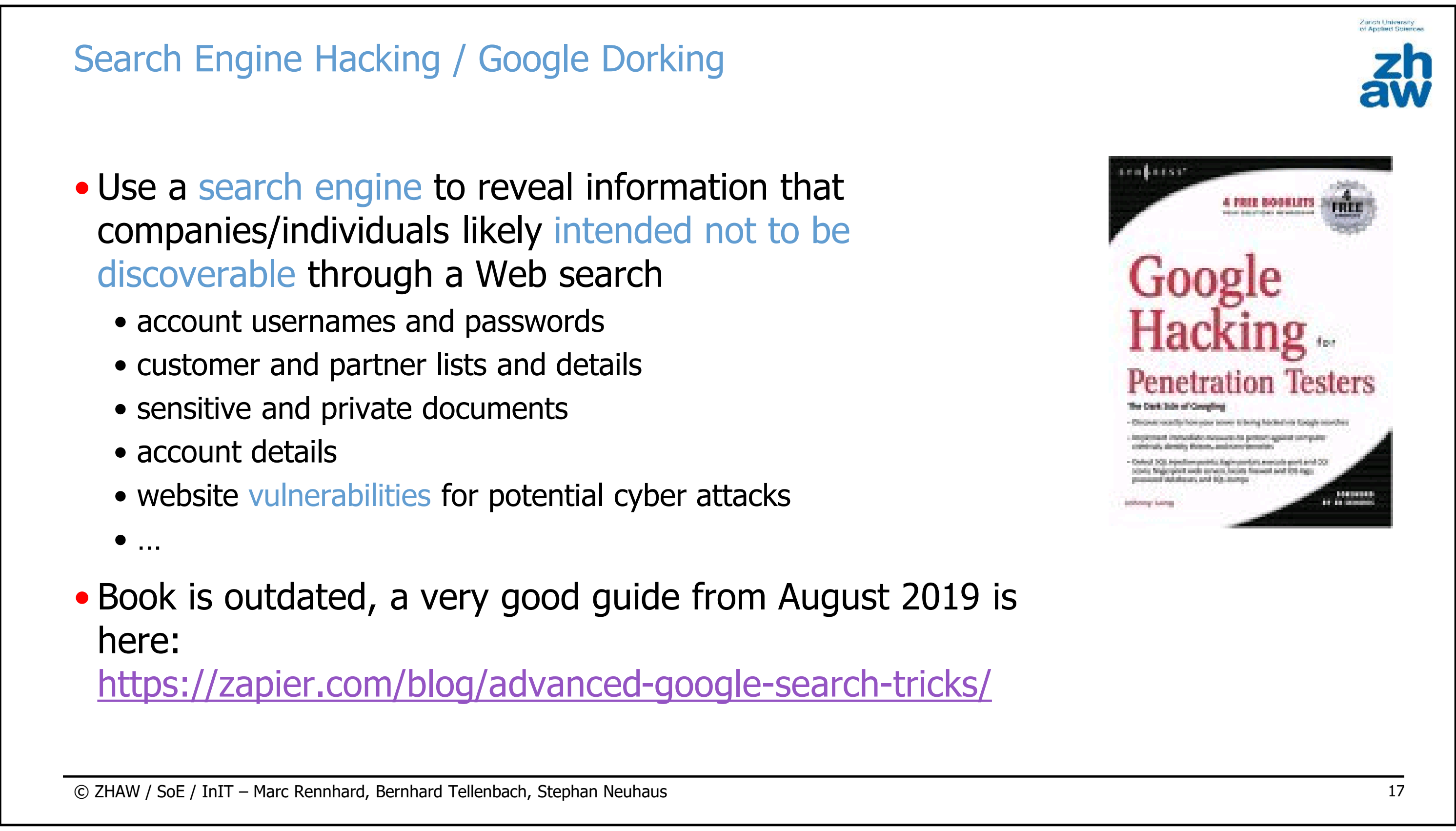
Source: https://en.wikipedia.org/wiki/Memento_Project

Search portal: http://timetravel.mementoweb.org/

Browsing the Target’s Website - Summary

Method	Semi-Active / Passive
Level	L2/L3
Information	Company data, organisation chart, employees, job openings, news/events, official points of contact, partners, publications, …
Tools	• Web browser (for online analysis) • Spiders (for offline analysis) [method: active] http://scrapy.org/ https://portswigger.net/burp/
Resources	• Websites of the target • https://archive.org/web/ • https://timetravel.mementoweb.org/
Limitations	• Rather inefficient • Quality of the search results from searches on the webpage sometimes quite bad

Search Engine Hacking



Google Hacking for Penetration Testers

Search Engine Hacking / Google Dorking

- Use a search engine to reveal information that companies/individuals likely intended not to be discoverable through a Web search
  - account usernames and passwords
  - customer and partner lists and details
  - sensitive and private documents
  - account details
  - website vulnerabilities for potential cyber attacks
  - …
- Book is outdated, a very good guide from August 2019 is here: https://zapier.com/blog/advanced-google-search-tricks/

Google Dorking - History

- 2002 : Johnny Long collects interesting Google search queries uncovering vulnerable systems and/or sensitive information => googleDorks
- 2005+ release of Google Hacking book by Johnny Long
- 2014 (!): U.S. Feds issued a warning to companies in the US to increase vigilance for Google Dorking activity by "malicious cyber actors“

Goolge Hacking - Examples

- Find websites running with wordpress at ZHAW

```
allinurl:zhaw.ch wp-content
```

Note:
inurl:zhaw.ch inurl:wp-content
does not work as expected

- ZHAW sites with “username” and “password” in the site’s content

```
zhaw intext:"username" intext:"password“
```

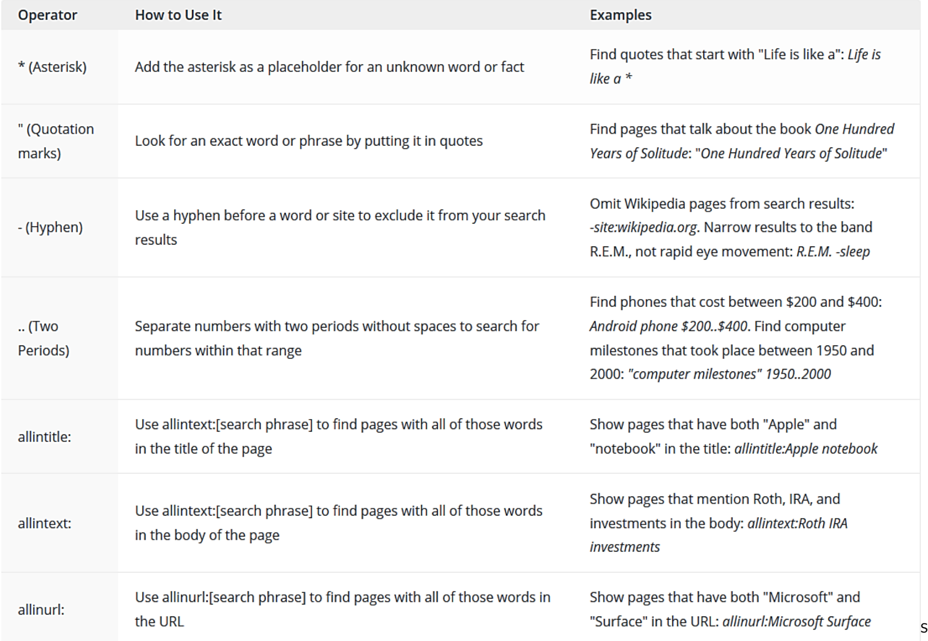
- Sites with “login” in the URL

```
site:zhaw.ch inurl:login
```

- Files with certain extensions that contain the word “login” at ZHAW

```
site:zhaw.ch ext:xml | ext:conf | ext:cnf | ext:reg | ext:inf |
ext:rdp | ext:cfg | ext:txt | ext:pdf |ext:ini login
```

Google Dorking – Some Operators (1)



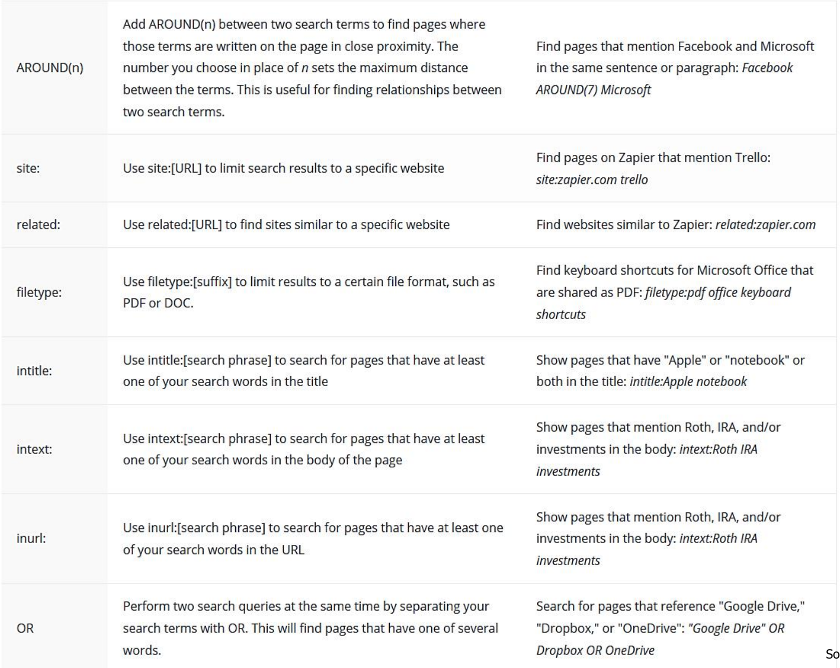
Operator	How to Use It	Examples
* (Asterisk)	Add the asterisk as a placeholder for an unknown word or fact	Find quotes that start with "Life is like a": *Life is like a **
" (Quotation marks)	Look for an exact word or phrase by putting it in quotes	Find pages that talk about the book *One Hundred Years of Solitude*: "*One Hundred Years of Solitude*"
- (Hyphen)	Use a hyphen before a word or site to exclude it from your search results	Omit Wikipedia pages from search results: *-site:wikipedia.org*. Narrow results to the band R.E.M., not rapid eye movement: *R.E.M. -sleep*
.. (Two Periods)	Separate numbers with two periods without spaces to search for numbers within that range	Find phones that cost between $200 and $400: *Android phone $200..$400*. Find computer milestones that took place between 1950 and 2000: *"computer milestones" 1950..2000*
allintitle:	Use allintext:[search phrase] to find pages with all of those words in the title of the page	Show pages that have both "Apple" and "notebook" in the title: *allintitle:Apple notebook*
allintext:	Use allintext:[search phrase] to find pages with all of those words in the body of the page	Show pages that mention Roth, IRA, and investments in the body: *allintext:Roth IRA investments*
allinurl:	Use allinurl:[search phrase] to find pages with all of those words in the URL	Show pages that have both "Microsoft" and "Surface" in the URL: *allinurl:Microsoft Surface*

Source: https://zapier.com/blog/advanced-google-search-tricks/

Knowing the operators of search engines helps to make your search more efficient.
Note that some of the operators might be removed/no longer working.

Source: https://zapier.com/blog/advanced-google-search-tricks/

Google Dorking – Some Operators (2)

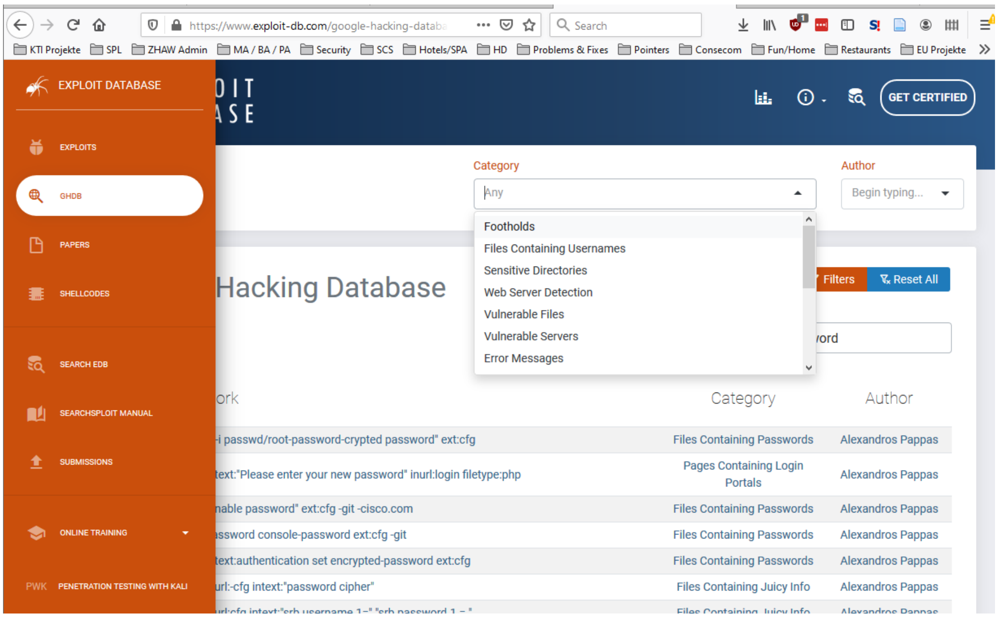


AROUND(n)	Add AROUND(n) between two search terms to find pages where those terms are written on the page in close proximity. The number you choose in place of *n* sets the maximum distance between the terms. This is useful for finding relationships between two search terms.	Find pages that mention Facebook and Microsoft in the same sentence or paragraph: *Facebook AROUND(7) Microsoft*
site:	Use site:[URL] to limit search results to a specific website	Find pages on Zapier that mention Trello: *site:zapier.com trello*
related:	Use related:[URL] to find sites similar to a specific website	Find websites similar to Zapier: *related:zapier.com*
filetype:	Use filetype:[suffix] to limit results to a certain file format, such as PDF or DOC.	Find keyboard shortcuts for Microsoft Office that are shared as PDF: *filetype:pdf office keyboard shortcuts*
intitle:	Use intitle:[search phrase] to search for pages that have at least one of your search words in the title	Show pages that have "Apple" or "notebook" or both in the title: *intitle:Apple notebook*
intext:	Use intext:[search phrase] to search for pages that have at least one of your search words in the body of the page	Show pages that mention Roth, IRA, and/or investments in the body: *intext:Roth IRA investments*
inurl:	Use inurl:[search phrase] to search for pages that have at least one of your search words in the URL	Show pages that mention Roth, IRA, and/or investments in the body: *intext:Roth IRA investments*
OR	Perform two search queries at the same time by separating your search terms with OR. This will find pages that have one of several words.	Search for pages that reference "Google Drive," "Dropbox," or "OneDrive": *"Google Drive" OR Dropbox OR OneDrive*

Source: https://zapier.com/blog/advanced-google-search-tricks/

(continued)

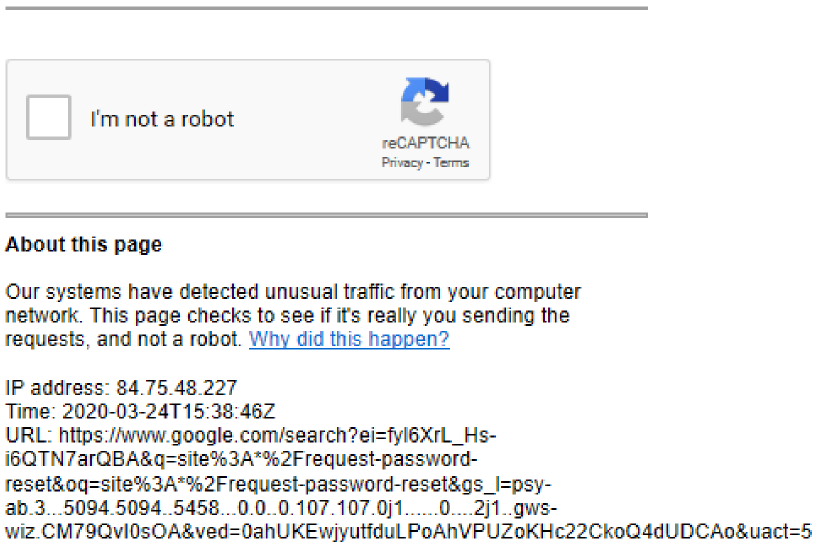
Google Hacking – Database with Useful Queries



ork	Category	Author
-i passwd/root-password-crypted password" ext:cfg	Files Containing Passwords	Alexandros Pappas
text:"Please enter your new password" inurl:login filetype:php	Pages Containing Login Portals	Alexandros Pappas
nable password" ext:cfg -git -cisco.com	Files Containing Passwords	Alexandros Pappas
assword console-password ext:cfg -git	Files Containing Passwords	Alexandros Pappas
text:authentication set encrypted-password ext:cfg	Files Containing Passwords	Alexandros Pappas
url:-cfg intext:"password cipher"	Files Containing Juicy Info	Alexandros Pappas
url:cfg intext:"srb username 1=" "srb password 1 = "	Files Containing Juicy Info	Alexandros Pappas

- Google Hacking Database (GHDB), a source for new and old search strings to search for things from different categories
- https://www.exploit-db.com/google-hacking-database/

Search Engine Hacking - Automation / Bot-Detection



About this page

Our systems have detected unusual traffic from your computer network. This page checks to see if it's really you sending the requests, and not a robot. Why did this happen?

IP address: 84.75.48.227
Time: 2020-03-24T15:38:46Z
URL: https://www.google.com/search?ei=fyl6XrL_Hs-i6QTN7arQBA&q=site%3A*%2Frequest-password-reset&oq=site%3A*%2Frequest-password-reset&gs_l=psy-ab.3...5094.5094..5458...0.0..0.107.107.0j1......0....2j1..gws-wiz.CM79Qvl0sOA&ved=0ahUKEwjyutfduLPoAhVPUZoKHc22CkoQ4dUDCAo&uact=5

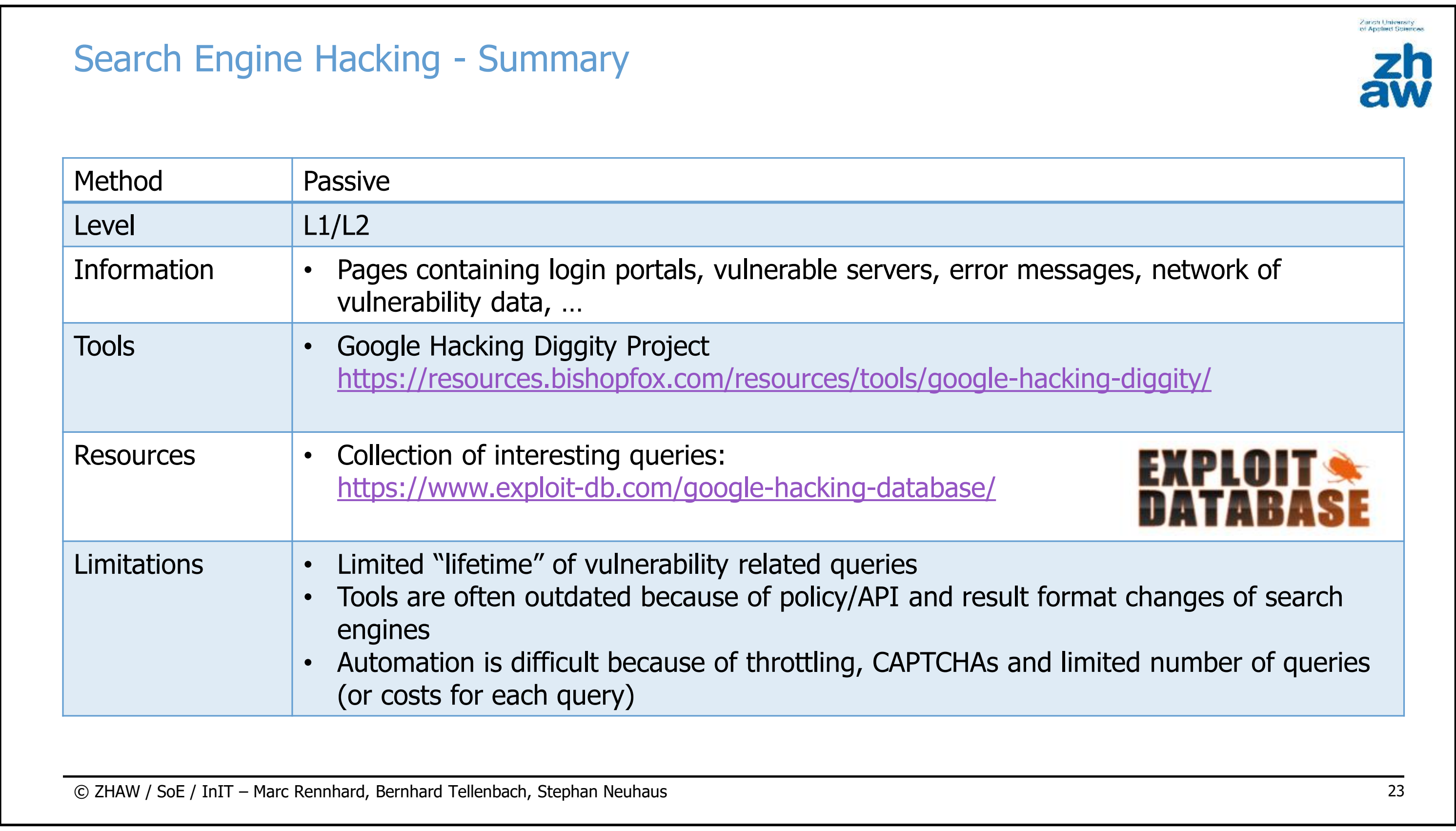
- Google's Bot Detection Approach after too many (or "suspicious"?) queries

Most search engines have a **limit** on how many queries are allowed per time unit to prevent "unfair" use without paying for the service.

When a computer runs automated queries, it violates Google Terms of Service. This includes using any software that sends queries to Google to determine how a website or webpage ranks on Google for various queries, 'Meta-searching' Google or performing 'offline' searches on Google.

If Google suspects **automated queries** from an IP address, google may show you a CAPTCHA or prevent you from querying their search engine for some time.

Furthermore, if Google suspects queries from malware or other "known-bad" queries, a CAPTCHA might also be shown.



Search Engine Hacking - Summary

Method	Passive
Level	L1/L2
Information	• Pages containing login portals, vulnerable servers, error messages, network of vulnerability data, …
Tools	• Google Hacking Diggity Project https://resources.bishopfox.com/resources/tools/google-hacking-diggity/
Resources	• Collection of interesting queries: https://www.exploit-db.com/google-hacking-database/
Limitations	• Limited "lifetime" of vulnerability related queries • Tools are often outdated because of policy/API and result format changes of search engines • Automation is difficult because of throttling, CAPTCHAs and limited number of queries (or costs for each query)

The **Google Hacking Diggity** project was for quite some time one of the "leading" google hacking tools (and more than that).

However, there was no update since 2013 and most of the stuff does not seem to work anymore or is not containing up-to-date queries.

This paper takes a closer look at Google Hacking from a security testing point of view:

Security Assessment by Google Hacking Automation Tools for the Web Sites of Korea and the USA Universities*, Mi Young Bae and Hankyu Lim, International Journal of Security and Its Applications Vol. 9, No. 5 (2015), pp. 163-174*

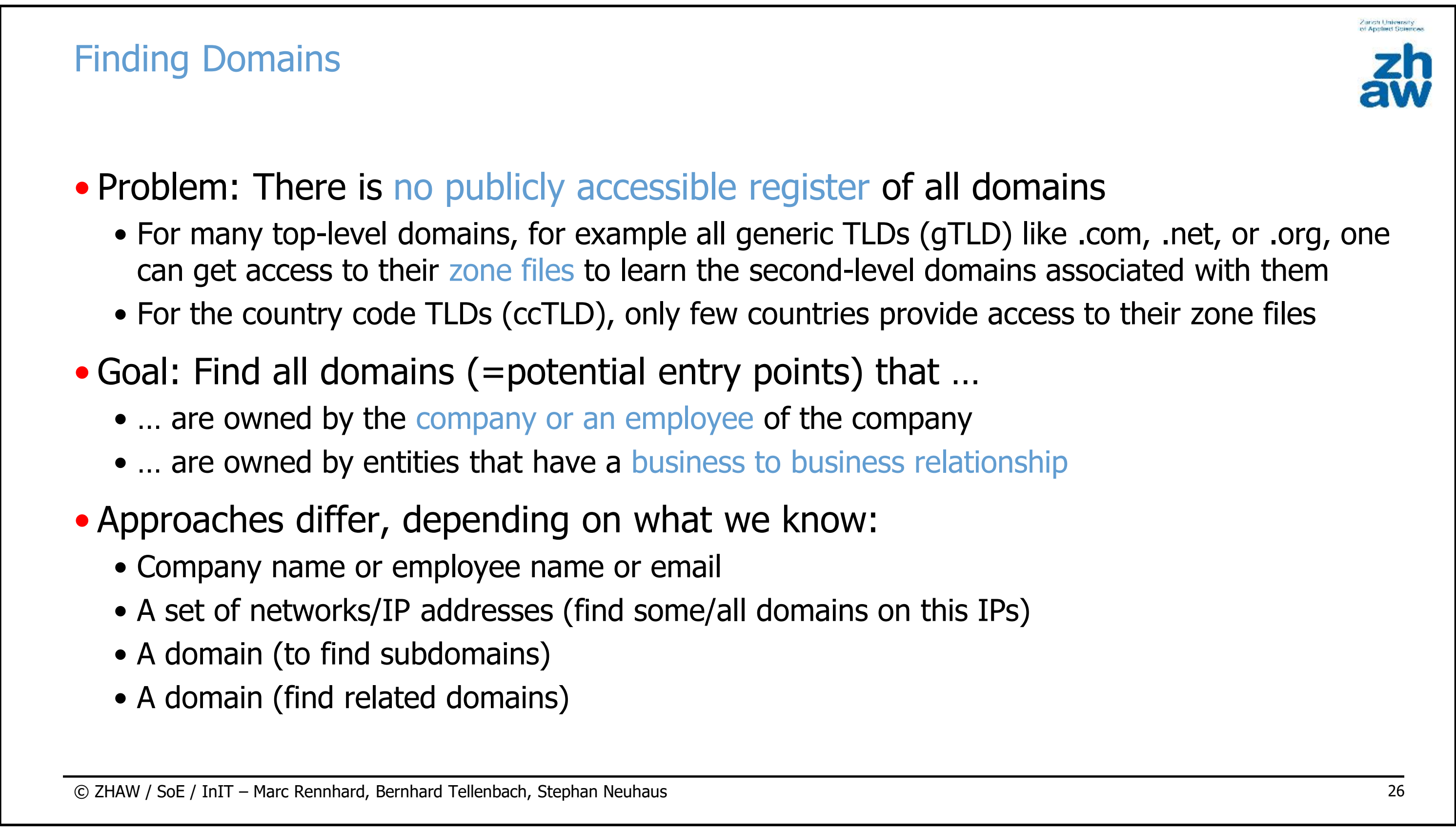
Zurich University
of Applied Sciences

zh
aw

Infrastructure Assets

Infrastructure assets

- Starting point could e.g. be an URL or company name
  - Here: https://www.zhaw.ch/de/engineering/institute-zentren/init/
- Information that could be relevant
  - Domains
  - IP addresses and network provider(s)
  - External infrastructure profile
  - (Defence) technologies used



Finding Domains

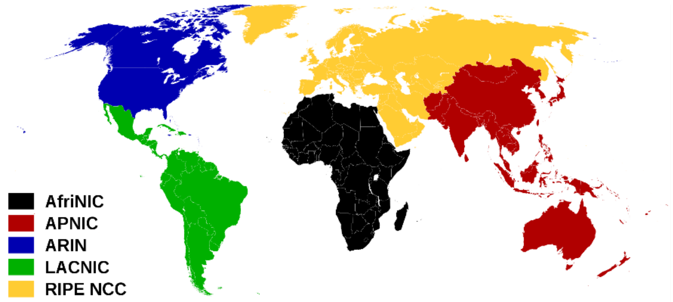
- Problem: There is no publicly accessible register of all domains
  - For many top-level domains, for example all generic TLDs (gTLD) like .com, .net, or .org, one can get access to their zone files to learn the second-level domains associated with them
  - For the country code TLDs (ccTLD), only few countries provide access to their zone files
- Goal: Find all domains (=potential entry points) that …
  - … are owned by the company or an employee of the company
  - … are owned by entities that have a business to business relationship
- Approaches differ, depending on what we know:
  - Company name or employee name or email
  - A set of networks/IP addresses (find some/all domains on this IPs)
  - A domain (to find subdomains)
  - A domain (find related domains)

Alexa Top X Pages

Alexa provides lists of the top domains sorted by country, category and more. It also provides the Alexa top 500 global sites *www.alexa.com/topsites* and even the top one million global sites.

Finding Domains: With Company Name / Employee Info

- Where to search for information on who owns a domain (company, holder name and email etc.)?
- WHOIS is a protocol for querying databases storing the registered users or assignees of an Internet resource (mainly domain name, IP address block, autonomous system)
- WHOIS servers operated by regional Internet registries (RIR) can be queried to find the Internet service provider responsible for a resource -> query the provider's server
- Entries are cross-referenced: A query to ARIN for a record which belongs to RIPE returns a pointer to the RIPE WHOIS server



- Challenges:
  - No standard for finding the responsible WHOIS server for a domain => manual, see example
  - Can we do a reverse lookup?

Regional Internet Registries

- The African Network Information Center (**AFRINIC**) serves Africa.
- The American Registry for Internet Numbers (**ARIN**) serves Antarctica, Canada, parts of the Caribbean, and the United States.
- The Asia-Pacific Network Information Centre (**APNIC**) serves East Asia, Oceania, South Asia, and Southeast Asia.
- The Latin America and Caribbean Network Information Centre (**LACNIC**) serves most of the Caribbean and all of Latin America.
- The Réseaux IP Européens Network Coordination Centre (**RIPE NCC**) serves Europe, Central Asia, Russia, and West Asia.

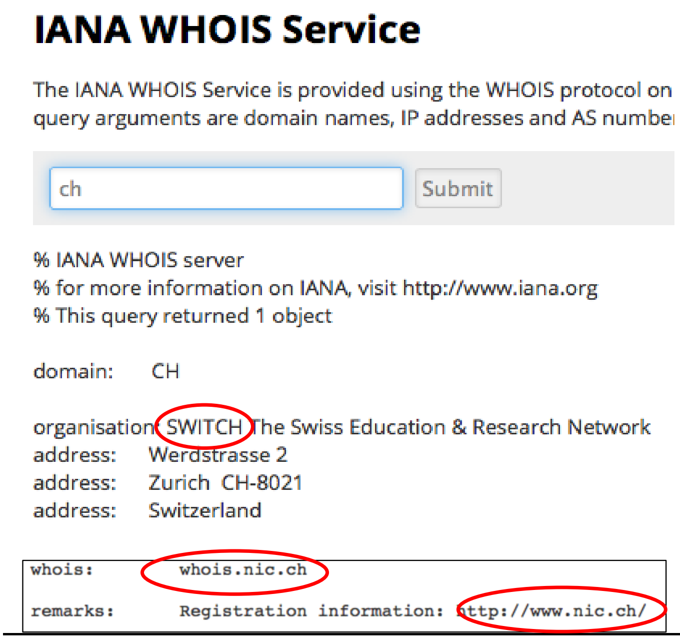
Finding Domains: With Company Name / Employee Info

- Apart from the RIR servers, servers are operated by the ISPs for their respective resources
- There are various possibilities to query for information
  - Command-line client (e.g., whois command on Linux)
  - Free web front-ends (e.g., https://www.nic.ch/whois/ for .ch domains)
- How to get the entry for a specific domain
  - Start with the database for the top level domains (TLD): whois.iana.org
  - Query for a TLD (e.g. ch) and search for the responsible organisation
  - Go to the responsible organisation and query their WHOIS database

IANA = Internet Assigned Numbers Authority

The WHOIS system also has some interesting information like contact information, name servers and location information.

Finding Domains: With Company Name / Employee Info



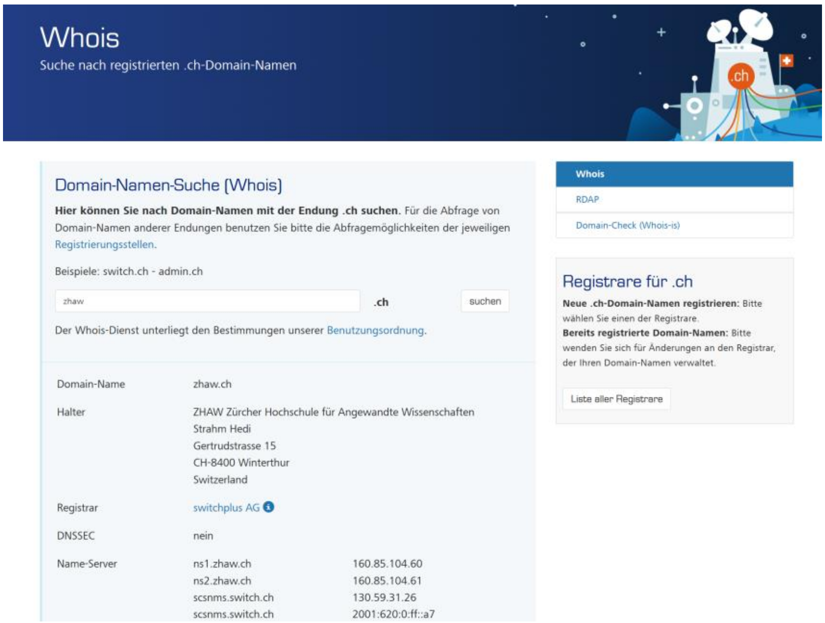
IANA WHOIS Service

The IANA WHOIS Service is provided using the WHOIS protocol on
query arguments are domain names, IP addresses and AS numbe

```
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object

domain:       CH

organisation: SWITCH The Swiss Education & Research Network
address:      Werdstrasse 2
address:      Zurich  CH-8021
address:      Switzerland

whois:        whois.nic.ch

remarks:      Registration information: http://www.nic.ch/
```

- For the ch TLD, this organisation is SWITCH and there is information about the WHOIS server and a URL for registration services

Finding Domains: With Company Name / Employee Info



Whois

Suche nach registrierten .ch-Domain-Namen

Domain-Namen-Suche (Whois)

Hier können Sie nach Domain-Namen mit der Endung .ch suchen. Für die Abfrage von Domain-Namen anderer Endungen benutzen Sie bitte die Abfragemöglichkeiten der jeweiligen Registrierungsstellen.

Beispiele: switch.ch - admin.ch

zhaw .ch suchen

Der Whois-Dienst unterliegt den Bestimmungen unserer Benutzungsordnung.

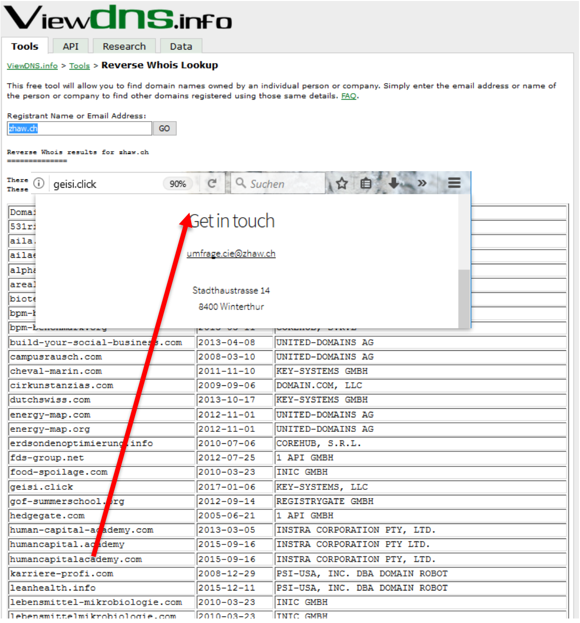
Domain-Name	zhaw.ch	
Halter	ZHAW Zürcher Hochschule für Angewandte Wissenschaften Strahm Hedi Gertrudstrasse 15 CH-8400 Winterthur Switzerland	
Registrar	switchplus AG	
DNSSEC	nein	
Name-Server	ns1.zhaw.ch	160.85.104.60
	ns2.zhaw.ch	160.85.104.61
	scsnms.switch.ch	130.59.31.26
	scsnms.switch.ch	2001:620:0:ff::a7

Registrare für .ch

Neue .ch-Domain-Namen registrieren: Bitte wählen Sie einen der Registrare.
Bereits registrierte Domain-Namen: Bitte wenden Sie sich für Änderungen an den Registrar, der Ihren Domain-Namen verwaltet.

Finding Domains: With Company Name / Employee Info

- Query the WHOIS system
  - Domain => owner/company
- Usually, no official reverse lookup
- Registrations might be protected to make tracing of the real owner hard (EU: GDPR)
- Use third party provider, e.g.:
  - http://viewdns.info/reversewhois/
  - https://whoisxmlapi.com
- They allow searches for any text in whois entries (registrant name, email address etc.)
  - Might be incomplete and/or list too many domains



ViewDNS.info > Tools > **Reverse Whois Lookup**

This free tool will allow you to find domain names owned by an individual person or company. Simply enter the email address or name of the person or company to find other domains registered using those same details. FAQ.

Registrant Name or Email Address: zhaw.ch

```
Reverse Whois results for zhaw.ch
==============

There
These
```

Get in touch

umfrage.cie@zhaw.ch

Stadthaustrasse 14
8400 Winterthur

Domai		
531ri		
aila.		
ailae		
alpha		
areal		
biote		
bpm-b		
bpm-benchmark.org		COREHUB, S.R.L.
build-your-social-business.com	2013-04-08	UNITED-DOMAINS AG
campusrausch.com	2008-03-10	UNITED-DOMAINS AG
cheval-marin.com	2011-11-10	KEY-SYSTEMS GMBH
cirkunstanzias.com	2009-09-06	DOMAIN.COM, LLC
dutchswiss.com	2013-10-17	KEY-SYSTEMS GMBH
energy-map.com	2012-11-01	UNITED-DOMAINS AG
energy-map.org	2012-11-01	UNITED-DOMAINS AG
erdsondenoptimierung.info	2010-07-06	COREHUB, S.R.L.
fds-group.net	2012-07-25	1 API GMBH
food-spoilage.com	2010-03-23	INIC GMBH
geisi.click	2017-01-06	KEY-SYSTEMS, LLC
gof-summerschool.org	2012-09-14	REGISTRYGATE GMBH
hedgegate.com	2005-06-21	1 API GMBH
human-capital-academy.com	2013-03-05	INSTRA CORPORATION PTY, LTD.
humancapital.academy	2015-09-16	INSTRA CORPORATION PTY LTD.
humancapitalacademy.com	2015-09-16	INSTRA CORPORATION PTY, LTD.
karriere-profi.com	2008-12-29	PSI-USA, INC. DBA DOMAIN ROBOT
leanhealth.info	2015-12-11	PSI-USA, INC. DBA DOMAIN ROBOT
lebensmittel-mikrobiologie.com	2010-03-23	INIC GMBH
lebensmittelmikrobiologie.com	2010-03-23	INIC GMBH

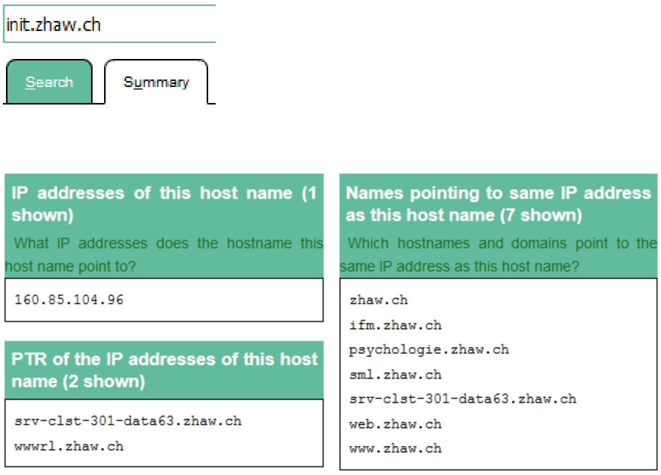
WhoisXML API, Inc. write the following about their data:

WhoisXML API, Inc. has been collecting and normalizing ownership data of domains and IP netblocks for several years. While this information is publicly available on the Internet, it is scattered into highly distributed and not always coherent data sources. Hence, trying to get these data in a useful from is really a challenge. WHOIS data, for instance, come primarily from servers still using a protocol dating back to the early days of Internet, and the operators of these servers impose several limitations on queries.

WhoisXML API has the appropriate infrastructure and expertise to collect the huge set of all these data and put it into a normalized form facilitating efficient queries. This complete and coherent database of current and historic ownership (domain WHOIS) data is the solid basis of advanced domain research and monitoring tools, now integrated into a Domain Research Suite.

Finding Domains: From a Set of Networks/IP Addresses

- Query the Domain Name System and make use the PTR records for reverse IP lookup – such entries are NOT mandatory!
  - PTR record maps an IP to a hostname
  - PTR records might not exist for an IP, only A record
- Find the domains (hostnames) associated with a given IP
  - Tool: https://www.robtex.com/dns-lookup/init.zhaw.ch (Shared tab)


init.zhaw.ch

Search | Summary

IP addresses of this host name (1 shown)

What IP addresses does the hostname this host name point to?

160.85.104.96

PTR of the IP addresses of this host name (2 shown)

srv-clst-301-data63.zhaw.ch
wwwrl.zhaw.ch

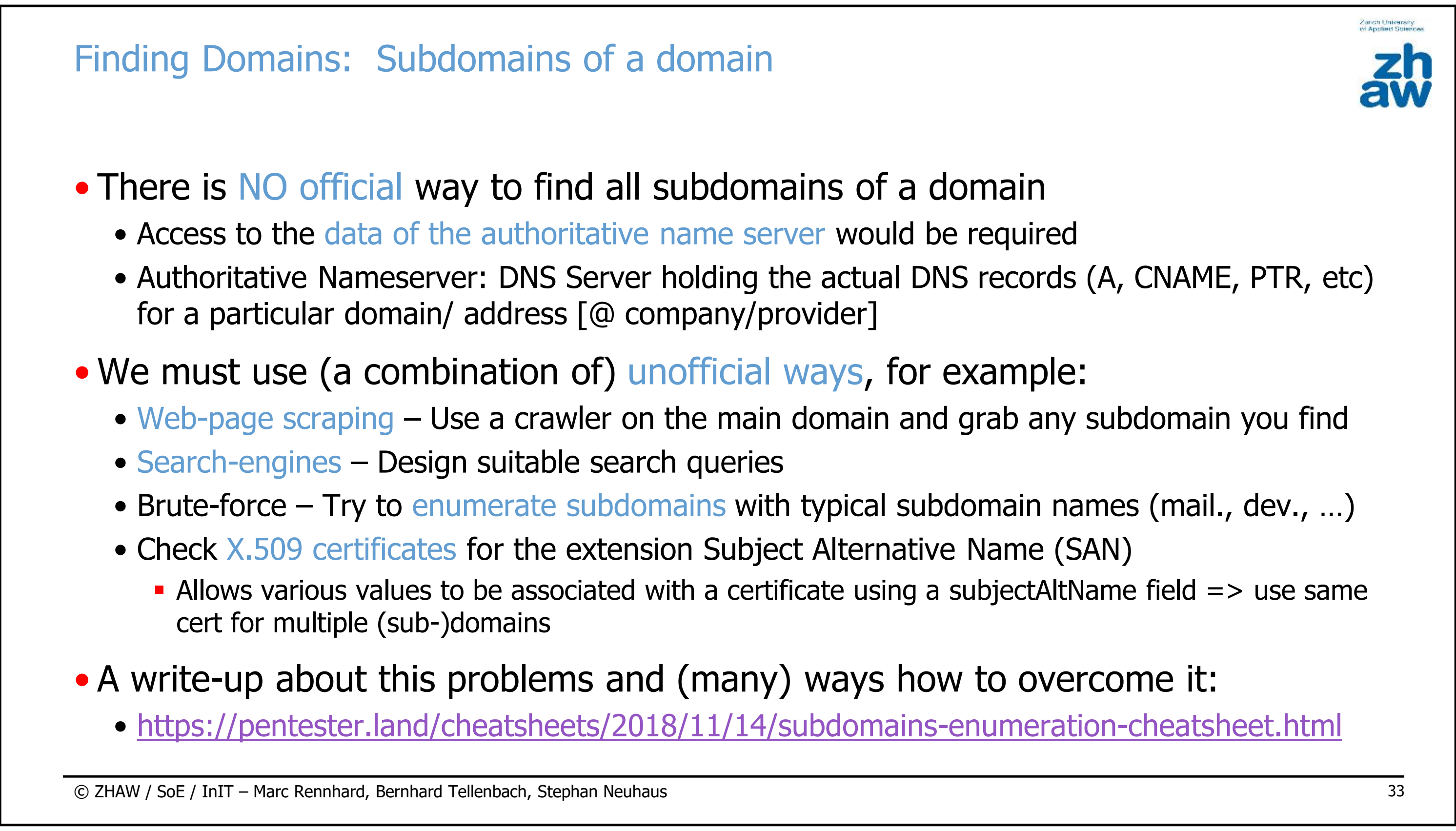
Names pointing to same IP address as this host name (7 shown)

Which hostnames and domains point to the same IP address as this host name?

zhaw.ch
ifm.zhaw.ch
psychologie.zhaw.ch
sml.zhaw.ch
srv-clst-301-data63.zhaw.ch
web.zhaw.ch
www.zhaw.ch

Some DNS entry types:

- **A:** Returns a 32-bit IPv4 address, most commonly used to map hostnames to an IP address of the host, but it is also used for DNSBLs, storing subnet masks in RFC 1101, etc.
- **AAAA**: Returns a 128-bit IPv6 address, most commonly used to map hostnames to an IP address of the host.
- **CNAME**: Alias of one name to another: the DNS lookup will continue by retrying the lookup with the new name.
- **PTR**: Pointer to a canonical name. Unlike a CNAME, DNS processing stops and just the name is returned. The most common use is for implementing reverse DNS lookups, but other uses include such things as DNS-SD.



Finding Domains: Subdomains of a domain

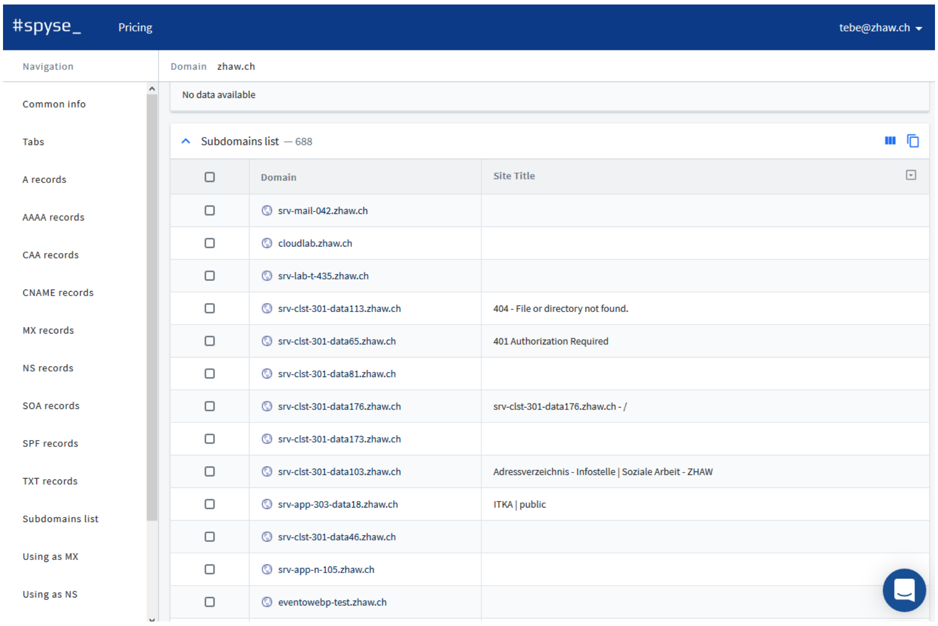
- There is NO official way to find all subdomains of a domain
  - Access to the data of the authoritative name server would be required
  - Authoritative Nameserver: DNS Server holding the actual DNS records (A, CNAME, PTR, etc) for a particular domain/ address [@ company/provider]
- We must use (a combination of) unofficial ways, for example:
  - Web-page scraping – Use a crawler on the main domain and grab any subdomain you find
  - Search-engines – Design suitable search queries
  - Brute-force – Try to enumerate subdomains with typical subdomain names (mail., dev., …)
  - Check X.509 certificates for the extension Subject Alternative Name (SAN)
    - Allows various values to be associated with a certificate using a subjectAltName field => use same cert for multiple (sub-)domains
- A write-up about this problems and (many) ways how to overcome it:
  - https://pentester.land/cheatsheets/2018/11/14/subdomains-enumeration-cheatsheet.html

Note: A recursive resolver would be a DNS server that queries an authoritative nameserver to resolve a domain/ address.

Finding Domains: Related Domains

- Examples of related domains:
  - Domains hosted on the same IP address
  - Domains using the same domain name server (NS)
    - NS is the NS of the hosting provider => many (irrelevant) relations
    - NS is the company's own NS => relations are probably few and relevant
  - Domains using the same MX (mailserver)
  - Relations based on data found on the web page for a given domain
- Use third-party tools that combine different data sources
  - … data from backward searchable domain database
  - … data from services listing all subdomains of a domain
  - Example: https://www.whoisxmlapi.com

Finding Domains: Subdomains & Related Domains



Domain zhaw.ch

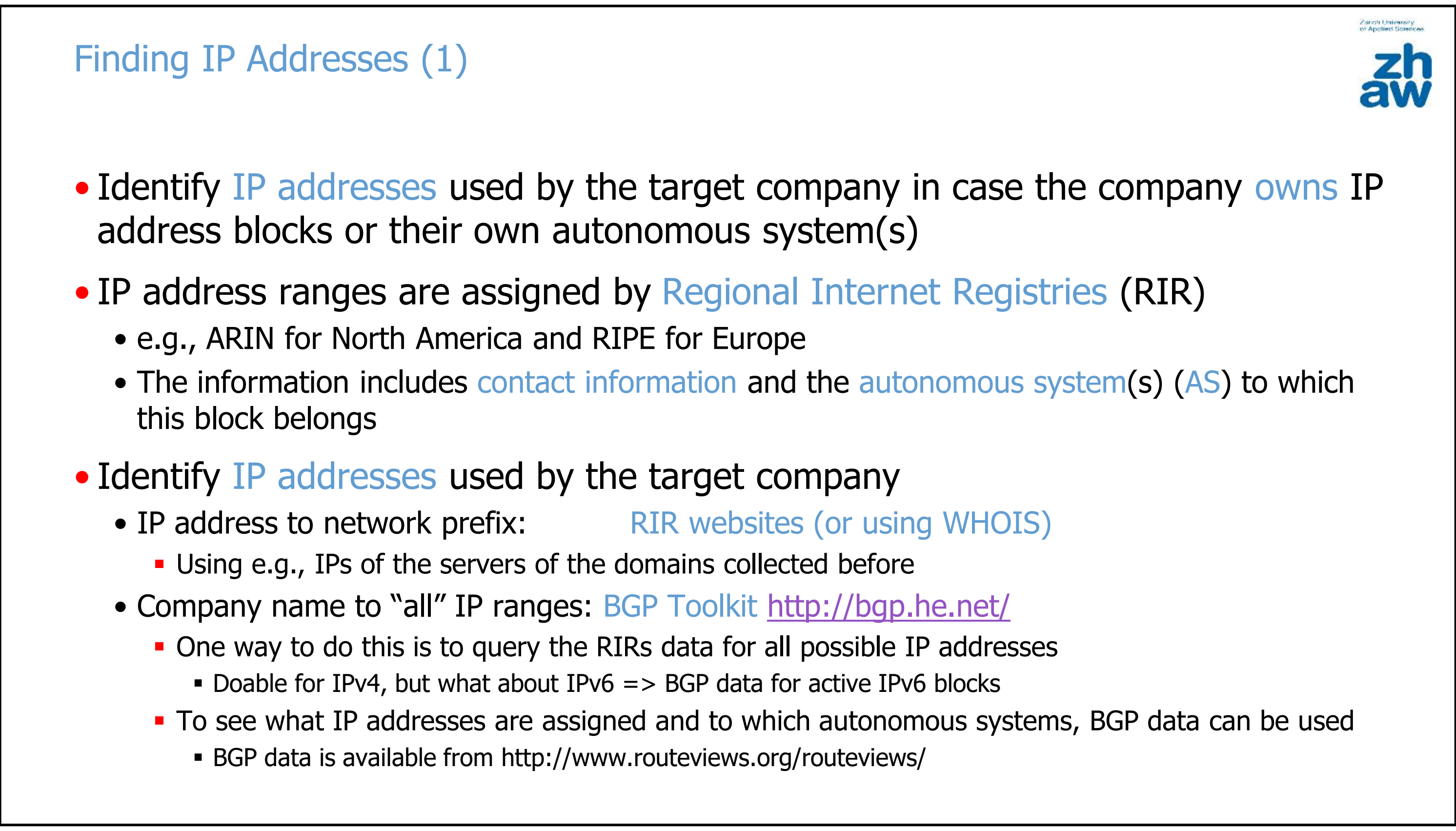
No data available

Subdomains list — 688

□	Domain	Site Title
□	srv-mail-042.zhaw.ch	
□	cloudlab.zhaw.ch	
□	srv-lab-t-435.zhaw.ch	
□	srv-clst-301-data113.zhaw.ch	404 - File or directory not found.
□	srv-clst-301-data65.zhaw.ch	401 Authorization Required
□	srv-clst-301-data81.zhaw.ch	
□	srv-clst-301-data176.zhaw.ch	srv-clst-301-data176.zhaw.ch - /
□	srv-clst-301-data173.zhaw.ch	
□	srv-clst-301-data103.zhaw.ch	Adressverzeichnis - Infostelle | Soziale Arbeit - ZHAW
□	srv-app-303-data18.zhaw.ch	ITKA | public
□	srv-clst-301-data46.zhaw.ch	
□	srv-app-n-105.zhaw.ch	
□	eventowebp-test.zhaw.ch	

Finding Domains - Summary

Method	Passive : WHOIS / search engines / 3rd party data sources Active : DNS
Level	L1 / L2
Information	Domain names and additional information like the owner of a domain, technical contact, contact phone and email, administrator’s name, name servers …
Tools	• WHOIS tools and websites • DNS tools • Search engines • https://findsubdomains.com/ • https://www.robtex.com/dns-lookup/init.zhaw.ch
Resources	• WHOIS, DNS, search engines
Limitations	• 3rd party data sources - queries might return irrelevant results or not all results



Finding IP Addresses (1)

- Identify IP addresses used by the target company in case the company owns IP address blocks or their own autonomous system(s)
- IP address ranges are assigned by Regional Internet Registries (RIR)
  - e.g., ARIN for North America and RIPE for Europe
  - The information includes contact information and the autonomous system(s) (AS) to which this block belongs
- Identify IP addresses used by the target company
  - IP address to network prefix: RIR websites (or using WHOIS)
    - Using e.g., IPs of the servers of the domains collected before
  - Company name to “all” IP ranges: BGP Toolkit http://bgp.he.net/
    - One way to do this is to query the RIRs data for all possible IP addresses
      - Doable for IPv4, but what about IPv6 => BGP data for active IPv6 blocks
    - To see what IP addresses are assigned and to which autonomous systems, BGP data can be used
      - BGP data is available from http://www.routeviews.org/routeviews/

BGP

Border Gateway Protocol (BGP) is a standardized exterior gateway protocol designed to exchange routing and reachability information among autonomous systems (AS) on the Internet. The protocol is classified as a path vector protocol. The Border Gateway Protocol makes routing decisions based on paths, network policies, or rule-sets configured by a network administrator and is involved in making core routing decisions.

BGP announcements contain information which network prefixes are reachable over which network path (AS-path).

Network Prefix

The IP address space is split into different networks identified by a network prefix in the form <network address>/<netmask>, e.g., 160.85.0.0/16.

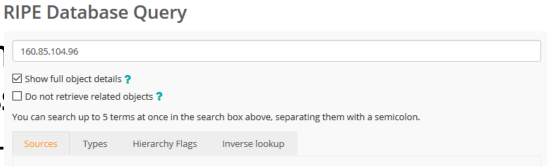
Large organisations usually have their own public IP space identified by a network prefix.

Autonomous System (AS)

An autonomous system (AS) is a collection of connected Internet Protocol (IP) routing prefixes under the control of one or more network operators on behalf of a single administrative entity / domain.

Finding IP Addresses (2)

- Getting the r
an IP addres
- Query the RI

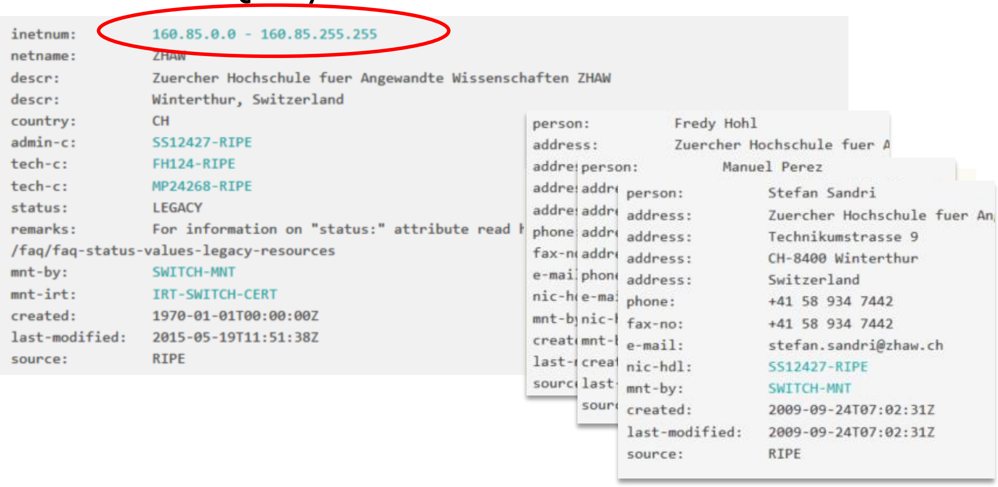


RIPE Database Query

```
160.85.104.96
```

☑ Show full object details ?
☐ Do not retrieve related objects ?

You can search up to 5 terms at once in the search box above, separating them with a semicolon.



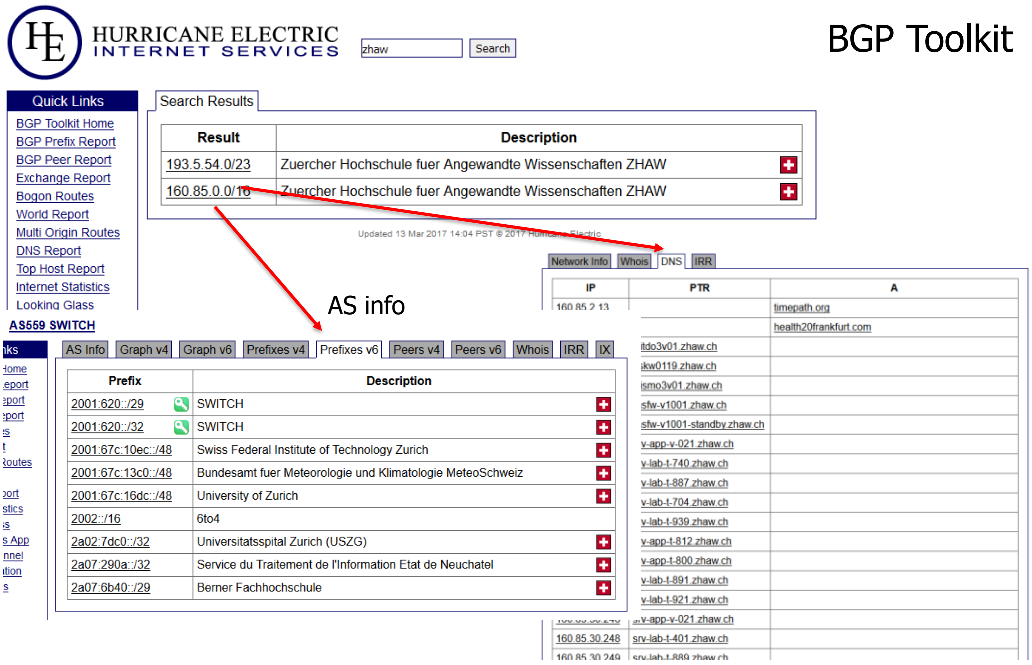
```
inetnum:        160.85.0.0 - 160.85.255.255
netname:        ZHAW
descr:          Zuercher Hochschule fuer Angewandte Wissenschaften ZHAW
descr:          Winterthur, Switzerland
country:        CH
admin-c:        SS12427-RIPE
tech-c:         FH124-RIPE
tech-c:         MP24268-RIPE
status:         LEGACY
remarks:        For information on "status:" attribute read h
/faq/faq-status-values-legacy-resources
mnt-by:         SWITCH-MNT
mnt-irt:        IRT-SWITCH-CERT
created:        1970-01-01T00:00:00Z
last-modified:  2015-05-19T11:51:38Z
source:         RIPE
```

```
person:         Fredy Hohl
address:        Zuercher Hochschule fuer A
addre
addre
addre
phone
fax-n
e-mai
nic-h
mnt-b
creat
last-
sourc
```

```
person:         Manuel Perez
addr
addr
addr
addr
phon
e-ma
nic-
mnt-
crea
last
sour
```

```
person:         Stefan Sandri
address:        Zuercher Hochschule fuer An
address:        Technikumstrasse 9
address:        CH-8400 Winterthur
address:        Switzerland
phone:          +41 58 934 7442
fax-no:         +41 58 934 7442
e-mail:         stefan.sandri@zhaw.ch
nic-hdl:        SS12427-RIPE
mnt-by:         SWITCH-MNT
created:        2009-09-24T07:02:31Z
last-modified:  2009-09-24T07:02:31Z
source:         RIPE
```

Finding IP Addresses (3)



BGP Toolkit

AS info

Result	Description
193.5.54.0/23	Zuercher Hochschule fuer Angewandte Wissenschaften ZHAW
160.85.0.0/16	Zuercher Hochschule fuer Angewandte Wissenschaften ZHAW

Prefix	Description
2001:620::/29	SWITCH
2001:620::/32	SWITCH
2001:67c:10ec::/48	Swiss Federal Institute of Technology Zurich
2001:67c:13c0::/48	Bundesamt fuer Meteorologie und Klimatologie MeteoSchweiz
2001:67c:16dc::/48	University of Zurich
2002::/16	6to4
2a02:7dc0::/32	Universitatsspital Zurich (USZG)
2a07:290a::/32	Service du Traitement de l'Information Etat de Neuchatel
2a07:6b40::/29	Berner Fachhochschule

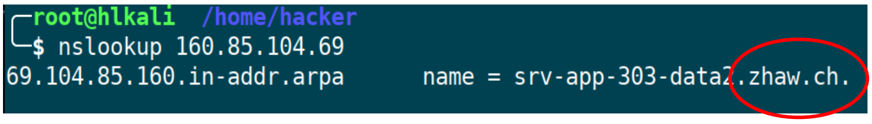
IP	PTR	A
160.85.2.13		timepath.org
		health20frankfurt.com
	itdo3v01.zhaw.ch	
	skw0119.zhaw.ch	
	ismo3v01.zhaw.ch	
	sfw-v1001.zhaw.ch	
	sfw-v1001-standby.zhaw.ch	
	v-app-v-021.zhaw.ch	
	v-lab-t-740.zhaw.ch	
	v-lab-t-887.zhaw.ch	
	v-lab-t-704.zhaw.ch	
	v-lab-t-939.zhaw.ch	
	v-app-t-812.zhaw.ch	
	v-app-t-800.zhaw.ch	
	v-lab-t-891.zhaw.ch	
	v-lab-t-921.zhaw.ch	
160.85.30.246	srv-app-v-021.zhaw.ch	
160.85.30.248	srv-lab-t-401.zhaw.ch	
160.85.30.249	srv-lab-t-889.zhaw.ch	

Finding IP Addresses (4)

- Identify IP addresses used by the target company in case the company does not own IP address blocks or their own autonomous system(s)
- Identify IP addresses used by the target company
  - Domains to IP addresses: Forward-DNS
    - IP address where the domain is hosted
    - Some additional IP addresses: name servers and mail servers
  - IP address to more IP addresses: Reverse-DNS and other methods
    - Determine the network block of an IP address and perform reverse DNS lookups or other checks to determine whether that IP address is also used by the target
  - Use the search function of services (e.g., with company names) that provide information about IP addresses
    - Search Engine Hacking (incomplete, web-only)
    - Shodan or Censys (see passive scanning slides)

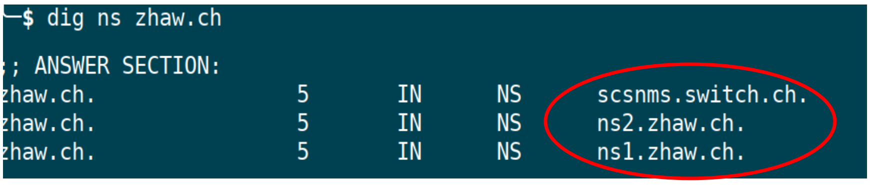
Finding IP Addresses (5)

- DNS system: Get IPs/Hostnames of name- and mail servers
- One way to do this:
  - Get the domain for the IP



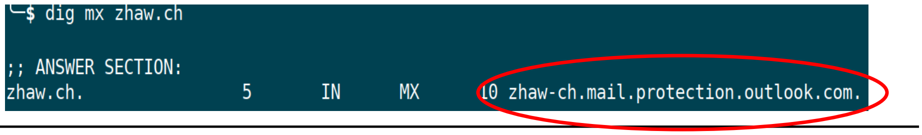
```
┌root@hlkali  /home/hacker
└$ nslookup 160.85.104.69
69.104.85.160.in-addr.arpa      name = srv-app-303-data2.zhaw.ch.
```

  - Use the dig command line tool (*ix):
    - DNS Servers



```
└$ dig ns zhaw.ch

;; ANSWER SECTION:
zhaw.ch.                 5       IN      NS      scsnms.switch.ch.
zhaw.ch.                 5       IN      NS      ns2.zhaw.ch.
zhaw.ch.                 5       IN      NS      ns1.zhaw.ch.
```

    - Mailserver



```
└$ dig mx zhaw.ch

;; ANSWER SECTION:
zhaw.ch.            5       IN      MX      10 zhaw-ch.mail.protection.outlook.com.
```

DNS Zone Transfers

Zone transfers are used to update the database of a slave name server with the data from the master name server. If configured correctly, a name server should allow a zone transfer only for its slave name server(s), so random users from random computers cannot easily download the entire database. If a name server happens to be incorrectly configured and a zone transfer can be done by anyone, this can be easily exploited using the nslookup command line tool.

In the ZHAW case, using nslookup to perform a zone transfer would be done as follows:

```
user@ubuntu> nslookup
> server ns1.zhaw.ch
Default server: ns1.zhaw.ch
Address: 160.85.104.60#53
> ls -d zhaw.ch.
The 'ls' command is not implemented.
```

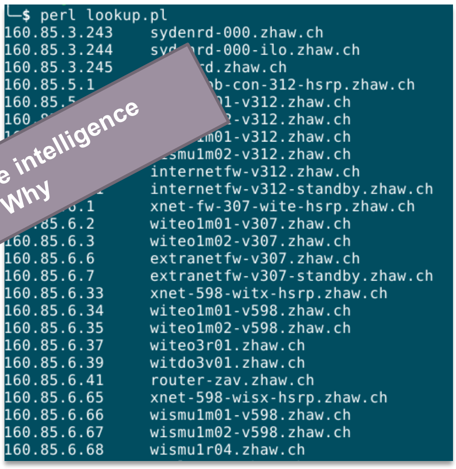
As you can see from the last line returned by the nameserver, the zone transfer could not be carried out, which is usually the case today. Nevertheless, one could give it a try.

Dig can also be used to attempts a zone transfer: dig zhaw.ch @ns1.zhaw.ch axfr

Finding IP Addresses (6)

- Use the DNS system to get all hostnames and “active” IP addresses
- Do reverse DNS lookups for all IP addresses, for example by scripting the requests.
- Example: Class B (/16) networks:

```
#! /usr/bin/perl

Use Socket;

$b_net = "160.85";
for ($i=0; $i<255; $i++) {
  for ($j=0; $j<255; $j++) {
    $ip = "$b_net.$i.$j";
    $ipaddr = inet_aton($ip);
    $name = gethostbyaddr($i                r);
    if ($name) {
      print "${ip}\t${name}\
    }
  }
}
```



```
└─$ perl lookup.pl
160.85.3.243      sydenrd-000.zhaw.ch
160.85.3.244      syd  rd-000-ilo.zhaw.ch
160.85.3.245           d.zhaw.ch
160.85.5.1             b-con-312-hsrp.zhaw.ch
160.85.5               1-v312.zhaw.ch
160                    -v312.zhaw.ch
                       m01-v312.zhaw.ch
                       smu1m02-v312.zhaw.ch
                  internetfw-v312.zhaw.ch
                  internetfw-v312-standby.zhaw.ch
      .1          xnet-fw-307-wite-hsrp.zhaw.ch
 85.6.2           witeo1m01-v307.zhaw.ch
160.85.6.3        witeo1m02-v307.zhaw.ch
160.85.6.6        extranetfw-v307.zhaw.ch
160.85.6.7        extranetfw-v307-standby.zhaw.ch
160.85.6.33       xnet-598-witx-hsrp.zhaw.ch
160.85.6.34       witeo1m01-v598.zhaw.ch
160.85.6.35       witeo1m02-v598.zhaw.ch
160.85.6.37       witeo3r01.zhaw.ch
160.85.6.39       witdo3v01.zhaw.ch
160.85.6.41       router-zav.zhaw.ch
160.85.6.65       xnet-598-wisx-hsrp.zhaw.ch
160.85.6.66       wismu1m01-v598.zhaw.ch
160.85.6.67       wismu1m02-v598.zhaw.ch
160.85.6.68       wismu1r04.zhaw.ch
```

Is this active or passive intelligence gathering? Why

Reverse DNS Lookups

Note that DNS entries do not always contain an inverse entry (PTR) which allows resolving an IP address into its hostname, although in many cases, they do. Therefore, the above script won’t necessarily detect all IP address to host mappings.

Finding IP Addresses - Summary

Method	Passive : RIR and other 3rd party data bases Semi-Active : (DNS) Active : DNS
Level	L1/L2/(L3)
Information	IPs and network prefixes of the target (and relevant third parties)
Tools	• WHOIS and related APIs (ICANN, IANA, RIPE,…) • nslookup and other DNS tools • Third party tools • BGP Toolkit (based on BGP and other data) • Shodan / Censys (scanning based)
Resources	• DNS System • WHOIS / RIRs • BGP Data • Website data
Limitations	• Passive discovery is almost certainly incomplete and the information should be verified

Scanning

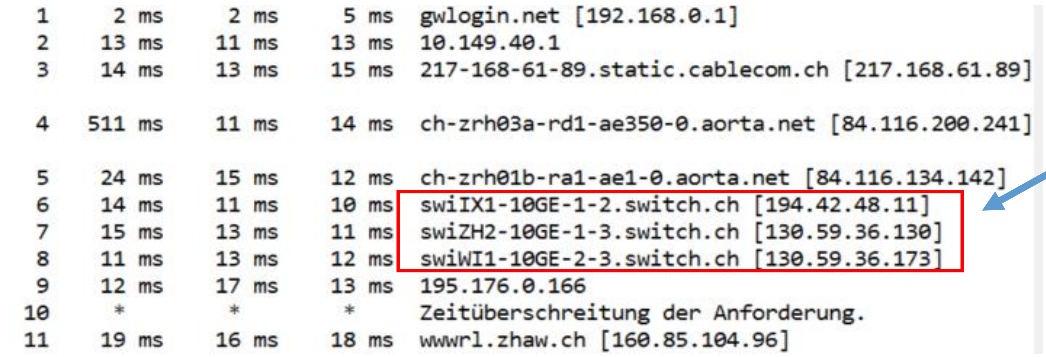
- Based on the previous results, the target company’s networks and hosts are examined in more detail during scanning
- Determine the network structure, especially when analysing larger environments
- Find hosts that are reachable / visible by the tester
  - Depends on the location of the tester, e.g. inside or outside the company
- Analyse the hosts in detail
  - Identify operating systems
  - Determine services running on the hosts and the corresponding software products
  - This can give hints at possible vulnerabilities present on a target host

Scanning – Network Structure (1)

- The network's structure is relevant when analysing larger environments
  - Provides information about interesting "areas" of a network (e.g. a DMZ)
    - Helps to prioritize which areas to analyse in detail during host scanning
  - It may provide "attack paths" into the network
    - Assume you want to compromise a host that cannot be reached directly from your location
    - Knowing the network structure helps to identify hosts that are in the same network than the target, which could then be used as a stepping stone
- Traditionally, traceroute is the tool of choice to analyse the network structure
  - Lists all hops (IP addresses) to the target system
  - The standard traceroute use UDP or ICMP packets
    - On *ix systems, UDP is usually the default and ICMP can be used with the -I option
  - There is also tcptraceroute that uses TCP packets
  - Its a good idea to use both options, especially if one is not successful

Scanning – Network Structure (2)

- Let’s start with a traceroute to www.zhaw.ch. What do we learn here?
  - Two(?) ZHAW hosts are visible
  - Probably one router and the web server itself
  - So we have learned a small part of the internal network structure and IP addresses
  - But we have no clue yet about network sizes etc.



```
  1     2 ms     2 ms     5 ms  gwlogin.net [192.168.0.1]
  2    13 ms    11 ms    13 ms  10.149.40.1
  3    14 ms    13 ms    15 ms  217-168-61-89.static.cablecom.ch [217.168.61.89]

  4   511 ms    11 ms    14 ms  ch-zrh03a-rd1-ae350-0.aorta.net [84.116.200.241]

  5    24 ms    15 ms    12 ms  ch-zrh01b-ra1-ae1-0.aorta.net [84.116.134.142]
  6    14 ms    11 ms    10 ms  swiIX1-10GE-1-2.switch.ch [194.42.48.11]
  7    15 ms    13 ms    11 ms  swiZH2-10GE-1-3.switch.ch [130.59.36.130]
  8    11 ms    13 ms    12 ms  swiWI1-10GE-2-3.switch.ch [130.59.36.173]
  9    12 ms    17 ms    13 ms  195.176.0.166
 10     *        *        *     Zeitüberschreitung der Anforderung.
 11    19 ms    16 ms    18 ms  wwwrl.zhaw.ch [160.85.104.96]
```

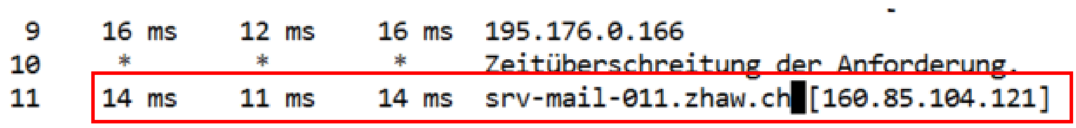
ZFH Access Net (SWITCH)

Firewalls

The single asterisk between 195.176.0.166 (Switch) and 160.85.104.96 (ZHAW) and is an indication for a border firewall. It is assumed to be part of ZHAW as it is in general unlikely that Internet Service Providers such as Switch perform filtering operations. It seems that the device itself does not generate ICMP error messages by filtering them (so traceroute does not get an answer and shows an asterisk), but the device does let through the following traceroute probes and also does not filter ICMP replies from the following hosts.

Scanning – Network Structure (3)

- traceroute to mx1.zhaw.ch

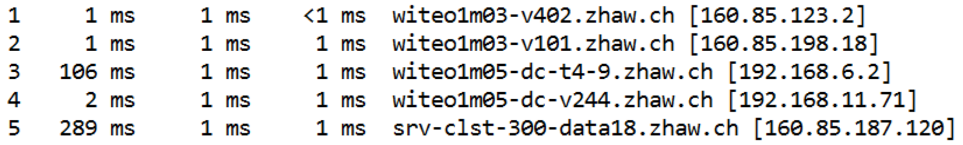


```
  9    16 ms    12 ms    16 ms  195.176.0.166
 10     *        *        *     Zeitüberschreitung der Anforderung.
 11    14 ms    11 ms    14 ms  srv-mail-011.zhaw.ch [160.85.104.121]
```

  - www and mx1 might sit behind the same router
  - It’s likely (though not guaranteed) that the hosts are in the same network
  - If they are in the same network, their IP addresses (104.96 and 104.121) tell us that the network is at least a /25 network
- Traceroute has its limits with firewalls that filter UDP or ICMP packets
  - An asterisk indicates that no answer was received from the host
  - So all we learn here is that “some filtering takes place” on the hop following 195.176.0.166

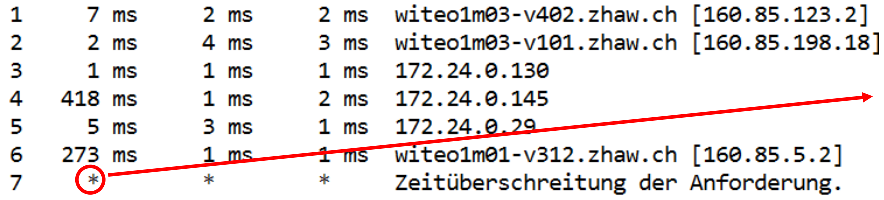
Scanning – Network Structure (4)

- If possible (compromise/guest), don't forget to scan from internal hosts



```
1     1 ms     1 ms    <1 ms  witeo1m03-v402.zhaw.ch [160.85.123.2]
2     1 ms     1 ms     1 ms  witeo1m03-v101.zhaw.ch [160.85.198.18]
3   106 ms     1 ms     1 ms  witeo1m05-dc-t4-9.zhaw.ch [192.168.6.2]
4     2 ms     1 ms     1 ms  witeo1m05-dc-v244.zhaw.ch [192.168.11.71]
5   289 ms     1 ms     1 ms  srv-clst-300-data18.zhaw.ch [160.85.187.120]
```

- Also, scan from internal to external:



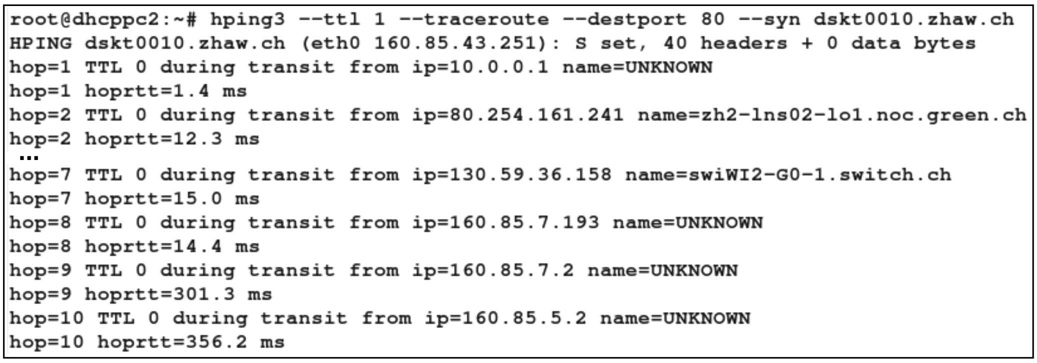
```
1     7 ms     2 ms     2 ms  witeo1m03-v402.zhaw.ch [160.85.123.2]
2     2 ms     4 ms     3 ms  witeo1m03-v101.zhaw.ch [160.85.198.18]
3     1 ms     1 ms     1 ms  172.24.0.130
4   418 ms     1 ms     2 ms  172.24.0.145
5     5 ms     3 ms     1 ms  172.24.0.29
6   273 ms     1 ms     1 ms  witeo1m01-v312.zhaw.ch [160.85.5.2]
7     *        *        *     Zeitüberschreitung der Anforderung.
```

Most likely, there's a firewall on the ZHAW border

- This gives more and more information about hosts, routers, firewalls,…

Scanning – Network Structure (5)

- An even more flexible tool than traceroute is hping3
  - Allows to specify protocol (ICMP/UDP/TCP) and destination port to be used
- Example: trace the route to dskt0010.zhaw.ch using TCP port 80 SYN probes:
  - TCP port 80 is more likely to get through firewalls than UDP or ICMP



```
root@dhcppc2:~# hping3 --ttl 1 --traceroute --destport 80 --syn dskt0010.zhaw.ch
HPING dskt0010.zhaw.ch (eth0 160.85.43.251): S set, 40 headers + 0 data bytes
hop=1 TTL 0 during transit from ip=10.0.0.1 name=UNKNOWN
hop=1 hoprtt=1.4 ms
hop=2 TTL 0 during transit from ip=80.254.161.241 name=zh2-lns02-lo1.noc.green.ch
hop=2 hoprtt=12.3 ms
 ...
hop=7 TTL 0 during transit from ip=130.59.36.158 name=swiWI2-G0-1.switch.ch
hop=7 hoprtt=15.0 ms
hop=8 TTL 0 during transit from ip=160.85.7.193 name=UNKNOWN
hop=8 hoprtt=14.4 ms
hop=9 TTL 0 during transit from ip=160.85.7.2 name=UNKNOWN
hop=9 hoprtt=301.3 ms
hop=10 TTL 0 during transit from ip=160.85.5.2 name=UNKNOWN
hop=10 hoprtt=356.2 ms
```

hping3

Hping3 is a very flexible tool that allows to generate all kinds of ICMP, UDP and TCP packets. Refer to the manpage for its options.

hping3 Options in the Example above

--ttl 1: Start with time-to-live = 1

--traceroute: Increment ttl for subsequent attempts

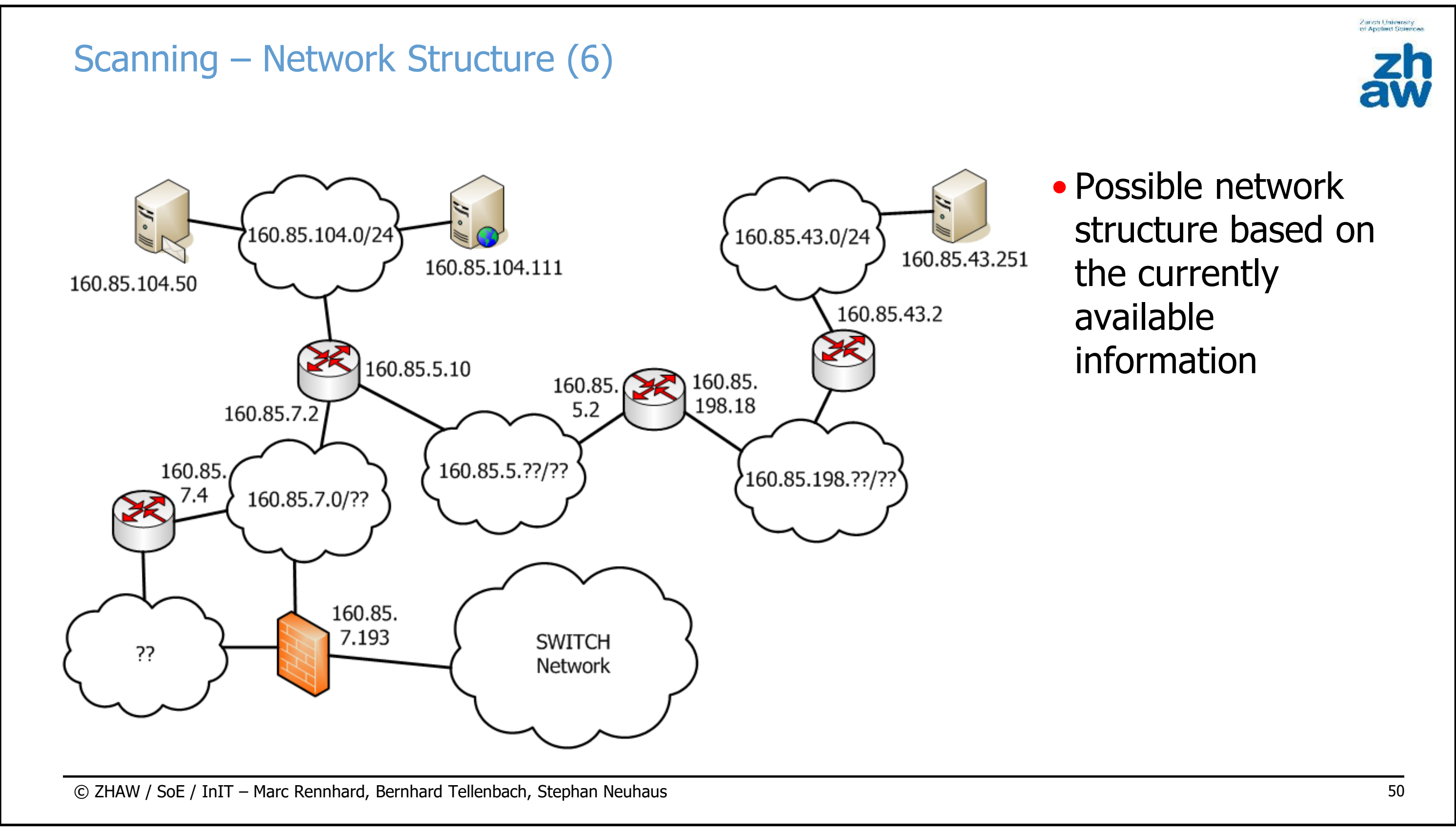
--destport 80: Use destination port 80

--syn: Set the SYN flag in the probes

--tr-stop (not used above): hping will exit once the first packet that isn't an ICMP time exceeded is received. This better emulates the traceroute behavior.

tcptraceroute

A similar tool to traceroute that uses TCP instead of UDP/ICMP probes.



Scanning – Network Structure (6)

- Possible network structure based on the currently available information

Network Structure

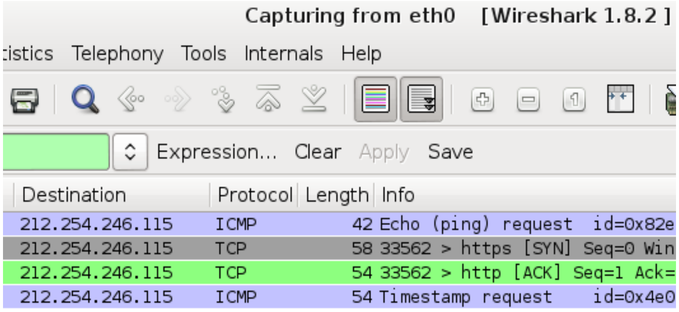
Of course, there are still many uncertainties with this structure and it’s definitely only a small part of a big network as employed by ZHAW, but it is a beginning and further analysis will allow to refine the structure more and more and eventually come to a result that is likely to be close to the real situation.

In addition, further findings – additional hosts found during host scanning or even compromising an internal host – will help to refine this structure by performing additional scans to these hosts and from the newly compromised host.

Scanning – nmap Host Discovery

- Ping scan: `nmap -sn www.csnc.ch`
  - ICMP echo request
  - TCP SYN 443 + TCP ACK 80
  - ICMP timestamp request
  - On a local network, ping scan switches to ARP requests!
- Usually, you do a port scan only on hosts answering the Ping scan
- Pentest: You might want to scan every host – some might not answer the ping-scan:

```
nmap -Pn <target>
```


Capturing from eth0 [Wireshark 1.8.2]
tistics Telephony Tools Internals Help
Expression... Clear Apply Save

```
Destination      Protocol Length Info
212.254.246.115  ICMP         42 Echo (ping) request  id=0x82e
212.254.246.115  TCP          58 33562 > https [SYN] Seq=0 Win
212.254.246.115  TCP          54 33562 > http [ACK] Seq=1 Ack=
212.254.246.115  ICMP         54 Timestamp request    id=0x4e0
```

-sn No port scan after ping scan. Host discovery only

-Pn Default port scan without firts doing a ping scan to decide whether to do a port scan of a host

Scanning – nmap Scan Techniques

Switch	Technique	Description
-sS	TCP Syn	Default option, fast, relatively stealthy, reliable, also referred to as half-open scanning
-sT	TCP Connect	Uses «connect» system call of the underlying OS rather than writing raw packets. Slower than TCP syn scan, more easily detectable
-sA	TCP Ack	Used for testing firewall rulesets
-sU	UDP	UDP scan, much slower than TCP
-sN	TCP Null	TCP scan with different flags set (FIN, PSH, URG) to avoid stateless firewalls
-sF	TCP FIN	
-sX	TCP XMAS	
-sO	IP Protocol	Used to detect IP protocols supported by the target

Scanning – nmap Port Discovery

- Port Ranges (by IANA)
  - Well-known ports: 1-1023
  - Registered ports: 1024-49151
  - Dynamic ports: 49152-65535
- Port Selection
  - All ports: -p- or -p1-65535
  - Specific port(s): -p22,53,110,143
  - Port ranges: -p20-25
  - Top 1000 ports: (default)
  - Top 100 ports: -F
  - Top 10 ports: --top-ports 10
- Combining UDP and TCP ports
  - --sU -sS -p U:53,T:21,80

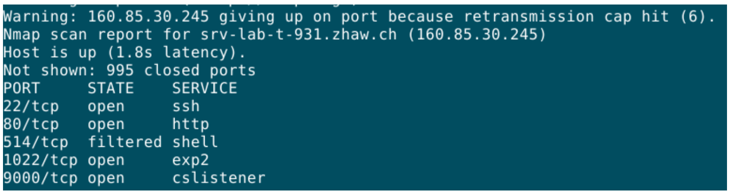
TCP	UDP
topports 10: 48%	topports 10: 50%
topports 50: 65%	topports 50: 86%
topports 100: 73%	-topports 100: 90%
topports 250: 83%	-topports 250: 94%
topports 500: 89%	topports 500: 97%
topports 1000: 93%	topports 1017: ~100%
topports 2000: 96%	
topports 3674: ~100%	

Effectiveness of different top port scans

Scanning – nmap Service/Version Detection

- Ports discovered during a scan are labelled with associated services:

  `nmap -sS -T4 -PN -n 160.85.30.245`

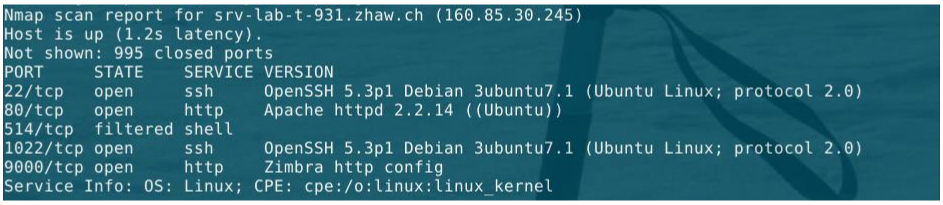


```
Warning: 160.85.30.245 giving up on port because retransmission cap hit (6).
Nmap scan report for srv-lab-t-931.zhaw.ch (160.85.30.245)
Host is up (1.8s latency).
Not shown: 995 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
80/tcp    open     http
514/tcp   filtered shell
1022/tcp open      exp2
9000/tcp open      cslistener
```

Tip: Use the **--reason switch** to learn why a port is marked as Open, Closed, Filtered…

- But ports can be arbitrarily assigned to applications. What now?

  `nmap -sV -PN -n 160.85.30.245`



```
Nmap scan report for srv-lab-t-931.zhaw.ch (160.85.30.245)
Host is up (1.2s latency).
Not shown: 995 closed ports
PORT      STATE    SERVICE VERSION
22/tcp    open     ssh     OpenSSH 5.3p1 Debian 3ubuntu7.1 (Ubuntu Linux; protocol 2.0)
80/tcp    open     http    Apache httpd 2.2.14 ((Ubuntu))
514/tcp   filtered shell
1022/tcp open      ssh     OpenSSH 5.3p1 Debian 3ubuntu7.1 (Ubuntu Linux; protocol 2.0)
9000/tcp open      http    Zimbra http config
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

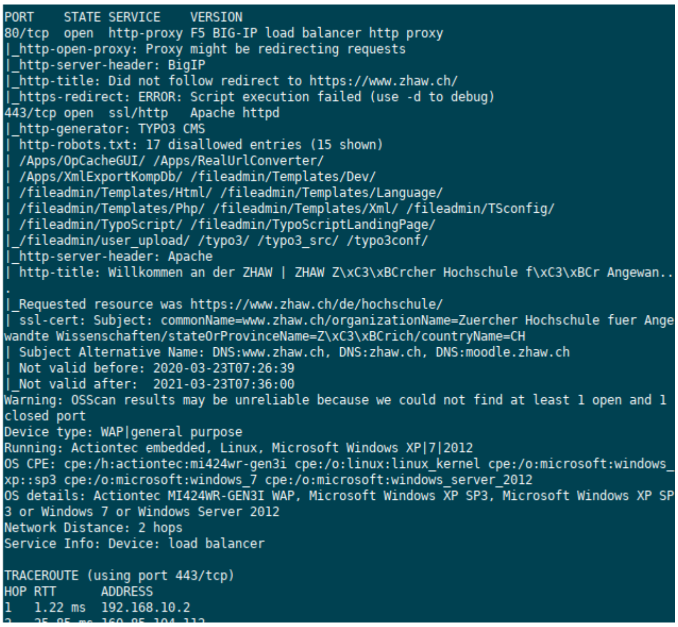
Scanning – nmap Service/Version Detection

- Detection of services/versions is based on interrogating the open ports using service probes and SYN Stealth Scan as scan method
  - Option: -sV (included in –A option)
- The nmap-service-probes database contains probes for querying various services and match expressions to recognize and parse responses
  - Mostly based on match expressions for the data returned when establishing a connection (or sending a UDP packet) => the "banner"
  - Additional probes (=request/packets) beyond getting the banner are the exception
  - On Kali linux found here: /usr/share/nmap/nmap-service-probes
  - Sample of a match rule:

```
match ftp m|^220[ -].*\r\n550 SSL/TLS required on the control channel\r\n|s
p/ProFTPD/ i/requires SSL/ cpe:/a:proftpd:proftpd/a
```

Scanning – Getting it All

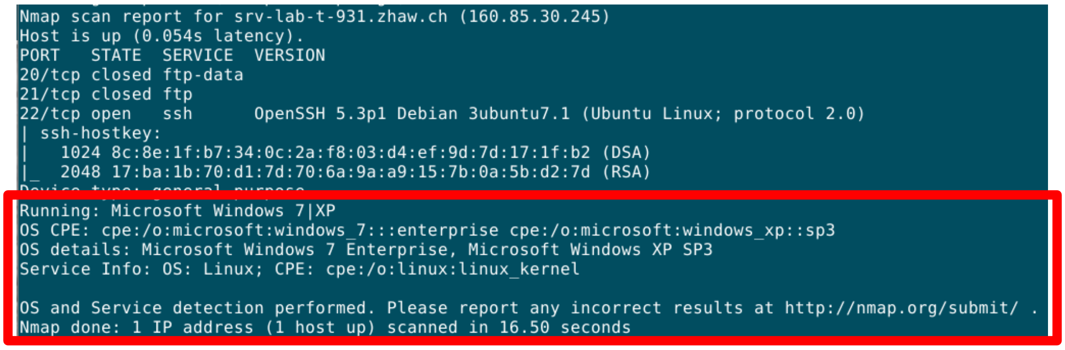
- For a maximum of information, we can use the –A option
- This performs OS detection, service version detection, script scanning, and traceroute
- It provides (if possible) the following information:
  - Service protocols (FTP, SSH,…)
  - Application names (ISC BIND, Apache,…)
  - Version numbers
  - Hostname, Device type, OS family
  - Common Platform Enumeration (CPE) representation



```
PORT    STATE SERVICE    VERSION
80/tcp  open  http-proxy F5 BIG-IP load balancer http proxy
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: BigIP
|_http-title: Did not follow redirect to https://www.zhaw.ch/
|_https-redirect: ERROR: Script execution failed (use -d to debug)
443/tcp open  ssl/http   Apache httpd
|_http-generator: TYPO3 CMS
| http-robots.txt: 17 disallowed entries (15 shown)
| /Apps/OpCacheGUI/ /Apps/RealUrlConverter/
| /Apps/XmlExportKompDb/ /fileadmin/Templates/Dev/
| /fileadmin/Templates/Html/ /fileadmin/Templates/Language/
| /fileadmin/Templates/Php/ /fileadmin/Templates/Xml/ /fileadmin/TSconfig/
| /fileadmin/TypoScript/ /fileadmin/TypoScriptLandingPage/
|_/fileadmin/user_upload/ /typo3/ /typo3_src/ /typo3conf/
|_http-server-header: Apache
| http-title: Willkommen an der ZHAW | ZHAW Z\xC3\xBCrcher Hochschule f\xC3\xBCr Angewan..
.
|_Requested resource was https://www.zhaw.ch/de/hochschule/
| ssl-cert: Subject: commonName=www.zhaw.ch/organizationName=Zuercher Hochschule fuer Ange
wandte Wissenschaften/stateOrProvinceName=Z\xC3\xBCrich/countryName=CH
| Subject Alternative Name: DNS:www.zhaw.ch, DNS:zhaw.ch, DNS:moodle.zhaw.ch
| Not valid before: 2020-03-23T07:26:39
|_Not valid after:  2021-03-23T07:36:00
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1
closed port
Device type: WAP|general purpose
Running: Actiontec embedded, Linux, Microsoft Windows XP|7|2012
OS CPE: cpe:/h:actiontec:mi424wr-gen3i cpe:/o:linux:linux_kernel cpe:/o:microsoft:windows_
xp::sp3 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2012
OS details: Actiontec MI424WR-GEN3I WAP, Microsoft Windows XP SP3, Microsoft Windows XP SP
3 or Windows 7 or Windows Server 2012
Network Distance: 2 hops
Service Info: Device: load balancer

TRACEROUTE (using port 443/tcp)
HOP RTT      ADDRESS
1   1.22 ms  192.168.10.2
2   25.85 ms 160.85.104.112
```

Scanning – nmap OS Detection

- The inner workings of OS detection are quite complex
  - Sending up to 16 TCP, UDP, and ICMP probes to known open and closed ports specially designed to exploit various ambiguities in the standard protocol RFC
  - Dozens of attributes in the responses are analysed and combined to generate a fingerprint (see https://nmap.org/book/osdetect-methods.html for details)
- Option: -O –v (-v is for verbose output)

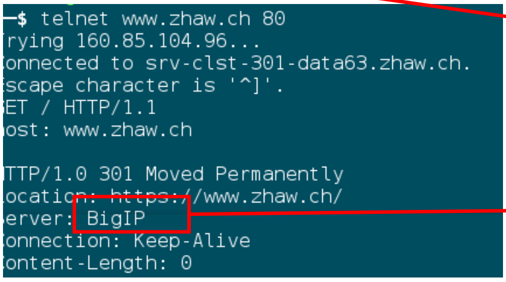


```
Nmap scan report for srv-lab-t-931.zhaw.ch (160.85.30.245)
Host is up (0.054s latency).
PORT   STATE  SERVICE  VERSION
20/tcp closed ftp-data
21/tcp closed ftp
22/tcp open   ssh      OpenSSH 5.3p1 Debian 3ubuntu7.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 8c:8e:1f:b7:34:0c:2a:f8:03:d4:ef:9d:7d:17:1f:b2 (DSA)
|_  2048 17:ba:1b:70:d1:7d:70:6a:9a:a9:15:7b:0a:5b:d2:7d (RSA)
Device type: general purpose
Running: Microsoft Windows 7|XP
OS CPE: cpe:/o:microsoft:windows_7:::enterprise cpe:/o:microsoft:windows_xp::sp3
OS details: Microsoft Windows 7 Enterprise, Microsoft Windows XP SP3
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.50 seconds
```

Scanning – Manual Banner Grabbing

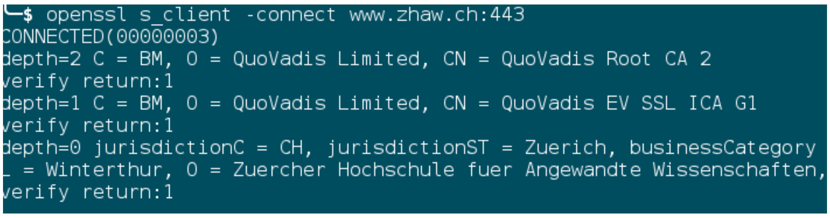
```
$ nc dskt0010.zhaw.ch 22
SSH-2.0-OpenSSH_5.9p1 Debian-5ubuntu1.10
```

Probably correct



```
—$ telnet www.zhaw.ch 80
rying 160.85.104.96...
onnected to srv-clst-301-data63.zhaw.ch.
scape character is '^]'.
ET / HTTP/1.1
ost: www.zhaw.ch

TTP/1.0 301 Moved Permanently
ocation: https://www.zhaw.ch/
erver: BigIP
onnection: Keep-Alive
ontent-Length: 0
```

Web server? => Web Application Firewall (WAF)!



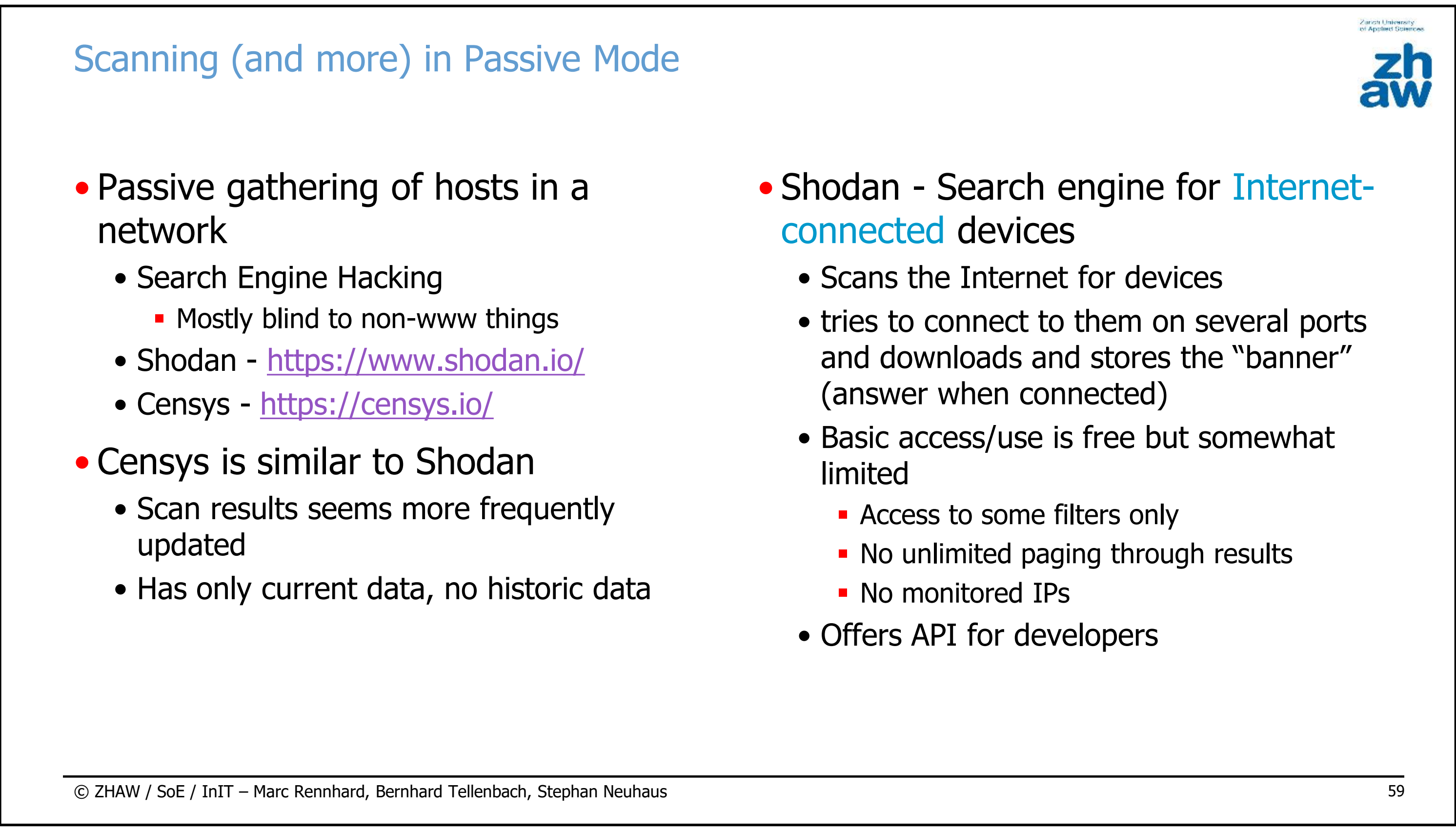
```
└─$ openssl s_client -connect www.zhaw.ch:443
CONNECTED(00000003)
depth=2 C = BM, O = QuoVadis Limited, CN = QuoVadis Root CA 2
verify return:1
depth=1 C = BM, O = QuoVadis Limited, CN = QuoVadis EV SSL ICA G1
verify return:1
depth=0 jurisdictionC = CH, jurisdictionST = Zuerich, businessCategory
L = Winterthur, O = Zuercher Hochschule fuer Angewandte Wissenschaften,
verify return:1
```

- Manual methods are also well suited to determine software versions
- For example, by using telnet, netcat or openssl (for SSL/TLS communications)

Banner

In general, one cannot assume that the banner/header information returned by a host is correct because many applications (e.g. Apache) allow to easily modify it and by modifying the source code and recompiling the application it is always possible to adapt information that identifies the software to any random string. Therefore such information can be the correct server software information but it cannot be taken for granted.

In general, modifying server information such that it does not give away all information with respect to detailed software version, module installed etc. is considered good security policy and should be enforced by system administrators.



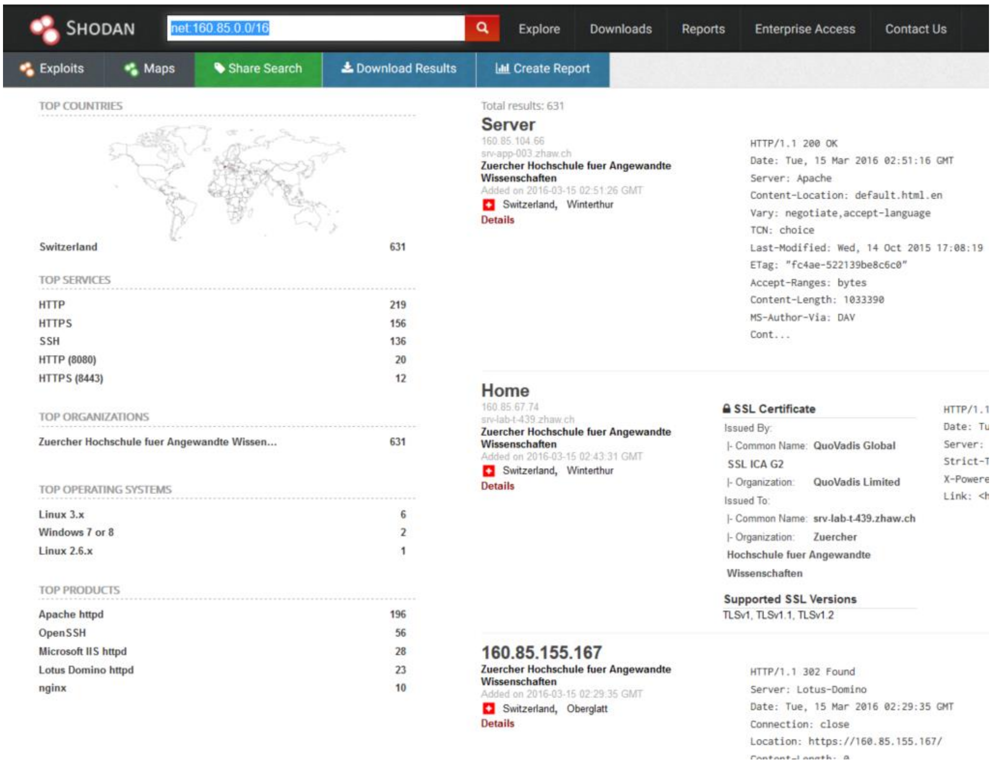
Scanning (and more) in Passive Mode

- Passive gathering of hosts in a network
  - Search Engine Hacking
    - Mostly blind to non-www things
  - Shodan - https://www.shodan.io/
  - Censys - https://censys.io/
- Censys is similar to Shodan
  - Scan results seems more frequently updated
  - Has only current data, no historic data
- Shodan - Search engine for Internet-connected devices
  - Scans the Internet for devices
  - tries to connect to them on several ports and downloads and stores the “banner” (answer when connected)
  - Basic access/use is free but somewhat limited
    - Access to some filters only
    - No unlimited paging through results
    - No monitored IPs
  - Offers API for developers

Shodan is a search engine that lets the user find specific types of computers (routers, servers, etc.) connected to the internet using a variety of filters. Some have also described it as a search engine of service banners, which are meta-data the server sends back to the client. This can be information about the server software, what options the service supports, a welcome message or anything else that the client can find out before interacting with the server.

Shodan collects data mostly on web servers (HTTP, port 80), as well as FTP (port 21), SSH (port 22) Telnet (port 23), SNMP (port 161), SIP (port 5060), and Real Time Streaming Protocol (RTSP, port 554). The latter can be used to access webcams and their video stream.

It was launched in 2009 by computer programmer John Matherly, who, in 2003, conceived the idea of searching devices linked to the Internet. The name Shodan is a reference to SHODAN, a character from the *System Shock* video game series.



TOP COUNTRIES	
Switzerland	631

TOP SERVICES	
HTTP	219
HTTPS	156
SSH	136
HTTP (8080)	20
HTTPS (8443)	12

TOP ORGANIZATIONS	
Zuercher Hochschule fuer Angewandte Wissen...	631

TOP OPERATING SYSTEMS	
Linux 3.x	6
Windows 7 or 8	2
Linux 2.6.x	1

TOP PRODUCTS	
Apache httpd	196
OpenSSH	56
Microsoft IIS httpd	28
Lotus Domino httpd	23
nginx	10

Total results: 631

Server
160.85.104.66
srv-app-003.zhaw.ch
Zuercher Hochschule fuer Angewandte Wissenschaften
Added on 2016-03-15 02:51:26 GMT
🇨🇭 Switzerland, Winterthur
Details

```
HTTP/1.1 200 OK
Date: Tue, 15 Mar 2016 02:51:16 GMT
Server: Apache
Content-Location: default.html.en
Vary: negotiate,accept-language
TCN: choice
Last-Modified: Wed, 14 Oct 2015 17:08:19
ETag: "fc4ae-522139be8c6c0"
Accept-Ranges: bytes
Content-Length: 1033390
MS-Author-Via: DAV
Cont...
```

Home
160.85.67.74
srv-lab-t-439.zhaw.ch
Zuercher Hochschule fuer Angewandte Wissenschaften
Added on 2016-03-15 02:43:31 GMT
🇨🇭 Switzerland, Winterthur
Details

SSL Certificate
Issued By:
|- Common Name: **QuoVadis Global SSL ICA G2**
|- Organization: **QuoVadis Limited**
Issued To:
|- Common Name: **srv-lab-t-439.zhaw.ch**
|- Organization: **Zuercher Hochschule fuer Angewandte Wissenschaften**

Supported SSL Versions
TLSv1, TLSv1.1, TLSv1.2

```
HTTP/1.1
Date: Tu
Server:
Strict-T
X-Powere
Link: <h
```

160.85.155.167
Zuercher Hochschule fuer Angewandte Wissenschaften
Added on 2016-03-15 02:29:35 GMT
🇨🇭 Switzerland, Oberglatt
Details

```
HTTP/1.1 302 Found
Server: Lotus-Domino
Date: Tue, 15 Mar 2016 02:29:35 GMT
Connection: close
Location: https://160.85.155.167/
Content-Length: 0
```

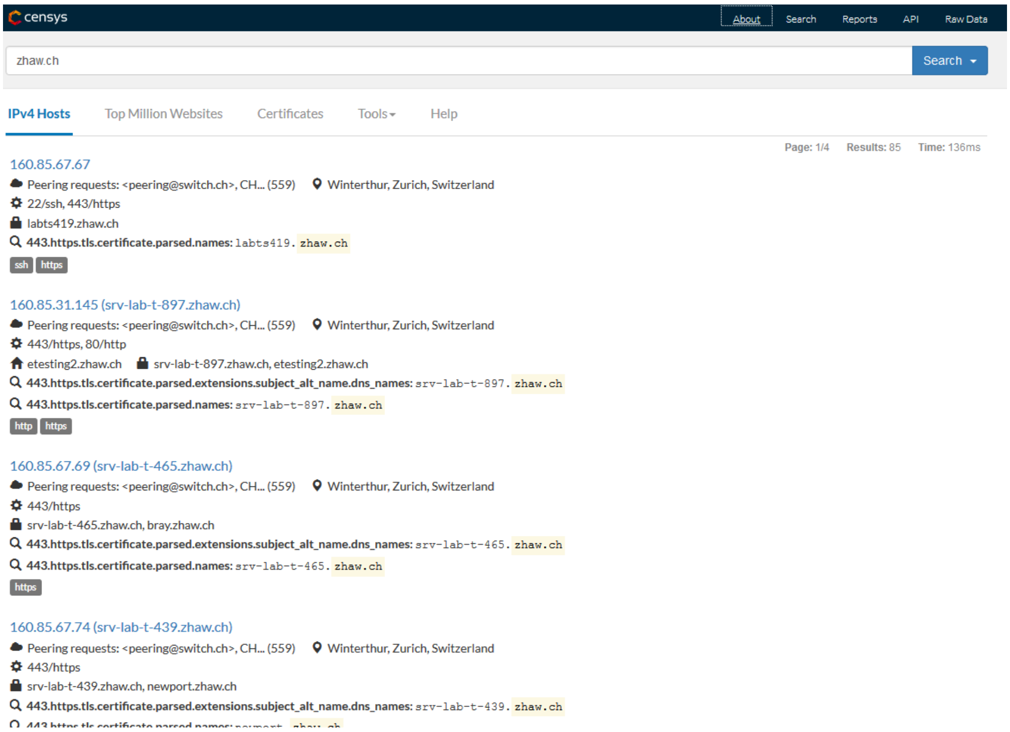
Shodan is a search engine that lets the user find specific types of computers (routers, servers, etc.) connected to the internet using a variety of filters. Some have also described it as a search engine of service banners, which are meta-data the server sends back to the client. This can be information about the server software, what options the service supports, a welcome message or anything else that the client can find out before interacting with the server.

Shodan collects data mostly on web servers (HTTP, port 80), as well as FTP (port 21), SSH (port 22) Telnet (port 23), SNMP (port 161), SIP (port 5060), and Real Time Streaming Protocol (RTSP, port 554). The latter can be used to access webcams and their video stream.

It was launched in 2009 by computer programmer John Matherly, who, in 2003, conceived the idea of searching devices linked to the Internet. The name Shodan is a reference to SHODAN, a character from the *System Shock* video game series.

Everything that has ZHAW in the banner and located in Switzerland:

- zhaw country:"CH"



Page: 1/4 Results: 85 Time: 136ms

160.85.67.67
Peering requests: <peering@switch.ch>, CH... (559) Winterthur, Zurich, Switzerland
22/ssh, 443/https
labts419.zhaw.ch
443.https.tls.certificate.parsed.names: `labts419. zhaw.ch`

160.85.31.145 (srv-lab-t-897.zhaw.ch)
Peering requests: <peering@switch.ch>, CH... (559) Winterthur, Zurich, Switzerland
443/https, 80/http
etesting2.zhaw.ch srv-lab-t-897.zhaw.ch, etesting2.zhaw.ch
443.https.tls.certificate.parsed.extensions.subject_alt_name.dns_names: `srv-lab-t-897. zhaw.ch`
443.https.tls.certificate.parsed.names: `srv-lab-t-897. zhaw.ch`

160.85.67.69 (srv-lab-t-465.zhaw.ch)
Peering requests: <peering@switch.ch>, CH... (559) Winterthur, Zurich, Switzerland
443/https
srv-lab-t-465.zhaw.ch, bray.zhaw.ch
443.https.tls.certificate.parsed.extensions.subject_alt_name.dns_names: `srv-lab-t-465. zhaw.ch`
443.https.tls.certificate.parsed.names: `srv-lab-t-465. zhaw.ch`

160.85.67.74 (srv-lab-t-439.zhaw.ch)
Peering requests: <peering@switch.ch>, CH... (559) Winterthur, Zurich, Switzerland
443/https
srv-lab-t-439.zhaw.ch, newport.zhaw.ch
443.https.tls.certificate.parsed.extensions.subject_alt_name.dns_names: `srv-lab-t-439. zhaw.ch`
443.https.tls.certificate.parsed.names: `newport. zhaw.ch`

Scanning – Summary

- Scanning serves to analyse the network structure and individual hosts in detail
- After scanning, you know the following information
  - Parts or all of the network structure
  - Hosts that are reachable from your location
- Of a subset of all hosts (or of all hosts if the analysed environment is small) you know more detailed information
  - Operating system
  - Available services (that are visible from your location)
  - Software versions of the services
  - Potential vulnerabilities that may be exploited
    - We’ll look at this when discussing the vulnerability analysis phase

Scanning - Summary

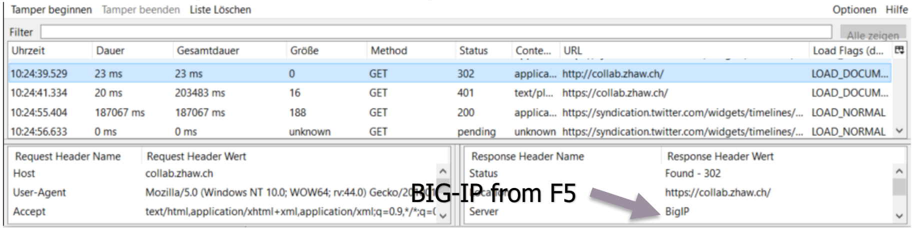
Method	Passive Semi-Active Active
Level	L1/L2/(L3)
Information	Network structure Services, software and operating systems used
Tools	• traceroute, nmap • Shodan / Censys • Search engine hacking
Resources	• The infrastructure itself • Shodan/Censys data
Limitations	• Passive discovery is challenging and is almost certainly incomplete • You can ask Shodan/Censys to not to scan your IPs • Short-lived hosts/services might not be captured • Delay until you see a new service/host in the results

Footprinting Defences

- Motivation: Additional attack vectors, know how to evade detection (stealth)
- Identify defensive systems: Firewalls, WAF, IDS, Anti-Virus, …
  - Brute-forcing protections, (D)DoS misuse, authentication type/protocol,…
  - Single- or multi-factor → attack vector must include getting 2nd factor
  - Federated systems → attack via other members of federation realm
- Active:
  - Inspect banners, HTTP responses, device fingerprinting,…
  - Social engineering (trick employees into providing information)
- Passive:
  - Search engine hacking (partners, presentations, projects,…)
  - Inspect banners, device fingerprints etc. (e.g., using Censys, Shodan etc.)

Footprinting Defences - Is there WAF in front of collab.zhaw.ch?

- Manual: Inspect HTTP responses



Uhrzeit	Dauer	Gesamtdauer	Größe	Method	Status	Conte...	URL	Load Flags (d...
10:24:39.529	23 ms	23 ms	0	GET	302	applica...	http://collab.zhaw.ch/	LOAD_DOCUM...
10:24:41.334	20 ms	203483 ms	16	GET	401	text/pl...	https://collab.zhaw.ch/	LOAD_DOCUM...
10:24:55.404	187067 ms	187067 ms	188	GET	200	applica...	https://syndication.twitter.com/widgets/timelines/...	LOAD_NORMAL
10:24:56.633	0 ms	0 ms	unknown	GET	pending	unknown	https://syndication.twitter.com/widgets/timelines/...	LOAD_NORMAL

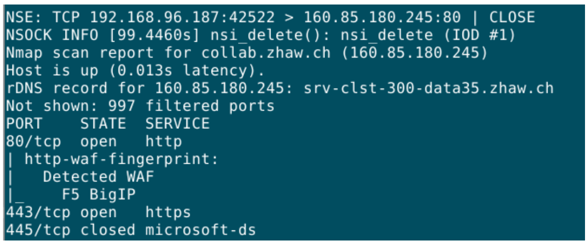
Request Header Name	Request Header Wert
Host	collab.zhaw.ch
User-Agent	Mozilla/5.0 (Windows NT 10.0; WOW64; rv:44.0) Gecko/201
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=(

Response Header Name	Response Header Wert
Status	Found - 302
Location	https://collab.zhaw.ch/
Server	BigIP

BIG-IP from F5

- Automated: Use nmap and its WAF detection capability

```
nmap --script=http-waf-fingerprint --script-trace collab.zhaw.ch
```



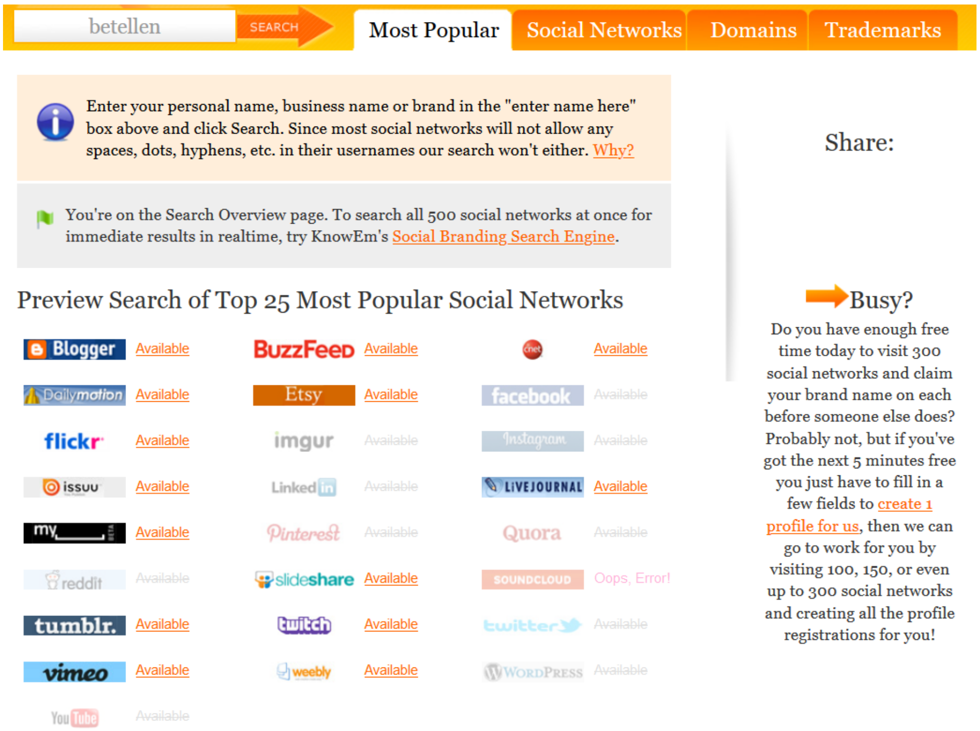
```
NSE: TCP 192.168.96.187:42522 > 160.85.180.245:80 | CLOSE
NSOCK INFO [99.4460s] nsi_delete(): nsi_delete (IOD #1)
Nmap scan report for collab.zhaw.ch (160.85.180.245)
Host is up (0.013s latency).
rDNS record for 160.85.180.245: srv-clst-300-data35.zhaw.ch
Not shown: 997 filtered ports
PORT    STATE  SERVICE
80/tcp  open   http
| http-waf-fingerprint:
|   Detected WAF
|_    F5 BigIP
443/tcp open   https
445/tcp closed microsoft-ds
```

Footprinting Defences - Summary

Method	Passive Semi-Active Active
Level	L1/L2/L3
Information	Products (brand, version,…), manuals
Tools	• Search engine hacking • Web browser (for online analysis) • Scanners (e.g., nmap)
Resources	• The infrastructure itself • 3rd party sources
Limitations	• If middle-boxes are configured to be “stealthy”, they might not be found

HUMINT - Social Relationships and more

- Human intelligence collection involves direct interaction
  - Physical (e.g. observation)
  - Verbal (e.g., phone call, chat, on-site meeting,…)
- Before HUMINT, you find out as much as you can about a person
  - Online accounts used by the person, especially social media accounts
  - Information posted on social media accounts
- Automate online account search: Use websites that tell you whether a username is still available for a given service like Facebook, Gmail etc.
  - Service does have to leak information whether a user exists or not
  - Many services still do (either at login-time or using the password reset function)
  - Websites that can do this (partially):
    http://knowem.com/
    http://checkusernames.com/



Enter your personal name, business name or brand in the "enter name here" box above and click Search. Since most social networks will not allow any spaces, dots, hyphens, etc. in their usernames our search won't either. Why?

You're on the Search Overview page. To search all 500 social networks at once for immediate results in realtime, try KnowEm's Social Branding Search Engine.

Preview Search of Top 25 Most Popular Social Networks

Blogger	Available	BuzzFeed	Available	cnet	Available
Dailymotion	Available	Etsy	Available	facebook	~~Available~~
flickr	Available	imgur	~~Available~~	Instagram	~~Available~~
issuu	Available	Linked in	~~Available~~	LiVEJOURNAL	Available
my_	Available	Pinterest	~~Available~~	Quora	~~Available~~
reddit	~~Available~~	slideshare	Available	SOUNDCLOUD	Oops, Error!
tumblr.	Available	twitch	Available	twitter	~~Available~~
vimeo	Available	weebly	Available	WordPress	~~Available~~
YouTube	~~Available~~				

Share:

Busy?

Do you have enough free time today to visit 300 social networks and claim your brand name on each before someone else does? Probably not, but if you've got the next 5 minutes free you just have to fill in a few fields to create 1 profile for us, then we can go to work for you by visiting 100, 150, or even up to 300 social networks and creating all the profile registrations for you!

Intelligence Gathering - Summary

- Intelligence Gathering is the first step performed by a penetration tester (or attacker)
- When done, you know general, IT-related information (but not only) about the target company
  - Domain names, IP ranges
  - Technical contact persons
  - Hostnames and IP addresses of some systems
  - …
- If you are lucky, you have discovered additional valuable information
  - E.g. critical information (internal system configurations etc.) that has been voluntarily disclosed by the employees

Link-Collection with links for doing OSINT (resources/tools):
https://www.andyblackassociates.co.uk/resources-andy-black-associates/osint-toolkit/

Appendix

Scanning – nmap Script Scan

- Nmap has a scripting engine (NSE)
  - Users can write their own scripts (LUA)
  - 500+ scripts (in LUA) to identify vulnerabilities and do other things
- Script categories

auth	(bypassing) authentication credentials
brute	brute force attacks for different protocols
default	run when –sC is specified
dos	test for denial of service / may crash vulnerable services
exploit	actively exploit vulnerabilities
fuzzer	send randomized/unexpected data
intrusive	not safe, may crash the target system
safe	should not crash services or use large amount of resources
…	

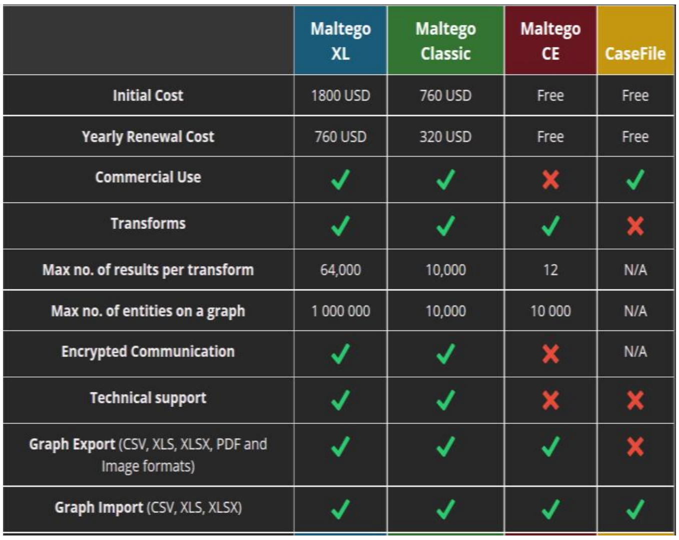
- Running a scan with the default set of scripts
  - nmap –sS –sC –Pn –p- <host>
  - nmap –sS --script=default –Pn –p- <host>
- Running a scan with a specific set of scripts
  - nmap –-script default,safe …
  - nmap --script «http-*» …
  - nmap --script «not intrusive» …
  - nmap --script «default or|and save» …
- Scripts may also accept arguments
  - nmap –sC –script-args ‘arg1=foo,arg2=bar’…
- Banner grabbing script:
  - nmap –sV –script=banner <target>

Maltego - One Tool to Rule them All (1)

- Maltego is proprietary software used for OSINT and forensics
- Provides library of transforms for discovery of data from open sources, and visualizing that information in a graph format, suitable for link analysis and data mining
- Transforms are scripts of code that execute specific tasks
  - Tasks or ‘transforms’ can be written in every computer language thereby increasing the appeal of this penetration testing tool
  - Scripts have an input entity (e.g., person name) and output entities (e.g. all email addresses found for it) using a specific strategy (e.g., googling)
- Maltego permits creating custom entities, allowing it to represent any type of information in addition to the basic entity types
  - Examples of entity types: people, groups, websites, domains, networks, devices, internet infrastructure, affiliations with online services (e.g., Twitter, Facebook)

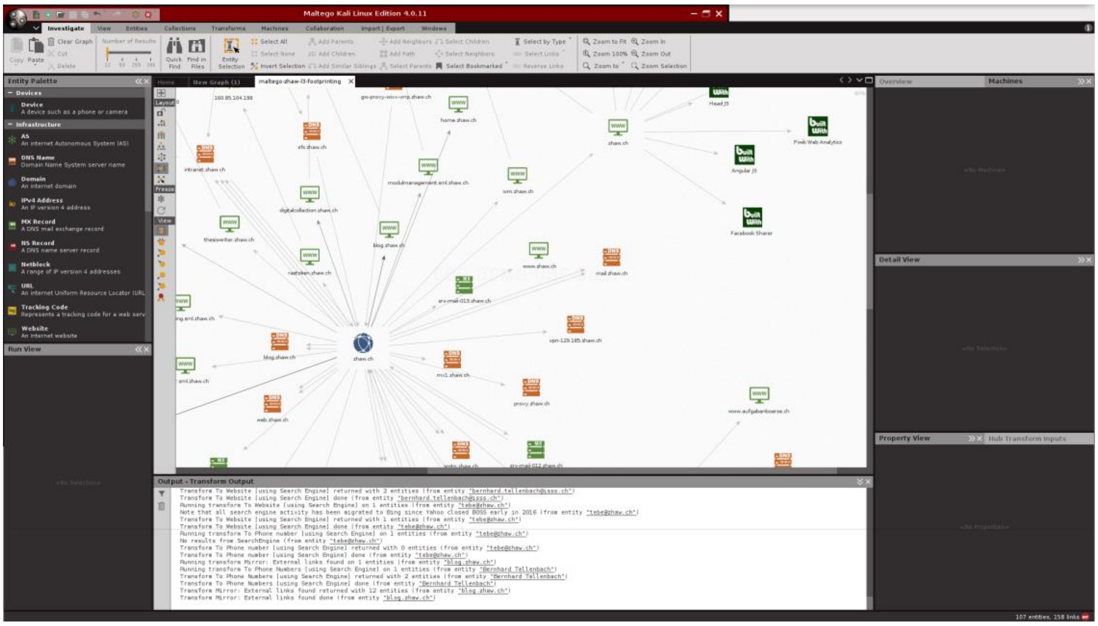
Maltego - One Tool to Rule them All (2)

- Automates many OSINT tasks:
  - Collecting email addresses linked to a person or company
  - Finding domain names and IP addresses of a company
  - Finding documents and devices
  - …
- Problem:
  - The tool is not free
  - Transforms are executed on servers not under your control => You can have your own servers => expensive



	Maltego XL	Maltego Classic	Maltego CE	CaseFile
Initial Cost	1800 USD	760 USD	Free	Free
Yearly Renewal Cost	760 USD	320 USD	Free	Free
Commercial Use	✓	✓	✗	✓
Transforms	✓	✓	✓	✗
Max no. of results per transform	64,000	10,000	12	N/A
Max no. of entities on a graph	1 000 000	10,000	10 000	N/A
Encrypted Communication	✓	✓	✗	N/A
Technical support	✓	✓	✗	✗
Graph Export (CSV, XLS, XLSX, PDF and Image formats)	✓	✓	✓	✗
Graph Import (CSV, XLS, XLSX)	✓	✓	✓	✓

Maltego - One Tool to Rule them All (2)



```
Transform To Website [using Search Engine] returned with 2 entities (from entity "bernhard.tellenbach@isss.ch")
Transform To Website [using Search Engine] done (from entity "bernhard.tellenbach@isss.ch")
Running transform To Website [using Search Engine] on 1 entities (from entity "tebe@zhaw.ch")
Note that all search engine activity has been migrated to Bing since Yahoo closed BOSS early in 2016 (from entity "tebe@zhaw.ch")
Transform To Website [using Search Engine] returned with 1 entities (from entity "tebe@zhaw.ch")
Transform To Website [using Search Engine] done (from entity "tebe@zhaw.ch")
Running transform To Phone number [using Search Engine] on 1 entities (from entity "tebe@zhaw.ch")
No results from SearchEngine (from entity "tebe@zhaw.ch")
Transform To Phone number [using Search Engine] returned with 0 entities (from entity "tebe@zhaw.ch")
Transform To Phone number [using Search Engine] done (from entity "tebe@zhaw.ch")
Running transform Mirror: External links found on 1 entities (from entity "blog.zhaw.ch")
Running transform To Phone Numbers [using Search Engine] on 1 entities (from entity "Bernhard Tellenbach")
Transform To Phone Numbers [using Search Engine] returned with 2 entities (from entity "Bernhard Tellenbach")
Transform To Phone Numbers [using Search Engine] done (from entity "Bernhard Tellenbach")
Transform Mirror: External links found returned with 12 entities (from entity "blog.zhaw.ch")
Transform Mirror: External links found done (from entity "blog.zhaw.ch")
```