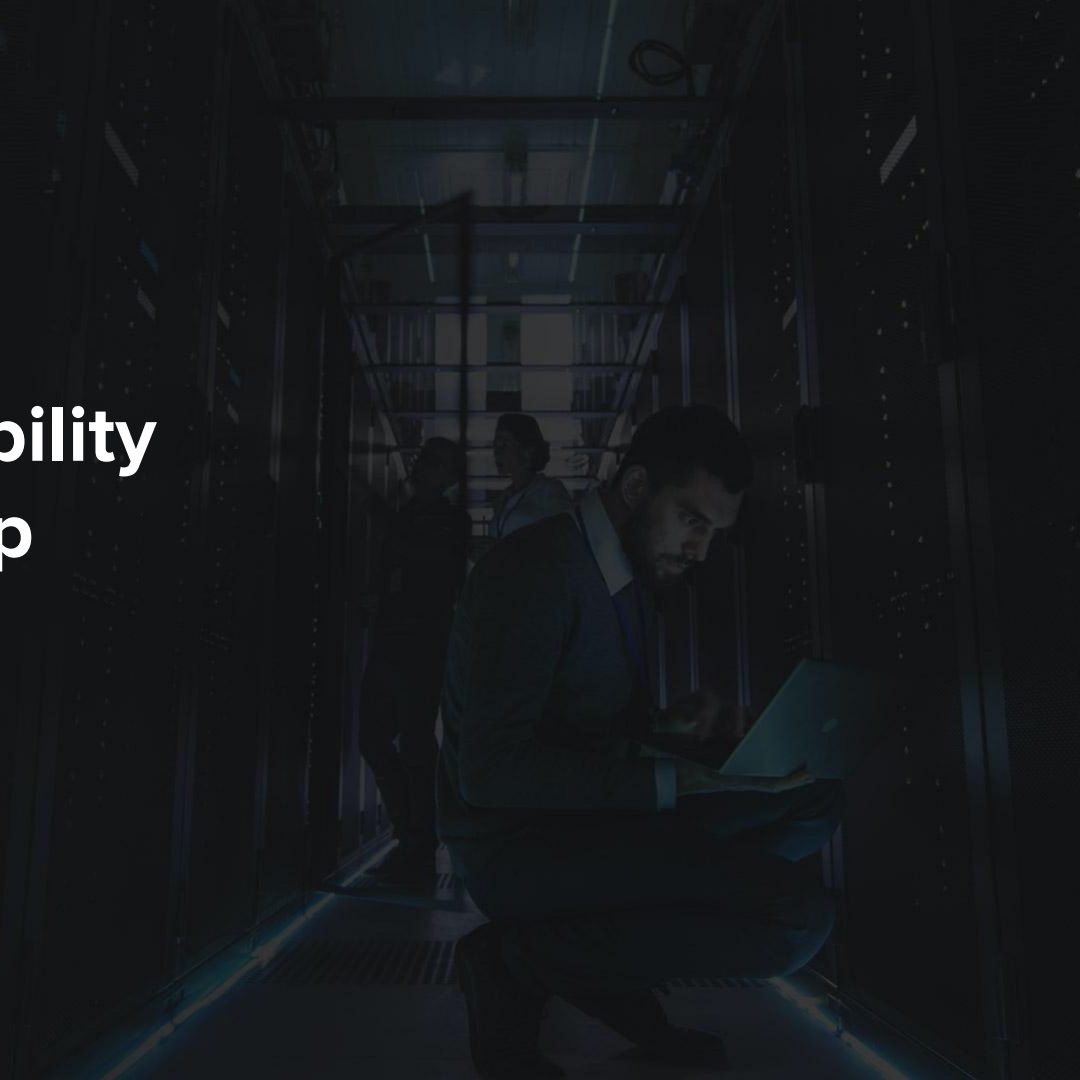




Recon and Vulnerability Detection Bootcamp

Instructor Intro and Agenda

ine.com



Instructor Introduction

- + **Phillip Wylie, CISSP, OSCP, GWAPT**
- + **INE Offensive Cyber Security Instructor**
- + Offensive Cyber Security Professional with over 23 years of experience in cybersecurity and information technology.
- + 9 years offensive security
- + Co-author of The Pentester Blueprint: Starting a Career as an Ethical Hacker

Agenda

- + Day 1: Passive Reconnaissance
- + Pentesting Methodology Overview
- + Information Gathering
- + Web Presence
- + Information Gathering Exercises

Agenda

- + Day 2: Active Reconnaissance
 - + Infrastructure
 - + DNS Enumeration and IP Enumeration
 - + Identifying Live Hosts
 - + Netblocks and Autonomous Systems
 - + Active Reconnaissance Exercises

Agenda

- + Day 3: Footprinting, Scanning, and Vulnerability Analysis
- + Mapping a Network
- + Port Scanning
- + Vulnerability Scanning
- + Footprinting, Scanning, and Vulnerability Analysis Exercises



Kali Linux VM Setup

ine.com



Kali Linux VM Setup

- + Requirements
- + VirtualBox or VMware
- + Kali Linux VM

<https://phoenixnap.com/kb/how-to-install-kali-linux-on-virtualbox>

Phillip Wylie

Offensive Cyber Security Expert



pwylie@ine.com



[@PhillipWylie](https://twitter.com/PhillipWylie)



<https://www.linkedin.com/in/phillipwylie/>

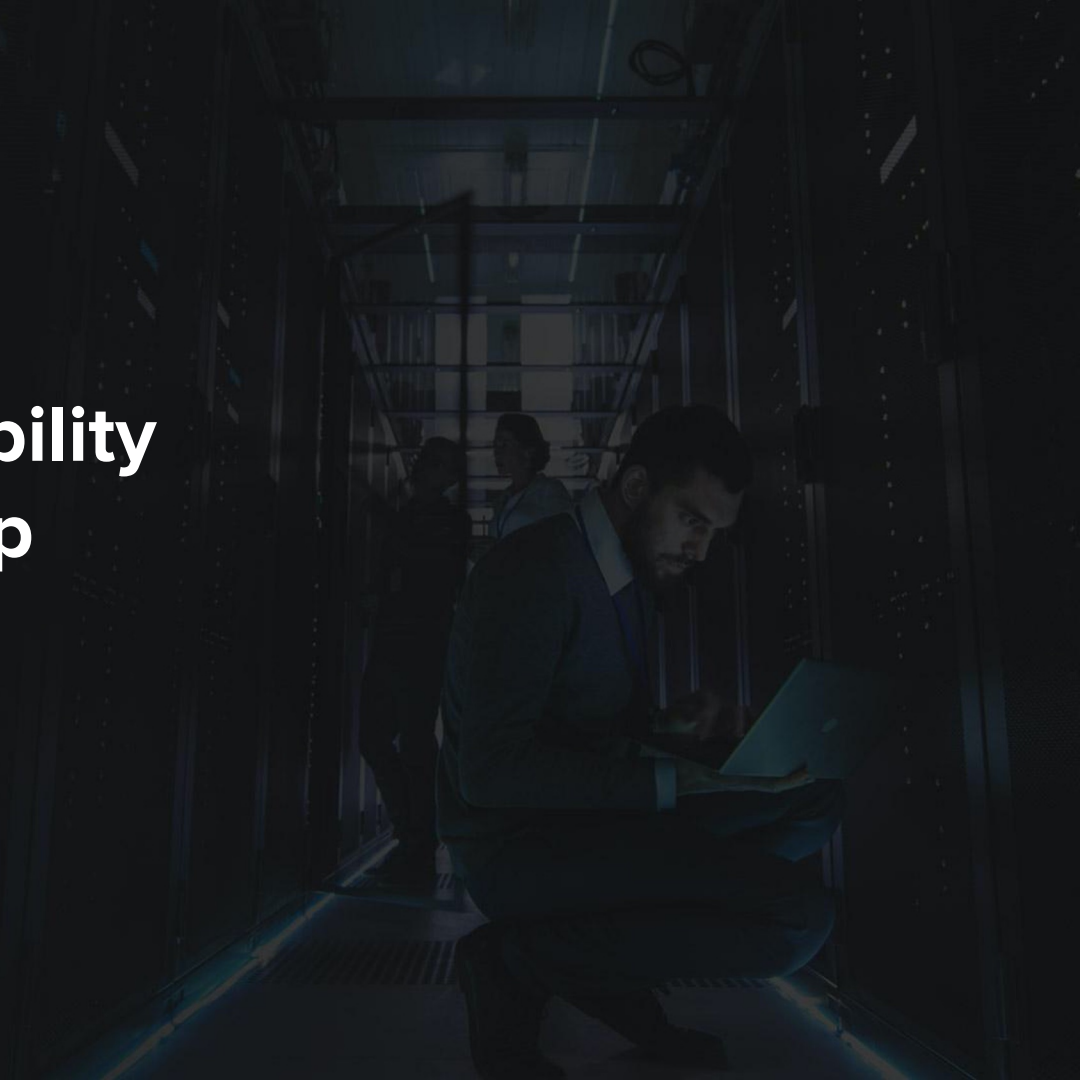




Recon and Vulnerability Detection Bootcamp

Day 1: Passive Reconnaissance

ine.com



Penetration Testing Methodology Overview

1.1. Penetration Testing Methodology Overview

- + In this module, you will learn the basic principles of Penetration Testing.
- + A penetration tester, much like an experienced hacker, performs a deep investigation of the remote system's security flaws. This activity requires methodology and skills!

1.1. Penetration Testing Methodology Overview

- + Penetration testers, unlike hackers, must **test for any and all vulnerabilities**, not just the ones that may grant them root access to a system. **Penetration testing is not about getting root!**
- + Furthermore, Penetration Testers cannot destroy their client's infrastructure; professional pentesting requires a thorough understanding of attack vectors and their potential.

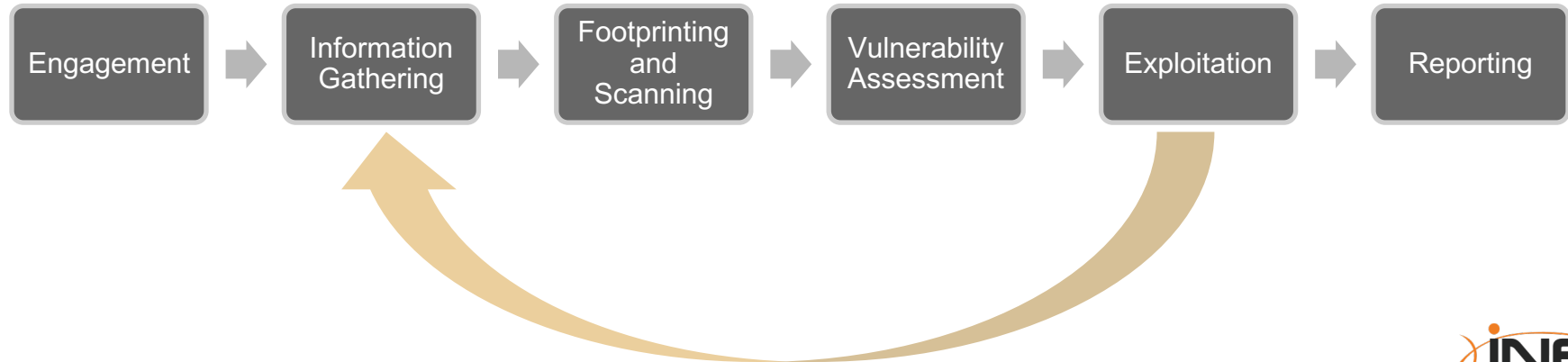
1.1. Penetration Testing Methodology Overview

Methodology Benefits

- + Consistent, Repeatable Process

1.1. Penetration Testing Methodology Overview

The phases of the **penetration testing process**. Do not underestimate the value of every step!



1.1. Penetration Testing Methodology Overview

- + Penetration Testing Execution Standards (PTES)
pentest-standard.org

Information Gathering

1.2. Information Gathering

- + **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.

1.2. Information Gathering

- + 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.

1.2. Information Gathering

- + 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.

1.2. Information Gathering

- + 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.

1.2. Information Gathering

- + 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.

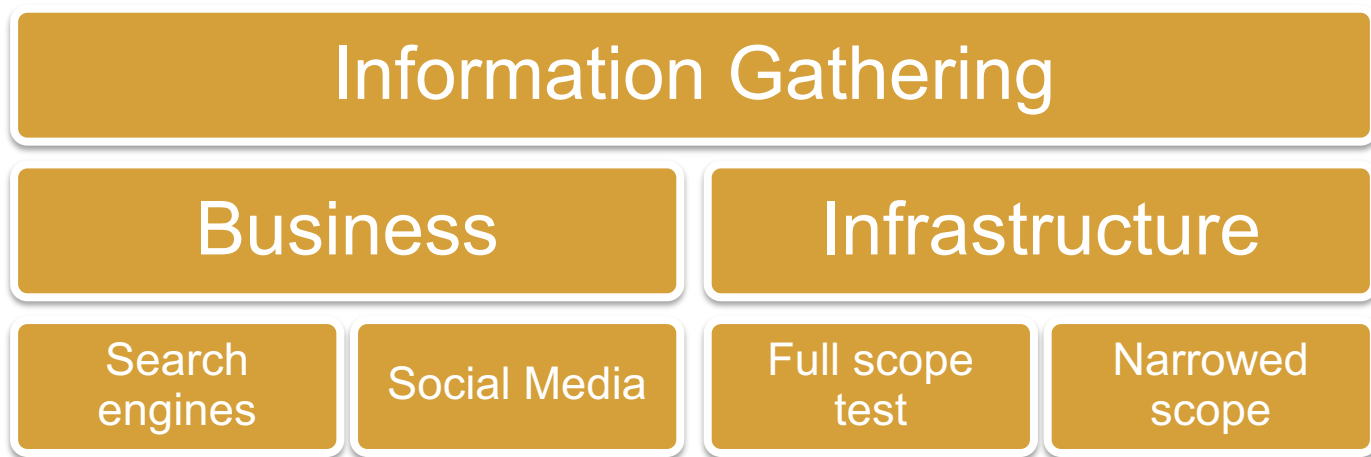
1.2. Information Gathering

- + 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

1.2. Information Gathering

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



1.2. Information Gathering

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

Passive

Active

1.2. Information Gathering

- + **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.

1.1. Information Gathering

- + **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 server logs so caution should be taken to prevent this.

1.2. Information Gathering

- + 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](http://freemind.sourceforge.net/wiki/index.php/Main_Page), [Xmind](https://www.xmind.net/), etc.) online. We suggest you use the one you are more comfortable with.

1.2. Information Gathering

- + When we start gathering and storing networking information, tools such as [Dradis](https://dradisframework.com/ce/), [Faraday](https://github.com/infobyte/faraday) and [Magitree](https://www.gremwell.com/what_is_magictree) 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



1.2. Information Gathering

- + 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 for download below this module.

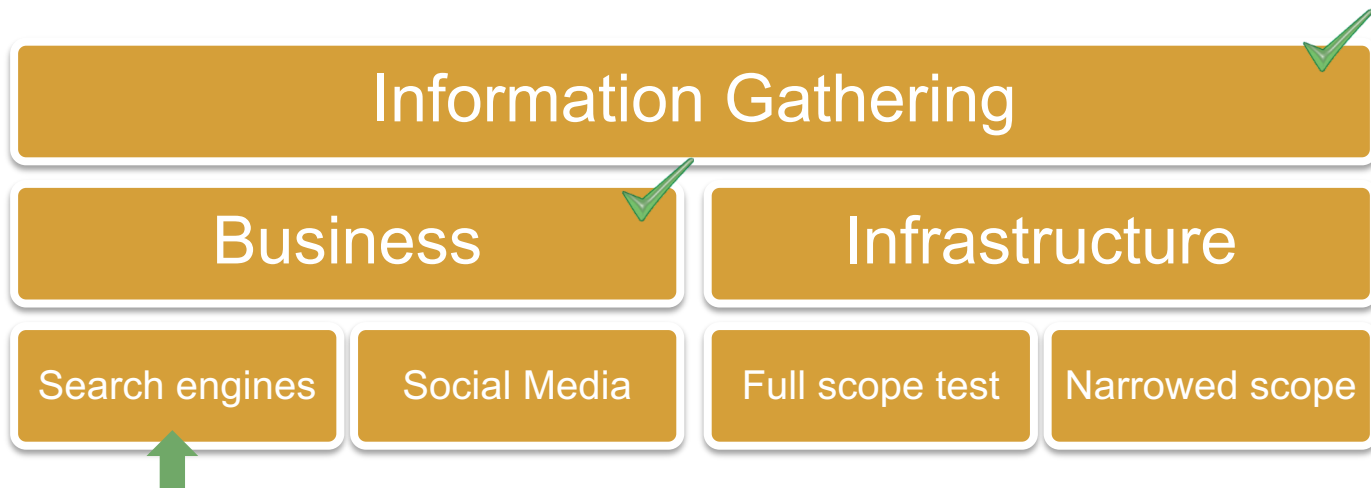
References

- + [Dradis](http://dradisframework.org/): <http://dradisframework.org/>
- + [Faraday](https://github.com/infobyte/faraday): <https://github.com/infobyte/faraday>
- + [FreeMind](http://freemind.sourceforge.net/wiki/index.php/Main_Page):
http://freemind.sourceforge.net/wiki/index.php/Main_Page
- + [Magitree](http://www.gremwell.com/what_is_magictree): http://www.gremwell.com/what_is_magictree
- + [Xmind](https://www.xmind.net/): <https://www.xmind.net/>

Search Engine

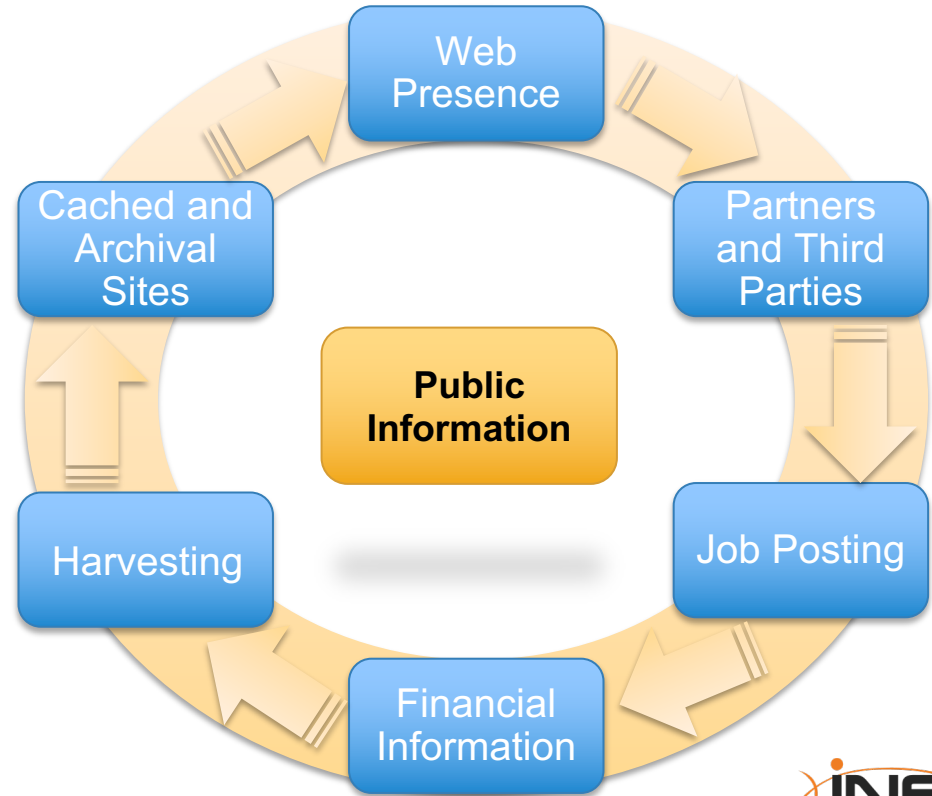
1.3. Search Engine

- + 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**.



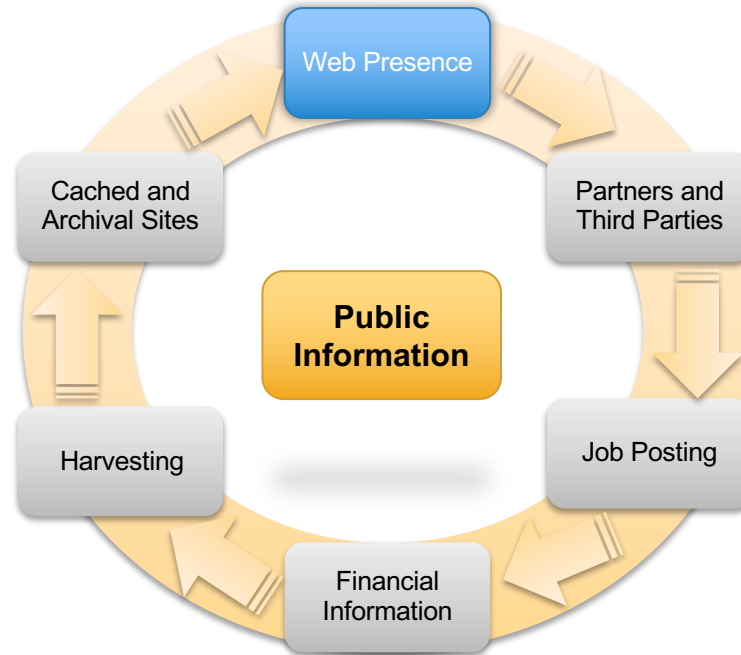
1.3.1. Search Engine

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



1.3.1.1. Web Presence

+ Let us begin with **Web Presence**.



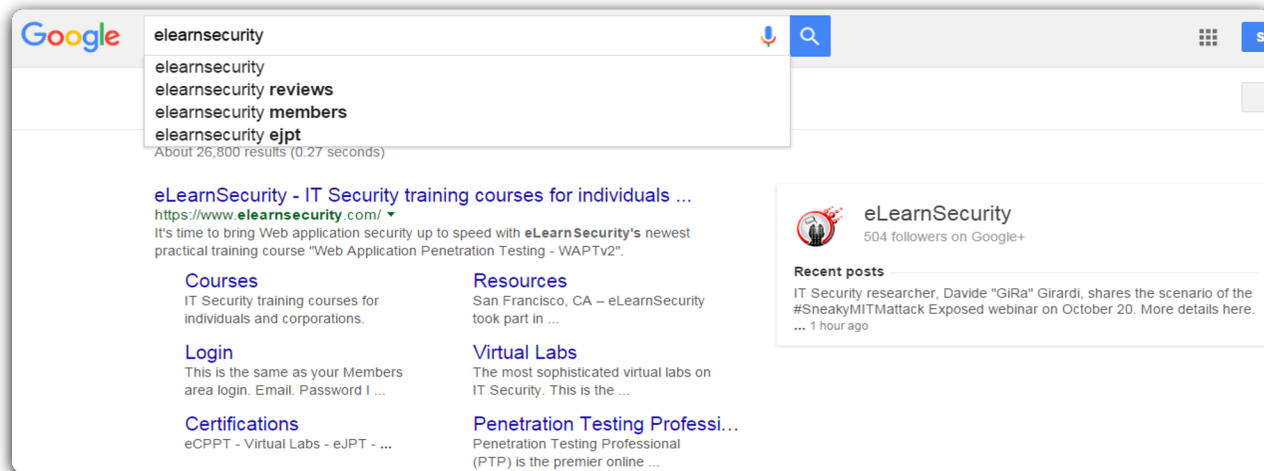
1.3.1.1. Web Presence

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;

1.3.1.1. Web Presence

- + 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.



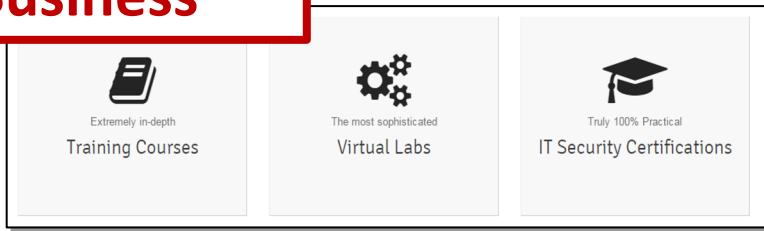
1.3.1.1. Web Presence

- + 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).

1.3.1.1. Web Presence

+ This is an example of information you can obtain:

Business



Location

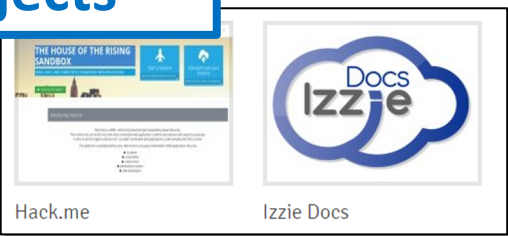
eLearnSecurity s.r.l.
P.I. 01997780505

Via Matteucci 36/38
Pisa, Italy

2040 Martin Ave.
95050, Santa Clara USA

Apricot Bldg, Dubai Silicon Oasis
Dubai, UAE

Projects

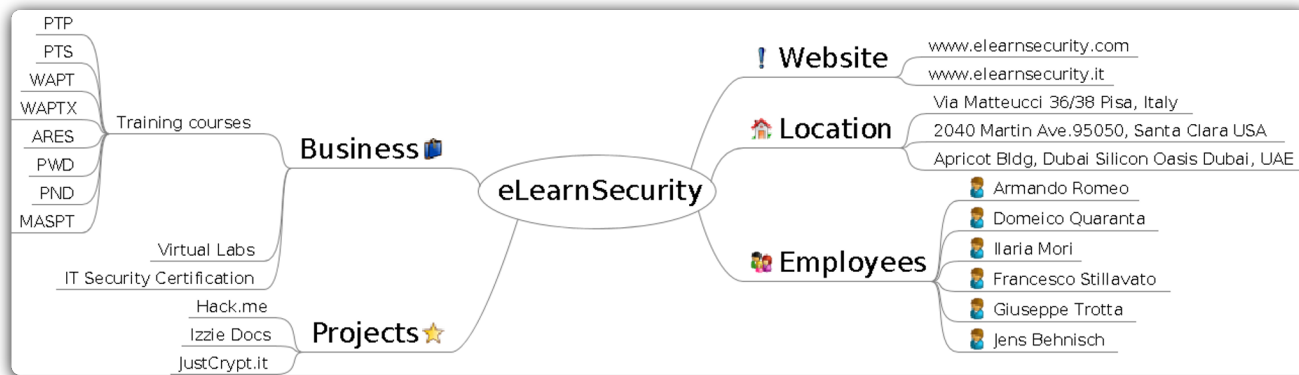


External links



1.3.1.1. 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:



1.3.1.1. Web Presence

- + 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.

1.3.1.1. Web Presence

- + 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.

1.3.1.1. Web Presence

+ 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

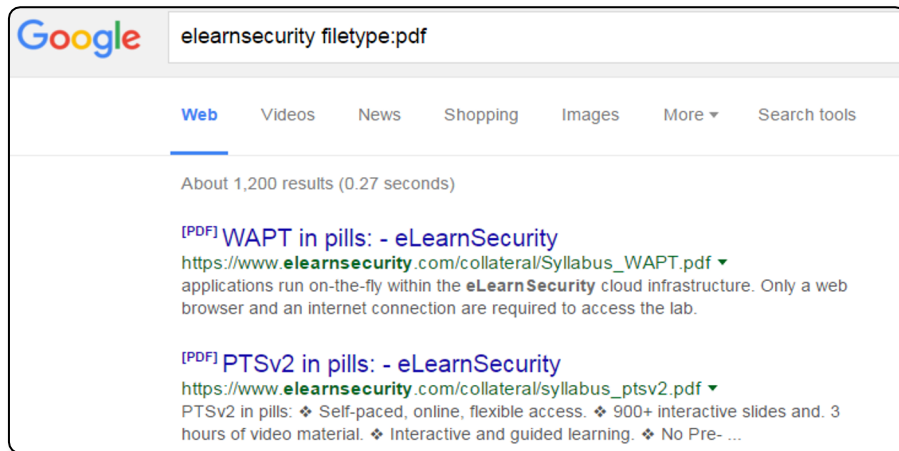
Filetype

[*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*

1.3.1.1. Web Presence

- + 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
```



1.3.1.1. Web Presence

- + 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.

1.3.1.1. Web Presence

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/>

1.3.1.1. Web Presence

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

- + [Bing](#)
- + [Yahoo](#)
- + [Ask](#)
- + [Aol](#)
- + [Pandastats.net](#)
- + [Dogpile.com](#)

1.3.1.1. Web Presence

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

Projects

[Enter in Hack.me](https://me.hack.me/)

<https://me.hack.me/> ▼ Traduci questa pagina

2013 All rights reserved | Scroll to top. Terms of Service. Developed, maintained and donated to the Community by eLearnSecurity.

External links

[Security Bloggers Network | Security Blogger Awards](http://www.securitybloggersnetwork.com/security-blogger-awards/)

www.securitybloggersnetwork.com/security-blogger-awards/ ▼ Traduci questa pagina

The Social Security Blogger Awards are announced each year at the end of the year at the US RSA show. Nominations are usually by a panel of blue collar ...

[opinion Archives - EH-Net Online Mag](http://www.ethicalhacker.net/tag/opinion)

[https://www.ethicalhacker.net/tag/opinion](http://www.ethicalhacker.net/tag/opinion) ▼ Traduci questa pagina

I was recently contacted by Don from The Ethical Hacker Network (EH-Net) and asked if I was interested in attending the Black Hat USA 2014 Briefings as the ...

[Book Review: Gray Hat Python - EH-Net Online Mag](http://www.ethicalhacker.net/features/book-reviews)

[www.ethicalhacker.net > Features > Book Reviews](http://www.ethicalhacker.net/features/book-reviews) ▼ Traduci questa pagina

01 lug 2009 - "Gray Hat Python" by Justin Seitz, one of the latest releases from publisher, No Starch Press, focuses on using the Python programming ...

Subdomains

[eLearnSecurity Blog](https://blog.elearnsecurity.com/)

<https://blog.elearnsecurity.com/> ▼ Traduci questa pagina

3 giorni fa - San Francisco, CA - eLearnSecurity took part in the AppSecUSA 2015 which is an event organized by The Open Web Application Security ...

[Username Password Login Forgot your Password? Email ...](https://members.elearnsecurity.com/)

<https://members.elearnsecurity.com/> ▼ Traduci questa pagina

Username. Password. Login. Forgot your Password? Email. Recovery.

[eLearnSecurity \(@eLearnSecurity\) | Twitter](https://twitter.com/elearnsecurity)

<https://twitter.com/elearnsecurity> ▼ Traduci questa pagina

3046 tweets • 199 photos/videos • 3281 followers. Check out the latest Tweets from eLearnSecurity (@eLearnSecurity)

[eLearnSecurity - Wikipedia, the free encyclopedia](https://en.wikipedia.org/wiki/eLearnSecurity)

<https://en.wikipedia.org/wiki/eLearnSecurity> ▼ Traduci questa pagina

eLearnSecurity (eLS) is a computer security professional certification training company that has differentiated itself by being one of the first companies to provide ...

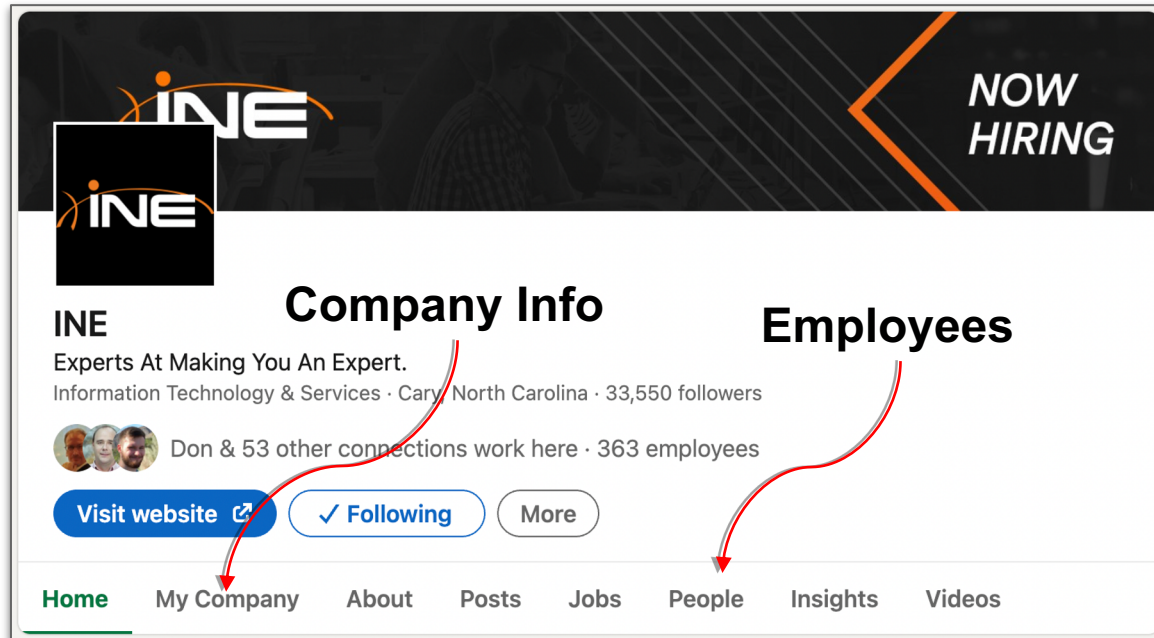


1.3.1.1. Web Presence

- + 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.

1.3.1.1. Web Presence

- + In our case, we can find employees, contact info, locations and more.



1.3.1.1. Web Presence

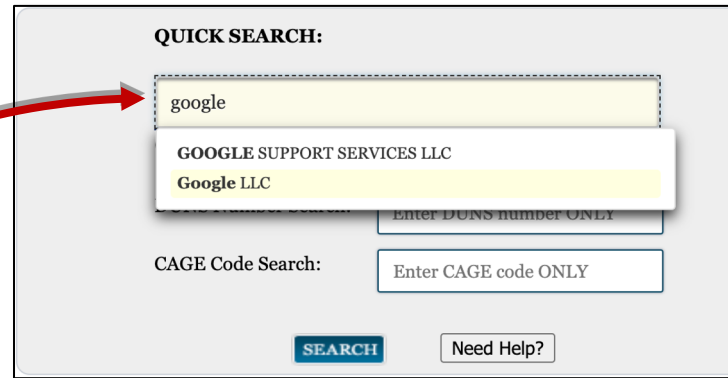
- + Websites like LinkedIn show even more information about companies and people that are related to that company especially if you have either a regular account or a premium one.
- + Unless you restrict your privacy settings, your visits to other LinkedIn profile's will subsequently notify those account owners.
- + Keep this in mind when performing stealthy operations.

1.3.1.1. Web Presence

- + 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.

1.3.1.1. Web Presence

- + We can retrieve the DUNS and CAGE code for a given company from the [following web site](#). Once you arrive click on Search Records:

The image shows a "QUICK SEARCH:" interface. It features a search input field containing the text "google". Below the input field is a dropdown menu with two search results: "GOOGLE SUPPORT SERVICES LLC" and "Google LLC". To the right of the input field is a button labeled "Enter DUNS number ONLY". Below the search results is a "CAGE Code Search:" section with an input field labeled "Enter CAGE code ONLY". At the bottom of the interface are two buttons: a blue "SEARCH" button and a "Need Help?" button.

1.3.1.1. Web Presence

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

Total records:1

Save PDFExport ResultsPrint

Result Page: 1Sort by RelevanceOrder by Descending

FILTER RESULTS

By Record Status

☒ Active

☐ Inactive

By Record Type

☐ Entity Registration

☐ Exclusion

Apply Filters

Your search for Google LLC* returned the following results...

Entity

Google LLC

Status: Active

DUNS: 060902413

CAGE Code: 1XAU1

View Details

Has Active Exclusion?: No

DoDAAC:

Expiration Date: 04/28/2021

Debt Subject to Offset?: No

Purpose of Registration: All Awards

1.3.1.1. Web Presence

- + 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:

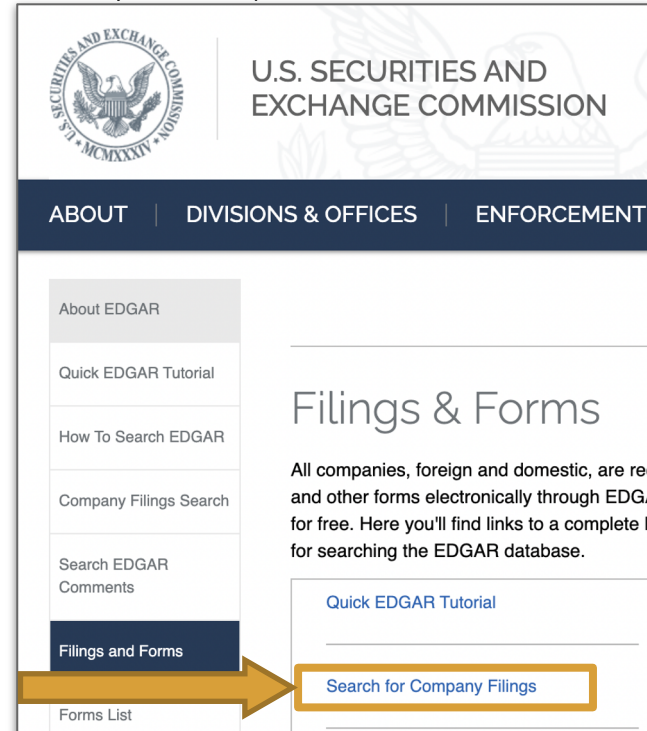
Entity Dashboard	Google LLC DUNS: 060902413 CAGE Code: 1XAU1 Status: Active Expiration Date: 04/28/2021 Purpose of Registration: All Awards	1600 Amphitheatre Pkwy Mountain View, CA, 94043-1351, UNITED STATES
<ul style="list-style-type: none">Entity OverviewEntity Registration<ul style="list-style-type: none">Core DataAssertionsReps & CertsPOCsExclusions<ul style="list-style-type: none">Active ExclusionsInactive ExclusionsExcluded Family Members	Entity Overview Entity Registration Summary Name: Google LLC Doing Business As: Google Business Type: Business or Organization Last Updated By: Jason Barlow Registration Status: Active Activation Date: 04/30/2020 Expiration Date: 04/28/2021	
RETURN TO SEARCH	Exclusion Summary Active Exclusion Records? No	

1.3.1.1. 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.

1.3.1.1. Web Presence

- + For this purpose you can use the EDGAR (Electronic Data Gathering, Analysis, and Retrieval system)
 - <http://sec.gov/edgar.shtml>



1.3.1.1. Web Presence

+ After that you can perform specific searches:

You can search information collected by the SEC using a variety of search tools.

EDGAR full text search

- New versatile tool lets you [search for keywords and phrases](#) in over 20 years of EDGAR filings, and filter by date, company, person, filing category, or location.

Boolean and advanced searching, including addresses

Search by:

- [Company or fund name, ticker symbol, central index key \(CIK\), file number, state, country, or standard industrial classification \(SIC\)](#)
- [Mutual fund name, ticker symbol, or SEC key](#), since February 2006
- [Variable insurance products by name of insurance company, underlying mutual fund, or contract](#), since February 2006

Search for:

- [A company's central index key \(CIK\) number](#)
- [Latest filings](#)
- [Daily filings by type \(current events\)](#)
- [Key mutual fund disclosures](#)
- [Mutual fund voting records](#)
- [Confidential treatment orders](#)
- [Effectiveness notices](#)
- [EDGAR correspondence](#)
- [Historical EDGAR documents \(historical archive search\)](#)

1.3.1.1. Web Presence

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

Document

APPLE INC CIK#: 0000320193 (see all company filings)

SIC: 3571 - ELECTRONIC COMPUTERS
State location: CA | State of Inc.: CA | Fiscal Year End: 0930
formerly: APPLE COMPUTER INC (filings through 2007-01-04)
formerly: APPLE COMPUTER INC/ FA (filings through 1997-07-28)
(Assistant Director Office: 3)
Get [insider transactions](#) for this issuer.

Filter Results: Filing Type: Prior to: (YYYYMMDD)

Items 1 - 40 [RSS Feed](#)

Filings	Format	Description
8-K	Documents	Current report, item 5.02 Acc-no: 0001181431-11-056354 (34 Act) Size: 12 KB
10-K	Documents Interactive Data	Annual report [Section 13 and 15(d), not S-K Item 405] Acc-no: 0001193125-11-282113 (34 Act) Size: 9 MB
8-K	Documents	Current report, items 2.02 and 9.01 Acc-no: 0001193125-11-273826 (34 Act) Size: 219 KB
8-K	Documents	Current report, item 8.01 Acc-no: 0001181431-11-051976 (34 Act) Size: 13 KB
8-K	Documents	Current report, item 5.02 Acc-no: 0001181431-11-047179 (34 Act) Size: 13 KB
UPLOAD	Documents	[Cover]SEC-generated letter Acc-no: 0000000000-11-049720 Size: 45 KB

Financial info

(in millions, except number of shares which are reflected in thousands and per share amount)

Three years ended September 24, 2011	2011	2010
Net sales	\$108,249	\$ 65,225
Cost of sales	64,431	39,541
Gross margin	43,818	25,684
Operating expenses:		
Research and development	2,429	1,782
Selling, general and administrative	7,599	5,517
Total operating expenses	10,028	7,299
Operating income	33,790	18,385
Other income and expense	415	155
Income before provision for income taxes	34,205	18,540
Provision for income taxes	8,283	4,527
Net income	\$ 25,922	\$ 14,013
Earnings per share:		
Basic	\$ 28.05	\$ 15.41
Diluted	\$ 27.68	\$ 15.15

Name and positions

[View E-mail](#)
Mr. Peter Oppenheimer
Senior Vice President and Chief Financial Officer
Apple, Inc.
1 Infinite Loop
Cupertino, California 95014

1.3.1.1. Web Presence

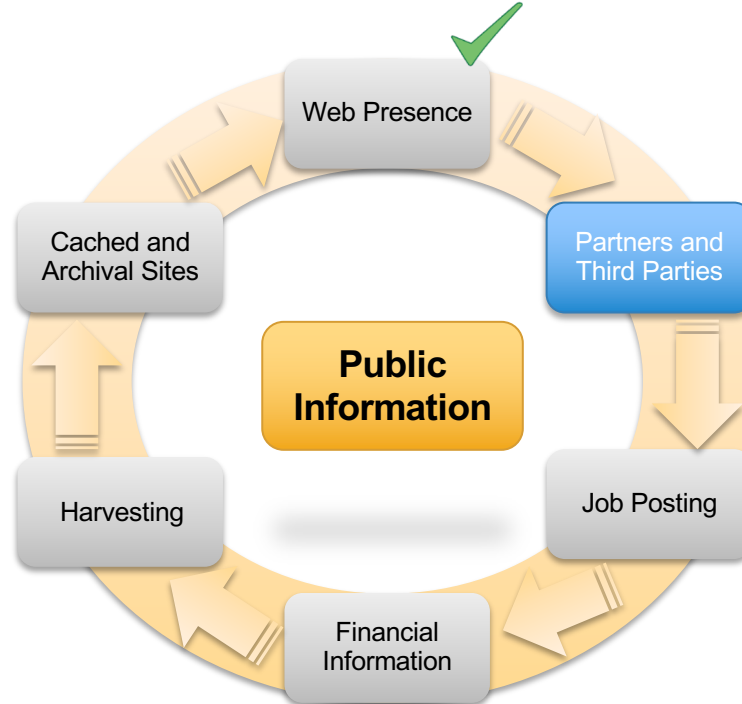
- + Note that **Information gathering** is not a linear process but actually a cyclical process.
- + When you find new organization projects, websites and subdomains, you have to repeat the whole investigation process for each of them. This will widen the attack surface thereby increasing the chances of a successful outcome of the penetration test.

1.3.1.1. 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!

1.3.1.2. Partners and Third Parties

- + We can now move on with Partners and third parties.

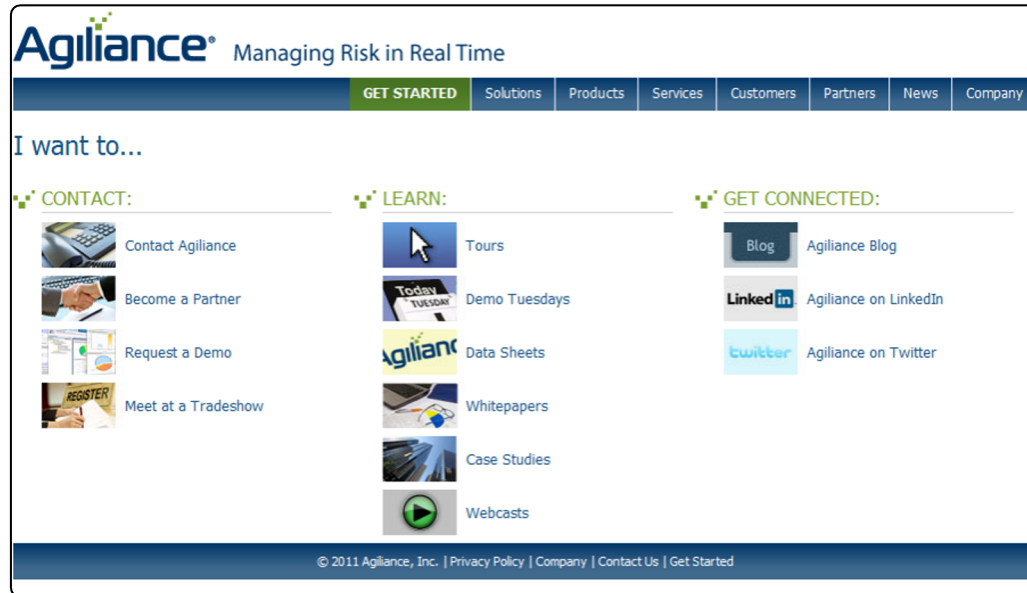


1.3.1.2. Partners and Third Parties

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

1.3.1.2. Partners and Third Parties

- + Let us use Agilience as sample case study:



1.3.1.2. Partners and Third Parties

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

The screenshot displays the BMC Atrium CMDB website, which is organized into several sections. On the left, a 'Partners' sidebar lists categories: MSSPs, Service Providers, Technology Providers, Access Management, Configuration, CMDB, Database Security, Help Desk, Threat & Advisory, SIEM, Vulnerability, Web App Sec, Content Providers, and 'Become a Partner'. The main content area is titled 'Configuration Management Technology Providers' and features logos for BMC Software, HP, and Microsoft. Below the Microsoft logo, it describes 'Microsoft Active Directory (AD)' as being deployed on most IT networks, listing assets like people, servers, and desktops. To the right, a 'Web Application Security' section highlights 'HP WebInspect' for identifying application vulnerabilities and mapping results to the NVD, and 'IBM Rational AppScan' for identifying vulnerabilities and importing assets from AppScan. A large, semi-transparent grid of partner logos is overlaid on the right side of the page. This grid includes logos for PricewaterhouseCoopers, Deloitte & Touche, KPMG, DRS, Cisco, Bell, and Accuvant. It also categorizes partners into 'Advisory Service Providers' (Big 4, Compliance & Risk Consultants), 'System Service Providers' (Security, Mobile, Telecom, Utility), 'Technology Providers' (Cloud, Managed Service, On Premise), and 'Content Providers' (Frameworks, Regulations & Standards). The 'OpenGRC by Agilience' logo is prominently displayed in the center of this grid. At the bottom right, the 'INE' logo is visible.

Partners

- MSSPs
- Service Providers
- Technology Providers
- Access Management
- Configuration
- CMDB
- Database Security
- Help Desk
- Threat & Advisory
- SIEM
- Vulnerability
- Web App Sec
- Content Providers
- Become a Partner

Configuration Management Technology Providers

BMC Atrium imports Atrium CMDB, allowing IT infrastructure and new entities are automatically assessments. Asset entities via risk and assignment of the owner as well as entered into the IT e

The HP Service Ma of entities from the HP Service Manager Risk Repository. This automation allows customers to jumpstart their risk and compliance management program.

Microsoft Active Directory (AD) is deployed on most IT networks. Generally, all assets, including people, servers, and desktops, are listed in the Active Directory server in their

Web Application Security

HP WebInspect is identifying all applic HP WebInspect imp and application vuln results in the applic are mapped to the N Database (NVD) bas score is assigned fro

IBM Rational App scanner that identif vulnerabilities. Agilience RiskVision AppScan imports application assets from AppScan results in the application inventory. Along with the application, it will also import all the vulnerabilities for those applications. Vulnerabilities are mapped to National Vulnerability Database (NVD). If a vulnerability

Partners Grid:

- Advisory Service Providers: Big 4, Compliance & Risk Consultants
- System Service Providers: Security, Mobile, Telecom, Utility
- Technology Providers: Cloud, Managed Service, On Premise
- Content Providers: Frameworks, Regulations & Standards

OpenGRC by Agilience

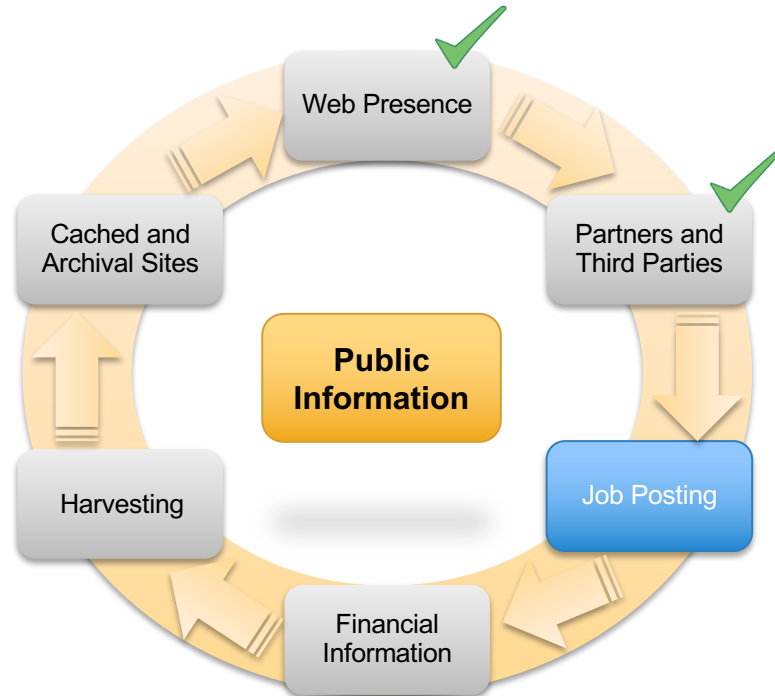
Partners Logos: PricewaterhouseCoopers, Deloitte & Touche, KPMG, DRS, Cisco, Bell, Accuvant, Circle, RedSeal, VeriSign, IMPERVA, APPLICATION SECURITY INS, McAfee, CSA, cloud security alliance, BITS, RAPID7, NetIQ, Qualys, skybox, e.

1.3.1.2. 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.

1.3.1.3. Job Posting

- + The next step is finding information from **Job Postings**.



1.3.1.3. Job Posting

- + 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**.

1.3.1.3. 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.

1.3.1.3. Job Posting

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

Agilience Current US Job Openings

Agilience offers competitive compensation and a full benefits package including medical, dental, vision, life insurance, child care reimbursement, and more.

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

REQUIREMENTS

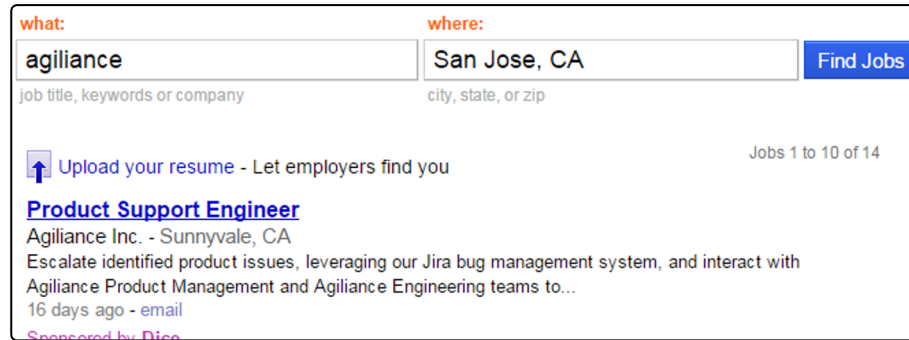
- Experience in the development of scalable applications
- Excellent working knowledge of Java, J2EE, and JSP
- Strong working knowledge of application servers like JBoss or WebSphere
- Strong working knowledge of MySQL and Oracle
- Experience with the Spring Framework
- Experience with JavaScript libraries like jQuery
- Experience with reporting frameworks like JasperReports
- Solid knowledge and application of engineering principles
- Understands development methodology
- 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 tasks.

1.3.1.3. Job Posting

- + 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 screenshot displays the Indeed job search interface. At the top, there are two input fields: 'what:' with the text 'agilience' and 'where:' with the text 'San Jose, CA'. To the right of these fields is a blue button labeled 'Find Jobs'. Below the 'what:' field, there is a placeholder text 'job title, keywords or company'. Below the 'where:' field, there is a placeholder text 'city, state, or zip'. Below the search fields, there is a link 'Upload your resume - Let employers find you' with an upward arrow icon. To the right of this link, it says 'Jobs 1 to 10 of 14'. Below this, there is a job listing for 'Product Support Engineer' at 'Agilience Inc. - Sunnyvale, CA'. The listing description reads: 'Escalate identified product issues, leveraging our Jira bug management system, and interact with Agilience Product Management and Agilience Engineering teams to...'. Below the description, it says '16 days ago - email'. At the bottom of the listing, it says 'Sponsored by Dice'.

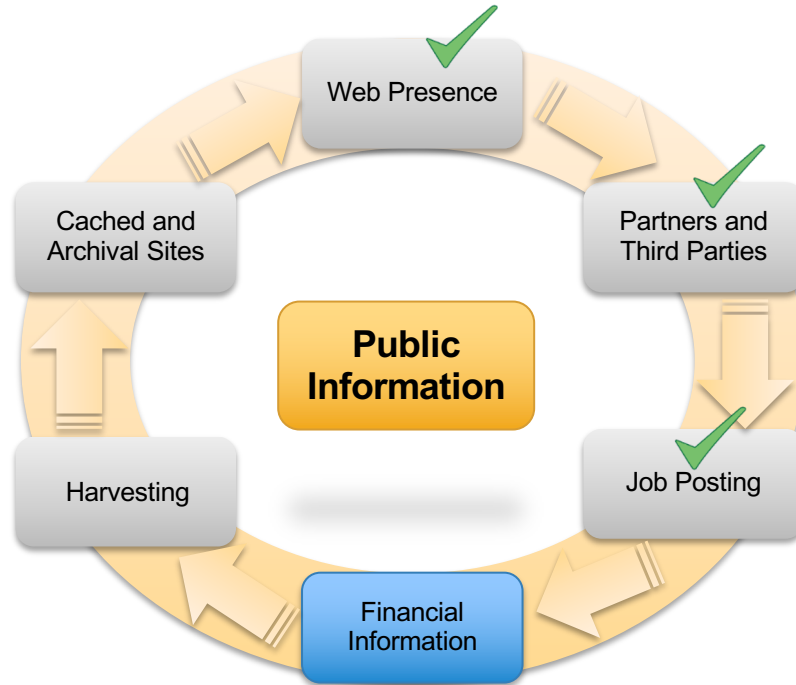
1.3.1.3. Job Posting

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

- + [LinkedIn](#)
- + [Indeed](#)
- + [Monster](#)
- + [Careerbuilder](#)
- + [Glassdoor](#)
- + [Simplyhired](#)
- + [Dice](#)

1.3.1.4. Financial

+ Let us focus now on **Financial Information**.



1.3.1.4. 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.

1.3.1.4. Financial

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

1.3.1.4. Financial

- + This snapshot shows what kind of information you can find:

The screenshot displays the Agilience company profile page. The page is divided into several sections:

- Overview:** This section contains financial information, highlighted by a blue box labeled "Financial info". It includes:
 - Funding Received: \$23.96M in 5 Rounds from 10 Investors
 - Most Recent Funding: \$5M Venture on May 13, 2014
 - Headquarters: Sunnyvale, CA
 - Description: Agilience provides IT solutions and services for businesses and government agencies.
 - Founders: Pravin Kothari
 - Categories: Security
 - Website: <http://www.agilience.com>
 - Social: Twitter icon
- Company Details:** This section contains company information, highlighted by a blue box labeled "Company info". It includes:
 - Founded: 2005
 - Contact: info@agilience.com | (408) 200-0400
 - Employees: 7 in CrunchBase
- Investors:** This section, highlighted by a blue box labeled "Investors", is titled "Graph Insights" and lists investors who have also invested in Agilience:
 - Beceem Communications: 2
 - Funambol: 2
 - Ikanos: 2
- Agilience's Current Team worked at:** This section lists companies where team members have previously worked:
 - Impres: 2
 - Sun Microsystems: 2
 - Hughes Network Systems: 1


The left sidebar shows the Agilience logo, a "FOLLOW" button, statistics (5 stars, 3K views), and a "CONTRIBUTE" button.

1.3.1.4. Financial

- + 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.

1.3.1.4. Financial

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

	2011 Inc. 5000 Rank		#39
	3-Year Growth		4909%
	2010 Revenue		\$6.3 M
	Jobs Added		20
Location	San Jose, CA	Country	United States
Founded	2005	Employees	
Employees	57		

1.3.1.4. Financial

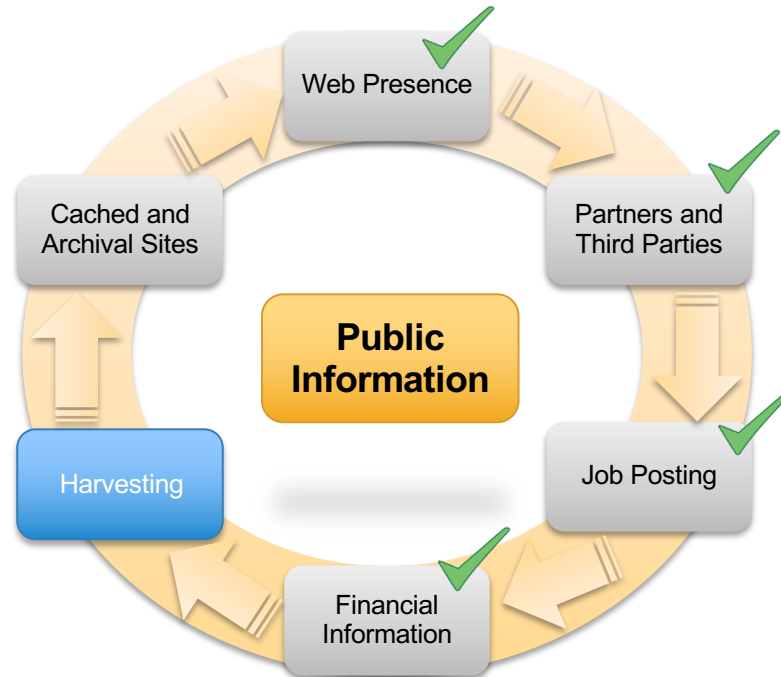
- + The following are additional resources that you can use to find out more financial information on your target.

The image displays four overlapping screenshots of financial resources:

- Google Finance:** Shows the Google logo and a sidebar with links to Finance, Markets, News, Portfolios, Stock screener, Google Domestic Trends, and Recent Quotes (30 days). The main content area features a "Market Summary" with a headline about a CEO's hospitalization.
- Yahoo Finance:** Shows the Yahoo! Finance header with navigation links (Home, Mail, Search, News, Sports, Finance) and a search bar. It includes a "Stocks to Watch" section and a market overview with Dow Jones and Nasdaq indices.
- U.S. Securities and Exchange Commission (EDGAR):** Features the SEC logo and a navigation menu (ABOUT, DIVISIONS, ENFORCEMENT, REGULATION, EDUCATION). The main section is "EDGAR | Company Filings", offering free access to over 20 million filings. It includes a search bar for "Company Name" and a "More Options" button.
- iNE:** A logo in the bottom right corner consisting of the letters "iNE" with a stylized orange arc above the "i".

1.3.1.5. Harvesting

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



1.3.1.5. 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.

1.3.1.5. Harvesting

- + 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.

1.3.1.5. Harvesting

- + 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*

1.3.1.5. Harvesting

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

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

About 14 results (0.22 seconds)

[PDF] PTSv2 in pills: - eLearnSecurity

https://www.elearnsecurity.com/collateral/syllabus_ptsv2.pdf ▼

PTSV2 in pills: ♦ Self-paced, online, flexible access. ♦ 900+ interactive slides and. 3 hours of video material. ♦ Interactive and guided learning. ♦ No Pre- ...

[PDF] Download PDF Syllabus - eLearnSecurity

https://www.elearnsecurity.com/collateral/Syllabus_PTSV3.pdf ▼

PTSV3 at a glance: ♦ Self-paced, online, flexible access. ♦ 1500+ interactive slides and. 4 hours of video material. ♦ Interactive and guided learning.

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

1.3.1.5. 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.

1.3.1.5. Harvesting

- + 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.

1.3.1.5. Harvesting

- + 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.

1.3.1.5. Harvesting

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

```
thearvester -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.)

1.3.1.5. Harvesting

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

```
[+] Emails found:
```

```
-----
```

```
armando@elearnsecurity.com  
davide@elearnsecurity.com  
jens@elearnsecurity.com  
hostmaster@elearnsecurity.com  
@elearnsecurity.com
```

Email
addresses

```
[+] Hosts found in search engines:
```

```
-----
```

```
[-] Resolving hostnames IPs...
```

```
199.193.116.231:www.elearnsecurity.com  
199.193.116.231:members.elearnsecurity.com  
162.220.56.82:blog.elearnsecurity.com  
162.220.56.82:Blog.elearnsecurity.com  
199.193.116.232:ns.elearnsecurity.com  
199.193.116.233:ns1.elearnsecurity.com
```

Hosts

1.3.1.5. Harvesting

- + 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
```

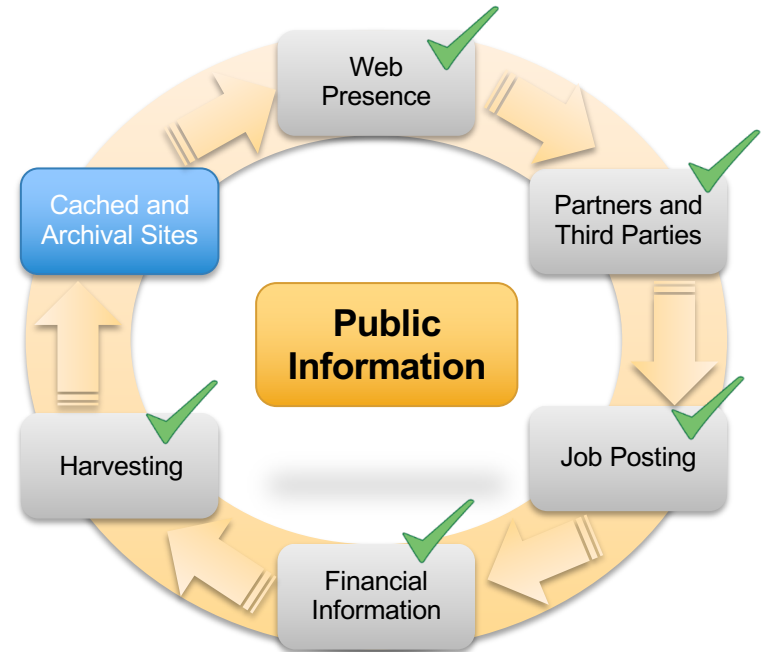
```
[ - ] Searching in Linkedin..  
      Searching 100 results..  
Users from Linkedin:  
=====  
Armando Romeo  
Jens Behnisch  
Jason Haddix  
Edcel Suyu  
Schuyler Dorsey  
Francesco Stillavato  
Domenico Quaranta
```

1.3.1.5. Harvesting

- + 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.

1.3.1.6 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**.

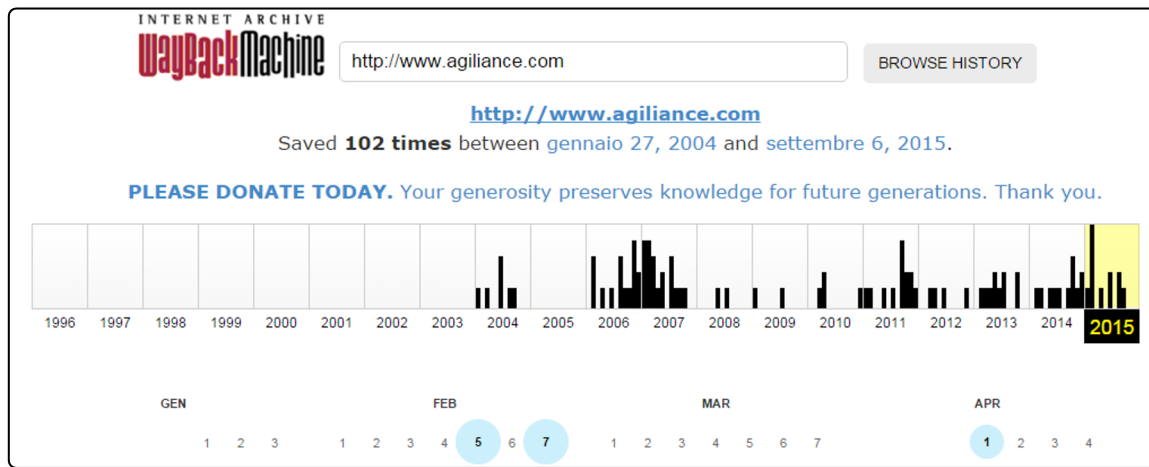


1.3.1.6 Cached and Archival Sites

- + 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.

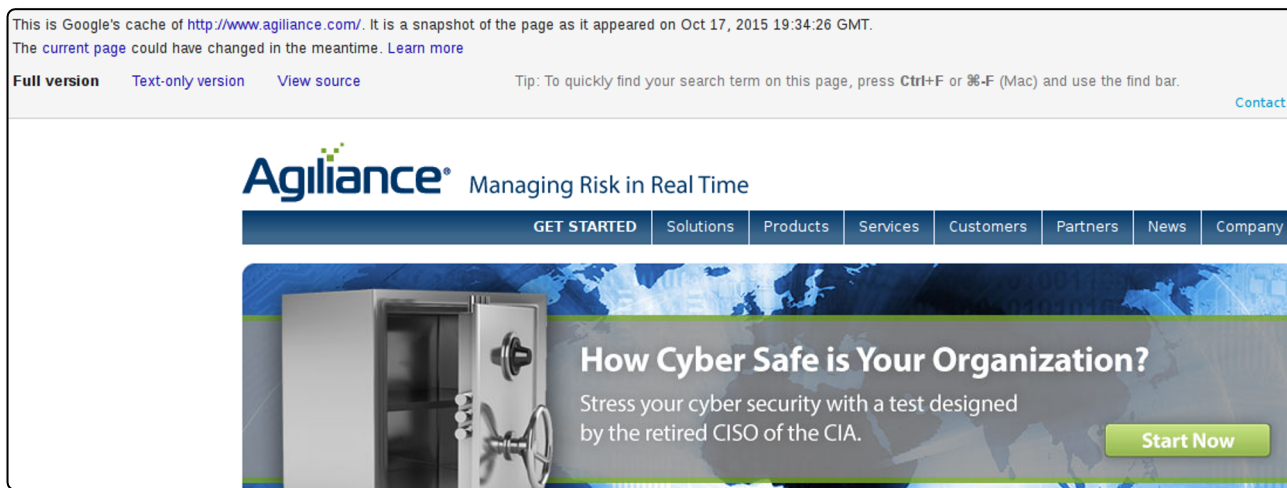
1.3.1.6 Cached and Archival Sites

- + 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.



1.3.1.6 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.



1.3.1. Search Engine

- + 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.

1.3.1. Search Engine

- + 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.

1.3.1. Search Engine

- + 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.

1.3.1. 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
 - + ...

References

- + Aol: <http://search.aol.com/aol/webhome>
- + Apache2 Ubuntu Default Page: <http://www.pandastats.net/>
- + Ask: <http://www.ask.com/>
- + Bing: <http://www.bing.com/>
- + CareerBuilder: <http://www.careerbuilder.com/>
- + Crunchbase: <http://www.crunchbase.com/>
- + Dice: <http://www.dice.com/>
- + Dogpile: <http://www.dogpile.com/>
- + EDGAR: <https://www.sec.gov/edgar.shtml>
- + eLSFoo: <http://www.elsfoo.com/>

References

- + FOCA: <https://www.elevenpaths.com/labstools/foca/index.html>
- + Glassdoor: <http://www.glassdoor.com/>
- + Google Hacking Database:
<http://pdf.textfiles.com/security/googlehackers.pdf>
- + Google Search Operators:
http://www.googleguide.com/advanced_operators_reference.html
- + Inc.: www.inc.com
- + Indeed: <http://www.indeed.com/>
- + Internet Archive: <http://www.archive.org/index.php>
- + LinkedIn: <http://www.linkedin.com/>

References

- + Refine web searches:
https://support.google.com/websearch/answer/136861?hl=en&ref_topic=3081620
- + SAM: <https://www.sam.gov/>
- + SimplyHired: <http://www.simplyhired.com/>
- + The Google Hacker's Guide: Understanding and Defending Against the Google Hacker: <http://pdf.textfiles.com/security/googlehackers.pdf>
- + theHarvester: <https://github.com/laramies/theHarvester>
- + Yahoo: <http://www.yahoo.com/>

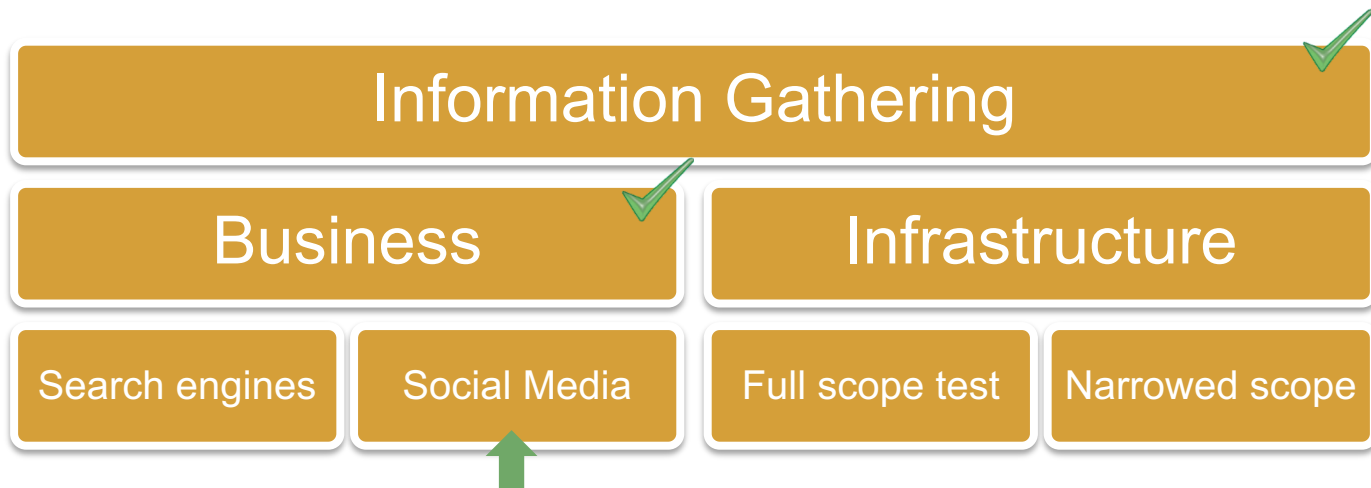
Social Media

1.4. 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).

1.3. Social Media

- + 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.



1.4. Social Media

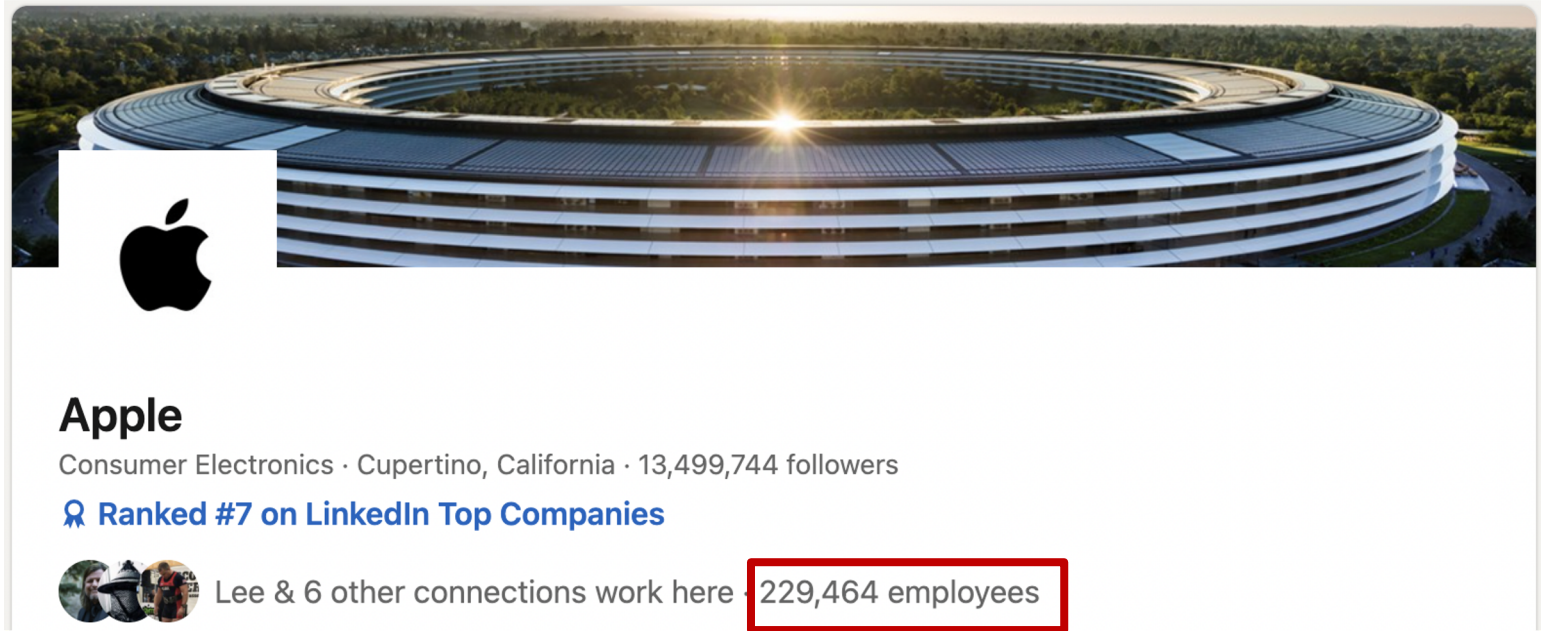
- + In this particular phase, social media is useful in the following ways:
 - + Learn about corporate culture, hierarchies, business processes, technologies, applications.
 - + To build a network map of people (relationships).
 - + Select the most appropriate target for a social engineering attack.

1.4. Social Media

- + 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.

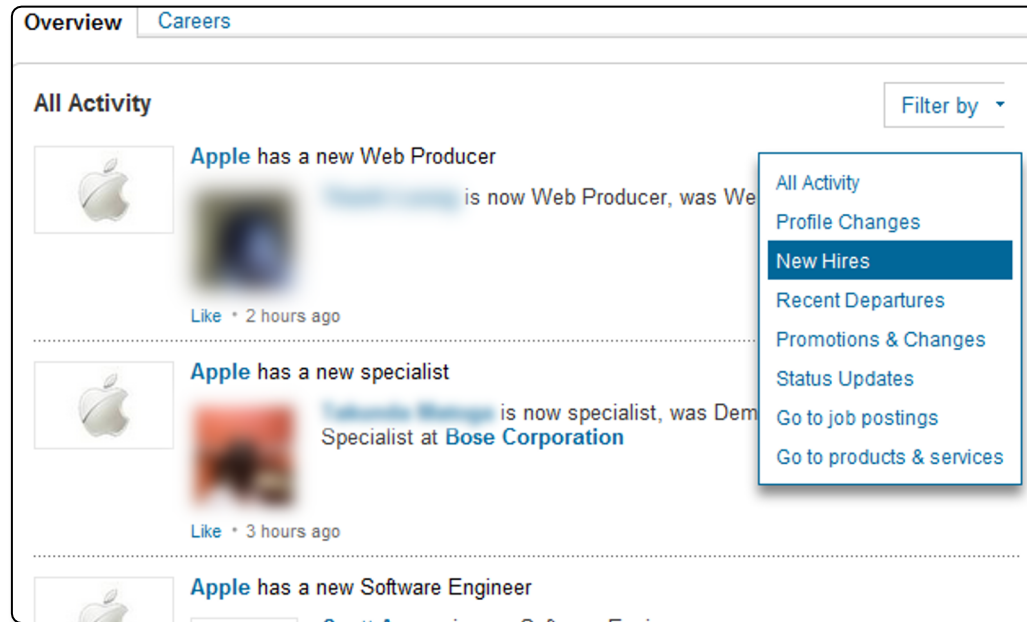
1.4. Social Media

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



1.4. Social Media

- + Retrieve more by searching in Apple activity:

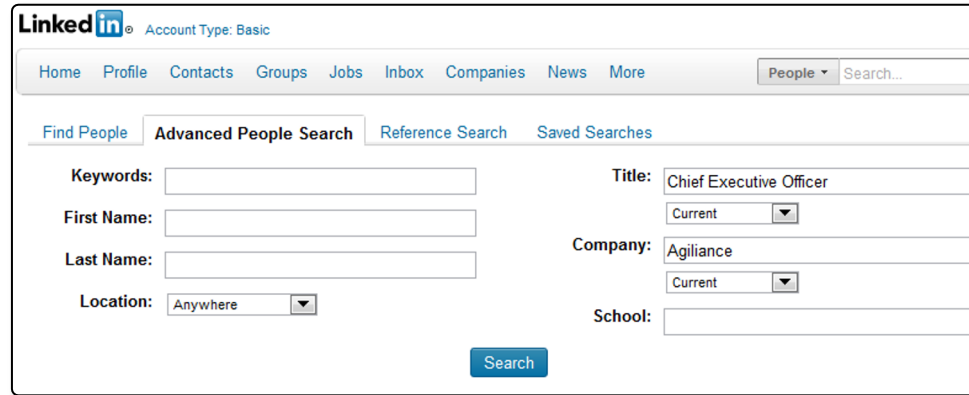


1.4. Social Media

- + 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 **Agilience**. Suppose we do not know who the **CEO** is.
- + You can click on advanced search in LinkedIn and start filling in search fields.

1.4. Social Media

- + This is an example of what we can type:



The screenshot shows the LinkedIn 'Advanced People Search' interface. At the top, the LinkedIn logo and 'Account Type: Basic' are visible. Below the navigation bar (Home, Profile, Contacts, Groups, Jobs, Inbox, Companies, News, More), there is a search bar with a 'People' dropdown and a 'Search...' button. The 'Find People' section is active, showing tabs for 'Find People', 'Advanced People Search', 'Reference Search', and 'Saved Searches'. The search criteria are as follows:

Field	Value
Keywords	
First Name	
Last Name	
Location	Anywhere
Title	Chief Executive Officer
Company	Agilance
School	

A blue 'Search' button is located at the bottom right of the search criteria section.

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

1.4. Social Media

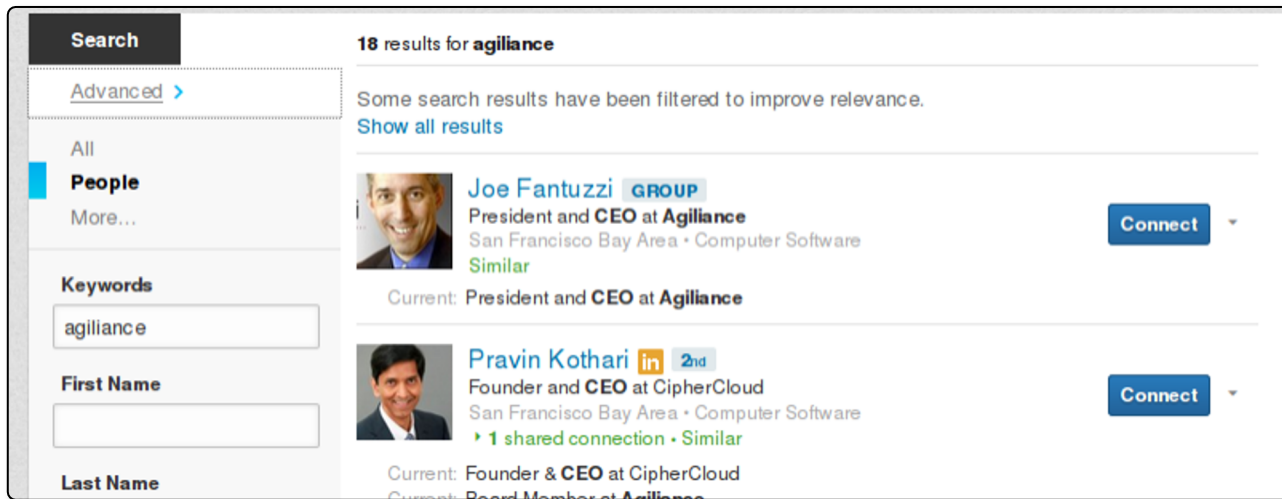
- + Note that when you perform these types of searches within *LinkedIn*, you may not see all the information about the people you are looking for as it depends upon the privacy settings of the target, relationship degree or shared groups.
- + If your target is a 1st or a 2nd connection, then you will 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.

1.4. Social Media

- + 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.

1.4. Social Media

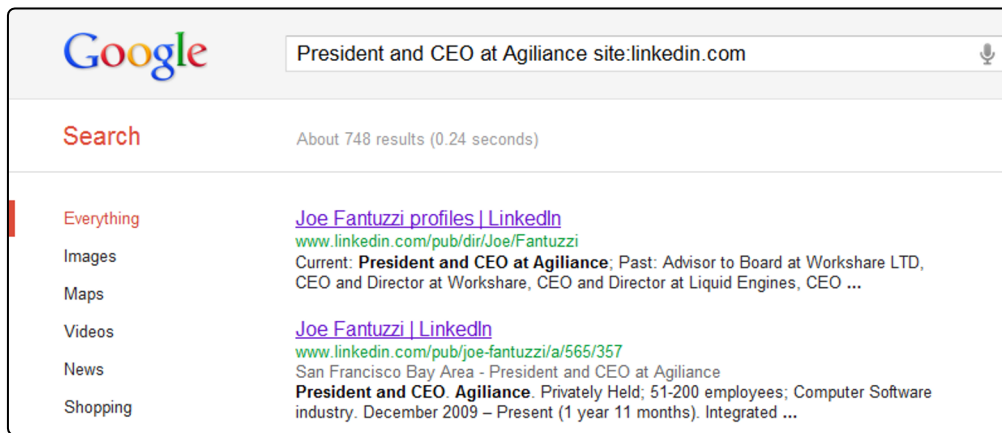
- + The following snapshot shows the results of our search. As you can see, we are able to see the contact information.



1.4. Social Media

- + 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 Agilience*' using the following filter:

site:linkedin.com



1.4. Social Media

- + 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.

The screenshot shows a LinkedIn search interface. On the left, a sidebar contains a 'Search' button, an 'Advanced' link, and filters for 'All', 'People' (selected), and 'More...'. Below these are input fields for 'Keywords' (containing 'vice president') and 'First Name'. The main content area displays '21 results for vice president' and a message that some results have been filtered. A 'Show all results' link is present. A profile card for 'Torsten George' is highlighted, showing his photo, title 'Global Marketing Executive / Product Evangelist', location 'San Francisco Bay Area', and industry 'Computer Software'. It also lists his current role at 'Agilience' and previous roles at 'Actividentity Inc.' and 'Cordys'. A 'Connect' button is visible. A larger, semi-transparent version of the profile card is overlaid on the right side of the image.

Search

Advanced >

All

People

More...

Keywords

vice president

First Name

21 results for **vice president**

Some search results have been filtered to
[Show all results](#)

Torsten George

Global Marketing Executive / Product Evangelist
San Francisco Bay Area • Computer Software

▶ 1 shared connection • Similar

Current: **Vice President**, Worldwide Marketing, Products, and Support at A...
Past: Vice President, Worldwide Marketing at Actividentity Inc.
Member, Strategic Advisory Board at Cordys
Director, On-Demand Services / General Manager at Actividentity ...

Torsten George
Global Marketing Executive / Product Evangelist
San Francisco Bay Area | Computer Software

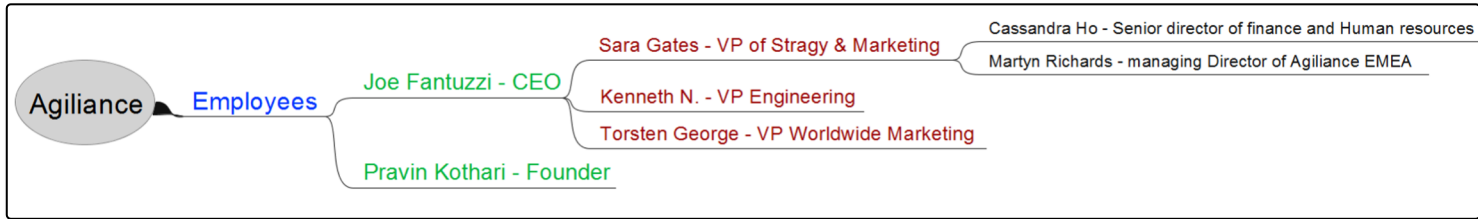
Current Agilience
Previous Actividentity Inc., Cordys, Solid Information Technology
Education Freie Universitaet Berlin, Germany

[Connect](#) [Send Torsten InMail](#)

[Connect](#)

1.4. Social Media

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



1.4. Social Media

- + 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.

1.4. Social Media

- + 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.

1.4. Social Media

- + 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

1.4.1. 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:

The screenshot shows the Pipl search interface. The search bar contains 'guy takeo kawasaki'. The results are displayed in a grid. The main result for 'Guy Takeo Kawasaki' is highlighted, showing a purple profile picture with a white 'G', his age (61 years old), and various contact details. A 'Possibly Related Results' box is overlaid on the right, showing two additional results for 'Guy Kawasaki' with their respective profile pictures and brief descriptions.

pipl Search By: First Middle Last + MORE OPTIONS

guy takeo kawasaki Location (open)

Guy Takeo Kawasaki
61 years old

SPONSORED: [Personal Info](#) | [Contact Info](#) | [Online](#)

PHONES: 650-327-1948, 259-273-3122, 650-387-1591, 831-724-7774, 650-327-1925, 650-325-2022

PLACES: Palo Alto, California
30 McCormick Lane, Atherton, California
10424 Love Creek Rd, Ben Lomond, California

Possibly Related Results

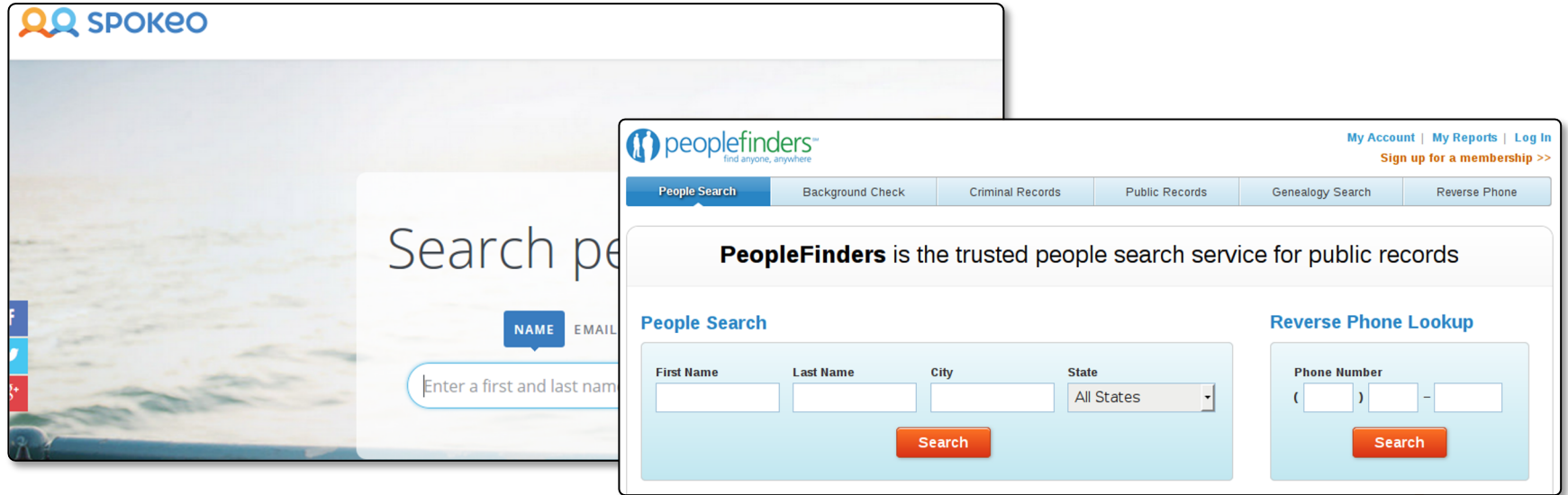
Guy Kawasaki
San Francisco & Palo Alto, California
SPONSORED: [Personal Info](#) | [Address History](#) | [Online Photos](#) | [Contact Info](#)
Co-founder at Garage Technology Ventures and 18 more jobs

Guy Kawasaki
California
SPONSORED: [Personal Info](#) | [Address History](#) | [Online Photos](#) | [Contact Info](#)
Known online as guy and guykawasaki

Sponsored Links
[Lookup 650-327-1948](#)

1.4.1. Social Media – People search

- + Other very useful websites that you can use to find more information on someone are [spokeo](https://www.spokeo.com/) and [peoplefinders](https://www.peoplefinders.com/):



The image displays two overlapping screenshots of people search websites. The background screenshot is the Spokeo homepage, featuring a search bar with a 'NAME' dropdown and a text input field for 'Enter a first and last name'. The foreground screenshot is the PeopleFinders homepage, which includes a navigation bar with links like 'People Search', 'Background Check', 'Criminal Records', 'Public Records', 'Genealogy Search', and 'Reverse Phone'. Below the navigation bar, there is a prominent banner stating 'PeopleFinders is the trusted people search service for public records'. The main content area contains two search forms: 'People Search' with fields for 'First Name', 'Last Name', 'City', and 'State' (a dropdown menu set to 'All States'), and a 'Search' button; and 'Reverse Phone Lookup' with a 'Phone Number' field in the format '() - ' and a 'Search' button.

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

1.4.1. Social Media – People search

- + We can even use [CrunchBase](https://www.crunchbase.com/) to find more information about our target:



The screenshot shows the profile of Guy Kawasaki on CrunchBase. It includes a profile picture, a 'FOLLOW' button, and a table of investments. The table has columns for Date, Invested In, Round, and Details. The investments listed are: Oct, 2013 (GotIt! / Angel, Personal Investment), Dec, 2011 (Buffer / Angel, Personal Investment), Dec, 2008 (Posterous / Angel, Personal Investment), May, 2006 (FilmLoop / Series B, Garage Technology Ventures), Jul, 2005 (Simply Hired / Series B, Garage Technology Ventures), Feb, 2005 (FilmLoop / Series A, Garage Technology Ventures), and Sep, 2004 (BitPass / Series B, Garage Technology Ventures).

Guy Kawasaki			
Investments (7)			
Date	Invested In	Round	Details
Oct, 2013	GotIt!	\$525k / Angel	Personal Investment
Dec, 2011	Buffer	\$400k / Angel	Personal Investment
Dec, 2008	Posterous	\$725k / Angel	Personal Investment
May, 2006	FilmLoop	\$7M / Series B	Garage Technology Ventures
Jul, 2005	Simply Hired	\$3M / Series B	Garage Technology Ventures
Feb, 2005	FilmLoop	\$5.6M / Series A	Garage Technology Ventures
Sep, 2004	BitPass	\$11.8M / Series B	Garage Technology Ventures

1.4.1. Social Media – People search

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

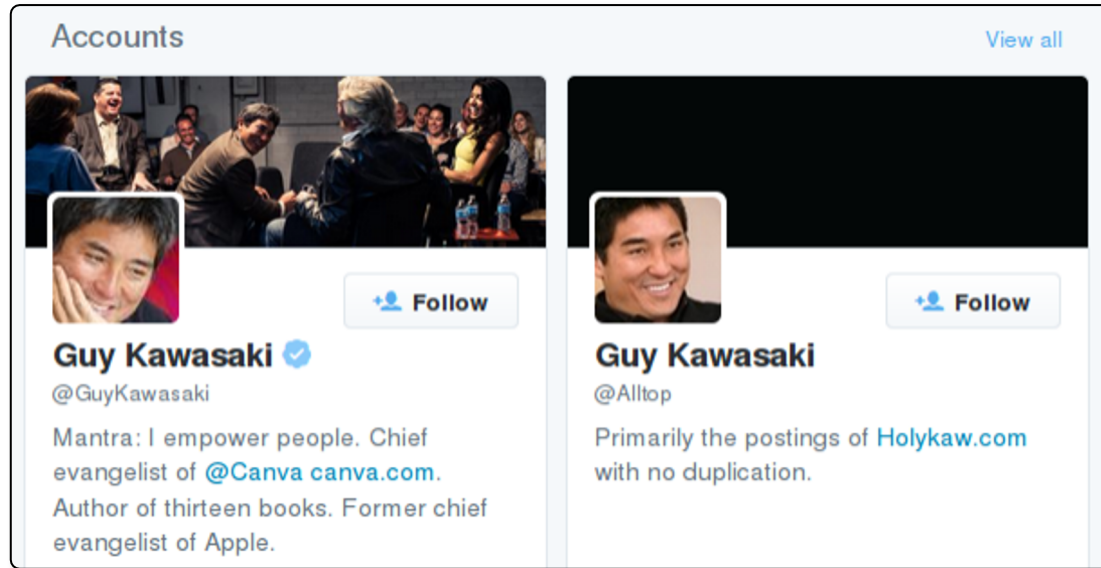
- Age
- Phone Number
- Business
- Addresses
- Occupation
- Interests

+ Further searching will tell us:

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

1.4.1. Social Media – People search

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



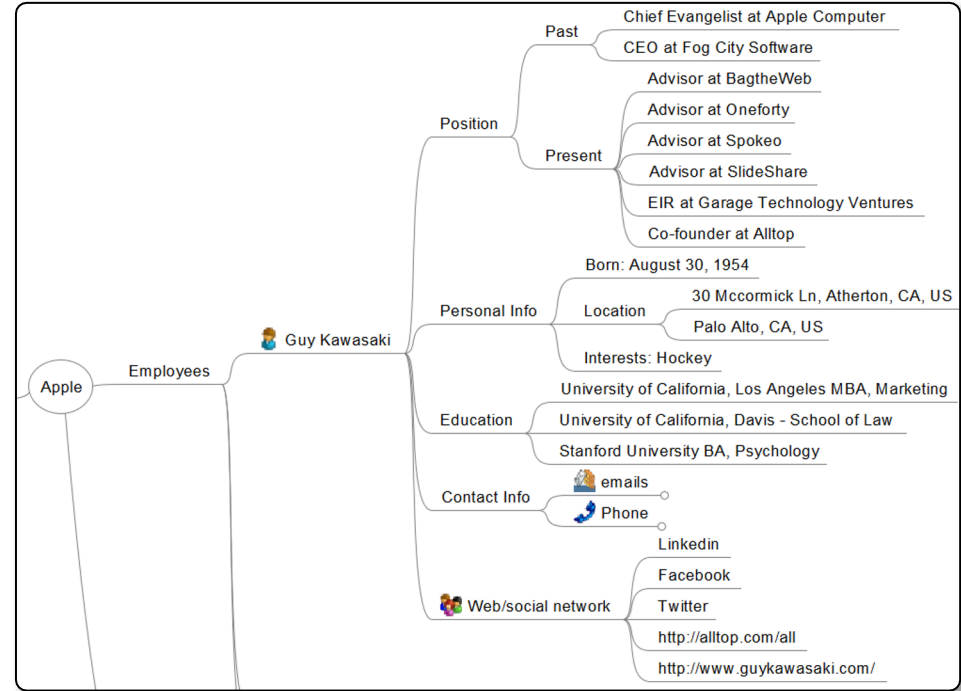
1.4.1. Social Media – People search

- + 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.



1.4.1. 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.

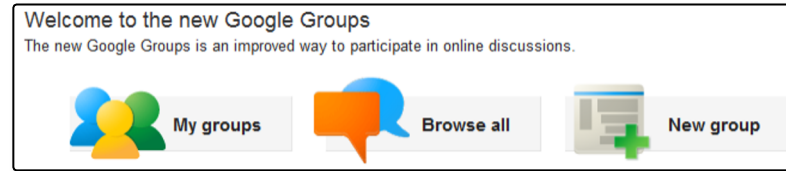


1.4.1. Social Media – People search

- + 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 pentest 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**.

1.4.1. Social Media - USENET

- + 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..

1.4.1. Social Media

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:

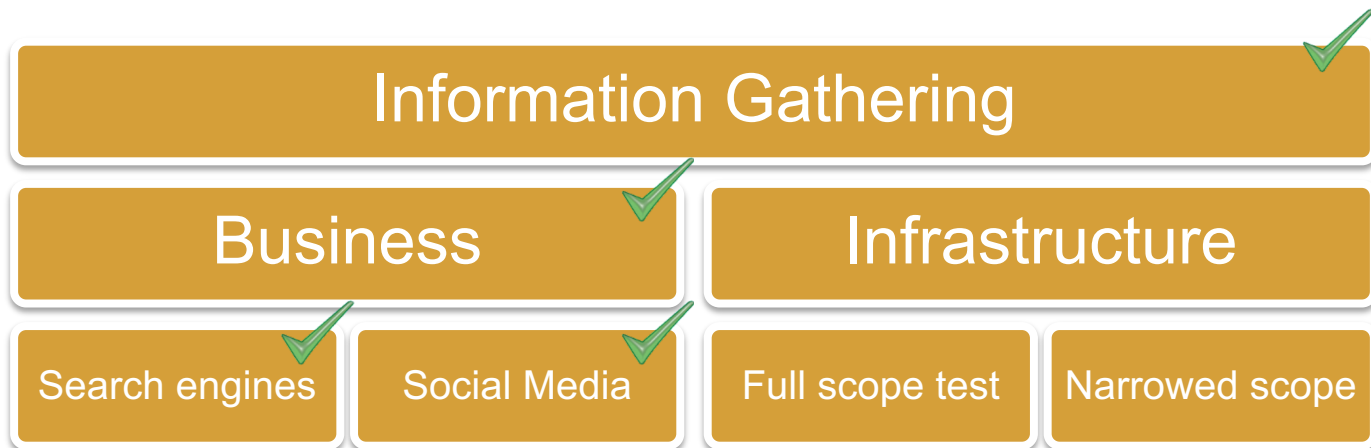
- Company hierarchy
- Personal details about board of directors
 - Email addresses
 - Phone numbers
 - Addresses
 - ...

1.4.1. Social Media

- + 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.

1.4.1. Social Media

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



1.4.1. Social Media

- + 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.

References

+ Pipl: <http://www.pipl.com/>

Q&A



Conclusion Day 1

+ Thank you for joining and see you tomorrow!

Phillip Wylie

Offensive Cyber Security Expert



pwylie@ine.com



[@PhillipWylie](https://twitter.com/PhillipWylie)



<https://www.linkedin.com/in/phillipwylie/>

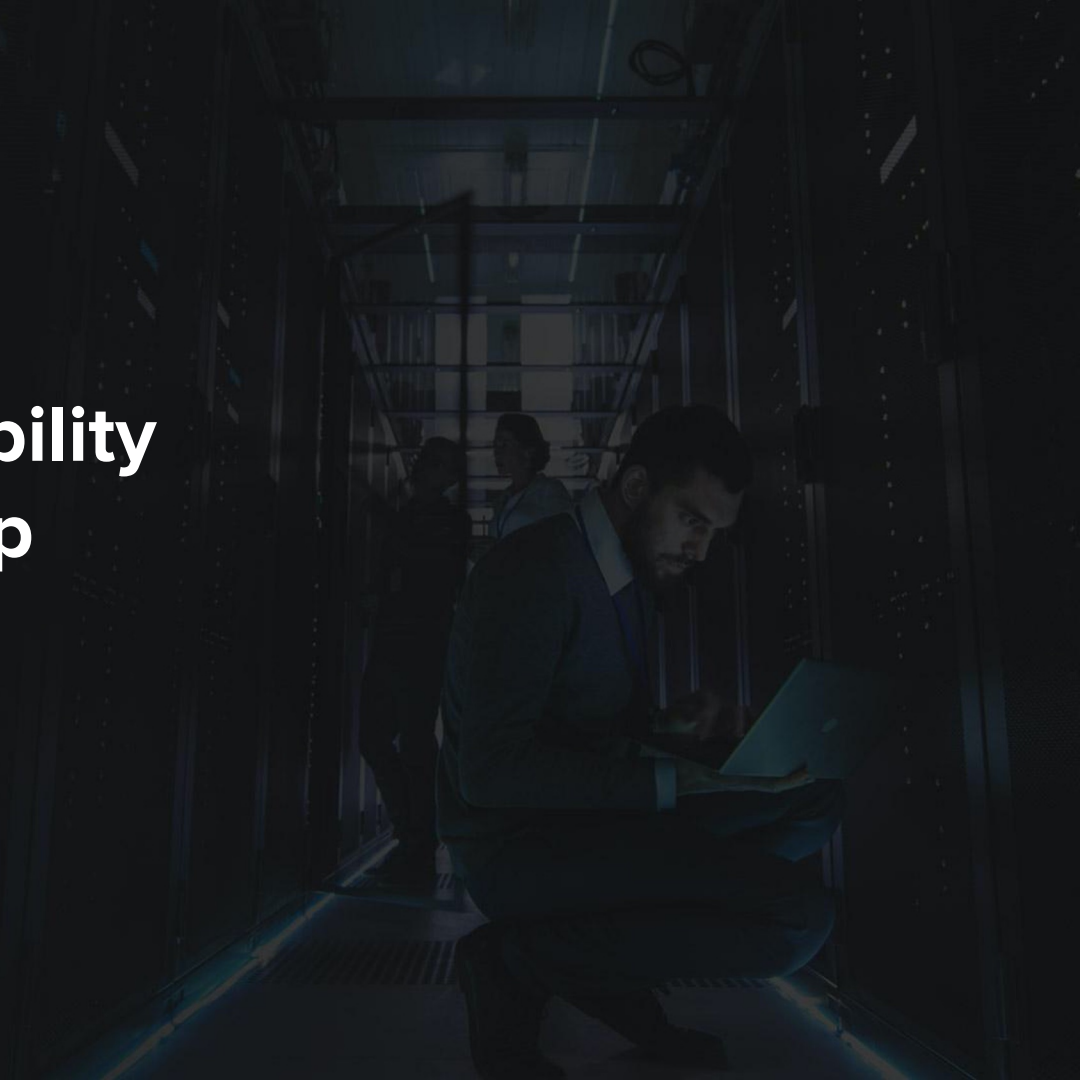




Recon and Vulnerability Detection Bootcamp

Day 2: Active Reconnaissance

ine.com



Active Reconnaissance

Infrastructure

1.5. Infrastructure

- + 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

1.5. Infrastructure

- + 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.

1.5. Infrastructure

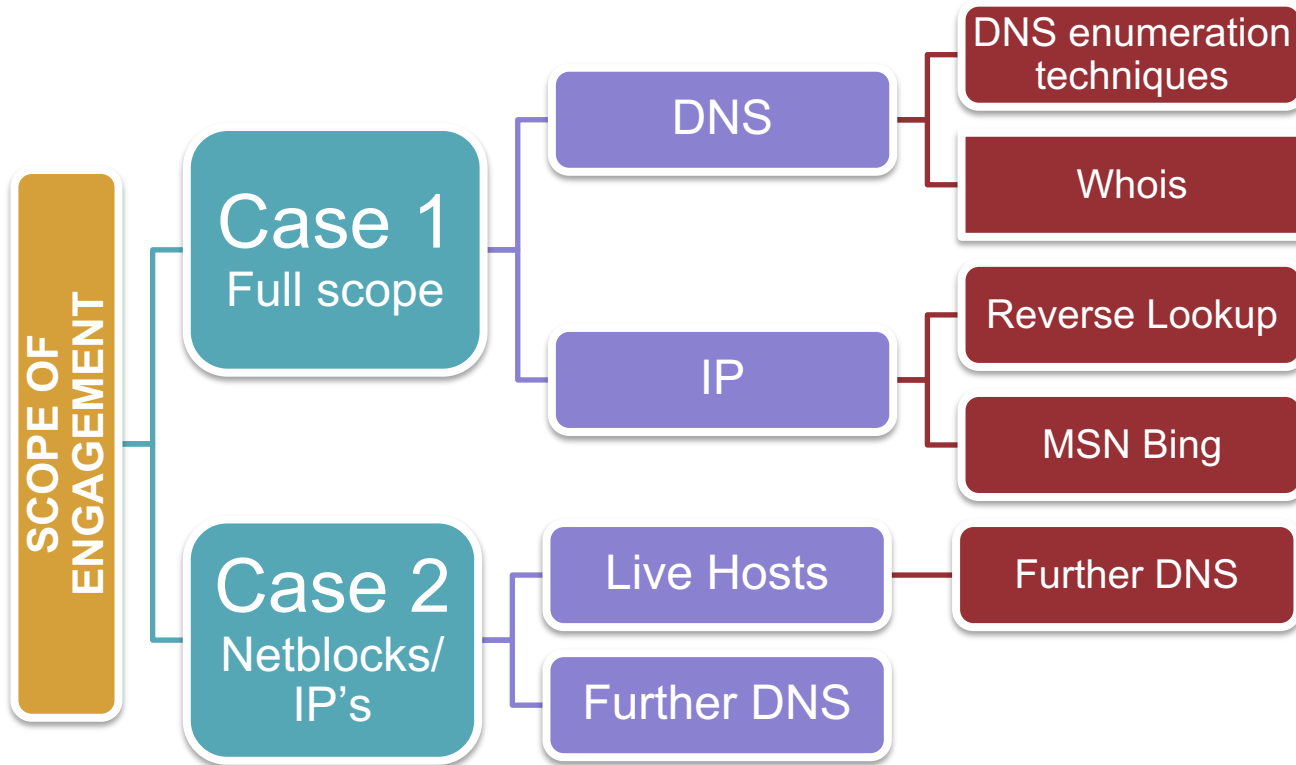
As the Scope of Engagement (SoE) for your penetration test, your customer can give you:

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.

1.5. Infrastructure

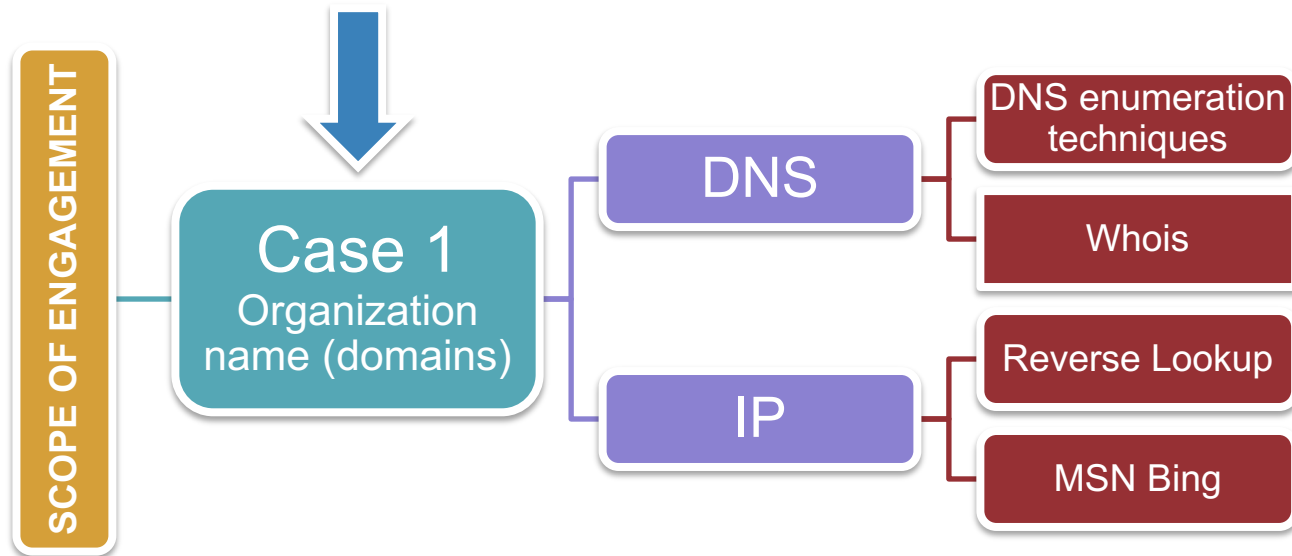


1.5. Infrastructure

- + 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.

1.5.1. Infrastructure – Domains

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



1.5.1. Infrastructure – Domains

- + 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.

1.5.1. Infrastructure – Domains

- + 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.

1.5.1. Infrastructure – Domains

- + **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

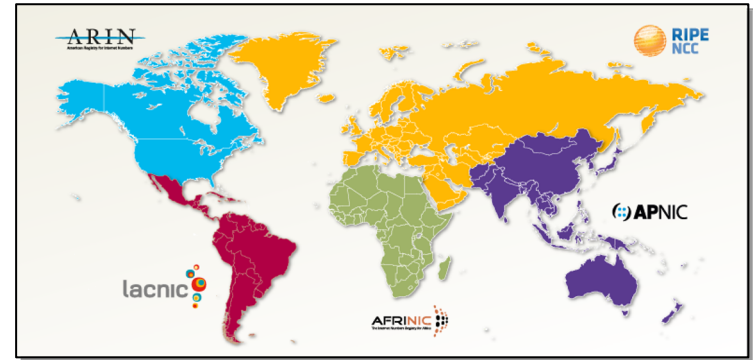
1.5.1. Infrastructure – Domains

- + 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.

1.5.1. Infrastructure – Domains

- + 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



1.5.1. Infrastructure – Domains

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

1.5.1. Infrastructure – Domains

- + 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.
- + 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.).

1.5.1. Infrastructure – Domains

- + 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/>

1.5.1. Infrastructure – Domains

- + Let us see an example of the WHOIS results: (our target domain will be `e1sfoo.com`)

Registrar info

Whois Record for ElearnSecurity.com

— Whois & Quick Stats

Registrant Org	Domains By Proxy, LLC was found in ~11,112,272 other domains	↗
Registrar	GODADDY.COM, LLC	
Registrar Status	clientDeleteProhibited, clientRenewProhibited, clientTransferProhibited, clientUpdateProhibited	
Dates	Created on 2009-03-30 - Expires on 2020-03-30 - Updated on 2015-03-30	↗
Name Server(s)	NS.ELEARNSECURITY.COM (has 3 domains) NS1.ELEARNSECURITY.COM (has 3 domains) NS5.DNSMADEEASY.COM (has 222,771 domains) NS6.DNSMADEEASY.COM (has 222,771 domains) NS7.DNSMADEEASY.COM (has 222,771 domains)	↗
IP Address	199.193.116.231 - 3 other sites hosted on this server	↗
IP Location	🇺🇸 - Florida - Tampa - Noc4hosts Inc.	

Domain servers

Website information

— Website

Website Title	eLearnSecurity - IT Security training courses for individuals and corporations
Server Type	Microsoft-IIS/7.5
Response Code	200
SEO Score	82%
Terms	271 (Unique: 167, Linked: 92)
Images	19 (Alt tags missing: 5)
Links	57 (Internal: 35, Outbound: 20)

1.5.1. Infrastructure – Domains

- + 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.

1.5.1. Infrastructure – Domains

- + Question: what information did we get from WHOIS that can help determine the infrastructure of the organization?
 - + Answer: **Name servers!**
- + These are servers that store all the DNS related information (records) about the domain.

1.5.1.1. DNS Enumeration

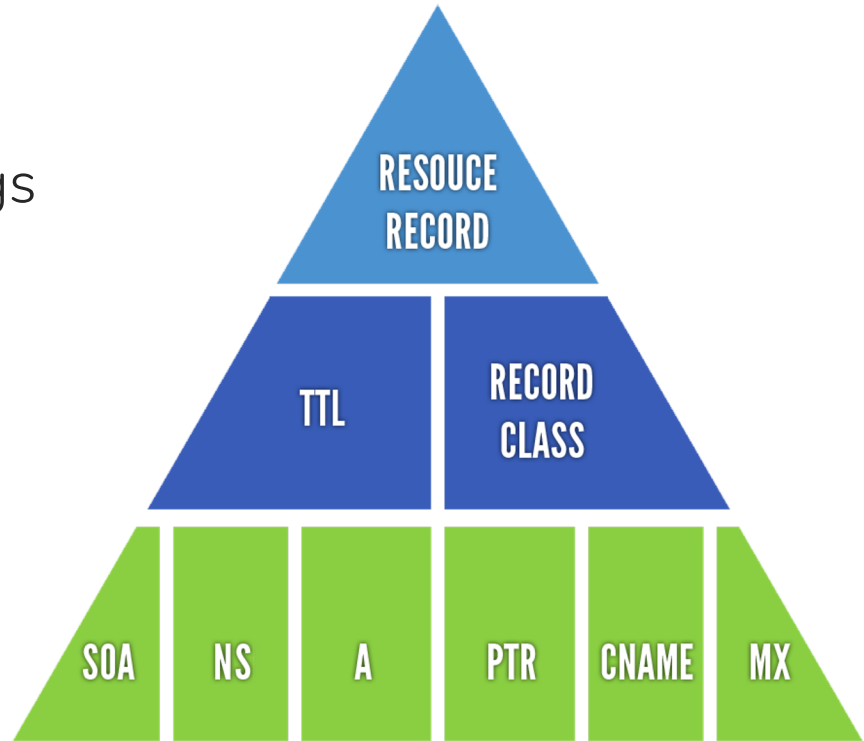
- + Let's now move on in our investigation and start collecting information about the targets' DNS. A **Domain Name System** (DNS) is a distributed database arranged hierarchically. Its purpose is to provide a means to use *hostnames* (like elearnsecurity.com) rather than *IP addresses* (like 199.193.116.231).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

1.5.1.1. DNS Enumeration

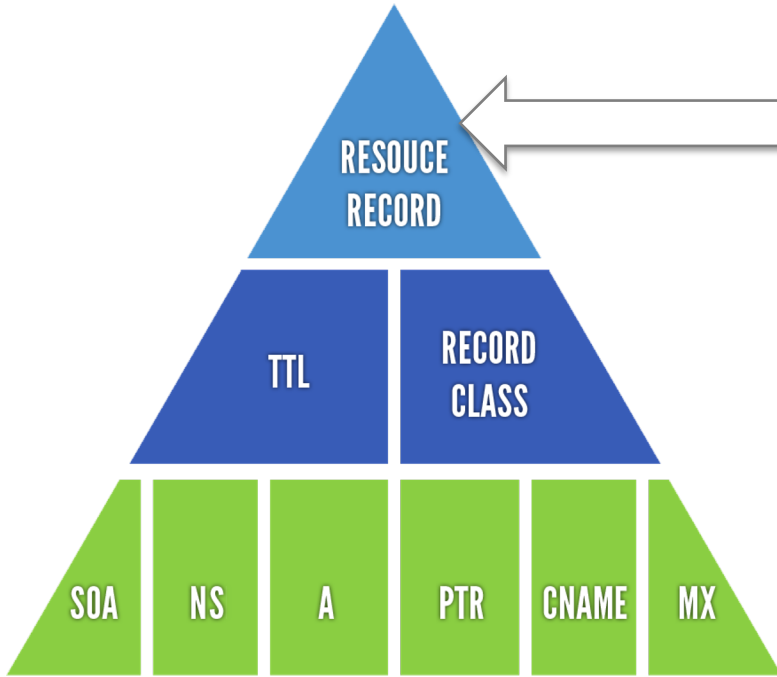
- + DNS servers contain textual records.
- + Each record has a given type, each with a different role.

1.5.1.1.1. DNS Records

- + DNS queries produce listings called Resource Records.
- + This is a representation of Resource Records.

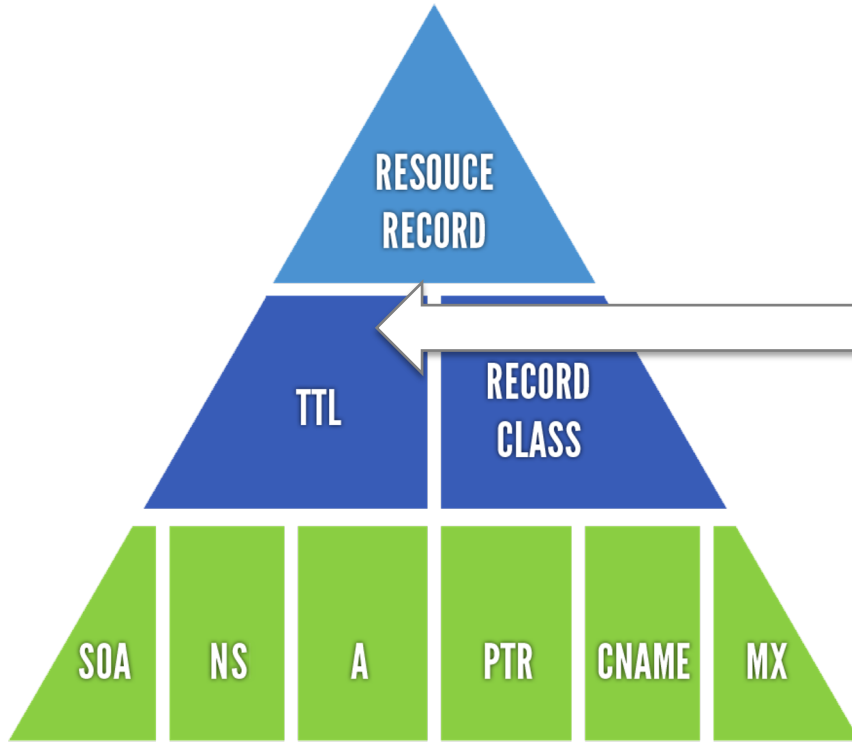


1.5.1.1.1. DNS Records



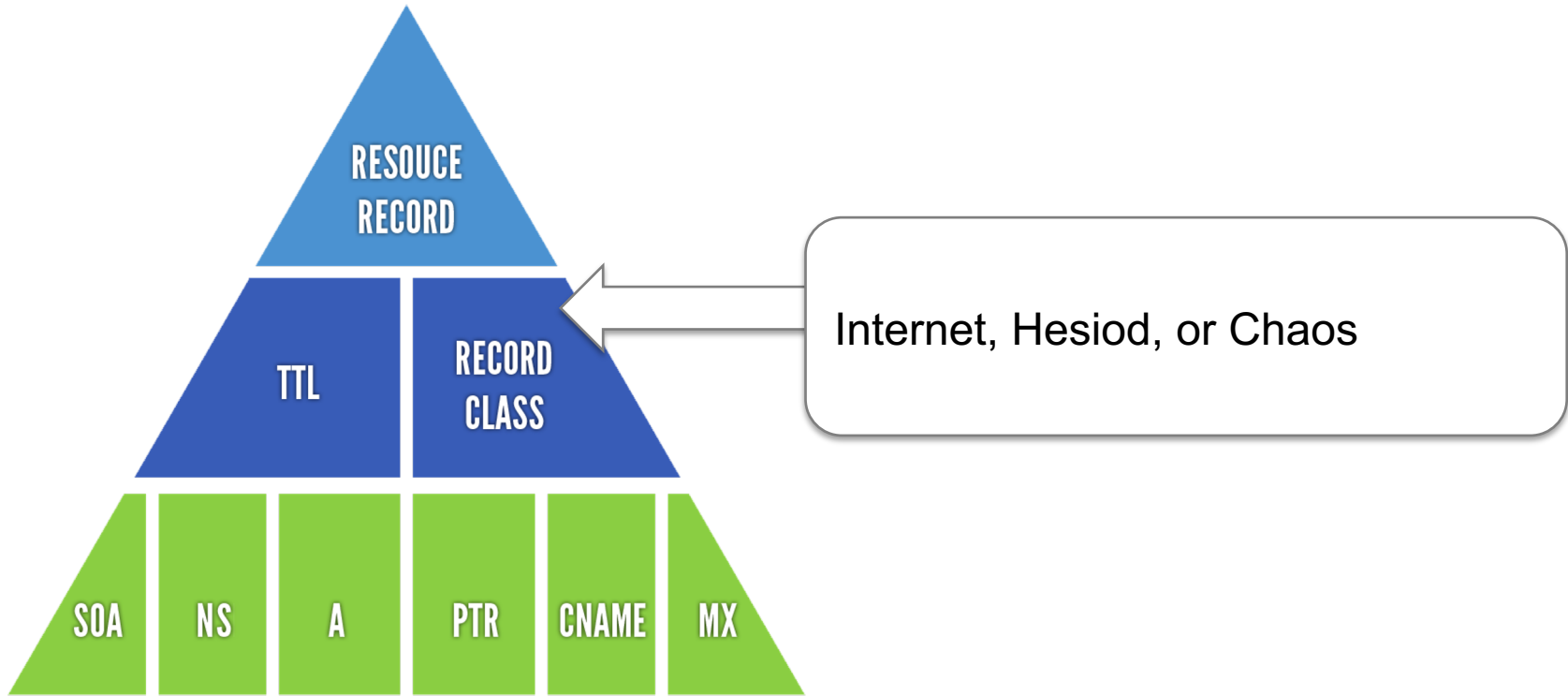
A Resource record starts with a domain name, usually a fully qualified domain name. If anything other than a fully qualified domain name is used, the name of the zone the record is in will automatically be appended to the end of the name.

1.5.1.1.1. DNS Records

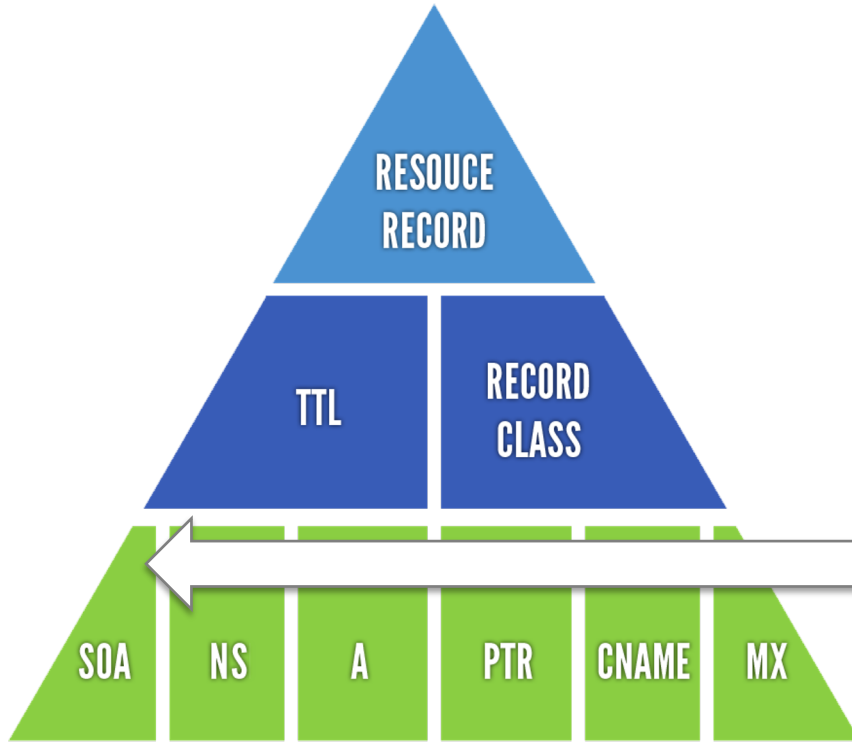


Time-To-Live (TTL), recorded in seconds, defaults to the minimum value determined in the Start of Authority (SOA) record.

1.5.1.1.1. DNS Records



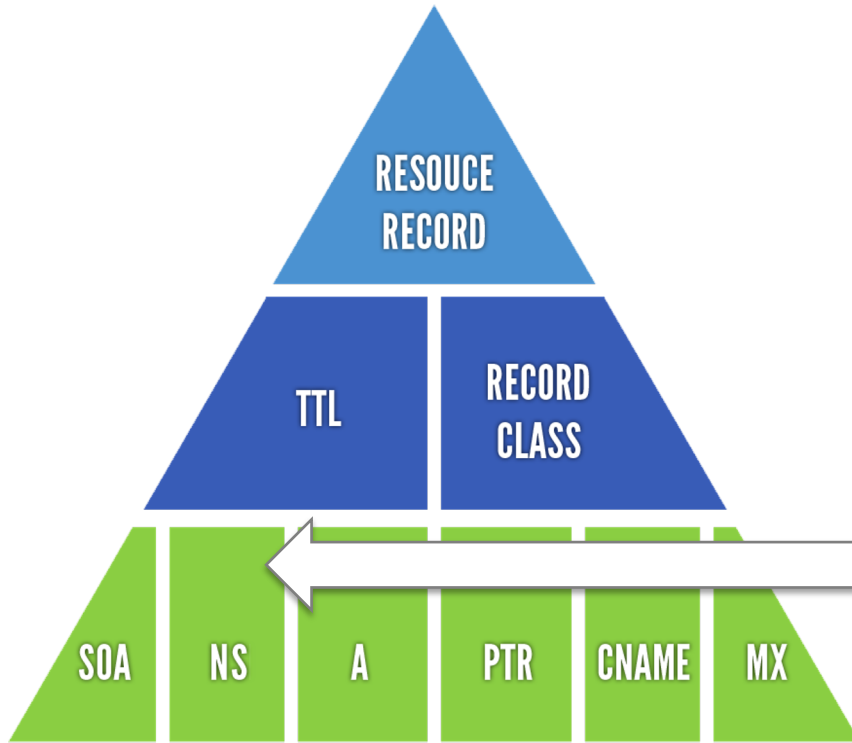
1.5.1.1.1. DNS Records



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

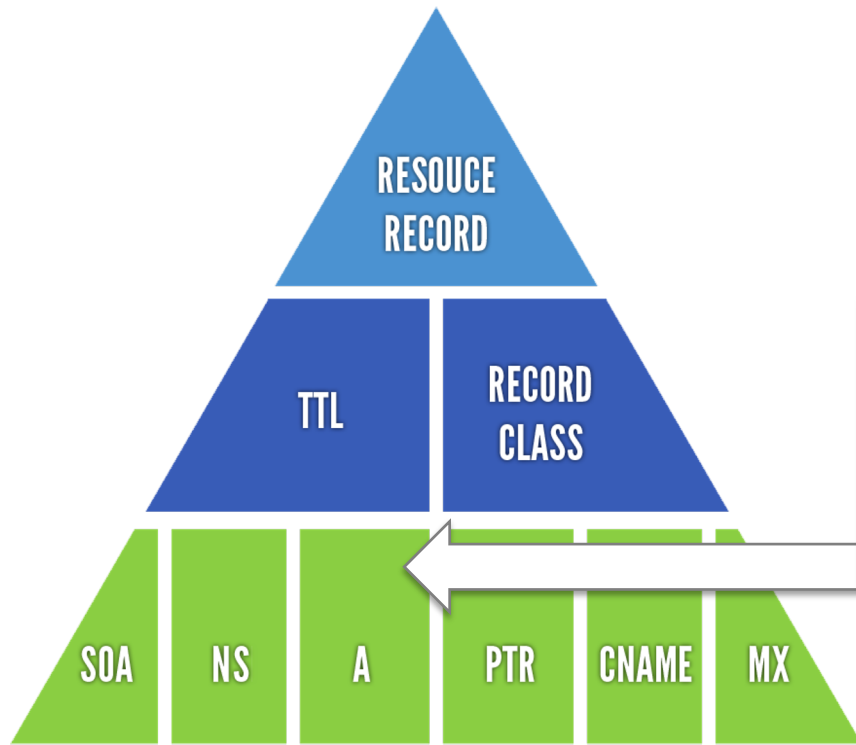
1.5.1.1.1. DNS Records



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.

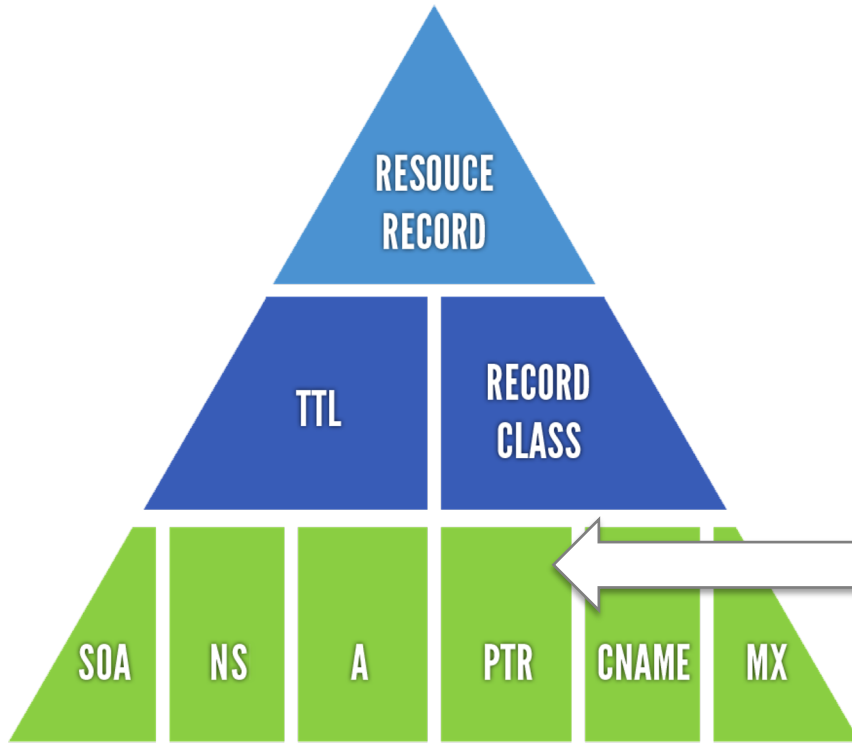
1.5.1.1.1. DNS Records



Address

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

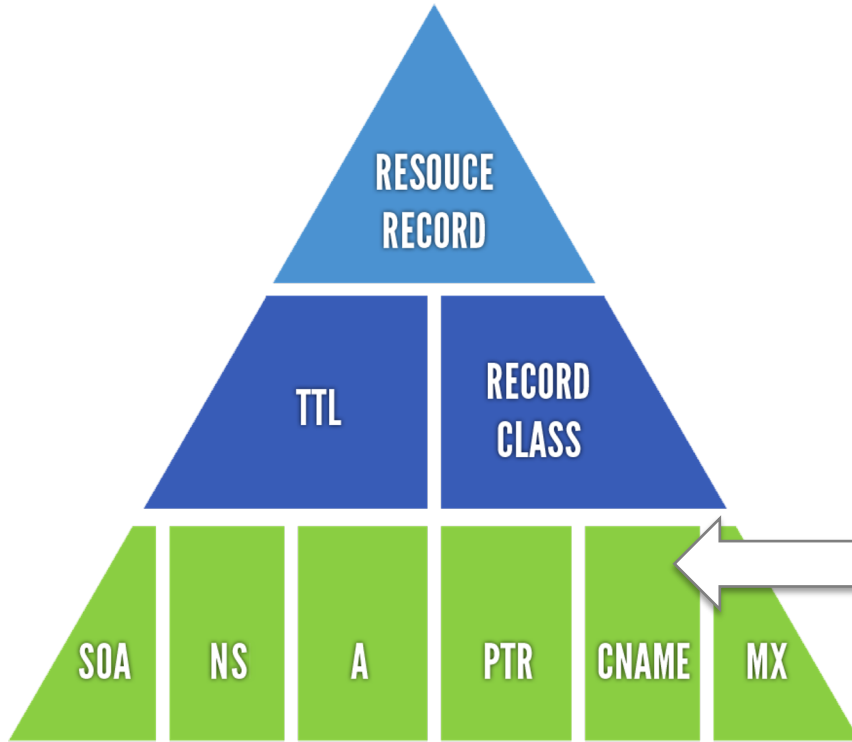
1.5.1.1.1. DNS Records



Pointer

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

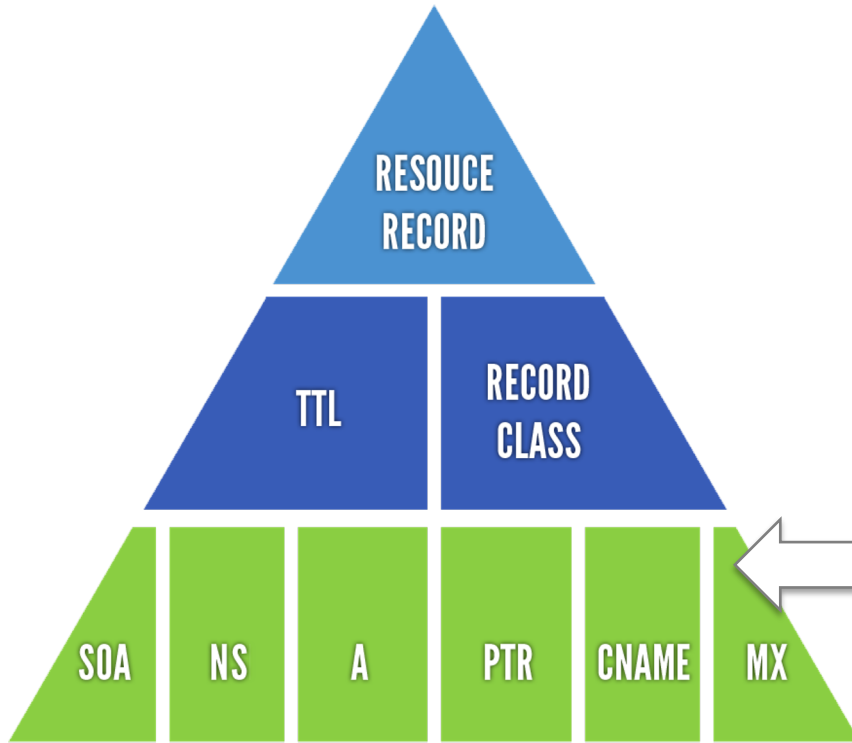
1.5.1.1.1. DNS Records



CNAME

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

1.5.1.1.1. DNS Records



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.

1.5.1.1. DNS Enumeration

- + 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.

1.5.1.1. DNS Enumeration

- + 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

1.5.1.1. DNS Enumeration

- + 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, you can use online tools such as: <http://network-tools.com/nslookup/>
- + Only domains with a PTR record set will respond to the above reverse lookup.

1.5.1.1. DNS Enumeration

- + 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, you can leverage online tools such as:
 - + <http://www.dnsqueries.com/en/>
 - + <http://www.mxtoolbox.com/>

1.5.1.1. DNS Enumeration

- + **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 subdomains of our domain (**A** records).

1.5.1.1. DNS Enumeration

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.

1.5.1.1. DNS Enumeration

- + 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.

1.5.1.1. 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)
```

1.5.1.1. DNS Enumeration

- + 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.

1.5.1.1. 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
```

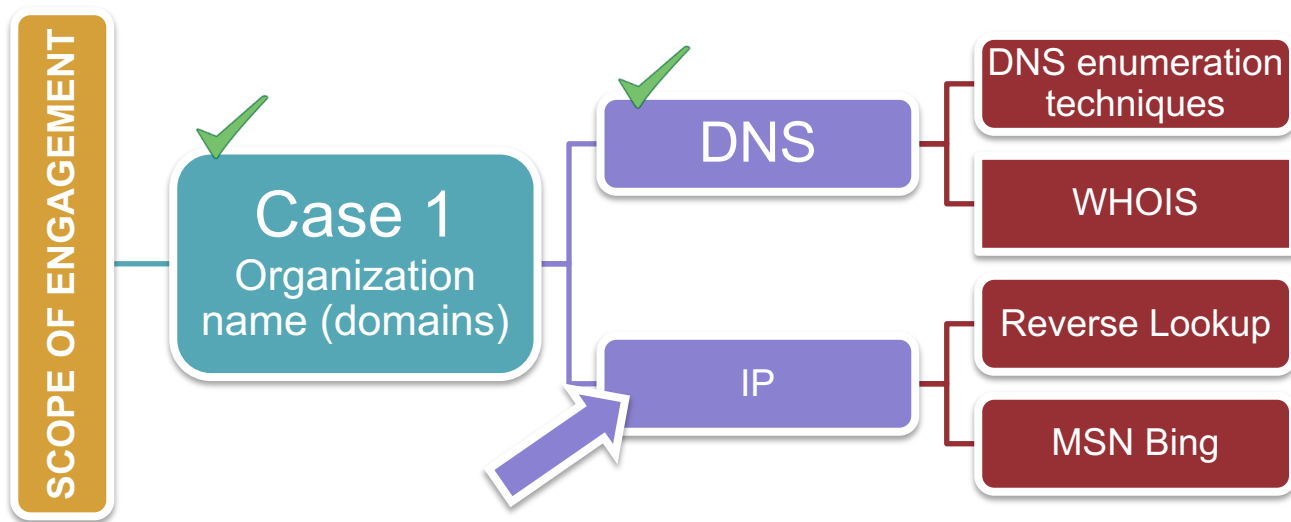
```
dig axfr @target.com target.com
```


1.5.1.1. DNS Enumeration

- + In the video on Information Gathering DNS, we will see how to use these commands in order to obtain as much information as we can about our target.

1.5.1.2. IP

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

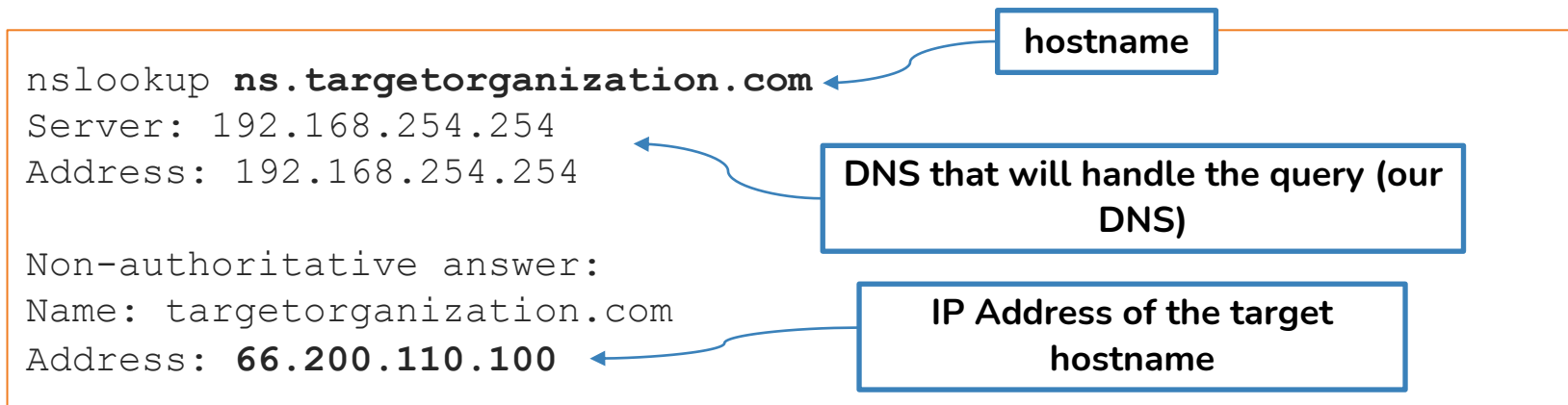


1.5.1.2. IP

- + 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!

1.5.1.2. IP

- + The simplest use of `nslookup` is to perform a lookup of a hostname.
- + This translates the hostname into an IP address.



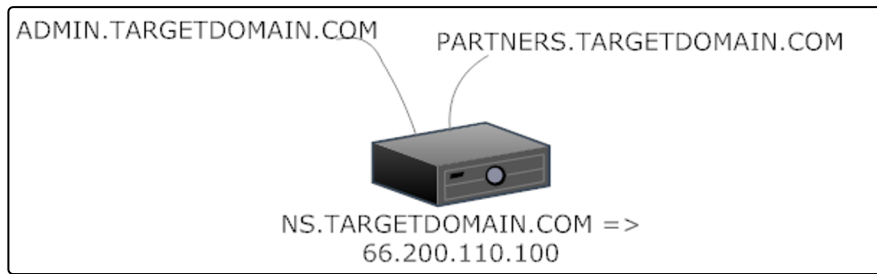
1.5.1.2. IP

- + 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?

1.5.1.2. IP

- + 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 subdomains run on the same web server.

1.5.1.2. IP

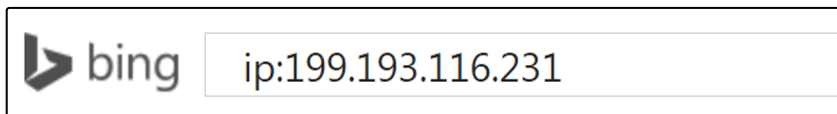


- + For example, you have discovered that the name server of the target organization is on 66.200.110.100. How do you determine other subdomains on the same IP?
- + The first technique to try is a **Reverse lookup**. The second is asking for either Google or Bing's help.

1.5.1.3. MSN Bing

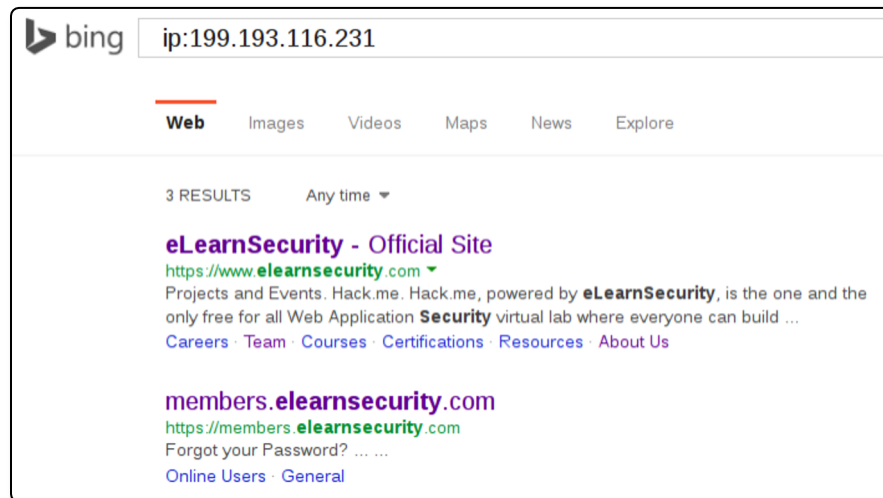
- + Bing offers a query filter that returns all the websites hosted on a given IP address. We just need to use the `ip` filter, followed by the IP address of our target.

```
ip:199.193.116.231
```



1.5.1.3. MSN Bing

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



1.5.1.3. 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:

- [Domaintools](#)
- [DNSlytics](#)
- [Networkappers](#)
- [Robtex](#)

<https://networkappers.com/tools/reverse-ip-checker>
<https://dnslytics.com/reverse-ip>
<http://reverseip.domaintools.com/>
<https://www.robtx.com/>



1.5.1.3. MSN Bing

- + Since we discovered new subdomains, this process might regress our steps back to the previous phases in order to 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.

1.5.1.4. Netblocks & AS

- + 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**

1.5.1.4. Netblocks & AS

- + 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

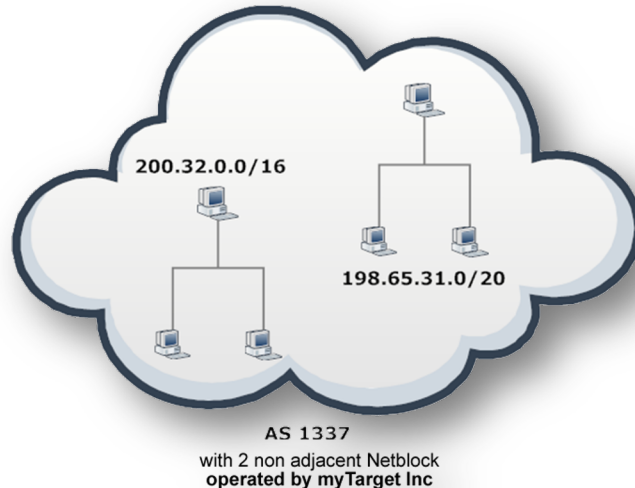
- + This network (netblock) can also be described as follows:
 - 192.168.0.0/16 (CIDR notation)
 - 192.168.0.0 with netmask 255.255.0.0

1.5.1.4. Netblocks & AS

- + 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.

1.5.1.4. Netblocks & AS

- + 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.



1.5.1.4. 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.

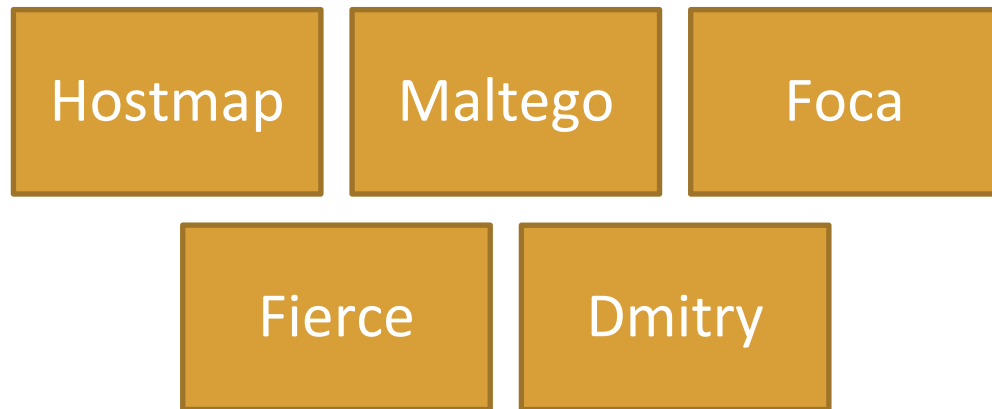
Network	
NetRange	66.200.96.0 - 66.200.111.255
CIDR	66.200.96.0/20
Name	SOLAR-VPS
Handle	NET-66-200-96-0-1
Parent	NET66 (NET-66-0-0-0-0)
Net Type	Direct Allocation
Origin AS	
Organization	Solar VPS (SVL-7)
Registration Date	2007-06-25
Last Updated	2007-06-25
Comments	
RESTful Link	http://whois.arin.net/rest/net/NET-66-200-96-0-1
Function	Point of Contact
Tech	RMB34-ARIN (RMB34-ARIN)
Abuse	RMB34-ARIN (RMB34-ARIN)
NOC	RMB34-ARIN (RMB34-ARIN)

1.5.1.4. Netblocks & AS

- + 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.

1.5.1.4. Netblocks & AS

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



- + Some of these tools will be shown later.

1.5.1.4. Netblocks & AS

- + 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.

1.5.2. Netblocks – IP's

- + We already have a list of IP addresses.
- + The first step is to identify which of those are alive.

1.5.2.1. Live Hosts

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.

1.5.2.1. Live Hosts

- + 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.

1.5.2.1. 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

1.5.2.1. Live Hosts

- + 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.

1.5.2.1. Live Hosts

- + 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.

1.5.2.1. Live Hosts

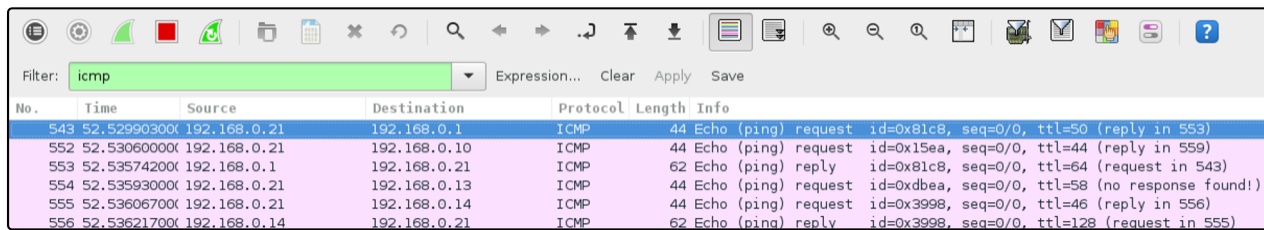
- + In order to perform a host discovery scan, we can use many different techniques however, the most common option is:

```
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.

1.5.2.1. Live Hosts

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



The screenshot shows the Nmap packet capture window with a filter set to 'icmp'. The table below represents the data shown in the window:

No.	Time	Source	Destination	Protocol	Length	Info
543	52.52990300	192.168.0.21	192.168.0.1	ICMP	44	Echo (ping) request id=0x81c8, seq=0/0, ttl=50 (reply in 553)
552	52.53060000	192.168.0.21	192.168.0.10	ICMP	44	Echo (ping) request id=0x15ea, seq=0/0, ttl=44 (reply in 559)
553	52.53574200	192.168.0.1	192.168.0.21	ICMP	62	Echo (ping) reply id=0x81c8, seq=0/0, ttl=64 (request in 543)
554	52.53593000	192.168.0.21	192.168.0.13	ICMP	44	Echo (ping) request id=0xdbea, seq=0/0, ttl=58 (no response found!)
555	52.53606700	192.168.0.21	192.168.0.14	ICMP	44	Echo (ping) request id=0x3998, seq=0/0, ttl=46 (reply in 556)
556	52.53621700	192.168.0.14	192.168.0.21	ICMP	62	Echo (ping) reply id=0x3998, seq=0/0, ttl=128 (request in 555)

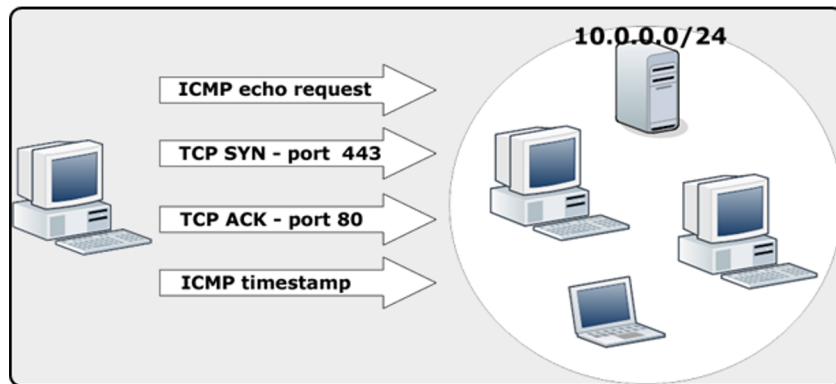
- + Notice that if you run the scan from a machine within the same network, Nmap runs an *ARP scan* instead of sending *ICMP packets*. To avoid this behavior, you can use the `--disable-arp-ping` or `--send-ip` option.

1.5.2.1. Live Hosts

- + 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.

1.5.2.1. Live Hosts

- + 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:



1.5.2.1. Live Hosts

- + 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 video on Host Discovery, we will see both some basic techniques and tools that we can use to discover alive hosts.

1.5.2.2. 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.

1.5.2.2. 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

1.5.2.2. Further DNS

- + 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.

1.5.2.2. Further DNS

- + 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.

1.5.2.3. Maltego

- + 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.

1.5.2.3. Maltego

- + 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, and then build on that information until you have a full map of the entity's entire internet presence.

1.5.2.3. Maltego

- + In the video on Maltego, 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.

References

- + [Better Whois](http://www.betterwhois.com/): <http://www.betterwhois.com/>
- + [dig\(1\): DNS lookup utility – Linux man page](http://linux.die.net/man/1/dig):
<http://linux.die.net/man/1/dig>
- + [DNSlytics – Reverse IP](https://dnslytics.com/reverse-ip): <https://dnslytics.com/reverse-ip>
- + [DNSQUERIES](http://www.dnsqueries.com/en/): <http://www.dnsqueries.com/en/>
- + [DOMAINTOOLS – Reverse IP Lookup](http://reverseip.domaintools.com/): <http://reverseip.domaintools.com/>
- + [fping](http://fping.org/): <http://fping.org/>
- + [Host Discovery](http://nmap.org/book/man-host-discovery.html): <http://nmap.org/book/man-host-discovery.html>
- + [Hurricane Electric BGP Toolkit](http://bgp.he.net/): <http://bgp.he.net/>

References

- + [Online Whois Tool](http://networking.ringofsaturn.com/Tools/whois.php): <http://networking.ringofsaturn.com/Tools/whois.php>
- + [Maltego](https://www.paterva.com/web6/products/maltego.php): <https://www.paterva.com/web6/products/maltego.php>
- + [MX Lookup](http://www.mxtoolbox.com/): <http://www.mxtoolbox.com/>
- + [Networkappers – Reverse IP Domain Checker](https://networkappers.com/tools/reverse-ip-checker):
<https://networkappers.com/tools/reverse-ip-checker>
- + [Nmap](http://nmap.org/): <http://nmap.org/>
- + [Nslookup](https://support.microsoft.com/en-us/kb/200525): <https://support.microsoft.com/en-us/kb/200525>
- + [RFC 3912 – WHOIS Protocol Specification](https://tools.ietf.org/html/rfc3912):
<https://tools.ietf.org/html/rfc3912>
- + [Robtex](https://www.robtex.com/): <https://www.robtex.com/>

References

- + What Is NsLookup? Use Our Online Tool To Query DNS Records:
<http://network-tools.com/nslook/>
- + Whois Lookup, Domain Availability, & IP Search:
<http://whois.domaintools.com/>
- + WHOIS Lookup & Domain Lookup | Network Solutions:
<http://www.networksolutions.com/whois/index.jsp>
- + WHOIS Search, Domain Name, Website, and IP Tools: <http://who.is/>

Tools



1.6. 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.

1.6. Tools

- + 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

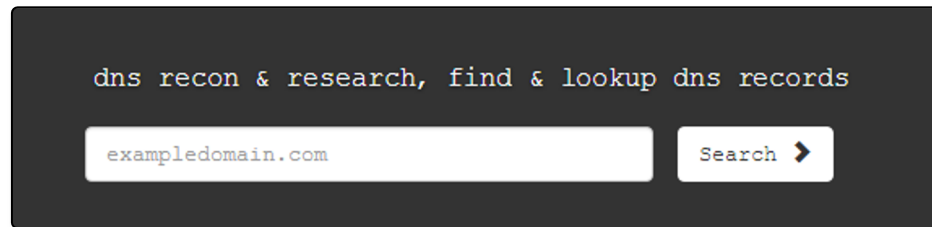
Maltego

Dmitry

Recon-ng

1.6.1. DNSdumpster

- + In the previous slides we have seen many different online tools useful to gather information on our target domain.
[DNSdumpster](https://dnsdumpster.com) 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.



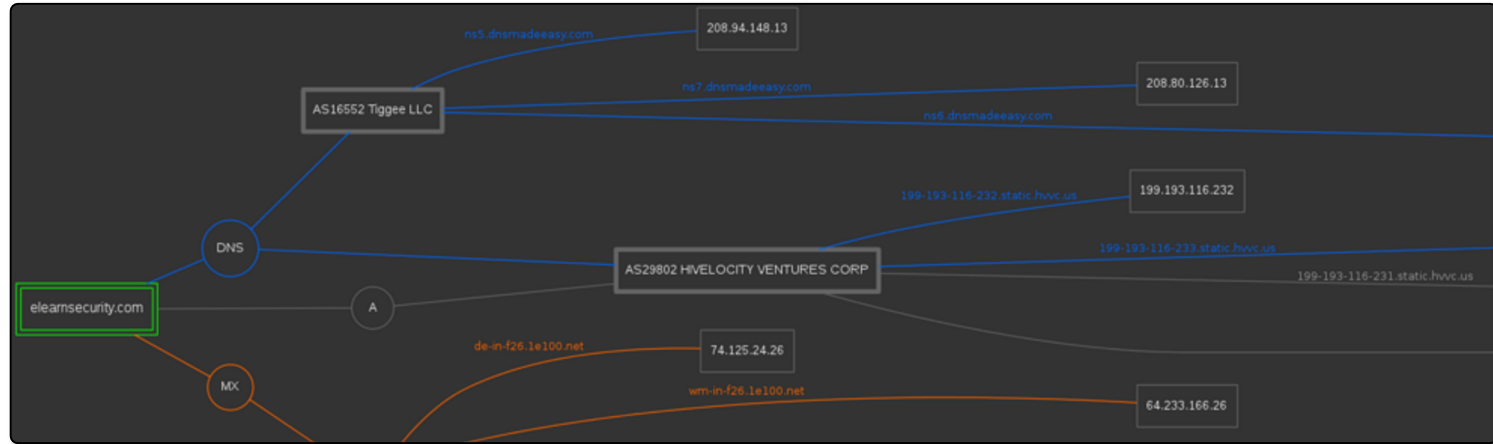
dns recon & research, find & lookup dns records

exampledomain.com

Search >

1.6.1. 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.



1.6.1. DNSdumpster

- + This is a very good tool to start our investigation. Moreover, remember that this tool 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

1.6.2. DNSEnum

- + 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>

1.6.2. 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)
- + Get extra names and subdomains via Google dorks (`allinurl:-www site:domain`)
- + Brute force subdomains from file, can also perform recursion on subdomain 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)

1.6.2. DNSEnum

- + Usage for the tool is :

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

- + Options include the following:

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

1.6.2. DNSEnum

- + 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
```

1.6.2. DNSEnum

- + 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 subdomains.

1.6.2. DNSEnum

- + It is also important to know that `dnsenum` comes with a wordlist file containing the most common DNS and subdomain 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`.

1.6.2. 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 subdomains obtained in the *elsfoosubs.txt*.

1.6.2. DNSEnum

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

1.6.2. DNSEnum

- + 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
```

1.6.3. Dnsmap

- + Although it is a very old tool, **dnsmap** still works great when it comes to subdomain enumeration and brute forcing. You can download it from [github](https://github.com).

1.6.3. Dnsmap

- + Dnsmap uses the primary domain that we provide as a target and then brute forces all the subdomains 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.

1.6.3. Dnsmap

- + 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
```

1.6.3. Dnsmap

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

- `$ dnsmap targetdomain.foo`
 - Example of subdomain brute forcing using dnsmap's built-in word-list
- `$ dnsmap targetdomain.foo -w wordlist.txt`
 - Example of subdomain brute forcing using a user-supplied wordlist
- `$ dnsmap targetdomain.foo -r /tmp/`
 - Example of subdomain 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.

1.6.3. Dnsmap

- + 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.

1.6.4 FOCA and Shodan

- + In the previous slides, we have seen some tools that can help us gather information starting with a simple domain name.
- + In the video on FOCA and Shodan, 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.

1.6.5 Conclusion

- + 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

- + [DNSdumpster](https://dnsdumpster.com/): <https://dnsdumpster.com/>
- + [dnsenum](https://github.com/fwaeytens/dnsenum): <https://github.com/fwaeytens/dnsenum>
- + [dnsmap](https://github.com/makefu/dnsmap): <https://github.com/makefu/dnsmap>
- + [FOCA](https://www.elevenpaths.com/labstools/foca/index.html):
<https://www.elevenpaths.com/labstools/foca/index.html>

Q&A



Conclusion Day 2

+ Thank you for joining and see you tomorrow!

Phillip Wylie

Offensive Cyber Security Expert



pwylie@ine.com



[@PhillipWylie](https://twitter.com/PhillipWylie)



<https://www.linkedin.com/in/phillipwylie/>

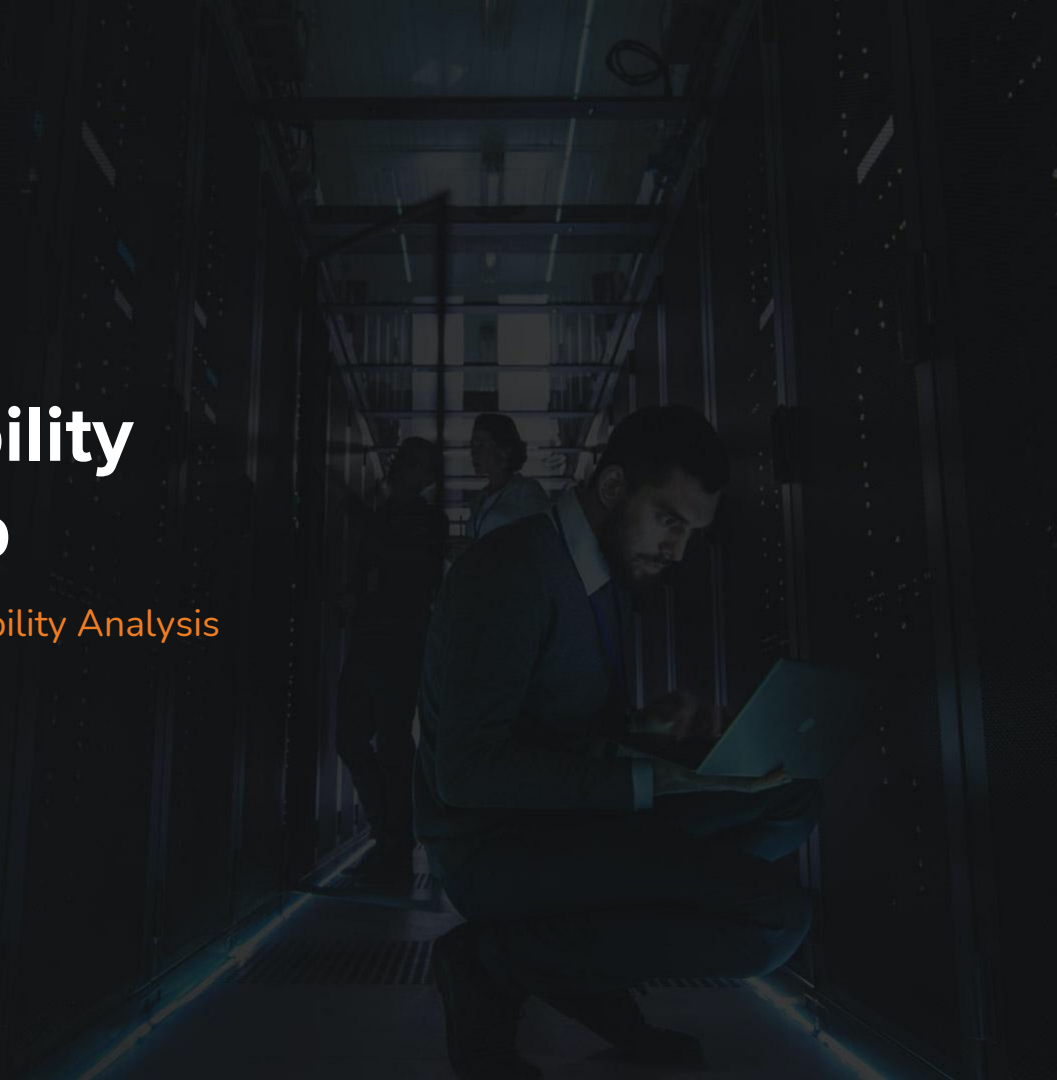




Recon and Vulnerability Detection Bootcamp

Day 3: Footprinting, Scanning, and Vulnerability Analysis

ine.com



Footprinting, Scanning, and Vulnerability Analysis

Footprinting and Scanning

1.7. OS Fingerprinting

- + Fingerprinting the Operating System of a host not only gives you information about the OS running on the system, but also helps you narrow down the number of potential vulnerabilities to check in the next phases.

1.7. OS Fingerprinting

- + There are tools that can make educated guesses about the OS, the version and even the patch level of a remote system.
- + Those tools exploit some singularities you can find in the network stack implementation of every operating system.

1.7.1. Port Scanning

- + After having detected and fingerprinted the live hosts, it's time for **port scanning**!
- + With a scan of live hosts, you can determine which **ports** are open on a remote system; this is a crucial phase of the engagement because any mistake made here will impact the next steps.

1.7.1. Port Scanning

- + Currently, the de facto port scanner is **nmap (network mapper)**.
- + With nmap, a penetration tester can exploit different scanning techniques to reveal open, closed and filtered ports.
- + nmap not only detects TCP/IP port state, it can be used to enumerate applications, services, OS types, and versions.
- + NSE (nmap scripting engine) scripts can be used to enhance the functionality nmap.



1.7.1. Port Scanning

- + **masscan** is another port scanner similar to nmap but has faster scanning capabilities.
- + According to masscan creator Robert Graham, it only takes “6 minutes at around 10 million packets per second” to fully scan the entire Internet.

1.7.2. Service Detection

- + **Service Detection**
- + Knowing just the port is not enough because a system administrator can configure a service to listen to any TCP or UDP port.
- + To detect which service is listening on a port, you can use nmap or other fingerprinting tools.

1.7.2. Service Detection

By knowing the services running on a machine, a penetration tester can infer:

- + The **operating system** and version.
- + The **purpose** of a particular IP address; for example, if it is a server or a client.
- + The **importance** of the host in the client's business. For example, an e-commerce enterprise will heavily rely upon its website and its database servers.

1.7.1. Footprinting and Scanning

Host Discovery

- + Discover live hosts for port and service scans.
- + The **purpose** of a particular IP address; for example, if it is a server or a client.
- + The **importance** of the host in the client's business. For example, an e-commerce enterprise will heavily rely upon its website and its database servers.

Vulnerability Analysis

1.7.2. Vulnerability Analysis

- + After a map of the network infrastructure and the services running on it is built, you can start the vulnerability analysis phase of the pentesting, which is also referred to as a vulnerability assessment.
- + A vulnerability assessment is also a type of security assessment. Think of it as a pentest without the exploitation phase.
- + Vulnerability analysis is made up of scanning and/or manual inspection.

1.7.2. Vulnerability Analysis

- + **Vulnerability Scanners**
- + A **vulnerability scanner** is computer software that is used to discover security flaws due to misconfiguration, missing patches, and software flaws.
- + While Nessus is more widely used, Nexpose by Rapid7, and Qualys are popular alternatives.
- + Nessus and OpenVas offer free versions of their vulnerability scanners.
- + Other types of vulnerability scanners include; web application, and cloud.

1.7.2. Vulnerability Analysis

- + Vulnerability scanners provide scan results, which can be saved as a report, or exported and imported into report writing tools such as Dradis.
- + After your vulnerability scan is complete, validate your findings to make sure they are not false positives.
- + Validation can be done using other scanners, tools, or manual methods.

1.7.2. Vulnerability Analysis

- + Vulnerability scanners are helpful tools for making large scope assessments easier and for discovering low hanging fruit.
- + **Don't rely solely on vulnerability scanners.**
- + Use a variety of tools including other vulnerability scanners.

1.7.3. Exploits

- + Exploit-db
- + searchsploit
- + Nessus scan results
- + Metasploit Framework
- + Vulnerability & Exploit Database
- + CXSecurity



Footprinting, Scanning, and Vulnerability Analysis Exercises

1.7.4. Scanning Lab Exercise

- + <https://my.ine.com/CyberSecurity/courses/6f986ca5/penetration-testing-basics> - **Scanning Lab**

1.7.5. Nessus Installation Exercise

- + Open the Nessus Essentials download page:
<https://www.tenable.com/products/nessus/nessus-essentials>
- + Register for Nessus Essentials download and activation code.
- + Download the 64bit Debian install file:

 **Nessus-8.13.1-debian6_amd64.deb**

Debian 9, 10 / Kali Linux 1, 2017.3, 2018, 2019,
2020 AMD64

- + Install from terminal: **# sudo dpkg -i Nessus*.deb**
- + Start Nessus daemon: **# /etc/init.d/nessusd start**

1.7.5. Nessus Installation Exercise

- + Open Nessus URL in browser: <https://localhost:8834>
- + Ignore security warning from self-signed certificate.
- + Select “Nessus Essentials” install option.
- + Enter activation code received in your email.

1.7.5. Nessus Lab

- + <https://my.ine.com/CyberSecurity/courses/6f986ca5/penetration-testing-basics> - **Nessus Lab**

References

- + <https://nmap.org>
- + <https://github.com/robertdavidgraham/masscan>
- + <https://tenable.com>
- + <https://www.rapid7.com/products/nexpose/>
- + <https://www.qualys.com>
- + <https://www.openvas.org>
- + <https://www.exploit-db.com/searchsploit>
- + <https://www.rapid7.com/db/>
- + <https://cxsecurity.com/exploit/>

Q&A



Conclusion Day 3 and Bootcamp

- + Thank you for joining and we hope to see you in future bootcamps!

Phillip Wylie

Offensive Cyber Security Expert



pwylie@ine.com



[@PhillipWylie](https://twitter.com/PhillipWylie)



<https://www.linkedin.com/in/phillipwylie/>

