v4

Penetration Testing Student

Information Gathering

Section 03 |Module 01

Table of Contents

Learning Objectives

By the end of this module, you should have a better understanding of:

- ✓ What OSINT is
- ✓ Basic techniques of collecting information about your target

1.1

Introduction

1.1 Introduction

Welcome to the **penetration testing** section of the course!

We start this module off by discussing all the phases of a penetration test, focusing on **tools, techniques, and methodologies** used by professionals to carry out a penetration test engagement.

1.1 Introduction

Information Gathering is the first and one of the most crucial phases of an engagement.

As you have already seen in the prerequisites section, this step of the process helps you understand the target organization, widen the attack surface and mount efficient and targeted attacks.

1.1 Introduction

Similarly to a black hat hacker, a penetration tester cannot leave any stone unturned.

In this module, you will see how to use public information to get a deeper understanding of the client's organization under the business and infrastructural point of view.

1.2

Open-Source Intelligence

1.2 Open-Source Intelligence

How does this support my pentesting career?

- Widening the attack surface
- Mounting targeted attacks
- Sharpening your tools in preparation for the next phases

1.2 Open-Source Intelligence

Until a few years ago, collecting information about a company involved:

- Getting information from the press
- Looking for addresses and phone numbers in the phone directory
- Visiting the company web site to get information about systems and products

1.2 Open-Source Intelligence

Nowadays, you can do the same thing more efficiently by exploiting information available on **social networks**, **public sites** and by **visiting the company websites**.

1.2.1 Social Networks Information Gathering

In the following slides, you will see how to use social networks to perform information gathering. In fact, many successful security breaches exploit the weakest link in the security chain: **humans!**

Every day, people get to work and actively use corporate systems and services, so their personal security posture on the Internet heavily influences the security of the companies they work for.

1.2.1 Social Networks Information Gathering

With the advent of social networks, hackers can now access information on people and products which were very hard to find only a few years ago.

Criminals can (and actually do) now exploit this valuable information to mount **sophisticated attacks**.

1.2.1 Social Networks Information Gathering

When the employees of a company post information about current projects, trips to conferences, phone numbers, and email addresses on social networks, they are actually giving out a goldmine to criminals.

This not only helps criminals in mounting phishing and impersonation attacks but also gives them the means to create a **technical** map of the **systems and technologies** used by the company.

1.2.1 Social Networks Information Gathering

You, as a professional penetration tester can do the same, by performing queries on common social networks like *Facebook, Twitter, LinkedIn, Google+* and so on.

Given the vast array of social networks out there, choosing the right ones for your engagement depends on the specific client and engagement.

1.2.1 Social Networks Information Gathering

While LinkedIn, Twitter, and Facebook are good in terms of a “general purpose" shot, you have to choose between other social networks by understanding not only the target company industry but also some of the interests of its employees.

Example:

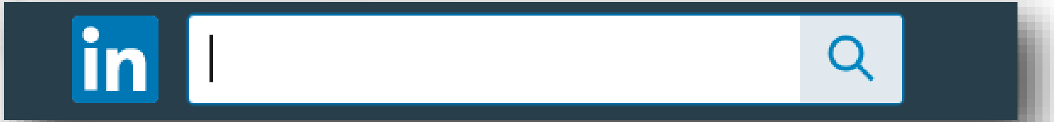
If the client is an advertising company, checking *Instagram* would be a great idea.

EXAMPLE

1.2.1.1 LinkedIn Example

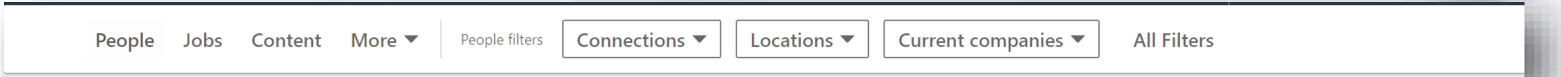
Let’s now see how to use LinkedIn's advanced search to find all Google’s employees in the US.

After logging in, you can open the advanced search by clicking on the magnifying glass icon on the right of the search bar.

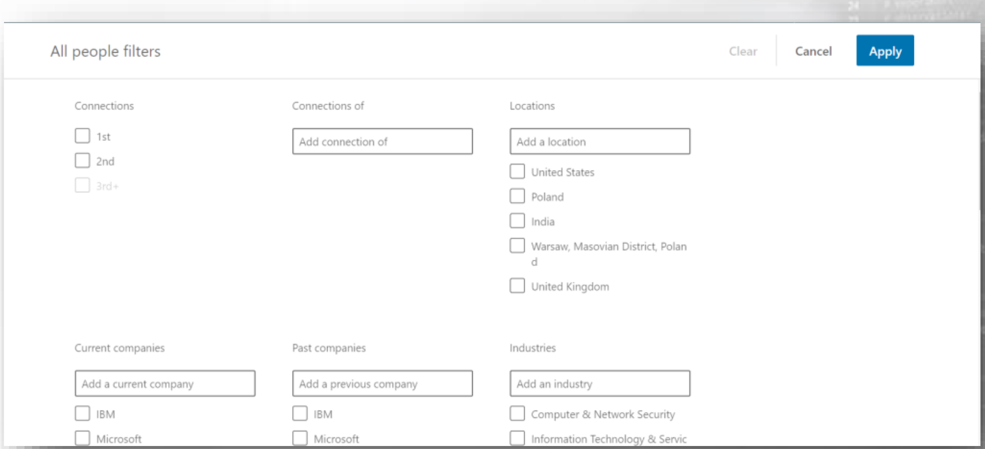


1.2.1.1 LinkedIn Example

Then, the additional search bar appears at the bottom:



If you choose *“All Filters”*, you will notice that even more search criteria appears:


All people filters

Clear Cancel Apply

Connections

□ 1st
□ 2nd
□ 3rd+

Connections of

Add connection of

Locations

Add a location

□ United States
□ Poland
□ India
□ Warsaw, Masovian District, Poland
□ United Kingdom

Current companies

Add a current company

□ IBM
□ Microsoft

Past companies

Add a previous company

□ IBM
□ Microsoft

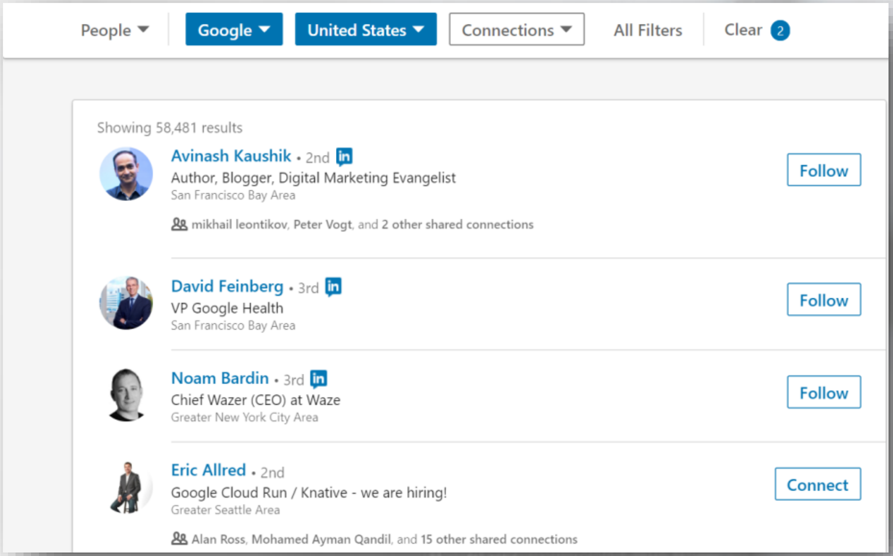
Industries

Add an industry

□ Computer & Network Security
□ Information Technology & Servic

1.2.1.1 LinkedIn Example

The search will eventually return hundreds of profiles to help you deepen your knowledge of the target company.



Showing 58,481 results

Avinash Kaushik • 2nd in
Author, Blogger, Digital Marketing Evangelist
San Francisco Bay Area
mikhail leontikov, Peter Vogt, and 2 other shared connections

David Feinberg • 3rd in
VP Google Health
San Francisco Bay Area

Noam Bardin • 3rd in
Chief Wazer (CEO) at Waze
Greater New York City Area

Eric Allred • 2nd
Google Cloud Run / Knative - we are hiring!
Greater Seattle Area
Alan Ross, Mohamed Ayman Qandil, and 15 other shared connections

1.2.1.1 LinkedIn Example

Many LinkedIn users also provide personal and work **phone numbers or email addresses** that can be exploited to mount a social engineering attack.

1.2.1.2 Linked Social Network Profiles

Many social networks allow users to **integrate** different accounts.

For example, you can link your Twitter and LinkedIn account; this feature automatically posts an update on a social network to others and can be exploited to **find missing information**.

EXAMPLE

1.2.1.2 Linked Social Network Profiles

You can find the **real name** of the person owning a **Twitter** account by performing a **web search** on LinkedIn, looking for matching updates.

LinkedIn forces its users to use their real name.

1.2.2 Public Sites Information Gathering

Social networks are not the only public source of information about companies. There are also many other interesting websites and databases that “leak” valuable information.

Let’s check some out!

1.2.2.1 Crunch Base

CrunchBase is an IT startup database where you can find detailed information about founders, investors, employees, buyouts, and acquisitions.

You can perform lookups by company name or people names.

http://www.crunchbase.com/

1.2.2.2 Government Sites

On the Internet, you can get a wide array of information about companies that have worked with a government or are currently working with one.

The information stored on those sites is different from government to government and from state to state.

EXAMPLE

1.2.2.2 Government Sites

For instance, the USA government provides the System for Award Management (SAM) and the GSA eLibrary which you can use to find information about contracts between private companies and the US Government.

https://www.sam.gov/
http://www.gsaelibrary.gsa.gov/

1.2.3 Whois

Another precious resource is the Whois database. You can use it to get information such as:

- Owner name
- Street addresses
- Email Address
- Technical contacts

regarding an Internet domain name.

1.2.3 Whois

You can query the database by using the `whois` command on Linux and OSX.

If you are running MS Windows, you can install the Sysinternal's Whois.

http://technet.microsoft.com/en-us/sysinternals/bb897435.aspx

EXAMPLE

1.2.3.1 Whois Example

Here we see some of the information you can get by performing a *whois* lookup for apple.com.

```
$ whois apple.com

Domain Name: apple.com
Registry Registrant ID:
Registrant Name: Domain Administrator
Registrant Organization: Apple Inc.
Registrant Street: 1 Infinite Loop
Registrant City: Cupertino
Registrant State/Province: CA
Registrant Postal Code: 95014
Registrant Country: US
Registrant Phone: +1.4089961010
Registrant Phone Ext:
Registrant Fax: +1.4089741560
Registrant Fax Ext:
Registrant Email: domains@apple.com
```

1.2.3.1 Whois Example

You can also find technical contacts.

```
Registry Admin ID:
Admin Name: Domain Administrator
Admin Organization: Apple Inc.
Admin Street: 1 Infinite Loop
Admin City: Cupertino
Admin State/Province: CA
Admin Postal Code: 95014
Admin Country: US
Admin Phone: +1.4089961010
Admin Phone Ext:
Admin Fax: +1.4089741560
Admin Fax Ext:
Admin Email: domains@apple.com
```

1.2.4 Browsing Client's Sites

Social networks, public sites and the *whois* services each give you fragmented information that you can put together to better understand your client's business.

1.2.4 Browsing Client's Sites

Finally, don’t forget that **browsing your client's actual websites** will give you plenty of information about:

- Products
- Services
- Technologies
- Company culture

1.2.4 Browsing Client's Sites

Many companies websites contain information about the board of directors profiles, current and future products, partners, suppliers, job vacancies and so on.

The more you know your target, the easier the later phases of your pentest will be.

1.2.5 Discovering Email Pattern

In case there is not a direct database or any other source of company emails, which often also works as logins to corporate services, you might want to try to identify them yourself.

1.2.5 Discovering Email Pattern

You should keep in mind, that companies tend to use one certain email schema for every employee; this makes internal communication of a company much easier.

1.2.5 Discovering Email Pattern

Usually, there is no complicated pattern. The structure of an email address should be intuitive, so other employees can easily communicate with each other by just knowing their co-worker name and/or surname.

Below are some examples of typical corporate email address format:

- **name.surname@company.com**
- **surname.name@company.com**
- **[first letter of name]surname@company.com**

1.2.5 Discovering Email Pattern

If you are able to find a company’s employees (i.e., using their official website, LinkedIn, or other social networking sites), you might be able to guess their email address.

1.2.5 Discovering Email Pattern

Many mail systems tend to inform the sender that mail was not delivered because it does not exist.

This is an excellent opportunity for a penetration tester to guess corporate email formats.

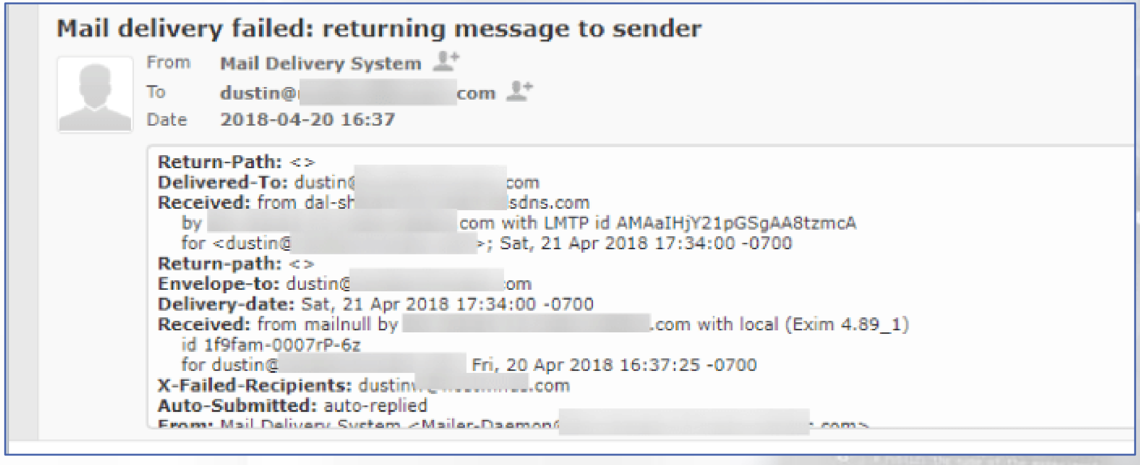
1.2.5 Discovering Email Pattern

You can try to first:

- Collect a reasonable number of employee data (name/surname)
- Try to construct a few possible email formats and apply them to each name/surname pair
- Try to send an email that does not alert potential victims (e.g., do not put a „phishing test" in subject, but choose something tricky like try to pretend it is just an advertisement)

1.2.5 Discovering Email Pattern

If you start to receive similar emails to the one below:



Mail delivery failed: returning message to sender

From Mail Delivery System
To dustin@[redacted]com
Date 2018-04-20 16:37

```
Return-Path: <>
Delivered-To: dustin@[redacted]com
Received: from dal-sh[redacted]sdns.com
   by [redacted]com with LMTP id AMAaIHjY21pGSgAA8tzmcA
   for <dustin@[redacted]>; Sat, 21 Apr 2018 17:34:00 -0700
Return-path: <>
Envelope-to: dustin@[redacted]om
Delivery-date: Sat, 21 Apr 2018 17:34:00 -0700
Received: from mailnull by [redacted].com with local (Exim 4.89_1)
   id 1f9fam-0007rP-6z
   for dustin@[redacted] Fri, 20 Apr 2018 16:37:25 -0700
X-Failed-Recipients: dustin[redacted].com
Auto-Submitted: auto-replied
From: Mail Delivery System <Mailer-Daemon@[redacted].com>
```

You should carefully inspect which of your sent emails did not generate such a message, which will be the one that will have the correct corporate mail schema.

Image Source: https://i1.wp.com/www.dbuggers.com/wp-content/uploads/2018/10/Mail-Delivery-Failed.png?resize=696%2C277&ssl=1

1.3

Subdomain Enumeration

1.3 Subdomain Enumeration

We have previously talked about widening the attack surface. An additional way to do so is by discovering as many websites owned by the company as possible.

1.3 Subdomain Enumeration

It's common for websites of the same company to share the same top level domain name. For example, careers.company.com, mail.company.com or business.company.com

Through subdomain enumeration a penetration tester can possibly identify additional resources of a target.

1.3 Subdomain Enumeration

It is very likely that such resources may contain outdated, buggy software, sensitive information, or even administrative interfaces that are not secured.

If you take a look at some bug bounty program writeups, you can quickly conclude that such forgotten resources are something common even in prestigious companies.

1.3 Subdomain Enumeration

In this course, we will focus on passive subdomain enumeration.

This means that we will try to identify subdomains without directly interacting with the target, but through open sources.

1.3 Subdomain Enumeration

Such an open source, can be a search engine.

For example, while Google is performing its indexing activities, it may index pages that were not meant for indexing. A penetration tester can leverage this to passively identify **some** target subdomains.

You can try this by typing the following in Google's search engine

site: company.com

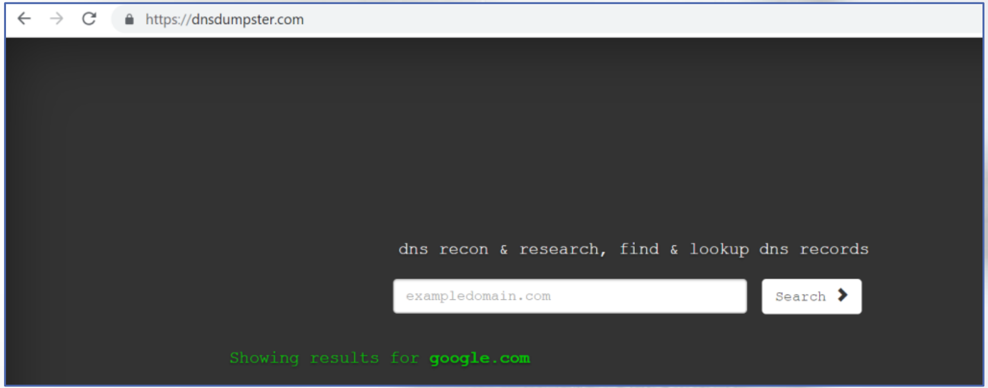
1.3 Subdomain Enumeration

Another open source that can facilitate passive subdomain enumeration is dnsdumpster.com, that utilizes data from google-indexed subdomains, but also checks sites like Bing or virustotal for similar information.

https://dnsdumpster.com/

1.3 Subdomain Enumeration

By typing in the main company domain, you will be presented with any subdomains found for this company.



Showing results for **google.com**

1.3 Subdomain Enumeration

There is also a tool that extends the capabilities of DNS enumeration, called **sublist3r**.

It is pre-installed on the latest Kali Linux version but can be downloaded from its github repository as well.

https://github.com/aboul3la/Sublist3r

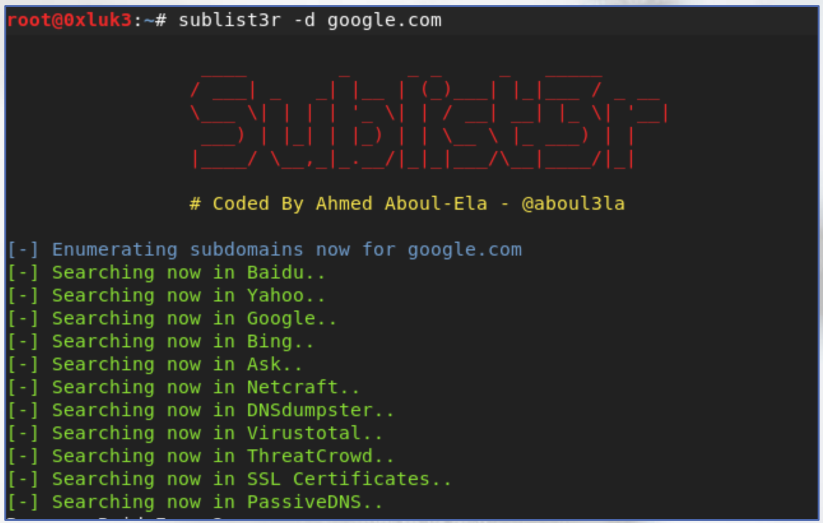
1.3 Subdomain Enumeration

In its basic usage, sublist3r will collect DNS data from various sources.

However, you should be aware that it is easily blocked by Google (its search engine does not like automated tools). For this reason, you should use it wisely.

1.3 Subdomain Enumeration

After running sublist3r with the **–d [domain]** flag, it starts searching for subdomains in various sources.



```
root@0xluk3:~# sublist3r -d google.com

                 ____        _     _ _     _   _____
                / ___| _   _| |__ | (_)___| |_|___ / _ __
                \___ \| | | | '_ \| | / __| __| |_ \| '__|
                 ___) | |_| | |_) | | \__ \ |_ ___) | |
                |____/ \__,_|_.__/|_|_|___/\__|____/|_|

                # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for google.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
```

1.3 Subdomain Enumeration

The aforementioned subdomain enumeration techniques will help you identify publicly available target assets. Each one of them may be vulnerable to attacks, which should be thouroughly checked during the penetration test.

1.3.1 Video – Subdomain Enumeration

Subdomain Enumeration

In the subdomain enumeration video you will get to know various techniques to enumerate your target's subdomains.

**Videos are only available in Full or Elite Editions of the course. To upgrade, click HERE. To access, go to the course in your members area and click the resources drop-down in the appropriate module line.*

1.4

The Importance of Information Gathering

1.4 The Importance of Information Gathering

Before closing this module, we at eLearnSecurity want to stress **how important information gathering is!**

1.4 The Importance of Information Gathering

A strong phase of Information Gathering makes the difference between a good and a bad penetration tester.

A good penetration tester spends 90% of his time widening the attack surface because he knows this is what it is all about. The other 10% is just a matter of launching the correct commands with the appropriate tool with a high success rate.

1.4 The Importance of Information Gathering

Let’s say you are playing darts.

Would you prefer having 1000 shots to throw at a microscopic target, or one single shot at an impossible to miss big target?

1.4 The Importance of Information Gathering

Lastly, as penetration tests are **cyclic processes**, each time you will get deeper inside your client's infrastructure, thus gaining access to more information.

1.4 The Importance of Information Gathering

Every information gathering stage will need the same focus and dedication as the first one.

Your penetration test will be **as strong as your weakest skill**, so do not underestimate information gathering!

References

References

CrunchBase

http://www.crunchbase.com/

Facebook

https://www.facebook.com/

LinkedIn

https://www.linkedin.com/

Twitter

https://twitter.com/

References

Sysinternal Whois

http://technet.microsoft.com/en-us/sysinternals/bb897435.aspx

DNSdumpster.com

https://dnsdumpster.com/

Sublist3r

https://github.com/aboul3la/Sublist3r

Videos

Subdomain Enumeration

In the subdomain enumeration video you will get to know various techniques to enumerate your target's subdomains, from basic to advanced ones.

**Videos are only available in Full or Elite Editions of the course. To upgrade, click HERE. To access, go to the course in your members area and click the resources drop-down in the appropriate module line.*