

So these are my notes of OSCP passive information gathering module ,
Here i will not down all the commands and stuff used ,

Lets get to it , shall we .

Passive information gathering also known as OSINT , open source intelligence
Is the process of collecting openly available information about the target.

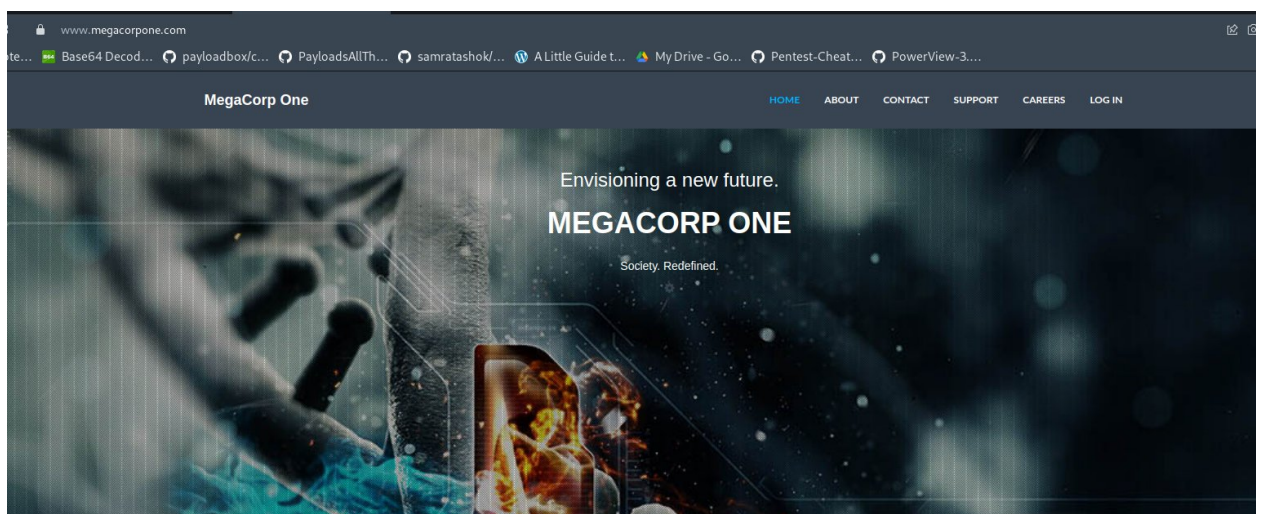
Without any direct interaction .

To clarify and expand target surface.

No suspicious interaction with the target.

1. Website Recon:

Browsing target website like this :



We can visit these pages and get further information :

[About](#) | [Contact](#) | [Support](#) | [Careers](#) | [Login](#)

Each page reveals some information which can be useful for us :


For example lets see their about page :

MegaCorp One


HOMEABOUTCONTACTSUPPORTCAREERSLOG IN

About.


MEET OUR TEAM




Joe Sheer
CHIEF EXECUTIVE OFFICER
Email: joe@megacorpone.com
Twitter: [@Joe_Sheer](https://twitter.com/Joe_Sheer)



Tom Hudson
WEB DESIGNER
Email: thudson@megacorpone.com
Twitter: [@TomHudsonMCO](https://twitter.com/TomHudsonMCO)



Tanya Rivera
SENIOR DEVELOPER
Email: trivera@megacorpone.com
Twitter: [@TanyaRiveraMCO](https://twitter.com/TanyaRiveraMCO)







Matt Smith
MARKETING DIRECTOR
Email: msmith@megacorpone.com
Twitter: [@MattSmithMCO](https://twitter.com/MattSmithMCO)

Here we can see different user , their social media accounts , their email formats

That ends with @megacorpone.com

Or like how last and first name are used in email addresses

Social Media



Social media information also can be useful for further phishing.

2. Whois Enumeration , it is a tool for looking into databases of domains and get information about the domain , like DNS servers , registrar etc.

It is a command line tool:

```
(root@kali)-[/home/kali]
# whois megacorpone.com | less
```

Results :

```
Domain Name: MEGACORPONE.COM
Registry Domain ID: 1775445745_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.gandi.net
Registrar URL: http://www.gandi.net
Updated Date: 2021-06-15T17:59:57Z
Creation Date: 2013-01-22T23:01:00Z
Registry Expiry Date: 2024-01-22T23:01:00Z
Registrar: Gandi SAS
Registrar IANA ID: 81
Registrar Abuse Contact Email: abuse@support.gandi.net
Registrar Abuse Contact Phone: +33.170377661
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: NS1.MEGACORPONE.COM
Name Server: NS2.MEGACORPONE.COM
Name Server: NS3.MEGACORPONE.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
> Last update of whois database: 2022-05-20T11:00:56Z <<<
```

```
Registry Registrant ID:
Registrant Name: Alan Grofield
Registrant Organization: MegaCorpOne
Registrant Street: 2 Old Mill St
Registrant City: Rachel
Registrant State/Province: Nevada
Registrant Postal Code: 89001
Registrant Country: US
Registrant Phone: +1.9038836342
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: 3310f82fb4a8f79ee9a6bfe8d672d87e-1696395@contact.gandi.net
Registry Admin ID:
Admin Name: Alan Grofield
Admin Organization: MegaCorpOne
Admin Street: 2 Old Mill St
```

We can get email , names of people who registered it , some contact numbers and other information .

We can also do reverse lookup , that is lookup through IP addresses.

```
(root@kali)-[/home/kali]
# whois 149.56.244.87 | less
```

Results :

```
# start
NetRange:      149.56.0.0 - 149.56.255.255
CIDR:          149.56.0.0/16
NetName:       HO-2
NetHandle:     NET-149-56-0-0-1
Parent:        NET149 (NET-149-0-0-0-0)
NetType:       Direct Allocation
OriginAS:
Organization:  OVH Hosting, Inc. (HO-2)
RegDate:       2016-02-09
Updated:       2016-02-10
Ref:           https://rdap.arin.net/registry/ip/149.56.0.0

OrgName:       OVH Hosting, Inc.
OrgId:         HO-2
Address:       800-1801 McGill College
City:          Montreal
StateProv:     QC
```

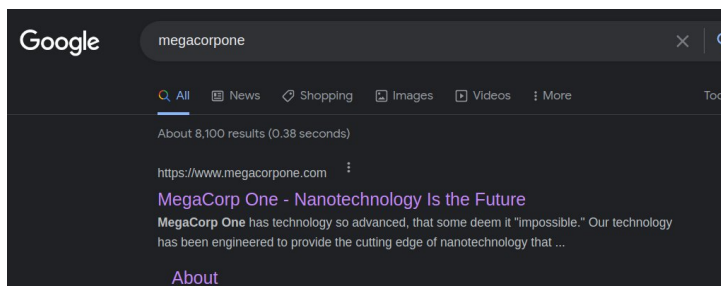
3. Google Hacking :

Google could be used to find critical data , misconfiguration in websites and vulnerabilities .

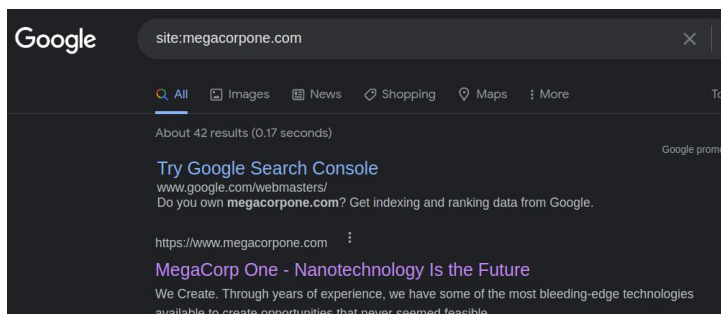
Usage of search strings and operators ,

Lets see it in action and how it refines our results :

Normal search via google leads to 8100 results , lets refine it further

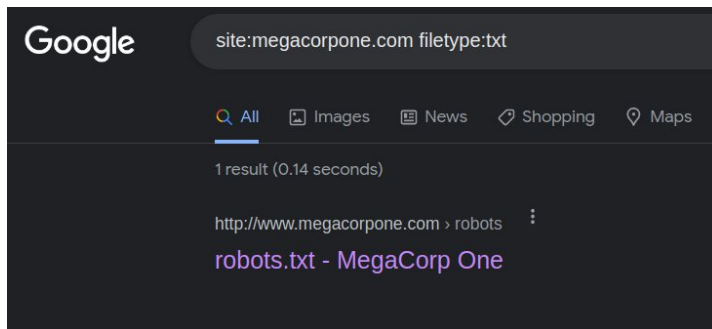


Using site:megacorpone.com operator



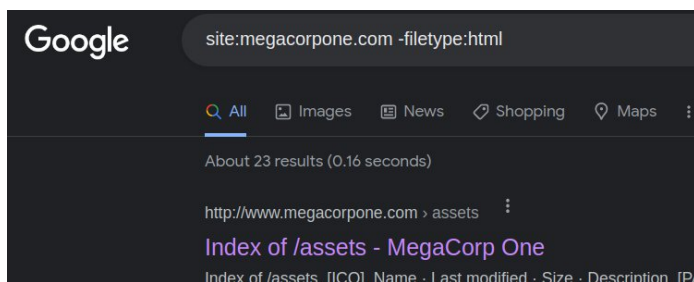
We now have just 42 results to deal with ,

Now use an additional filetype:txt , to search for filrtypes or in this case txt files,



Add a minus or “-“ to your operator to exclude those results ,

Lets see an example to exclude normal HTML pages and find good stuff:




Operators example – intitle , intext , inurl etc. are there which can be found online and there is a database of all this that is named as :

Google Hacking Database:

A screenshot of the Exploit Database website. The page title is 'Google Hacking Database'. There is a search bar and a 'Quick Search' button. Below the search bar, there is a table with columns: 'Date Added', 'Dork', 'Category', and 'Author'. The table contains several rows of search queries and their corresponding categories and authors.

Date Added	Dork	Category	Author
2022-01-12	site:vps-* vps.ovh.net	Web Server Detection	Chahine Boutighane
2022-01-12	inurl:adminpanel site:gov.*	Footholds	Asheet Tirkey
2021-11-19	site:gov.* intitle:"index of" *.csv	Files Containing Juicy Info	Midhun Mohanan
2021-11-19	site:papaly.com + keyword	Files Containing Juicy Info	Gabriel Tarsia
2021-11-19	Fwd: intitle:"Index of/" intext:"resource/"	Files Containing Juicy Info	Mugdha Bansode
2021-11-19	Google to wordpress	Files Containing Juicy Info	Aitor Herrero
2021-11-19	Fwd: intitle:"atvise - next generation"	Files Containing Juicy Info	Mugdha Bansode

4. Netcraft : <https://searchdns.netcraft.com> :



[Services](#)
[Solutions](#)
[News](#)
[Company](#)
[Resources](#)
[Report Fraud](#)
[Request Trial](#)

Hostnames matching *.megacorpone.com

Search with another pattern?

2 results

Rank	Site	First seen	Netblock	OS	Site Report
51183	www.megacorpone.com	March 2013	OVH Hosting, Inc.	Linux - Debian	
596288	intranet.megacorpone.com		OVH Hosting, Inc.	unknown	

We can gather various information about the target from her like technologies used.

Site Technology (fetched 12 days ago)

Application Servers

An application server is a server that provides software applications with services such as security, data services, transaction support, and distributed systems.

Technology	Description	Popular sites
Apache	Web server software	www.victor
Debian	No description	www.smtp

Server-Side

5. Recon-ng: module based framework for web based information gathering :

It is like metasploit and has marketplace to download modules, set modules , set options and run them to gather information :

Searching modules :

```
[recon-ng][default] > marketplace search github
[*] Searching module index for 'github'...

+-----+-----+-----+-----+
| Path                                     | Version | Status | Updat |
+-----+-----+-----+-----+
| recon/companies-multi/github_miner      | 1.1     | not installed | 2020-0 |
| recon/profiles-contacts/github_users    | 1.0     | not installed | 2019-0 |
| recon/profiles-profiles/profiler         | 1.0     | not installed | 2019-0 |
| recon/profiles-repositories/github_repos | 1.1     | not installed | 2020-0 |
| recon/repositories-profiles/github_commits | 1.0     | not installed | 2019-0 |
| recon/repositories-vulnerabilities/github_dorks | 1.0     | not installed | 2019-0 |
+-----+-----+-----+-----+

D = Has dependencies. See info for details.
K = Requires keys. See info for details.
```

Getting info about a module :

```
[recon-ng][default] > marketplace info recon/domains-hosts/google_site_web
```

path	recon/domains-hosts/google_site_web
name	Google Hostname Enumerator
author	Tim Tomes (@lanmaster53)
version	1.0
last_updated	2019-06-24
description	Harvests hosts from Google.com by using the 'site' search operator. Updates the 'hosts' table with the results.
required_keys	[]
dependencies	[]
files	[]
status	not installed

Installing and loading a module :

```
[recon-ng][default] > marketplace install recon/domains-hosts/google_site_web
[*] Module installed: recon/domains-hosts/google_site_web
[*] Reloading modules...
[recon-ng][default] > modules load recon/domains-hosts/google_site_web
```

Getting info , setting options required and running a module :

```
[recon-ng][default] > modules load recon/domains-hosts/google_site_web
[recon-ng][default][google_site_web] > info
```

```

Name: Google Hostname Enumerator
Author: Tim Tomes (@lanmaster53)
Version: 1.0

Description:
Harvests hosts from Google.com by using the 'site' search operator. Updates the 'hosts' table with the results.

Options:
  Name      Current Value  Required  Description
  -----
SOURCE      default        yes       source of input (see 'info' for details)

Source Options:
  default    SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
  <string>   string representing a single input
  <path>     path to a file containing a list of inputs
  query <sql> database query returning one column of inputs

[recon-ng][default][google_site_web] > options set SOURCE megacorpone.com
SOURCE => megacorpone.com
[recon-ng][default][google_site_web] > run
```

```

MEGACORPONE.COM

[*] Searching Google for: site:megacorpone.com
```

6. Open-Source Code :

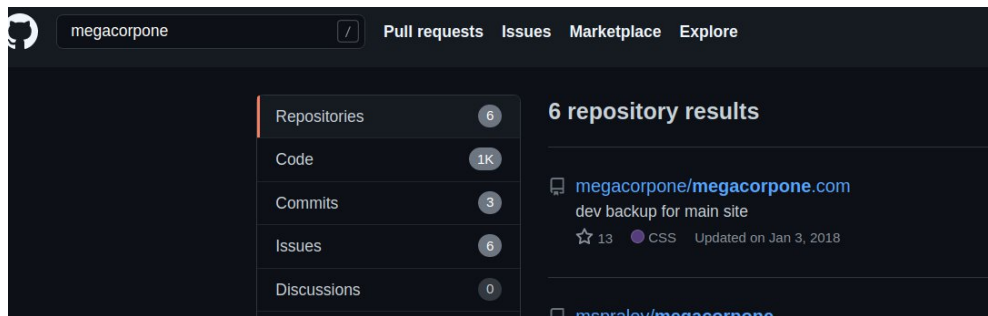
Open source projects that have their code available online to read from platforms like github , gitlab , sourceforge .

We can find technologies and programming languages used by organizations .

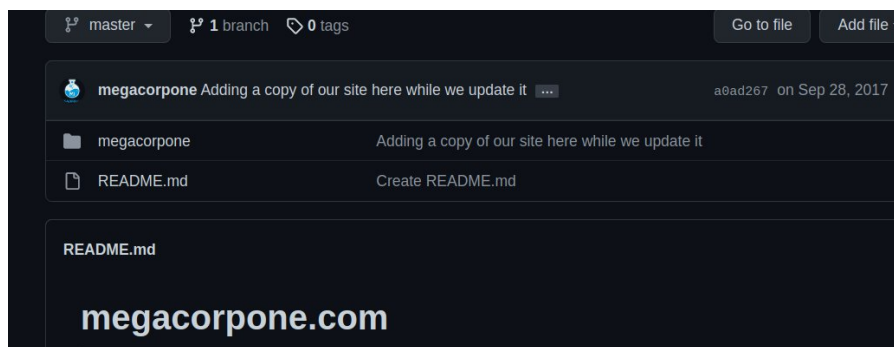
By mistake , sensitive data and credentials can also be found there .

Lets see it in action:

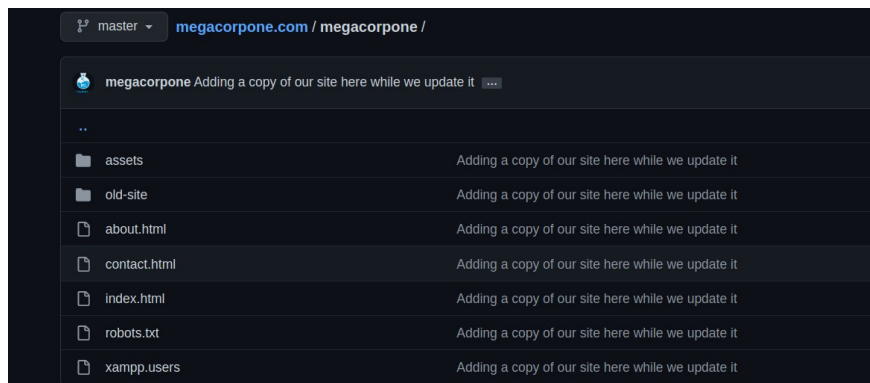
Searching github :



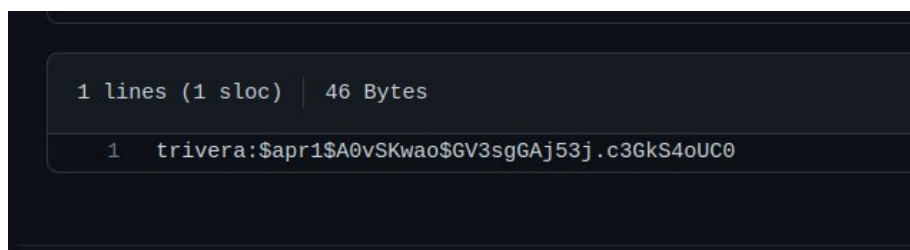
Opening its repository:



Further exploration :



Xampp.users file (interesting):



Credentials found :-)

7. Shodan :

It searches for all internet connected devices .

8. Security Headers Scanner :

The screenshot shows the Security Headers Scanner interface. At the top, there's a navigation bar with 'Home', 'About', and 'Donate' links. Below the header, a large red banner says 'Scan your site now' with a search bar containing 'www.megacorpone.com' and a 'Scan' button. Below the banner, there's a 'Security Report Summary' section. It features a large red 'F' grade icon. The report details include: Site: <http://www.megacorpone.com/> - (Scan again over https), IP Address: 149.56.244.87, Report Time: 20 May 2022 11:56:08 UTC, Headers: Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, and Permissions-Policy (all marked with red 'X' icons), and Warning: Grade capped at A, please see warnings below. At the bottom, there's a 'Supported By' section.

9. SSL server Test :

This free online service performs a deep analysis of the configuration of any SSL web server on the public Internet.

Test encryption strength.

The screenshot shows the Qualys SSL Labs website. The header includes the Qualys logo and navigation links: 'Home', 'Projects', 'Qualys Free Trial', and 'Contact'. Below the header, the page title is 'SSL Report: www.megacorpone.com (149.56.244.87)'. The report was assessed on Fri, 20 May 2022 11:59:49 UTC. A 'Summary' section displays an overall rating of 'B' in a yellow box. To the right of the rating is a horizontal bar chart showing scores for Certificate, Protocol Support, Key Exchange, and Cipher Strength. Below the chart, there are three informational bars: 'Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).', 'This server supports TLS 1.0 and TLS 1.1. Grade capped to B. [MORE INFO >](#)', and 'This server supports TLS 1.3.'

To find vulnerabilities in encryption side of things.

Pastebin : it is a basic text pasting and sharing platform . We can found information pasted by organization users and stuff.

User Information Gathering :

Gather information about usernames , employee list ,PII's etc to create a username and password list . For social engineering , credential stuffing , password attacks etc.

1. Email Harvesting

The tool we will be using here is theHarvester , which is a command-line tool to enumerate emails , users , domains :

```
(root@kali)-[/home/kali]
# theHarvester -d www.megacorpone.com -b google

*****
*                                     *
* [theHarvester]                     *
* [theHarvester]                     *
* [theHarvester]                     *
* [theHarvester]                     *
* [theHarvester]                     *
* theHarvester 4.0.3                  *
* Coded by Christian Martorella       *
* Edge-Security Research              *
* cmartorella@edge-security.com       *
*                                     *
*                                     *
*****

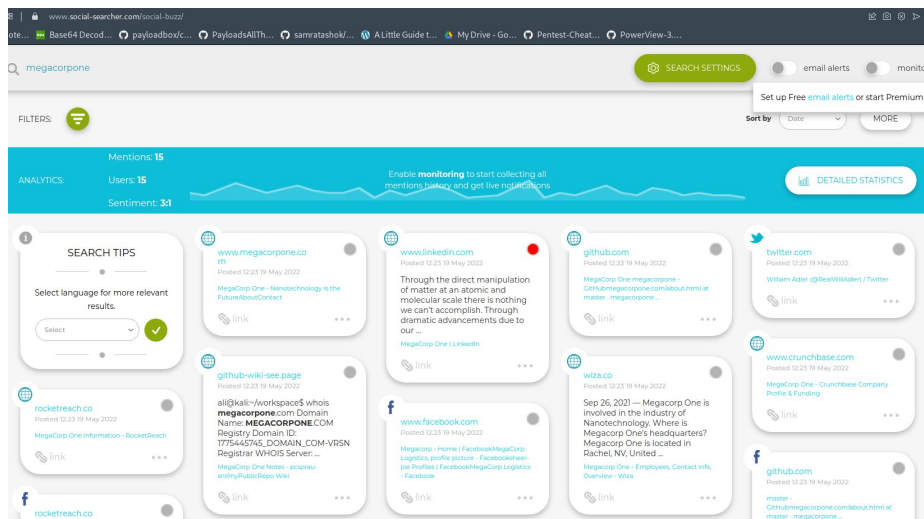
[+] Target: www.megacorpone.com
```

2. Password Dumps : can be useful for brute-force attacks ,

Can be found on pastebin ,

Rockyou.txt is a good example of this .

3. Social Media Tools :



4. Site-specific tools :

<https://github.com/digininja/twofi> – for twitter wordlist

<https://github.com/initstring/linkedin2username> - linkedin to username enumeration

5. Stackoverflow website can be used to get information about companies technologies used .

Information Gathering Framework:

<https://osintframework.com>

<https://www.maltego.com> - a bit hard to learn .

This module is done for now. :-)