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
-

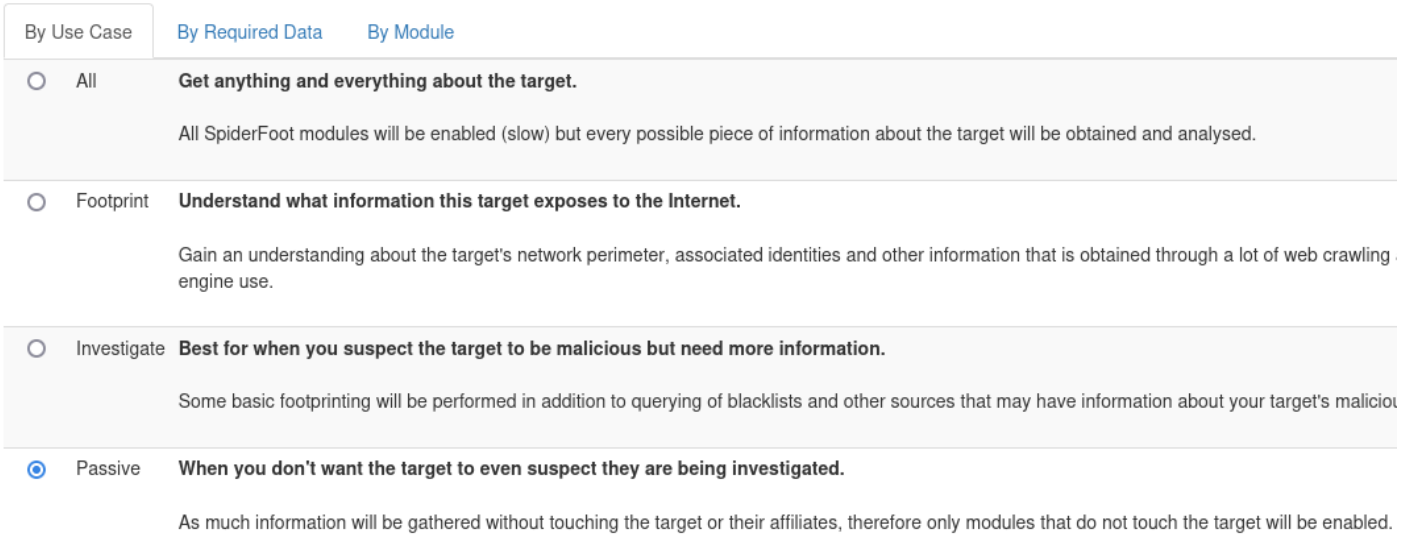
    - Links to an external site.. (Links to an external site.)
    - theHarvester
- Answer as many of the following question as you can. Ensure that you **screenshot where you got the answer**:
    - Where is the website hosted (locally or with a third party)
    - where is the company located, if there 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.

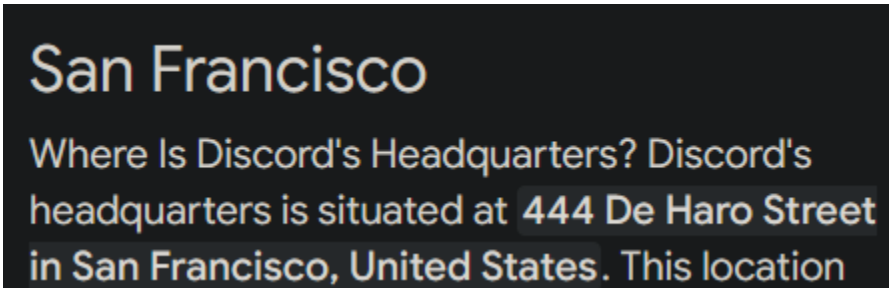


I believe the website is being hosted here but is being hosted with AWS and CludFlare

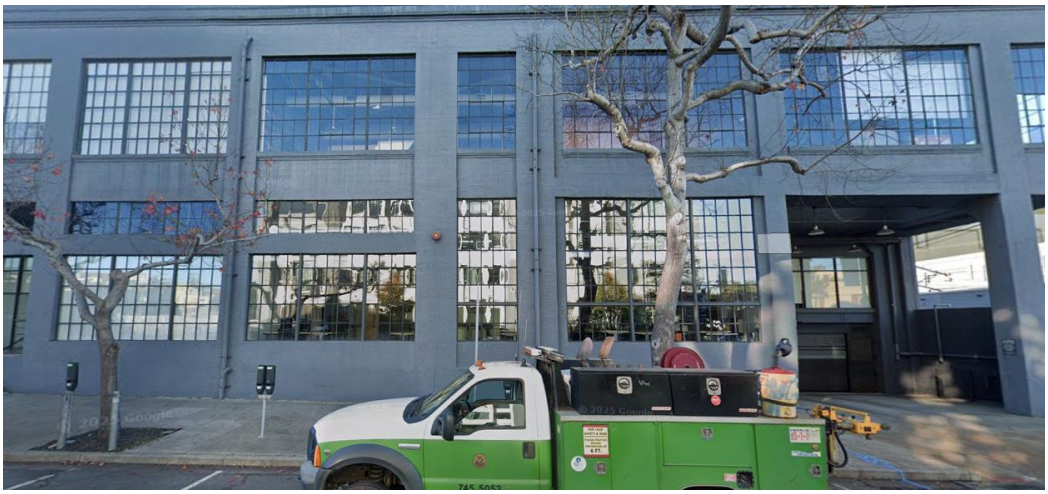
Toronto, Ontario, ON, Canada, CA	162.159.135.232
Toronto, Ontario, ON, Canada, CA	162.159.128.233
Toronto, Ontario, ON, Canada, CA	162.159.138.232
Toronto, Ontario, ON, Canada, CA	162.159.137.232

Amazon AWS: http://www.amazon.com/aws/	34.210.109.146	sfp_hosting
Amazon AWS: http://www.amazon.com/aws/	34.217.231.110	sfp_hosting
Cloudflare Inc: https://www.cloudflare.com/	162.159.135.232	sfp_hosting
Cloudflare Inc: https://www.cloudflare.com/	162.159.128.233	sfp_hosting
Cloudflare Inc: https://www.cloudflare.com/	162.159.138.232	sfp_hosting

Google for this



Picture of headquarters



Lots of sub websites, over 200. Here is 3

☐	http://blog.discord.com/
☐	http://canary.discord.com/
☐	http://creator-support.discord.com/

MegaCorp

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

Browse / Country Name

	Data Element	Source Data Element
☐	Canada	Montreal, Quebec, QC, Canada, CA
☐	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	fb.mail.gandi.net
Information technology companies of France	fb.mail.gandi.net

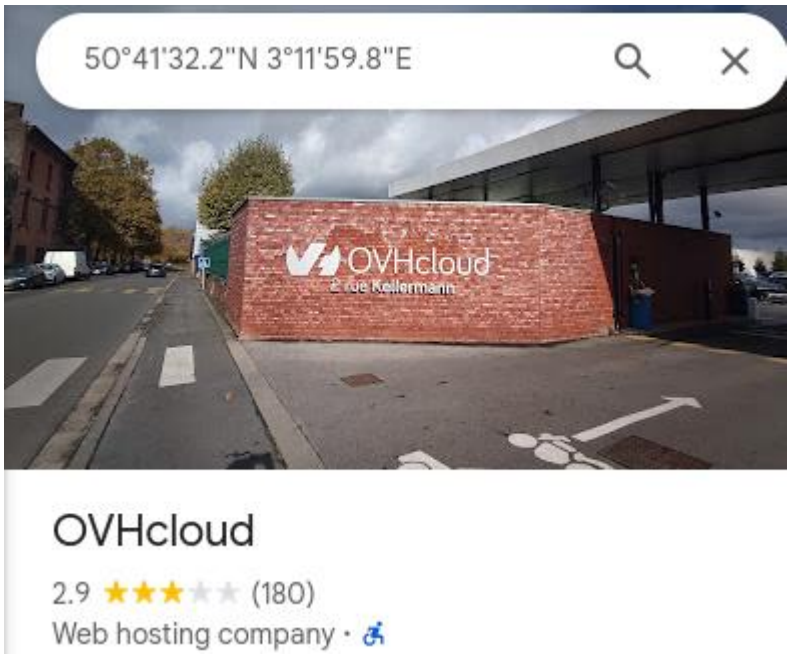
I believe these are the scanners using DuckDuckGo to do manual searches.
Lastly for Mega Corp here is the Operating system for the main domain

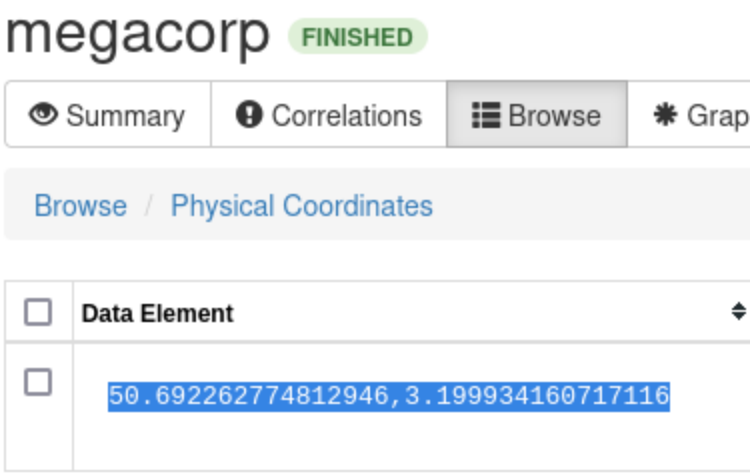
Apache/2.4.38 (Debian)	megacorpone.com
Apache/2.4.38 (Debian)	www.megacorpone.com

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



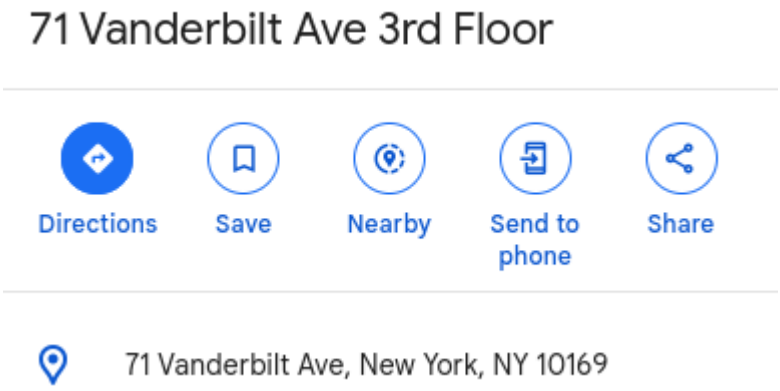


Okay lastly **exploitdb**

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

Data Element	Source Data Element
Menifee, California, CA, United States, US	192.124.249.13

I then learned they are owned by Offensive security.



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

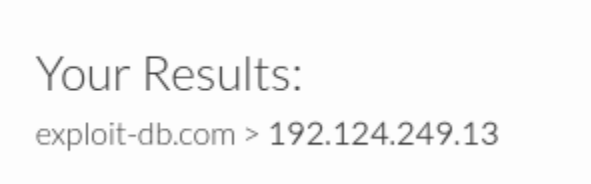
innrwrld@exploit-db.com

j0fer@exploit-db.com

loneferret@exploit-db.com

ragecyr@exploit-db.com

IP

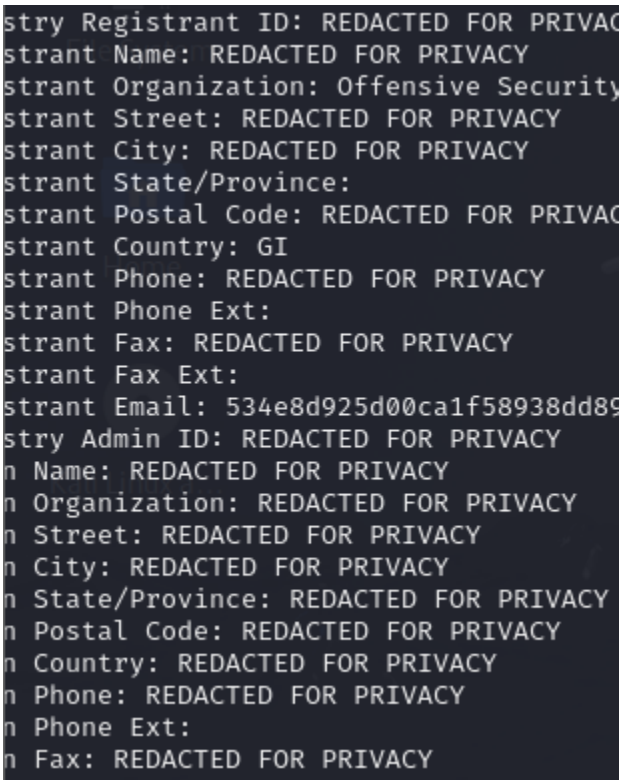


Part C:

- 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.



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)

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