

Practical 2

Aim: Use of open-source intelligence and passive reconnaissance

OPEN-SOURCE INTELLIGENCE (OSINT)

Open-Source Intelligence Cycle



Sources: ICAC

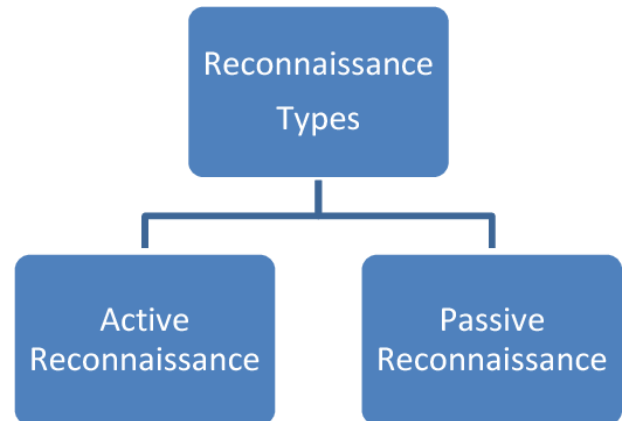


Fig 2: Types of Reconnaissance

A) Sublist3r

Install sub lister using sudo apt install sublist3r

```

kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ sudo apt install sublist3r
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  sublist3r
0 upgraded, 1 newly installed, 0 to remove and 528 not upgraded.
Need to get 620 kB of archives.
After this operation, 1,944 kB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 sublist3r all 1.1-4 [
620 kB]
Fetched 620 kB in 1s (511 kB/s)
Selecting previously unselected package sublist3r.
(Reading database ... 398680 files and directories currently installed.)
Preparing to unpack .../sublist3r_1.1-4_all.deb ...
Unpacking sublist3r (1.1-4) ...
Setting up sublist3r (1.1-4) ...
Processing triggers for kali-menu (2023.4.3) ...
Processing triggers for man-db (2.11.2-3) ...

(kali@kali)-[~]
$
  
```

Once the tool is installed you can use

sublist3r -d github.com -t 3 -d yahoo

To find all the subdomains of GitHub using bing search engine

```
(kali@kali)-[~]
$ sudo sublist3r -d packtpub.com

# Coded By Ahmed Aboul-Ela - @aboul3la

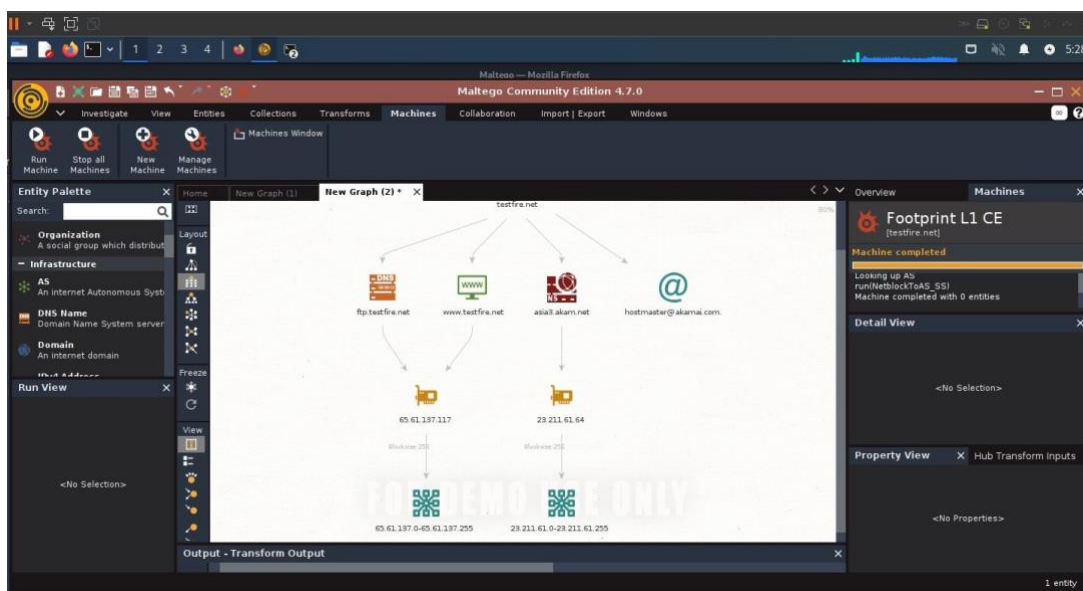
[-] Enumerating subdomains now for packtpub.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSDumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
[-] Total Unique Subdomains Found: 45
www.packtpub.com
birmingham.packtpub.com
careers.packtpub.com
cdn.packtpub.com
courses.packtpub.com
data.packtpub.com
dev.packtpub.com
invoices.dev.packtpub.com
test-pomerium.dev.packtpub.com
dev-epic.packtpub.com
downloads.packtpub.com
epic.packtpub.com
freeaudit.packtpub.com
helpdesk.packtpub.com
invoices.packtpub.com
ithelpdesk.packtpub.com
landing.packtpub.com
```

In our case, it didn't find anything

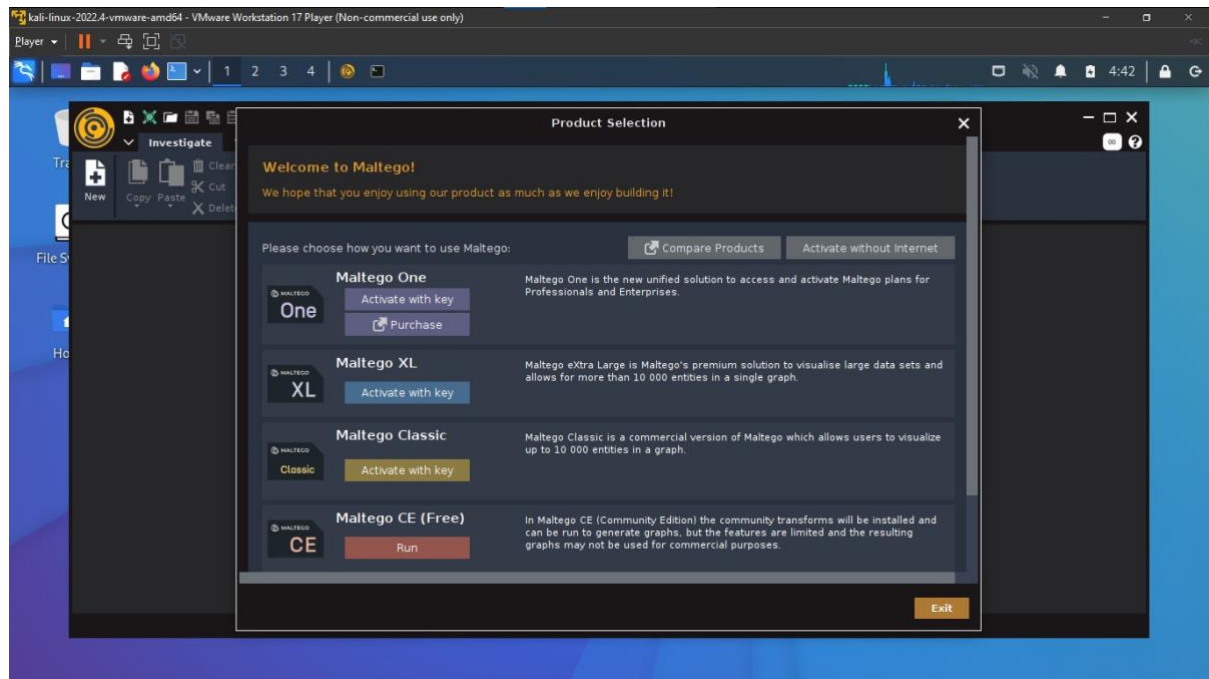
B) Maltego

Install maltego if not already installed (sudo apt install maltego)

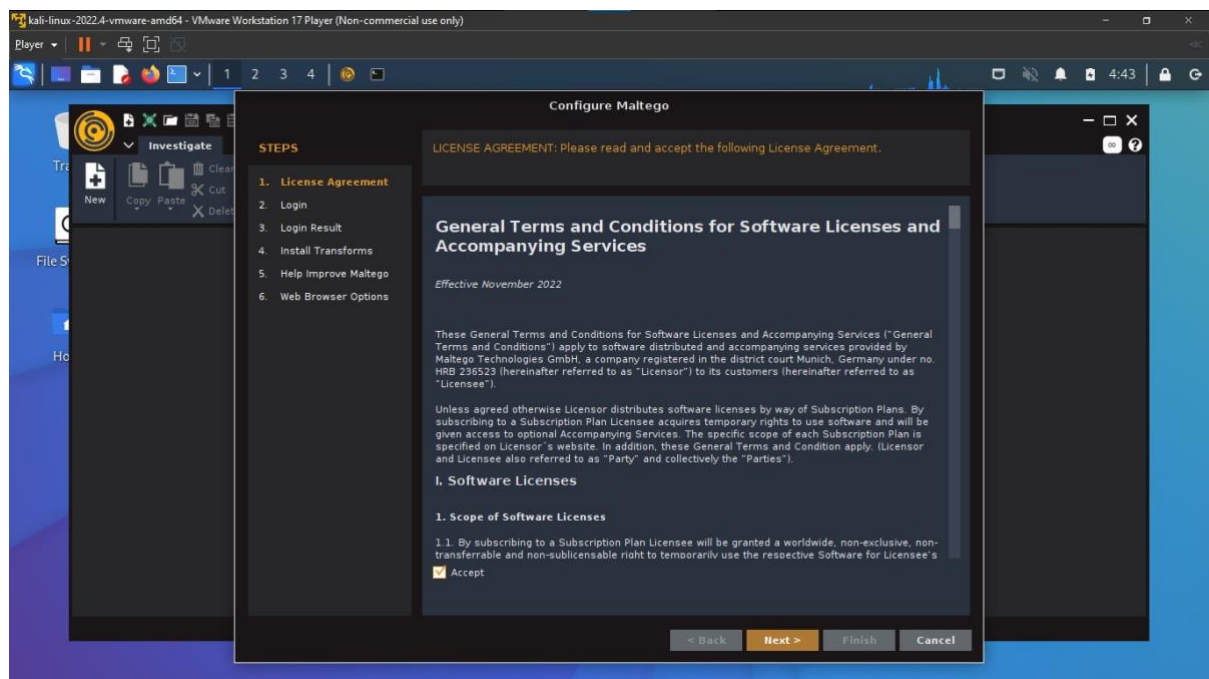
In order to access Maltego you will need to create an account [here](#).



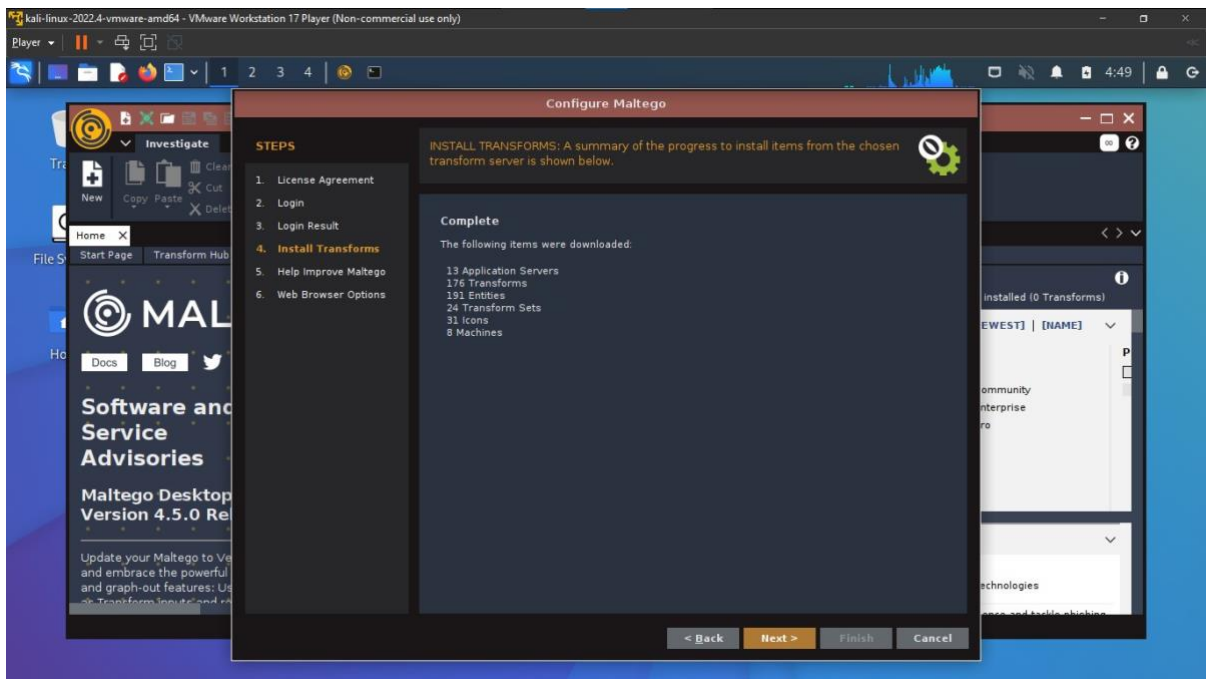
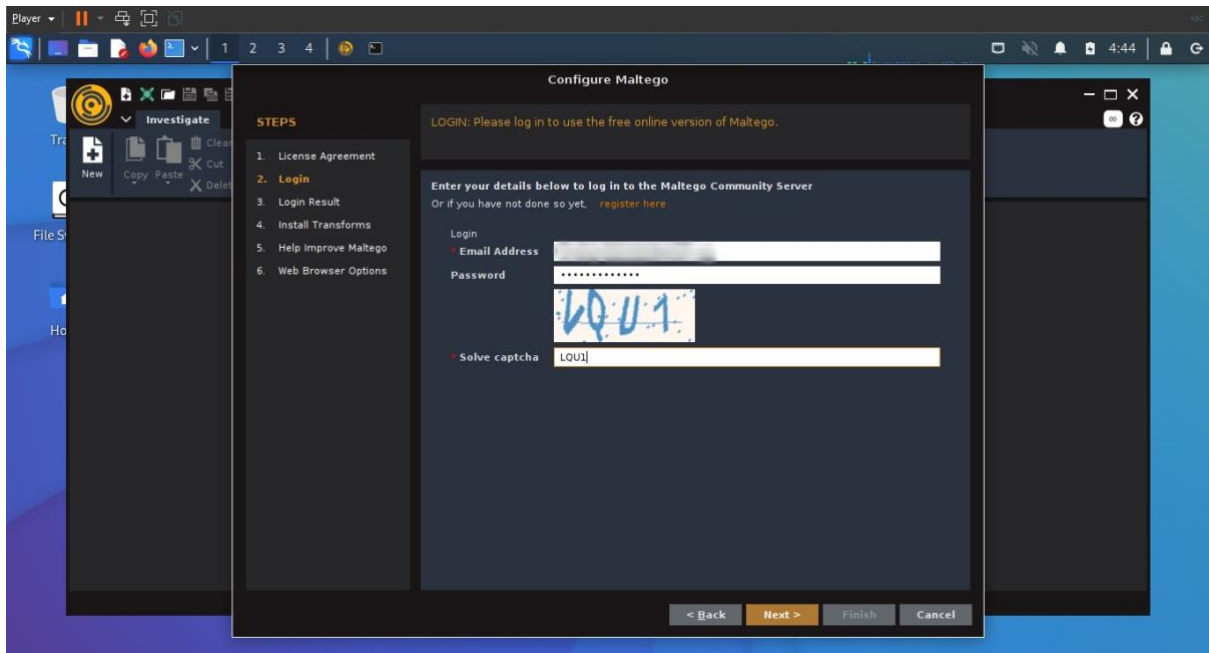
Once the account is created and you are successfully logged in to the Maltego application you should see this screen. Click run

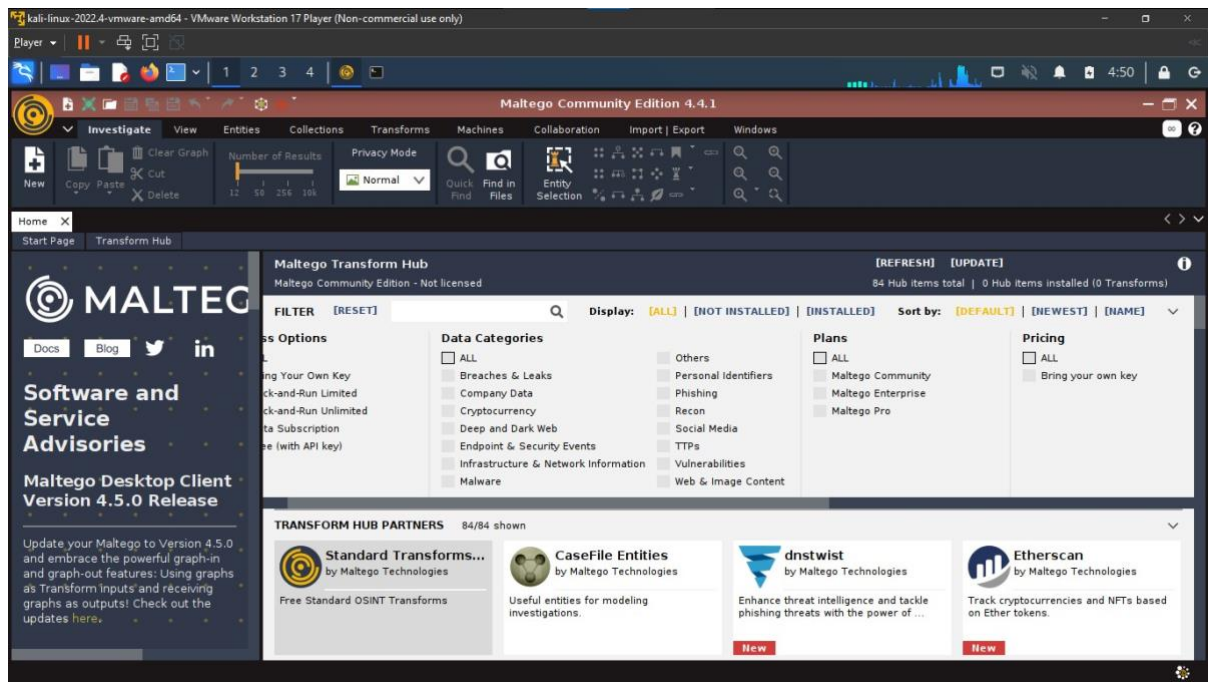


Tick Accept and Next

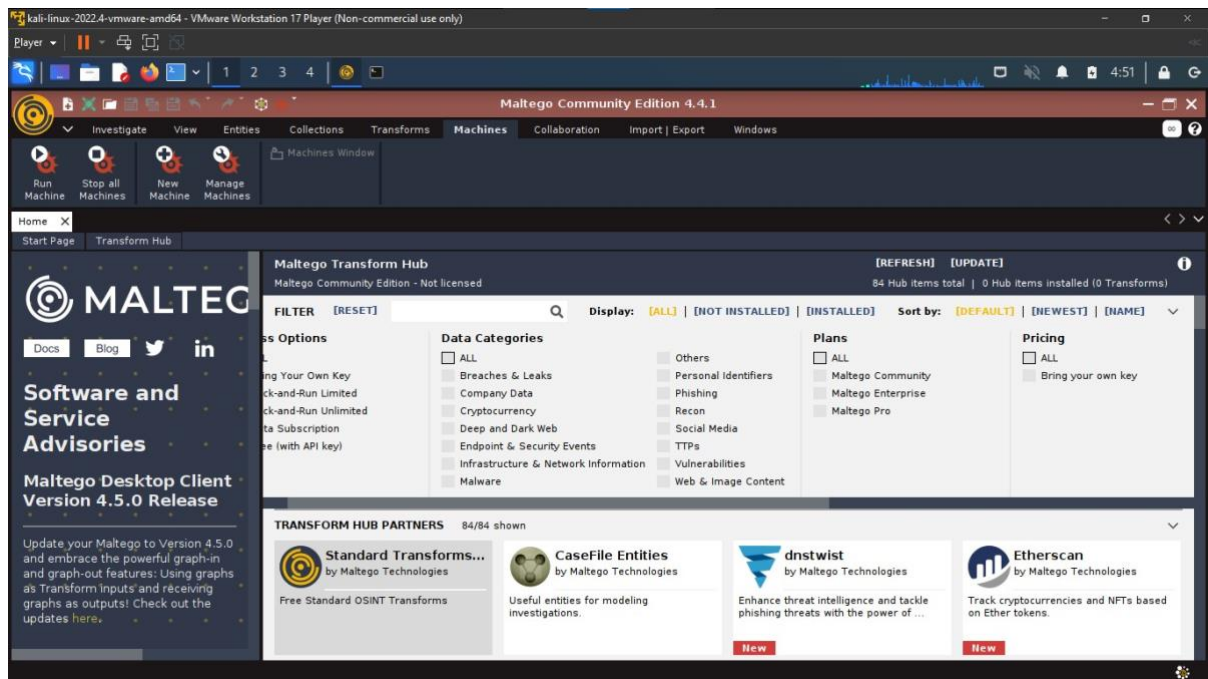


Log in and complete the challenge

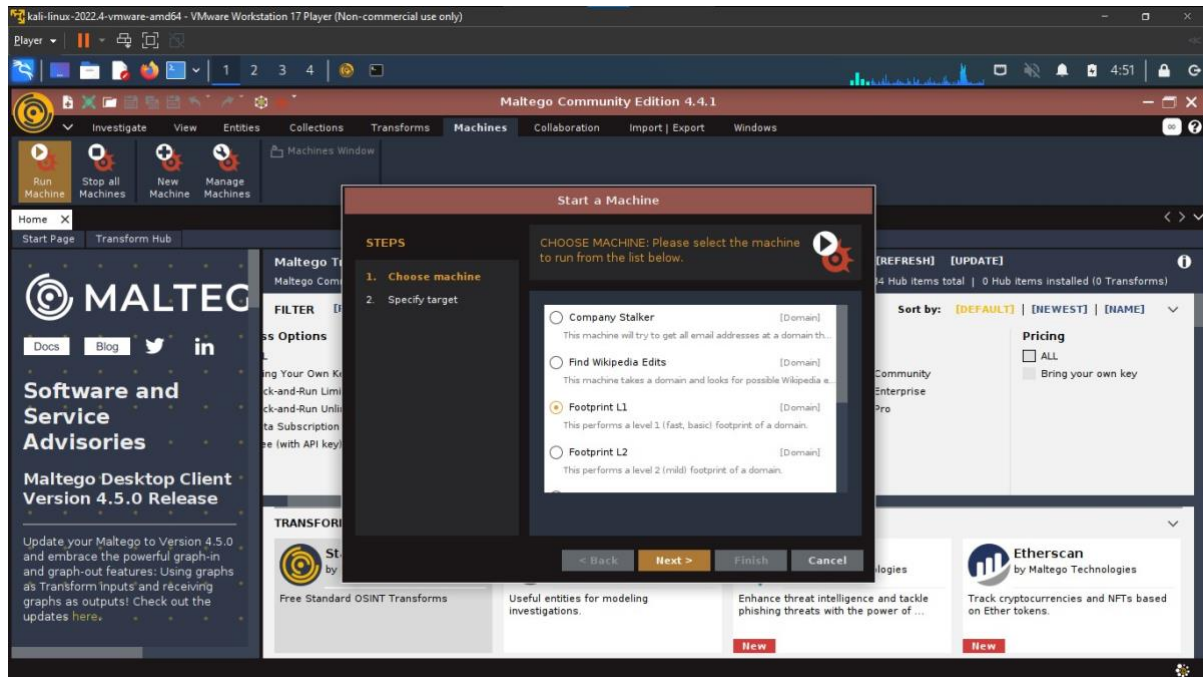




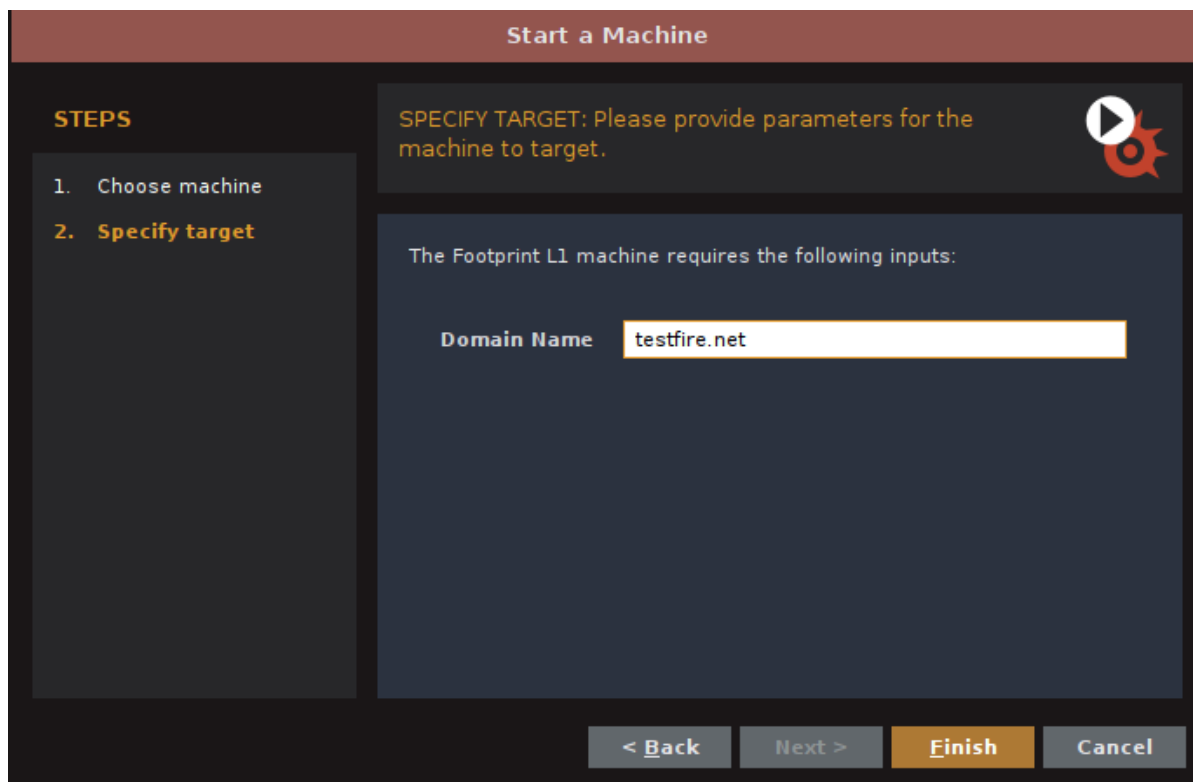
Under Machines Click run Machine



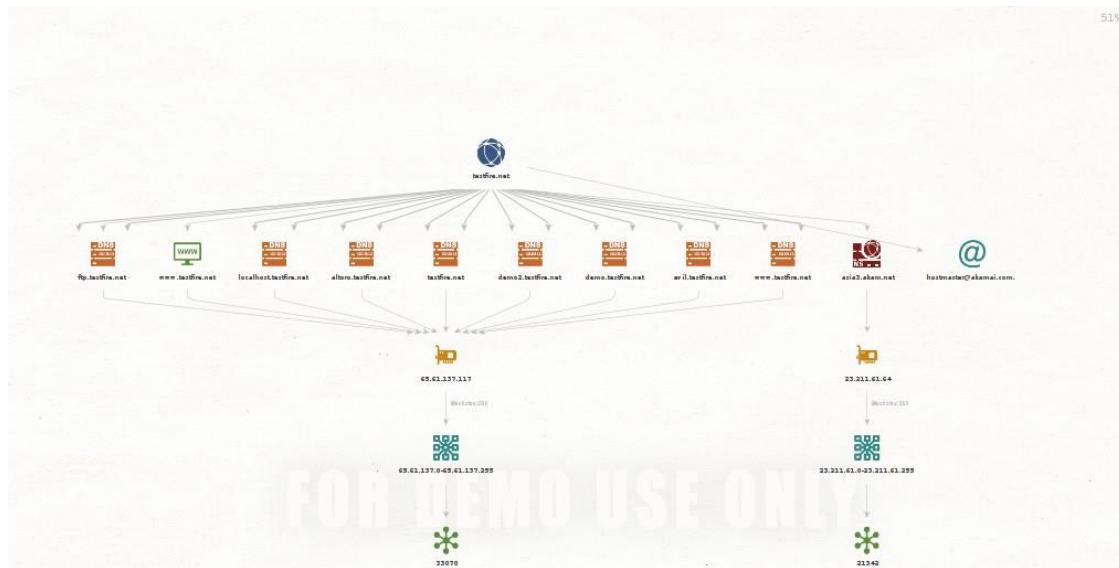
Click of Footprint 1 & Next



Enter a domain I am using testfire.net



Output graph



C) OSRFramework

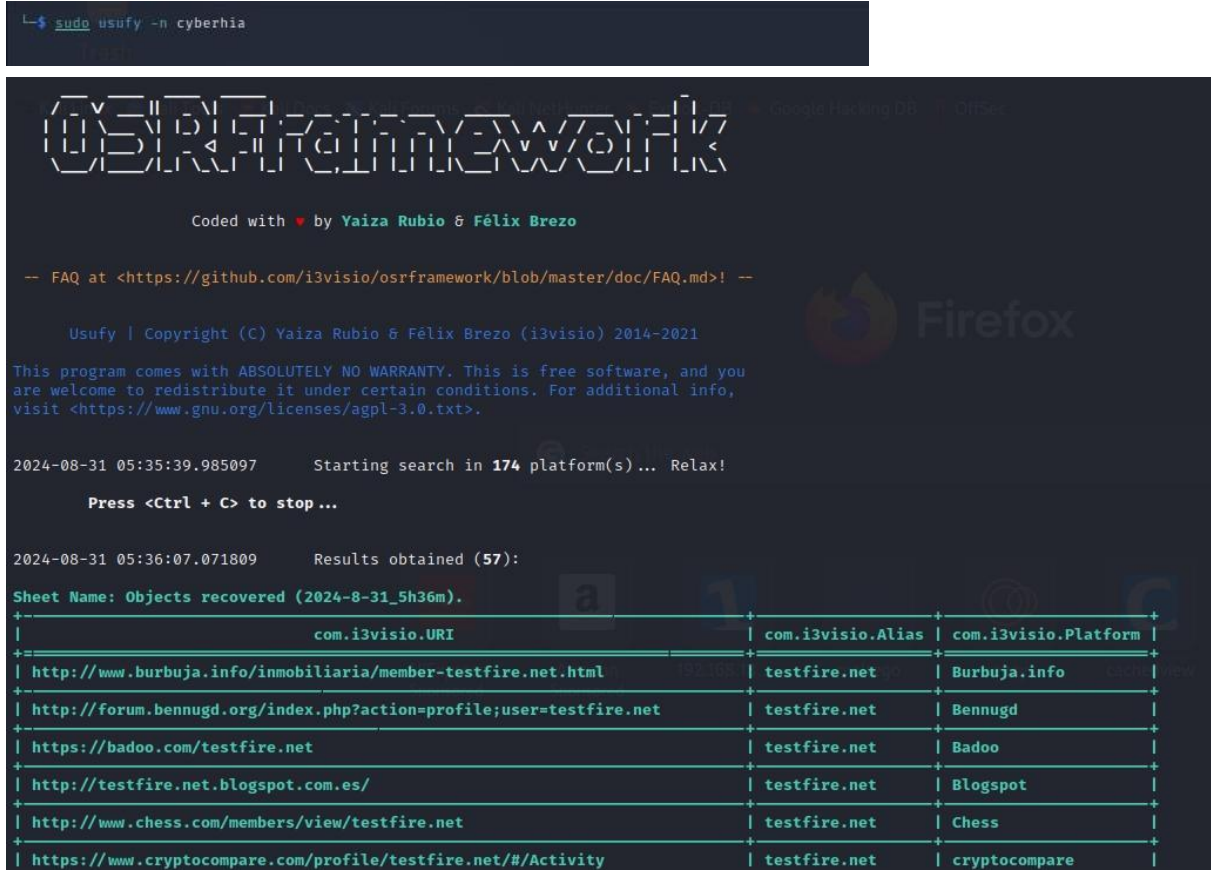
Install OSRFramework (sudo pip install osrframework)

```
$ sudo pip install osrframework
Collecting osrframework
  Downloading osrframework-0.20.5.tar.gz (203 kB)
    203.1/203.1 kB 4.5 MB/s eta 0:00:00
  Preparing metadata (setup.py) ... done
Collecting bs4
  Downloading bs4-0.0.1.tar.gz (1.1 kB)
  Preparing metadata (setup.py) ... done
Collecting cfsrape
  Downloading cfsrape-2.1.1-py3-none-any.whl (12 kB)
Requirement already satisfied: colorama in /usr/lib/python3/dist-packages (from osrframework) (0.4.5)
Collecting configparser
  Downloading configparser-6.0.0-py3-none-any.whl (19 kB)
Requirement already satisfied: decorator in /usr/lib/python3/dist-packages (from osrframework) (5.1.1)
Collecting duckpy
  Downloading duckpy-3.2.0-py3-none-any.whl (5.0 kB)
Requirement already satisfied: networkx in /usr/lib/python3/dist-packages (from osrframework) (2.6.3)
Collecting oauthlib<=1.0.0
  Downloading oauthlib-3.2.2-py3-none-any.whl (151 kB)
    151.7/151.7 kB 7.2 MB/s eta 0:00:00
Collecting pyexcel==0.2.1
  Downloading pyexcel-0.2.1.zip (63 kB)
    63.0/63.0 kB 5.2 MB/s eta 0:00:00
  Preparing metadata (setup.py) ... done
Collecting pyexcel_io==0.1.0
  Downloading pyexcel-io-0.1.0.tar.gz (11 kB)
  Preparing metadata (setup.py) ... done
Collecting pyexcel_ods==0.1.1
  Downloading pyexcel-ods-0.1.1.zip (11 kB)
  Preparing metadata (setup.py) ... done
Collecting pyexcel_text==0.2.0
  Downloading pyexcel-text-0.2.0.zip (12 kB)
  Preparing metadata (setup.py) ... done
Collecting pyexcel_xls==0.1.0
  Downloading pyexcel-xls-0.1.0.tar.gz (5.8 kB)
  Preparing metadata (setup.py) ... done
Collecting pyexcel_xlsx==0.1.0
```

Usufy: This tool is used for searching on multiple search engines to identify the keywords in a URL and to automatically enumerate and store all the results in .csx format. The following is the output of cyberhia as a keyword usufy

usufy -n cyberhia

```
└─$ sudo usufy -n cyberhia
```



```
OSRFramework 1.0.0
Coded with ❤ by Yaiza Rubio & Félix Brezo

-- FAQ at <https://github.com/i3visio/osrframework/blob/master/doc/FAQ.md>! --

Usufy | Copyright (C) Yaiza Rubio & Félix Brezo (i3visio) 2014-2021
This program comes with ABSOLUTELY NO WARRANTY. This is free software, and you
are welcome to redistribute it under certain conditions. For additional info,
visit <https://www.gnu.org/licenses/agpl-3.0.txt>.

2024-08-31 05:35:39.985097    Starting search in 174 platform(s)... Relax!

Press <Ctrl + C> to stop ...

2024-08-31 05:36:07.071809    Results obtained (57):
Sheet Name: Objects recovered (2024-8-31_5h36m).
+-----+-----+-----+
| com.i3visio.URI | com.i3visio.Alias | com.i3visio.Platform |
+-----+-----+-----+
| http://www.burbuja.info/inmobiliaria/member-testfire.net.html | testfire.net | Burbuja.info |
| http://forum.bennugd.org/index.php?action=profile;user=testfire.net | testfire.net | Bennugd |
| https://badoo.com/testfire.net | testfire.net | Badoo |
| http://testfire.net.blogspot.com.es/ | testfire.net | Blogspot |
| http://www.chess.com/members/view/testfire.net | testfire.net | Chess |
| https://www.cryptocompare.com/profile/testfire.net/#/Activity | testfire.net | cryptocompare |
```

Searchfy: This searches for a keyword in Facebook, Github, Instagram, Twitter, YouTube, etc.

sudo searchfy -q cyberhia

```
(kali@kali)-[~]
└─$ sudo searchfy -q cyberhia
```



```
Searchfy | Copyright (C) Yaiza Rubio & Félix Brezo (i3visio) 2014-2021

This program comes with ABSOLUTELY NO WARRANTY. This is free software, and you
are welcome to redistribute it under certain conditions. For additional info,
visit <https://www.gnu.org/licenses/agpl-3.0.txt>.

2023-09-12 05:01:43.382732      Starting search in different platform(s) ... Relax!

Press <Ctrl + C> to stop ...

[*] Launching search using the Github module ...
[*] Launching search using the Instagram module ...
[*] Launching search using the KeyServerUbuntu module ...

2023-09-12 05:01:45.893157      Results obtained:

+-----+
| No data found ... |
+-----+

2023-09-12 05:01:45.893261      You can find all the information collected in the following files:
./profiles.csv

2023-09-12 05:01:45.893291      Finishing execution ...

Total time used:      0:00:02.510559
Average seconds/query: 2.510559 seconds

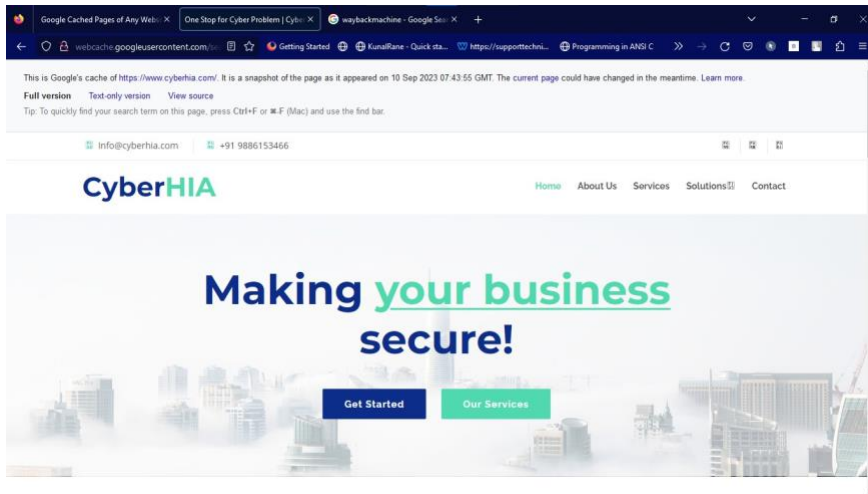
Did something go wrong? Is a platform reporting false positives? Do you need to
integrate a new one and you don't know how to start? Then, you can always place
an issue in the Github project:
https://github.com/i3visio/osrframework/issues
Note that otherwise, we won't know about it!
```

D) Web Archives

First tool is cached view

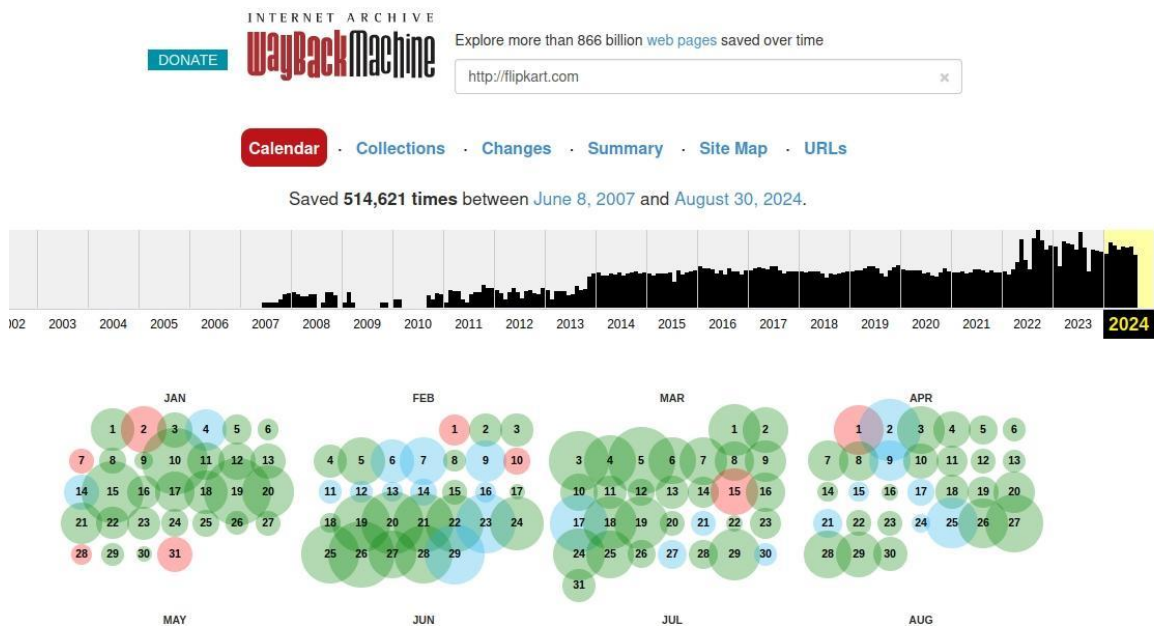
I shows the cached version of a given website





Another tool is wayback machine

It shows the archives of the websites at a given time



F) Web Scraping

Gathering usernames and email addresses

The Harvester is a Python script that searches through popular search engines and other sites for email addresses, hosts, and sub-domains. Using the Harvester is relatively simple as there are only a few commands to set.

the harvester -d github.com -l 500 -b yahoo

```
(kali㉿kali)-[~]
$ theHarvester -d github.com -l 500 -b yahoo
*****
*                                     *
*  _ _ _ _ _  ^  ^  _ _ _ _ _  _ _ _ _ _  _ _ _ _ _  _ _ _ _ _  *
*  | | | | |  /  /  | | | | |  | | | | |  | | | | |  | | | | |  *
*  | | | | |  v  v  | | | | |  | | | | |  | | | | |  | | | | |  *
*  _ _ _ _ _  _ _ _ _ _  _ _ _ _ _  _ _ _ _ _  _ _ _ _ _  _ _ _ _ _  *
*  theHarvester 4.4.3                                     *
*  Coded by Christian Martorella                           *
*  Edge-Security Research                                   *
*  cmartorella@edge-security.com                           *
*  *                                                         *
*****

[*] Target: github.com

[*] Searching Yahoo.

[*] No IPs found.

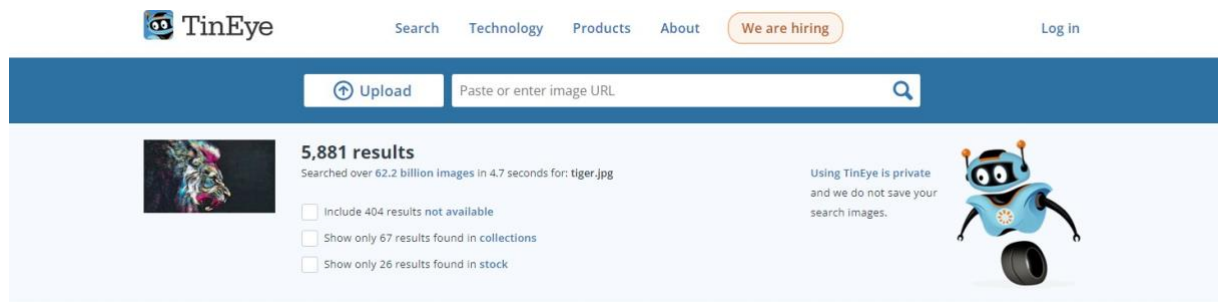
[*] Emails found: 2
-----
git@github.com
press@github.com

[*] Hosts found: 7
-----
cli.github.com
desktop.github.com
docs.github.com
education.github.com
enterprise.github.com
resources.github.com
skills.github.com

(kali㉿kali)-[~]
$
```

G) Obtaining user information

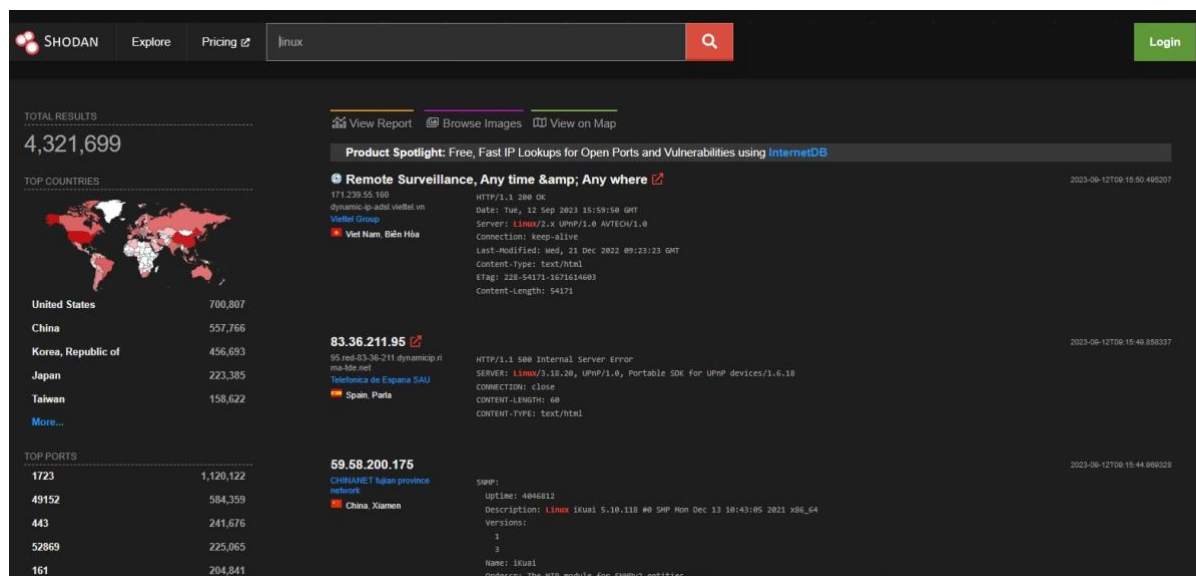
TinEye is a tool to reverse search an image and see where it is being used



H) Online Search Portals

Shodan is a widely known tool in cyber security community it is used to search and gather information about devices and systems

In this example we are checking all the computers that use linux



Censys is another search engine to gather useful information about the target

The screenshot shows the Censys search engine interface. At the top, there's a search bar with the text 'rdnational.ac.in' and a 'Search' button. Below the search bar, there's a 'Results' section with a 'Hosts' tab selected. The 'Hosts' section displays two results: '114.143.218.18 (static-18.218.143.114-tataidc.co.in)' and '103.21.58.98 (sdin-pp-wb4.webhostbox.net)'. Each result shows details like the operating system, services, and ports. On the left side, there are filters for 'Host Filters', 'Labels', 'Autonomous System', 'Location', 'Service Filters', 'Service Names', and 'Ports'.

I) Google Hacking Database

Here is a simple example of Google dork to search any plaintext password on WordPress sites

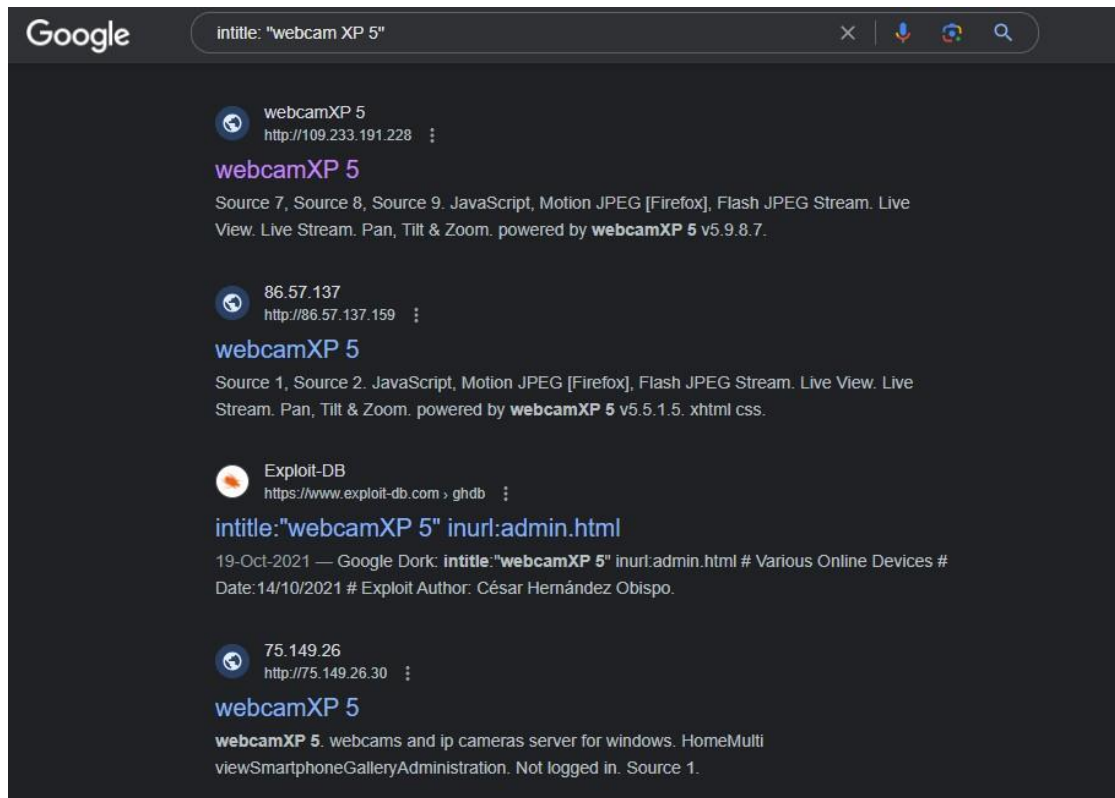
Enter the below search term in Google

inurl:/wp-content/uploads/ ext:txt “username” AND “password” | “pwd” | “pw”

The screenshot shows Google search results for the query 'inurl:/wp-content/uploads ext:txt "username" AND "password" | "pwd" | "pw"'. The search bar at the top contains the query. Below the search bar, there's a 'Tools' button. The search results show 'About 1,200 results (0.39 seconds)'. The first result is from 'ostademusic.com' with a file named 'pass.txt'. The second result is from 'Haldwani Realtors' with a file named 'pasd.txt'. The third result is from 'Charlers, Tyler, Zack & Shearer, P. C.' with a file named 'Sawchuck-apr25.txt'. The fourth result is from 'Selectabase' with a file named 'accounts.txt'.

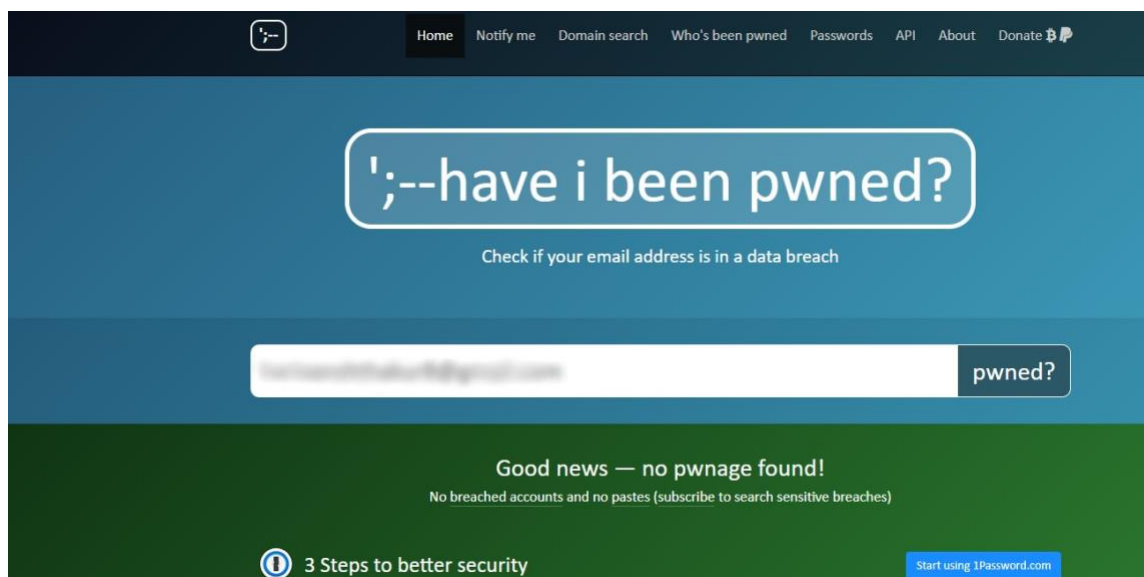
Another search term to get webcams

Intitle: "webcam XP 5"



J) Security breaches

haveibeenpwned.com tells about a given email if it has been breached/leaked in past cyber security attacks



K) Profiling users for password lists

Note: List of commonly used passwords are stored in `/usr/share/wordlists` directory in kali linux

CUPP (Common User Password Profiler) is a tool that allows pentesters to generate a wordlist specific to a particular user. (if not already installed; `sudo apt install cupp`)

To start the interactive process

cupp -i

```
cupp.py! | cat # Common words with Google search address
# User
# Passwords if found in Kali NetHunter, Exploit-DB, etc
# Profiler

[ Muris Kurgas | j0rgan@remote-exploit.org ]
[ Mebus | https://github.com/Mebus/ ]

[+] Insert the information about the victim to make a dictionary
[+] If you don't know all the info, just hit enter when asked! ;)

> First Name: Mayuresh
> Surname: Tiwari
> Nickname: Mayur
> Birthdate (DDMMYYYY): 05/06/2003

[-] You must enter 8 digits for birthday!
> Birthdate (DDMMYYYY): 05062003

> Partners) name: Urmila
> Partners) nickname: Urmi
> Partners) birthdate (DDMMYYYY): 02102003

> Child's name: Sherlock
> Child's nickname: Sher
> Child's birthdate (DDMMYYYY): 01022030

> Pet's name: Subbu
> Company name: Govt Of India

> Do you want to add some key words about the victim? Y/[N]: n
> Do you want to add special chars at the end of words? Y/[N]: y
> Do you want to add some random numbers at the end of words? Y/[N]:
> Leet mode? (i.e. leet = 1337) Y/[N]: 8369

[+] Now making a dictionary...
[+] Sorting list and removing duplicates...
[+] Saving dictionary to mayuresh.txt, counting 11765 words.
```

```
~/mayuresh .txt [Read Only] - Mousepad
File Edit Search View Document Help
+ [Icons] x [Icons] [Icons] [Icons] [Icons] [Icons] [Icons] [Icons] [Icons] [Icons] [Icons] [Icons] [Icons]
1371 Mayuresh 50
1372 Mayuresh 6
1373 Mayuresh 65
1374 Mayuresh @
1375 Mayuresh @!
1376 Mayuresh @$
1377 Mayuresh @%
1378 Mayuresh @&
1379 Mayuresh @*
1380 Mayuresh @@
1381 Mayuresh _5
1382 Mayuresh _6
1383 Mayurtiwari
1384 Sher !!
1385 Sher !!!
1386 Sher !! $
1387 Sher !! %
1388 Sher !! &
1389 Sher !! '#'
1390 Sher !! *
1391 Sher !! @
1392 Sher! $
1393 Sher! $!
```

L) Creating custom wordlists for cracking password

Cewl is a tool that scrapes a web page and generates a wordlist based on the keywords found on that web page (sudo apt install cewl)

```
(kali㉿kali)-[~]
└─$ cewl www.google.com -w google.txt
CeWL 5.5.2 (Grouping) Robin Wood (robin@digi.ninja) (https://digi.ninja/)

(kali㉿kali)-[~]
└─$ cat google.txt | head -n 10
the
your
you
requests
page
computer
network
This
may
google

(kali㉿kali)-[~]
└─$ wc google.txt
258 258 2486 google.txt

(kali㉿kali)-[~]
└─$
```