

Colby Heilner  
Professor Torres  
2/9  
IT 140  
Lab 2

*Part A:*

- Define passive information gathering and discuss some **"PASSIVE"** information gathering tools and techniques

While studying for the Security+ I had some questions on passive and active information gathering. One of the main passive methods I remember is WHO Is records. From what I understand "passive" information gathering means that you are not directly interacting with the Ips, network, or machine of the company's you are gathering information on.

*Part B:*

- You have been contracted to conduct a **"PASSIVE"** information gathering penetration test against the companies listed below.

[\(Links to an external site.\)](#)

- [The Discord App](#)
- [Links to an external site.](#)
- [Megacorpone](#)
- [Links to an external site.](#)
- [Exploit-DB](#)
- - [Links to an external site.](#)
- Use the tools listed below for your passive information gathering penetration test:
  - [The Osint Framework](#)
-

- [Links to an external site.. \(Links to an external site.\)](#)
- theHarvester
- Answer as many of the following question as you can. Ensure that you **screenshot where you got the answer:**
  - Where is the website hosted (locally or with a third party)
  - where is the company located, if there are branch offices, where are they located
  - are there any sub-websites owned by the website listed
  - what IP addresses are associated with these sites
  - who administers the sites, list all administrators that you find
  - who is the CEO/President
  - how many people work at the site/company
  - what is the IP block for the site
  - what type of email server is being used by the site (see if you can find the version number)
  - What is the physical location of the IP address
  - try to find a picture of the company location (picture of the building)
  - when does the site expire
  - what programming language is the website built with
  - Find emails associated with the sites
  - Find a list of employees that work at the site
  - Can you name any hardware at the sites
  - Is the site running on Linux or Windows servers
  - how much money did the site/business make last year
  - is the company facing any financial problems
  - is the company undergoing any mergers/acquisitions/sales

To format this better I will move it down here.

### **discord.com**

For a lot of my information, I used Spider Foot which I believe is a lot like the harvester.

I would type the domain in, and I would choose to run passive scans for my information.

By Use Case

By Required Data

By Module

☐

All

**Get anything and everything about the target.**  
  
All SpiderFoot modules will be enabled (slow) but every possible piece of information about the target will be obtained and analysed.

☐

Footprint

**Understand what information this target exposes to the Internet.**  
  
Gain an understanding about the target's network perimeter, associated identities and other information that is obtained through a lot of web crawling engine use.

☐

Investigate

**Best for when you suspect the target to be malicious but need more information.**  
  
Some basic footprinting will be performed in addition to querying of blacklists and other sources that may have information about your target's malicious activities.

☒

Passive

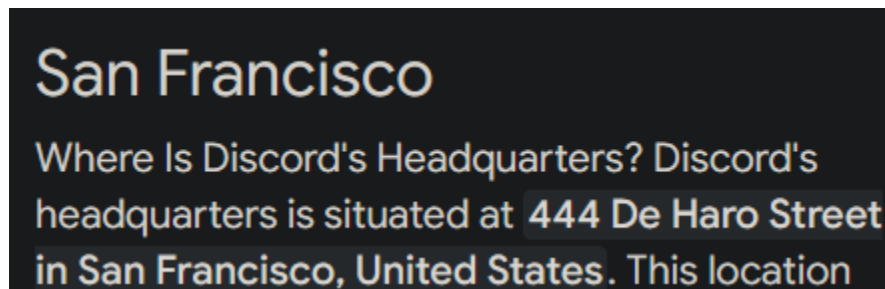
**When you don't want the target to even suspect they are being investigated.**  
  
As much information will be gathered without touching the target or their affiliates, therefore only modules that do not touch the target will be enabled.

I believe the website is being hosted here but is being hosted with AWS and CludFlare

Toronto, Ontario, ON, Canada, CA	162.159.135.232
Toronto, Ontario, ON, Canada, CA	162.159.128.233
Toronto, Ontario, ON, Canada, CA	162.159.138.232
Toronto, Ontario, ON, Canada, CA	162.159.137.232

Amazon AWS: <a href="http://www.amazon.com/aws/">http://www.amazon.com/aws/</a>	34.210.109.146	sfp_hosting
Amazon AWS: <a href="http://www.amazon.com/aws/">http://www.amazon.com/aws/</a>	34.217.231.110	sfp_hosting
Cloudflare Inc: <a href="https://www.cloudflare.com/">https://www.cloudflare.com/</a>	162.159.135.232	sfp_hosting
Cloudflare Inc: <a href="https://www.cloudflare.com/">https://www.cloudflare.com/</a>	162.159.128.233	sfp_hosting
Cloudflare Inc: <a href="https://www.cloudflare.com/">https://www.cloudflare.com/</a>	162.159.138.232	sfp_hosting

Google for this



Picture of headquarters



Lots of sub websites, over 200. Here is 3

<input type="checkbox"/>	<code>http://blog.discord.com/</code>
<input type="checkbox"/>	<code>http://canary.discord.com/</code>
<input type="checkbox"/>	<code>http://creator-support.discord.com/</code>

## MegaCorp

<code>149.56.244.87</code>	<code>www.megacorpone.com</code>
<code>167.114.21.64</code>	<code>admin.megacorpone.com</code>
<code>167.114.21.67</code>	<code>intranet.megacorpone.com</code>
<code>167.114.21.68</code>	<code>mail.megacorpone.com</code>
<code>167.114.21.69</code>	<code>mail2.megacorpone.com</code>
<code>167.114.21.71</code>	<code>siem.megacorpone.com</code>
<code>51.222.39.63</code>	<code>ns2.megacorpone.com</code>

[Browse](#) / [Country Name](#)

<input type="checkbox"/>	Data Element	Source Data Element
<input type="checkbox"/>	Canada	Montreal, Quebec, QC, Canada, CA
<input type="checkbox"/>	United States	megacorpone.com

Some emails associated with the site

Data Element	Source Data Element
joe@megacorpone.com	megacorpone.com
joe@megacorpone.com	megacorpone.com
mcarlow@megacorpone.com	megacorpone.com
test@megacorpone.com	megacorpone.com

Even though this is a factitious site this is still interesting information

Companies based in Paris	<a href="#">fb.mail.gandi.net</a>
Information technology companies of France	fb.mail.gandi.net

I believe these are the scanners using DuckDuckGo to do manual searches.

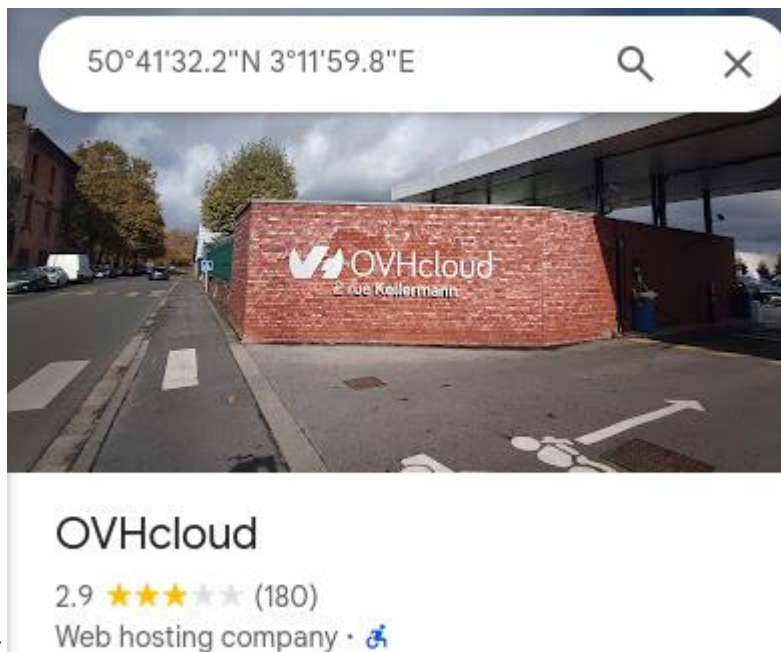
Lastly for Mega Corp here is the Operating system for the main domain

Apache/2.4.38 (Debian)	megacorpone.com
Apache/2.4.38 (Debian)	www.megacorpone.com

Raw DNS records also give me more subdomains

```
megacorpone.com. 300 IN MX 20 spool.mail.gandi.net.
megacorpone.com. 300 IN MX 50 mail.megacorpone.com.
megacorpone.com. 300 IN MX 60 mail2.megacorpone.com.
megacorpone.com. 300 IN MX 10 fb.mail.gandi.net.
```

Finally, this is hosted by OVHcloud because there are coordinates to them in my spider



foot

megacorp **FINISHED**

 Summary  Correlations  Browse  Graph

Browse / Physical Coordinates

<input type="checkbox"/>	Data Element	⌵
<input type="checkbox"/>	50.692262774812946, 3.199934160717116	

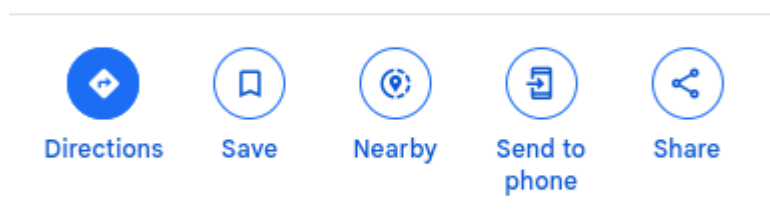
Okay lastly **exploitdb**

Alot of my different modules are pointing towards this as location but it just leads to a grocery store back alley.

<input type="checkbox"/>	Data Element	⌵	Source Data Element
<input type="checkbox"/>	Menifee, California, CA, United States, US		192.124.249.13

I then learned they are owned by Offensive security.

71 Vanderbilt Ave 3rd Floor



 71 Vanderbilt Ave, New York, NY 10169

Located at

**Some key people are**

Ning Wang, CEO Jim O'Gorman, Chief Strategy Officer Devon Kearns, Technical Operations Dr. Matteo Memelli, R&D

Due to some stack overflow modules, I got a list of usernames people have given up.

DJMcCarthy12	user15502206
anjanb	user2370139



Bills                      user2370139  
maxgonz  
supersixsix

## Emails

dookie@exploit-db.com

---

h@exploit-db.com

---

info@exploit-db.com

---

innrwrld@exploit-db.com

---

j0fer@exploit-db.com

---

loneferret@exploit-db.com

---

ragecyr@exploit-db.com

## IP

### Your Results:

exploit-db.com > 192.124.249.13

## Part C:

- How would you protect your company from this type of attack/research without limiting your companies ability to function?

I looked up a few ways to help with protection of data and here is what I found.

Hide a lot of public records if possible. Always i see this when looking up whois records.

```
stry Registrant ID: REDACTED FOR PRIVACY
strant Name: REDACTED FOR PRIVACY
strant Organization: Offensive Security
strant Street: REDACTED FOR PRIVACY
strant City: REDACTED FOR PRIVACY
strant State/Province:
strant Postal Code: REDACTED FOR PRIVACY
strant Country: GI
strant Phone: REDACTED FOR PRIVACY
strant Phone Ext:
strant Fax: REDACTED FOR PRIVACY
strant Fax Ext:
strant Email: 534e8d925d00ca1f58938dd89
stry Admin ID: REDACTED FOR PRIVACY
n Name: REDACTED FOR PRIVACY
n Organization: REDACTED FOR PRIVACY
n Street: REDACTED FOR PRIVACY
n City: REDACTED FOR PRIVACY
n State/Province: REDACTED FOR PRIVACY
n Postal Code: REDACTED FOR PRIVACY
n Country: REDACTED FOR PRIVACY
n Phone: REDACTED FOR PRIVACY
n Phone Ext:
n Fax: REDACTED FOR PRIVACY
```

These have been purposely removed. Another thing companies can do would be to Perform Regular OSINT Recon on Your Own Company

- Use the same tools attackers use:
  - SpiderFoot (Comprehensive OSINT scanning)
  - theHarvester (Email, subdomain, host discovery)
  - Amass (DNS enumeration)
  - Shodan & Censys (Find exposed services)

Companies should ALWAYS have training on potential leaks that could happen with social media. Just like social engineering training.