RECON-ng

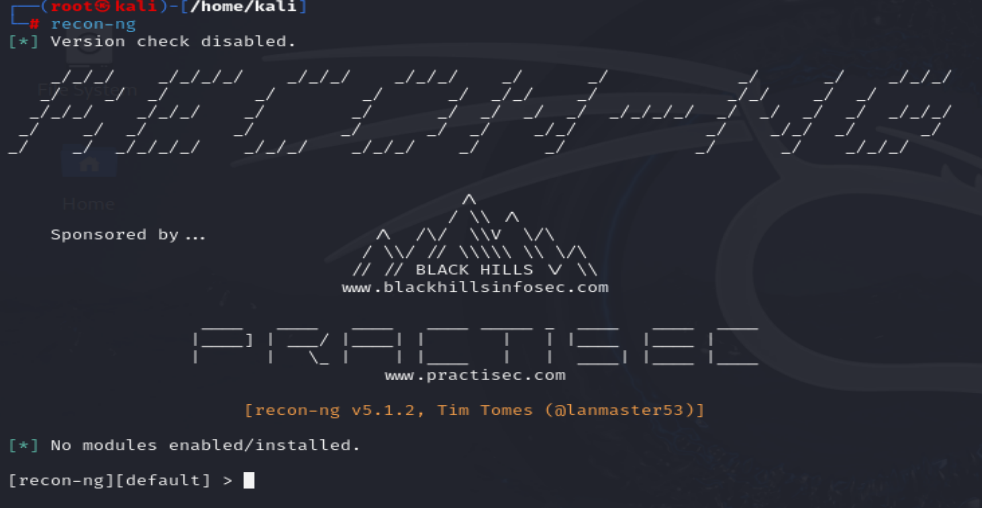
Recon-ng is a full-featured Web Reconnaissance framework written in Python. Complete with independent modules, database interaction, built-in convenience functions, interactive help, and command completion, Recon-ng provides a powerful environment in which open-source web-based reconnaissance can be conducted quickly and thoroughly.

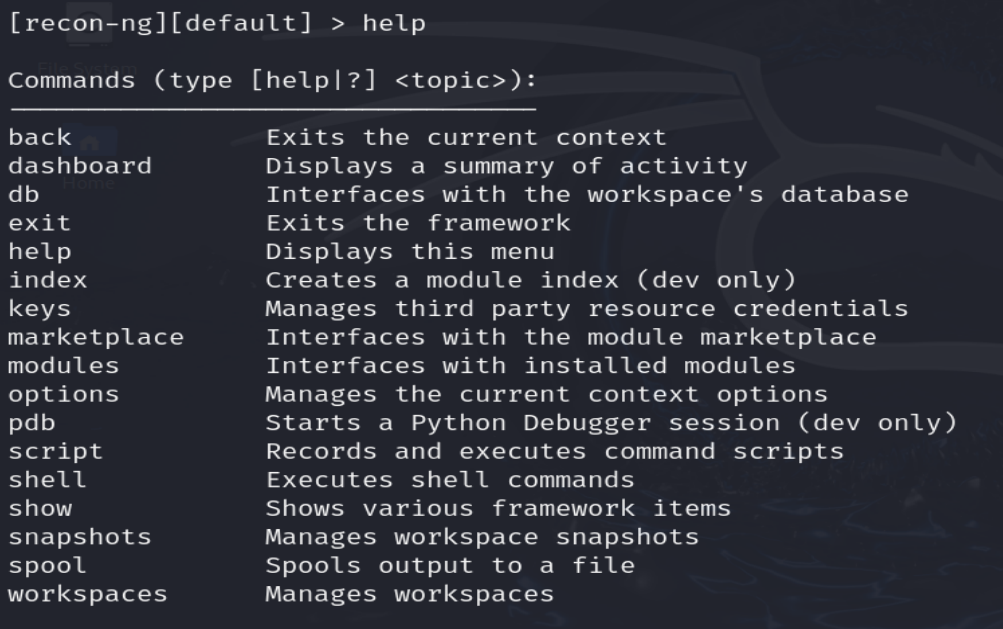
Recon-ng has a look and feel similar to the Metasploit Framework, reducing the learning curve for leveraging the framework.

However, it is quite different. Recon-ng is not intended to compete with existing frameworks, as it is designed exclusively for web-based open-source reconnaissance. If you want to exploit, use the Metasploit Framework. If you want to Social Engineer, use the Social Engineer Toolkit. If you want to conduct reconnaissance, use Recon-ng.

To start Recon-ng in Kali Linux in the terminal type.

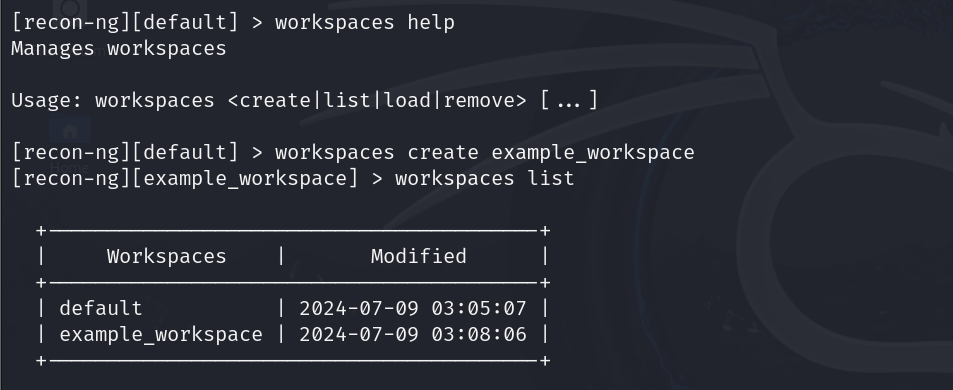
Command: **recon-ng**





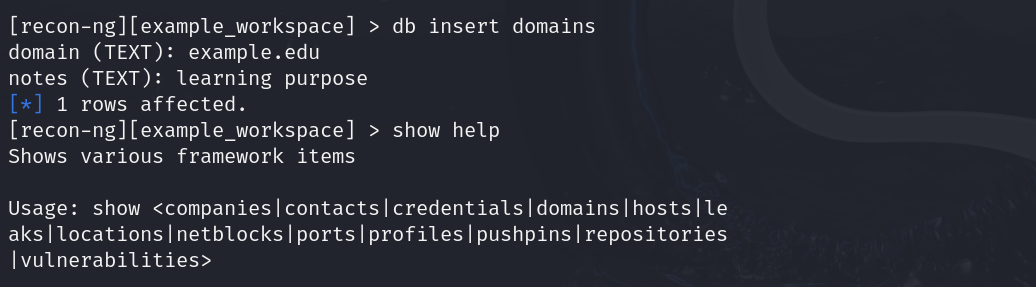
To add workspace type

Command: workspaces create example\_workspace



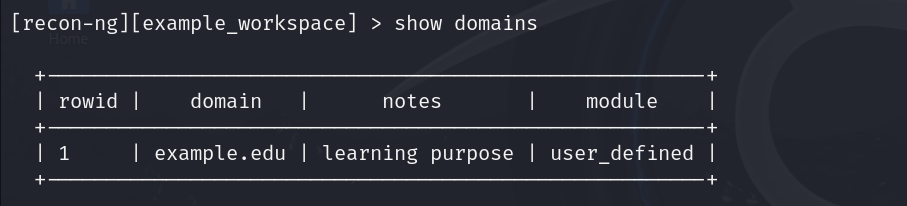
To add domains about which you want to gather information type

Command: db insert domains



To check whether the domain is added successfully type

Command: show domains



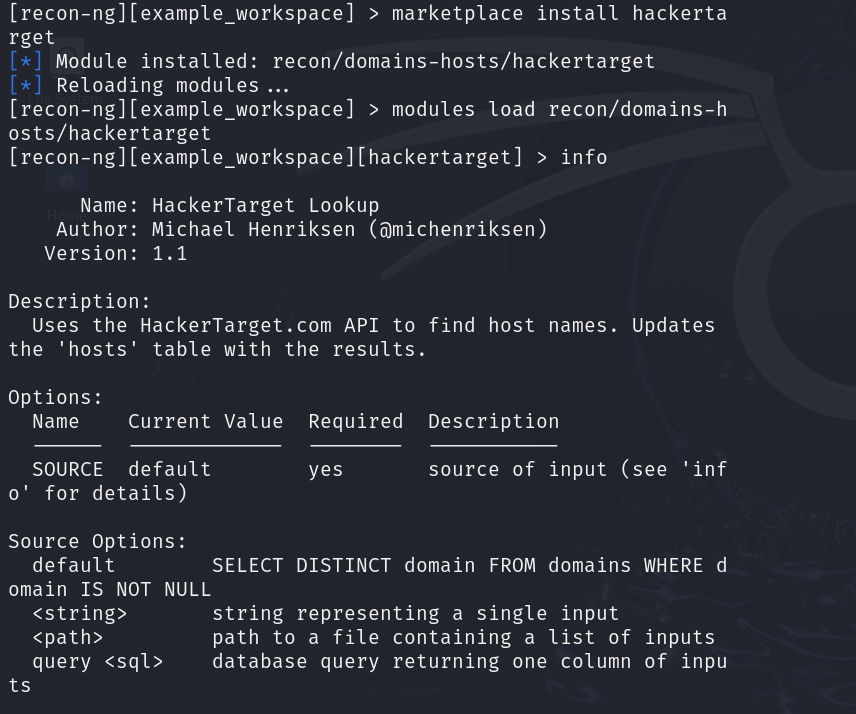
**Using hackertarget to find sub-domains:**

Let's install and load it:

Command: marketplace install hackertarget  
Command: modules load recon/domains-hosts/hackertarget

Type info to view the SOURCE, currently set at default as show below:

Command: info

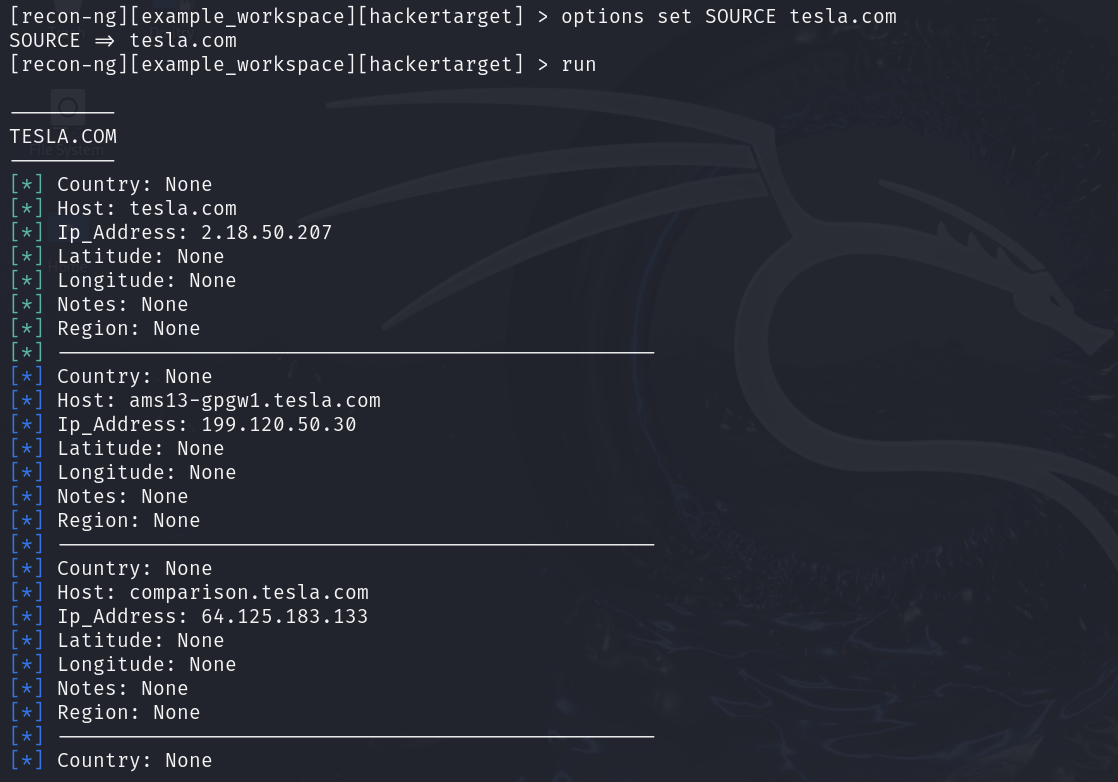


Now set the SOURCE to:

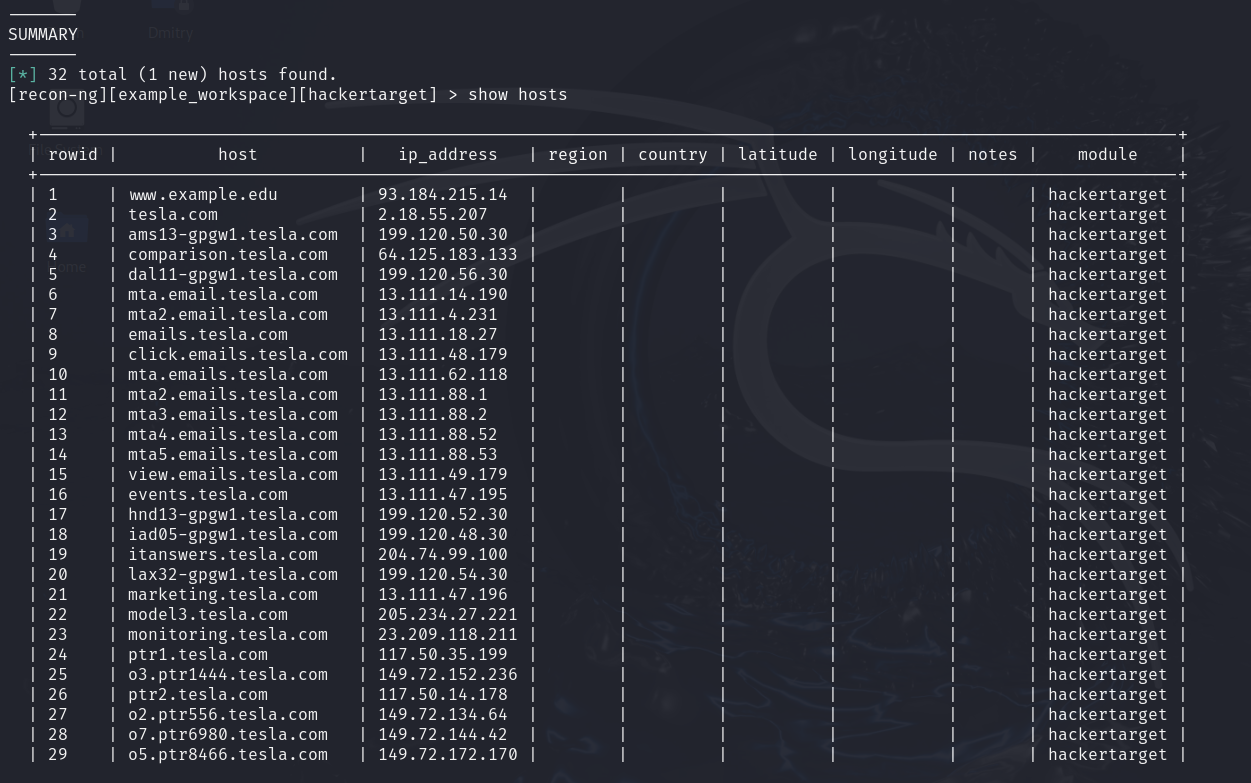
Command: options set SOURCE tesla.com

Run the module:

Command: run



Command:show hosts



**Generate a report**

Now that you have harvested a number of hosts, you will prepare a report containing all the information.

Install the reporting module to report in html format.

Command: marketplace install reporting/html

Load the module:

Command: modules load reporting/html

To configure the reporting information, type info to see the values.

You will need to assign these values, CREATOR, CUSTOMER and FILENAME.

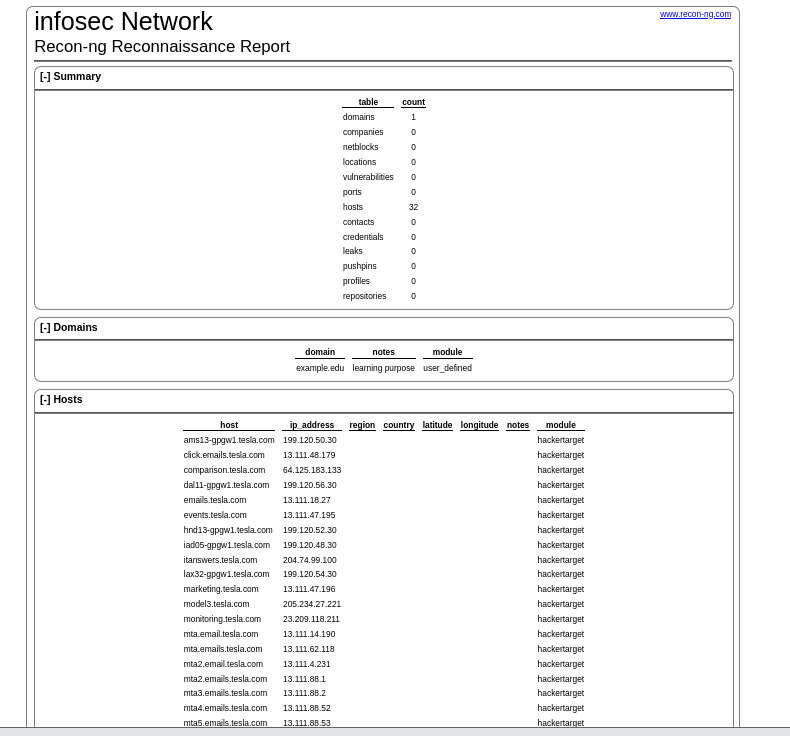
Set your name[CREATOR], customer name[CUSTOMER], path to export and the file name[FILENAME].

Command: options set CREATOR Micky  
Command: options set CUSTOMER infosec Network  
Command: options set FILENAME /home/kali/host.html

Run the module to export:

Command: run

The generated report is saved to to the HOME folder in desktop.



There is not much in this report, but when you start running multiple modules and add in geolocation reports can get very complex. Recon-ng does a great job keeping track of everything.

**Gather contacts associated with a domain**

Set a domain and perform footprinting on it to extract contact available in the domain.

The module selected to perform this technique uses the ARIN Whois RWS to harvest POC data from whois queries for the given domain.

Install and load the module:

Command: marketplace install recon/domains-contacts/whois\_pocs

Command: modules load recon/domains-contacts/whois\_pocs

Check the options required to run the module:

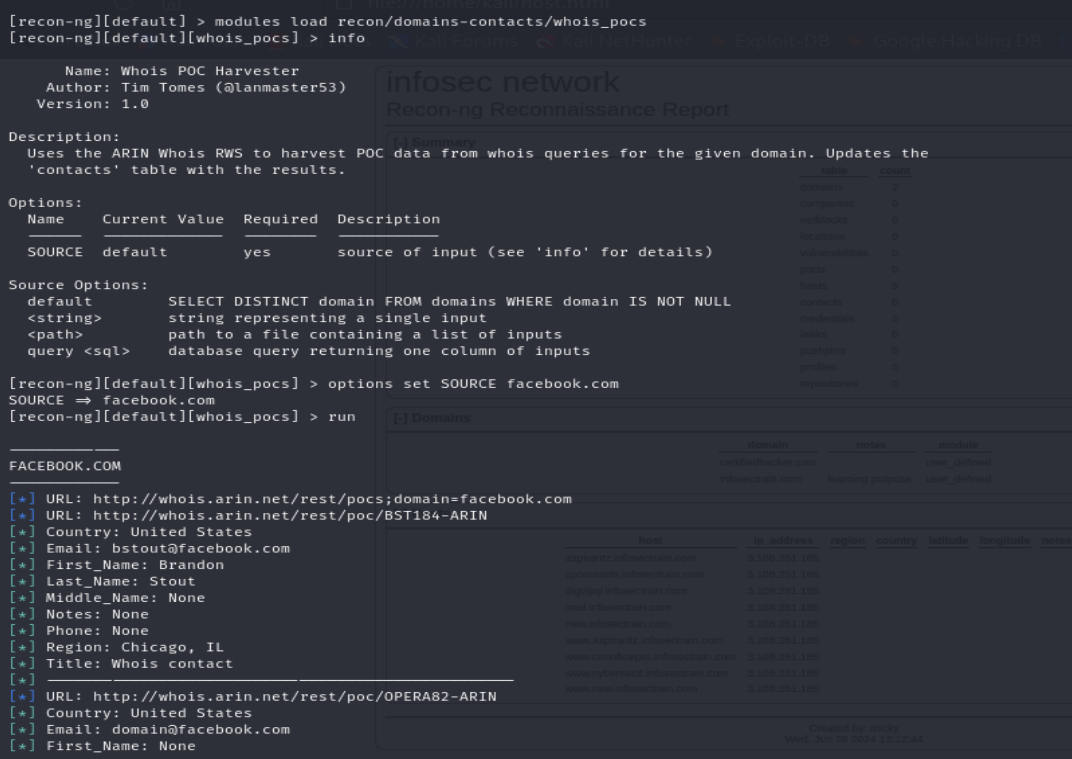
Command: info

Set the SOURCE value to target domain:

Command: options set SOURCE facebook.com

Run the module:

Command: run



**Profile existence:**

We can search the existence of user profiles in various websites using the **recon/profiles-profiles/profiler**.

Install and load the module:

Command: marketplace install recon/profiles-profiles/profiler

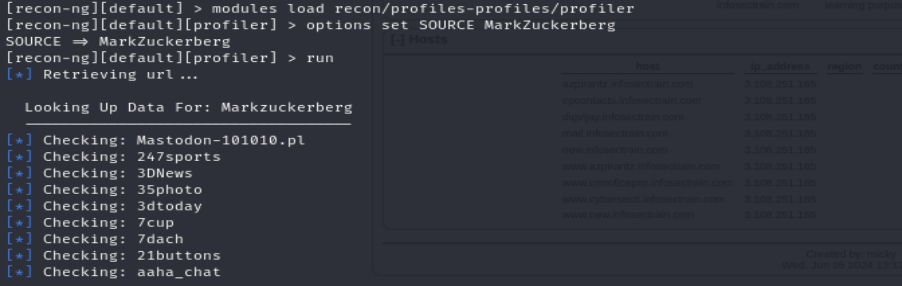
Command: modules load recon/profiles-profiles/profiler

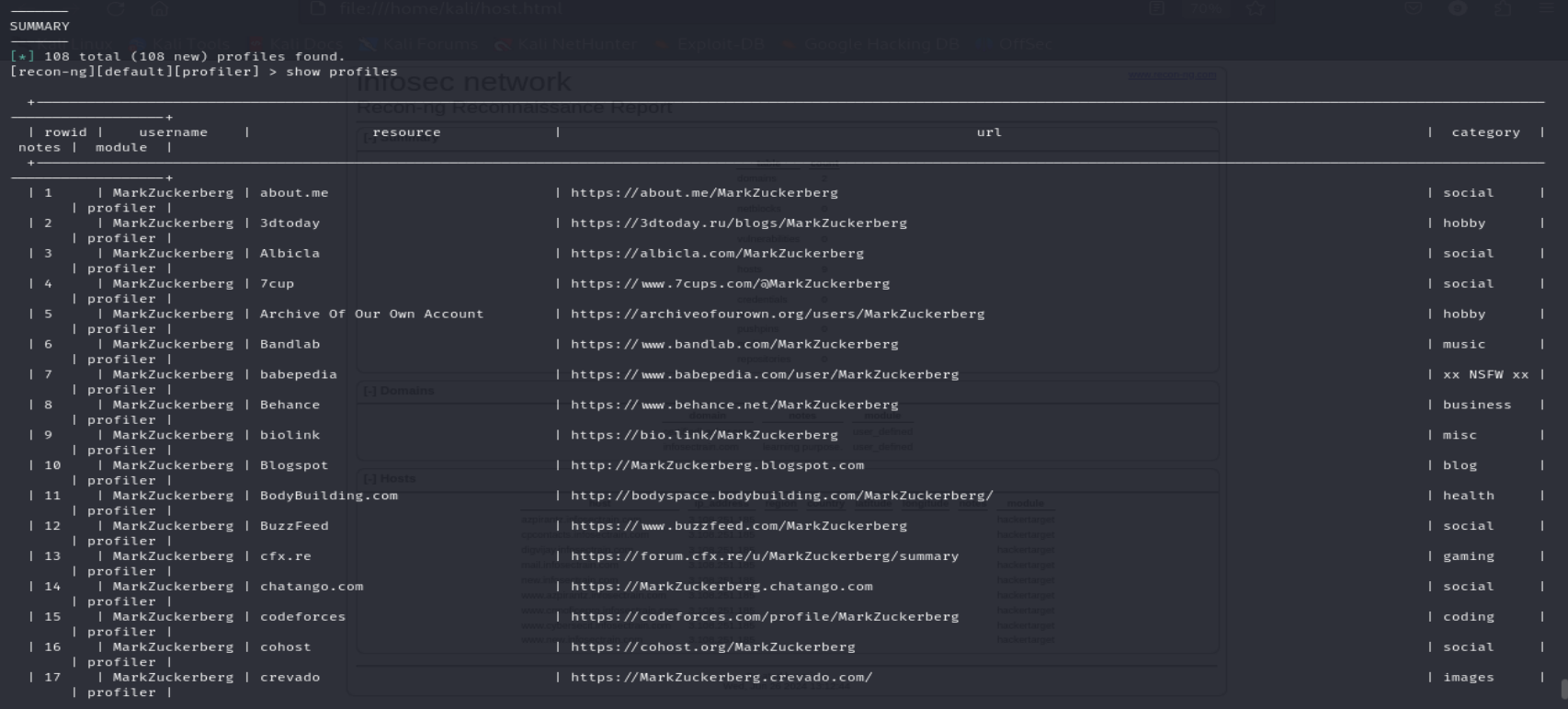
Set the SOURCE value (Target username):

Command: options set SOURCE MarkZuckerberg

Run the module:

Command: run





The recon/profiles-profiles/profiler module searches for this username and returns the URL of the profile in various websites (found with the matching username).