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.

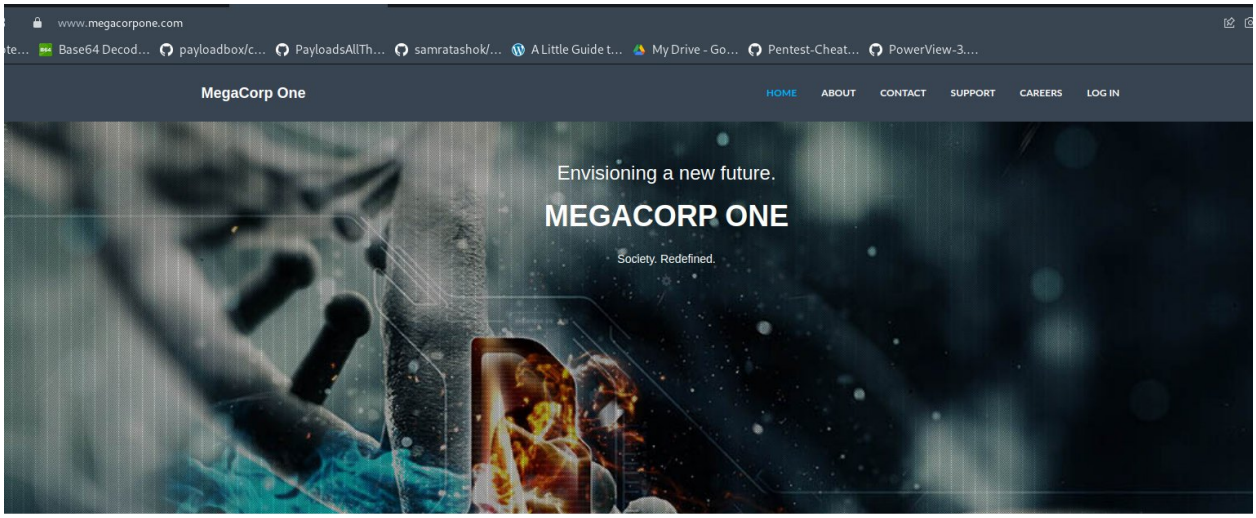
Without any direct interaction .

To clarify and expand target surface.

No suspicious interaction with the target.

1. Website Recon:

Browsing target website like this :

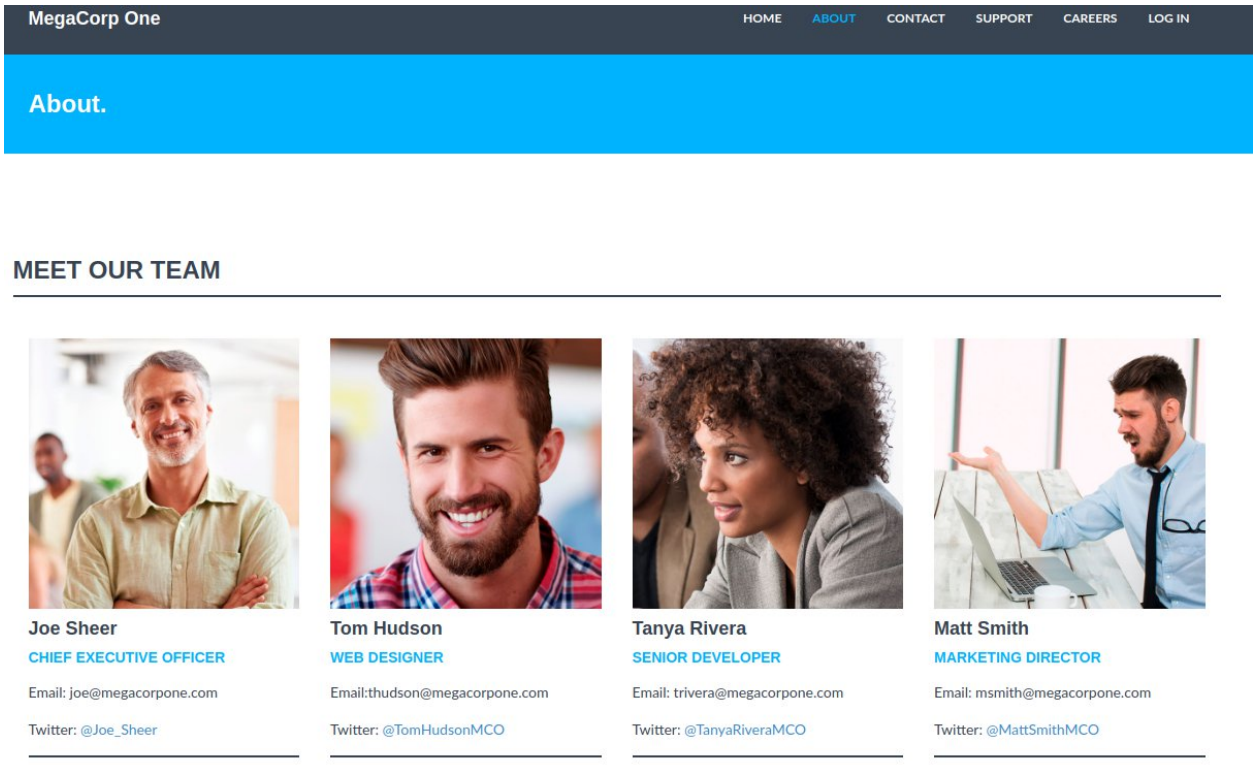



We can visit these pages and get further information :

About | Contact | Support | Careers | Login

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

For example lets see their about page :




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

That ends with [@megacorpone.com](@megacorpone.com)

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


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
```

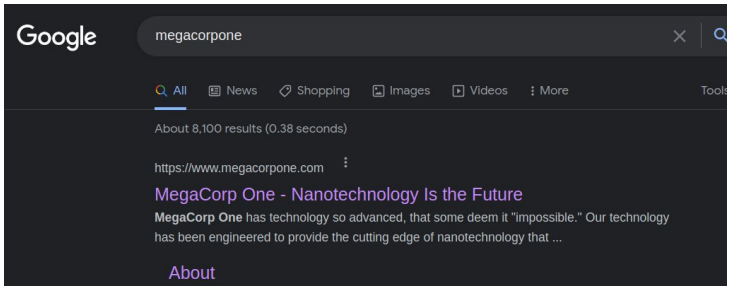
3. Google Hacking :

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

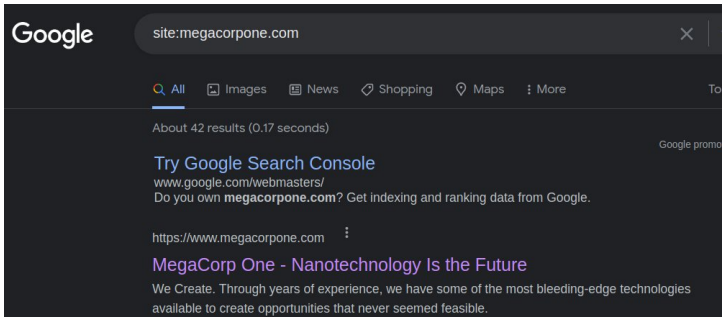
Usage of search strings and operators ,

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

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

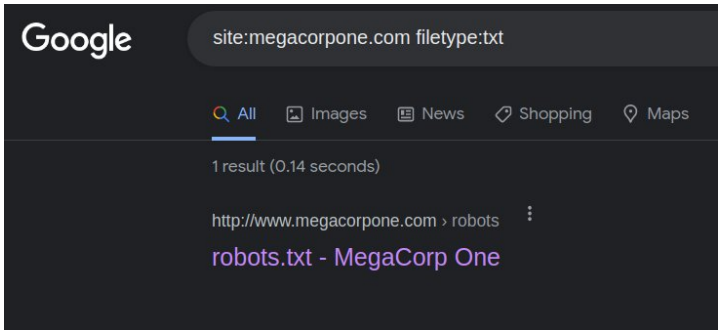



Using site:megacorpone.com operator



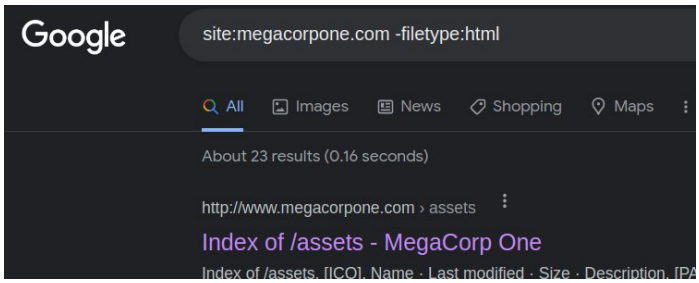
We now have just 42 results to deal with ,

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



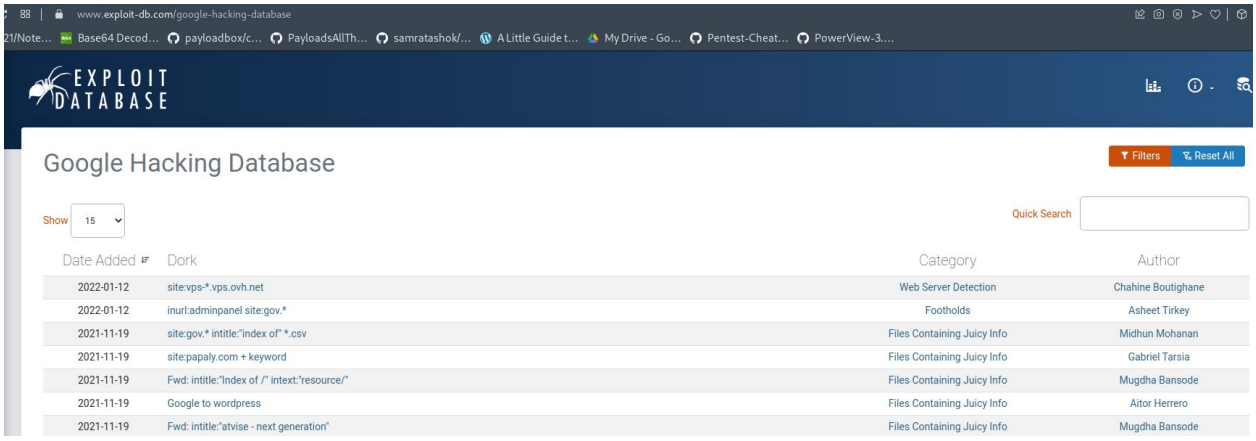

Add a minus or “-“ to your operator to exclude those results ,

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



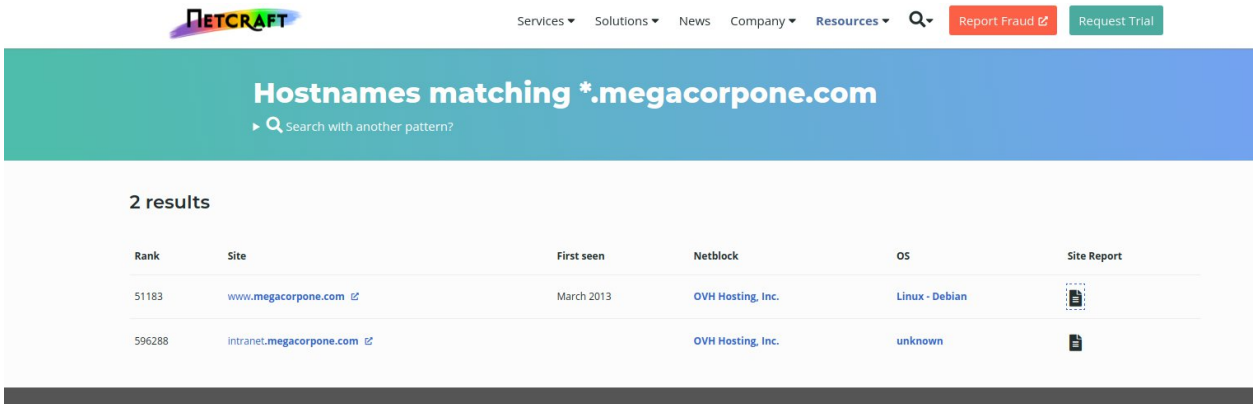

Operators example – intitle , intext , inurl etc. are there which can be found online and there is a database of all this that is named as :

Google Hacking Database:

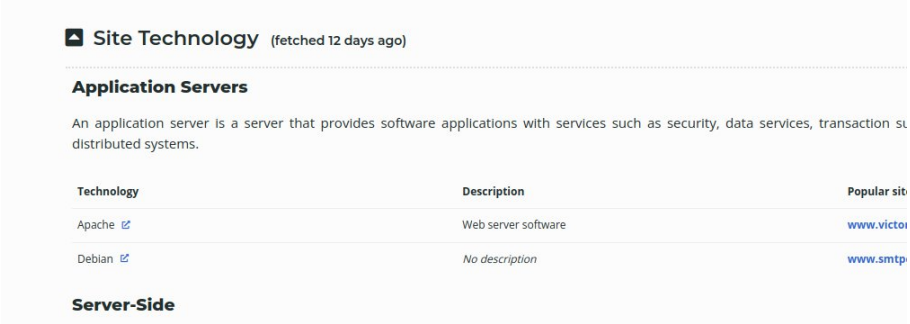



.

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




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




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 th
  | 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][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 :

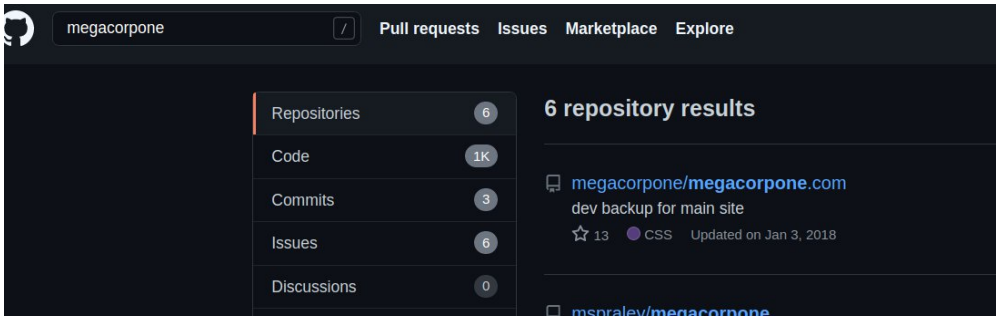
Open source projects that have their code available online to read from platforms like github , gitlab , sourceforge .

We can find technologies and programming languages used by organizations .

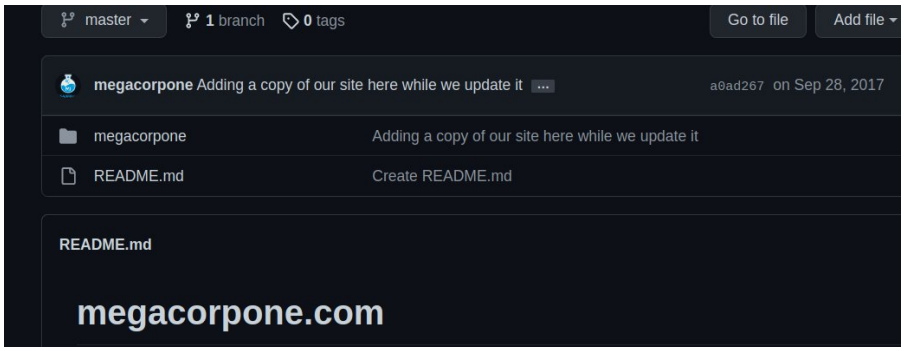
By mistake , sensitive data and credentials can also be found there .

Lets see it in action:

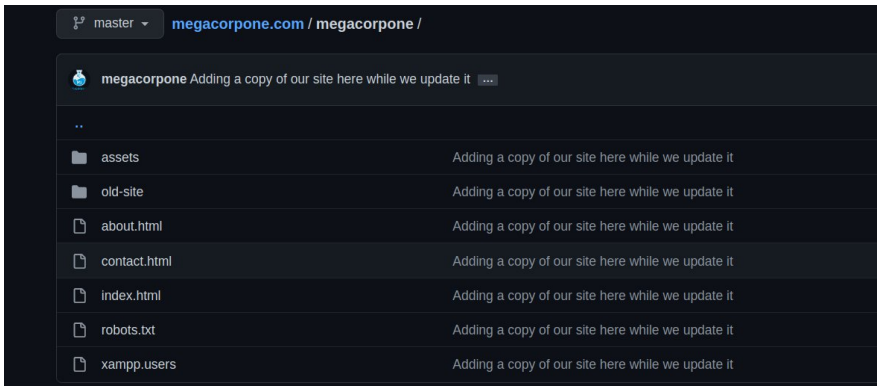
Searching github :



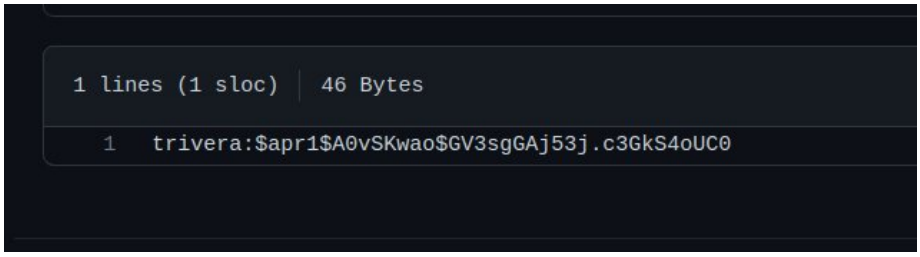

Opening its repository:




Further exploration :




Xampp.users file (interesting):

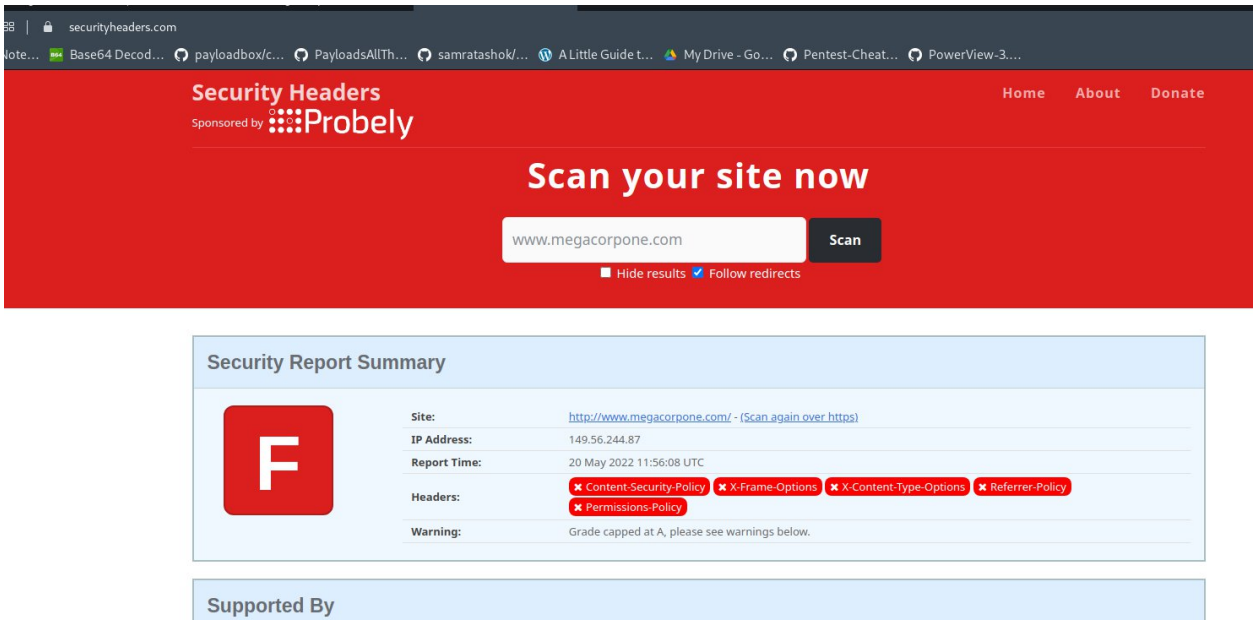



Credentials found :-)

7. Shodan :

It searches for all internet connected devices .

8. Security Headers Scanner :

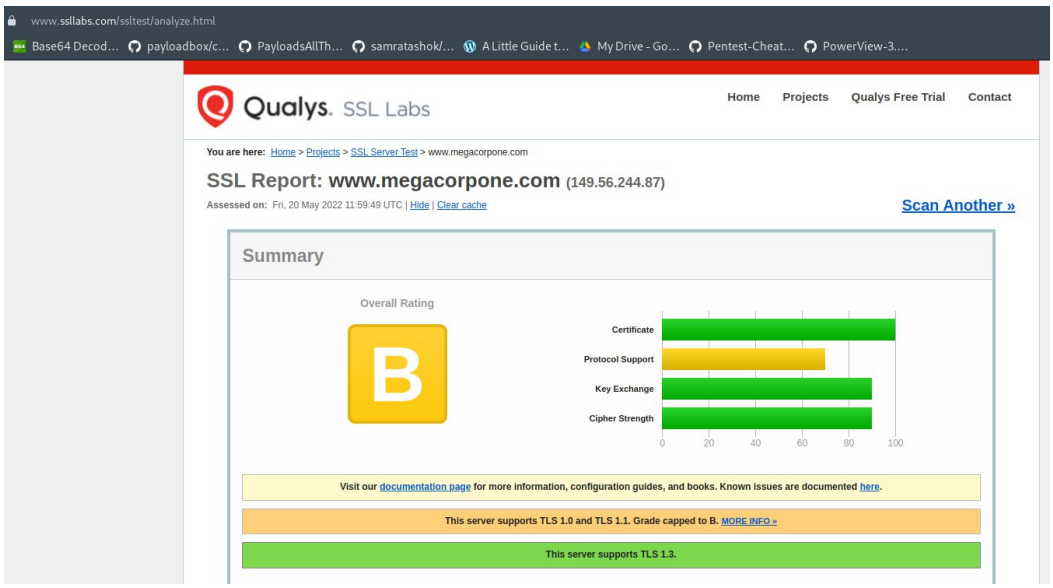



.

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.




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

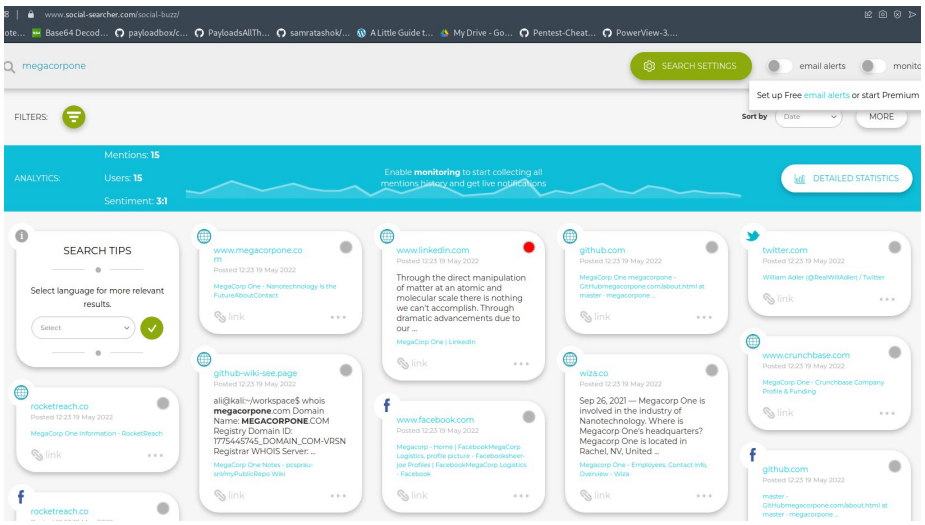
The tool we will be using here is theHarvester , which is a command-line tool to enumerate emails , users , domains :


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. :-)