Lab - Using OSINT Tools

Objectives

In this lab, you will explore several OSINT tools that are commonly used by pentesters.

- Examine OSINT resources
- Use SpiderFoot
- Investigate Recon-ng
- Find interesting files with Recon-ng

Background / Scenario

When performing information gathering activities, passive reconnaissance uses open, publicly accessible data to guide active reconnaissance efforts and to gather information about the enterprise and employees. In OSINT, it is the data that is open source. OSINT tools may or may not be open source. Some tools are free and open, others require registration to use free versions, and others require a fee for use. OSINT commonly uses data sources that are available to any hacker, so part of the PenTesting effort is to report on sensitive information that is commonly available in order to evaluate vulnerabilities that it may cause.

The objectives of OSINT are:

- To determine the digital footprint of the organization.
- Determine what data about the organization is available to cyber criminals.

Required Resources

- Kali VM customized for Ethical Hacker course
- Internet access

Instructions

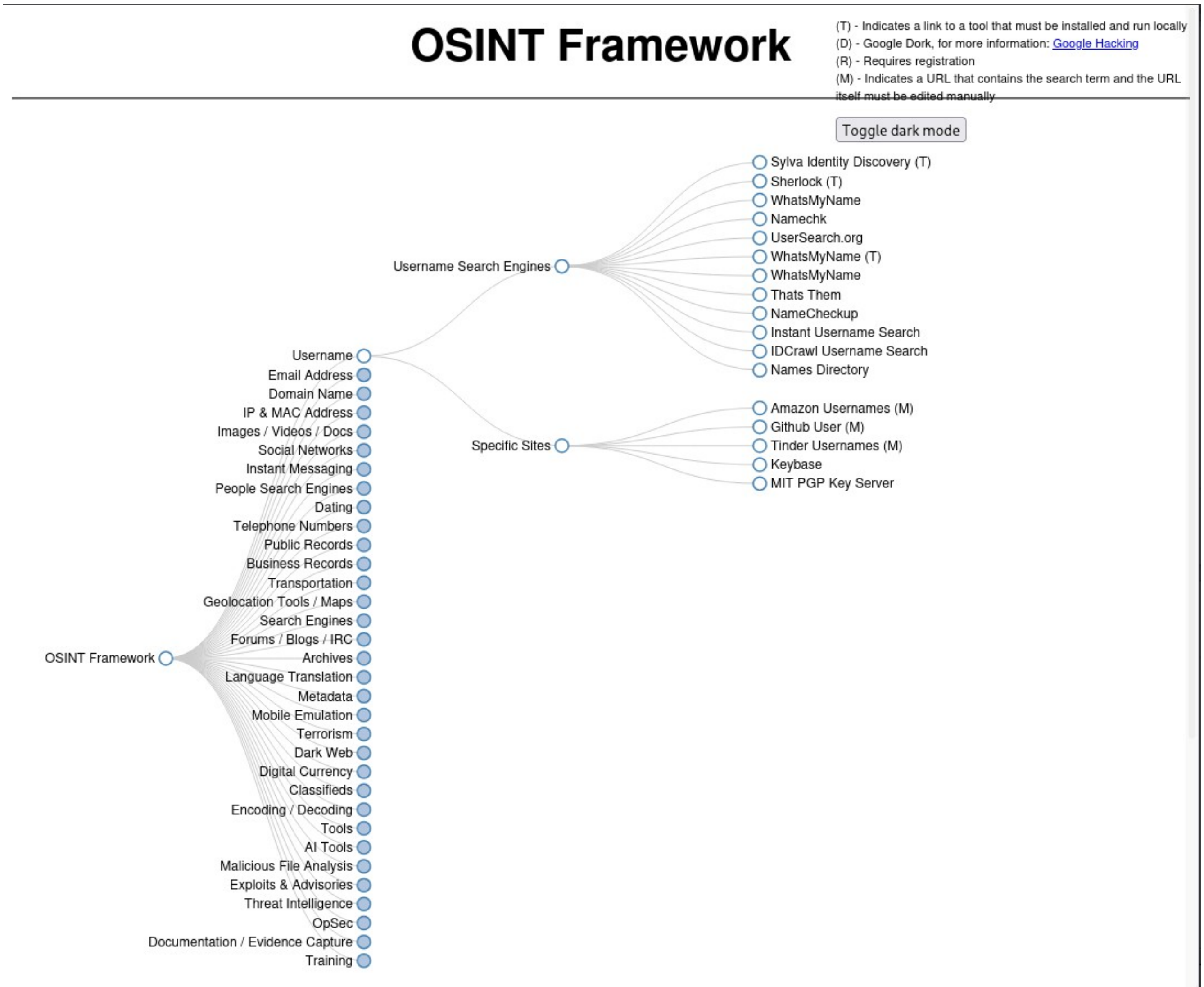
Part 1: Examine OSINT Resources

Step 1: Access the OSINT Framework

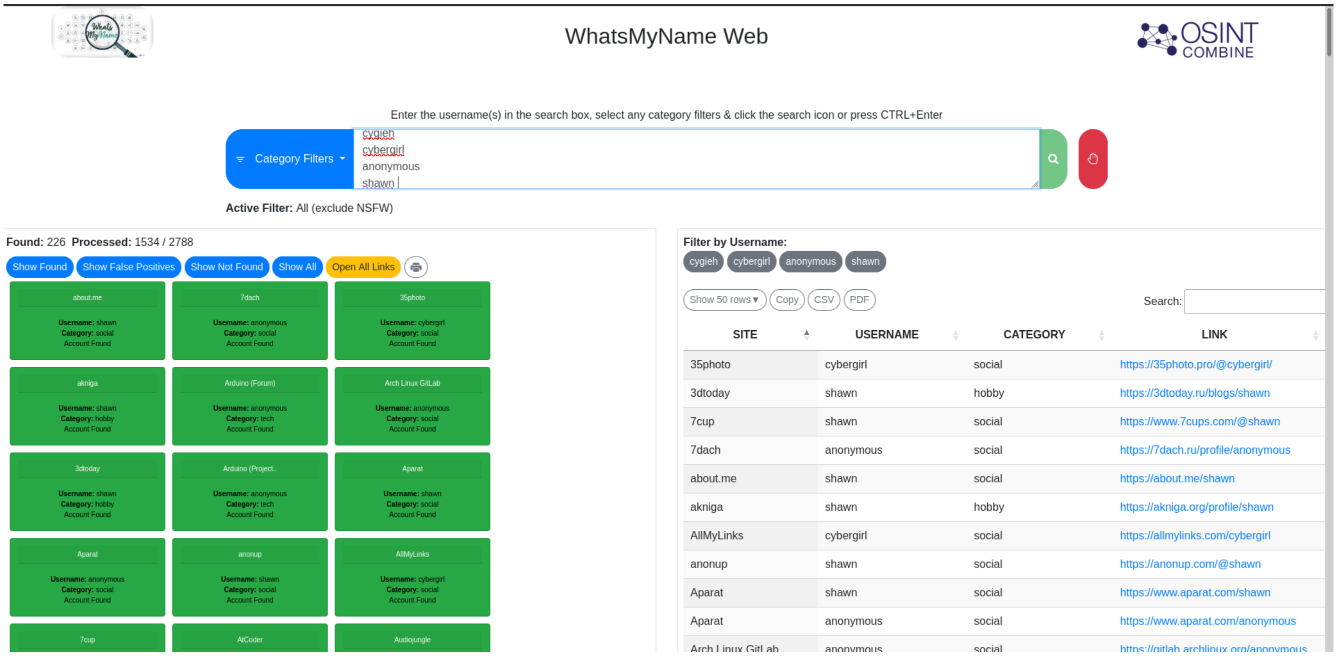
The OSINT Framework is a useful way to visualize the OSINT tools and resources that are available. Unfortunately, it has become a bit outdated, with some resources no longer available. It is still valuable to help you understand the types of tools available and their uses. In many cases, the links are still good.

- Go to the OSINT Framework site at https://osintframework.com/.

- You will see a vertical tree-like structure that consists of categories of OSINT tools and resources that can be reached from the framework. Click **Username** at the top of the tree. You will then see two subcategories appear. Click each to open the resource trees for each subcategory. Note in the upper-right corner of the page is a legend that identifies the type of resource.

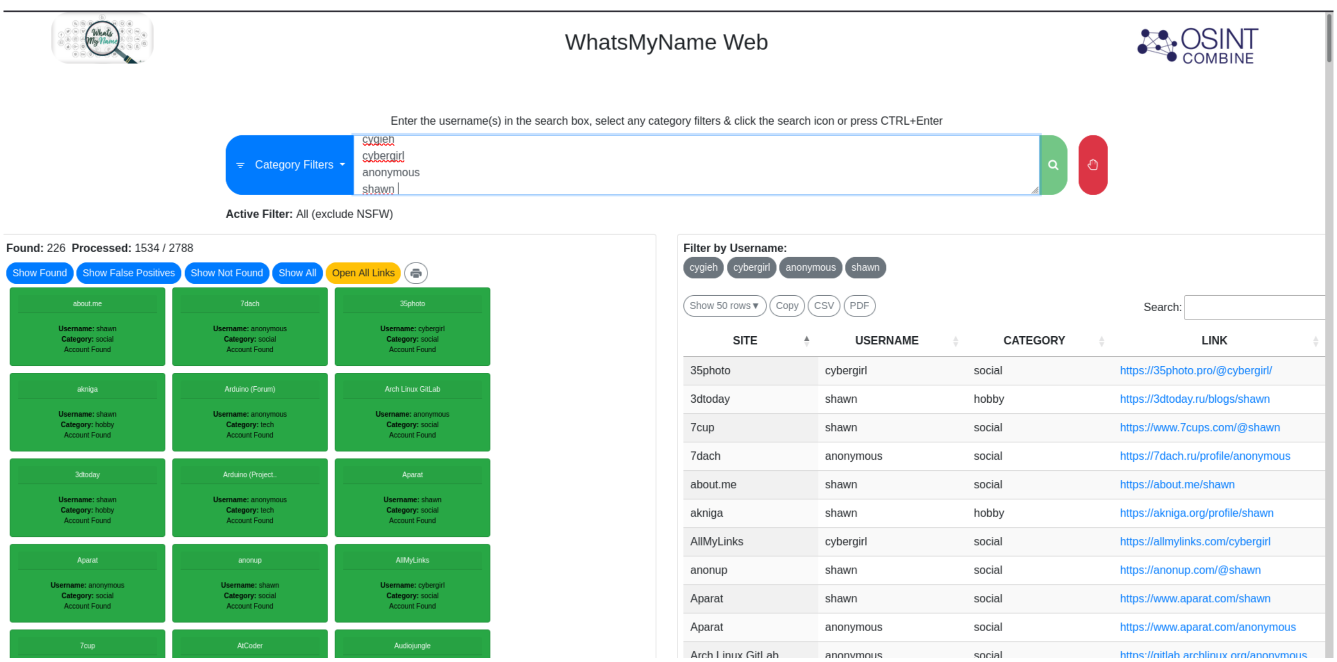


- Under **Username Search Engines**, click **"WhatsMyName(T)"**.
- The link takes you to a Git repository for the WhatsMyName project. In the **README.md** content for the tool, the various sites that implement WhatsMyName are listed. Feel free to explore these, but we will click the first link https://whatsmyname.app/ to visit a free website that implements WhatsMyName. The parent organization for the site, https://www.osintcombine.com/, has several interesting free tools available.
- In the search box, type in a few usernames, each on a separate line. Use your own usernames or others that you find. Try searching the internet for **common username wordlist** for other potential search terms. You can filter the results based on the category filters, but for now, just click the green magnifying glass button to start the search.

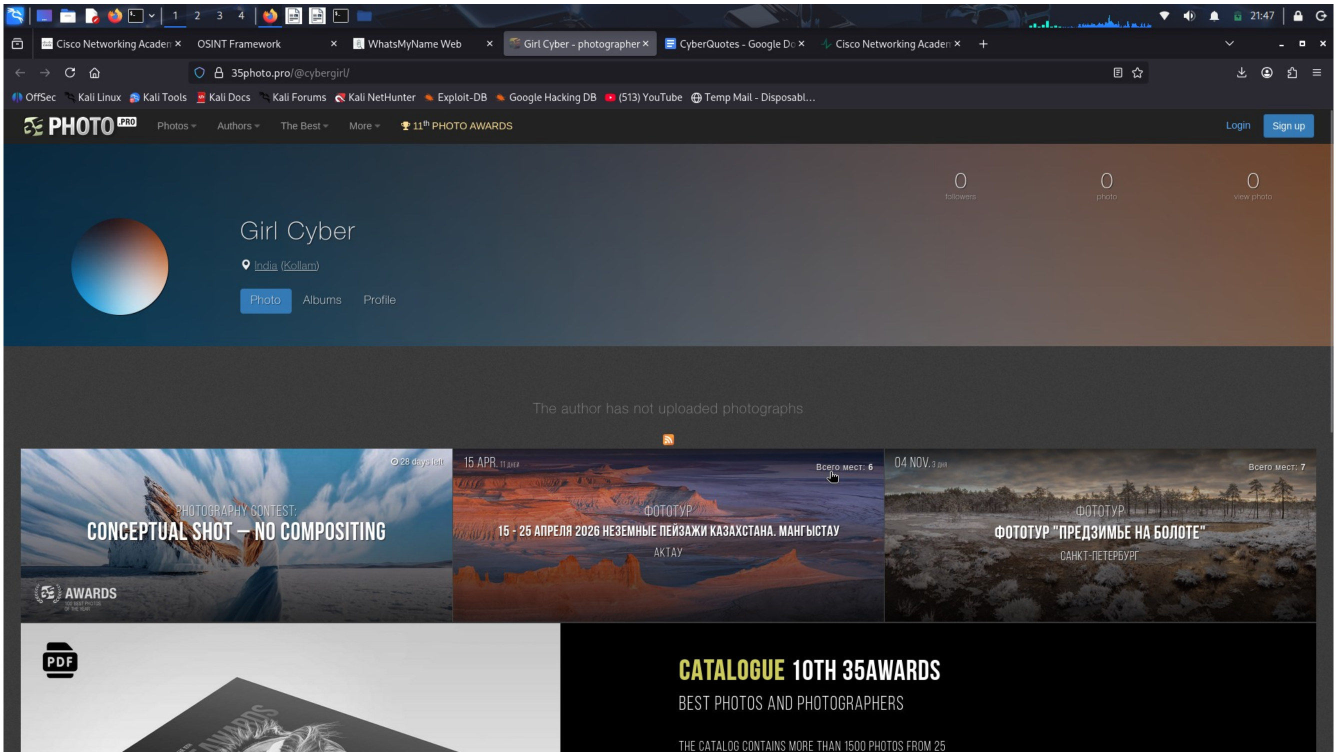


In a pentest, you would use another tool, such as **SpiderFoot** (below) to find usernames in email addresses that are associated with a company or domain.

- Investigate the results. You can open the links to the accounts either from the green rectangles or the table of results.



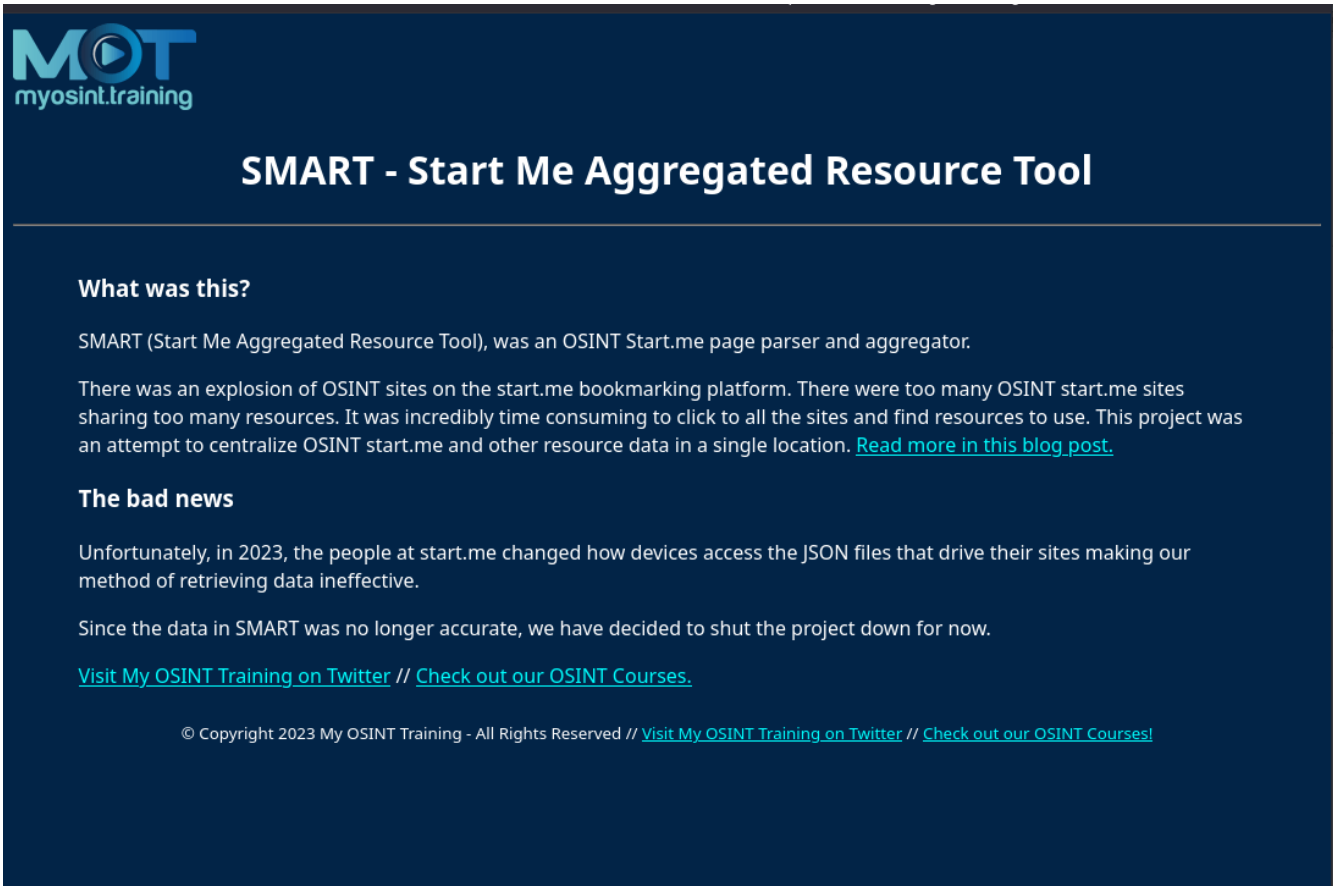
- WhatsMyName provides a very flexible report of the results. The results table can be sorted by column, and you can export the results as CSV or PDF for reporting purposes. In addition, you can easily filter by username and search within the results. Finally, you get links for the profile pages for the users at many different sites.



Step 2: Investigate SMART - Start Me Aggregated Resource Tool.

The start.me web service is a popular bookmark manager and productivity tool. The people at My OSINT Training (MOT) have set up a search system that finds all OSINT-related links that people have bookmarked and shared on start.me. There are many. You can enter OSINT-relevant search terms to find links to related resources.

a. Go to https://smart.myosint.training/.



Disclaimer!: Sadly we will not proceed with the next strps for SMART because the project is shutdown!

b. In the search box, enter the term **usernames**. You will see a list of username-related OSINT tools that other people have found.
c. Open some of the links to review the resources. Be careful however, these websites come from public sources. Some may be malicious.
d. Choose some of the categories that you saw in the OSINT Framework and see what links appear.
e. Use this site to search for OSINT tools and resources to help you in your pentesting work.

Part 2: Use SpiderFoot

SpiderFoot is an automated OSINT scanner. It is included with Kali

SpiderFoot seeds its scan with one of the following:

- Domain names
- IP addresses
- Subnet addresses
- Autonomous System Numbers (ASN)
- Email addresses
- Phone numbers
- Personal names

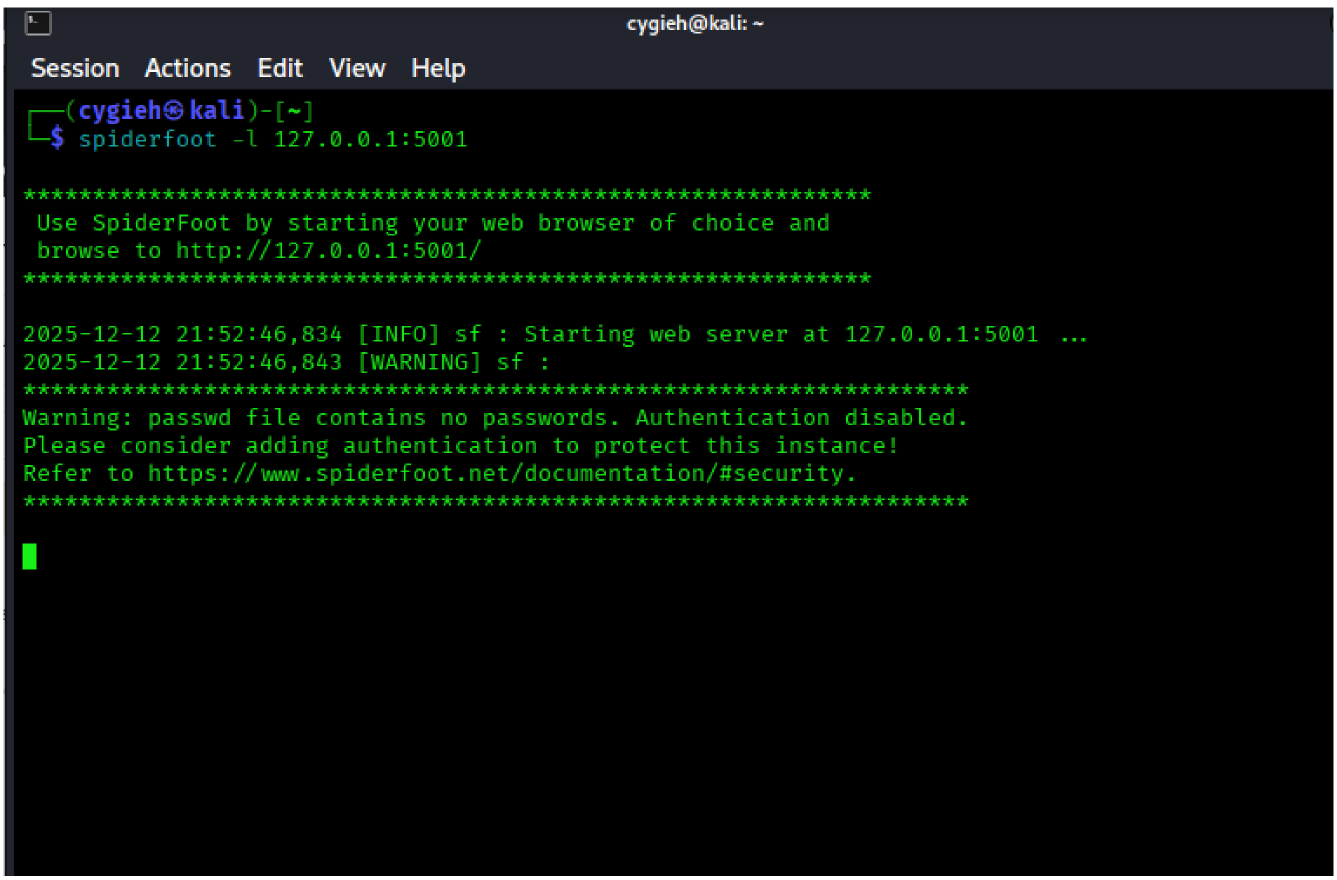
SpiderFoot offers the option of choosing scans based on use case, required data, and by SpiderFoot module.

The use cases are:

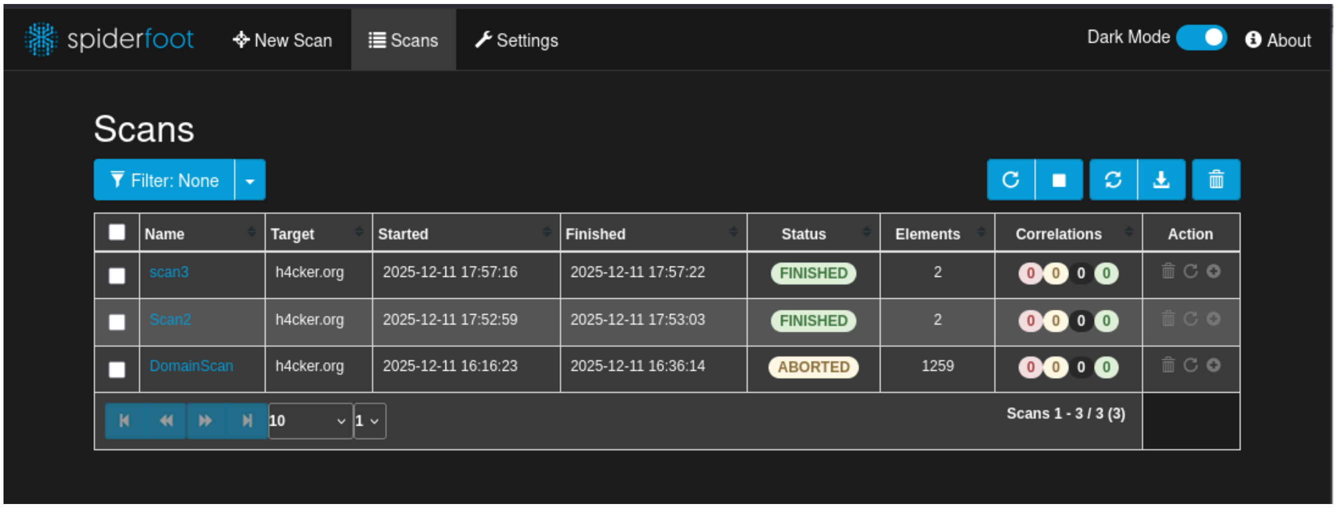
- **All –** Get every possible piece of information about the target. This use case can take a very long time to complete.
- **Footprint –** Understand the target's network perimeter, associated identities and other information that is yielded by extensive web crawling and search engine use.
- **Investigate –** This is or targets that you suspect of malicious behavior. Footprinting, blacklist lookups, and other sources that report on malicious sites will be returned.
- **Passive –** This type of scan is used if it is undesirable for the target to suspect that it is being scanned. This is a form of passive OSINT.

Step 1: Start and run SpiderFoot.

In a terminal, enter the following command: **spiderfoot -l 127.0.0.1:5001**



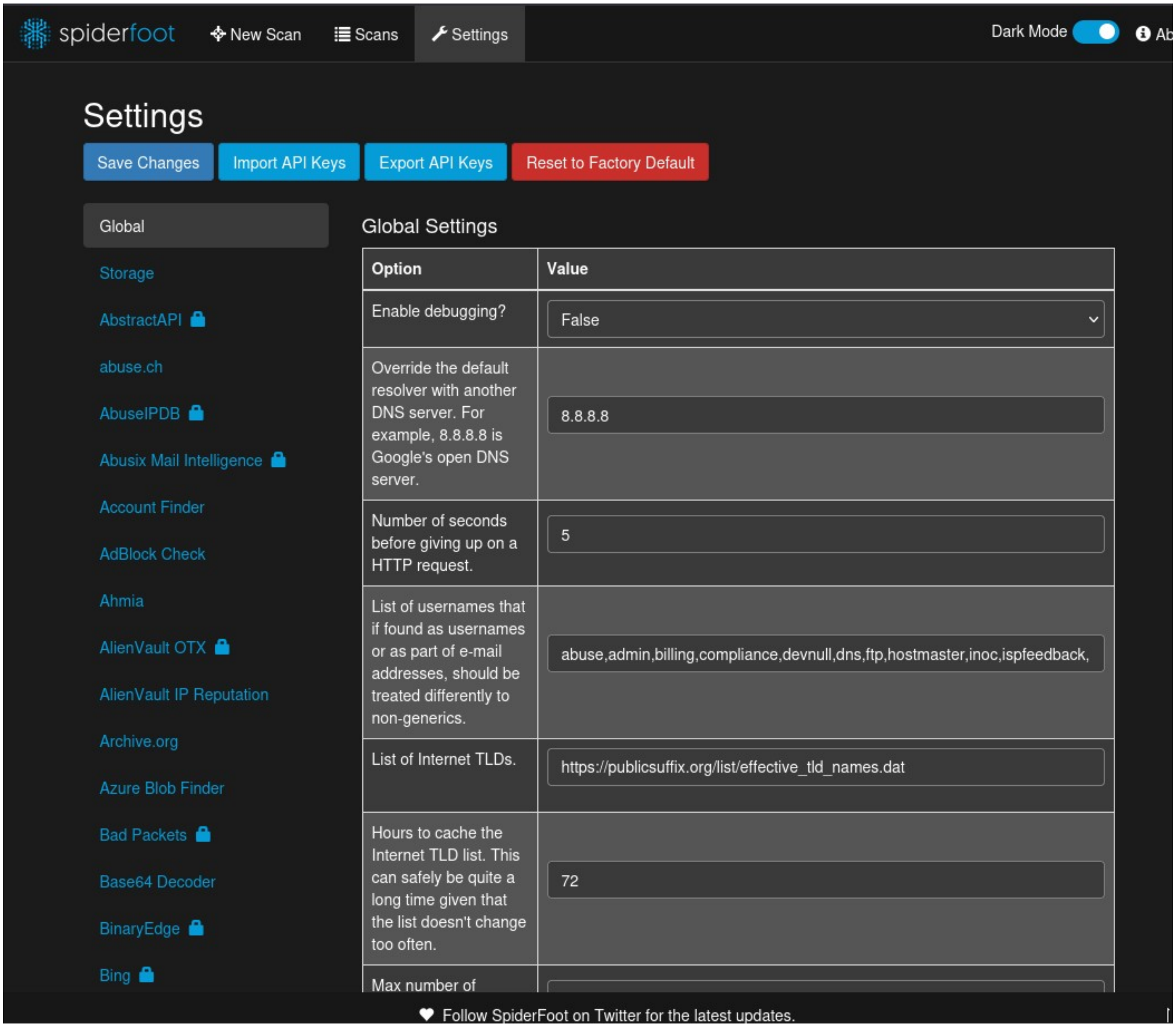
The command should run without errors. Open a browser and enter the IP address and port for the SpiderFoot GUI. You will see the SpiderFoot interface appear. If this is the first time that SpiderFoot has been opened in this VM, you will see the Scans screen. This screen displays a list of all the scans recently run.



Step 2: Explore SpiderFoot.

- Before we get started, look at the scanners that SpiderFoot uses to build its reports. Go to the **Settings** tab.
- The first two entries in the menu at the left are concerned with the operation of SpiderFoot. The entries below this are for the scanners that SpiderFoot uses. There are over 200 of them.

Click the scanners to see their SpiderFoot module name, details about the scanner, and settings that can be made, if any. Complete the table below with some examples. The Scanner name is in the settings menu. The module name appears in the details for the scanner.



All SpiderFoot modules are referred to as sfp_[module name].

> **Hint**: scanners with a lock next to them indicate an API key is necessary. Further information regarding the key requirements is provided in the details for the scanner. Click the “?” icon next to the API Settings option.

Hint: You can interact with SpiderFoot from the terminal too. You can display all the modules that are available in SpiderFoot and pipe the output to a text file. Enter **spiderfoot –h** to view the command line options.

The **grep** command can then be used to search the file for keywords. This will not provide information

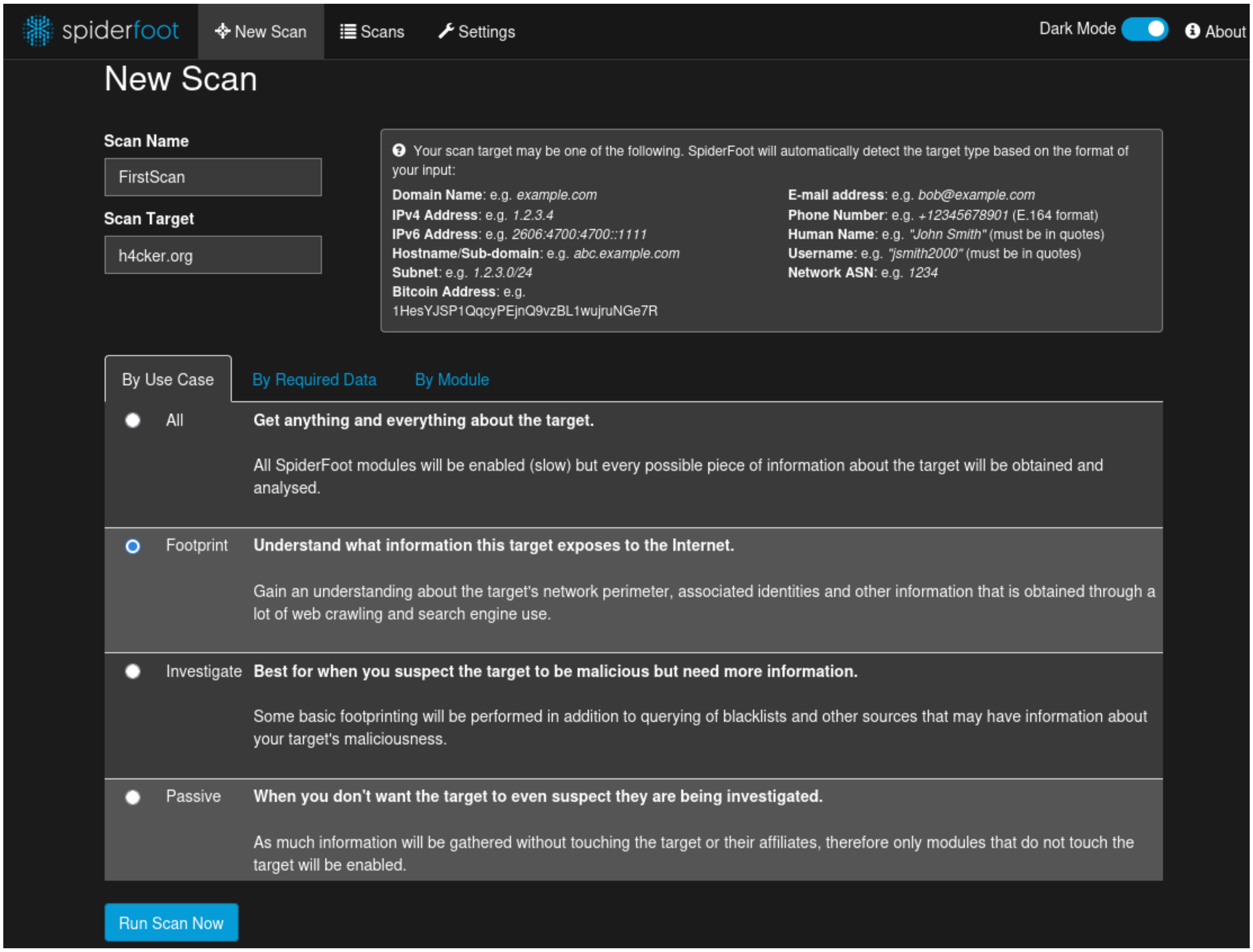
Information Type	Scanner/Module Name	API key requred? Free?
Possible accounts associated with a domain	Account Finder sfp_accounts	No, N/A
Links that are associated with the target	Cross-Referencer, sfp_crossref	no
Email addresses associated with the target	EmailCrawlr, sfp_emailcrawlr	Yes, free plan
Domains and URLs that are associated with the target	grep.app, sfp_grep_app	Yes, free plan
Geolocation information	ipapi.com, sfp_ipapicom	Yes, free plan
Data breach information	Leak-Lookup, sfp_keybase	Yes, free

Step 3: Run a SpiderFoot Scan for a Domain.

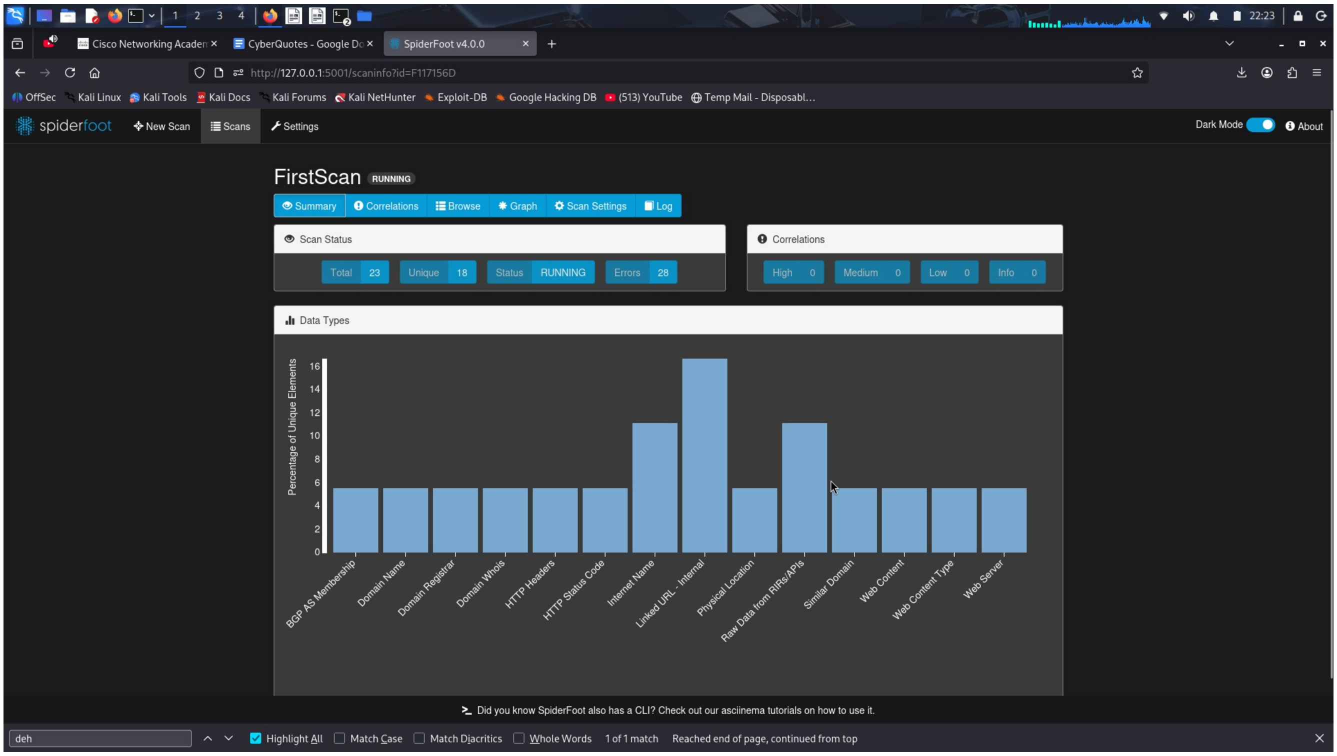
- Click the **New Scan** tab in the GUI.
- Enter a **name** for the scan and select a **target**. In this case, we will use **h4cker.org**.
- You will scan **by use case.** Note that you can also scan by the type of information required or by selecting the individual scanner modules that you would like to use. By executing narrower scans, you can learn more about the modules and information that can be gathered.
- Select the scan use case as **Footprint**.

Note: The **All** use case scan may use active scanning. Unless you have permission to scan the target, you should avoid this setting. To be completely safe, the Passive use case should avoid any problems with unauthorized scanning.

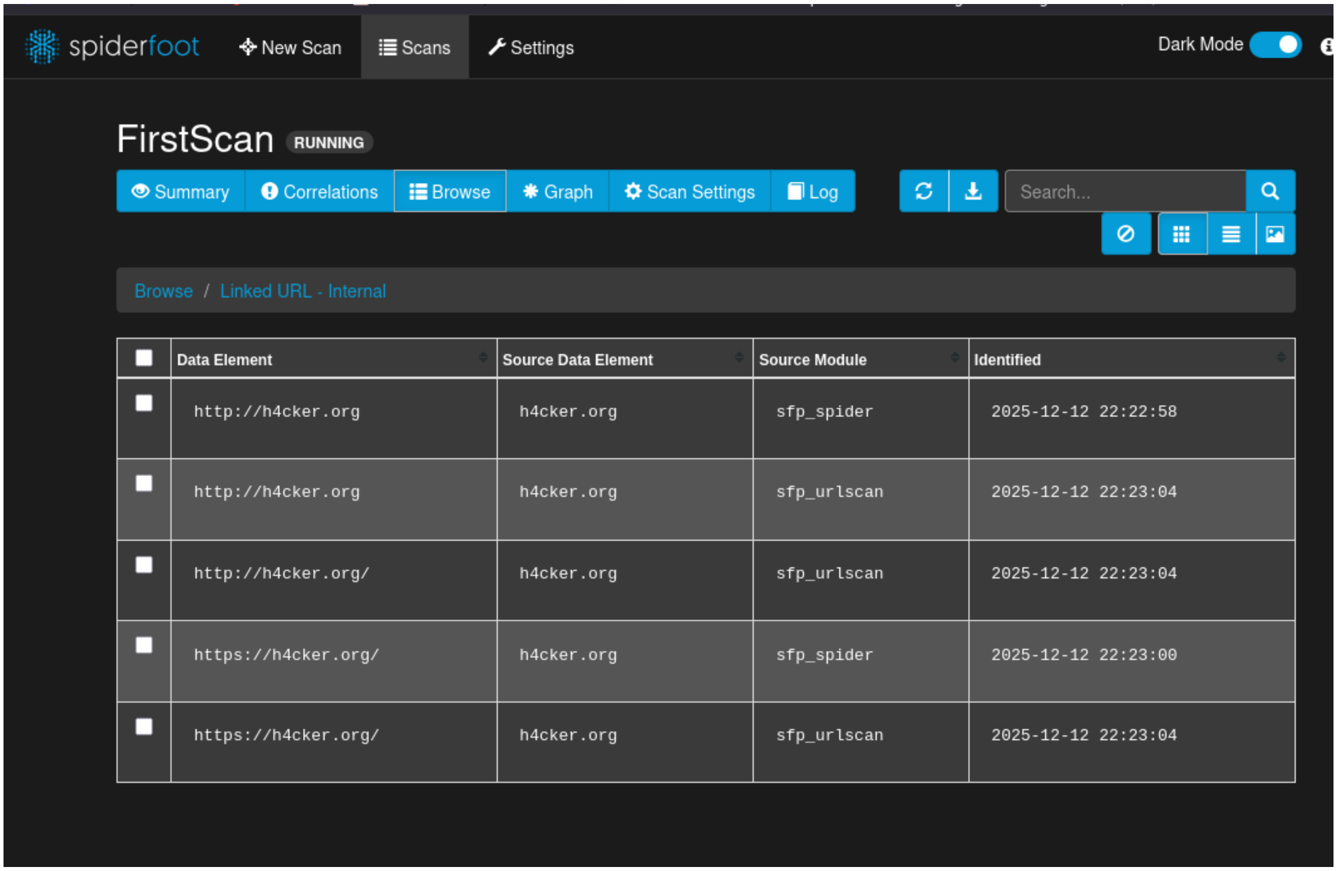
- Click the **Run Scan Now** button.



- You should see a bar graph appear. The scan statistics will start to increment, and new bars will appear in the graph as new results are obtained. Mouse over the bars for a summary of the findings for that data type.

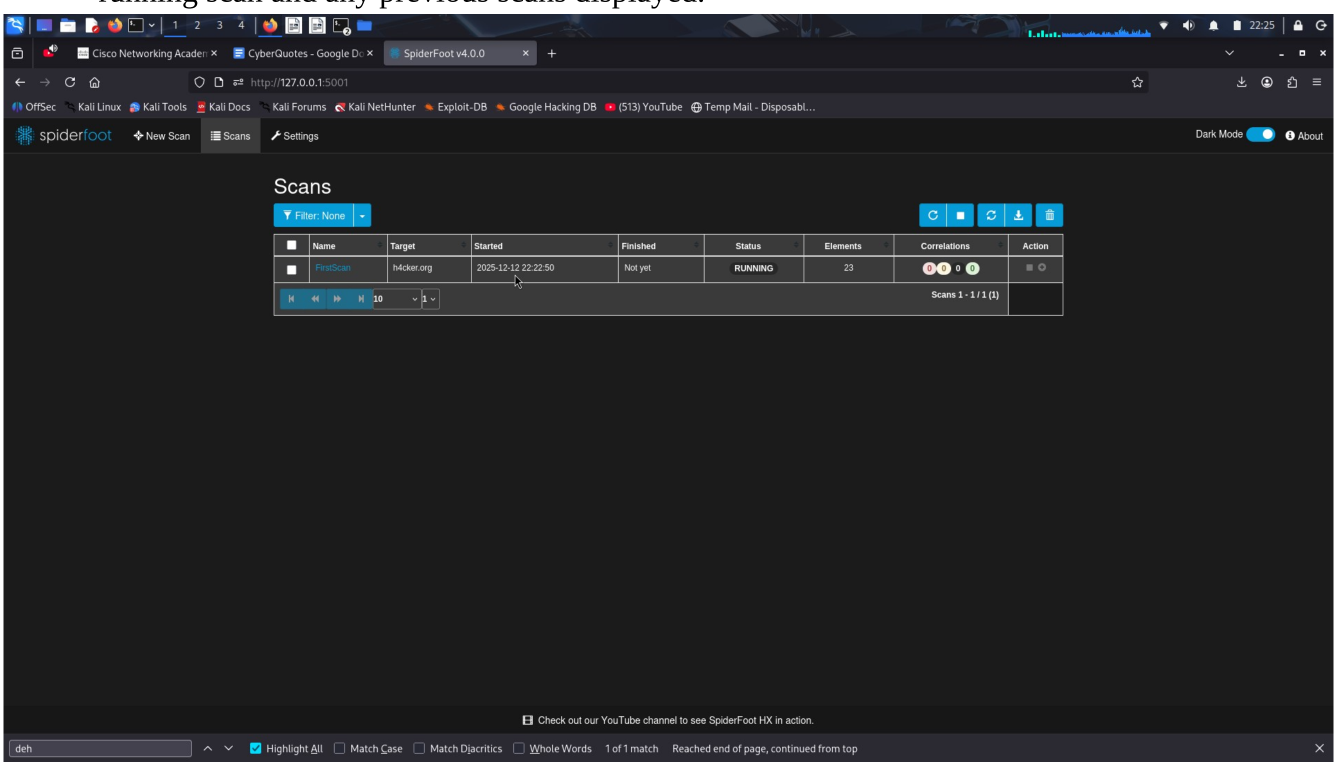


- SpiderFoot scans are very detailed and can take a very long time. Give this scan at least 30 minutes so that there is a nice collection of information. To get the most details, a scan could take hours. While the scan is running, you can browse the results.



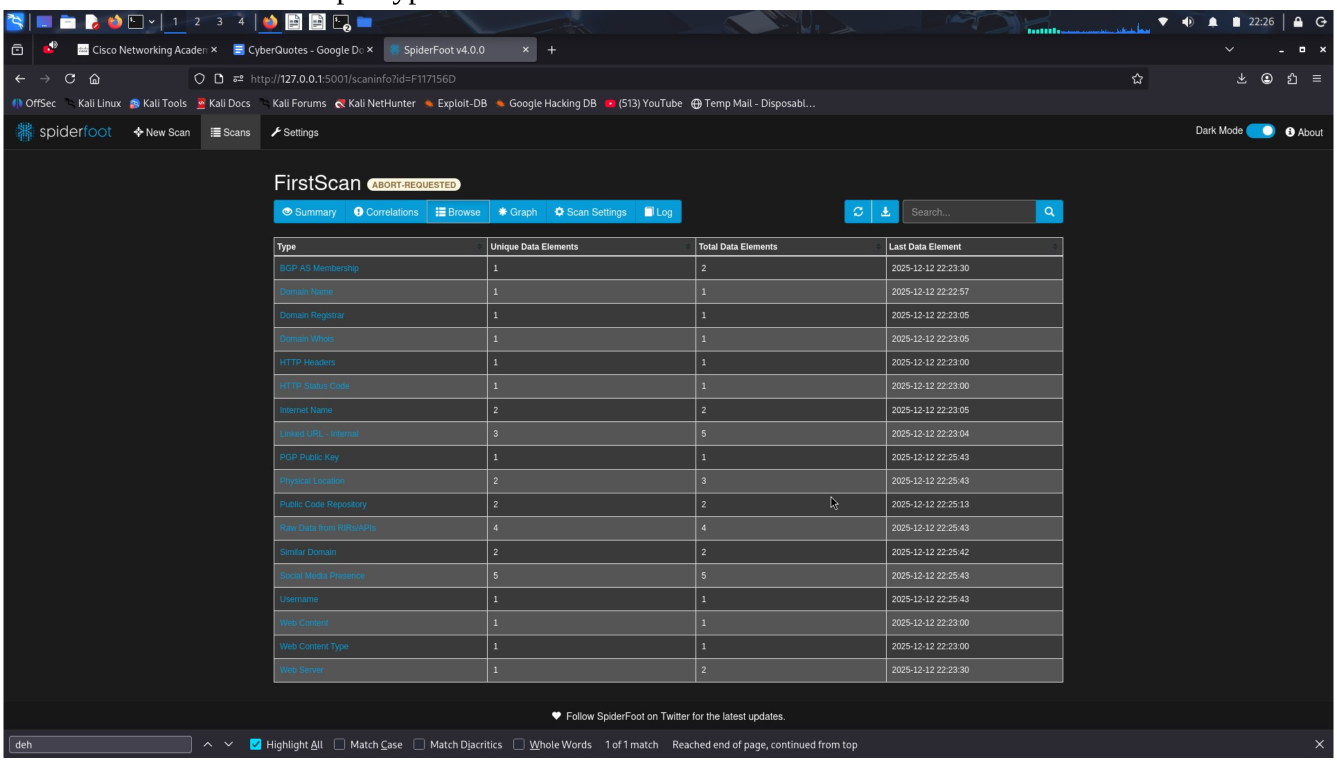
Step 4: Investigate Scan Results.

a. Go back to the scan results, by clicking the **Scans** tab. You will see a table with the currently running scan and any previous scans displayed.

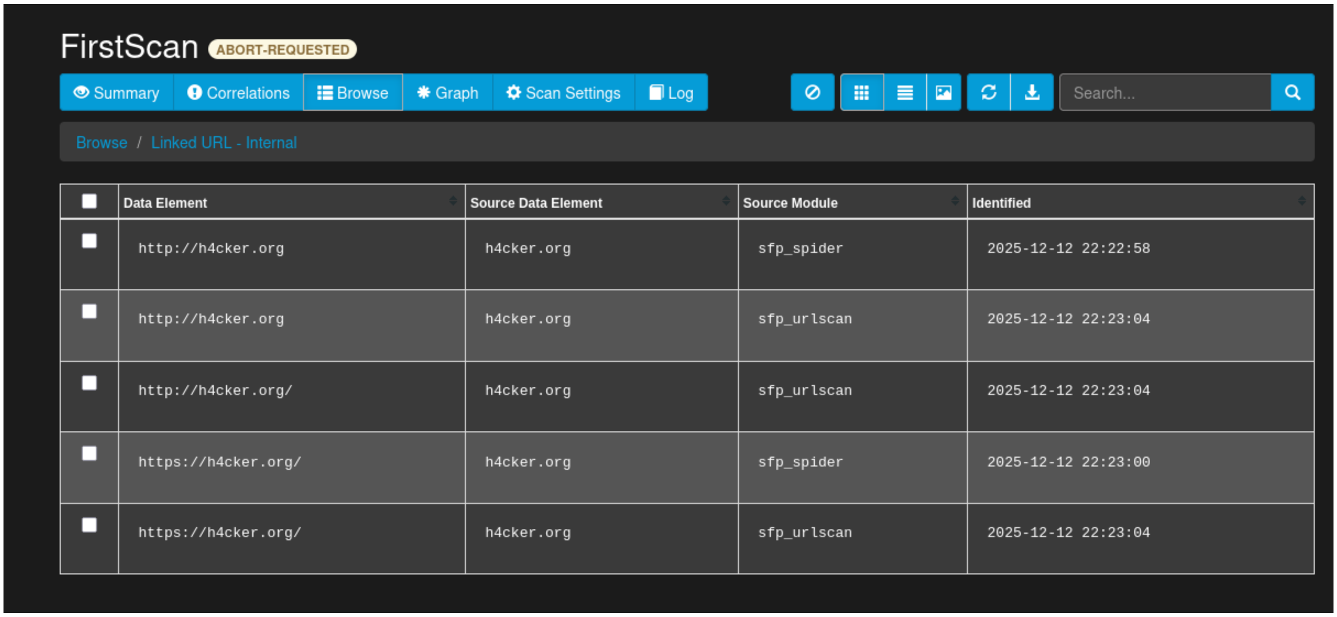


b. Click the black square in the right-most column of the scans table to stop the scan. Some information is not available until the scan is aborted or completed.

c. Click the name of the scan in the table to return to the scan view. You will be taken to the **Browse** tab. Each row in the table represents data found by the various modules. Some modules contribute to multiple types of data.



d. Investigate the results.



Step 5: Register API Keys (optional).

API keys will enhance the functionality of SpiderFoot. Some of these API keys require free registration. The pentesting tools that are available are constantly evolving. Some tools or services that were once free and open can become fee-based over time.

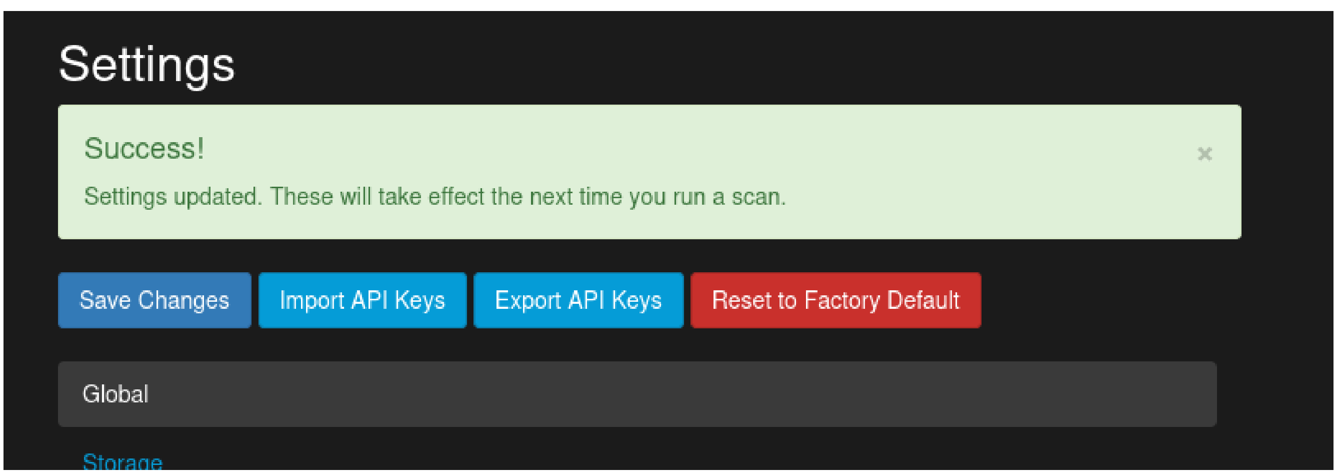
Note: Some APIs may limit your results after you have reached a prescribed number of uses.

a. Go to the **Settings** tab.
b. Find the four modules in the table below. Open the page for the module and complete the table including the type of information that module searches for. For each module in the table, click the ? next to the API option. Follow the instructions to get API keys for the four modules.

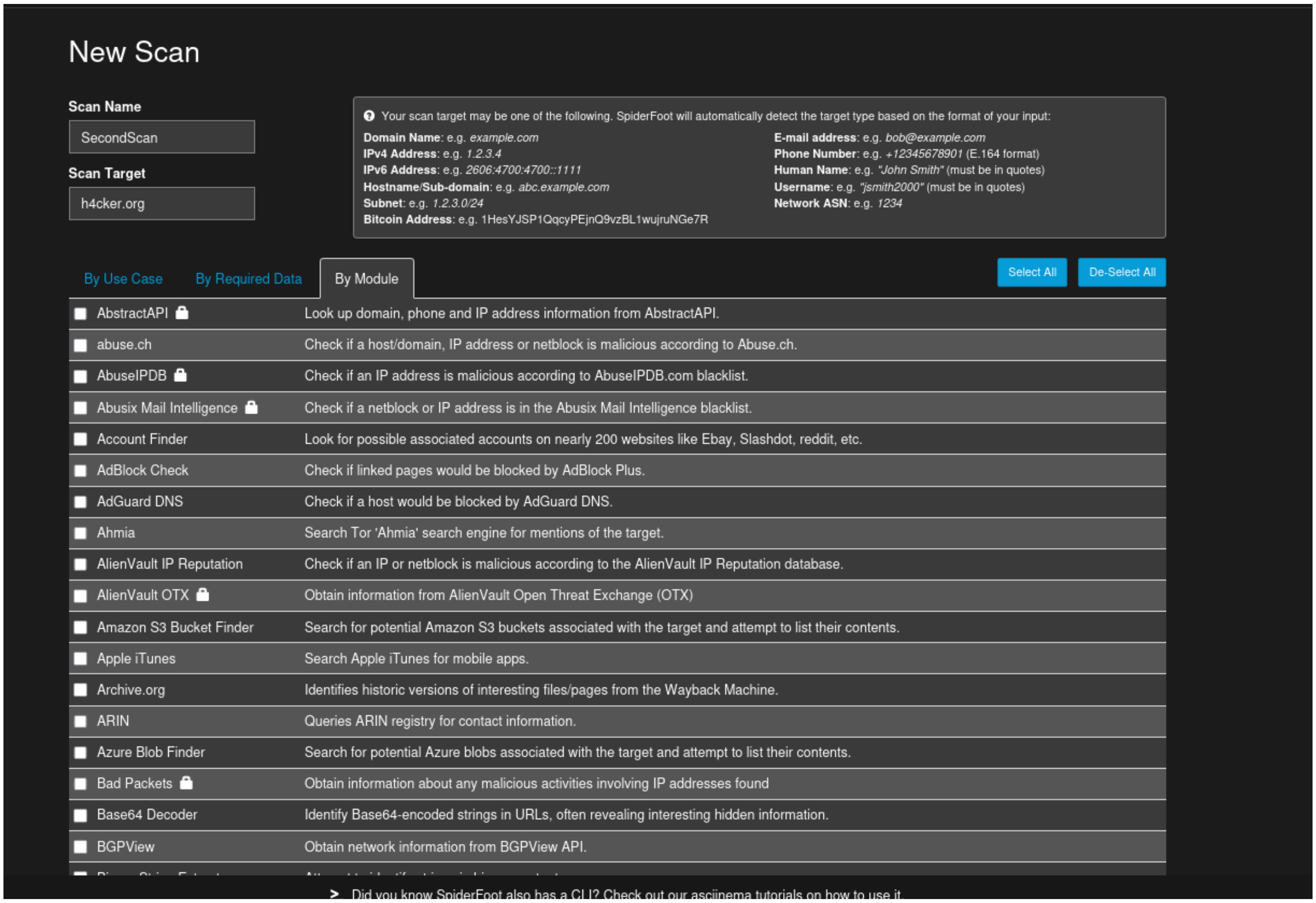
Module	Type of Information	Your API Key, etc
Builtwith	Answer Area and country based analytics for all web technologies.	Answer Area 1a03b92a-d53d-45c5-8e45-c5748fe97713
Hunter.io	Answer Area Check for e-mail addresses and names	Answer Area Enter your answer here
Onion.link	Answer Area Enabling search and global access to Tor's onionsites.	Answer Area AIzaSyDk22nIZk8Pjy6-dIF2byq1FdJ5BgYweds
IntelligenceX	Answer Area Obtain information about identified IP addresses, domains, e-mail addresses	Answer Area f816f212-c462-40d8-a829-3a028b2dd1e5

Module	Type of Information	Your API Key, etc
Builtwith	web software in use	Answers will vary.
Hunter.io	email address search	Answers will vary.
Onion.link	Tor onion site search	Answers will vary.
IntelligenceX	everything	Answers will vary.

Enter the API keys in the settings for each module. Be sure to save your changes.

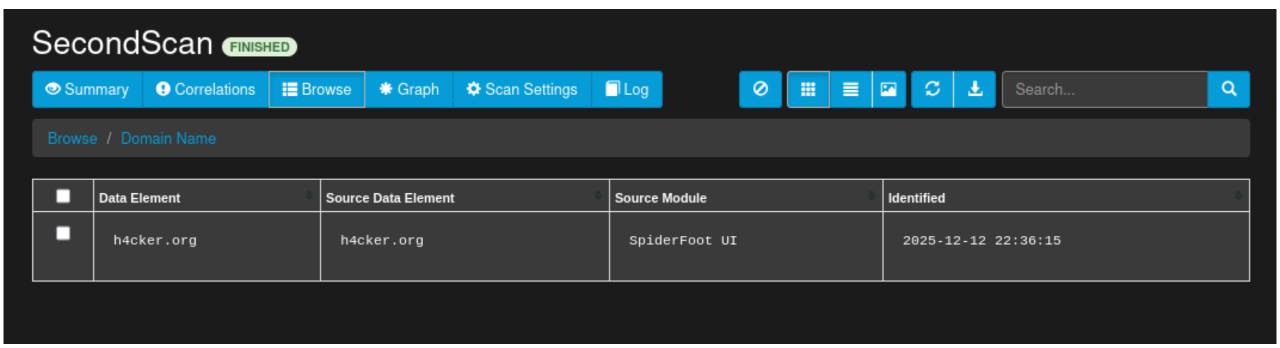


- Click **New Scan**. Go to the By Module tab. Select only the modules for which you have added API keys. All other modules should be unchecked.
- Enter the target as **h4cker.org** and click **Start Scan**. Feel free to scan other domains but be sure to observe the terms and conditions of this course.

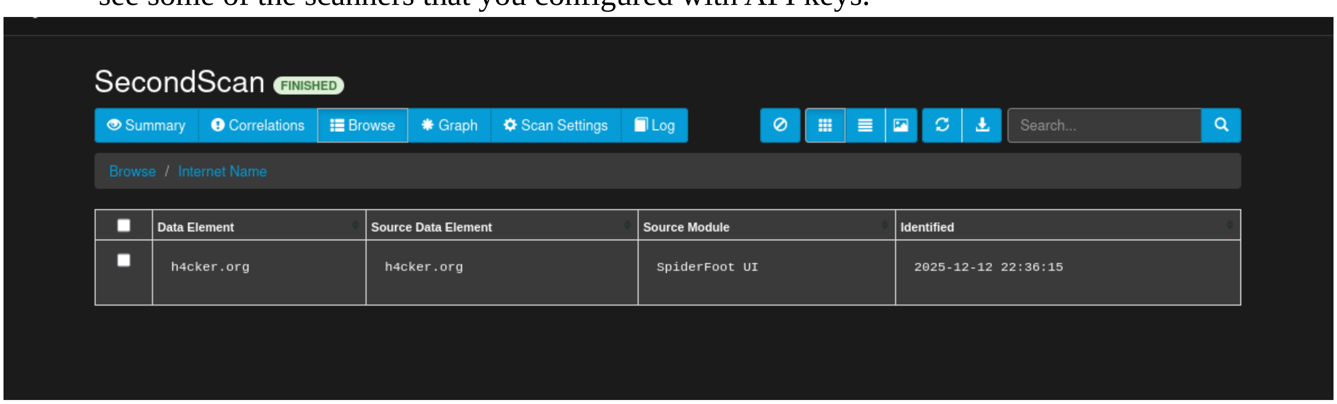


Step 6: Analyze Results of API Modules Scans.

a. This scan should not take very long.



b. Browse the scan to look at the results. Pay attention to the **Source Module** column. You should see some of the scanners that you configured with API keys.



c. Go to the Leak Site URL type in the table of results.

Part 3: Investigate Recon-ng

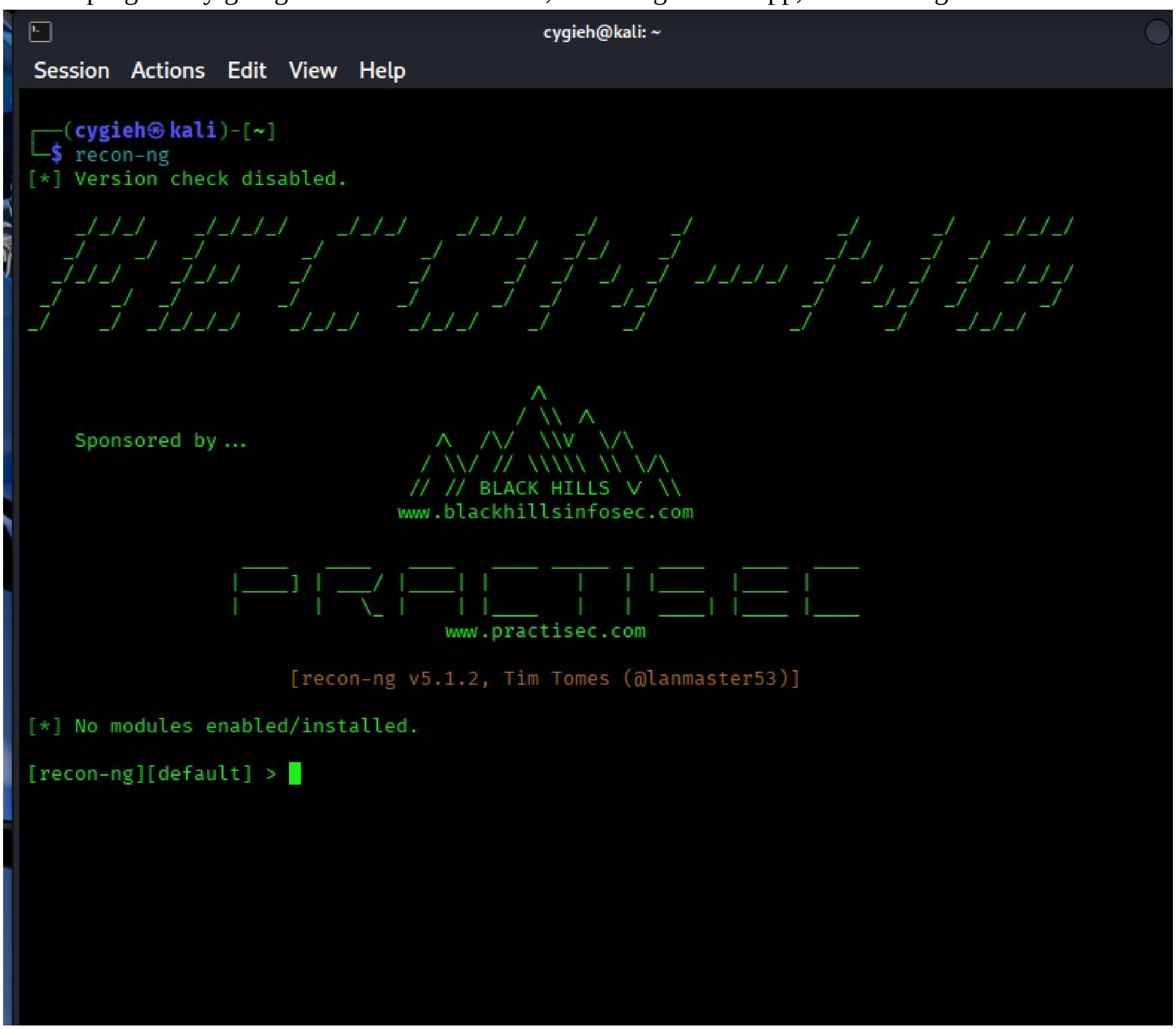
Recon-ng is an OSINT framework that is similar to the Metasploit exploitation framework or the Social-Engineering Tooklit (SET).

Recon-ng is used to perform a wide range of reconnaissance activities on different settings that you provide. Some modules are available with the Kali installation and others are available for download and installation in the Recon-ng modules marketplace.

Step 1: Create a workspace.

Recon-ng has auto complete. Press the tab button to complete commands and command options. Use the tab key twice to list the available commands and options at different places in the command line. This is very handy.

a. To run Recon-ng, open a new terminal window and enter **recon-ng**. You can also start the program by going to the Kali tools menu, searching for the app, and clicking the icon.



b. Note that the terminal prompt changes to indicate that you are working within the Recon-ng framework. Enter **help** to get a sense of the commands that are available.

```
[recon-ng][default] > help

Commands (type [help|?] <topic>):
---------------------------------
back            Exits the current context
dashboard       Displays a summary of activity
db              Interfaces with the workspace's database
exit            Exits the framework
help            Displays this menu
index           Creates a module index (dev only)
keys            Manages third party resource credentials
marketplace     Interfaces with the module marketplace
modules         Interfaces with installed modules
options         Manages the current context options
pdb             Starts a Python Debugger session (dev only)
script          Records and executes command scripts
shell           Executes shell commands
show            Shows various framework items
snapshots       Manages workspace snapshots
spool           Spools output to a file
workspaces      Manages workspaces

[recon-ng][default] >
```

c. Recon-ng uses workspaces to isolate investigations from one another. Workspaces can be created for different parts of a test or different customers for example. Type **workspaces help** to view options for the workspaces command.

```
[recon-ng][default] > workspaces help
Manages workspaces

Usage: workspaces <create|list|load|remove> [ ... ]

[recon-ng][default] >
```

How can you display the available workspaces?

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

  +----------------------------------+
  | Workspaces |       Modified      |
  +----------------------------------+
  | default    | 2025-12-12 22:46:12 |
  +----------------------------------+
```

How can you create a workspace?

```
[recon-ng][default] > workspaces create jana
[recon-ng][jana] > back
```

How can you remove a workspace?

```
[recon-ng][default] > workspaces remove jana
[recon-ng][default] >
```

Create a workspace named **test** by entering **workspaces create** followed by the workspace name. Note that the prompt has changed to indicate that you are in this workspace.

Type **help** to see the commands that are available within workspaces.

```
[recon-ng][default] > workspaces create test
[recon-ng][test] > help

Commands (type [help|?] <topic>):
---------------------------------
back            Exits the current context
dashboard       Displays a summary of activity
db              Interfaces with the workspace's database
exit            Exits the framework
help            Displays this menu
index           Creates a module index (dev only)
keys            Manages third party resource credentials
marketplace     Interfaces with the module marketplace
modules         Interfaces with installed modules
options         Manages the current context options
pdb             Starts a Python Debugger session (dev only)
script          Records and executes command scripts
shell           Executes shell commands
show            Shows various framework items
snapshots       Manages workspace snapshots
spool           Spools output to a file
workspaces      Manages workspaces

[recon-ng][test] >
```

Step 2: Investigate modules.

Recon-ng is a modular framework. Modules are Python programs with different functions. They are stored in an external marketplace that permits developers to create their own modules and contribute them for use by others.

Return to the Recon-ng prompt. Enter the **modules search** command. This will display the currently installed modules.

Step 3: Investigate the module marketplace.

Recon-ng will not function without modules. In this step, we will install modules from the Recon-ng marketplace. The module marketplace is a GitHub public repository. Search the web for **recon-ng-marketplace** to view the repository. Explore the folders to learn more about the modules.

a. In the terminal, view help for the **marketplace** command. Use the **search** option to list all the modules that are currently available.

```
[recon-ng][default] > marketplace search
```

cygieh@kali: ~

Session Actions Edit View Help

```
  | recon/netblocks-hosts/censys_netblock            | 2.1     | not installed | 2022-01-31 |
 |
  | recon/netblocks-hosts/reverse_resolve            | 1.0     | not installed | 2019-06-24 |
 |
  | recon/netblocks-hosts/shodan_net                 | 1.2     | not installed | 2020-07-21 |
 |
  | recon/netblocks-hosts/virustotal                 | 1.0     | not installed | 2019-06-24 |
 |
  | recon/netblocks-ports/census_2012                | 1.0     | not installed | 2019-06-24 |
 |
  | recon/netblocks-ports/censysio                   | 1.0     | not installed | 2019-06-24 |
 |
  | recon/ports-hosts/migrate_ports                  | 1.0     | not installed | 2019-06-24 |
 |
  | recon/ports-hosts/ssl_scan                       | 1.1     | not installed | 2021-08-24 |
 |
  | recon/profiles-contacts/bing_linkedin_contacts   | 1.2     | not installed | 2021-08-24 |
 |
  | recon/profiles-contacts/dev_diver                | 1.1     | not installed | 2020-05-15 |
 |
  | recon/profiles-contacts/github_users             | 1.0     | not installed | 2019-06-24 |
 |
  | recon/profiles-profiles/namechk                  | 1.0     | not installed | 2019-06-24 |
 |
  | recon/profiles-profiles/profiler                 | 1.2     | not installed | 2023-12-30 |
 |
  | recon/profiles-profiles/twitter_mentioned        | 1.0     | not installed | 2019-06-24 |
 |
  | recon/profiles-profiles/twitter_mentions         | 1.0     | not installed | 2019-06-24 |
 |
  | recon/profiles-repositories/github_repos         | 1.1     | not installed | 2020-05-15 |
 |
  | recon/repositories-profiles/github_commits       | 1.0     | not installed | 2019-06-24 |
 |
  | recon/repositories-vulnerabilities/gists_search  | 1.0     | not installed | 2019-06-24 |
 |
  | recon/repositories-vulnerabilities/github_dorks  | 1.0     | not installed | 2019-06-24 |
 |
  | reporting/csv                                    | 1.0     | not installed | 2019-06-24 |
 |
  | reporting/html                                   | 1.0     | not installed | 2019-06-24 |
 |
  | reporting/json                                   | 1.0     | not installed | 2019-06-24 |
 |
  | reporting/list                                   | 1.0     | not installed | 2019-06-24 |
 |
  | reporting/proxifier                              | 1.0     | not installed | 2019-06-24 |
 |
  | reporting/pushpin                                | 1.0     | not installed | 2019-06-24 |
 |
  | reporting/xlsx                                   | 1.0     | not installed | 2019-06-24 |
 |
  | reporting/xml                                    | 1.1     | not installed | 2019-06-24 |
 |
  +--------------------------------------------------------------------------------------------
-+

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

[recon-ng][default] >
```

b. Note that the modules are organized by their category and type. This appears as a path prepended to the name of the module. You can filter the output by adding a search term to the marketplace search command. Try a few different search terms that are related to OSINT information to get a sense of the modules that are available.

```
[recon-ng][default] > marketplace search grep | reporting
[*] Searching module index for 'grep | reporting'...
[!] No modules found.
Searches marketplace modules

Usage: marketplace search [<regex>]

[recon-ng][default] > marketplace info
Shows detailed information about available modules

Usage: marketplace info <<path>|<prefix>|all>
```

To learn more about individual modules, use the **marketplace info** command followed by the full name of the module, including its category and type. It is easier to select the name of the module and copy and paste it into the command line.

```
[recon-ng][default] > marketplace info reporting/xml

  +------------------------------------------------------------------------+
  | path          | reporting/xml                                          |
  | name          | XML Report Generator                                   |
  | author        | Eric Humphries (@e2fsck) and Tim Tomes (@lanmaster53)  |
  | version       | 1.1                                                    |
  | last_updated  | 2019-06-24                                             |
  | description   | Creates an XML report.                                 |
  | required_keys | []                                                     |
  | dependencies  | []                                                     |
  | files         | []                                                     |
  | status        | not installed                                          |
  +------------------------------------------------------------------------+

[recon-ng][default] >
```

Step 4: Install a new module.

Recon-ng accesses modules from the Github repository and downloads them to Kali when they are installed.

a. Search the marketplace modules using **bing** as a search term. Locate a module that requires no dependencies or API keys.

```
[recon-ng][default] > marketplace info bing

  +---------------------------------------------------------------------------------------------------------------------------
---------------------------------------------------------------------------------------------------------------------------------
---------------------------------------------------------------------------------------------------------------------------------
---------------------------------------------------------------------------------------------------------------------------------
----------------------------+
  | path          | recon/companies-contacts/bing_linkedin_cache

                            |
  | name          | Bing Cache Linkedin Profile and Contact Harvester

                            |
  | author        | Joe Black (@MyChickenNinja), @fullmetalcache, and Brian King

                            |
  | version       | 1.0

                            |
  | last_updated  | 2019-06-24

                            |
  | description   | Harvests profiles from LinkedIn by querying the Bing API cache for LinkedIn pa
s related to the given companies, and adds them to the 'profiles' table. The module will then pars
the resulting information to extract the user's full name and job title (title parsing recently im
oved). The user's full name and title are then added to the 'contacts' table. This module does not
ccess LinkedIn at any time. |
  | required_keys | ['bing_api']

                            |
  | dependencies  | []
```

```
+--------------------------------------------------------------------------------------------------------------+
| path          | recon/domains-hosts/bing_domain_web                                                          |
| name          | Bing Hostname Enumerator                                                                     |
| author        | Tim Tomes (@lanmaster53)                                                                     |
| version       | 1.1                                                                                          |
| last_updated  | 2019-07-04                                                                                   |
| description   | Harvests hosts from Bing.com by using the 'site' search operator. Updates the 'hosts' table with the results. |
| required_keys | []                                                                                           |
| dependencies  | []                                                                                           |
| files         | []                                                                                           |
| status        | not installed                                                                                |
+--------------------------------------------------------------------------------------------------------------+


+--------------------------------------------------------------------------------------------------------------
```

- View information for this module.
- To install the module, copy the full name, including the path, to the clipboard.
- Enter the **marketplace install** command followed by the full name of the module.
- `[recon-ng][default] >` **`marketplace install recon/domains-hosts/bing_domain_web`**
- After installation, enter the **modules search** command to verify that the new module is now available.

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

  Recon
  -----
    recon/domains-hosts/bing_domain_web

[recon-ng][default] >
```

- Repeat the process to install the **hackertarget** module.

```
[recon-ng][default] > marketplace install hackertarget
[*] Module installed: recon/domains-hosts/hackertarget
[*] Reloading modules ...
[recon-ng][default] > module search
[!] Invalid command: module search.
[recon-ng][default] > modules search

  Recon
  -----
    recon/domains-hosts/bing_domain_web
    recon/domains-hosts/hackertarget

[recon-ng][default] >
```

Step 5: Run the new modules

a. Create a new workspace. Name it as you wish.

```
[recon-ng][default] > workspaces create Test1
[recon-ng][Test1] >
```

b. To start working with a module, it must be initialized. Enter **modules load hackertarget** to begin working with the module. Note that the prompt changes to reflect the loaded module.

```
[recon-ng][Test1] > modules load hackertarget
[recon-ng][Test1][hackertarget] >
```

c. Each module is its own environment. The developers of recon-ng have taken care to keep the framework consistent, so the same commands are available for each module. However, the options can vary. Type **info** at the module prompt to view important details about the module.

```
[recon-ng][Test1][hackertarget] > info

      Name: HackerTarget Lookup
    Author: Michael Henriksen (@michenriksen)
   Version: 1.1

Description:
  Uses the HackerTarget.com API to find host names. 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][Test1][hackertarget] >
```

- Instead of passing options at the command line, in Recon-ng you set the options and then enter a simple command to execute the module. Use the **options set source** command to set the only option for this module. Complete the command by specifying the target as **hackxor.net**.
- Verify the option setting with the **info** command.

```
[recon-ng][Test1][hackertarget] > options set source hackxor.net
SOURCE => hackxor.net
[recon-ng][Test1][hackertarget] > info

      Name: HackerTarget Lookup
    Author: Michael Henriksen (@michenriksen)
   Version: 1.1

Description:
  Uses the HackerTarget.com API to find host names. Updates the 'hosts' table with the results.

Options:
  Name    Current Value  Required  Description
  ------  -------------  --------  -----------
  SOURCE  hackxor.net    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][Test1][hackertarget] >
```

- Type **run** to execute the module.

```
[recon-ng][Test1][hackertarget] > run

-----------
HACKXOR.NET
-----------
[*] Country: None
[*] Host: Host: research1.hackxor.net
[*] Ip_Address: 138.68.117.124
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] --------------------------------------------------
[*] Country: None
[*] Host: dreaded.hackxor.net
[*] Ip_Address: 138.68.117.124
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] --------------------------------------------------
[*] Country: None
[*] Host: hkrb.hackxor.net
[*] Ip_Address: 138.68.117.124
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] --------------------------------------------------
[*] Country: None
[*] Host: hmrc.hackxor.net
[*] Ip_Address: 138.68.117.124
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] --------------------------------------------------
[*] Country: None
[*] Host: intranet.hackxor.net
[*] Ip_Address: 10.60.10.18
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] --------------------------------------------------
[*] Country: None
[*] Host: research1.hackxor.net
[*] Ip_Address: 138.68.117.124
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] --------------------------------------------------
[*] Country: None
[*] Host: transparency.hackxor.net
[*] Ip_Address: 138.68.117.124
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] --------------------------------------------------
```

- Inspect the output of the command. The output is stored in a database so you can refer to it later. The data that is stored is specific to the workplace in which it was gathered.
- Enter the **dashboard** command. This queries the Recon-ng database and provides a summary of the information that has been gathered. It is specific to this workspace.

```
[recon-ng][Test1][hackertarget] > dashboard

  +------------------------------------------+
  |             Activity Summary             |
  +------------------------------------------+
  |              Module              | Runs |
  +------------------------------------------+
  | recon/domains-hosts/hackertarget | 1    |
  +------------------------------------------+


  +----------------------------+
  |       Results Summary      |
  +----------------------------+
  |     Category    | Quantity |
  +----------------------------+
  | Domains         | 0        |
  | Companies       | 0        |
  | Netblocks       | 0        |
  | Locations       | 0        |
  | Vulnerabilities | 0        |
  | Ports           | 0        |
  | Hosts           | 7        |
  | Contacts        | 0        |
  | Credentials     | 0        |
  | Leaks           | 0        |
  | Pushpins        | 0        |
  | Profiles        | 0        |
  | Repositories    | 0        |
  +----------------------------+

[recon-ng][Test1][hackertarget] >
```

- The **show** command displays the data for specific categories. Enter the **show hosts** command to display the list of hosts that were discovered.

```
[recon-ng][Test1][hackertarget] > show hosts

  +------------------------------------------------------------------------------------------------
------------------------------+
  | rowid |              host            |   ip_address   | region | country | latitude | longitude |
 notes |    module     |
  +------------------------------------------------------------------------------------------------
------------------------------+
  | 1     | Host: research1.hackxor.net | 138.68.117.124 |        |         |          |           |
        | hackertarget |
  | 2     | dreaded.hackxor.net         | 138.68.117.124 |        |         |          |           |
        | hackertarget |
  | 3     | hkrb.hackxor.net            | 138.68.117.124 |        |         |          |           |
        | hackertarget |
  | 4     | hmrc.hackxor.net            | 138.68.117.124 |        |         |          |           |
        | hackertarget |
  | 5     | intranet.hackxor.net        | 10.60.10.18    |        |         |          |           |
        | hackertarget |
  | 6     | research1.hackxor.net       | 138.68.117.124 |        |         |          |           |
        | hackertarget |
  | 7     | transparency.hackxor.net    | 138.68.117.124 |        |         |          |           |
        | hackertarget |
  +------------------------------------------------------------------------------------------------
------------------------------+

[*] 7 rows returned
[recon-ng][Test1][hackertarget] >
```

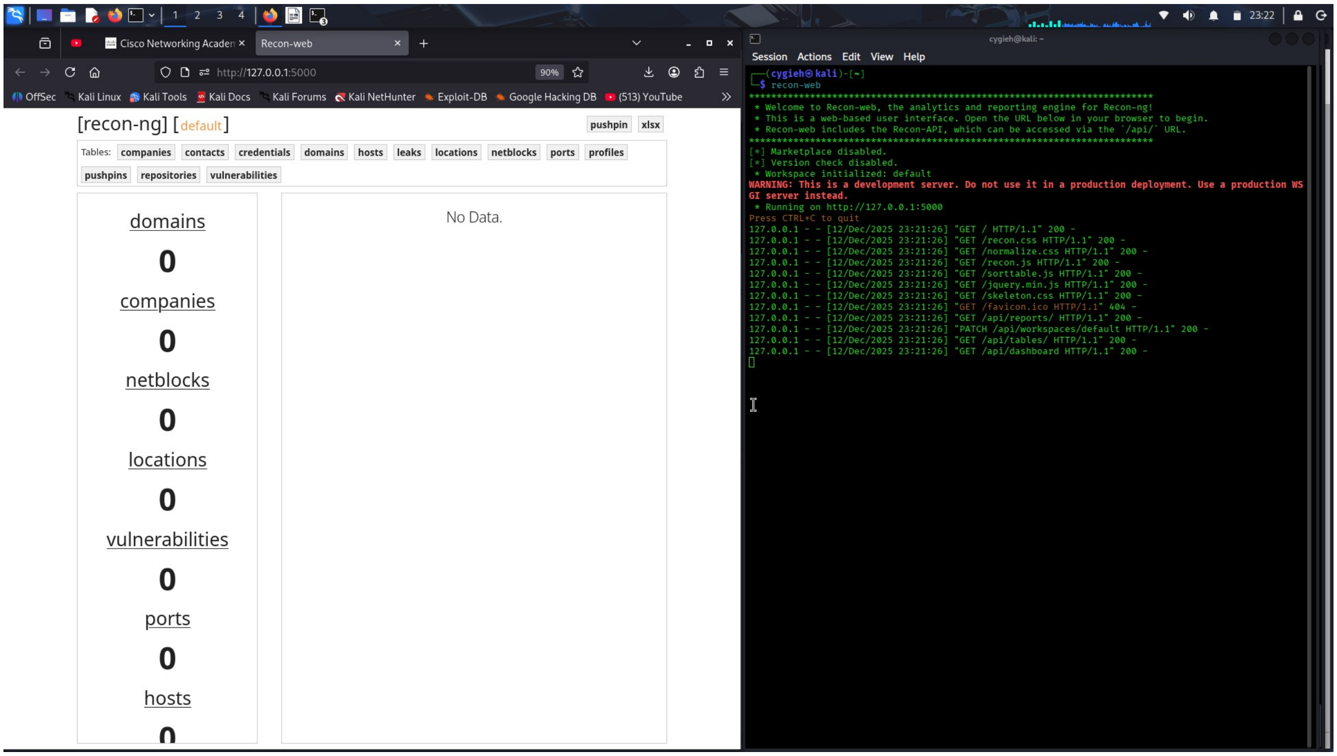
- Now repeat the process with the **bing** module. Compare the results with the **hackertarget** module.

```
Session  Actions  Edit  View  Help
[recon-ng][default] > workspaces create Test2
[recon-ng][Test2] > modules load bing
[recon-ng][Test2][bing_domain_web] > info

      Name: Bing Hostname Enumerator
    Author: Tim Tomes (@lanmaster53)
   Version: 1.1

Description:
  Harvests hosts from Bing.com by using the 'site' search operator. Updates the 'hosts' table with t
he
  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][Test2][bing_domain_web] > options set source bing.net
SOURCE => bing.net
[recon-ng][Test2][bing_domain_web] > info

      Name: Bing Hostname Enumerator
    Author: Tim Tomes (@lanmaster53)
   Version: 1.1

Description:
  Harvests hosts from Bing.com by using the 'site' search operator. Updates the 'hosts' table with t
he
  results.

Options:
  Name    Current Value  Required  Description
  ------  -------------  --------  -----------
  SOURCE  bing.net       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][Test2][bing_domain_web] > run

--------
BING.NET
--------
[*] URL: https://www.bing.com/search?first=0&q=domain%3Abing.net
[recon-ng][Test2][bing_domain_web] > dashboard

  +-------------------------------------------+
  |             Activity Summary              |
  +-------------------------------------------+
  |              Module              | Runs |
  +-------------------------------------------+
```

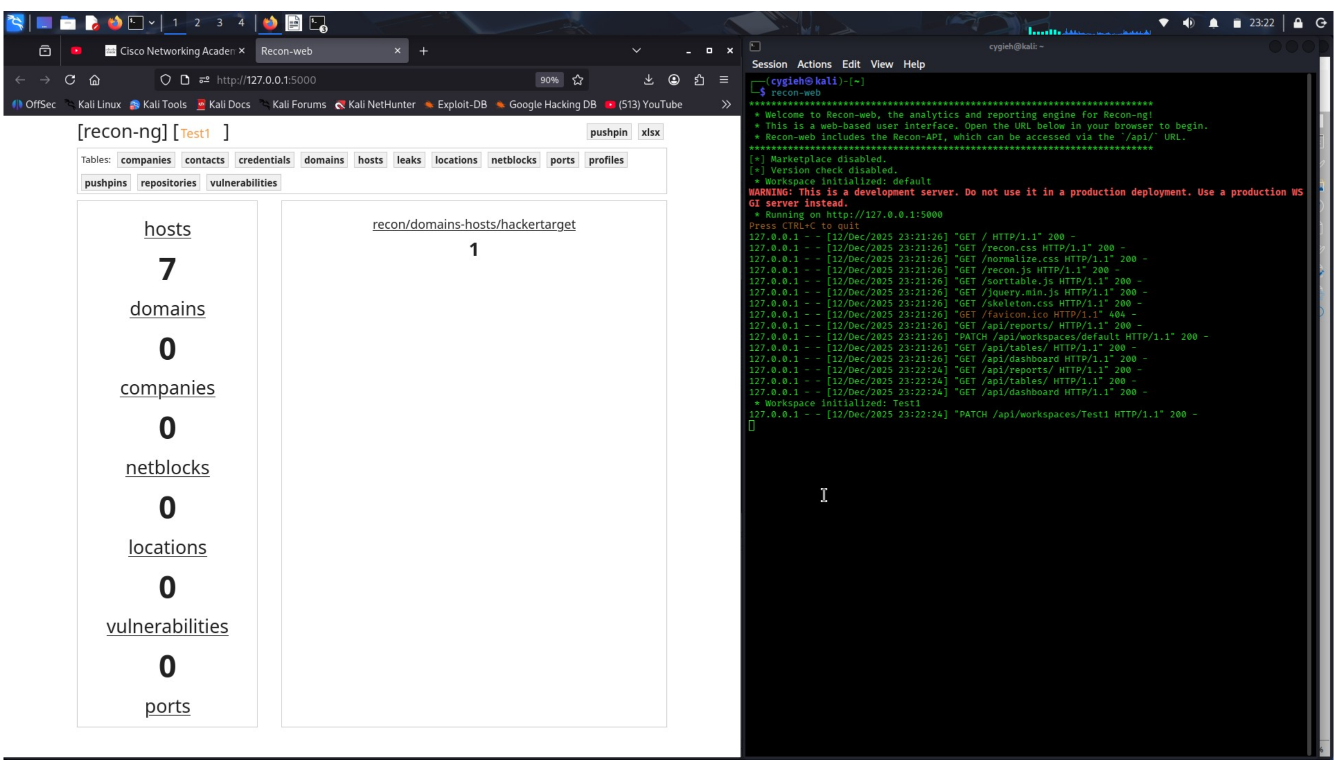
Step 6: Investigate the web interface.

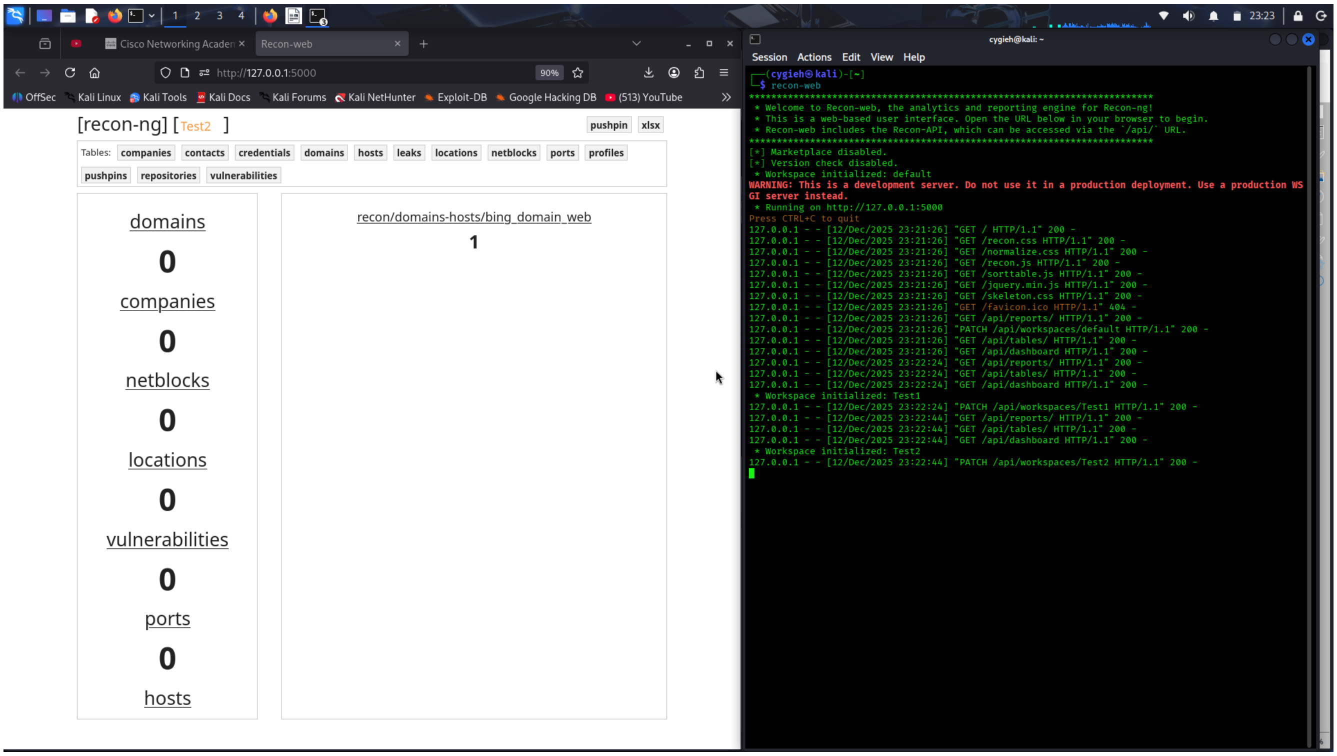
Recon-ng has a web interface that simplifies and improves viewing results that are stored in Recon-ng databases. It also allows easy export of the results tables for reporting purposes.

a. Open a new terminal.
b. Enter the **recon-web** command to start the Recon-ng server process. Note the command output.
c. In a new browser tab, access the webpage using the URL information provided in the output.



d. The web interface shows data from the default workspace when first opened. Click the orange workspace name at the top of the page to display data from different workspaces.





Part 4: Find Interesting Files with Recon-ng

In this part of the lab, we will install and use another plugin.

Step 1: Install another module.

a. Search the marketplace for a module that will discover interesting files in a domain. The plugin that you use should have no dependencies or key requirements.

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

  +---------------------------------------------------------------------------------------------------+
  |                       Path                          | Version |     Status    |  Updated   | D | K |
  +---------------------------------------------------------------------------------------------------+
  | discovery/info_disclosure/cache_snoop               | 1.1     | not installed | 2020-10-13 |   |   |
  | recon/companies-domains/pen                         | 1.1     | not installed | 2019-10-15 |   |   |
  | recon/companies-domains/viewdns_reverse_whois       | 1.1     | not installed | 2021-08-24 |   |   |
  | recon/companies-multi/censys_tls_subjects           | 2.1     | not installed | 2022-01-31 | * | * |
  | recon/contacts-domains/censys_email_to_domains      | 2.1     | not installed | 2022-01-31 | * | * |
  | recon/contacts-domains/migrate_contacts             | 1.1     | not installed | 2020-05-17 |   |   |
  | recon/domains-companies/censys_companies            | 2.1     | not installed | 2022-01-31 | * | * |
  | recon/domains-companies/pen                         | 1.1     | not installed | 2019-10-15 |   |   |
  | recon/domains-companies/whoxy_whois                 | 1.1     | not installed | 2020-06-24 |   | * |
  | recon/domains-contacts/hunter_io                    | 1.3     | not installed | 2020-04-14 |   | * |
  | recon/domains-contacts/metacrawler                  | 1.1     | not installed | 2019-06-24 | * |   |
  | recon/domains-contacts/pen                          | 1.1     | not installed | 2019-10-15 |   |   |
  | recon/domains-contacts/pgp_search                   | 1.4     | not installed | 2019-10-16 |   |   |
  | recon/domains-contacts/whois_pocs                   | 1.0     | not installed | 2019-06-24 |   |   |
  | recon/domains-contacts/wikileaker                   | 1.0     | not installed | 2020-04-08 |   |   |
  | recon/domains-hosts/builtwith                       | 1.1     | not installed | 2021-08-24 |   | * |
  | recon/domains-hosts/censys_domain                   | 2.1     | not installed | 2022-01-31 | * | * |
  | recon/domains-hosts/mx_spf_ip                       | 1.0     | not installed | 2019-06-24 |   |   |
  | recon/domains-hosts/ssl_san                         | 1.0     | not installed | 2019-06-24 |   |   |
  | recon/domains-vulnerabilities/ghdb                  | 1.1     | not installed | 2019-06-26 |   |   |
  | recon/domains-vulnerabilities/xssed                 | 1.1     | not installed | 2020-10-18 |   |   |
  | recon/hosts-domains/migrate_hosts                   | 1.1     | not installed | 2020-05-17 |   |   |
  | recon/hosts-hosts/virustotal                        | 1.0     | not installed | 2019-06-24 |   | * |
  | recon/netblocks-hosts/virustotal                    | 1.0     | not installed | 2019-06-24 |   | * |
  +---------------------------------------------------------------------------------------------------+

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

Install and load the plugin.

```
[recon-ng][default] > marketplace install discovery/info_disclosure/cache_snoop
[*] Module installed: discovery/info_disclosure/cache_snoop
[*] Reloading modules...
[recon-ng][default] > modules load discovery/info_disclosure/cache_snoop
[recon-ng][default][cache_snoop] >
```

Step 2: Run the new module.

a. Set the source option to **hackxor.net** or another location of your choice. (Please comply with the terms of the course when choosing a domain.) The h4cker.org website is interesting also.
b. Run the command. This module creates a .csv file in the recon-ng/data folder.
c. Locate the file and view the contents. Some of these files can be downloaded or viewed using the URLs in the command output.