Penetration Testing Professional

Information Gathering

Section 2: Network Security – Module 1

v5.0

1.1 Information Gathering Introduction

1.2 Search Engines

1.3 Social Media

1.4 Infrastructures

1.5 Tools

Information Gathering Introduction

Penetration-Testing (also known as Ethical Hacking) must follow a methodical, organized, and controlled process in order to both effectively review targets and keep the penetration tester safe from consequences if issues arise.

While there are many steps associated with an engagement, none are more important than the act of information gathering or footprinting a designated target.

The detail with which one gathers information for the engagement will determine the effectiveness of the outcome for the entire penetration test.

Pentesters performing *information gathering* must not only be meticulous, but also must know and use different techniques in order to obtain information. Being this detail driven will allow the tester to record only the needed data on the intended target.

One must define an accurate scope of engagement in order to ensure that the right information is pursued and obtained in full. In essence, it is like starting with a single seed of grass, and ending up with a sod farm containing grass as far as the eye can see.

Nurturing and building on that single grass seed, resulted in a multiplied return.

The Information gathering phase is focused on two essential aspects of all targets: Business and Infrastructure.

There are numerous sub-components to both of these categories to be considered when gathering information about your target organization.

The Business side of information gathering deals with collecting information regarding the type of business, its stakeholders, assets, products, services, employees and generally non-technical information.

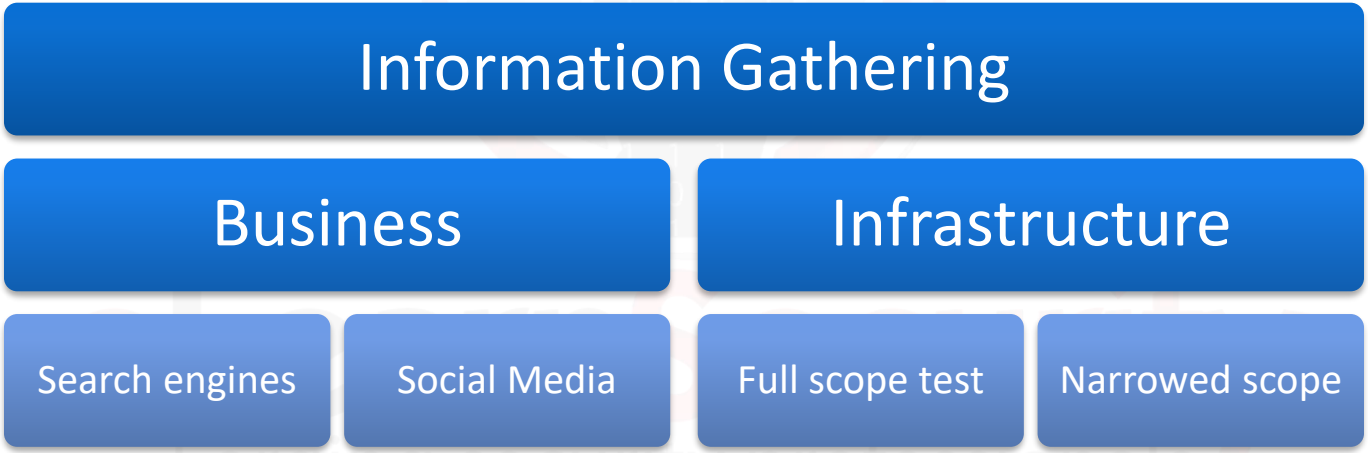
The organization will probably operate its business purpose through an Infrastructure such as networks, systems, domains, IP addresses and so on.

The second phase of the Information Gathering process will focus on uncovering this type of information.

At the end of the Information Gathering process you should at least have the following important information about the target:

Infrastructure	Business
Network Maps	Web presence (domains)
Network Blocks	Physical locations
IP addresses	Employees / Departments
Ports	Emails
Services	Partners and third parties
DNS	Press / news releases
Operating systems	Documents
Alive machines	Financial information
Systems	Job postings

The following chart shows how we will proceed with our process. These are tasks that we will unpack in the coming slides.



Before starting the process, it is important to note that information gathering techniques can be classified into two main disciplines:

Passive

Active

1.1. Information Gathering Introduction

MAP REF

Passive or OSINT (Open Source INTelligence) information gathering is gathering as much information about our target (network, system...) without exposing our presence.

In this phase we not only try to gather information such as web presence, partners, financial info, and physical plants but also, infrastructure related information using publicly available resources (accessible by anyone).

With the spread of Social Networking, this is getting easier.

Active information gathering techniques interact directly with the target system. In this phase, we will gather information about ports, services, running systems, net blocks and so on.

In general, active techniques can reveal the investigation to the organization through IDS or servers logs so caution should be taken to prevent this.

In the coming phases, you will amass a large amount of information therefore, consider how you will collect and record it.

In the first section, we will use a mind mapping technology in order to keep the information well organized. You can find these tools (such as FreeMind, Xmind, etc.) online. We suggest you use the one you are more comfortable with.

http://freemind.sourceforge.net/wiki/index.php/Main_Page
https://www.xmind.net/

When we start gathering and storing networking information, tools such as Dradis, Faraday and Magitree can be very useful due to the fact that they are specifically designed to keep track of networks/vulnerability scans.

As you will see, these tools can facilitate the sharing of gathered information with your colleagues and, in addition, allow you to import scans and reports created with tools like *Burp Suite*, *Nessus*, *Nexpose*, *Nmap* and so on.

https://dradisframework.com/ce/
https://github.com/infobyte/faraday

https://www.gremwell.com/what_is_magictree

Also, please make sure to read the Methodology : Handling information guide that will teach you how to collect and store information about your target.

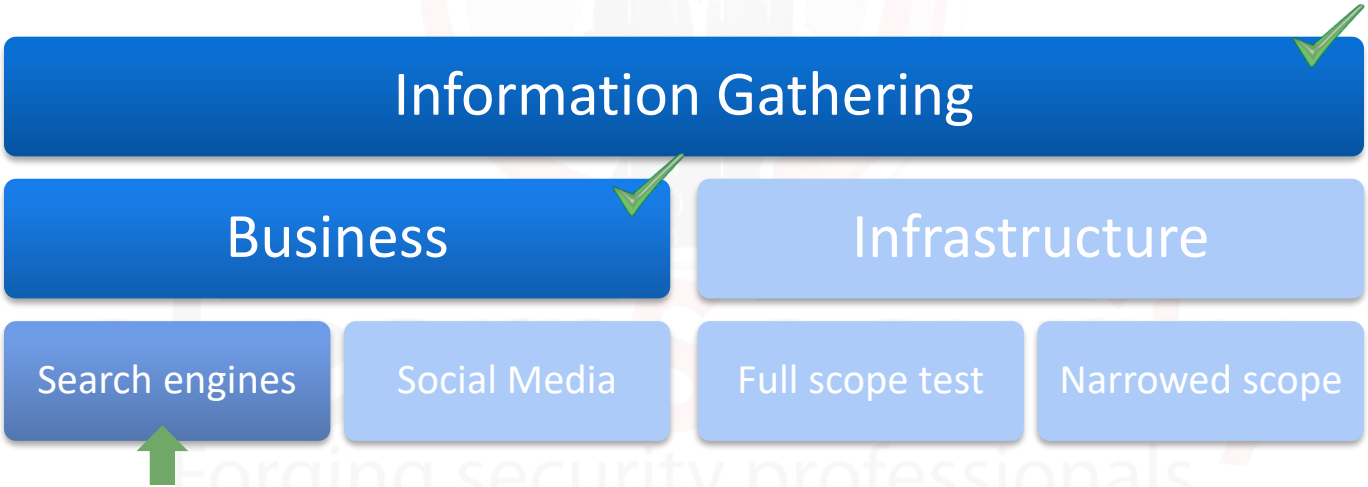
You can find it in the Members area under the Resources tab.

https://members.elearnsecurity.com/course/resources/name/ptp_v5_section_2_module_1_attachment_eLearnSecurity_Handling_Information

Search Engine

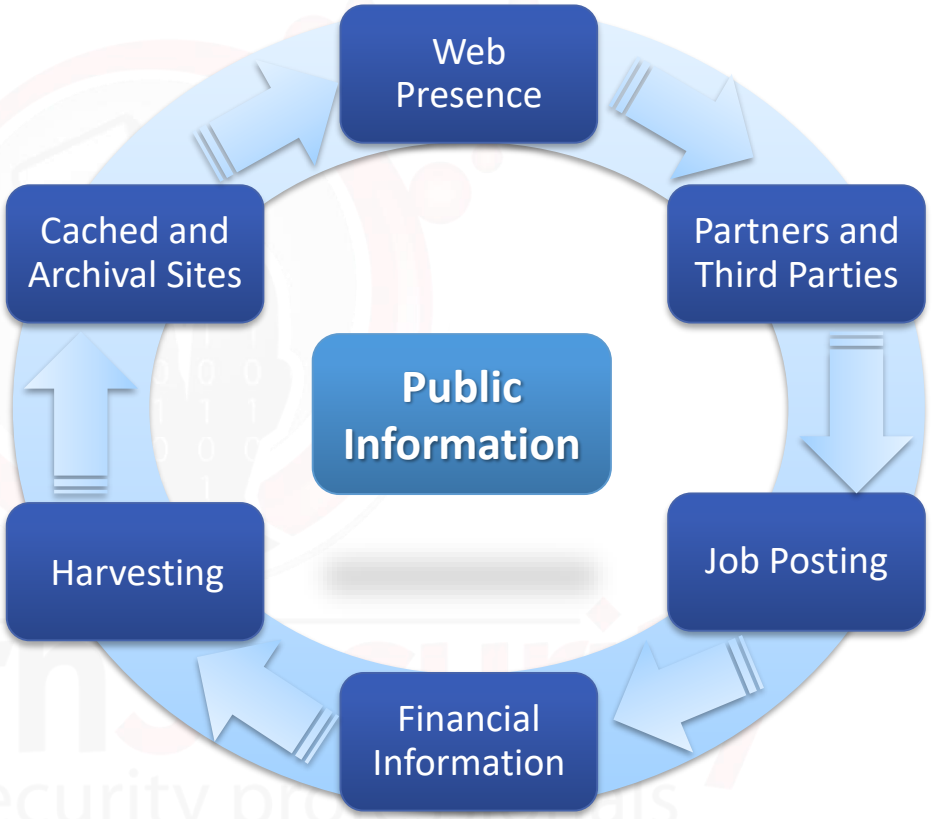
We are now going to see the tasks that a Pentester will undergo in order to perform Business Information Gathering.

Let's start with Search Engines.

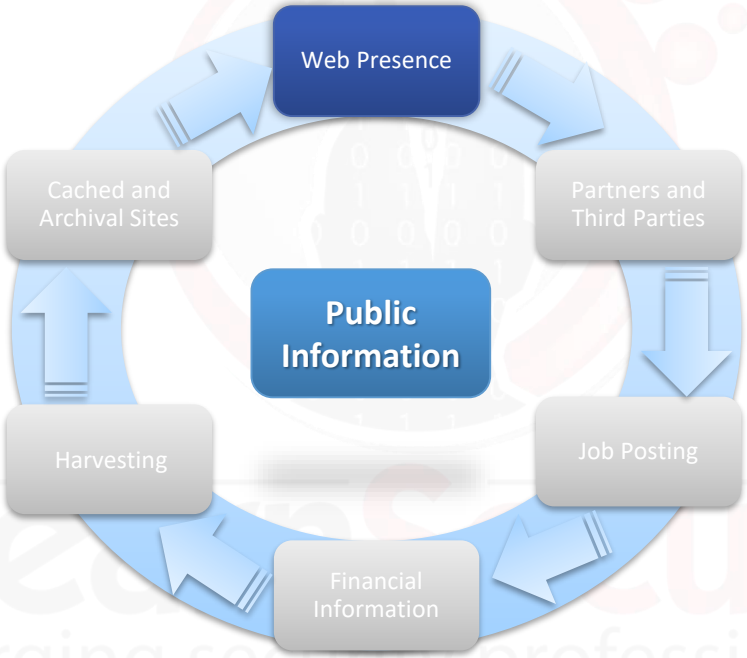


1.2.1. Search Engine

During the Business related information gathering phase, there is a great deal of diverse research conducted and are as follows:



Let us begin with Web Presence.

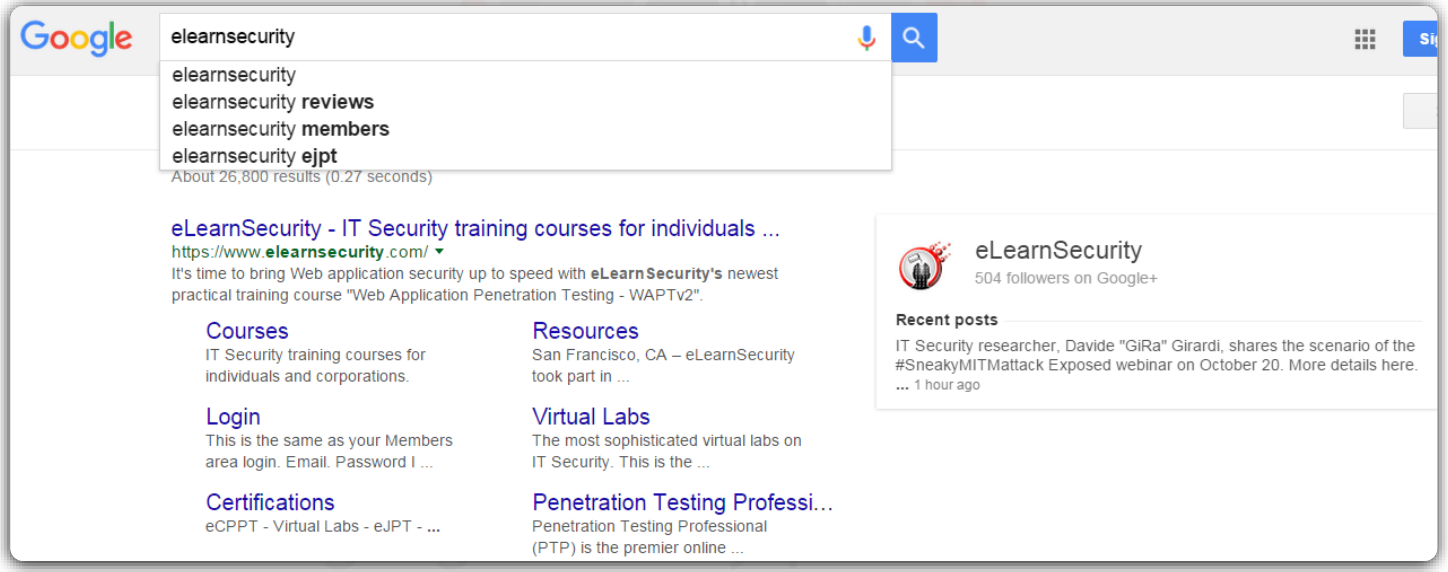


1.2.1.1. Web Presence

In this phase, you will learn a great deal more about your target including:

- What they do;
- What is their business purpose;
- Physical and logical locations;
- Employees and departments;
- Email and contact information;
- Alternative web sites and sub-domains;
- Press releases, news, comments, opinions;

The best way to start is to search the company name in order to find the company website. You can easily do it with most common search engines such as Google or Bing.



Organizations' web sites are usually the best source of information on a target. This is the place where customers, clients and the general public go to understand them.

So the web site is like window shopping where the organization provides the most important information on display for all to see.

Let's study the company website and see what information we mine from it (using elearnsecurity.com).

This is an example of information you can obtain:

Business

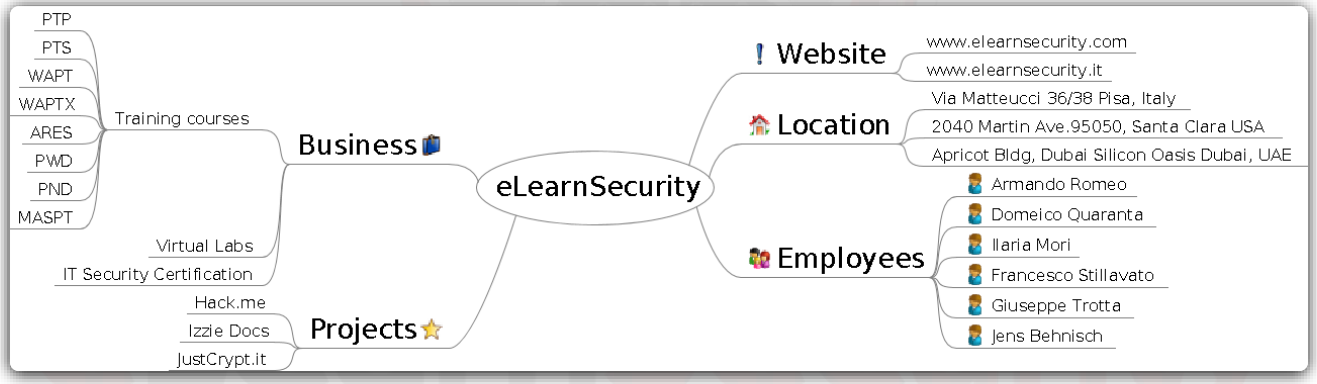
Projects

External links

Location

1.2.1.1. Web Presence

Each time you find something new on the target company, jot it down in your mind mapping tool. In our case this is what we were able to gather thus far:



Once we have analyzed the website in depth and saved the extracted information (in our mind mapping tool), we can move on with analyzing information that is publicly available on the internet.

The first step is to leverage the power of advanced search engines like Google and its dorks.

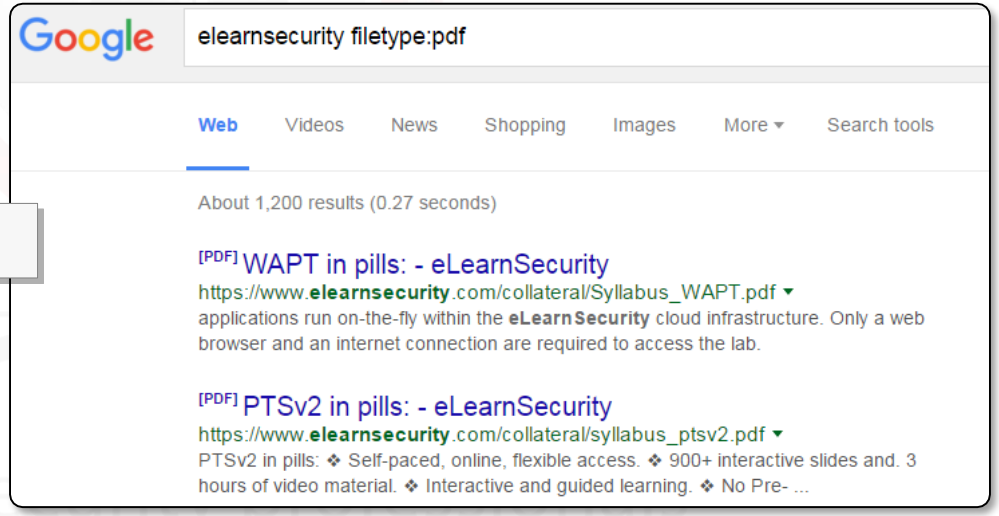
Google offers the opportunity to perform advanced search queries using special operators. Beyond the common operators (*AND*, *OR*, *+*, -, “”) there are more specific filters that you can use.

The following are just few of them:

Cache	[***cache:www.website.com***] will show the cached content of website.com (*type this command in the address bar*)
Link	[***link:www.website.com***] will display websites that have links to the specific website. In this case the command will show all webpages that have a link to www.website.com
Site	[***google dorks site:www.website.com***] limits the search results to the website given. In this case it will show the results of *google dorks* search *within www.website.com*
Filetype	[***google dorks filetype:pdf***] searches for all document with a specific extension. In this case it will display all *PDF* documents related to the query string *google dorks*

Let us see an example of how to use Google dorks to find all the PDF documents that are somehow related to the query string `elearnsecurity`.

```
elearnsecurity filetype:pdf
```



The previous command shows all the PDF files that contain the word elearnsecurity or that are somehow linked to the word elearnsecurity.

This type of search can be very useful in finding documents that are no longer linked in the webpage. Google usually stores this information for a long period of time.

For more information about operators and filters you can refer to the Google documentation listed below:

- https://support.google.com/websearch/answer/136861?hl=en&ref_topic=3081620
- www.googleguide.com/advanced_operators_reference.html
- http://pdf.textfiles.com/security/googlehackers.pdf
- https://www.exploit-db.com/google-hacking-database/

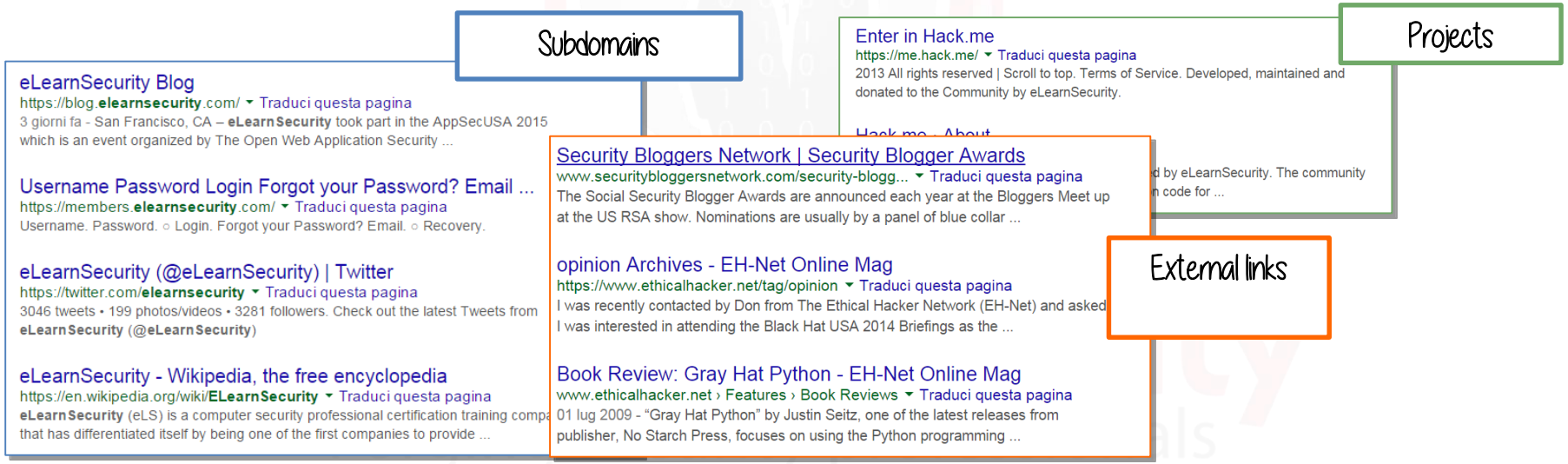
Below are a few additional search engines that could help you retrieve further information:

- Bing
- Yahoo
- Ask
- Aol
- Pandastats.net
- Dogpile.com






The following snapshots show the kind of information that you can retrieve using search engine.

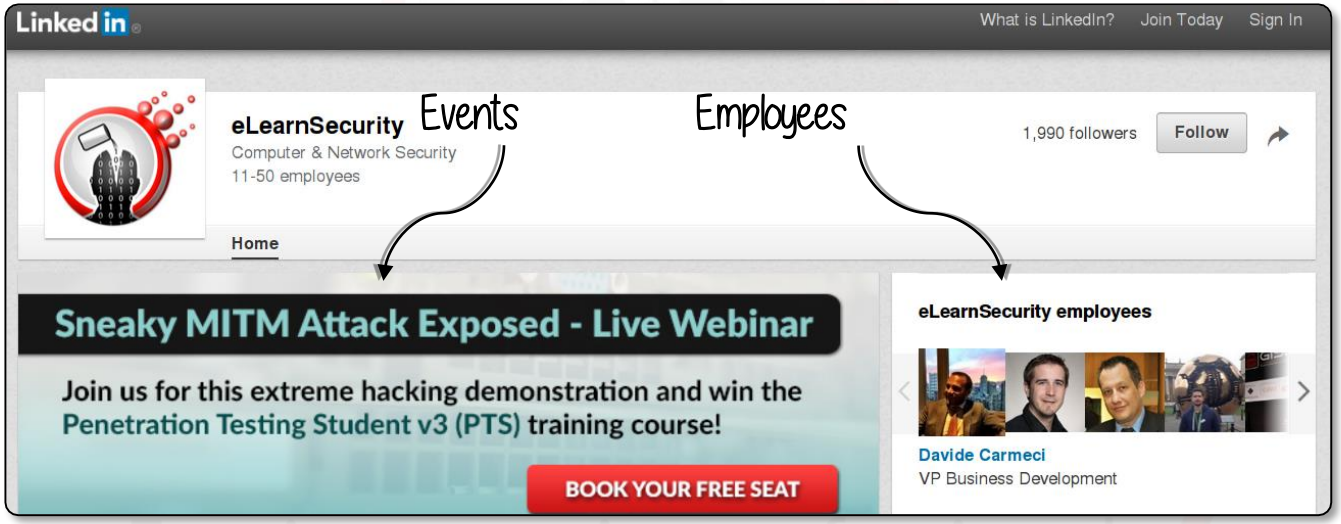


1.2.1.1. Web Presence

The web presence of an organization is not only its website but also any kind of corporate account to third party services.

The simplest example is a company page on LinkedIn.

In our case, we can find employees, events, products, contact info, locations and more.



Websites like LinkedIn show even more information about companies and people that are related to that company especially if you have either a regular account or a premium one.

Unless you restrict your privacy settings, your visits to other LinkedIn profile's will subsequently notify those account owners.

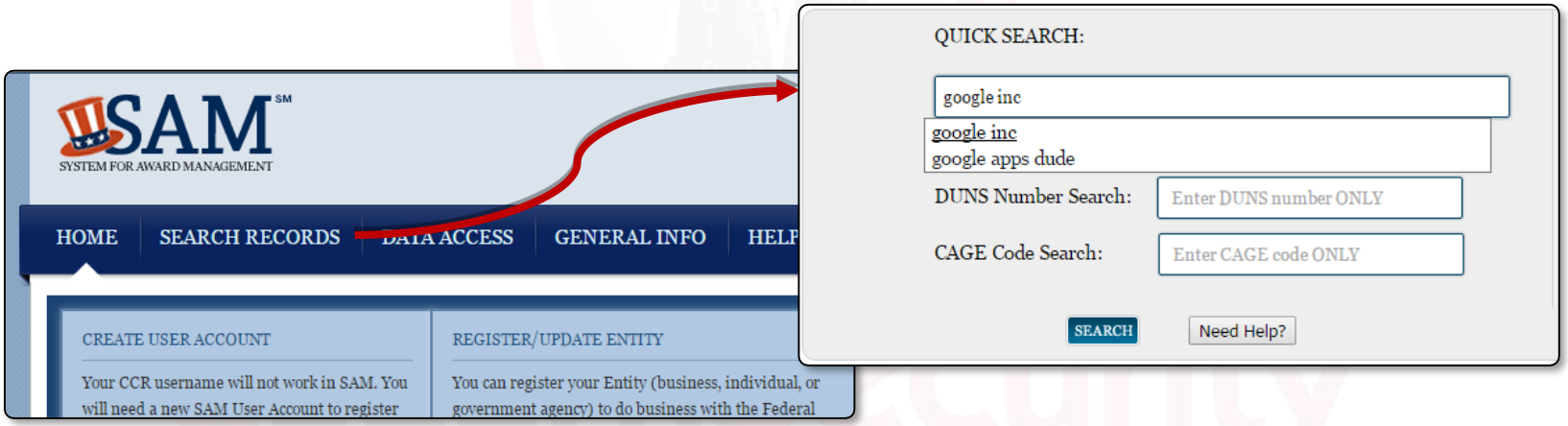
Keep this in mind when performing stealthy operations.

Organizations that operate globally and have a desire to sell to the U.S. government or government agencies, are required to possess two codes useful to us:

- DUNS number (DUNS and Bradstreet)
- CAGE code (or NCAGE for a non U.S. business)

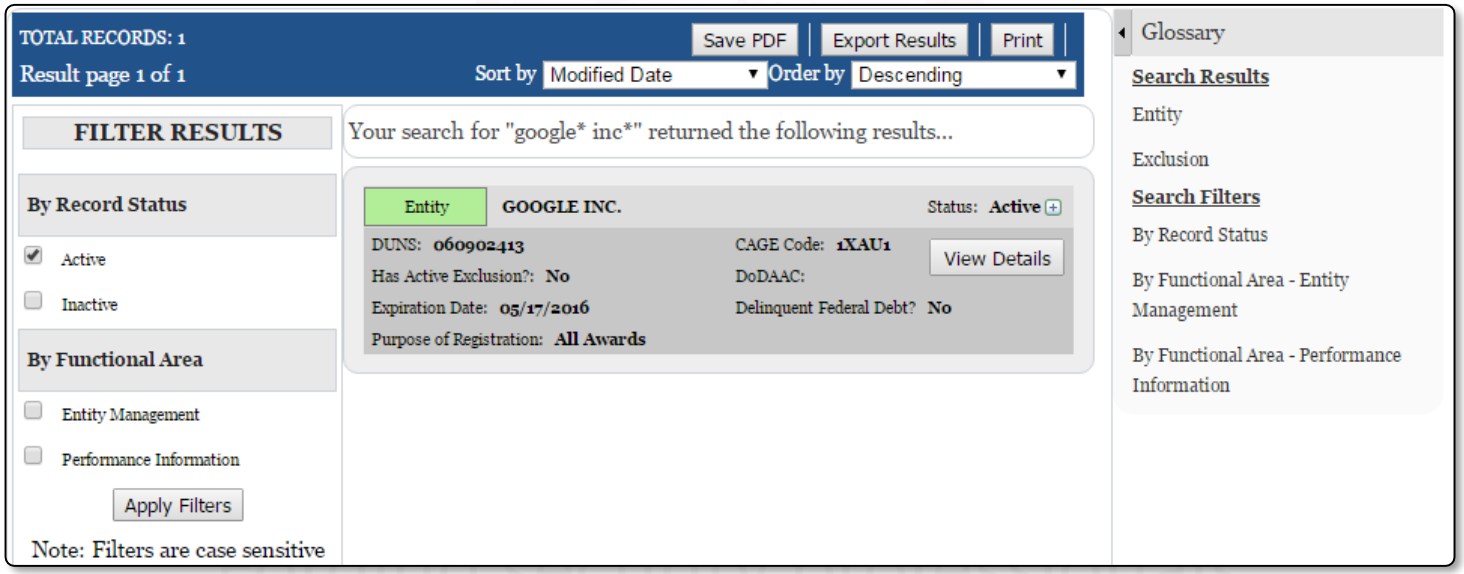
These two codes allows us to retrieve even more information such as contacts, products lists, active / inactive contracts with the government and much more.

We can retrieve the DUNS and CAGE code for a given company from the following web site. Once you arrive click on Search Records:

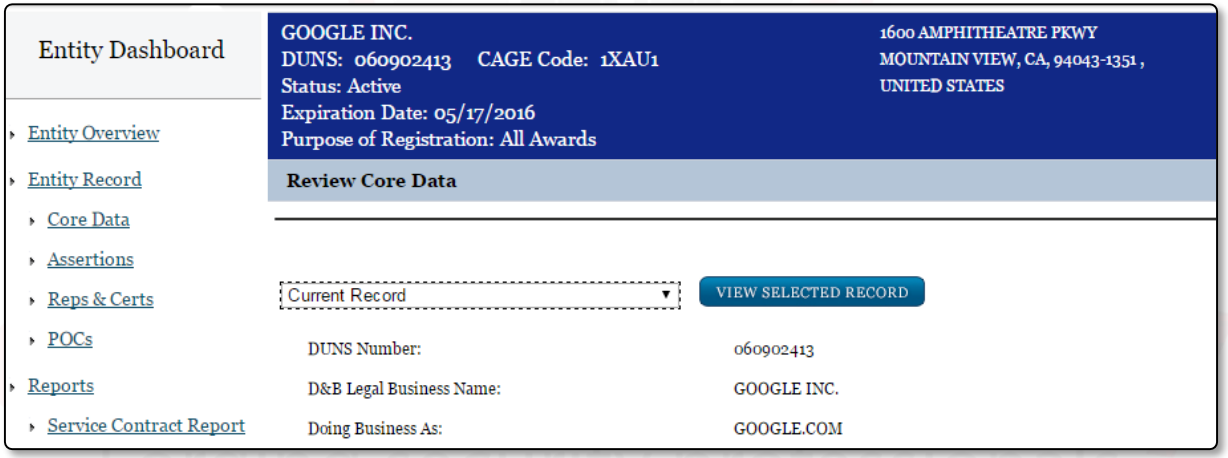


https://www.sam.gov/errors/pageIE11Bellow.html

As soon as we hit enter, a new page will appear, showing some information about the company and its codes:



To retrieve even more information, we can click on View Details. In the right navigation pane of the new page, we are able to perform further searches:



1.2.1.1. Web Presence

You have probably noticed by now that this process is not set in the stone and is never the same for all the organizations.

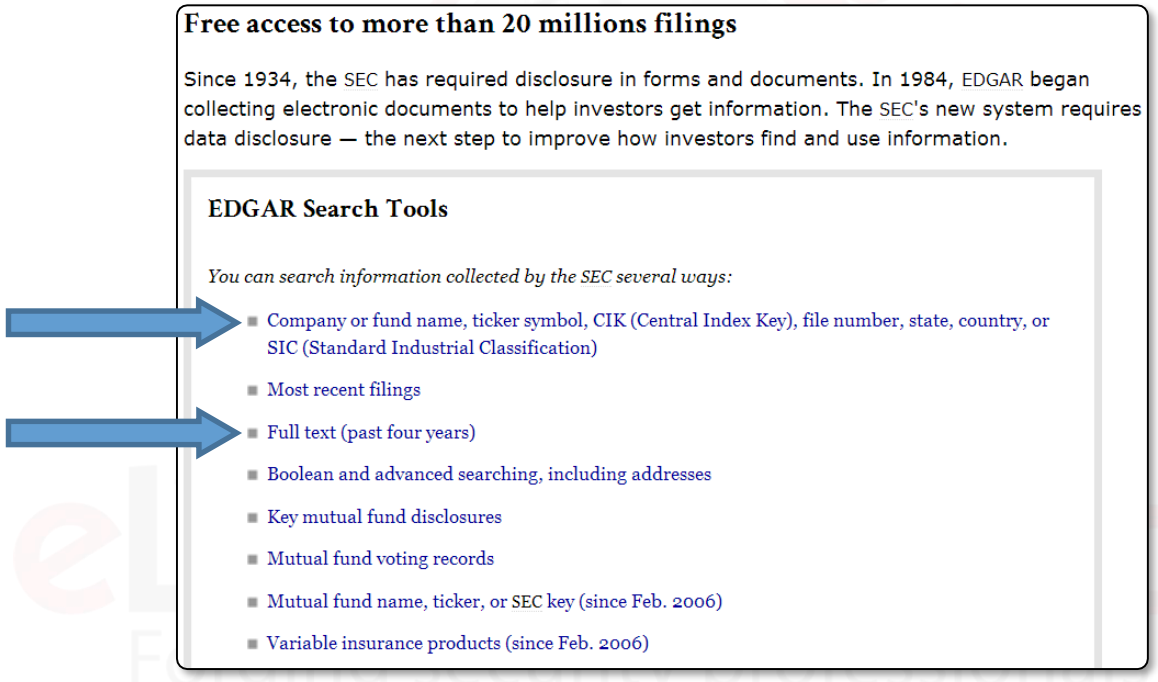
Organizations belonging to different industries can be investigated through search in different publicly available databases. Compliance and regulations might force companies to publish different kind of information publicly.

An example is publicly traded companies that have to file their financial documents to SEC database.

For this purpose you can use the EDGAR (Electronic Data Gathering, Analysis, and Retrieval system)

- http://www.sec.gov/edgar.shtml

After that you can perform specific searches:



Free access to more than 20 millions filings

Since 1934, the SEC has required disclosure in forms and documents. In 1984, EDGAR began collecting electronic documents to help investors get information. The SEC's new system requires data disclosure — the next step to improve how investors find and use information.

EDGAR Search Tools

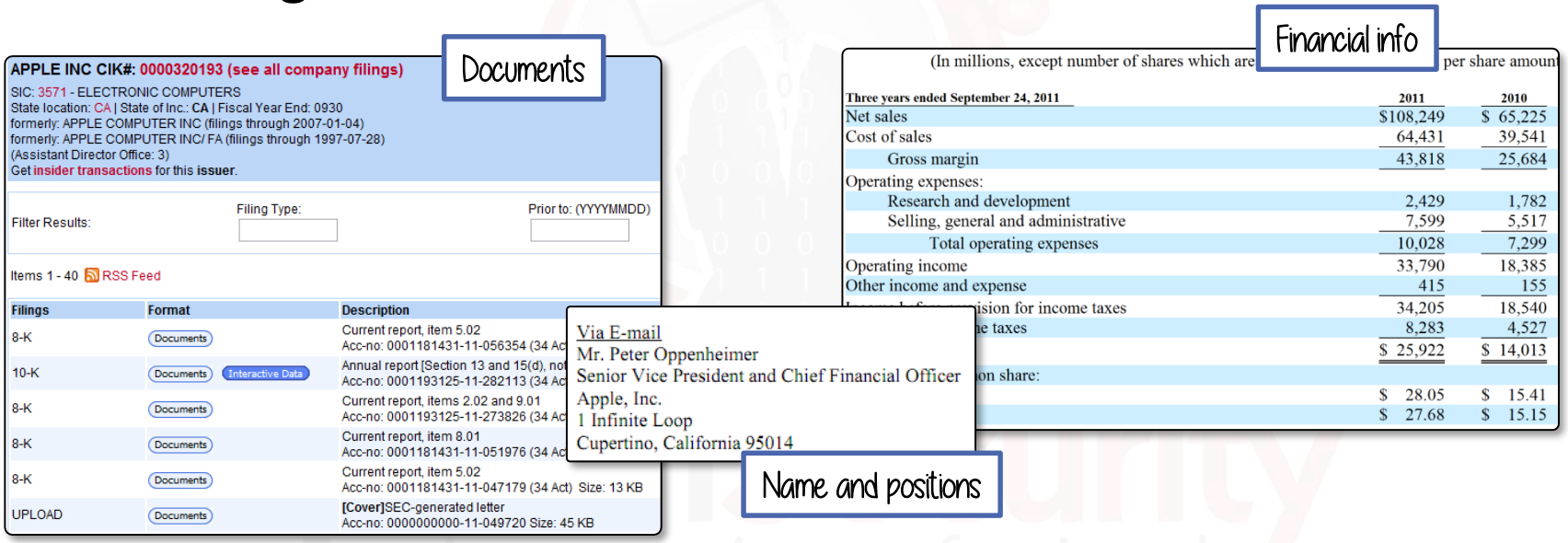
You can search information collected by the SEC several ways:

- Company or fund name, ticker symbol, CIK (Central Index Key), file number, state, country, or SIC (Standard Industrial Classification)
- Most recent filings
- Full text (past four years)
- Boolean and advanced searching, including addresses
- Key mutual fund disclosures
- Mutual fund voting records
- Mutual fund name, ticker, or SEC key (since Feb. 2006)
- Variable insurance products (since Feb. 2006)

1.2.1.1. Web Presence

MAP REF

With these kind of search you will able to see documents like the following:



Note that Information gathering is not a linear process but actually a cyclical process.

When you find new organization projects, websites and subdomains, you have to repeat the whole investigation process for each of them. This will widen the attack surface thereby increasing the chances of a successful outcome of the penetration test.

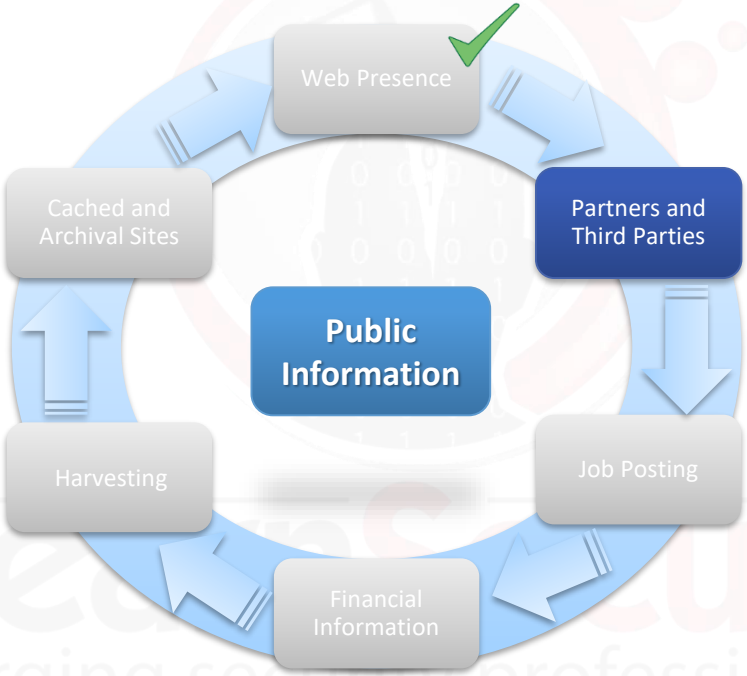
1.2.1.1. Web Presence

Since in this phase we will obtain a huge amount of information, a good practice would be to organize it in a clear and clever way.

Remember to use your mind mapping tool to store your findings!

1.2.1.2. Partners and Third Parties

We can now move on with Partners and third parties.



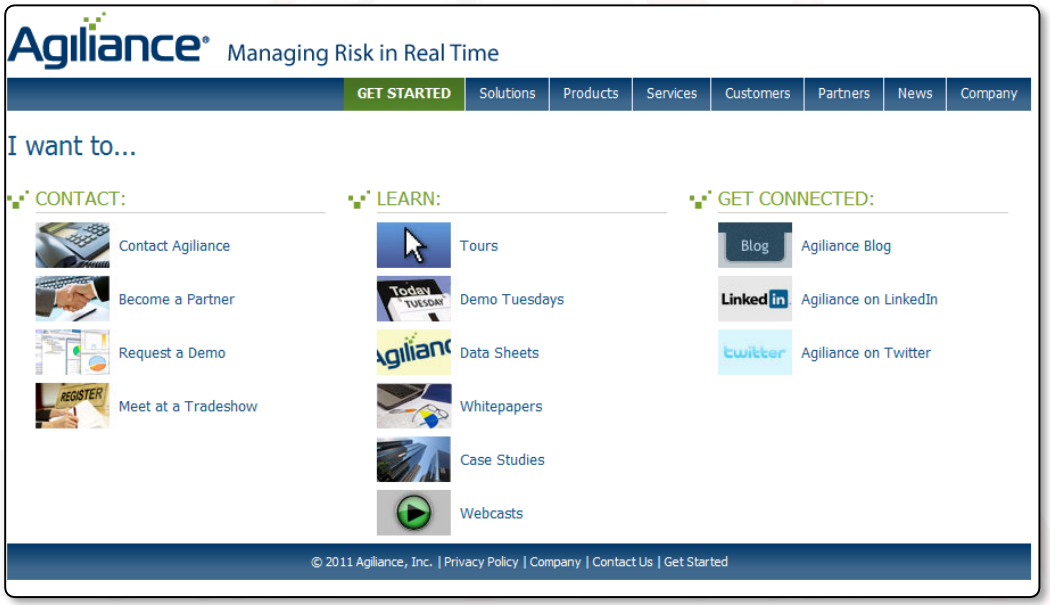
1.2.1.2. Partners and Third Parties

Other useful information that you can gather about the company are mergers and acquisitions, partnerships, third parties...

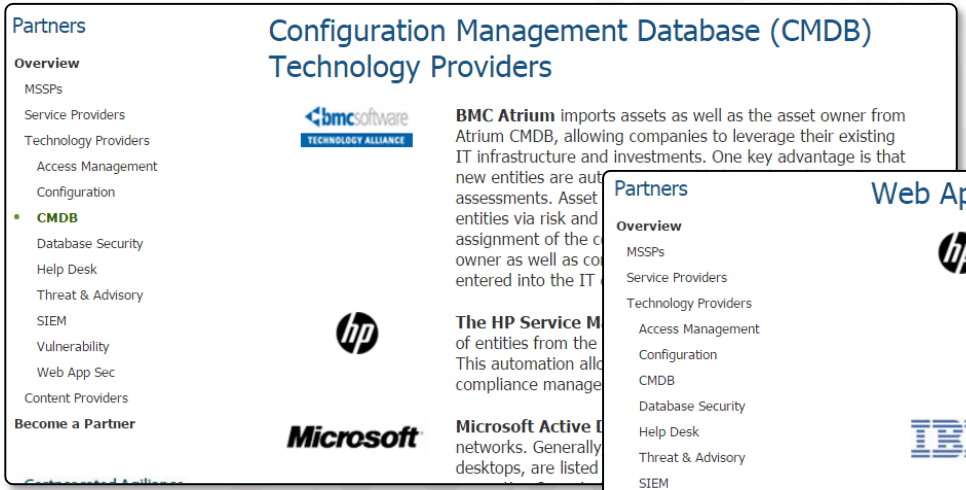
With these you can deduce what type of technologies and systems they use internally. You can take advantage of this information in later phases of the pen test.

You can also use it to perform a more effective social engineering attack with a higher chance of success.

Let us use Agiliance as sample case study:



Surfing the website you can easily gather information about their partners:

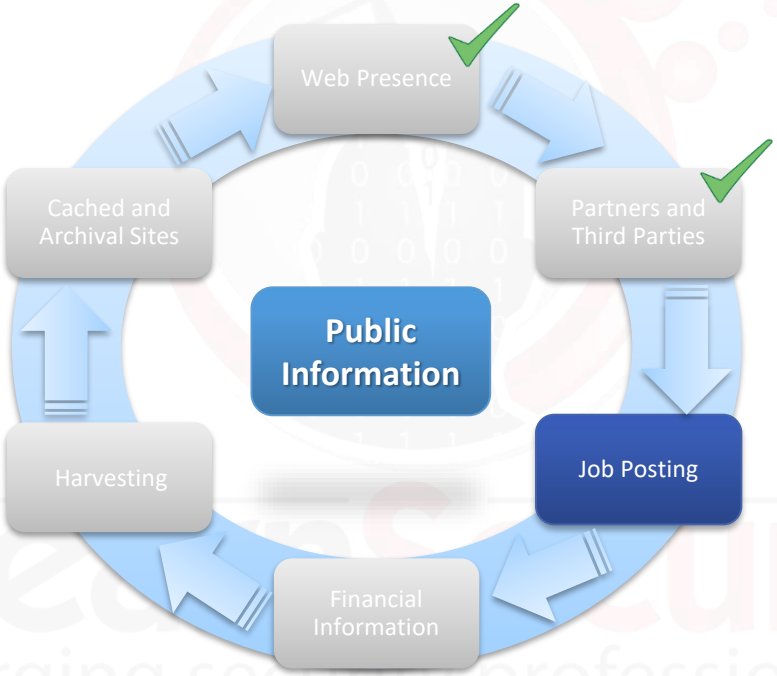


1.2.1.2. Partners and Third Parties

From these web pages, you can gather information such as the technology stack the organization uses (hardware and software), tools, systems and so on.

Remember that every piece of information you can acquire may come in handy later on.

The next step is finding information from Job Postings.



At this point of the process you should have already collected a large amount of data.

Is this all you will collect? Absolutely Not! This is a long process that you will even want to expand the scope with experience.

Now we can start looking for job postings and frequenting job boards.

1.2.1.3. Job Posting

Many organizations have a web site section including open positions and career opportunities.

This might not seem like harmful information however, an investigator can deduce internal hierarchies, vacancies, projects, responsibilities, weak departments, financed projects, technology implementations and more.

Let us see an example in our case study.

From the corporate website, we can find useful information about job openings.

Agiliance Current US Job Openings

Agiliance offers competitive compensation and a full benefit package including stock options, medical, dental, vision, life insurance, child care reimbursement, and more.

#AG4.51 Sales Director
#AG4.52 Senior Sales Engineer
#AG4.57 Quality Assurance - US Technica
#AG4.59a Java Server Software Develope
#AG4.59b Senior Java Server Software De
#AG4.59c Principal Java Server Software
#AG4.60a Java/JavaScript Software Devel
#AG4.61 Product Support Engineer
#AG4.62 Product Marketing Manager
#AG4.66 HR, Office and Projects Coordina
#AG4.67 GRC Solution Architect
#AG4.68 Product Manager

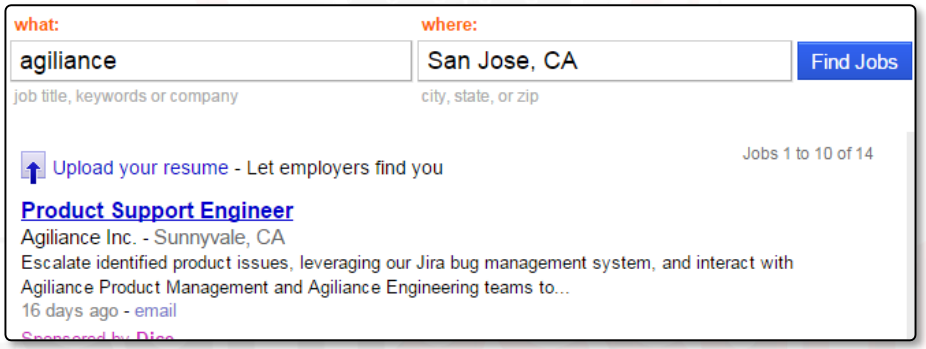
REQUIREMENTS

- Experience in the development of scalable, high p
- Excellent working knowledge of Java, J2EE, JSP,
- Strong working knowledge of application servers or JBoss.
- Strong working knowledge of MySQL and/or Orac
- Experience with the Spring Framework is a plus.
- Experience with JavaScript libraries like jQuery an is a plus.
- Experience with reporting frameworks like Jasper
- Solid knowledge and application of engineering c
- Understands development methodology and deve
- Problem solving capabilities and analytical skills.
- Excellent verbal and written communication skills,
- Ability to work in a team environment.
- Enthusiasm to learn new tools and technologies.
- Degree in Computer Science (or equivalent).
- 2-5 years of experience required.

Skills

- Apache, Tomcat, Oracle 11g, and MySQL system administration fundamentals.
- Familiarity with at least one interpreted language and frameworks such as JAVA, JSP, AJAX, Hibernate, Web Services, etc.
- Experience with Salesforce.com, Cisco WebEx, FTP, SQLYog, and LDAP Browser.
- Familiarity with standard concepts, practices, and procedures relating to Microsoft Windows Operating Systems, Microsoft Windows networking, and troubleshooting Microsoft Windows network environments.
- Development and debugging of SQL scripts and queries.
- Development and debugging of Oracle data base issues and queries.
- Good working knowledge of security tools, techniques, and methodologies such as Kerberos, SAML, LDAP, and SiteMinder.
- Strong verbal and written communication skills for delivery in document, Web, and presentation form, as well as over the phone.
- People skills that promote personal relationship building between virtual teams - working directly with varied headquarters and overseas resources.
- Highly organized, self-directed with strong ability to prioritize and manage multiple

If you do not find useful information on the organization website, you can use more specific search engines such as Indeed.

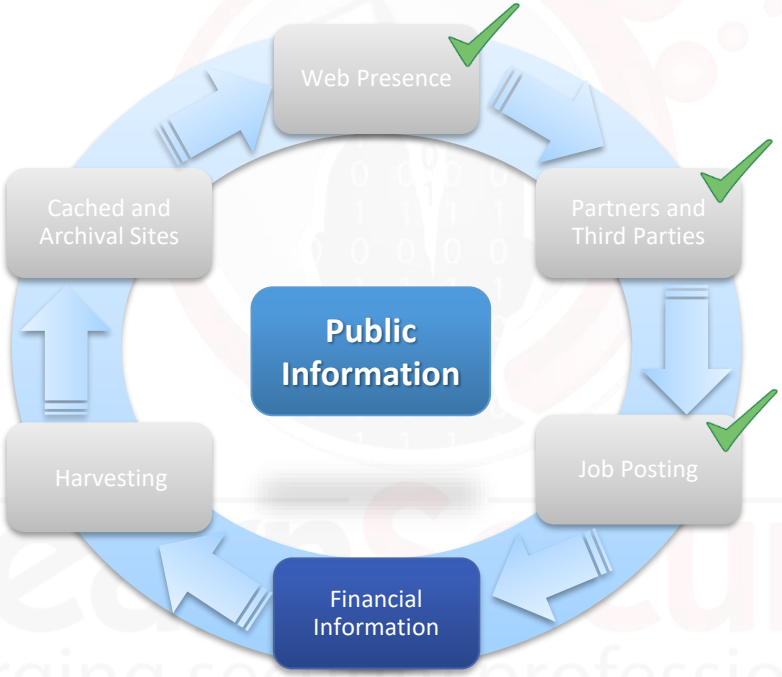


https://www.indeed.com/

The following is a list of websites that you can use to find job posts:

- LinkedIn
- Indeed
- Monster
- Careerbuilder
- Glassdoor
- Simplyhired
- Dice

Let us focus now on Financial Information.



1.2.1.4. Financial

More useful information can be acquired from financial details about the organization.

For example, you can easily find out if the organization:

- is going to invest in a specific technology
- might be subject to a possible merge with another organization
- has critical assets and business services

Let us see which tools we can use to gather this information.

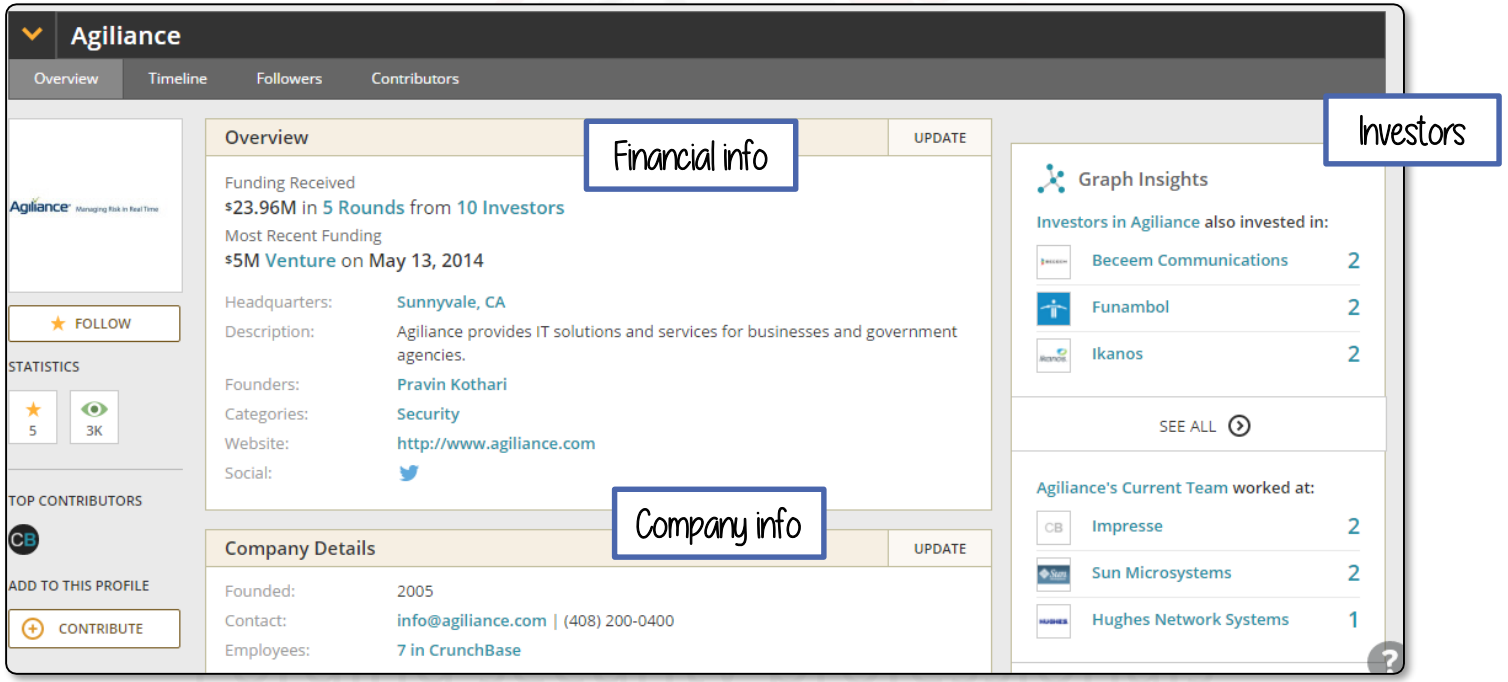
The first we will examine is www.crunchbase.com. *CrunchBase* is a database where you can find information about:

- Companies
- People
- Investors and financial information

CrunchBase

The power of *CrunchBase* is grounded on the concept of anyone being able to edit information in it.

This snapshot shows what kind of information you can find:

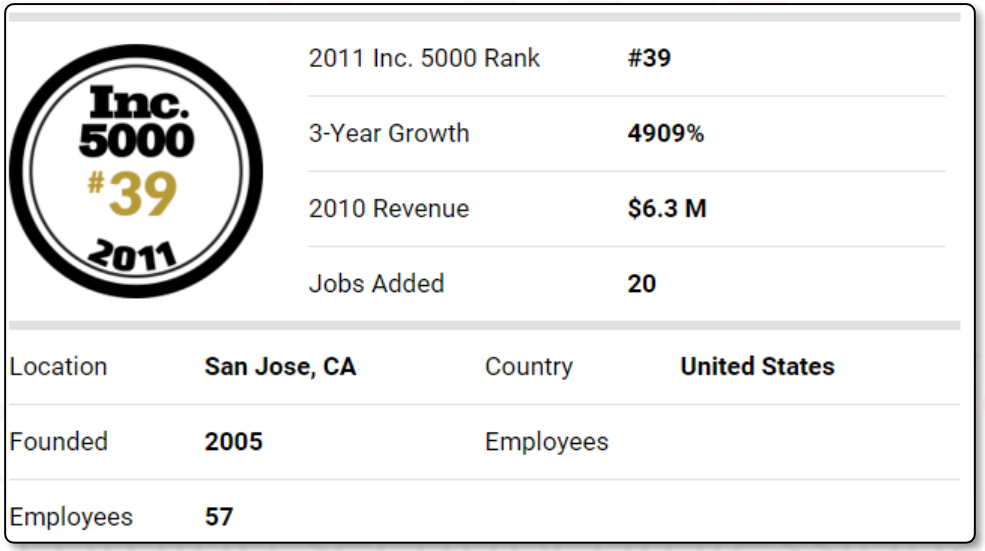


Another useful online resource is www.inc.com.

Inc. focuses its attention on growing companies and provides advice, resources and information to companies.

Moreover, Inc. offers a list of the 500/5000 fastest-growing private companies, showing very useful information and statistics on them.

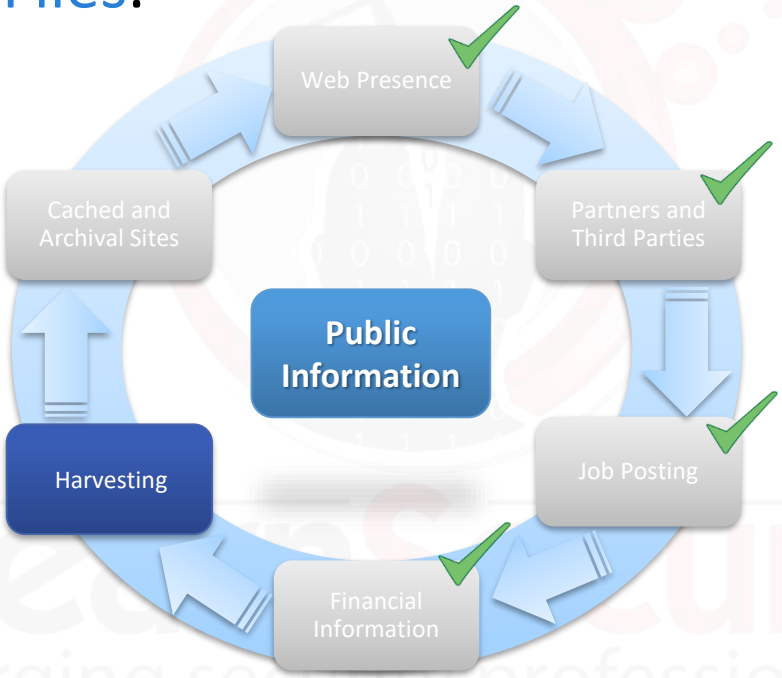
The following snapshot shows the result of a search of our target company, providing us a different look on some information.



The following are additional resources that you can use to find out more financial information on your target.

1.2.1.5. Harvesting

Let us find out what kind of information we can gather from Documents and Files.



1.2.1.5. Harvesting

In this phase, we unpack methods for gathering company documents such as charts (detailing the corporate structure), database files, diagrams, papers, documentation, spreadsheets and so on.

Moreover, this is the right time to begin harvesting emails, accounts (Twitter, Facebook, etc.), names, roles and more.

It is important to know that when a document is created, it automatically stores information (*metadata*) like who created it, date and time of creation, software used, computer name and so on.

If we are able to retrieve documents online and inspect the underlying metadata, we can extract useful information.

First, let's see a simple way to find online files and documents using Google Dorks. To do this we can use the following google filters:

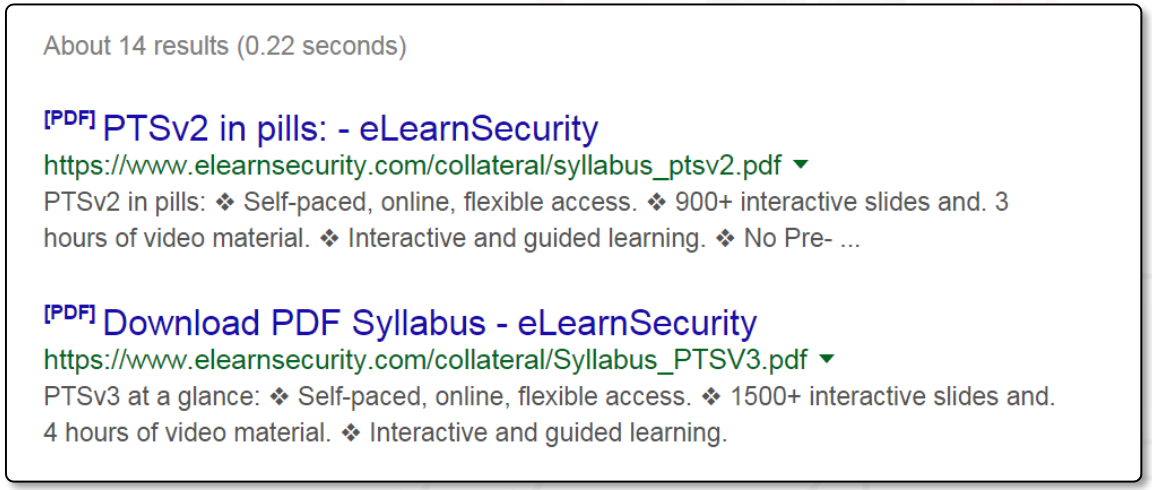
```
site:[website] and filetype:[filetype]
```

This will narrow down the results and display only the links to files with the `[filetype]` extension and stored in the website `[website]`.

Let us see an example for *elearnsecurity.com*

With the following search string we will obtain all the .pdf files in the elearnsecurity.com domain:

```
site:elearnsecurity.com filetype:pdf
```



Note: you can perform this searches for other types of files, such as doc, txt, xls, databases extensions and more.

1.2.1.5. Harvesting

As you can imagine, doing this manually can be very tedious and time consuming. A very useful tool that allows us to automatically find and download files is FOCA.

By querying search engines like *google* and *bing*, Foca is able retrieve files and then attempt to extract metadata such as names, usernames, password, OS etc.

Note that this tool works only on Windows unfortunately.

https://www.elevenpaths.com/labstools/foca/index.html

Remember that in this phase, our goal is to retrieve only business information.

Since tools like FOCA allow us to download and extract *infrastructure information* as well, (OS, servers, IP addresses, path etc.) we will see how to use those types of “assets” later on.

In the following slides, we will see some other tools that will help automate additional information gathering. The first tool we are going to see is theHarvester. You can download it here.

Thanks to search engines and social networks (*Google*, *Bing*, *LinkedIn, etc.*), *theHarvester* is able to enumerate email accounts, user names, domains and hostnames.

https://github.com/laramies/theHarvester

Once we have the tool installed on our machine, we can run the following command in order to retrieve information about elearnsecurity.com:

```
theharvester -d elearnsecurity.com -l 100 -b google
```

where:

- `-d` is the domain or the company to search
- `-l` limits the results to the value specified
- `-b` is the data sources. (I.e. you can set Bing, Google, LinkedIn, etc.)

The following screenshot shows part of the results of the previous command:

It is important to know that different search engines return different results, therefore, you should try different data sources in order to obtain the best results. For example, LinkedIn returns a list of names related to *eLearnSecurity*:

```
theharvester -d elearnsecurity.com -l 100 -b linkedin
```

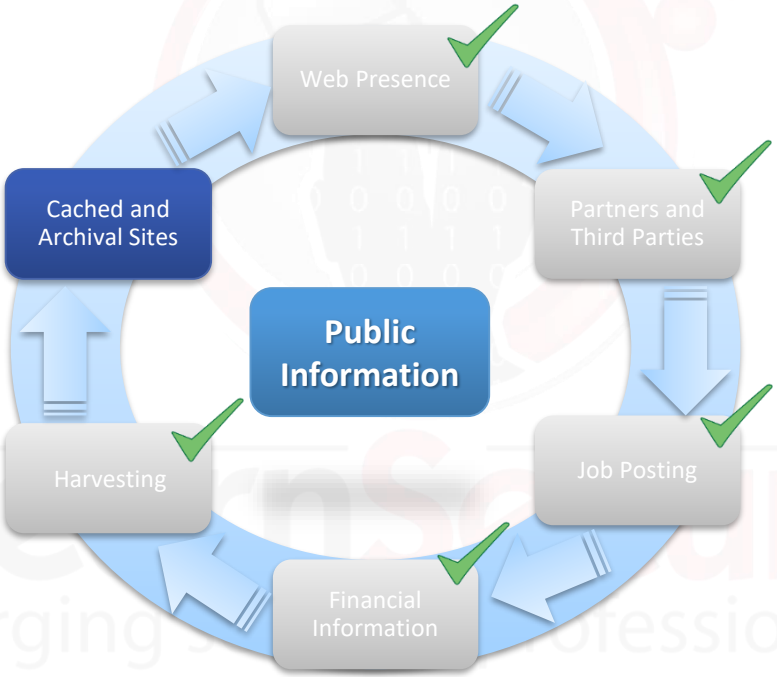
```
[-] Searching in Linkedin..
        Searching 100 results..
Users from Linkedin:
====================
Armando Romeo
Jens Behnisch
Jason Haddix
Edcel Suyo
Schuyler Dorsey
Francesco Stillavato
Domenico Quaranta
```

At the end of this phase we should have a list of names, email addresses, documents, telephone numbers, usernames and so on.

Remember to log everything, and if needed, go deeper in research for each item of your list.

1.2.1.6 Cached and Archival Sites

In the last step (not really last, this is a cyclic process) we will see how to gather information from Cached and archival sites.



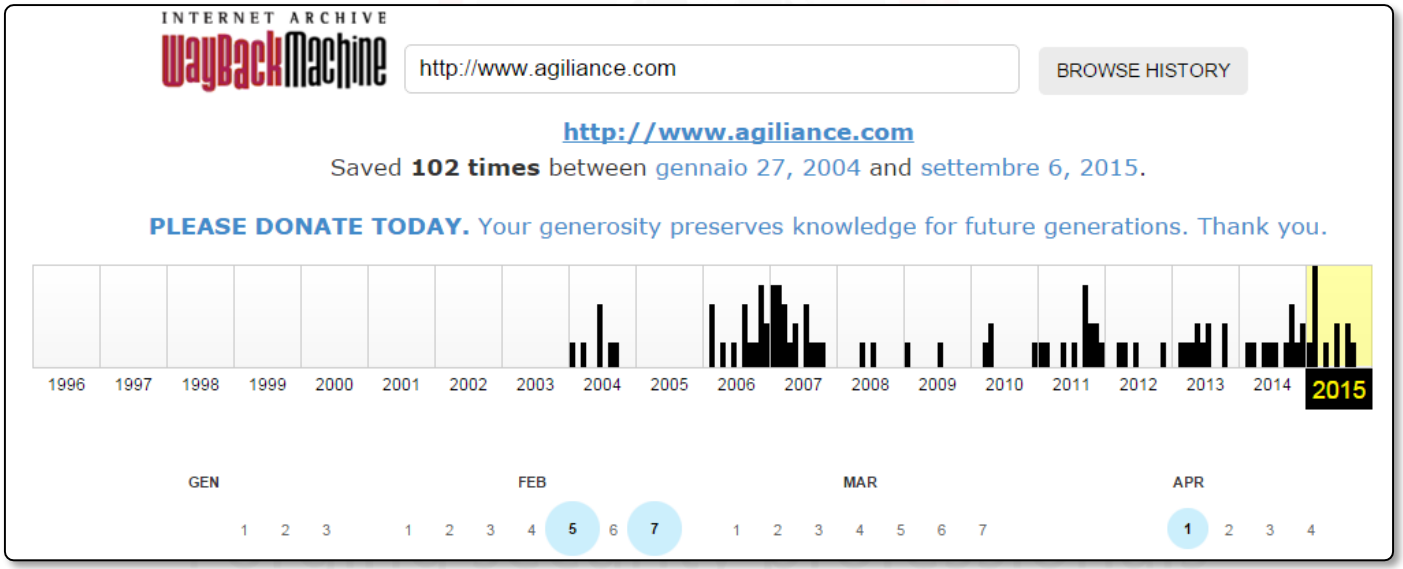
1.2.1.6 Cached and Archival Sites

Since information on the web changes so quickly, sometimes seeking an older version of a site could prove useful to our cause.

Consider a job post. If the organization deletes it from the website, you will “lose” that information; if you could see the web page, before the update, you could harvest that information. Turns out this is entirely possible through cache and archival technology.

1.2.1.6 Cached and Archival Sites

A website that can help us is archive.org. Here you can simply search a specific domain and then navigate through different date and versions of that specific domain.



https://archive.org/

1.2.1.6 Cached and Archival Sites

Similarly, you can use the Google dork `cache:URL`. With this technique, you will see a cached version of the website.

By now, you should have a healthy amount of useful information about your target organization.

Due to the fact that the process takes such a long time, it could be useful to repeat some of the previous steps in order to see if something has changed.

To conclude the first part of the information gathering process, it is imperative to focus on the employees of our target organization.

This is a very important task that can reveal a great deal of information. Thanks to social networks, we can take advantage of private information that is carelessly revealed on the web with little to no thought from the employee.

The best way to learn how to perform effective information gathering is by doing it.

In the next slide you will find a special lab on a real world target organization you will need to use the techniques learned in the course thus far and apply them.

1.2.1. Search Engine

eLSFoo is a fictitious company created by eLearnSecurity. You are given authorization to perform Information gathering on this organization (no attacks are allowed against the target).

Your goal is to create a mind map containing information about *eLSFoo*:

- Employees
- Emails
- …

Lab : Real world Information Gathering

Labs are available in
FULL and ELITE plans only

eLSFoo Information Gathering

Each lab has its own manual
Find it in your members area

eLearnSecurity has created eLSFoo, a fictitious company located at www.elsfoo.com.

Apply all the learned techniques to find and collect information regarding the company.

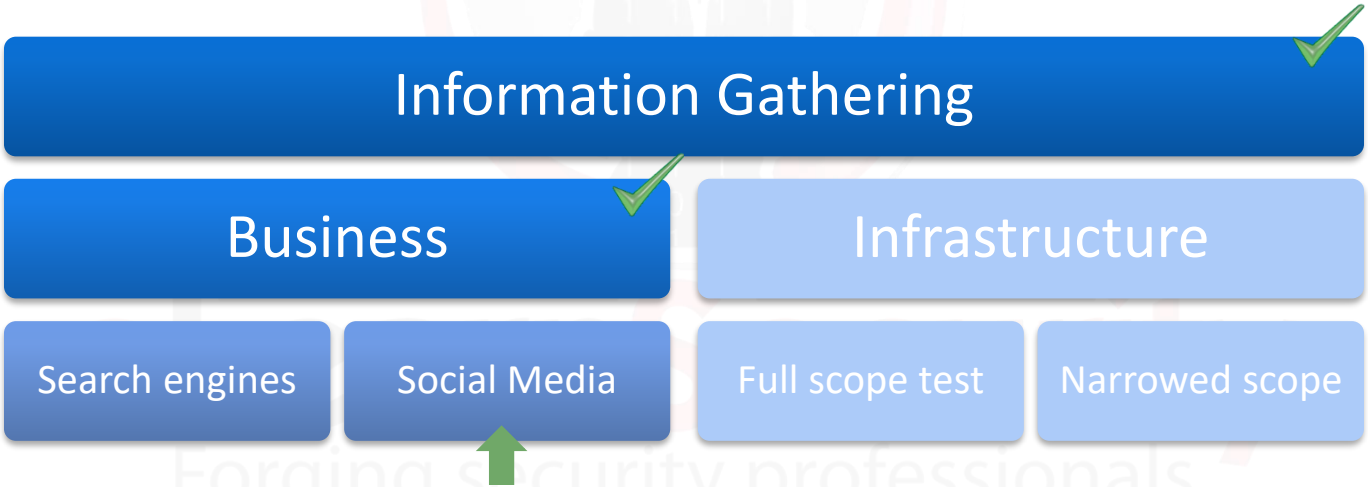
Social Media

The spread of Social networks has made Information gathering extremely important (and effective).

With the help of social media, a penetration tester can easily gather employee's personal information such as: phone numbers, addresses, history, CV, opinions, responsibilities, projects and so on.

Since humans are the *weakest link in the IT security chain*, a good penetration test must take care of them (if in the scope).

During the entire Information Gathering process we are going to see the Social Media tasks. Keep that in mind as you are going through the slides.



In this particular phase, social media is useful in the following ways:

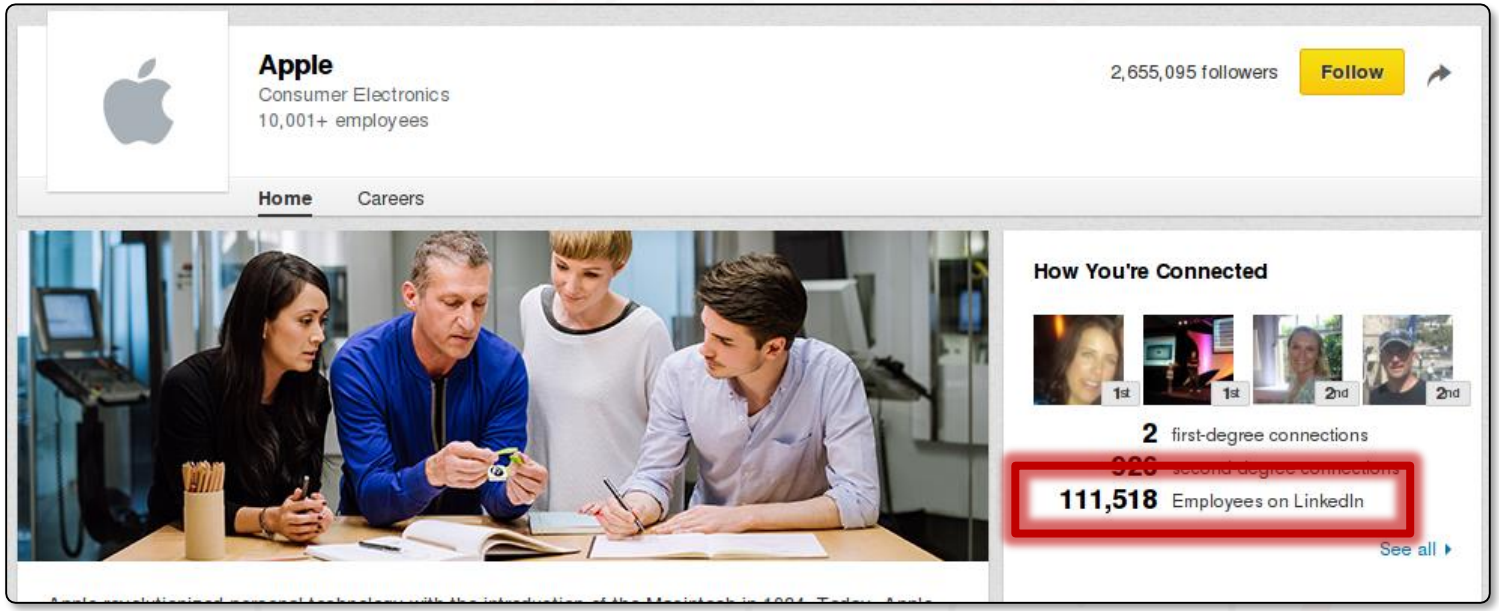
- Learn about corporate culture, hierarchies, business processes, technologies, applications.
- To build a network map of people (relationships).
- Select the most appropriate target for a social engineering attack.

In the previous phase you should have already compiled a list of managers, employees etc. What we have to do now, is gather information on every person on this list.

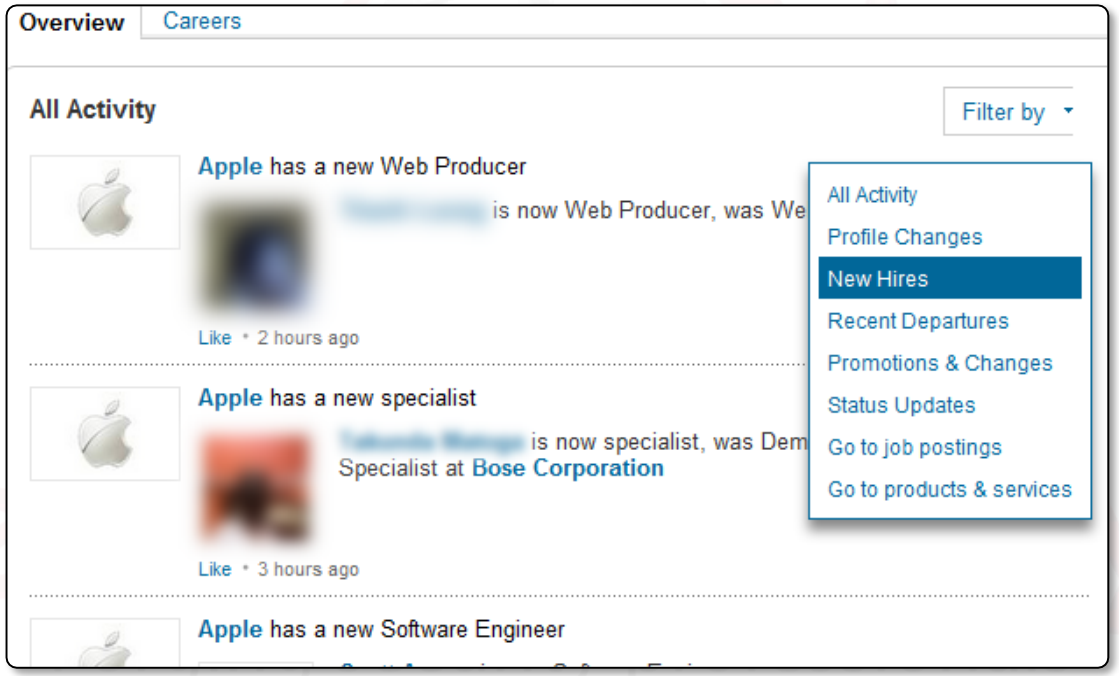
We will use *Apple* for our case study.

Let's take a step back and review how to mine employee lists from social media.

You can use LinkedIn to gather (most of) them:



Retrieve more by searching in Apple activity:

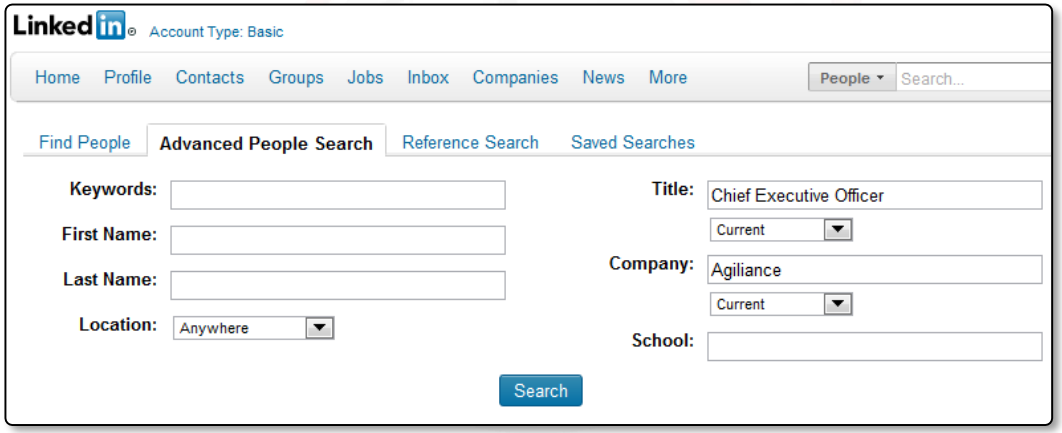


On LinkedIn, you can perform advanced search functions on people based upon: current title, position, location, company and so on.

Let's presumably say we have the desire to start building a network map of people in Agiliance. Suppose we do not know who the CEO is.

You can click on advanced search in LinkedIn and start filling in search fields.

This is an example of what we can type:



In the next page, we can refine our search by a more specific location, business and more.

Note that when you perform these types of searches within *LinkedIn*, you may not see all the information about the people you are looking for as it depends upon the privacy settings of the target, relationship degree or shared groups.

If your target is a 1st or a 2nd connection, then you will see all their information. If he/she is a 3rd connection you will see only the name and the first letter of the surname.

In all other cases, you will even less limited information, and no full name.

When this occurs, you can do the following:

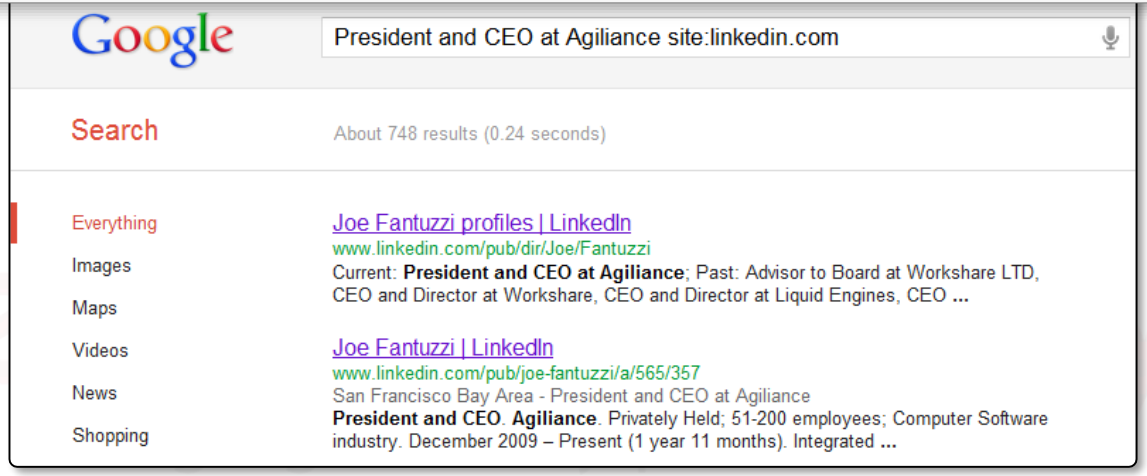
- upgrade your LinkedIn account
- use a specific query in a search engine (Google, Bing...), in order to find (if exists) the public LinkedIn profile of the target

Let’s go back and see what we can retrieve from the previous search.

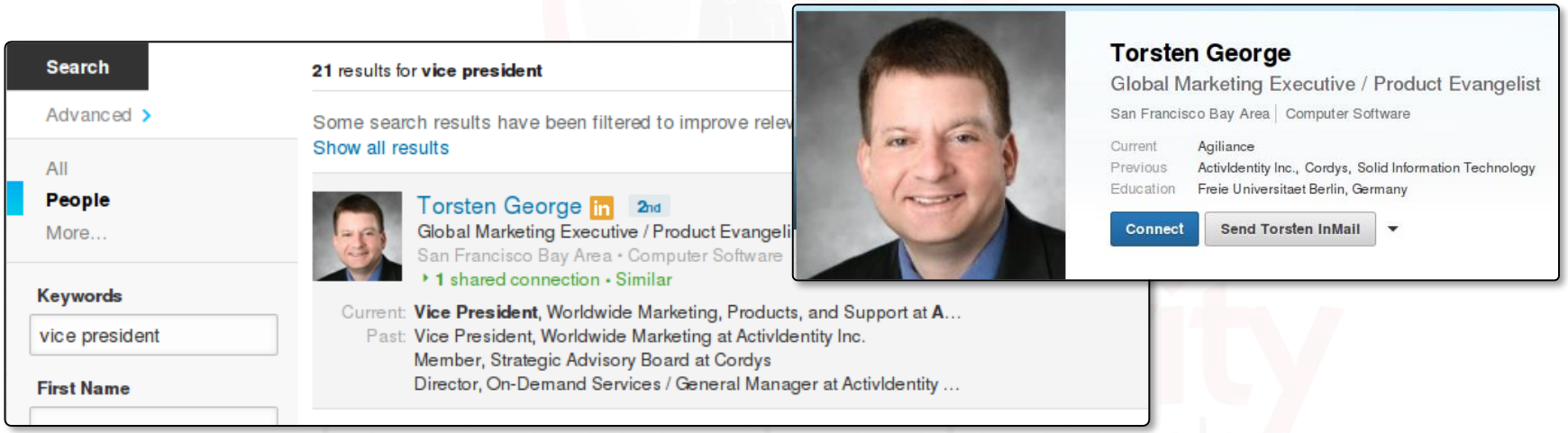
The following snapshot shows the results of our search. As you can see we are able to see the contact information.

As we said, if LinkedIn does not return a profile, we can still leverage a search engine. In this case it is enough to search '*President and CEO at Agiliance*' using the following filter:

```
site:linkedin.com
```



We can continue our investigation for additional titles and positions in the company and create a people map. Let's now search for a V.P.



After a few more searches, you should be able to start building a good network of people:

Why is building a network of people important?

Social engineering (among the other things) is the art of exploiting trust relationships.

If your target is Bob and you know that Bob trusts Adam therefore, you can get to Bob through Adam. Figuring out this trust relationship is an important part of the information gathering process.

Once you get a list of people, you can start collecting personal information on them.

Once again, *LinkedIn* offers the ability to see the connections a person has with both other colleagues and, friends. This could help you in building a people network map.

Moreover, thanks to social networks like *Twitter*, *Facebook* and *Linkedin*, you can infer the level of relationship between two people.

Twitter is especially good at that very function because you can see public conversations between two people.

We have seen how to get info from LinkedIn, but there are many other sources where you can mine additional data.

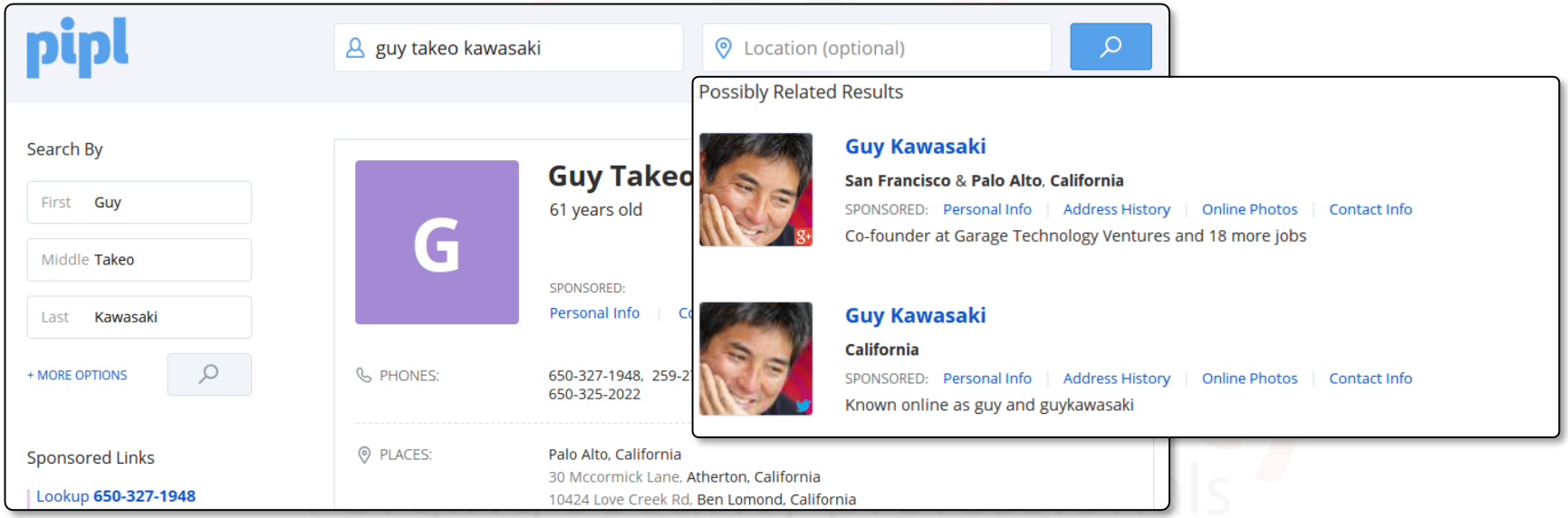
People search

Social Networks

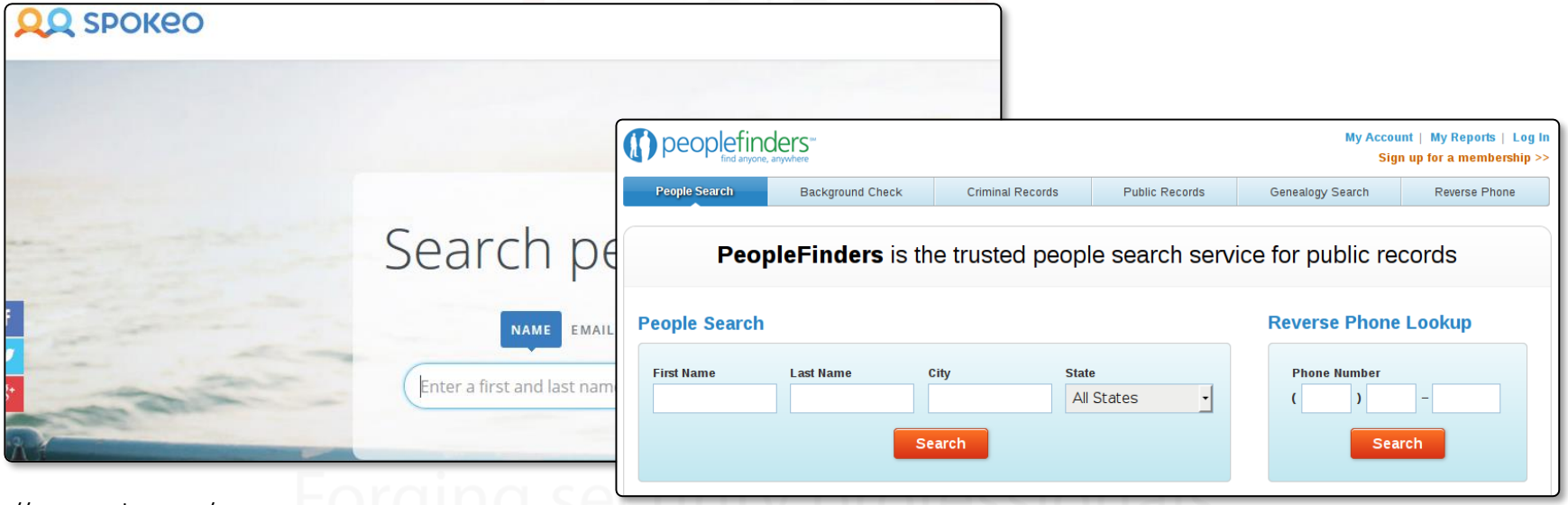
Usenet

1.3.1. Social Media – People search

We can use www.pipl.com to retrieve more information about individuals. Let the famous *Guy Kawasaki* be our target and let's see what we can uncover about him using this tool:



Other very useful websites that you can use to find more information on someone are spokeo and peoplefinders:



https://www.spokeo.com/
https://www.peoplefinders.com/

We can even use CrunchBase to find more information about our target:

https://www.crunchbase.com/

1.3.1. Social Media – People search

At this point of our information gathering phase we already know some information seen below:

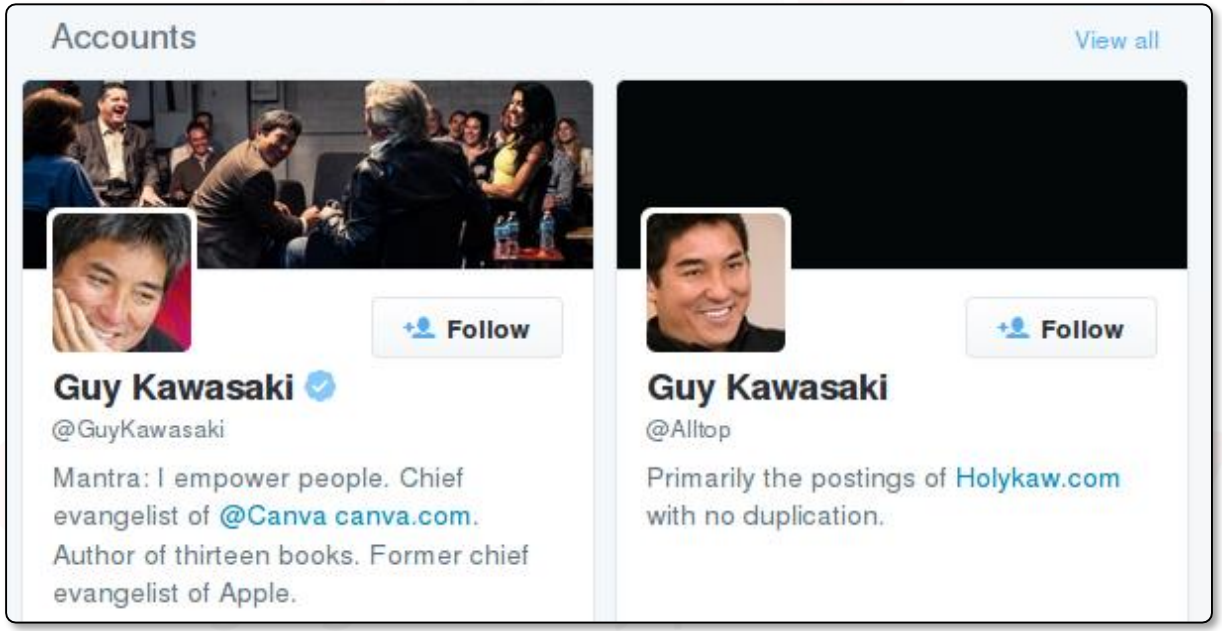
- Age
- Phone Number
- Business
- Addresses
- Occupation
- Interests

Further searching will tell us:

- Email addresses
- Related Documents
- Website Owned
- Financial Info

1.3.1. Social Media – People search

While discussing Social Networks, let's see what we can retrieve by searching "Guy Kawasaki" on Twitter.

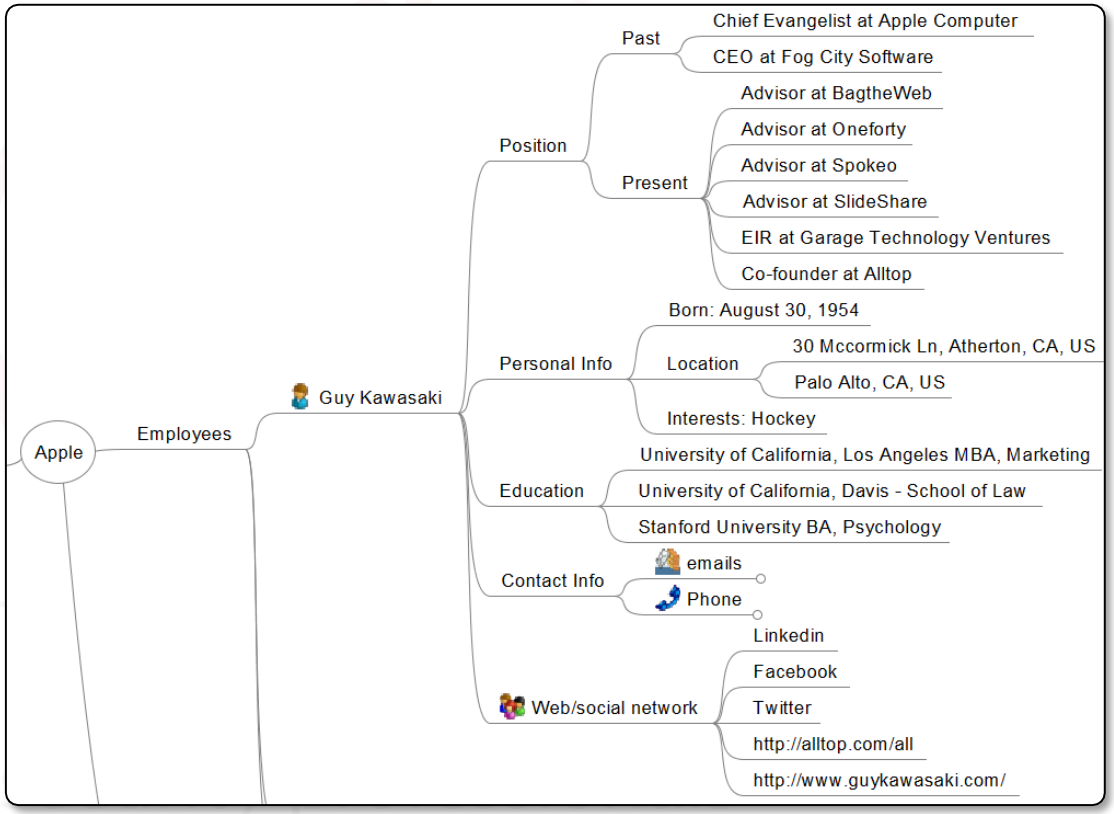


1.3.1. Social Media – People search

By inspecting the messages and information published online we can retrieve information such as projects, travel, interests and so on. Some of this information may be useful later on.

1.3.1. Social Media – People search

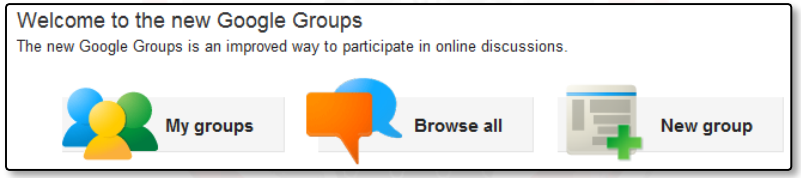
Now that we have all this information, let us put it all together and organize it in our mind mapping tool.



At this point, we have amassed a healthy amount of information on our target. In our examples we just barely scratched the surface of the information available online. In a real pen test engagement you will probably need go deeper in detail.

At this point we are almost done, but there is another area that we did not touch yet: usenet and newsgroups.

Usenet is a world-wide distributed discussion system. It consists of a set of newsgroups with names that are classified hierarchically by subject.



We can also find additional information by searching for individuals' name or email in Google groups. This may lead us to further sensitive data shared by the target company and its employees..

Your turn

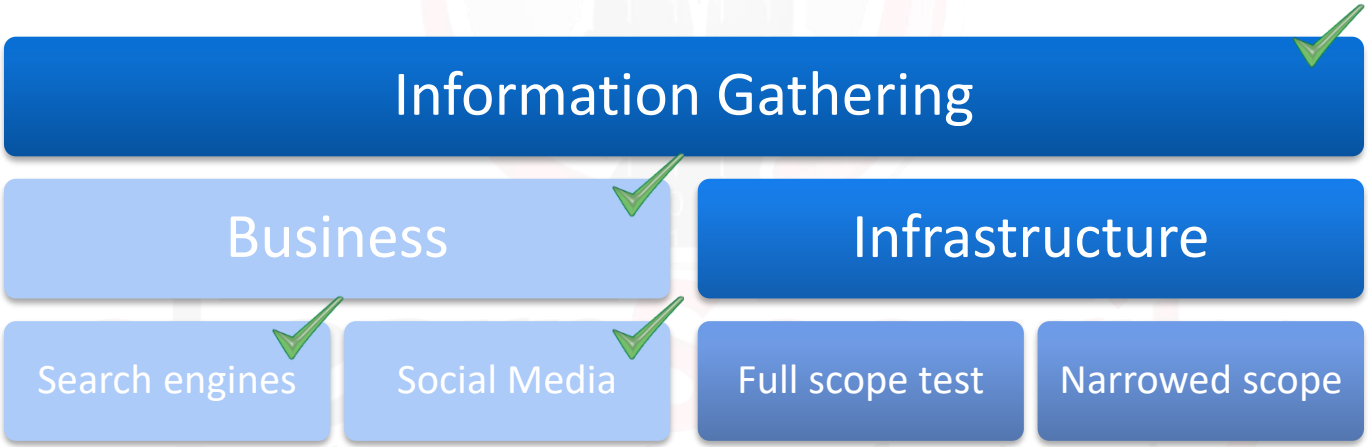
Once again, we want you to try these techniques on eLSFoo! All is theory until you apply the skills you have learned! You can try to collect and organize information such as:

- Company hierarchy
- Personal details about board of directors
  - Email addresses
  - Phone numbers
  - Addresses
  - …

At this point of our information gathering process, we have gained quite a bit of information however, we focused mainly on the organization's business and people.

We can now start gathering more technical information about infrastructure, systems, networks and so on.

The following chart sums up the tasks already performed and also outlines what we are going to see in the coming slides.



All the information gathered thus far was public and accessible by anyone. In the next section we will see techniques that need the targets' (customers) authorization.

You are not authorized to use these techniques against the organizations in the previous slides.

INFRASTRUCTURES

Having collected business information, we will now move on to collecting infrastructure details.

The main goal here is to retrieve data such as:

- Domains
- Netblocks or IP addresses
- Mail servers
- ISP's used
- Any other technical information

Keep in mind that during this process you could possibly retrieve information that is outside the scope of engagement. So, be careful! If you do not have authorization then please avoid performing further action on out of scope assets.

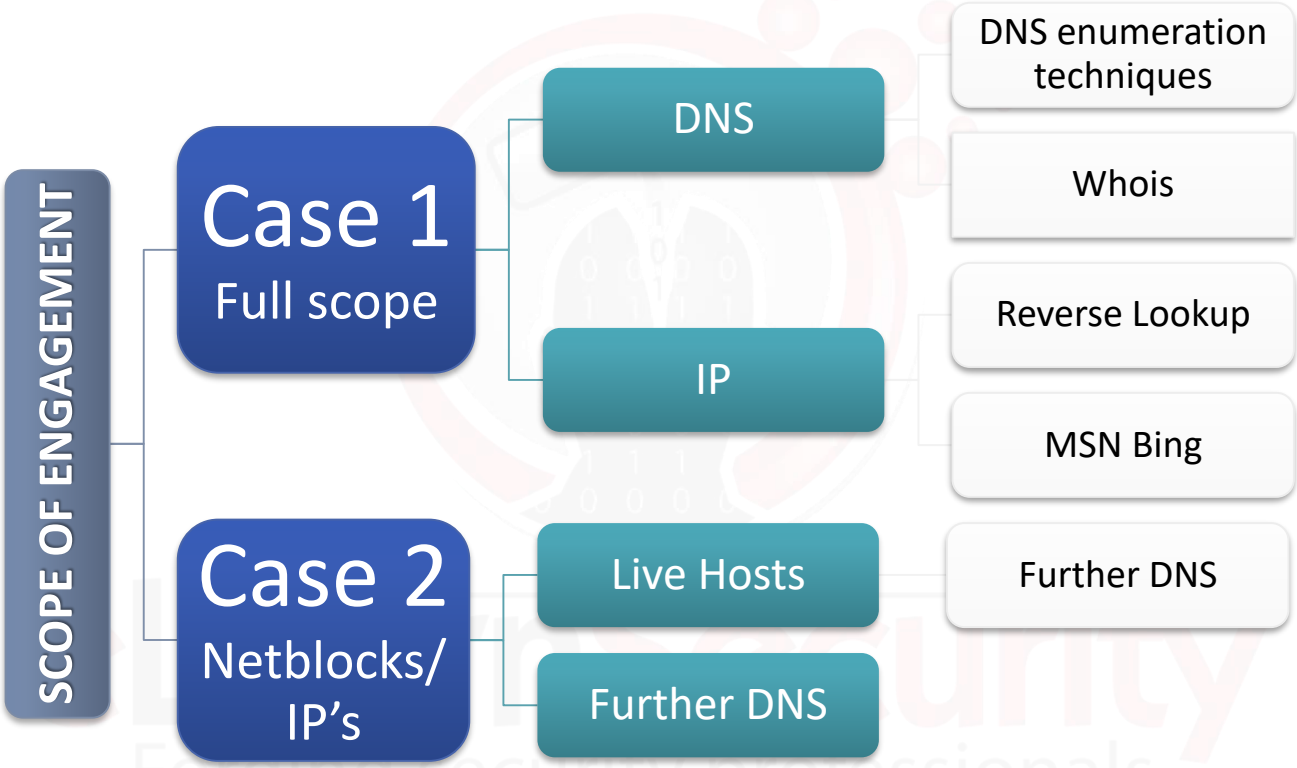
As the Scope of Engagement (SoE) for your penetration test, your customer can give you:

1. The name of the organization (full scope test)
2. IP addresses or net blocks to test

From this moment on, the approach heavily depends upon the SOE. In the following slides, we will assume the below listed cases:

- We have the name of the organization (full scope)
- We only have specific net block(s) to test.

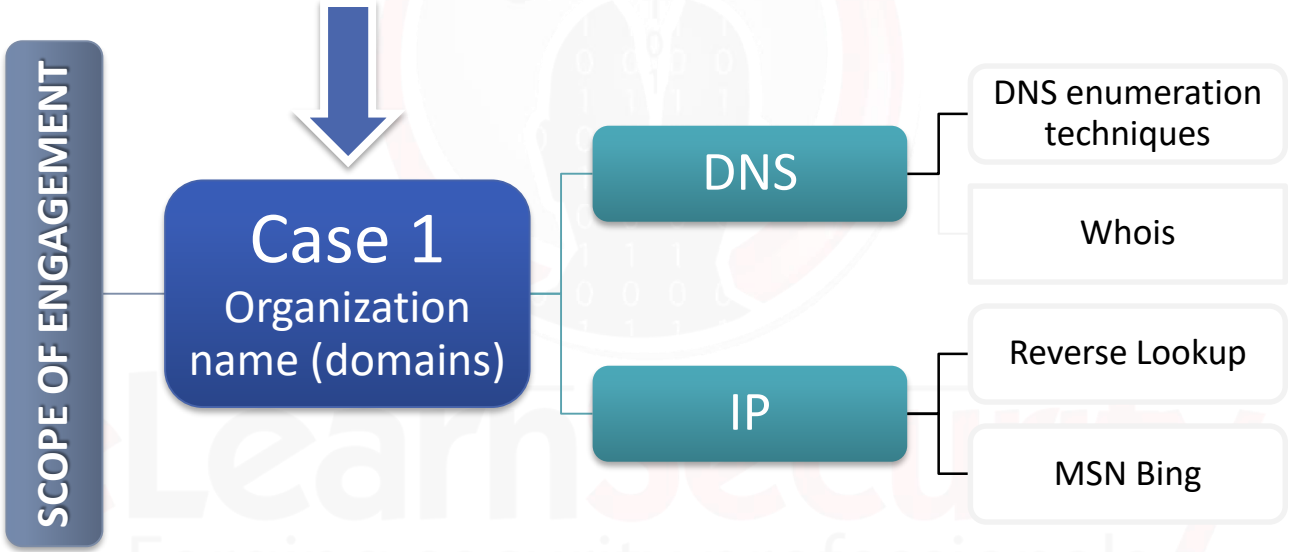
1.4. Infrastructures



Let’s first consider a full scope engagement.

In this case, your engagement is similar to how a malicious hacker would attack. Indeed the hacker only knows the target organization name at the beginning and then, he tries to derive as much information from that.

This process aims to collect all the hostnames related to the organization and the relative IP addresses.



This process ends when we obtain the following information:

- Domains
- DNS Servers in use
- Mail servers
- IP addresses

We assume at this point that you know the organization's website domain.

The first source for information, given a domain name, is WHOIS.

This is a public database and should be the first step in any investigation on infrastructure-related information.

WHOIS (pronounced "who is"; not an acronym) is a query/response protocol, widely used for querying an official domain registrar's database, in order to determine:

- The owner of a domain name
- IP address or range
- Autonomous system
- Technical contacts
- Expiration date of the domain

WHOIS lookups were traditionally made using a command line interface, but a number of simplified web-based tools now exist for looking up domain ownership details from different databases. Web-based WHOIS clients still rely on the WHOIS protocol to connect to a WHOIS server and execute lookups however, command-line WHOIS clients are still quite widely used by system administrators.

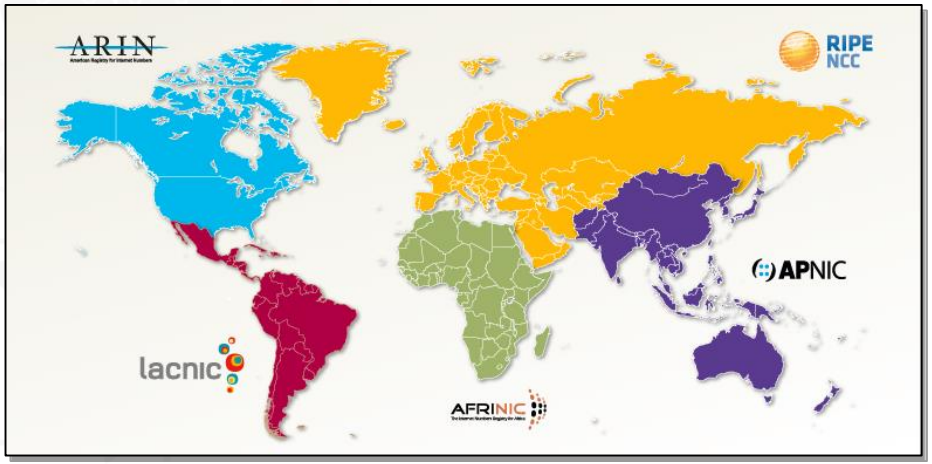
WHOIS normally runs on TCP port 43.

https://tools.ietf.org/html/rfc3912

Further Information

A Regional Internet Registry (RIR) is an organization that manages resources such as IP addresses and Autonomous Systems for a specific region. There are five main RIR provides for WHOIS information:

- AFRINIC
- APNIC
- RIPE NCC
- ARIN
- LACNIC



A wealth of information can be obtained from WHOIS searches that will kick start your investigation into the right direction:

- Number Resource Records
- Network Numbers (IP Addresses) referred to as NETs.
- Autonomous System Numbers referred to as ASNs.
- Organization records referred to as ORGs.
- Point of Contact records referred to as POCs.
- Authoritative information for Autonomous System Numbers and registered outside of the RIR being queried

Note that the RIRs are not responsible for the information within the databases they maintain.

The responsibility for the records validity belongs to the individual organizations. They have to keep their record information accurate and up to date.

Note

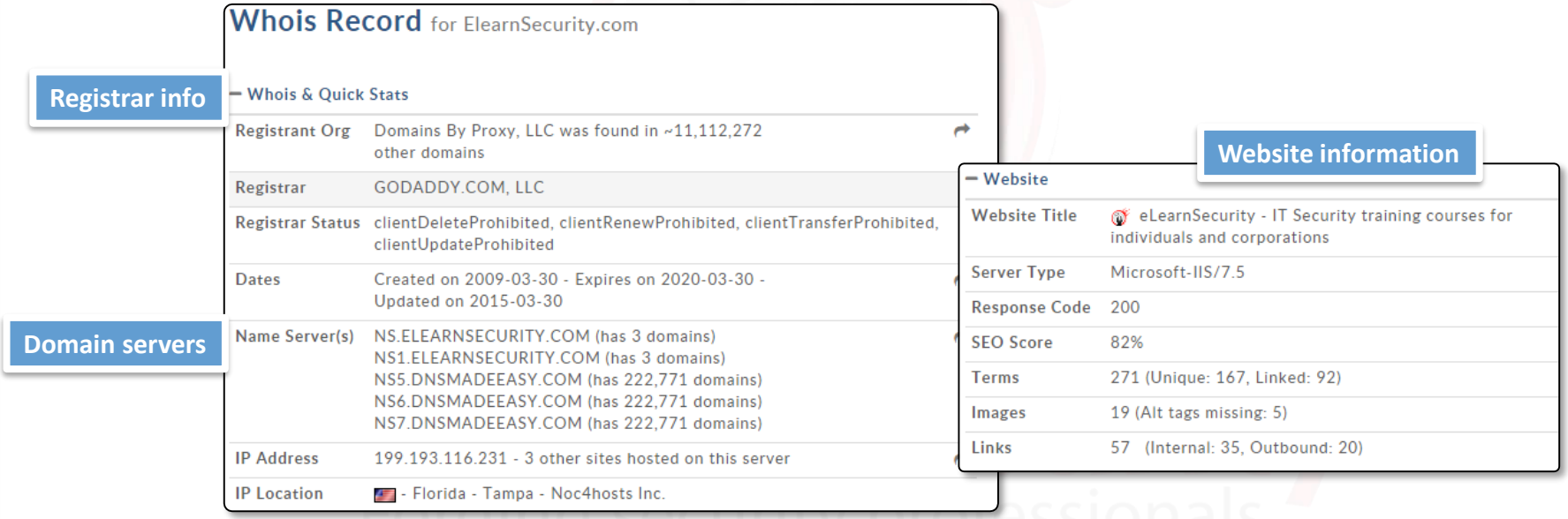
While using WHOIS databases, be sure to try different searching techniques on your target.

For example, be sure to search for just the name of the target company with no domain, then continue on to other searches leveraging different variations of domain names (i.e. target, target.com, target.net, etc.).

There are a lot of online tools that allow you to use WHOIS, such as:

- http://who.is
- http://whois.domaintools.com
- http://bgp.he.net/
- http://networking.ringofsaturn.com/Tools/whois.php
- http://www.networksolutions.com/whois/index.jsp
- http://www.betterwhois.com/

Let us see an example of the WHOIS results: (our target domain will be `elsfoo.com`)



The Domain Name System server hosted on dnsmadeeasy.com is an example of a system that would not be part of the penetration test engagement because is out of scope.

If you have a FULL or ELITE plan you can click on the image on the left to start the video

Question: what information did we get from WHOIS that can help determine the infrastructure of the organization?

Answer: Name severs!

These are servers that store all the DNS related information (records) about the domain.

Let's now move on in our investigation and start collecting information about the targets' DNS. A Domain Name System (DNS) is a distributed database arranged hierarchically. Its purpose is to provide a means to use *hostnames* (like elearnsecurity.com) rather than *IP addresses* (like 199.193.116.231).

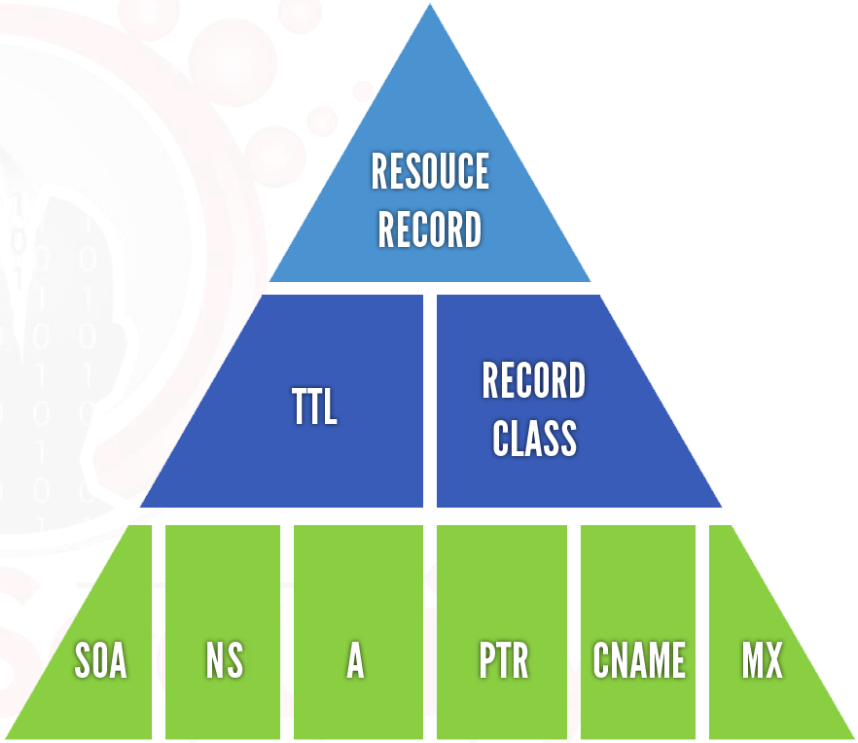
DNS is a key aspect of Information Security as it binds a hostname to an IP address and many protocols such as SSL are as safe as the DNS protocol they bind to.

DNS servers contain textual records.

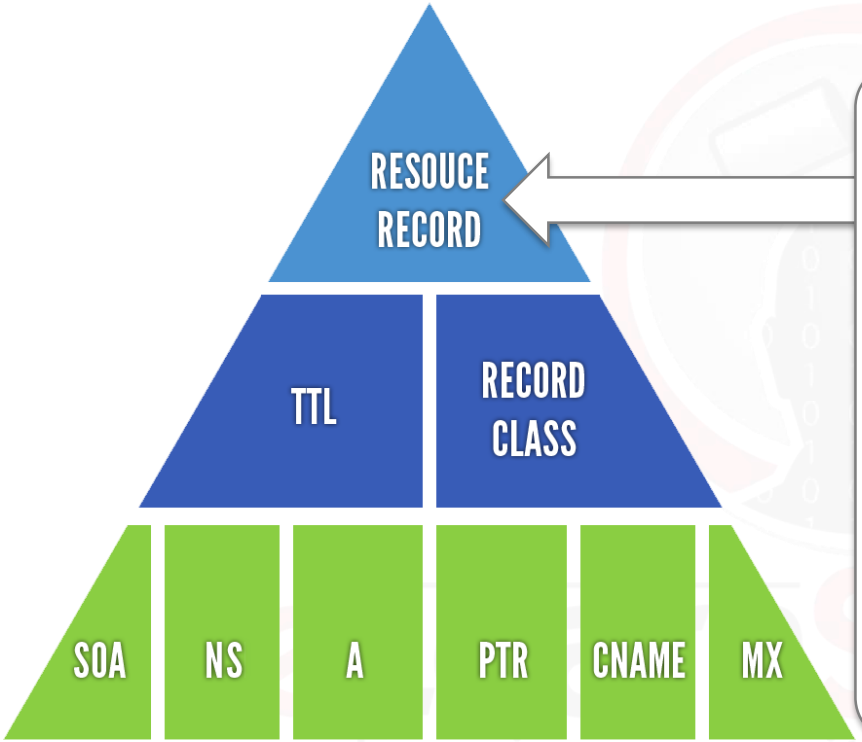
Each record has a given type, each with a different role.

DNS queries produce listings called Resource Records.

This is a representation of Resource Records.

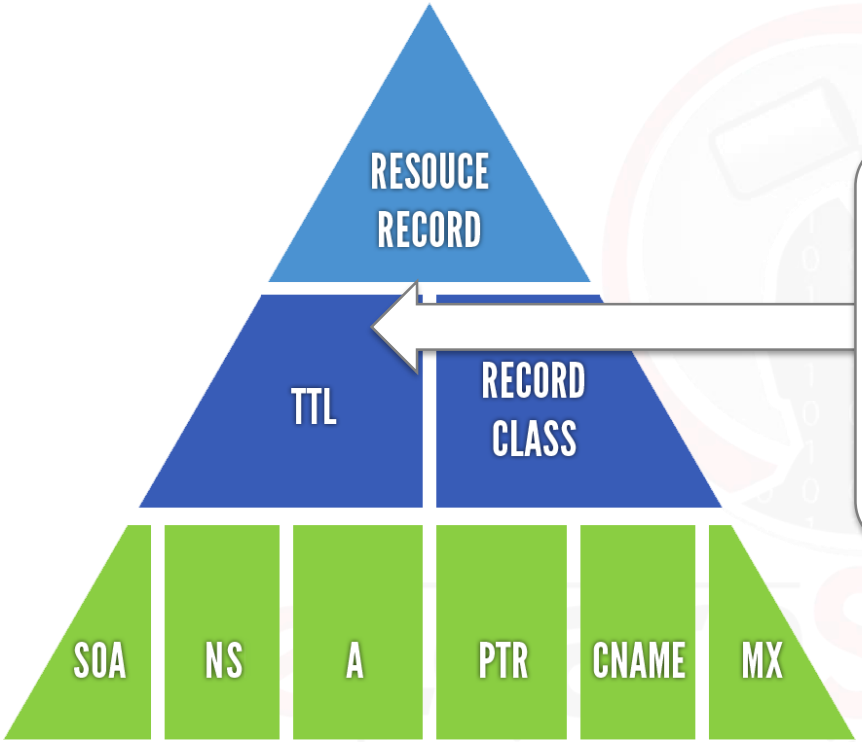


1.4.1.1.1. DNS Records



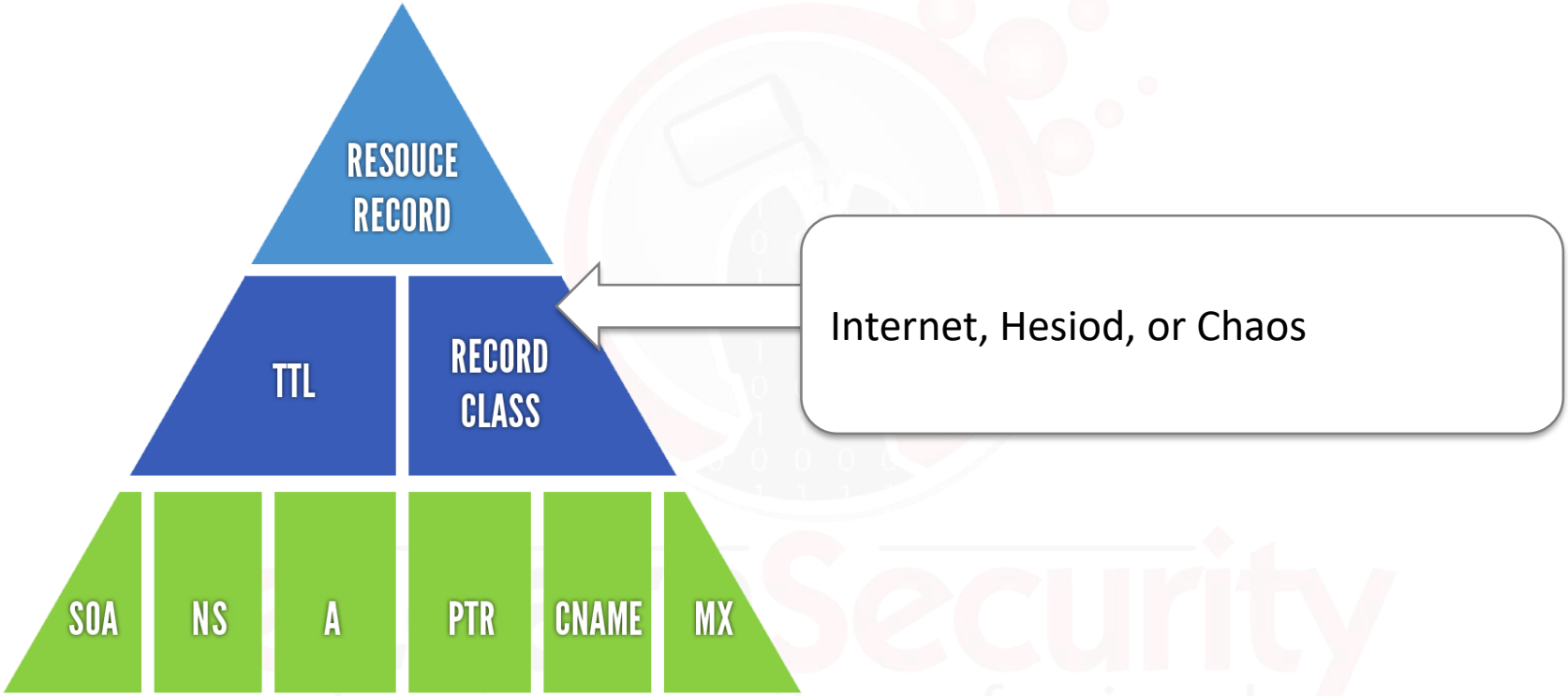
A Resource record starts with a domain name, usually a fully qualified domain name. If anything other than a fully qualified domain name is used, the name of the zone the record is in will automatically be appended to the end of the name.

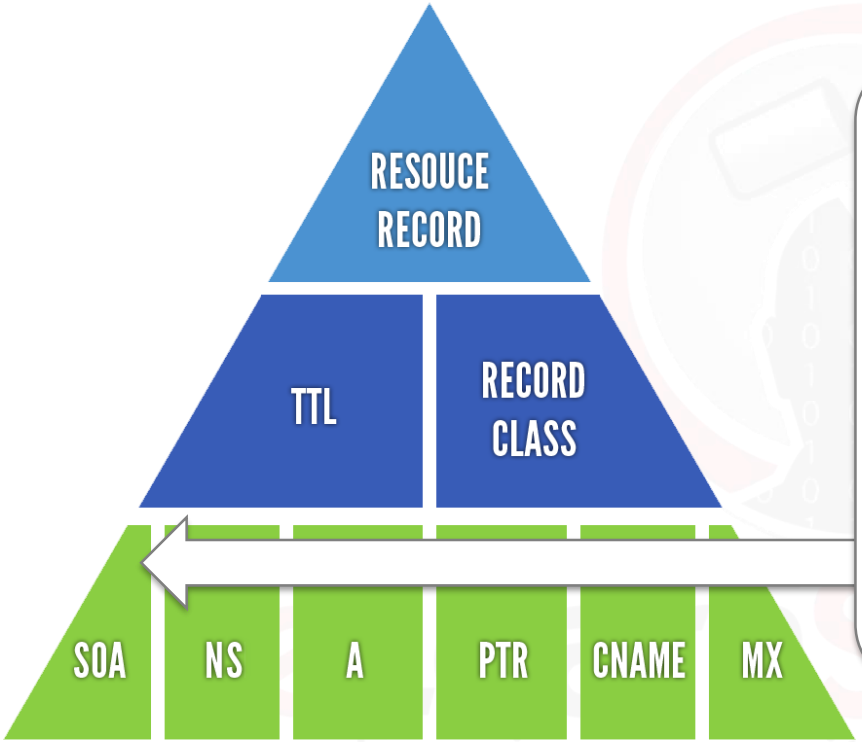
1.4.1.1.1. DNS Records



Time-To-Live (TTL), recorded in seconds, defaults to the minimum value determined in the Start of Authority (SOA) record.

1.4.1.1.1. DNS Records



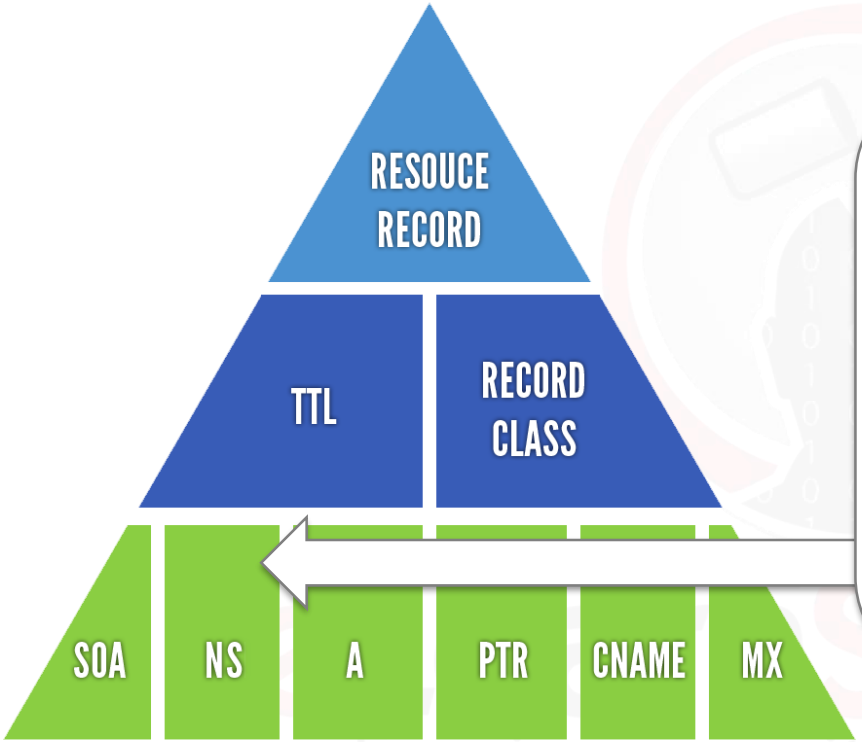


Start of Authority

Indicates the beginning of a zone and it should occur first in a zone file.

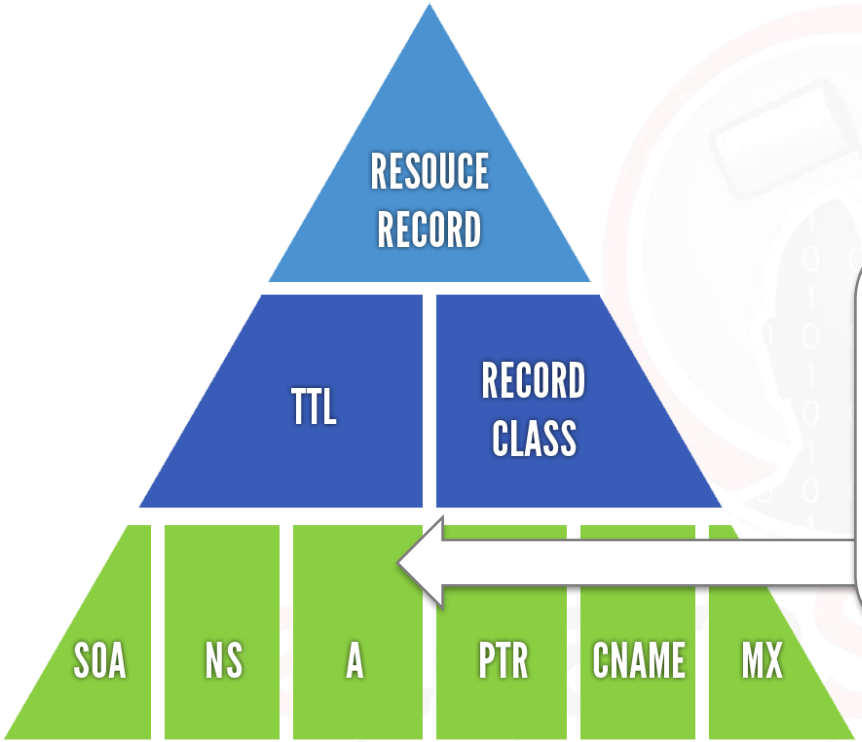
There can be only one SOA record per zone.

Defines certain values for the zone such as a serial number and various expiration timeouts



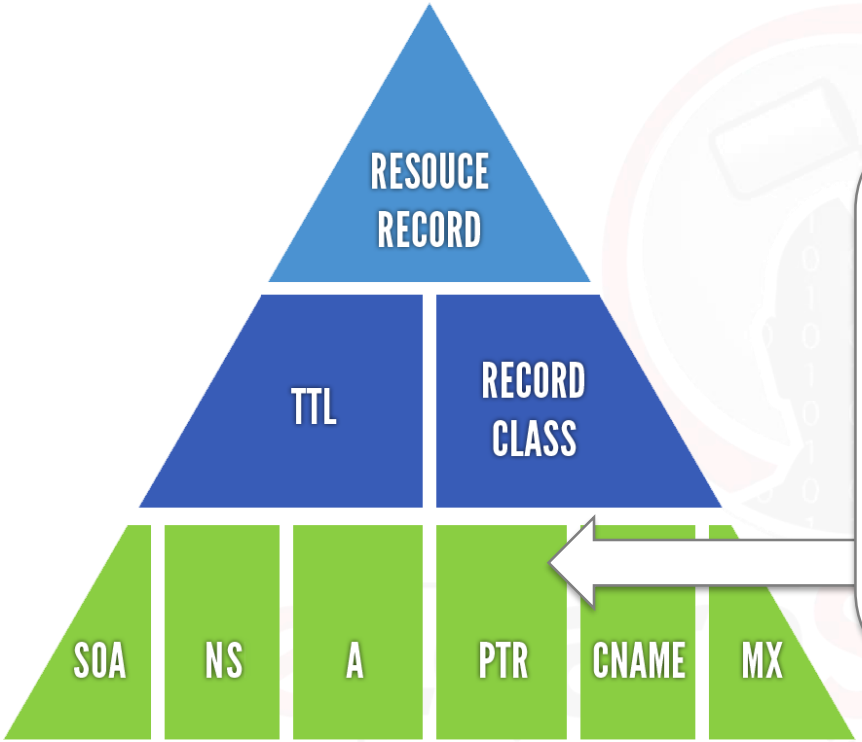
Name Server
Defines an authoritative name server for a zone.
Defines and delegates authority to a name server for a child zone.
NS Records are the GLUE that binds the distributed database together.

1.4.1.1.1. DNS Records



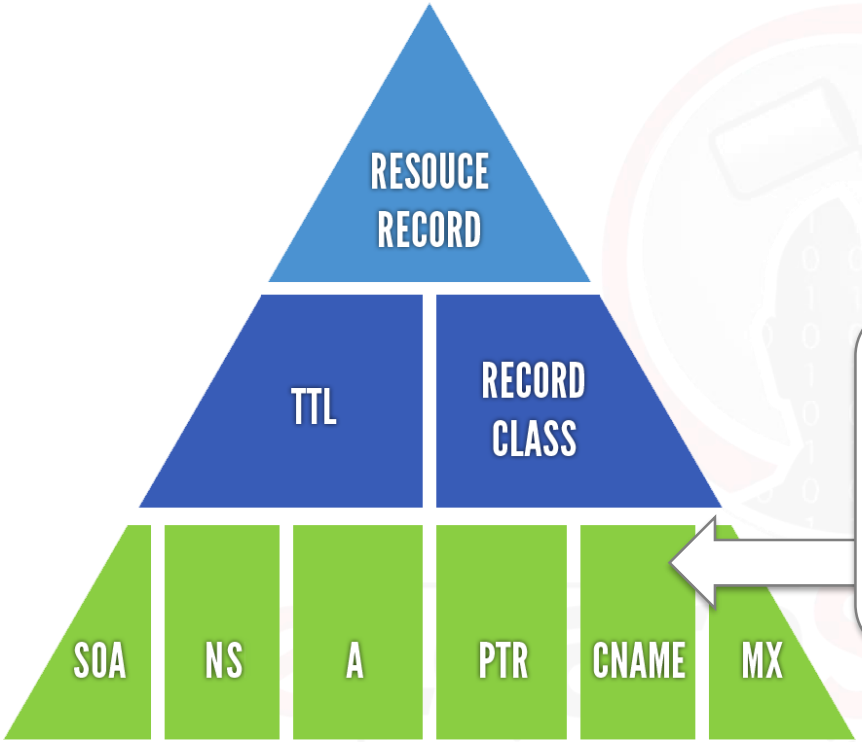
Address
The A record simply maps a hostname to an IP address. Zones with A records are called 'forward' zones.

1.4.1.1.1. DNS Records

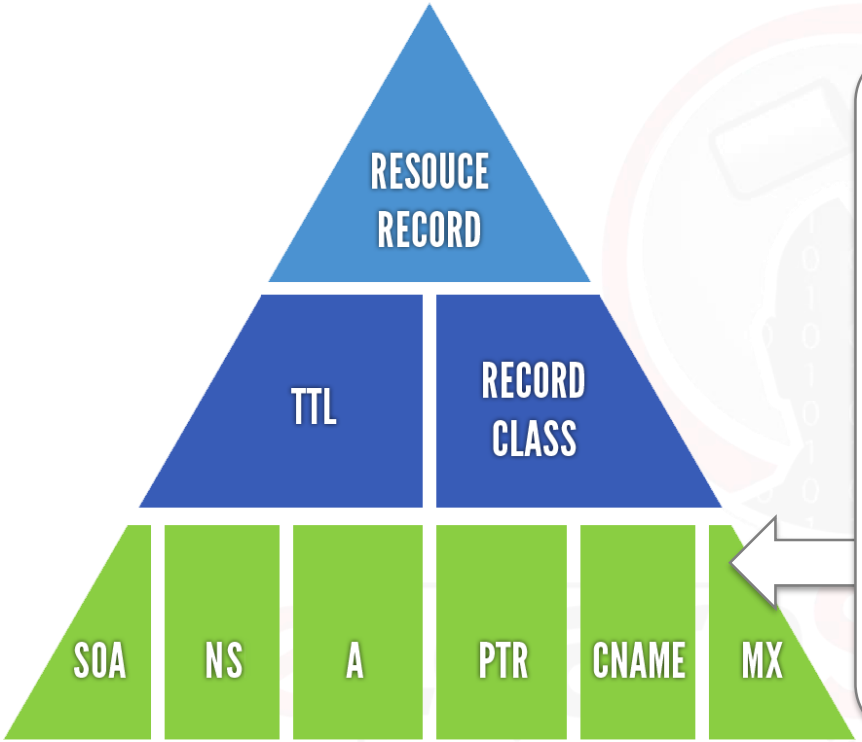


Pointer
The PTR record maps an IP address to a Hostname.
Zones with PTR records are called 'reverse' zones.

1.4.1.1.1. DNS Records



CNAME
The CNAME record maps an alias hostname to an A record hostname.



Mail Exchange

The MX record specifies a host that will accept email on behalf of a given host.

The specified host has an associated priority value

A single host may have multiple MX records.

The records for a specific host make up a prioritized list.

A DNS Lookup is the simplest query a DNS server can receive. It asks the DNS to resolve a given hostname to the corresponding IP. You can do so with `nslookup`:

```
nslookup targetorganization.com
```

In order to obtain the IP addresses of an organization, an attacker will first try to determine the hostnames and then try to resolve them.

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/cc725991(v=ws.11)

In order to collect the highest number of domains and subdomains related to the organization, we can use different techniques.

- DNS lookup
- MX lookup
- Zone transfers

With Reverse DNS lookup, we will receive the IP address associated to a given domain name. This process queries for DNS pointer records (PTR). For this task you can use *nslookup*

```
nslookup -type=PTR IPaddress
```

or online tools such as:

- http://network-tools.com/nslook/

Only domains with a PTR record set will respond to the above reverse lookup.

With the MX(Mail Exchange) lookup, we retrieve a list of servers responsible for delivering e-mails for that domain.

Once again you can use `nslookup`,

```
nslookup -type=MX domain
```

or leverage online tools such as:

- http://www.dnsqueries.com/en/
- http://www.mxtoolbox.com/

Zone transfers are usually a misconfiguration of the remote DNS server. They should be enabled only for trusted IP addresses (usually trusted downstream name servers).

When zone transfers are enabled, we can enumerate the entire DNS record for that zone.

This includes all the sub domains of our domain (A records).

How does this technique work?

In order to request the entire record, we will have to ask the server that houses this record (organization's name server).

This server can be found by executing:

```
nslookup -type=NS domain.com
```

There are usually two name servers. Take note of both of them.

You can finally issue a zone transfer request using this command:

```
nslookup
server [NAMESERVER FOR mydomain.com]
ls -d mydomain.com
```

If we are lucky, we will see a screen similar to our next slide.

1.4.1.1. DNS Enumeration


```
>nslookup
>server mydomain.com
>ls -d mydomain.com
[mydomain.com]
Mydomain.com.                                SOA          ct5154 hostmaster. (18 900 566 45874 5550)
Mydomain.com.                                A            66.200.100.84
Mydomain.com.                                NS           ns.mydomain.com
Mydomain.com.                                MX           30          aspmx2.googlemail.com
Mydomain.com.                                MX           30          aspmx3.googlemail.com
Mydomain.com.                                MX           20          alt1.aspm.l.google.com
Mydomain.com.                                MX           20          alt2.aspm.l.google.com
Mydomain.com.                                MX           10          aspmx.l.google.com
Mydomain.com.                                TXT                      “v=spf1 ip4:66.200.100.32 mx
include:aspmx.googlemail.com ~all”
Mydomain.com.                                TXT                      “google-site-
verification=omuynasdh867ajh_8djuhadn_sadi8nad_S-Q”
Admin                                        A            66.200.100.77
ns                                           A            66.200.100.54
ns1                                          A            66.200.100.44
www                                          A            66.200.100.70
mydomain.com                      SOA        ct5154 hostmaster. (18 900 566 45874 5550)
```

The command's we have seen so far were issued on a Windows machine. The *Linux nslookup* version has some limitations, therefore we suggest a more powerful tool called dig.

In the following slide we will see how to run the same command with dig.

Also something to be aware of: learn both tools, *nslookup* is universal among all the desktop operating systems therefore, having knowledge of both is important.

https://linux.die.net/man/1/dig

1.4.1.1. DNS Enumeration

+short is optional: returns minimal output

```
nslookup target.com
```

```
dig target.com +short
```

```
nslookup -type=PTR target.com
```

```
dig target.com PTR
```

```
nslookup -type=MX target.com
```

```
dig target.com MX
```

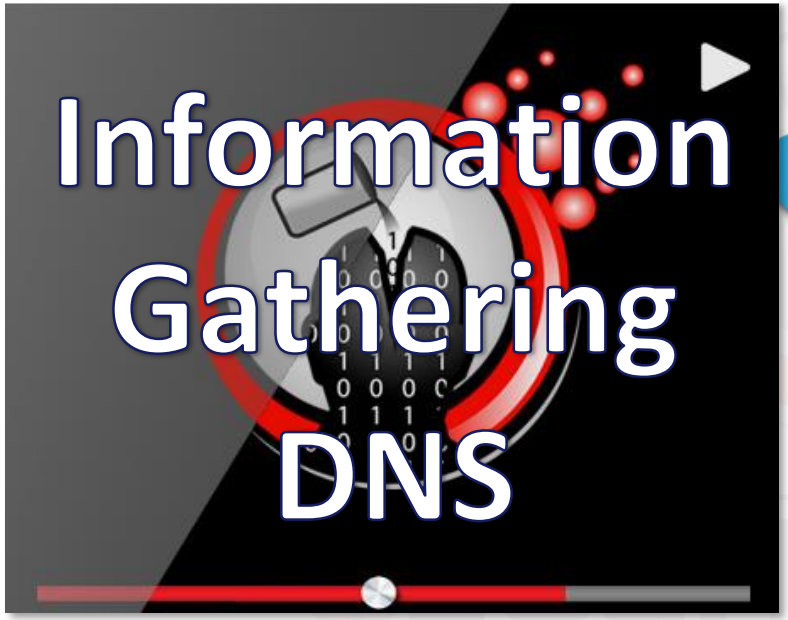
```
nslookup -type=NS target.com
```

```
dig target.com NS
```

```
nslookup
> server target.com
> ls -d target.com
```

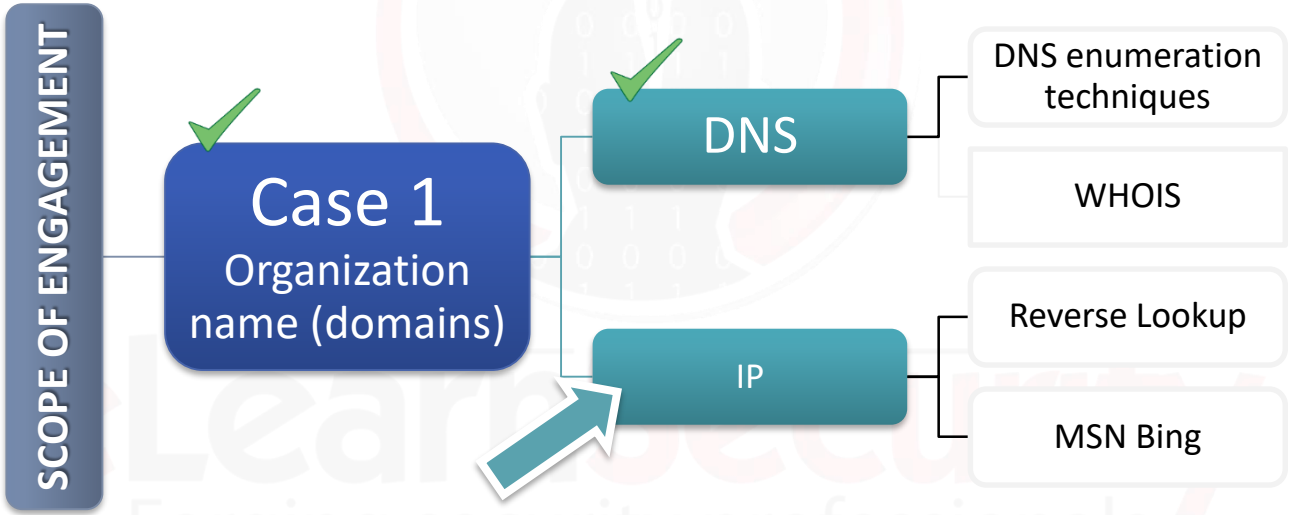
```
dig axfr @target.com target.com
```

In the next video we will see how to use these commands in order to obtain as much information as we can about our target.



If you have a FULL or ELITE plan you can click on the image on the left to start the video

Now that we know how to gather DNS information, let's move on and analyze IP addresses.



Once we have found a number of host names related to the organization, we can move on with both determining their relative IP addresses and, potentially any Netblocks associated with the organization.

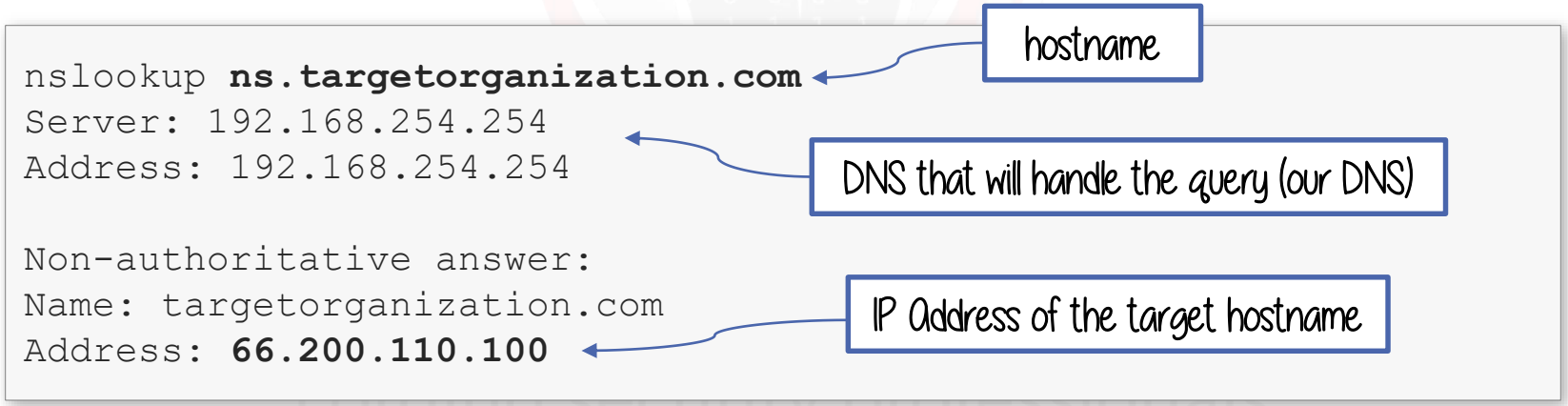
Mail servers, *Nameservers*, *Domains* and *subdomains* will all be used in this phase.

The first task we should try and tackle is to resolve all of the hostnames we have in order to determine what IP addresses are used by the organization.

Once again, `nslookup` is our friend!

The simplest use of `nslookup` is to perform a lookup of a hostname.

This translates the hostname into an IP address.



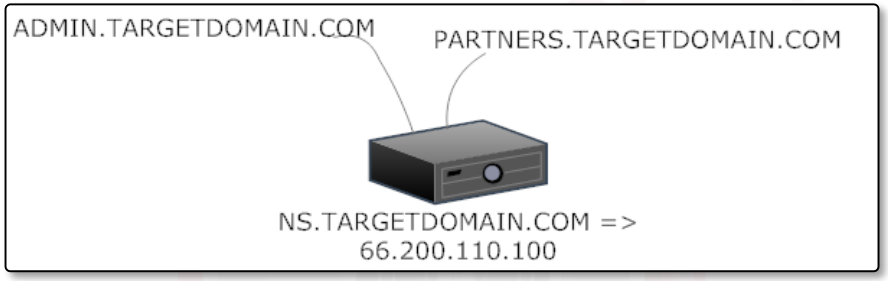
Once we retrieve one or more IP addresses corresponding to the domains, we have to consider the following:

- Is this IP address hosting only that given domain?
- Who does this IP address belong to?

It is possible that more than one domain is configured on the same IP address, even if a `PTR` record is not set.

This is a common scenario with shared hosting where hundreds of websites are configured on the same server.

This is also typical in corporate networks where multiple sub domains run on the same web server.



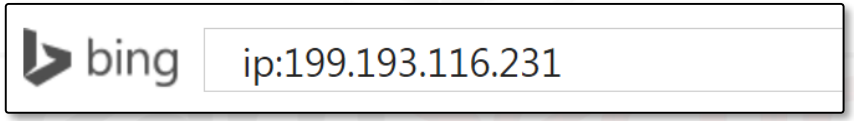
For example, you have discovered that the name server of the target organization is on 66.200.110.100. How do you determine other sub domains on the same IP?

The first technique to try is a Reverse lookup. The second is asking for either Google or Bing's help.

1.4.1.3. MSN Bing

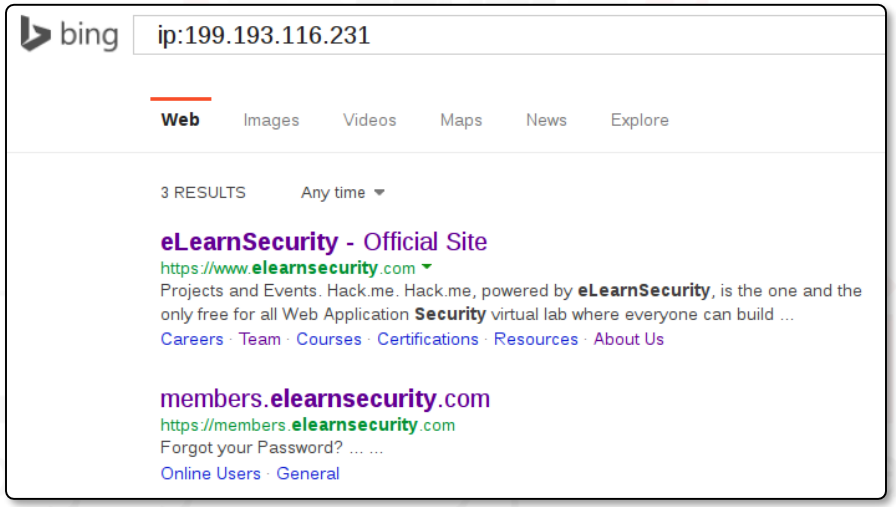
Bing offers a query filter that returns all the websites hosted on a given IP address. We just need to use the `ip` filter, followed by the IP address of our target.

```
ip:199.193.116.231
```



1.4.1.3. MSN Bing

The following is an example of the results that we can obtain. In this specific case there are two sub domains bound to the IP address specified: `www` and `members`.



1.4.1.3. MSN Bing

In addition to Bing, there are also few other online tools and web sites that allow subdomain enumeration from a specific IP address. If you suspect that the Bing results are either inaccurate or incomplete, try using one of the following tools:

- Domain-neighbors
- Domaintools
- Robtex

https://dnslytics.com/reverse-ip
http://reverseip.domaintools.com/

https://www.robtex.com/

Since we discovered new sub domains, this process might regress our steps back to the previous phases in order enumerate the data further.

Remember that this is a cyclical process of uncovering the infrastructure of the target organization. For a larger engagement, you will have to map IP addresses and related domains using mind mapping tools.

Let us go back to our investigation. Once we retrieve a list of IP addresses, the next question we should ask ourselves is:

Who is the owner?

Before visualizing how to obtain this information, let's first clarify the following:

netblocks

autonomous systems

Netblocks

A netblock is a range or set of IP addresses, usually assigned to someone and has both a starting and an ending IP address. The following is an example of netblock:

192.168.0.0 – 192.168.255.255

This network (netblock) can also be described as follows:

- 192.168.0.0/16 (CIDR notation)
- 192.168.0.0 with netmask 255.255.0.0

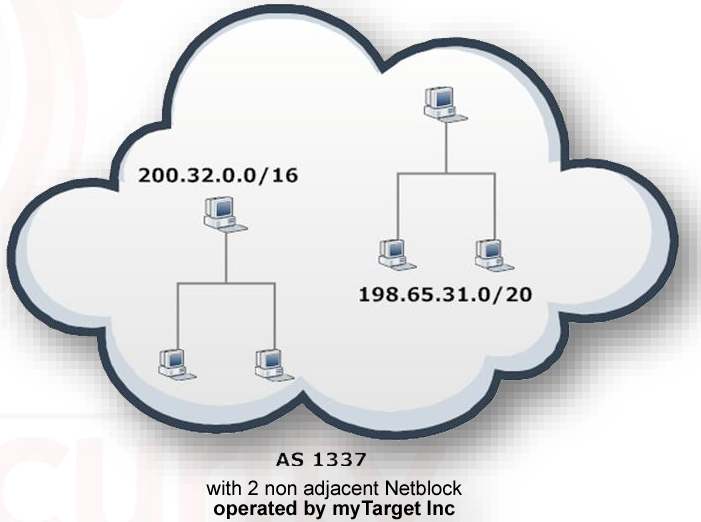
Note that larger netblocks are given to larger organizations, such as *Internet Service Providers* (ISP) and Government entities.

Individuals or small organizations usually buy one or more IP addresses from the ISP. This is why running WHOIS on these smaller netblocks, point to the ISP and not to the individual or the smaller organization leasing a sub-pool.

Autonomous System

An Autonomous System is made of one or more net blocks under the same administrative control.

Big corporations and ISP's have an autonomous system, while smaller companies will barely have a netblock.



1.4.1.4. Netblocks & AS

Let us now find out who the owner of the IP address is. We can feed *whois.arin.net* (or one of the WHOIS tools seen earlier) with the IP address of our target.

Network	
NetRange	66.200.96.0 - 66.200.111.255
CIDR	66.200.96.0/20
Name	SOLAR-VPS
Handle	NET-66-200-96-0-1
Parent	NET66 (NET-66-0-0-0-0)
Net Type	Direct Allocation
Origin AS	
Organization	Solar VPS (SVL-7)
Registration Date	2007-06-25
Last Updated	2007-06-25
Comments	
RESTful Link	http://whois.arin.net/rest/net/NET-66-200-96-0-1

NETBLOCK

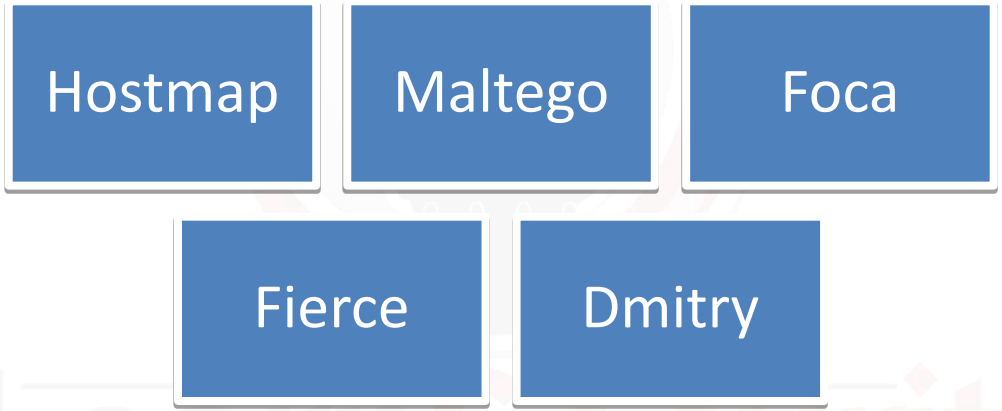
OWNER

Function	Point of Contact
Tech	RMB34-ARIN (RMB34-ARIN)
Abuse	RMB34-ARIN (RMB34-ARIN)
NOC	RMB34-ARIN (RMB34-ARIN)

As you can tell from the previous slide, the owner of the netblock is *Solar VPS*. A further investigation into *Solar VPS* will tell us that it is a hosting provider leasing the IP address to our target organization.

We must understand that adjacent IP addresses might not be owned by our organization, as it does not own the entire netblock.

Note that you can use tools that automatically perform these operations:



Some of these tools will be shown later.

So far we have seen how to get information on the target organization by simply knowing its name. Let us instead see the tasks needed to be performed if the contract with your client indicates specific IP addresses or net blocks.

Of course, this makes the process easier as you can skip the uncovering net blocks.

1.4.2. Netblocks – IP's

We already have a list of IP addresses.

The first step is to identify which of those are alive.

Case 2
Netblocks/IP's

Once we have our pool of IP addresses, we have to identify the devices and the role(s) played by each IP in the target organization. Is it a server or a workstation?

In this early phase we do not want to enumerate the services. This will be subject of next stages. We want to determine which IP's are alive.

We can:

1. Determine hosts (IP) that are alive
2. Determine if they have an associated host name/domain

As you can see, by uncovering additional domains and host names associated to these IP addresses, we will gather additional information and apply the information gathering techniques on both host names and domains that we have already studied.

1.4.2.1. Live Hosts

There are different methods that one can use to identify live hosts. The most common is the ICMP ping sweep. It consists of *ICMP ECHO requests* sent to multiple hosts. If a given host is alive, it will return an *ICMP ECHO reply*.

Many tools allow us to perform a ICMP ping sweep. The following are just a few of them.

- fping
- nmap
- hping

fping

Let us briefly introduce these tools. If you do not have fping already installed on your machine, you can download it here.

You can perform a simple scan with the following command:

```
fping -a -g 192.168.1.0/24
```

where `-a` shows systems that are alive and `-g` generate a target list from a supplied IP netmask or a starting and ending IP address.

http://fping.org/

Nmap

Another tool that you can use is Nmap. You can download it at the following address: http://nmap.org/.

Nmap is the most popular scanning tool. It allows users the ability to perform very sophisticated scans with very good results. For now though, we will only deal with its sweeping capabilities.

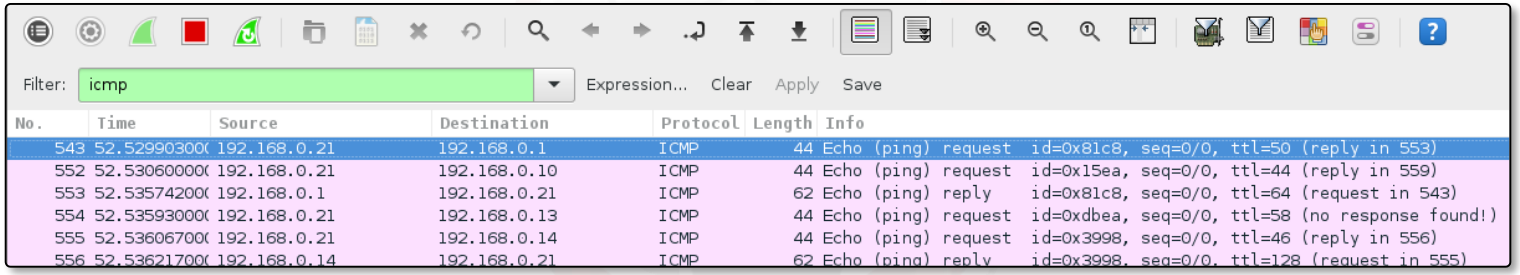
In order to perform a host discovery scan, we can use many different techniques however, the most common option is:

```
nmap -sn 10.0.0.0/24
```

The `-sn` option, also known as ping scan / ping sweep, tells Nmap not to run a port scan on the remote hosts, but instead return only the hosts that respond to the probes sent.

You will learn more about it in the next video.

The following picture shows the ICMP requests under the hood while using Nmap.

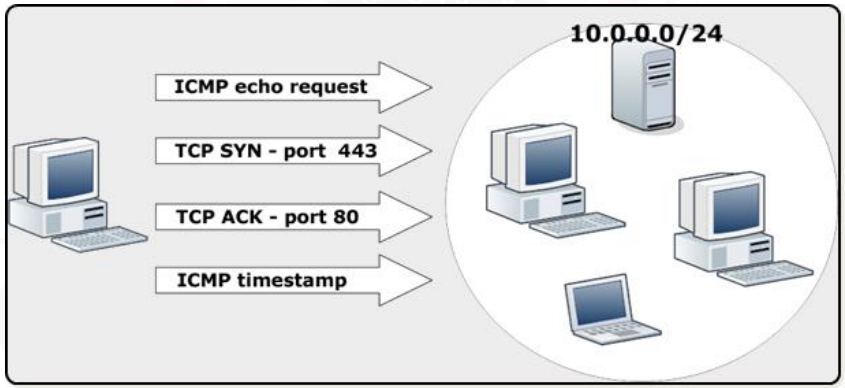


Notice that if you run the scan from a machine within the same network, Nmap runs an *ARP scan* instead of sending *ICMP packets*. To avoid this behavior, you can use the `--disable-arp-ping` or `--send-ip` option.

Nowadays though, ICMP is often disabled on perimeter routers and firewalls, and even on latest Windows clients (via Windows Firewall).

ICMP scans are then no longer reliable in determining whether a host is alive or not.

There are other kinds of techniques that Nmap uses to detect live hosts. Indeed the default host discovery achieved with `-sn` command consists of more than just a simple ICMP echo request:



For a complete list of commands, see the reference manual at this link:

- http://nmap.org/book/man-host-discovery.html

Nmap will be covered in deeper details in the next modules. For now, we are just scratching the surface of this great tool and trying to remain in context of the sections. In the next video we will see both some basic techniques and tools that we can use to discover alive hosts.

If you have a FULL or ELITE plan you can click on the image on the left to start the video

1.4.2.2. Further DNS

Now that we know how to discover live hosts, let us investigate more and see how we can find further DNS within the target network

This step deals with using Nmap to enumerate all the DNS servers that exist in the remote network.

As you probably noticed, these are steps that you could perform more than once. This happens because each time we find a new domain or a new IP, it could give us other useful information to aid us in further investigations.

Remember, this is a cyclical process.

1.4.2.2. Further DNS

In order to determine if DNS servers are in place in a given netblock, we should first know something more about DNS. A DNS server runs on:

- TCP port 53
- UDP port 53

We can increase our surface by using Nmap to scan the entire network and find hosts that have these ports open. To do this, we can use the following two commands:

```
nmap -sS -p53 [NETBLOCK]
```

```
nmap -sU -p53 [NETBLOCK]
```

The first can be used to run a TCP scan, while the second can be used to run an UDP scan.

Once we retrieve more DNS servers, we can perform a reverse lookup to find out if they are serving any particular domain.

Moreover, we can try zone transfer techniques on them as well as any of the techniques studied before.

Before the end of the chapter, we would like you to become familiar with Maltego. Maltego bills itself as a source intelligence and forensics application.

It is very unique among the tools available today.

https://www.paterva.com/web7/

Maltego uses what it calls transformations to discover information about specific targets.

For instance you can begin with a server address and enumerate various information regarding that server, then build on that information until you have a full map of the entities entire internet presence.

In the next video we will see some use cases that will show you the power that Maltego will bring to your engagements.

Note

The community version of the tool (free to use) will work just fine for our purposes. In order to obtain and use Maltego, you will have to register on their website.

If you have a FULL or ELITE plan you can click on the image on the left to start the video

Tools

We will now leverage the power of automation to make our investigation techniques faster and even more reliable through the use of tools.

Notice that there is a large amount of tools that you can use in this phase however, the ones we are going to see in the next slides are the most used. We do encourage you to use other tools as well.

The following is a small list of the most common tools that you can use in this phase. We are not going to unpack them all but we encourage you to use them and test each one.

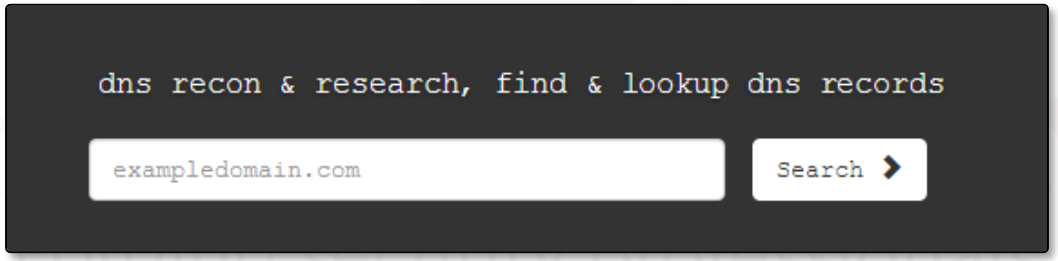
DNSdumpster | DNSEnum | Fierce | Dnsmap | Metagoofil

Foca | Maltego | Dmitry | Recon-ng

1.5.1. DNSdumpster

In the previous slides we have seen many different online tools useful to gather information on our target domain. DNSdumpster is a free domain research tool that can discovered hosts related to a specific domain.

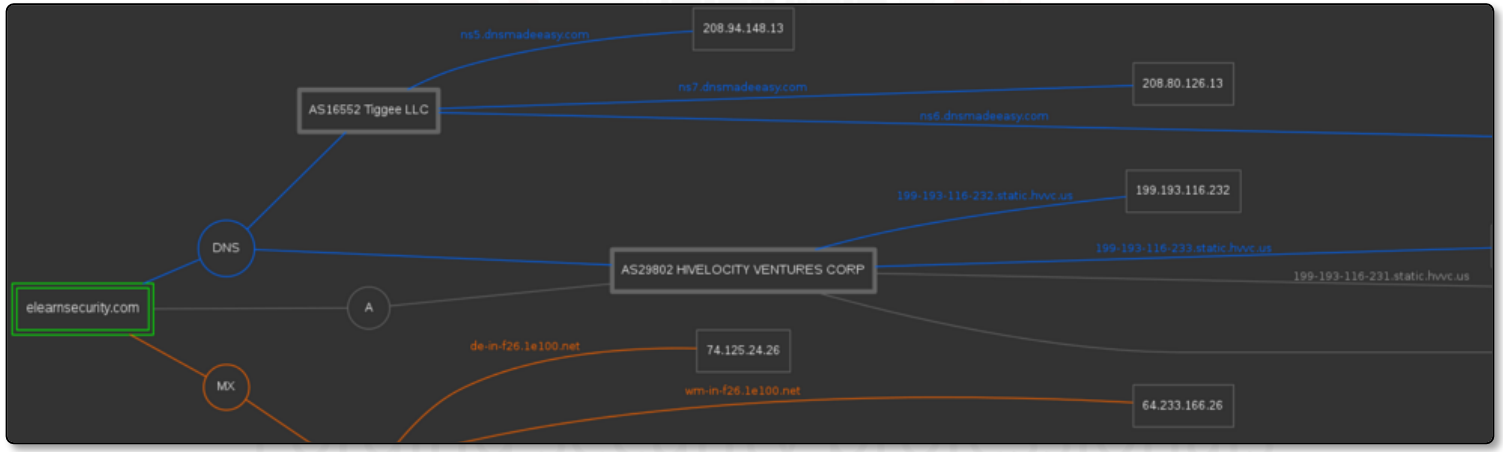
It is straightforward to use: you just need to type the target domain and it will return all the results.



https://dnsdumpster.com/

1.5.1. DNSdumpster

As you will see, it gives us additional information such as: the hosting behind the target domain, the location of the servers, the DNS records (MX, A, etc.) and it also creates a map with all the information obtained.



1.5.1. DNSdumpster

This is a very good tool to start our investigation. Moreover, remember that this tools is not intrusive.

Host Records (A) ** this data may not be current as it uses a static database (updated monthly)

blog.elearnsecurity.com	162.220.56.82 162-220-56-82.static.hvvc.us	AS29802 HIVELOCITY VENTURES CORP United States
elearnsecurity.com	199.193.116.231 199-193-116-231.static.hvvc.us	AS29802 HIVELOCITY VENTURES CORP United States
members.elearnsecurity.com	199.193.116.231 199-193-116-231.static.hvvc.us	AS29802 HIVELOCITY VENTURES CORP United States
www.elearnsecurity.com	199.193.116.231 199-193-116-231.static.hvvc.us	AS29802 HIVELOCITY VENTURES CORP United States

The purpose of DNSEnum is to gather as much information as possible about a domain. The tool can be downloaded from the following address:

- https://github.com/fwaeytens/dnsenum

The program currently performs the following operations:

- Get the host's addresses (A record)
- Get the name servers (threaded)
- Get the MX record (threaded)
- Perform AXFR queries on name servers (threaded)

1.5.2. DNSEnum

- Get extra names and sub domains via Google dorks (`allinurl:-www site:domain`)
- Brute force sub domains from file, can also perform recursion on sub domain that have NS records (all threaded)
- Calculate C class domain network ranges and perform WHOIS queries on them (threaded)
- Perform reverse lookups on net ranges (C class or/and WHOIS net ranges) (threaded)

Usage for the tool is :

```
dnsenum.pl [options] <domain>
```

Options include the following:

--private	Show and save private IPs at the end of the file domain_ips.txt.
--subfile <file>	Write all valid subdomains to this file.
--threads <value>	The number of threads that will perform different queries.
-p, --pages <value>	-p, --pages <value> The number of Google search pages to process when scraping names, the default is 20 pages, the -s switch must be specified.
-s, --scrap <value>	The maximum number of subdomains that will be scraped from Google.
-f, --file <file>	Read subdomains from this file to perform brute force.

Let us see now how to run *dnsenum* against *elsfoo.com*. The command will be similar to the following:

```
dnsenum elsfoo.com
```

```
-----   elsfoo.com   -----


Host's addresses:
__________________

elsfoo.com.                              5


Name Servers:
______________

ns6.dnsmadeeasy.com.                     5
ns7.dnsmadeeasy.com.                     5
```

```
Mail (MX) Servers:
___________________

aspmx3.googlemail.com.                   5          IN
aspmx.l.google.com.                      5          IN
alt1.aspmx.l.google.com.                 5          IN
alt2.aspmx.l.google.com.                 5          IN
aspmx2.googlemail.com.                   5          IN


Trying Zone Transfers and getting Bind Versions:
_________________________________________________


Trying Zone Transfer for elsfoo.com on ns6.dnsmadeeasy
```

We can see the tool focuses on different sections:

1. In the host address section it performed a reverse lookup on the domain.
2. The tool determined the Name Servers used by the domain.
3. The tool searches for any MX records for the domain.
4. Lastly, it tried zone transfers to see if it could enumerate any sub domains.

It is also important to know that `dnsenum` comes with a wordlist file containing the most common DNS and sub domain names. This will be useful in running brute force attacks.

You can find the file in the main folder of the tool. In our case it is located in `/usr/share/dnsenum`.

Let’s now try a more complex execution of the tool using the following command:

```
dnsenum --subfile elsfoosubs.txt -v
-f /usr/share/dnsenum/dns.txt
-u a -r elsfoo.com
```

With this command, we can store the sub domains obtained in the *elsfoosubs.txt*.

We are going to receive verbose output with the `-v` option, and subsequently, we are going to use the `dns.txt` file to do the brute force of sub domains using the `-f` option.

We are also using the `-u` a option to update any file that may already exist and performing a recursive brute force on any discovered domains with the `-r` option.

From this test, we see the results change towards the end where the brute force occurs. We can see when the brute force attempts fail or succeed based upon the status provided. If the brute force is successful, we see the pertinent information returned instead of the "*A record query failed: NXDOMAIN*" status.

```
zensus2011.elsfoo.com A record query failed: NXDOMAIN
zfa.elsfoo.com A record query failed: NXDOMAIN
zilverfonds.elsfoo.com A record query failed: NXDOMAIN
zoek.elsfoo.com A record query failed: NXDOMAIN
_sip.elsfoo.com A record query failed: NXDOMAIN
_spf.elsfoo.com A record query failed: NXDOMAIN
_tls.elsfoo.com A record query failed: NXDOMAIN
```

Although it is a very old tool, dnsmap still works great when it comes to sub domain enumeration and brute forcing. You can download it from github.

https://github.com/makefu/dnsmap

Dnsmap uses the primary domain that we provide as a target and then brute forces all the sub domains by using:

- a dictionary file that comes with the tool
- a word list file that the user makes.

There are many different word lists that you can find online: a simple google search returns a huge amount of resources.

https://www.google.com/search?q=subdomain+wordlists&cad=h

Let us see a basic example of how to use *dnsmap*. In this case we are going to use the default wordlist that comes with the tool:

```
dnsmap elsfoo.com
```

```
dnsmap 0.30 - DNS Network Mapper by pagvac (gnucitizen.org)

[+] searching (sub)domains for elsfoo.com using built-in wordlist
[+] using maximum random delay of 10 millisecond(s) between requests

admin.elsfoo.com
IP address #1: 209.133.210.155

intranet.elsfoo.com
IP address #1: 209.133.210.155

ns1.elsfoo.com
IP address #1: 209.133.210.155

private.elsfoo.com
IP address #1: 209.133.210.155
```

The following is a short list of options that can be used:

- `$ dnsmap targetdomain.foo`
  - Example of sub domain brute forcing using dnsmap's built-in word-list
- `$ dnsmap targetdomain.foo -w wordlist.txt`
  - Example of sub domain brute forcing using a user-supplied wordlist
- `$ dnsmap targetdomain.foo -r /tmp/`
  - Example of sub domain brute forcing using the built-in wordlist and saving the results to /tmp/
- `$ dnsmap-bulk.sh domains.txt /tmp/results`
  - For brute forcing a list of target domains in a bulk fashion use the bash script provided.

As you can see from the results, as more tools are executed, our results keep growing.

Again, it is very important to be very meticulous about saving information from the tools for use in the later phases. This will ensure a complete and thorough test.

In the previous slides, we have seen some tools that can help us gather information starting with a simple domain name.

In the next video we will see the tool called FOCA. We introduced it in the early phase of our information gathering, when we talked about harvesting and metadata. As you will see, *FOCA* allows us to mine a ton of information about the target infrastructure. This occurs by analyzing data extracted from an online document.

https://www.elevenpaths.com/labstools/foca/index.html

Video: FOCA and Shodan

If you have a FULL or ELITE plan you can click on the image on the left to start the video

We are at the end of this long process called Information Gathering. Once again, we give you the chance to try all the techniques you have learned on a real target: *elsfoo.com*.

REFERENCES

References

FreeMind

http://freemind.sourceforge.net/wiki/index.php/Main_Page

Dradis

https://dradisframework.com/ce/

Methodology: Handling Information

https://members.elearnsecurity.com/course/resources/name/ptp_v5_section_2_module_1_attachment_eLearnSecurity_Handling_Information

Google Operators #2

http://www.googleguide.com/advanced_operators_reference.html

Xmind

https://www.xmind.net/

Magictree

http://www.gremwell.com/what_is_magictree

Google Operators #1

https://support.google.com/websearch/answer/2466433?hl=en&ref_topic=3081620&visit_id=0-636620933356181961-1111523074&rd=1

Google Operators #3

http://pdf.textfiles.com/security/googlehackers.pdf

Google Operators #4

http://www.mrjoeyjohnson.com/Google.Hacking.Filters.pdf

Edgar

https://www.sec.gov/edgar.shtml

TheHarvester

https://github.com/laramies/theHarvester

Archive

https://archive.org/

WHOIS

https://tools.ietf.org/html/rfc3912

Online WHOIS #1

https://who.is/

Online WHOIS #2

http://whois.domaintools.com/

Online WHOIS #3

https://bgp.he.net/

References

Nslookup

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/cc725991(v=ws.11)

Nslookup Online

https://network-tools.com/nslook/

DNSqueries

https://www.dnsqueries.com/en/

MXToolBox

https://mxtoolbox.com/

Dig

https://linux.die.net/man/1/dig

Domain-neighbors

https://dnslytics.com/reverse-ip

Domaintools

http://reverseip.domaintools.com/

Robtex

https://www.robtex.com/

References

Fping

http://fping.org/

Nmap

https://nmap.org/

Maltego

https://www.paterva.com/web7/

DNSDumpster

https://dnsdumpster.com/

DNSenum

https://github.com/fwaeytens/dnsenum

Dnsmap

https://github.com/makefu/dnsmap

Foca

https://www.elevenpaths.com/labstools/foca/index.html

WHOIS Lookup

Information Gathering
DNS

Host Discovery with
Fping, Hping3 and
Nmap

Maltego

FOCA and Shodan

Information Gathering

eLearnSecurity has created eLSFoo, a fictitious company located at www.elsfoo.com.