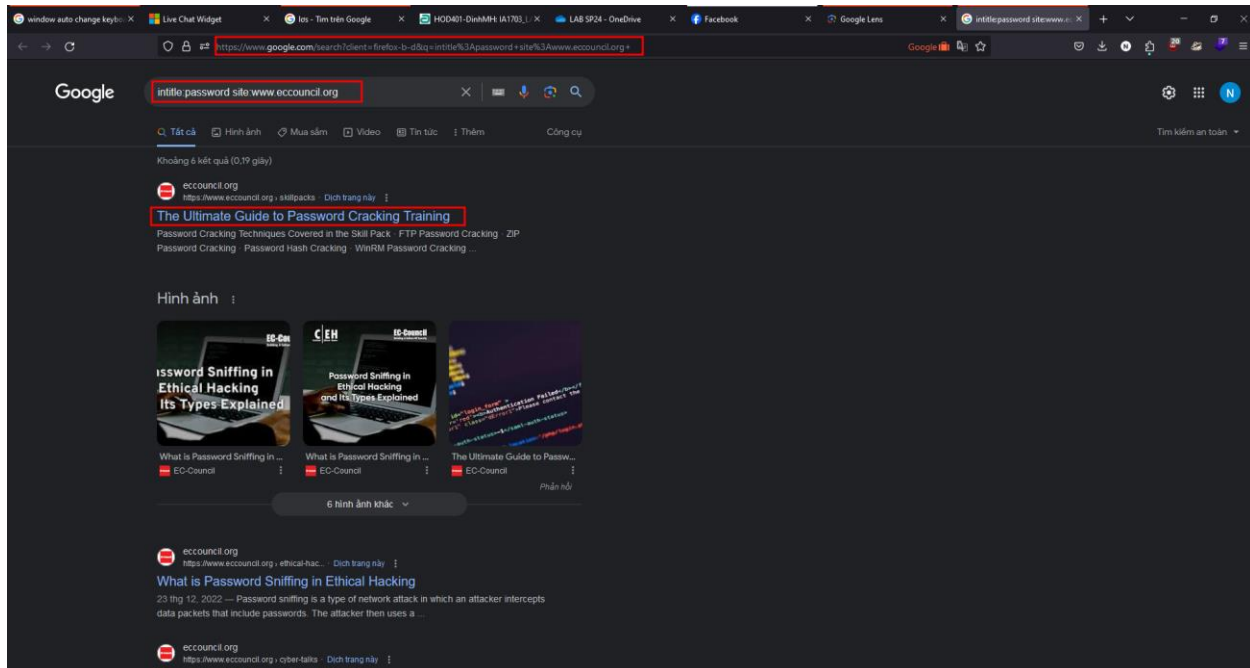
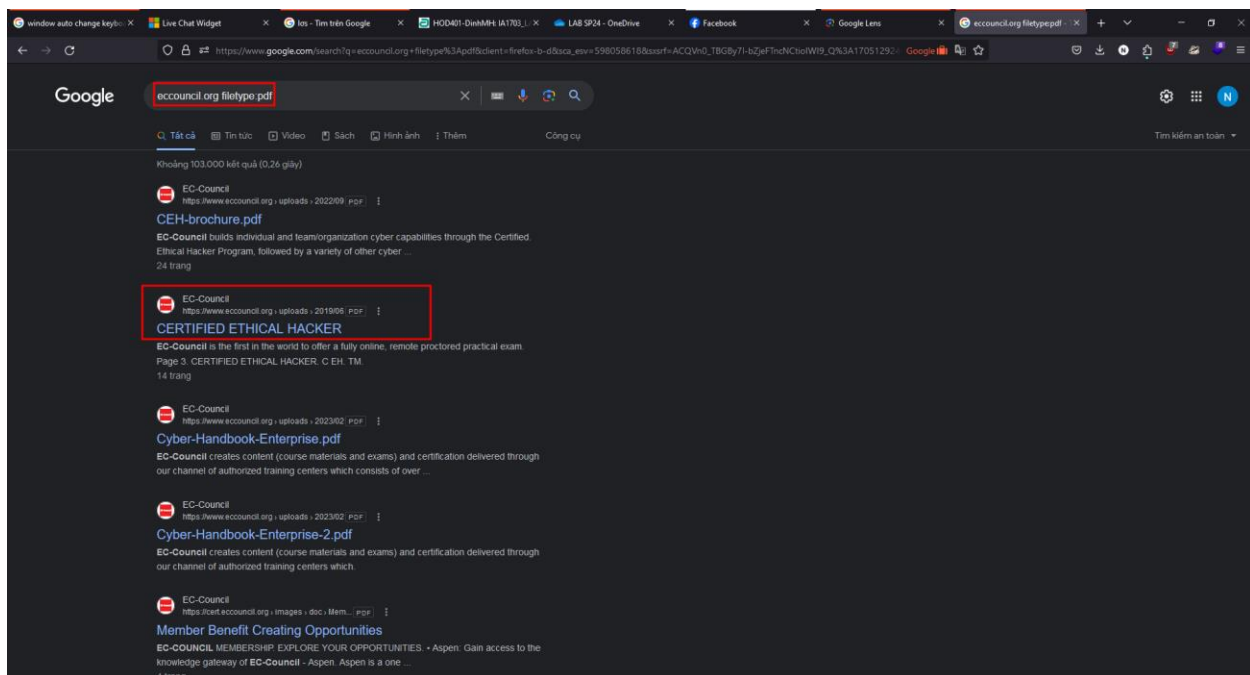


Task 1.1 Perform advance google hacking for password file

Type `intitle:password site:www.eccouncil.org` and press Enter. This search command uses `intitle` and `site` Google advanced operators, which restrict results to pages on the `www.eccouncil.org` website that contain the term `password` in the title. An example is shown in the screenshot below.



Now, navigate back to `https://www.google.com`. In the search bar, type the command `EC-Council filetype:pdf` and press Enter to search your results based on the file extension.



The page appears displaying the PDF file, as shown in the screenshot.



Apart from the aforementioned advanced Google operators, you can also use the following to perform an advanced search to gather more information about the target organization from publicly available sources.

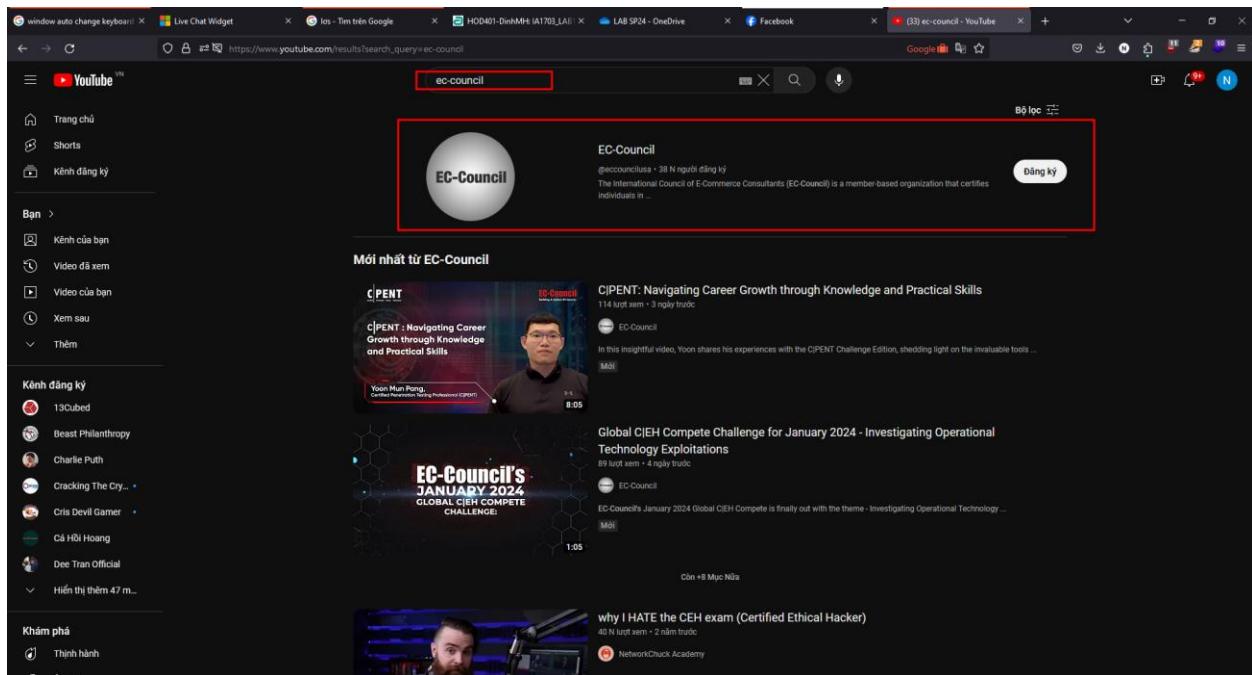
- **cache:** This operator allows you to view cached version of the web page.
[cache: www.google.com]- Query returns the cached version of the website www.google.com
- **allinurl:** This operator restricts results to pages containing all the query terms specified in the URL.
[allinurl: google career]-Query returns only pages containing the words "google" and "career" in the URL
- **inurl:** This operator restricts the results to pages containing the word specified in the URL
[inurl: copy site:www.google.com]-Query returns only pages in Google site in which the URL has the word "copy"
- **allintitle:** This operator restricts results to pages containing all the query terms specified in the title.
[allintitle: detect malware]-Query returns only pages containing the words "detect" and "malware" in the title
- **inanchor:** This operator restricts results to pages containing the query terms specified in the anchor text on links to the page.
[Anti-virus inanchor:Norton]-Query returns only pages with anchor text on links to the pages containing the word "Norton" and the page containing the word "Anti-virus"
- **allinanchor:** This operator restricts results to pages containing all query terms specified in the anchor text on links to the page.
[allinanchor: best cloud service provider]-Query returns only pages in which the anchor text on links to the pages contain the words "best," "cloud," "service," and "provider"

- link: This operator searches websites or pages that contain links to the specified website or page.
[link:www.googleguide.com]-Finds pages that point to Google Guide's home page
- related: This operator displays websites that are similar or related to the URL specified.
[related:www.certifiedhacker.com]-Query provides the Google search engine results page with websites certifiedhacker.com
- info: This operator finds information for the specified web page.
[info:gothotel.com]-Query provides information about the national hotel directory GotHotel.com home page
- location: This operator finds information for a specific location.
[location: 4 seasons restaurant]-Query give you results based around the term 4 seasons restaurant

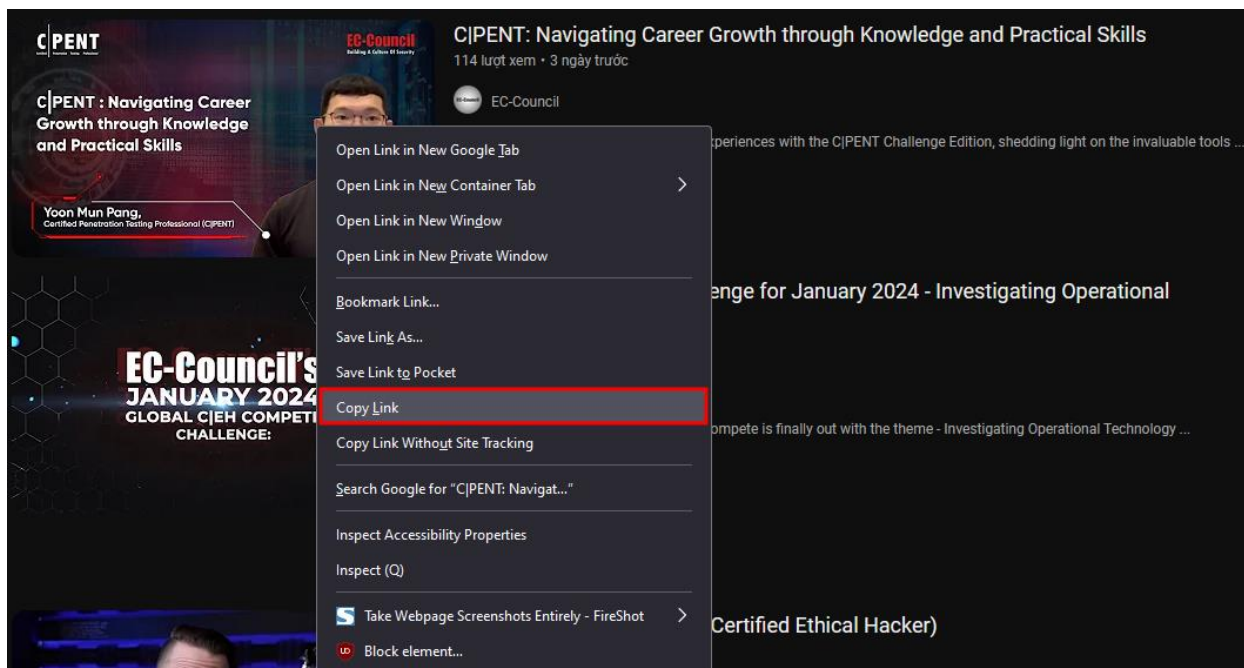
Task 2: Gather Information from Video Search Engines

In the Windows 10 virtual machine, open any web browser (here, Mozilla Firefox) and navigate to <https://www.youtube.com/>.

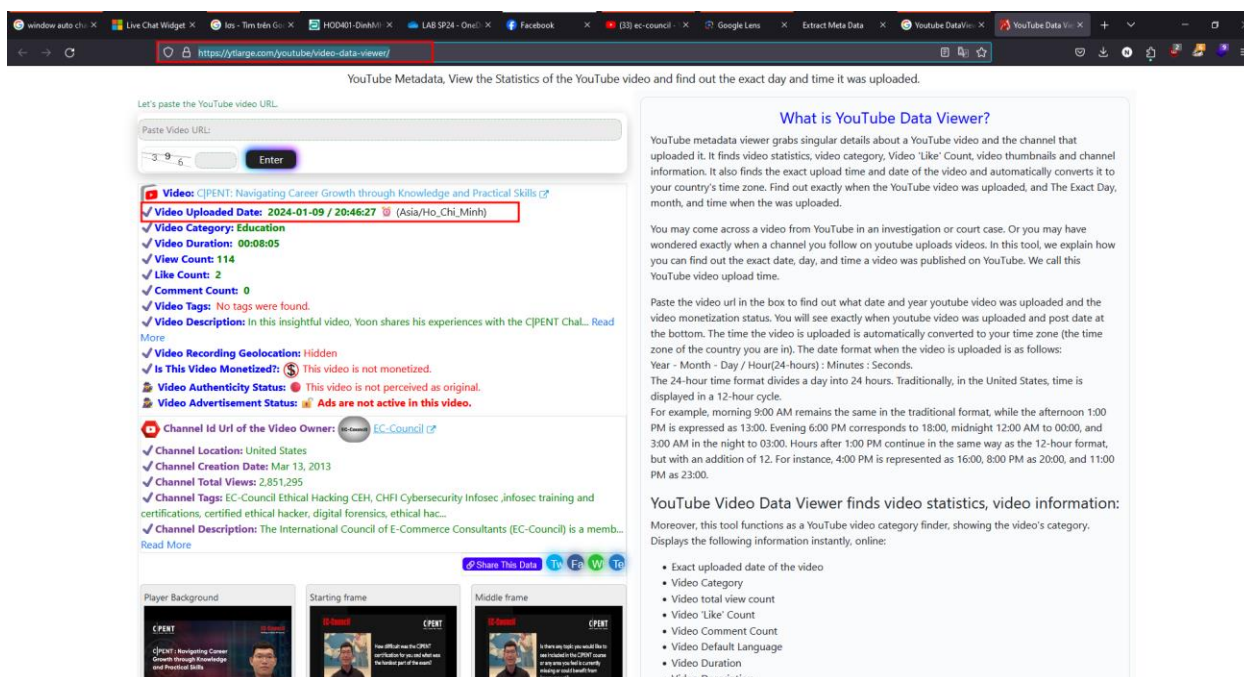
In the search bar, search for your target organization (here, ec-council). You will see all the latest videos uploaded by the target organization.



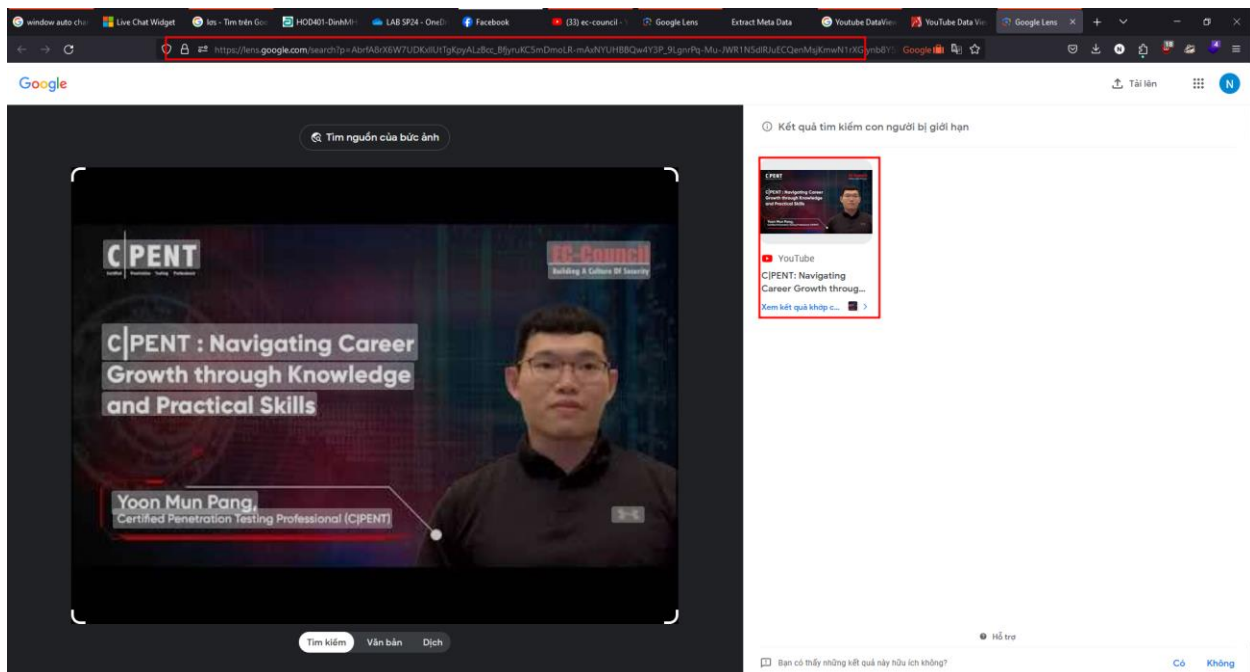
Select any video of your choice, right-click on the video title, and click **Copy Link**.



After the video link is copied, open another browser tab in Mozilla Firefox, and then navigate to <https://ytlarge.com/youtube/video-data-viewer/>. In the Enter YouTube URL search box, paste the copied YouTube video link and click Go.



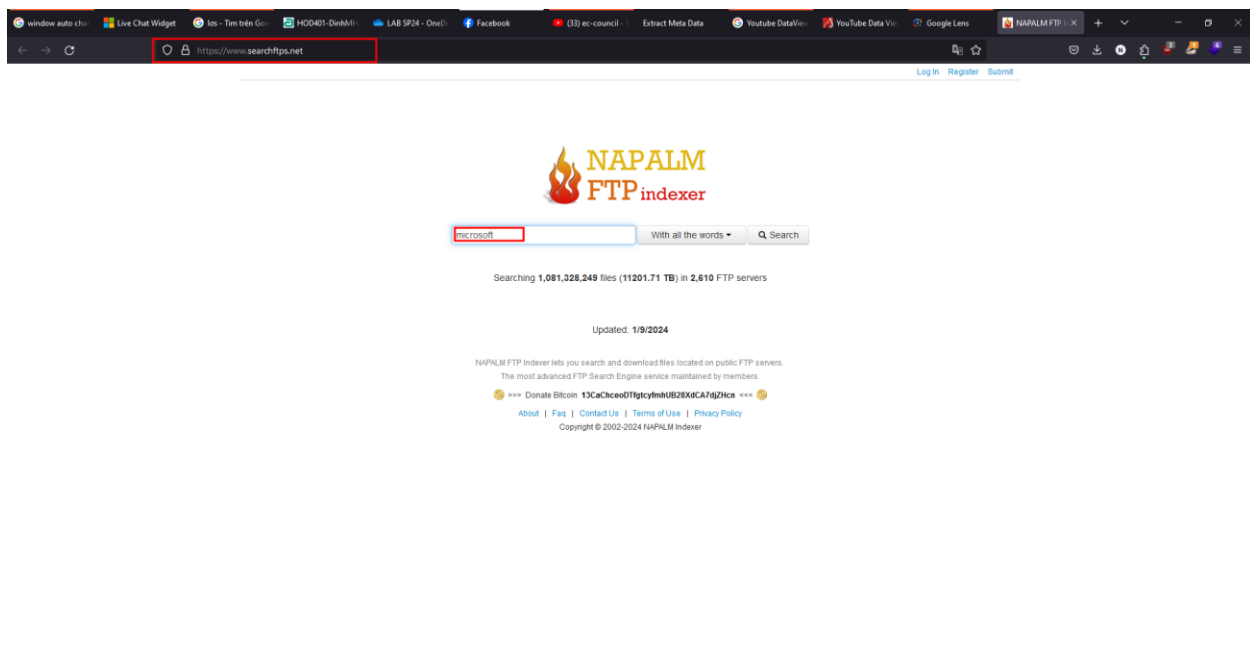
A new tab in Google opens, and the results for the reverse image search are displayed.



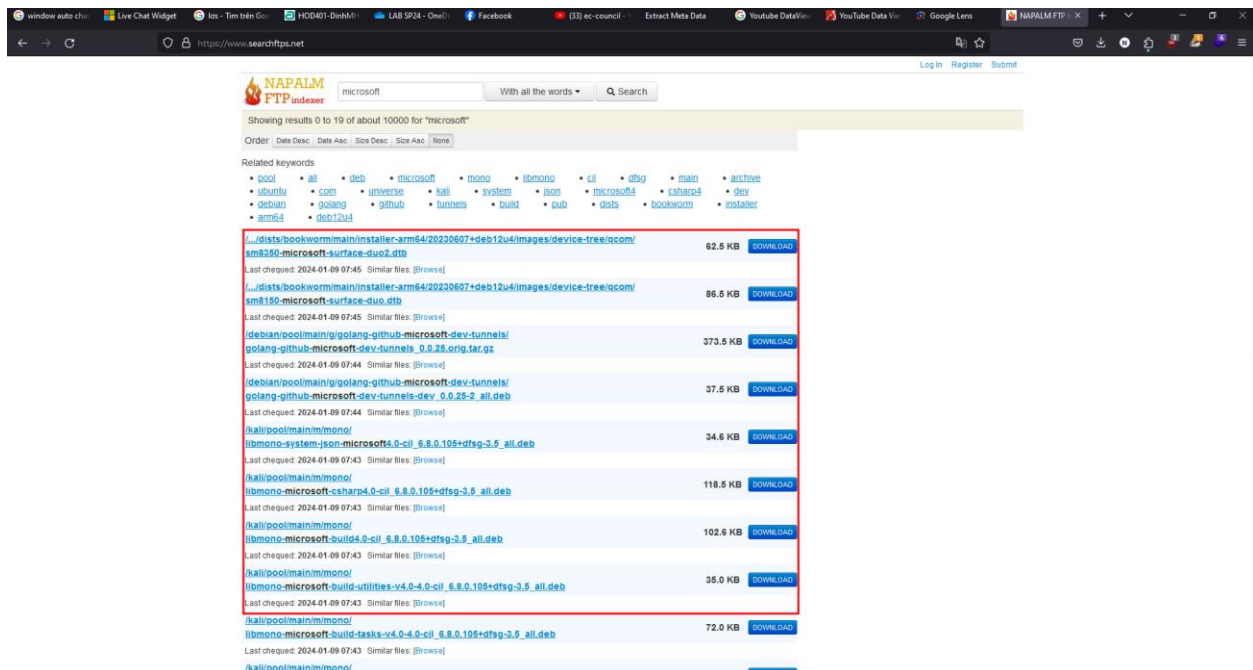
Task 3: Gather information from FTP search engine

In the Windows 10 virtual machine, open any web browser (here, Mozilla Firefox) and navigate to <https://www.searchftps.net/>.

In the search bar, type microsoft and click Search.



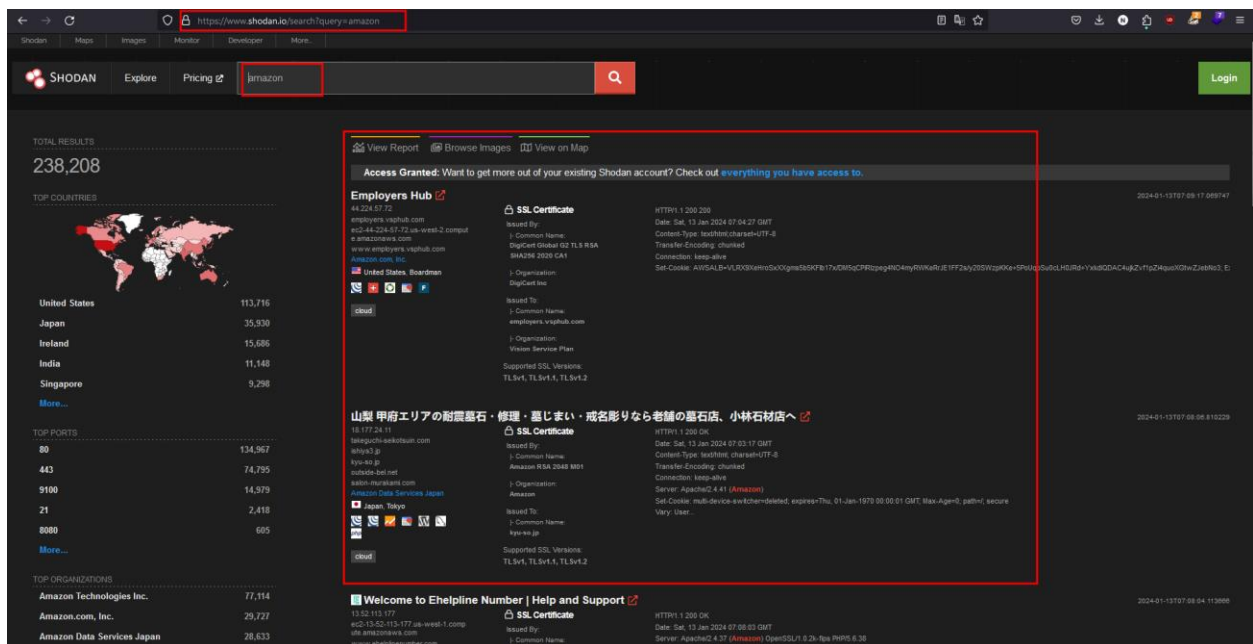
You will get the search results with the details of the FTP in the target organization, as shown in the screenshot.



Task 4: Gather information from IOT search engine

In the Windows 10 virtual machine, open any web browser (here, Mozilla Firefox) and navigate to <https://www.shodan.io/>.

In the search bar, type amazon and press Enter. You will obtain the search results with the details of all the vulnerable IoT devices related to amazon in various countries, as shown in the screenshot.



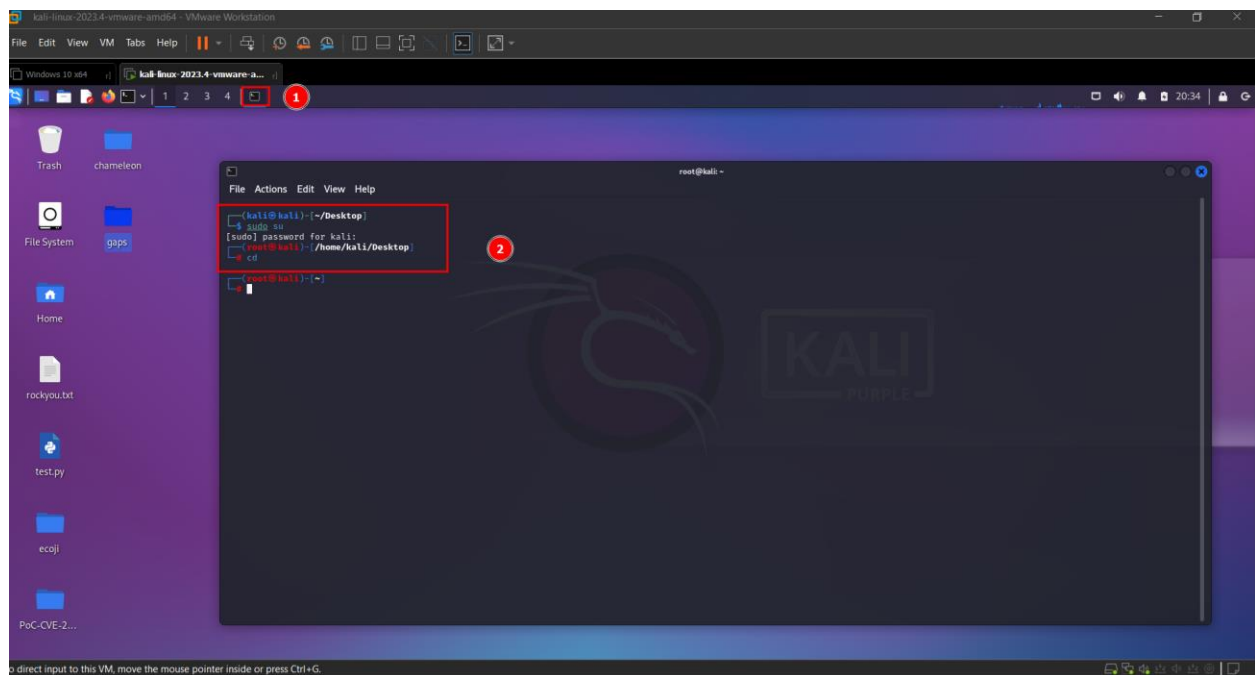
LAB 03

Here, we will gather information about the employees (name and job title) of a target organization that is available on LinkedIn using the Harvester tool.

1. Turn on Kali Security virtual machine.
2. In the login page, the Kali username will be selected by default. Enter password as toor in the Password field and press Enter to log in to the machine.
3. Click the Terminal icon at the top of the Desktop window to open a Terminal window.
4. A Parrot Terminal window appears. In the terminal window, type `sudo su` and press Enter to run the programs as a root user.
5. In the [sudo] password for Kali field, type toor as a password and press Enter.

Note: The password that you type will not be visible.

6. Now, type `cd` and press Enter to jump to the root directory



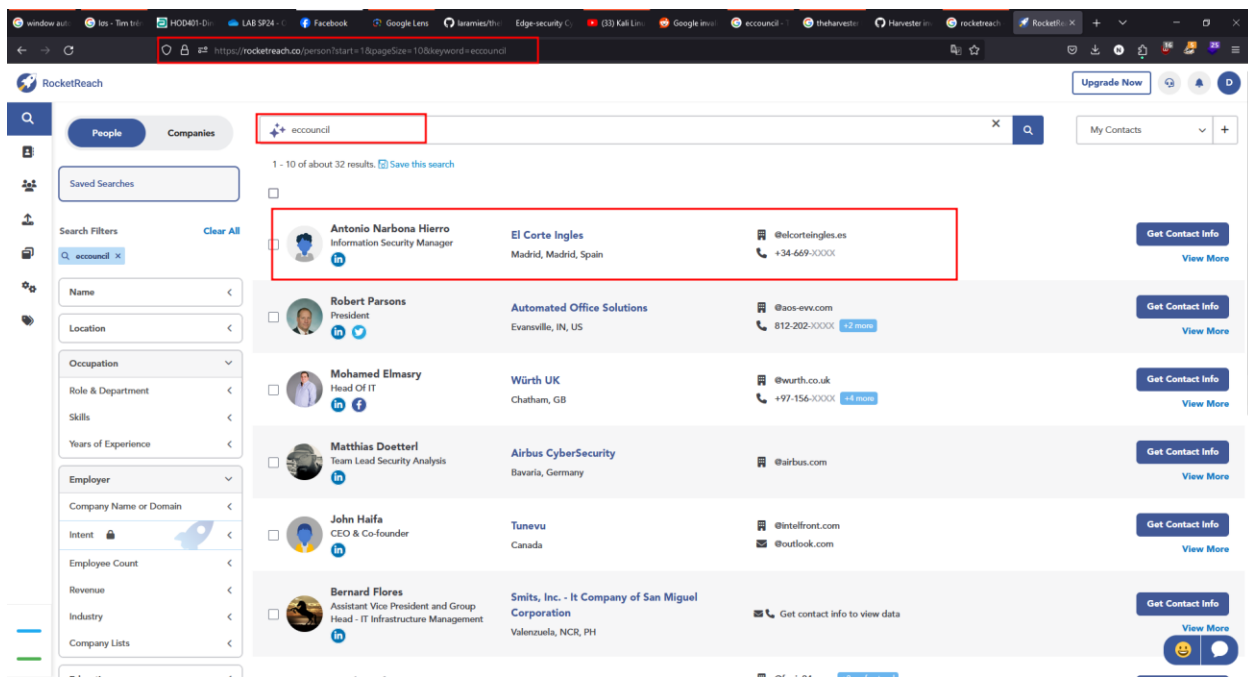
7. In the terminal window, type `theHarvester -d eccouncil -l 200 -b linkedin` and press Enter to see 200 results of EC-Council from the LinkedIn source. Scroll down to view all the 200 results of the employees of the EC-Council.

Note: In this command, `-d` specifies the domain or company name to search, `-l` specifies the number of results to be retrieved, and `-b` specifies the data source as LinkedIn.

But due to theHarvester using Google to search for the information, due to this article:

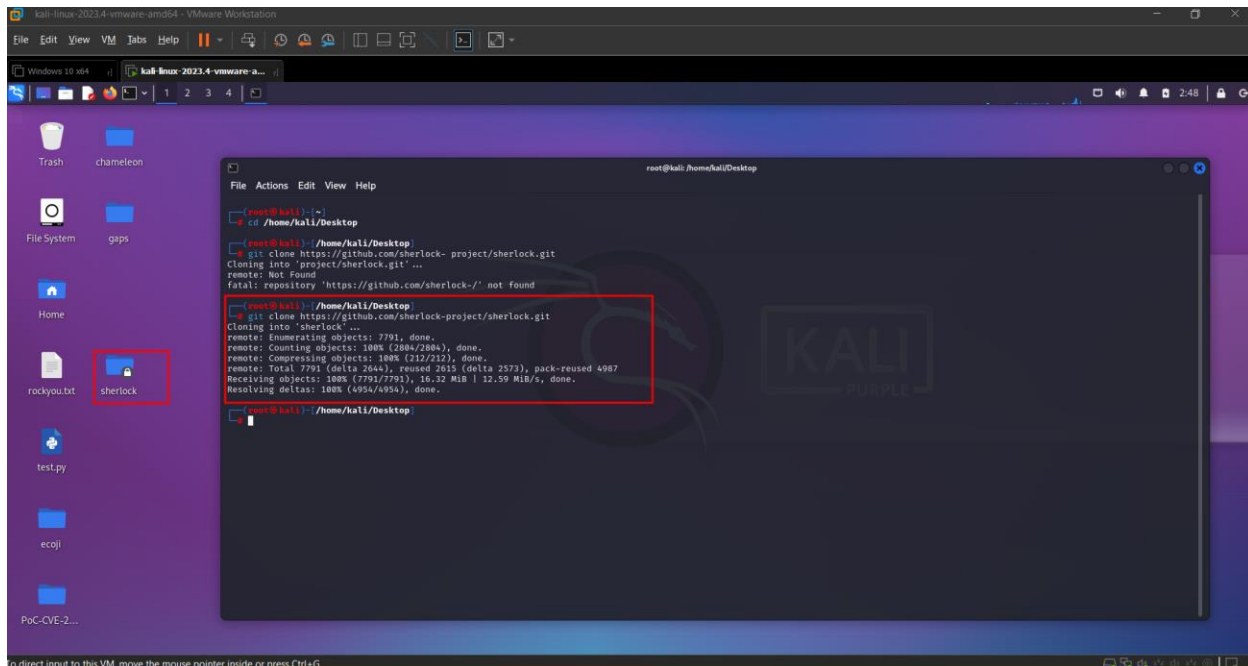
<https://github.com/laramies/theHarvester/issues/1224>

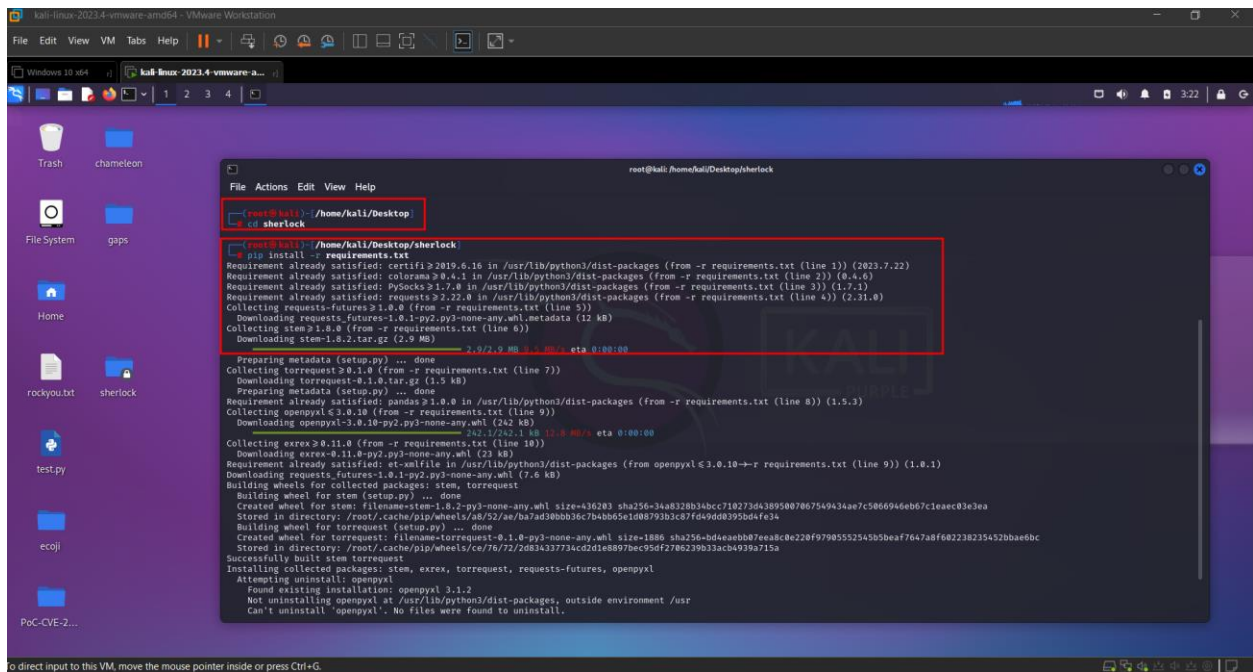
Instead we will use rocketsearch



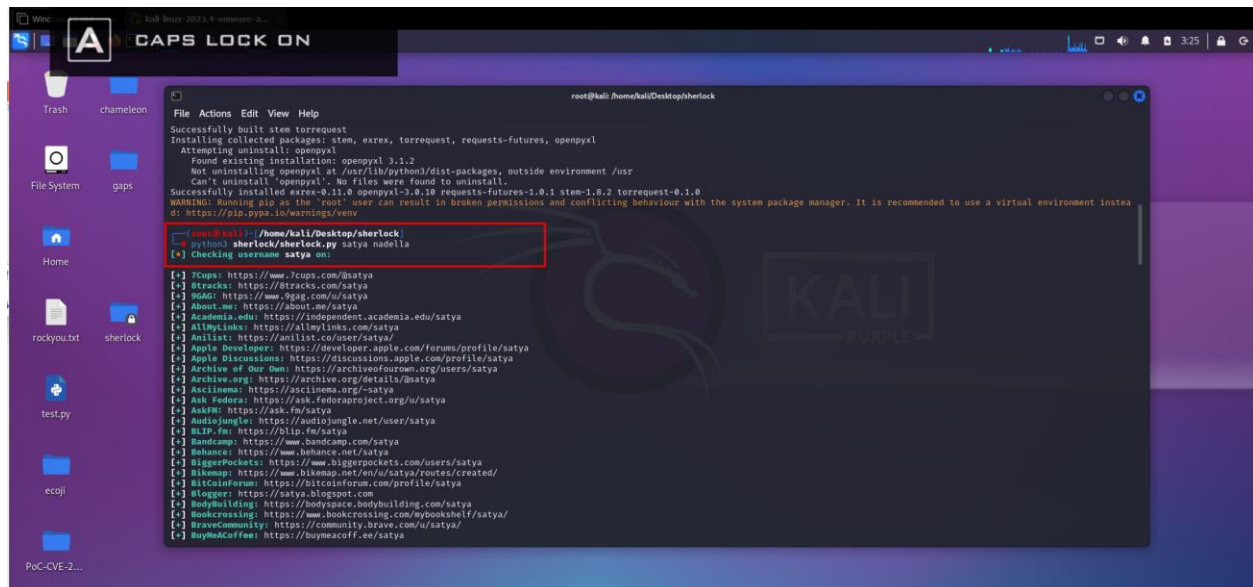
Task 2: Gather information using Sherlock

In the Parrot Terminal window, type `git clone https://github.com/sherlock-project/sherlock.git` and press Enter





Now, type `python3 sherlock.py satya nadella` and press Enter. You will get all the URLs related to Satya Nadella, as shown in the screenshot. Scroll down to view all the results.



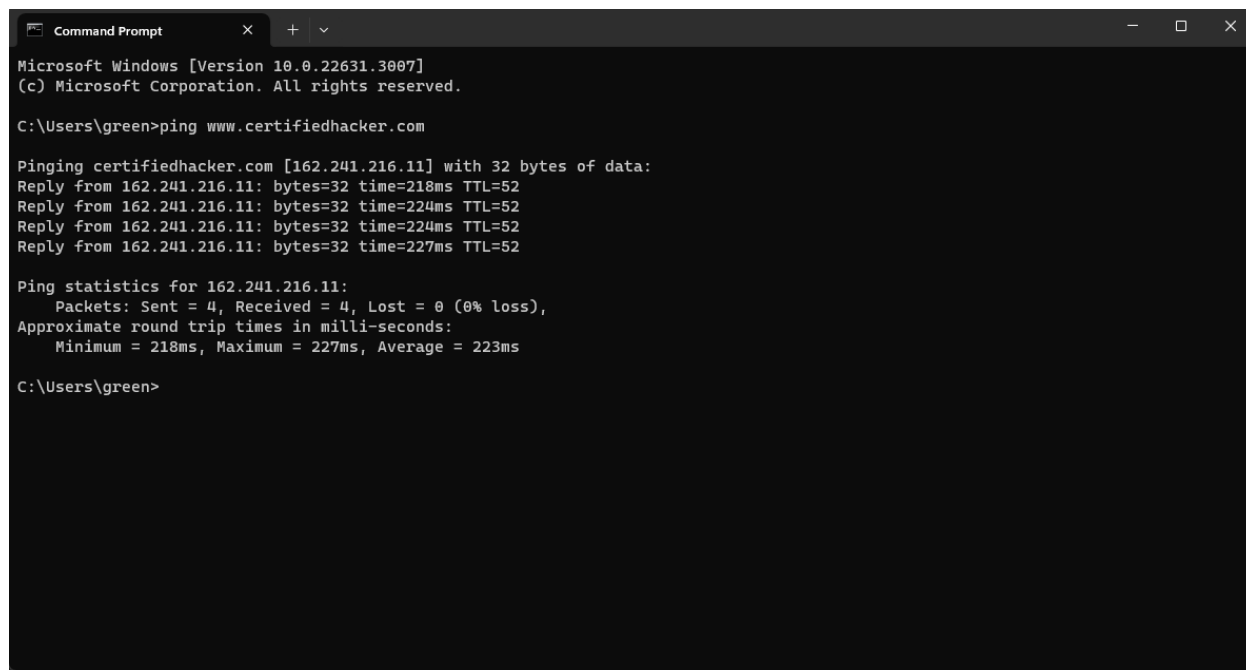
Task 3: Gather Information using Followerhonk

Open any web browser (here, Mozilla Firefox) and navigate to <https://followerwonk.com/analyze>. In the screen name search bar, type your target individual's twitter tag (here, @satyanadella) and click the Do it button to analyze the users whom the target person follows.

This site is not available for analyzing the person follows anymore

LAB 04: Gather Information About a Target Website using Ping Command Line Utility

Open the Command Prompt window. Type `ping www.certifiedhacker.com` and press Enter to find its IP address. The displayed response should be similar to the one shown in the screenshot



```
Microsoft Windows [Version 10.0.22631.3007]
(c) Microsoft Corporation. All rights reserved.

C:\Users\green>ping www.certifiedhacker.com

Pinging certifiedhacker.com [162.241.216.11] with 32 bytes of data:
Reply from 162.241.216.11: bytes=32 time=218ms TTL=52
Reply from 162.241.216.11: bytes=32 time=224ms TTL=52
Reply from 162.241.216.11: bytes=32 time=224ms TTL=52
Reply from 162.241.216.11: bytes=32 time=227ms TTL=52

Ping statistics for 162.241.216.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 218ms, Maximum = 227ms, Average = 223ms

C:\Users\green>
```

Note the target domain's IP address in the result above (here, 162.241.216.11). You also obtain information on Ping Statistics such as packets sent, packets received, packets lost, and approximate round-trip time.

In the Command Prompt window, type `ping www.certifiedhacker.com -f -l 1500` and press Enter

- **ping:** This is the command itself, indicating that you want to send a network ping.
- **www.certifiedhacker.com:** This is the hostname or IP address of the destination you want to ping. In this case, it's "www.certifiedhacker.com." The `ping` command will send a series of network packets to this destination.
- **-f:** This option sets the "Don't fragment" flag in the packet. It means that the packet should not be divided into smaller fragments during transmission. If the packet is too large for the network to handle in one piece, it will be dropped, and you'll receive an error message.
- **-l 1500:** This option sets the size of the data portion of the ping packet to 1500 bytes. The data portion is the actual content of the packet, excluding the headers. In this case, it's set to 1500 bytes, which is often the maximum size that can be transmitted over a standard Ethernet connection without fragmentation.

```
C:\Users\green>ping www.certifiedhacker.com -f -l 1500

Pinging certifiedhacker.com [162.241.216.11] with 1500 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 162.241.216.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

The response, Packet needs to be fragmented but DF set, means that the frame is too large to be on the network and needs to be fragmented. The packet was not sent as we used the switch with the ping command, and the ping command returned this error.

In the Command Prompt window, type ping www.certifiedhacker.com -f -l 1300 and press Enter.

```
C:\Users\green>ping www.certifiedhacker.com -f -l 1300

Pinging certifiedhacker.com [162.241.216.11] with 1300 bytes of data:
Reply from 162.241.216.11: bytes=1300 time=220ms TTL=52
Reply from 162.241.216.11: bytes=1300 time=217ms TTL=52
Reply from 162.241.216.11: bytes=1300 time=224ms TTL=52
Reply from 162.241.216.11: bytes=1300 time=206ms TTL=52

Ping statistics for 162.241.216.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 206ms, Maximum = 224ms, Average = 216ms

C:\Users\green>
```

Now, try different values until you find the maximum frame size. For

instance, ping www.certifiedhacker.com -f -l 1473 replies with Packet needs to be fragmented but DF set, and ping

www.certifiedhacker.com -f -l 1472 replies with a successful ping. It indicates that 1472 bytes are the maximum frame size on this machine's network

```
C:\Users\green>ping www.certifiedhacker.com -f -l 1432

Pinging certifiedhacker.com [162.241.216.11] with 1432 bytes of data:
Reply from 162.241.216.11: bytes=1432 time=213ms TTL=52
Reply from 162.241.216.11: bytes=1432 time=220ms TTL=52
Reply from 162.241.216.11: bytes=1432 time=208ms TTL=52
Reply from 162.241.216.11: bytes=1432 time=211ms TTL=52

Ping statistics for 162.241.216.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 208ms, Maximum = 220ms, Average = 213ms

C:\Users\green>ping www.certifiedhacker.com -f -l 1472

Pinging certifiedhacker.com [162.241.216.11] with 1472 bytes of data:
Reply from 192.168.1.1: Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 162.241.216.11:
    Packets: Sent = 4, Received = 1, Lost = 3 (75% loss),

C:\Users\green>
```

In Command Prompt, type `ping www.certifiedhacker.com -i 3` and press Enter. This option sets the time to live (-i) value as 3.

```
C:\Users\green>ping www.certifiedhacker.com -i 3

Pinging certifiedhacker.com [162.241.216.11] with 32 bytes of data:
Reply from 42.112.3.125: TTL expired in transit.
Reply from 42.112.3.125: TTL expired in transit.
Request timed out.
Reply from 42.112.3.125: TTL expired in transit.

Ping statistics for 162.241.216.11:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
```

Reply from 42.112.3.125: TTL expired in transit means that the router discarded the frame because its TTL has expired (reached 0).

Minimize the command prompt shown above and launch a new command prompt. Type `ping www.certifiedhacker.com -i 2 -n 1` and press Enter. Here, we set the TIL value to 2 and the -n value to 1 to check the life span of the packet.

```
C:\Users\green>ping www.certifiedhacker.com -i 2 -n 1

Pinging certifiedhacker.com [162.241.216.11] with 32 bytes of data:
Reply from 100.123.1.166: TTL expired in transit.

Ping statistics for 162.241.216.11:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),

C:\Users\green>
```

Changing until it can reach

```
C:\Users\green>ping www.certifiedhacker.com -i 27 -n 1

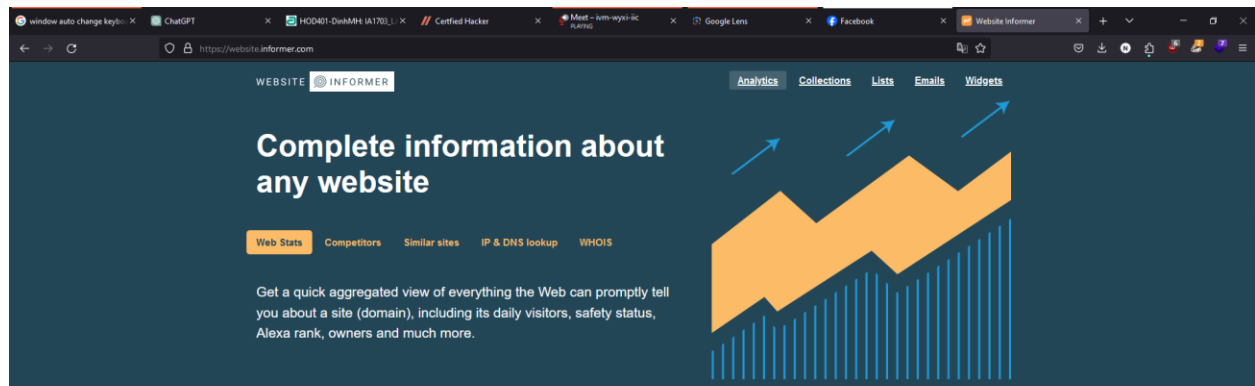
Pinging certifiedhacker.com [162.241.216.11] with 32 bytes of data:
Reply from 162.241.216.11: bytes=32 time=219ms TTL=52

Ping statistics for 162.241.216.11:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 219ms, Maximum = 219ms, Average = 219ms

C:\Users\green>
```

Task: Gather Information about a Target Website using Website Informer

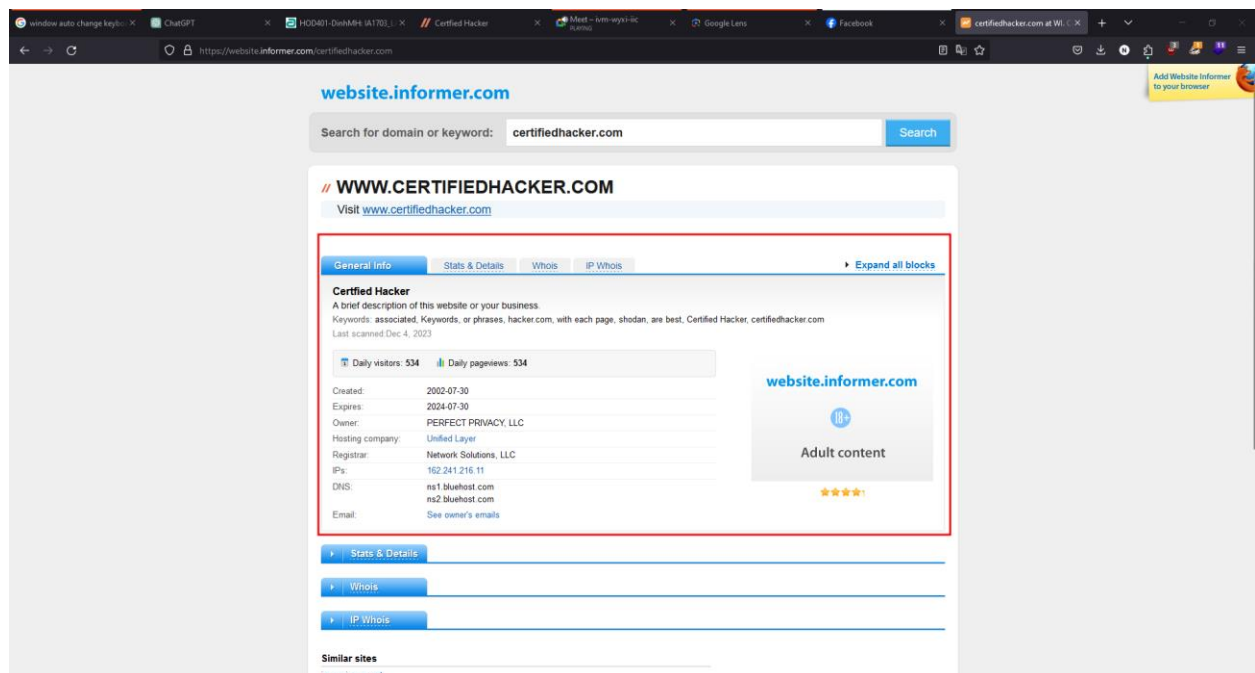
In the Windows 10 virtual machine, open a web browser (here, Mozilla Firefox), type `https://website.informer.com` in the address bar, and press Enter. The Website Informer website appears, as shown in the screenshot.



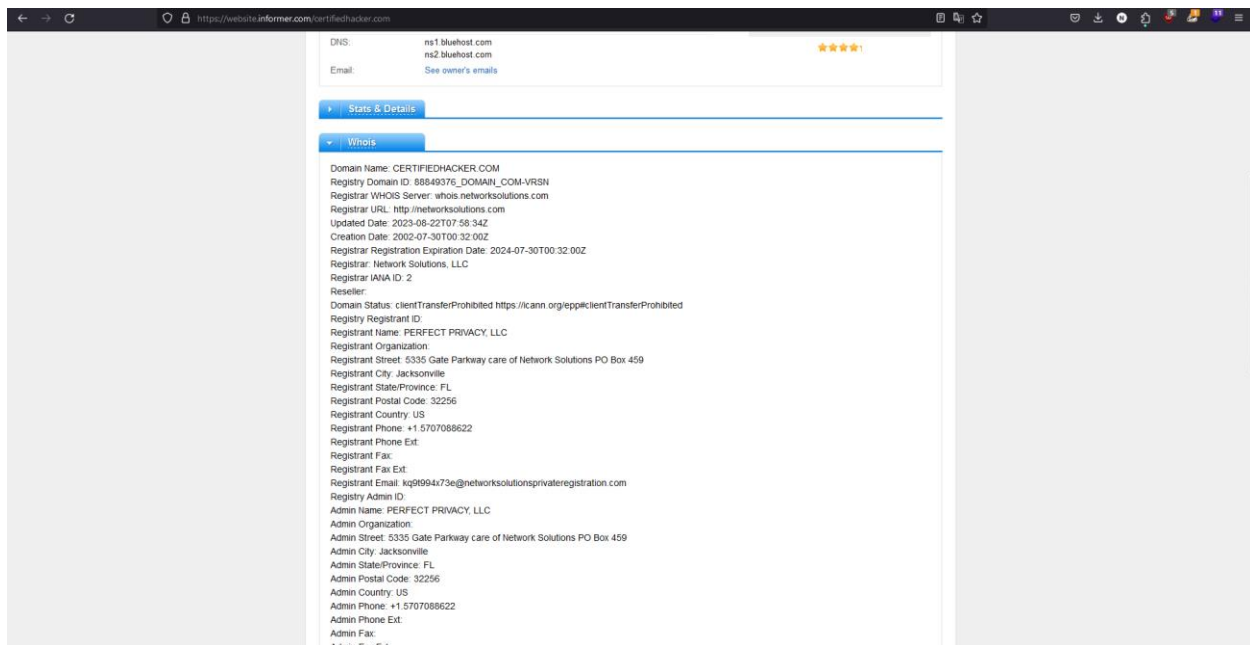
Website Informer is a special service for web masters that gathers detailed information on websites. The service is very easy-to-use — simply search for the URL, keyword or install our Widget and there you go!

Add Website Informer widget to your browser

In the General Info tab, information such as Created, Expires, Owner, Hosting company, Registrar, IPs, DNS, and Email associated with the target website is displayed as shown in the screenshot.



Click on the Whois tab to view detailed Whois information about the target website, as shown in the screenshot

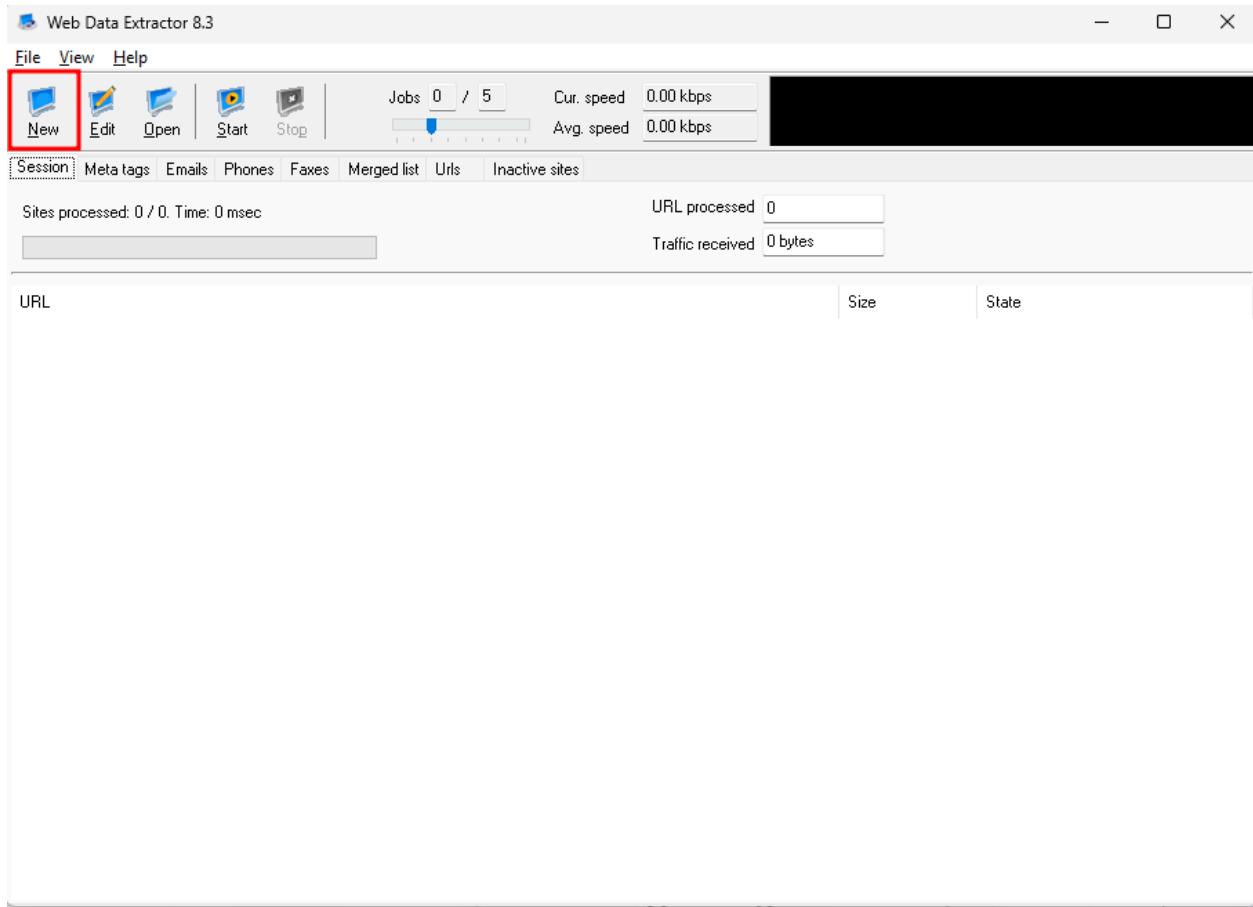


Similarly, you can click on the Stats & Details and IP Whois tabs to view the detailed information of the target website.

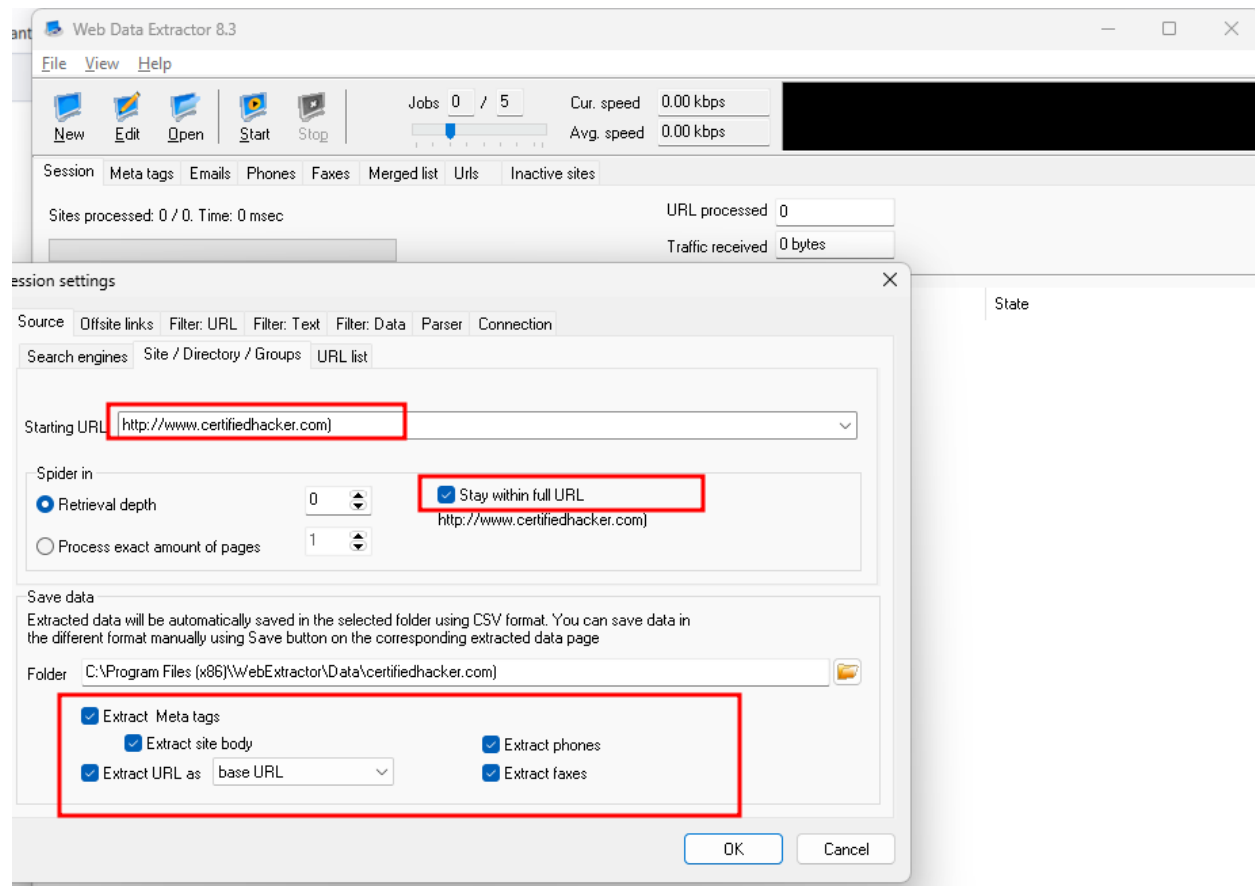
This concludes the demonstration of gathering information about a target website using the Website Informer online tool.

Close all open windows and document all the acquired information

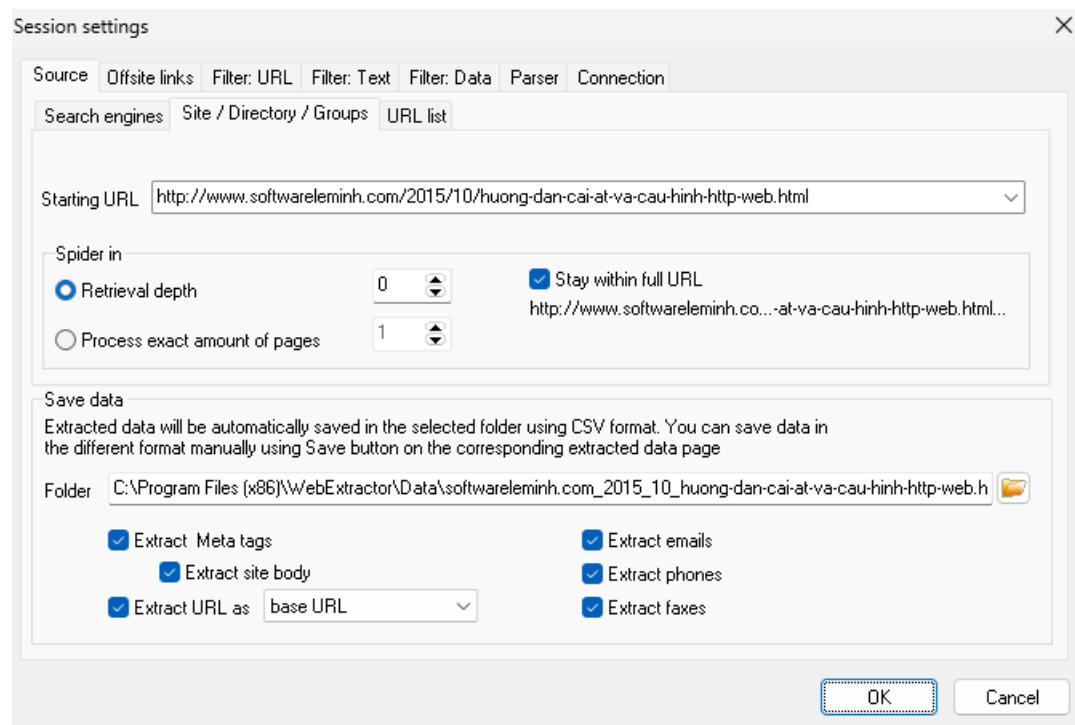
The Web Data Extractor main window appears. Click New to start a new session.

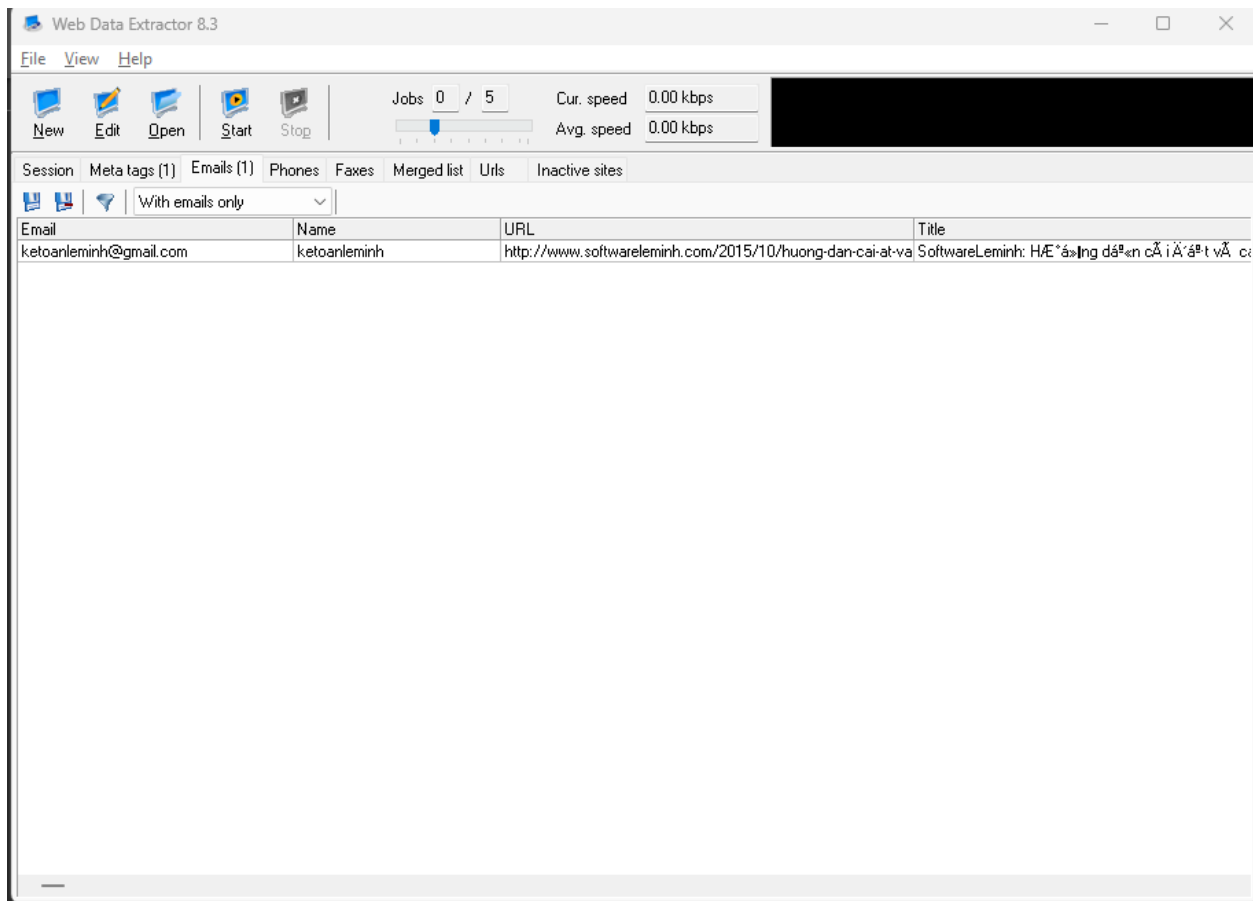


The Session settings window appears; type a URL (here, <http://www.certifiedhacker.com>) in the Starting URL field. Check all the options, as shown in the screenshot, and click OK



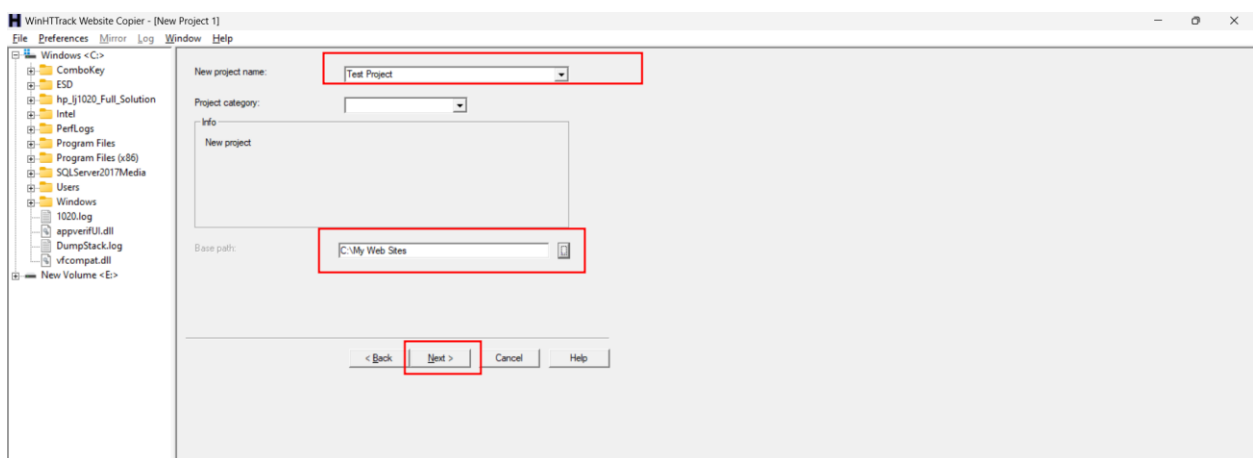
Click Start, but due to the old website, I have to change to another web to another URL



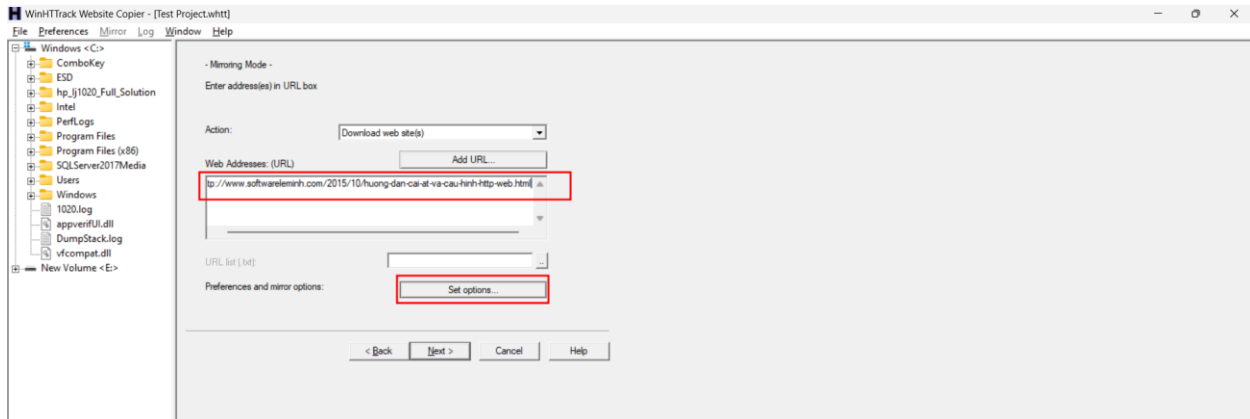


Mirror a Target Website using HTTrack Web Site Copier

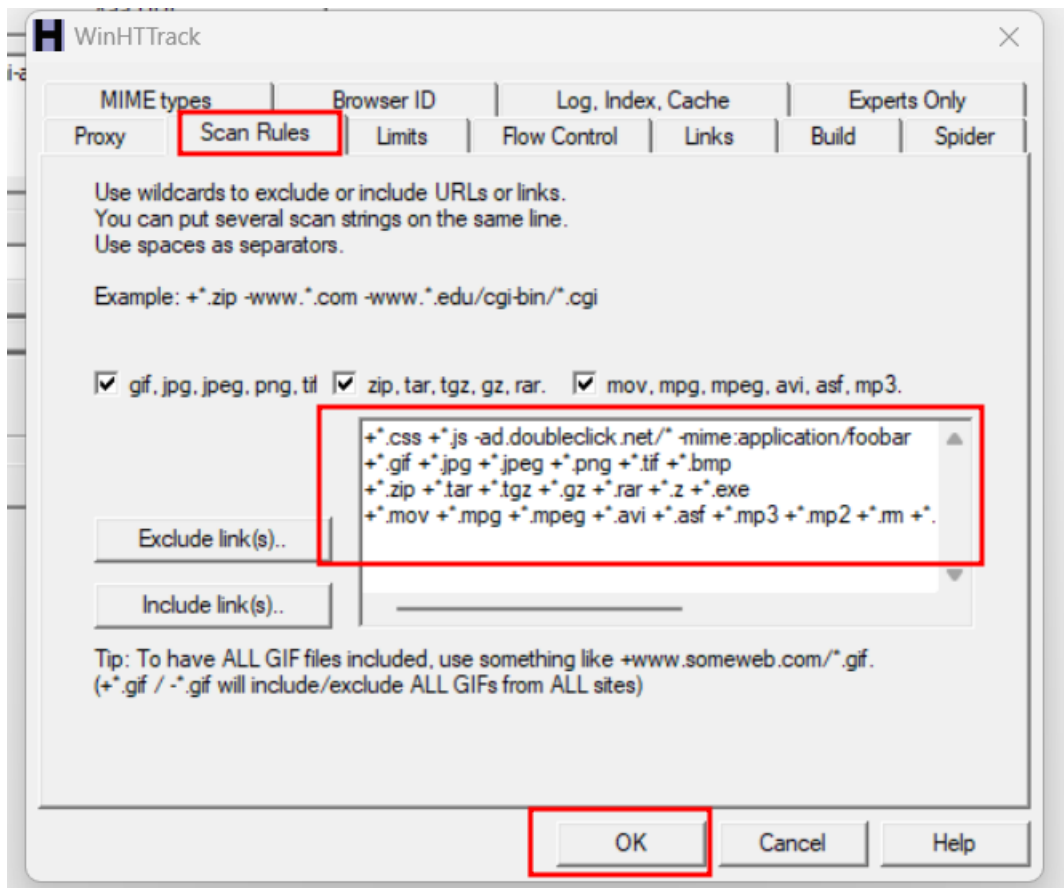
Enter the name of the project (here, Test Project) in the New project name: field. Select the Base path: to store the copied files; click Next >



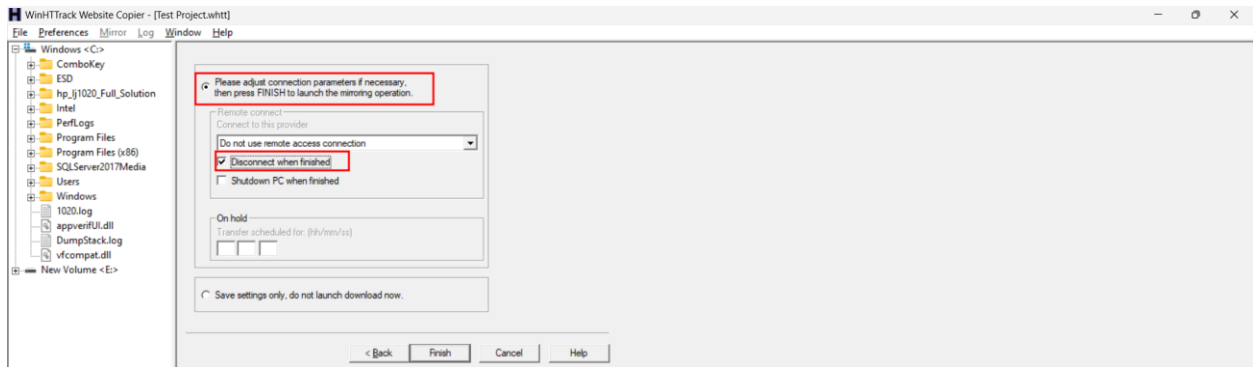
Enter a target URL in the Web Addresses: (URL) field and click Set options...



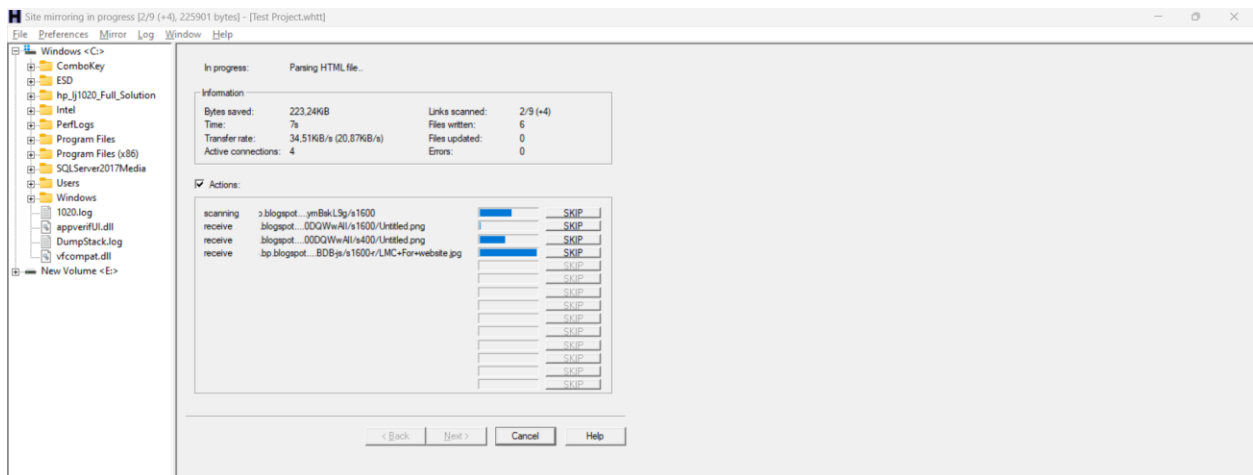
WinHTTrack window appears, click the Scan Rules tab and select the checkboxes for the file types as shown in the following screenshot; click OK.



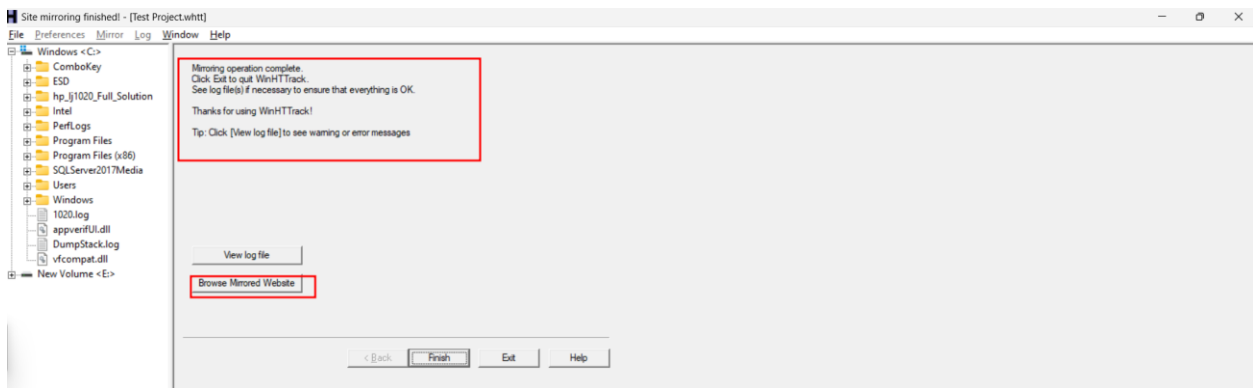
By default, the radio button will be selected for Please adjust connection parameters if necessary, then press FINISH to launch the mirroring operation. Check Disconnect when finished and click Finish to start mirroring the website.



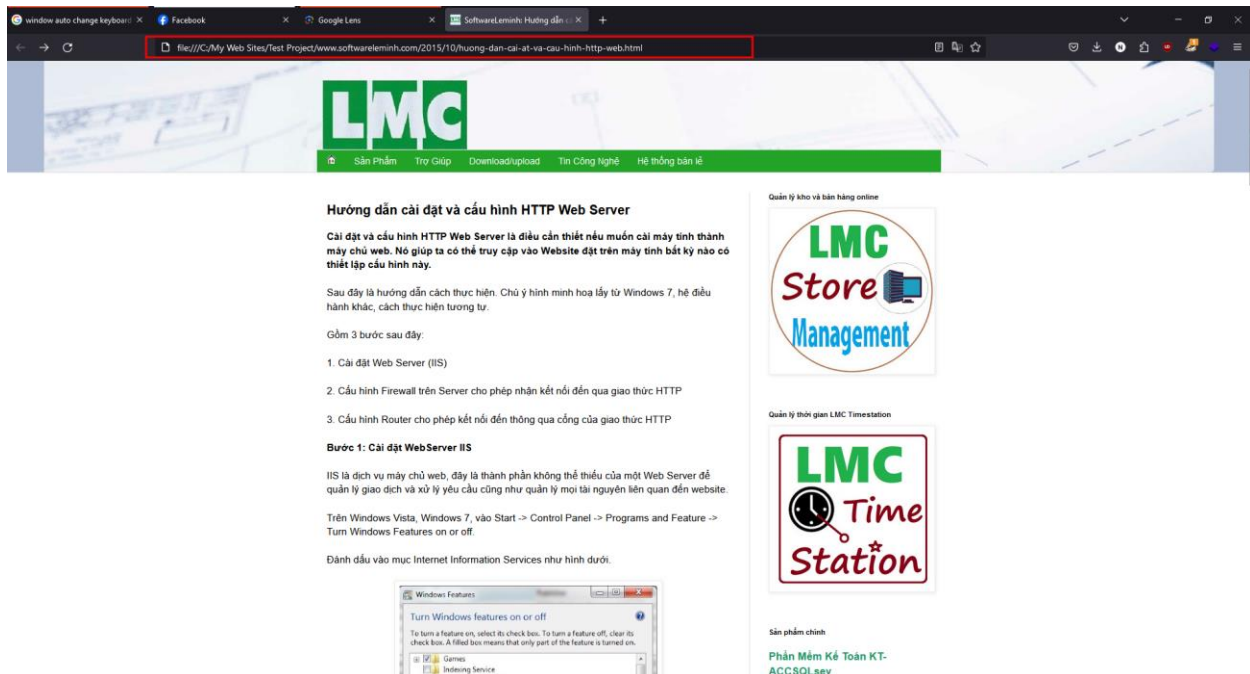
Site monitoring is displayed like below



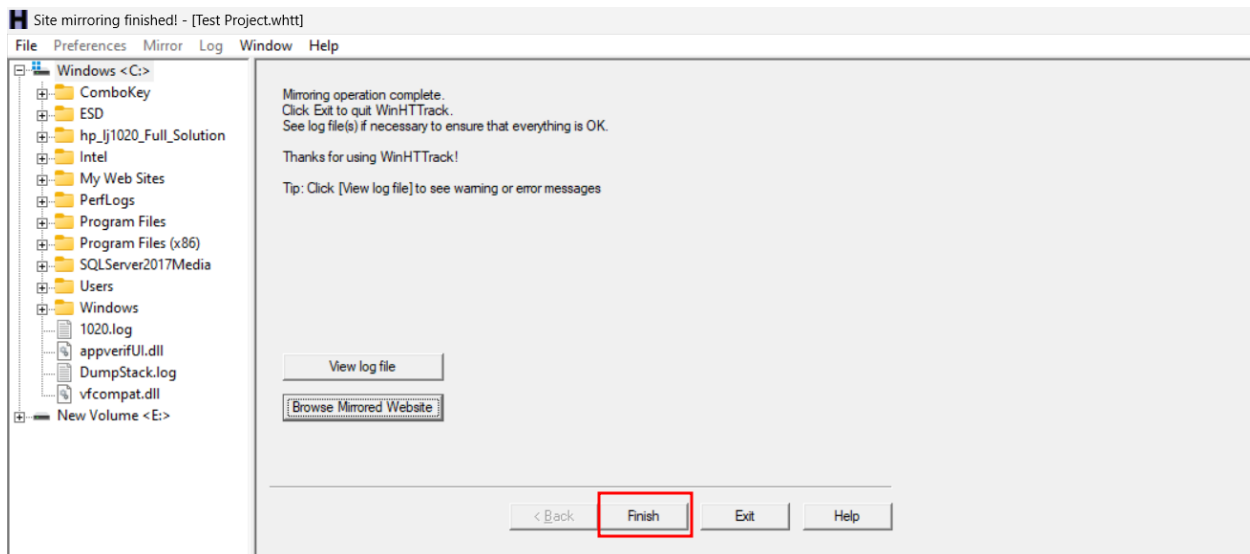
Once the site mirroring is completed, WinHTTrack displays the message Mirroring operation complete; click on Browse Mirrored Website

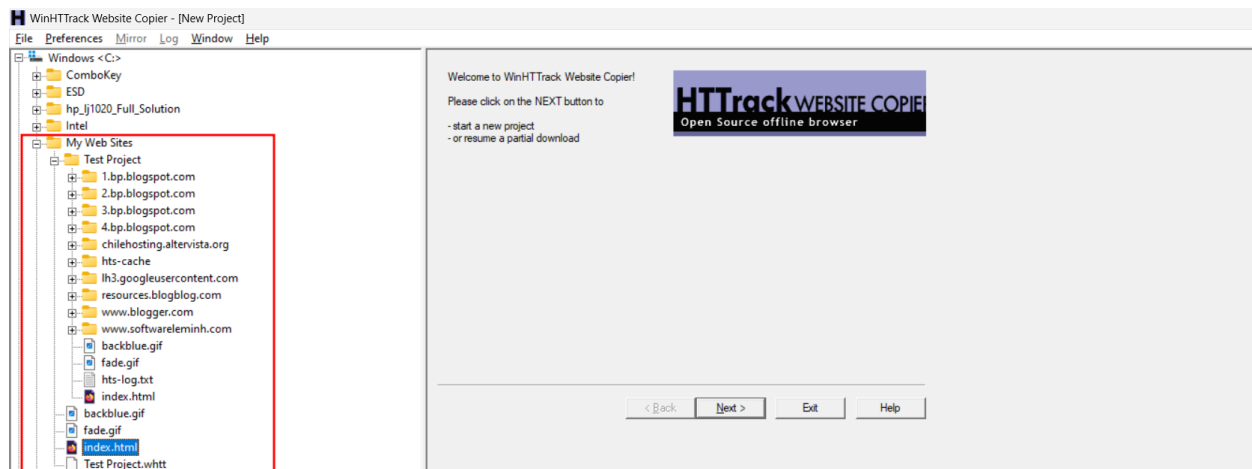


The website will be cloned like below:



Once done with your analysis, close the Firefox window and click Finish on the WinHTTrack window to complete the process

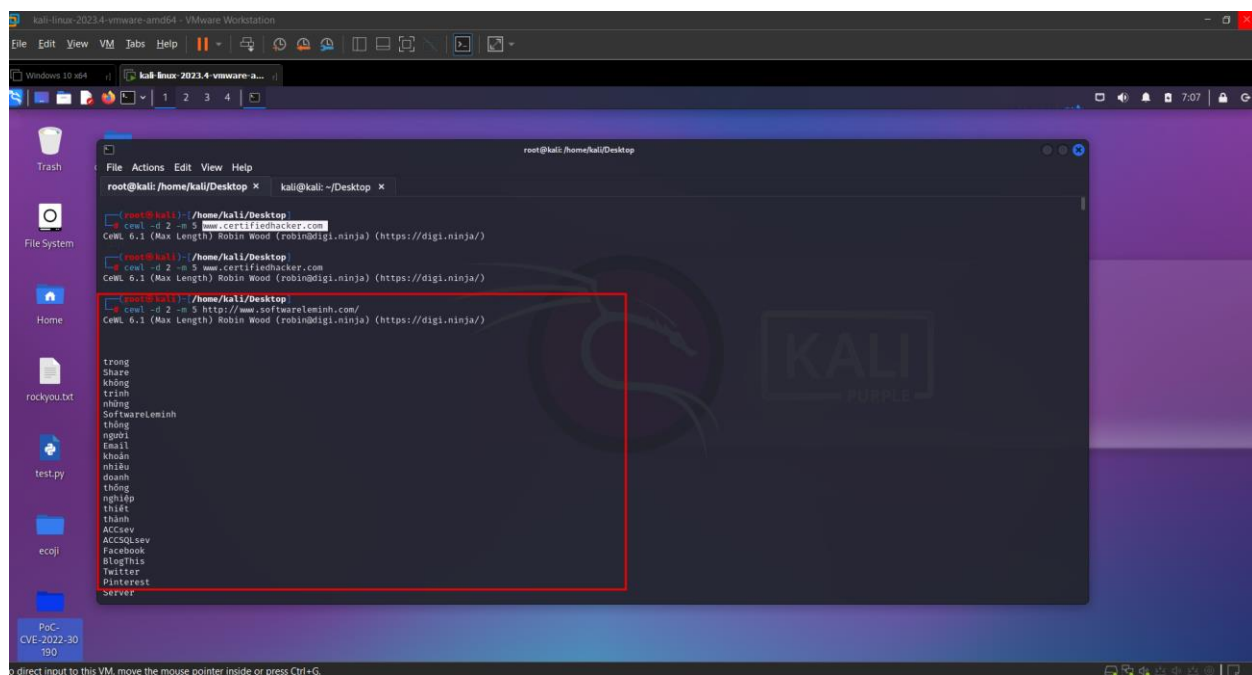




Gather a Wordlist from the Target Website using CeWL

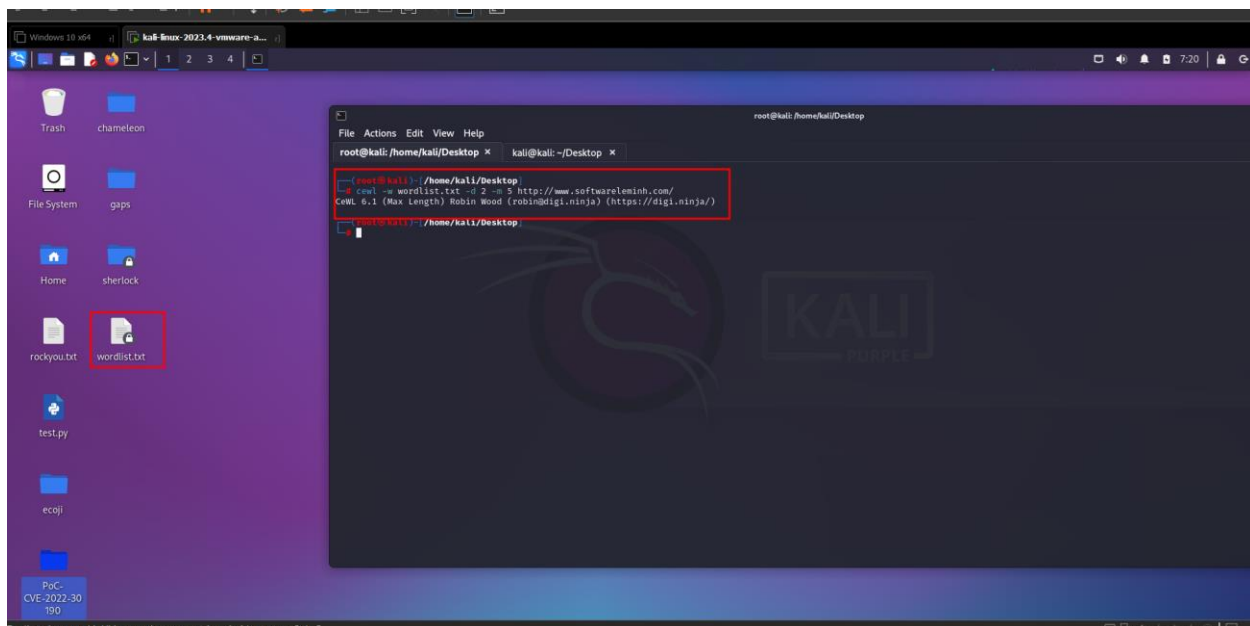
In the Kali Terminal window, type `cewl -d 2 -m 5 www.certifiedhacker.com` in this case the web don't work so I use my web instead and press Enter.

Note: -d represents the depth to spider the website (here, 2) and -m represents minimum word length (here, 5).

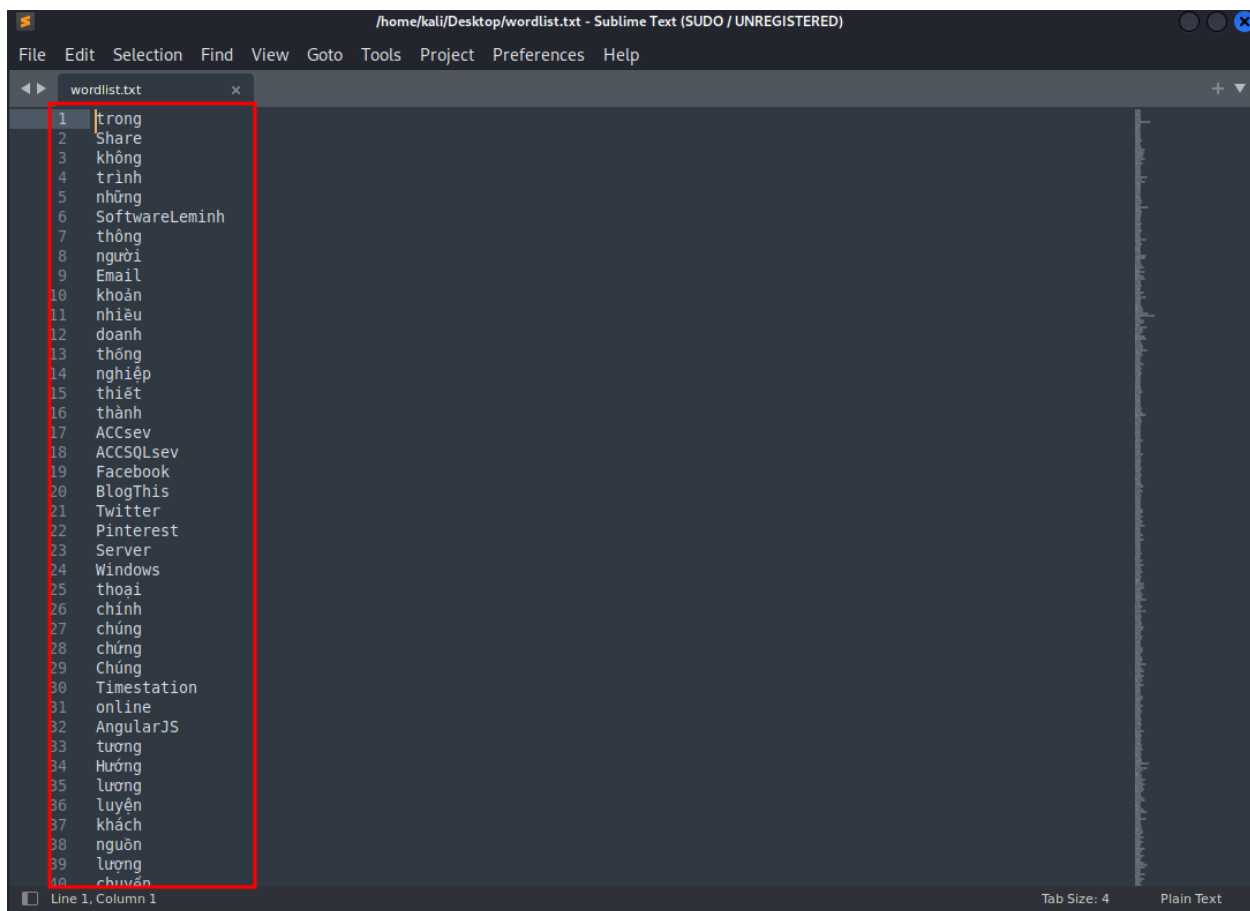


Alternatively, this unique wordlist can be written directly to a text file by typing `cewl -w wordlist.txt -d 2 -m 5 http://www.softwareleminh.com/`

Note:-w - Write the output to the file (here, wordlist.txt)



Watching in sublime text, we can easily see that the result is saved in a file

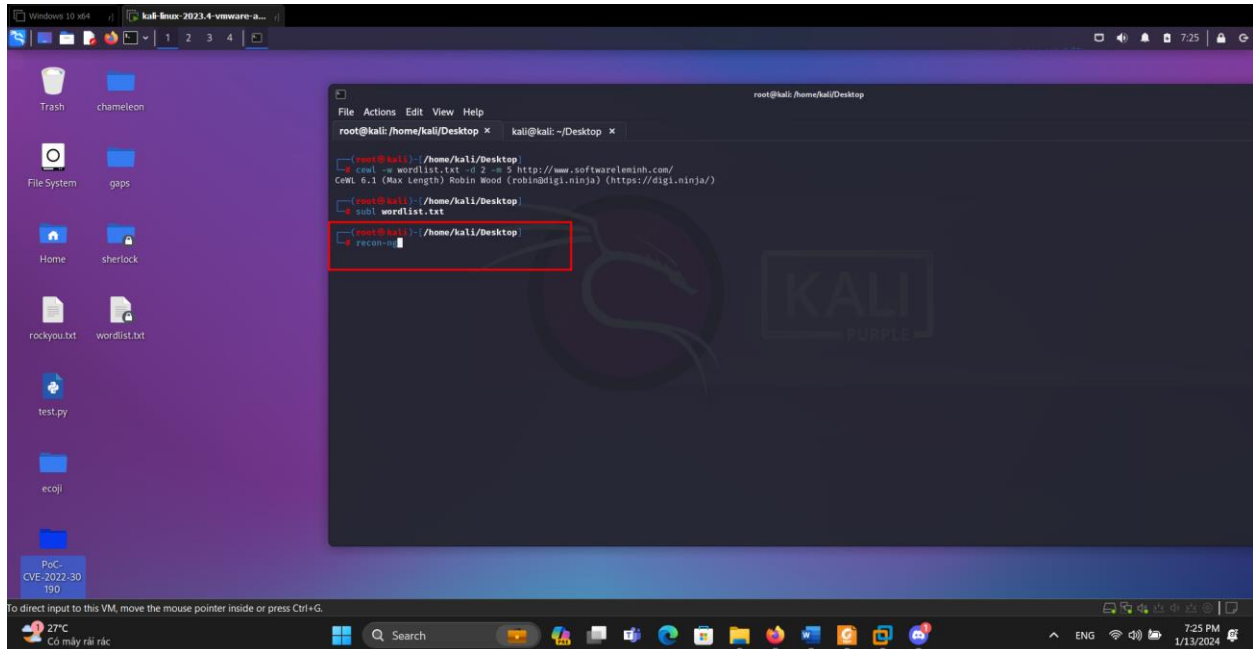


This wordlist can be used further to perform brute-force attacks against the previously obtained emails of the target organization's employees.

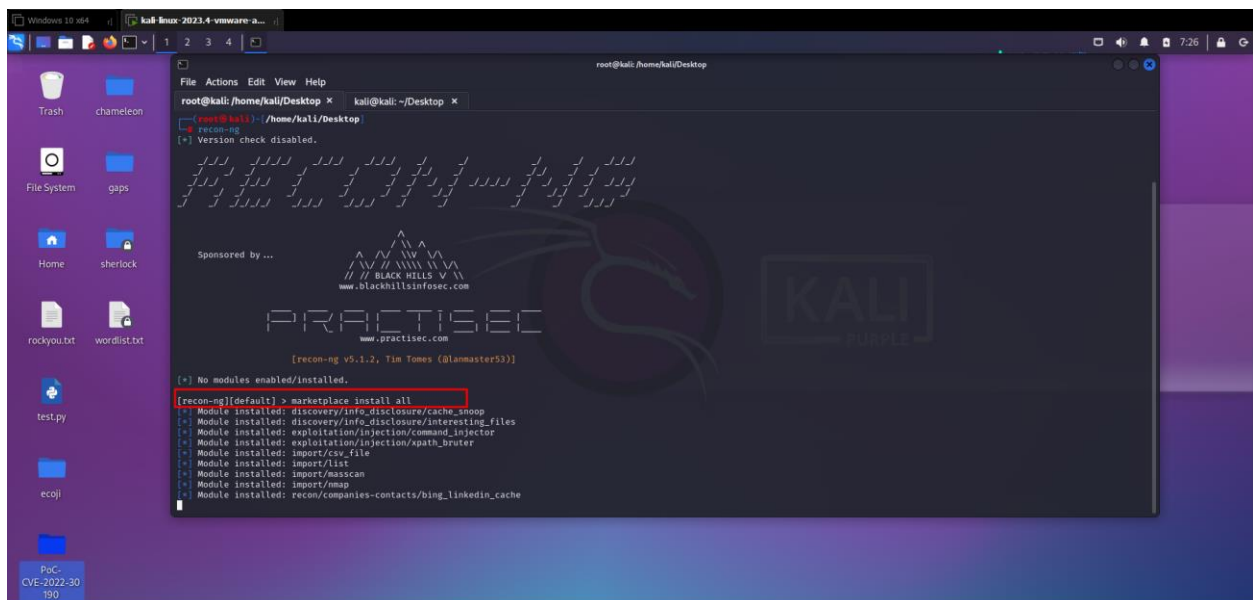
This concludes the demonstration of gathering wordlist from the target website using CeWL.

Lab 9

Type the command `recon-ng` and press Enter to launch the application.

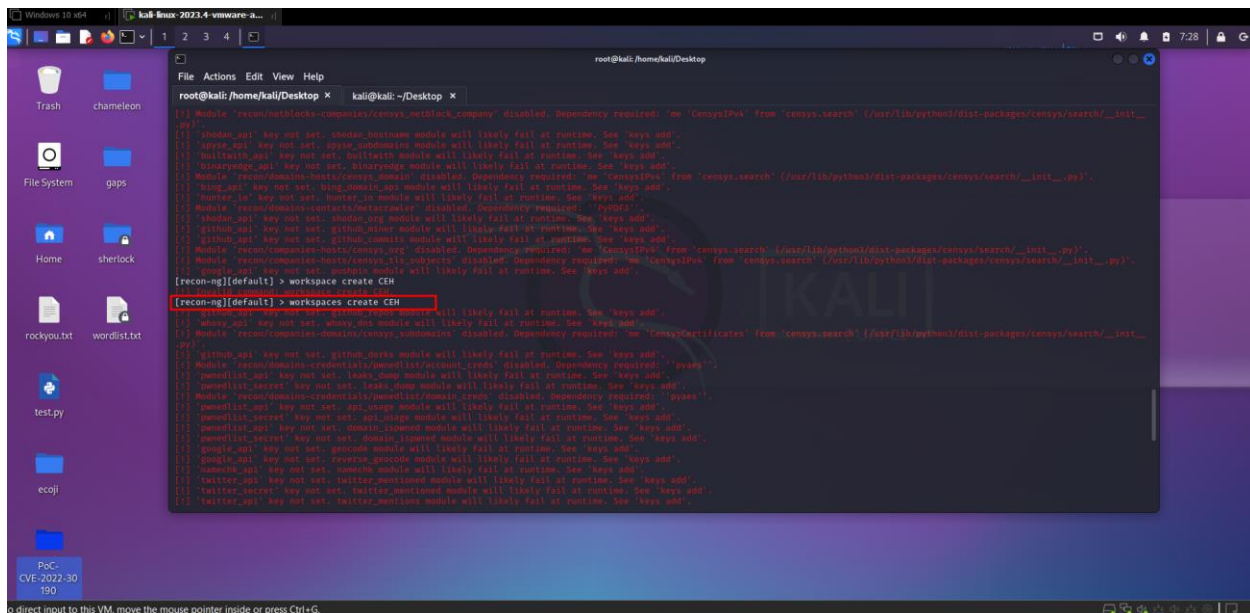


Type **marketplace install all** and press Enter to install all the modules available in recon-ng.



Create a workspace in which to perform network reconnaissance. In this lab, we shall be creating a workspace named CEH.

To create the workspace, type the command `workspaces create CEH` and press Enter. This creates a workspace named CEH.



Enter “workspaces list” to see all the workspaces

```
[!] Invalid command: clear.
[recon-ng][CEH] > workspaces list

+-----+-----+
| Workspaces | Modified |
+-----+-----+
| CEH        | 2024-01-13 07:28:20 |
| default    | 2024-01-13 07:25:58 |
+-----+-----+

[recon-ng][CEH] > 
```

Add a domain in which you want to perform network reconnaissance

Type the command db insert domains and press Enter.

In the domain (TEXT) option, type certifiedhacker.com and press Enter.

In the notes (TEXT) option, press Enter. This adds certifiedhacker.com to the present workspace.

You can view the added domain by issuing the show domains command, as shown in the screenshot.

```
[recon-ng][CEH] > workspaces list
```

Workspaces	Modified
CEH	2024-01-13 07:28:20
default	2024-01-13 07:25:58

```
[recon-ng][CEH] > db insert domain
[*] Invalid table name.
[recon-ng][CEH] > db insert domains
domain (TEXT): http://www.softwareleminh.com/
notes (TEXT):
[*] 1 rows affected.
[recon-ng][CEH] > show domains
```

rowid	domain	notes	module
1	http://www.softwareleminh.com/		user_defined

```
[*] 1 rows returned
[recon-ng][CEH] > █
```

Harvest the hosts-related information associated by loading network reconnaissance modules such as `brute_hosts`, `Netcraft`, and `Bing`.

Type `modules load brute` and press Enter to view all the modules related to brute forcing. In this lab, we will be using the `recon/domains-hosts/brute_hosts` module to harvest hosts.

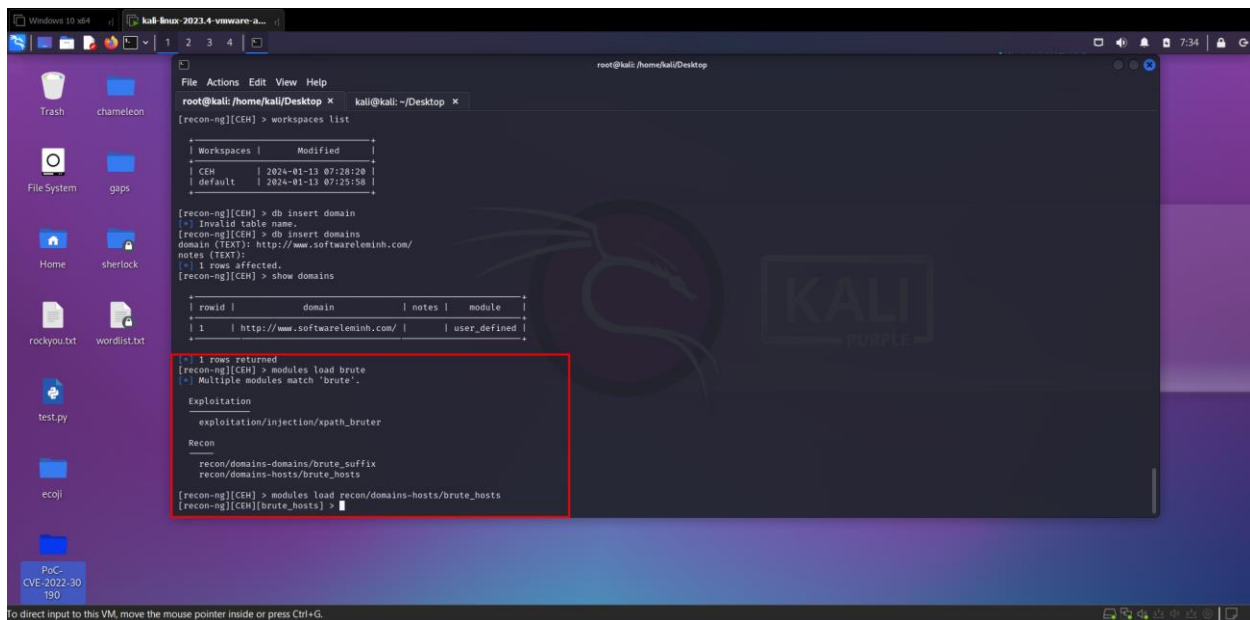
```
[*] 1 rows returned
[recon-ng][CEH] > modules load brute
[*] Multiple modules match 'brute'.
```

Exploitation
exploitation/injection/xpath_bruter

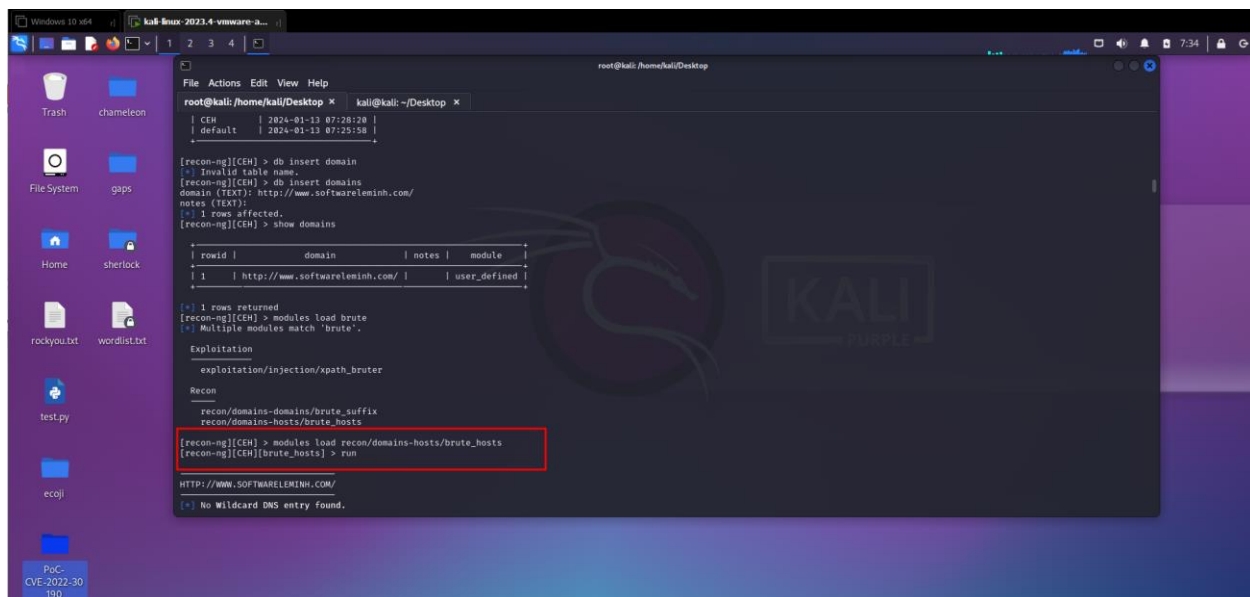
Recon
recon/domains-domains/brute_suffix
recon/domains-hosts/brute_hosts

```
[recon-ng][CEH] > █
```

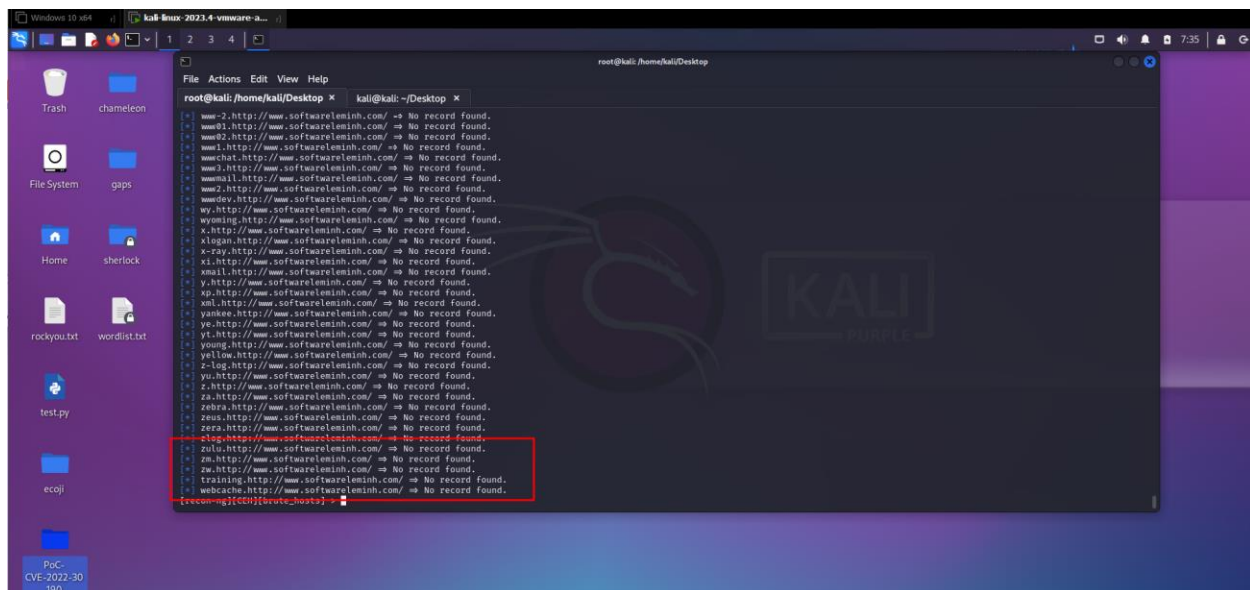
To load the `recon/domains-hosts/brute_hosts` module, type the `modules load recon/domains-hosts/brute_hosts` command and press Enter.



Type run and press Enter. This begins to harvest the hosts, as shown in the screenshot.



Observe that hosts have been added by running the recon/domains- hosts/brute_hosts module.



You have now harvested the hosts related to `certifiedhacker.com` using the `brute hosts` module. You can use other modules such as `Netcraft` and `Bing` to harvest more hosts.

Note: Use the back command to go back to the CEH attributes terminal

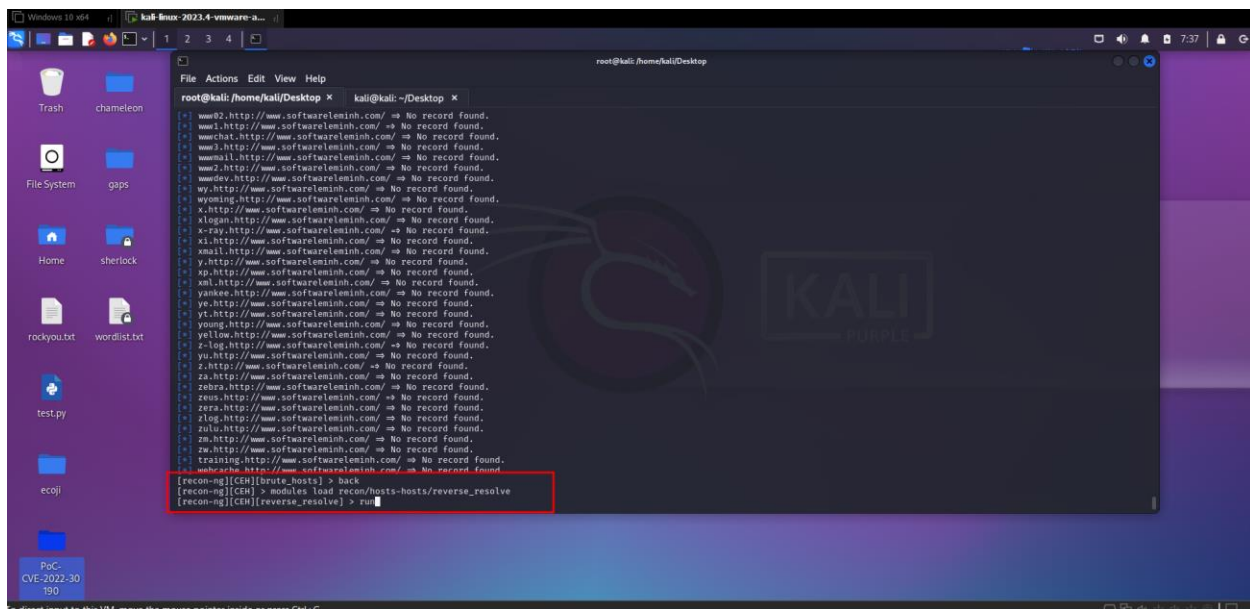
To resolve hosts using the Bing module, use the following commands:

- back
- modules load recon/domains-hosts/bing_domain_web
- . run

26. Now, perform a reverse lookup for each IP address (the IP address that is obtained during the reconnaissance process) to resolve to respective hostnames.

27. Type `modules load reverse_resolve` command and press Enter to view all the modules associated with the `reverse_resolve` keyword. In this lab, we will be using the `recon/hosts-hosts/reverse_resolve` module.

28. Type the modules `load recon/hosts-hosts/reverse_resolve` command and press Enter to load the module.



Type the modules load reporting/html command and press Enter.

Observe that you need to assign values for CREATOR and CUSTOMER options while the FILENAME value is already set, and you may change the value if required.

Type:

a. options set FILENAME /root/Desktop/results.html and press Enter. By issuing this command, you are setting the report name as results.html and the path to store the file as Desktop.

b. options set CREATOR [your name] (here, Jason) and press Enter.

C. options set CUSTOMER Certifiedhacker Networks (since you have performed network reconnaissance domain) and press Enter.

