Lab- Using OSINT Tools

This lab work was done as given in the “information gathering and vulnerability scanning” module in Cisco’s ethical hacking course.

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

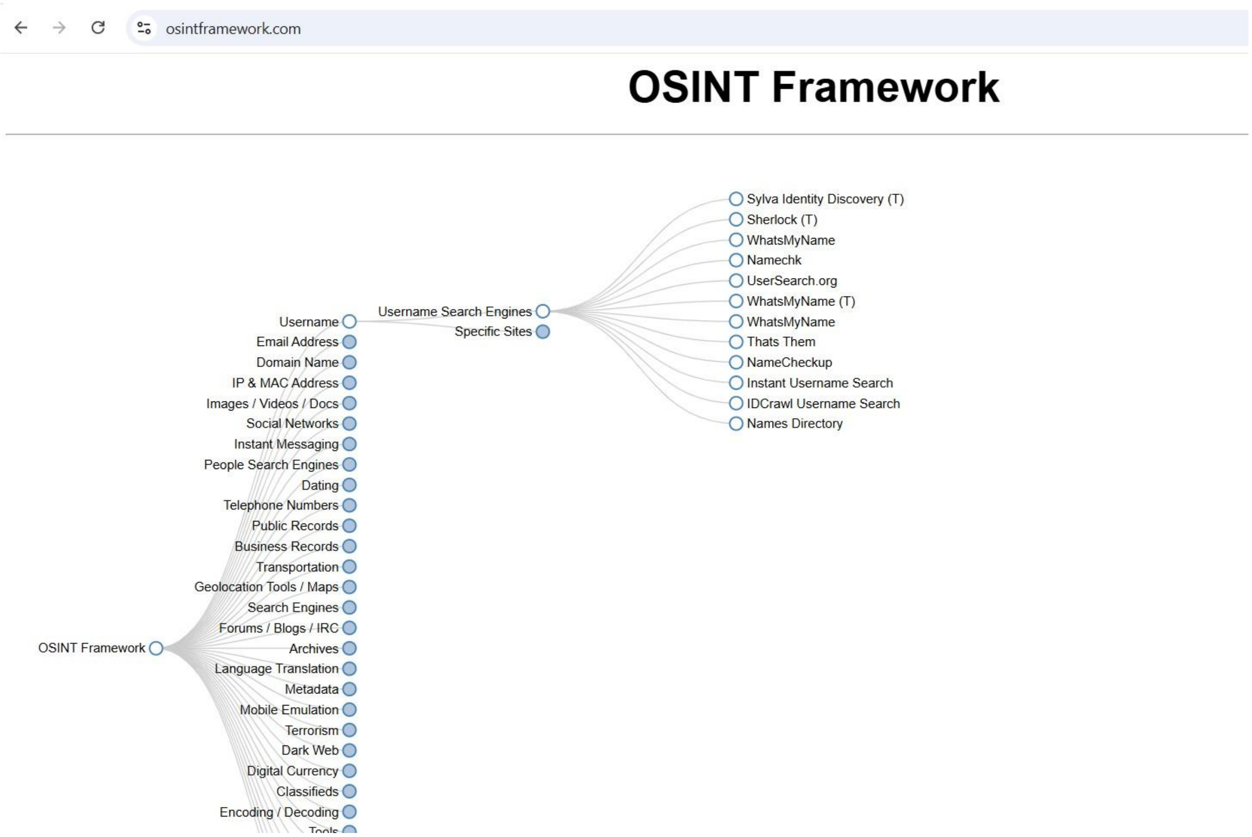
Required Resources

- Kali VM customized for Ethical Hacker course
- Internet access

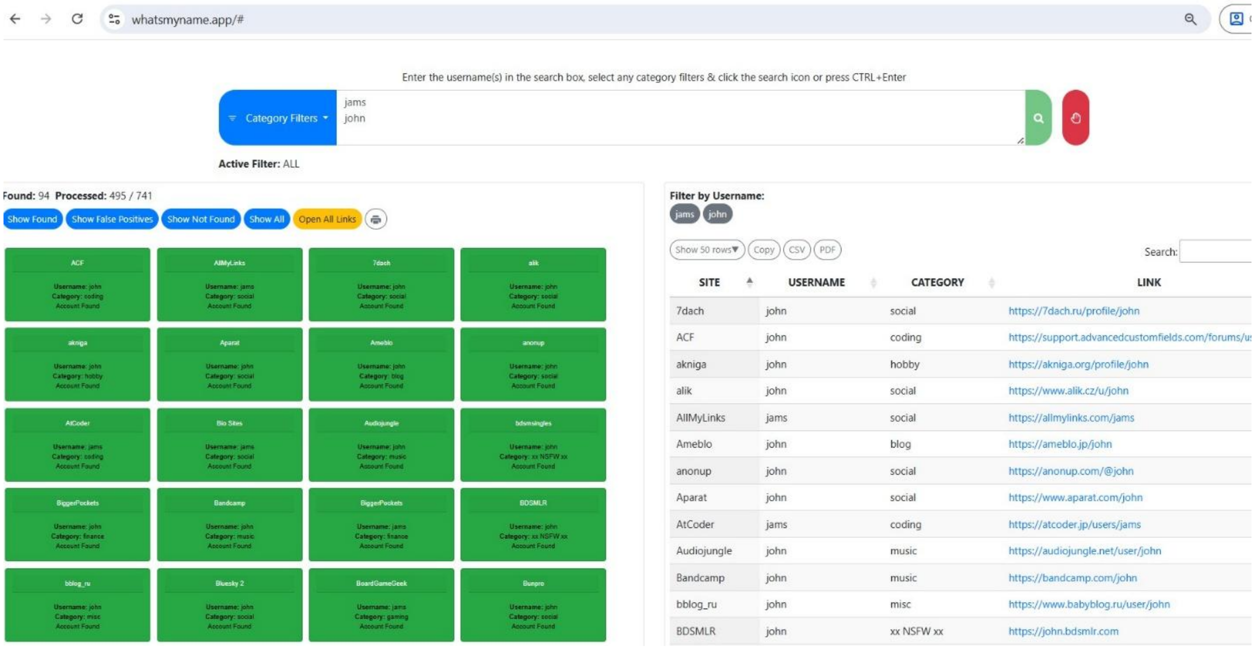
Part 1: Examine OSINT Resources

Step 1: Access the OSINT Framework

1. Go to the OSINT Framework site at https://osintframework.com/.
2. Click Username and click "WhatsMyName(T)" under Username Search Engines.



3. Now go to https://whatsmyname.app/ to visit a website that implements WhatsMyName.
4. In the search box, type in a few usernames (i.e., jams, john), each on a separate line.
5. Investigate the results. You can open the links to the accounts either from the green rectangles or the table of results.



Enter the username(s) in the search box, select any category filters & click the search icon or press CTRL+Enter

jams
john

Active Filter: ALL

Found: 94 **Processed:** 495 / 741

ACF
Username: john
Category: coding
Account Found

AllMyLinks
Username: jams
Category: social
Account Found

7dach
Username: john
Category: social
Account Found

alik
Username: john
Category: social
Account Found

akniga
Username: john
Category: hobby
Account Found

Aparat
Username: john
Category: social
Account Found

Ameblo
Username: john
Category: blog
Account Found

anonup
Username: john
Category: social
Account Found

AtCoder
Username: jams
Category: coding
Account Found

Bio Sites
Username: jams
Category: social
Account Found

Audiojungle
Username: john
Category: music
Account Found

bdsmsingles
Username: john
Category: xx NSFW xx
Account Found

BiggerPockets
Username: john
Category: finance
Account Found

Bandcamp
Username: john
Category: music
Account Found

BiggerPockets
Username: jams
Category: finance
Account Found

BDSMLR
Username: john
Category: xx NSFW xx
Account Found

bblog_ru
Username: john
Category: misc
Account Found

Bluesky 2
Username: john
Category: social
Account Found

BoardGameGeek
Username: jams
Category: gaming
Account Found

Bunpro
Username: john
Category: social
Account Found

Filter by Username:
jams john

SITE	USERNAME	CATEGORY	LINK
7dach	john	social	https://7dach.ru/profile/john
ACF	john	coding	https://support.advancedcustomfields.com/forums/u
akniga	john	hobby	https://akniga.org/profile/john
alik	john	social	https://www.alik.cz/u/john
AllMyLinks	jams	social	https://allmylinks.com/jams
Ameblo	john	blog	https://ameblo.jp/john
anonup	john	social	https://anonup.com/@john
Aparat	john	social	https://www.aparat.com/john
AtCoder	jams	coding	https://atcoder.jp/users/jams
Audiojungle	john	music	https://audiojungle.net/user/john
Bandcamp	john	music	https://bandcamp.com/john
bblog_ru	john	misc	https://www.babyblog.ru/user/john
BDSMLR	john	xx NSFW xx	https://john.bdsmlr.com

6. 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 receive links to the profile pages of users on various sites.

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

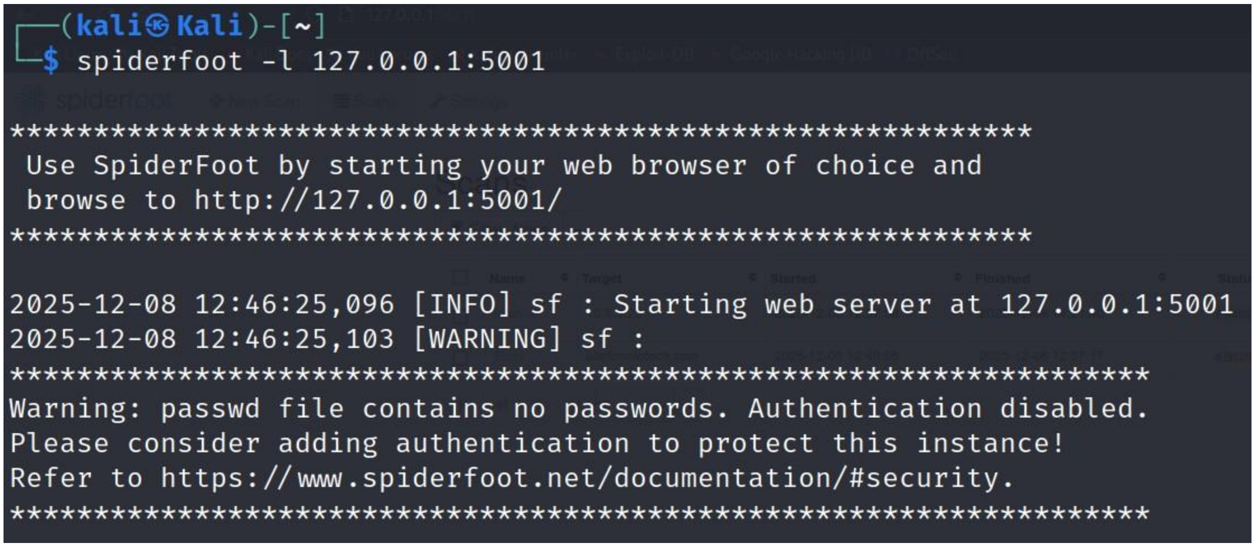
SpiderFoot offers the option of choosing scans based on use case, required data, and by SpiderFoot module. The use cases are:

1. All – Get every possible piece of information about the target. This use case can take a very long time to complete.
2. Footprint – Understand the target's network perimeter, associated identities, and other information that is yielded by extensive web crawling and search engine use.
3. Investigate – These are targets that you suspect of malicious behavior. Footprinting, blacklist lookups, and other sources that report on malicious sites will be returned.
4. Passive – This type of scan is used if the target shouldn't 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:

```
┌──(kali㉿Kali)-[~]
└─$ spiderfoot -l 127.0.0.1:5001
```



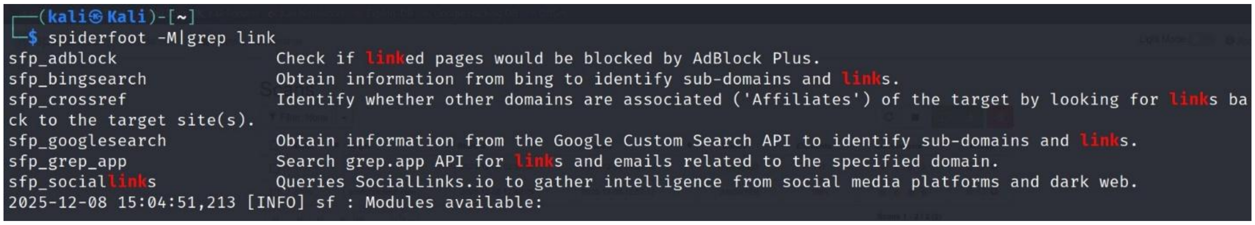
```
┌──(kali㉿Kali)-[~]
└─$ spiderfoot -l 127.0.0.1:5001
*************************************************************
 Use SpiderFoot by starting your web browser of choice and
 browse to http://127.0.0.1:5001/
*************************************************************

2025-12-08 12:46:25,096 [INFO] sf : Starting web server at 127.0.0.1:5001
2025-12-08 12:46:25,103 [WARNING] sf :
********************************************************************
Warning: passwd file contains no passwords. Authentication disabled.
Please consider adding authentication to protect this instance!
Refer to https://www.spiderfoot.net/documentation/#security.
********************************************************************
```

Open a browser and enter the IP address and port for the SpiderFoot GUI

Step 2: Explore SpiderFoot

1. Enter **spiderfoot –h** to view the command line options.
2. Use the **grep** command to search the file for keywords.

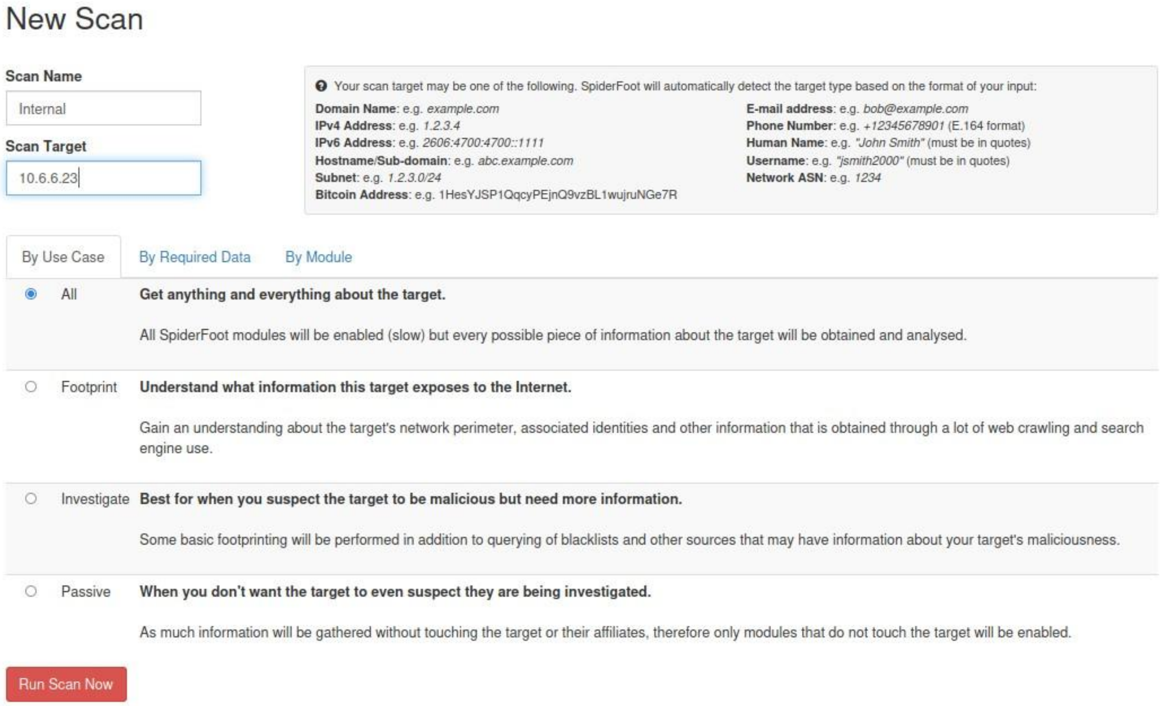
```
┌──(kali㉿Kali)-[~]
└─$ spiderfoot -M | grep [search term]
```



```
┌──(kali㉿Kali)-[~]
└─$ spiderfoot -M|grep link
sfp_adblock                Check if linked pages would be blocked by AdBlock Plus.
sfp_bingsearch             Obtain information from bing to identify sub-domains and links.
sfp_crossref               Identify whether other domains are associated ('Affiliates') of the target by looking for links ba
ck to the target site(s).
sfp_googlesearch           Obtain information from the Google Custom Search API to identify sub-domains and links.
sfp_grep_app               Search grep.app API for links and emails related to the specified domain.
sfp_sociallinks            Queries SocialLinks.io to gather intelligence from social media platforms and dark web.
2025-12-08 15:04:51,213 [INFO] sf : Modules available:
```

Step 3: Run a SpiderFoot Scan

1. Click the New Scan tab in the GUI.
2. Enter a name for the scan and select a target. Here, I will use the IP address **10.6.6.23** for scanning.
3. You can use any domain name after taking the required permission for penetration testing.



New Scan

Scan Name: Internal

Scan Target: 10.6.6.23

Your scan target may be one of the following. SpiderFoot will automatically detect the target type based on the format of your input:

Domain Name: e.g. *example.com*
IPv4 Address: e.g. *1.2.3.4*
IPv6 Address: e.g. *2606:4700:4700::1111*
Hostname/Sub-domain: e.g. *abc.example.com*
Subnet: e.g. *1.2.3.0/24*
Bitcoin Address: e.g. 1HesYJSP1QqcyPEjnQ9vzBL1wujruNGe7R
E-mail address: e.g. *bob@example.com*
Phone Number: e.g. *+12345678901* (E.164 format)
Human Name: e.g. *"John Smith"* (must be in quotes)
Username: e.g. *"jsmith2000"* (must be in quotes)
Network ASN: e.g. *1234*

● All — **Get anything and everything about the target.**

All SpiderFoot modules will be enabled (slow) but every possible piece of information about the target will be obtained and analysed.

○ Footprint — **Understand what information this target exposes to the Internet.**

Gain an understanding about the target's network perimeter, associated identities and other information that is obtained through a lot of web crawling and search engine use.

○ Investigate — **Best for when you suspect the target to be malicious but need more information.**

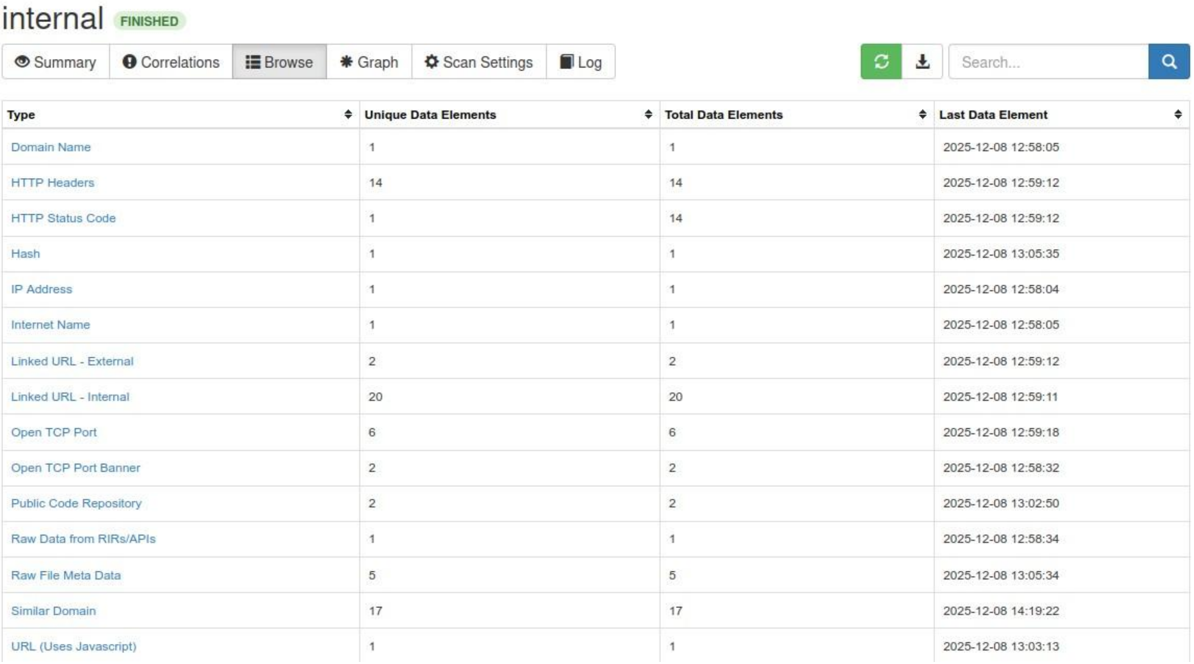
Some basic footprinting will be performed in addition to querying of blacklists and other sources that may have information about your target's maliciousness.

○ Passive — **When you don't want the target to even suspect they are being investigated.**

As much information will be gathered without touching the target or their affiliates, therefore only modules that do not touch the target will be enabled.

Step 4: Investigate Scan Results

1. Go back to the scan results by clicking the Scans tab.
2. You will see a table with the currently running scan and any previous scans displayed.
3. Click on the link and get the scan report.



internal FINISHED

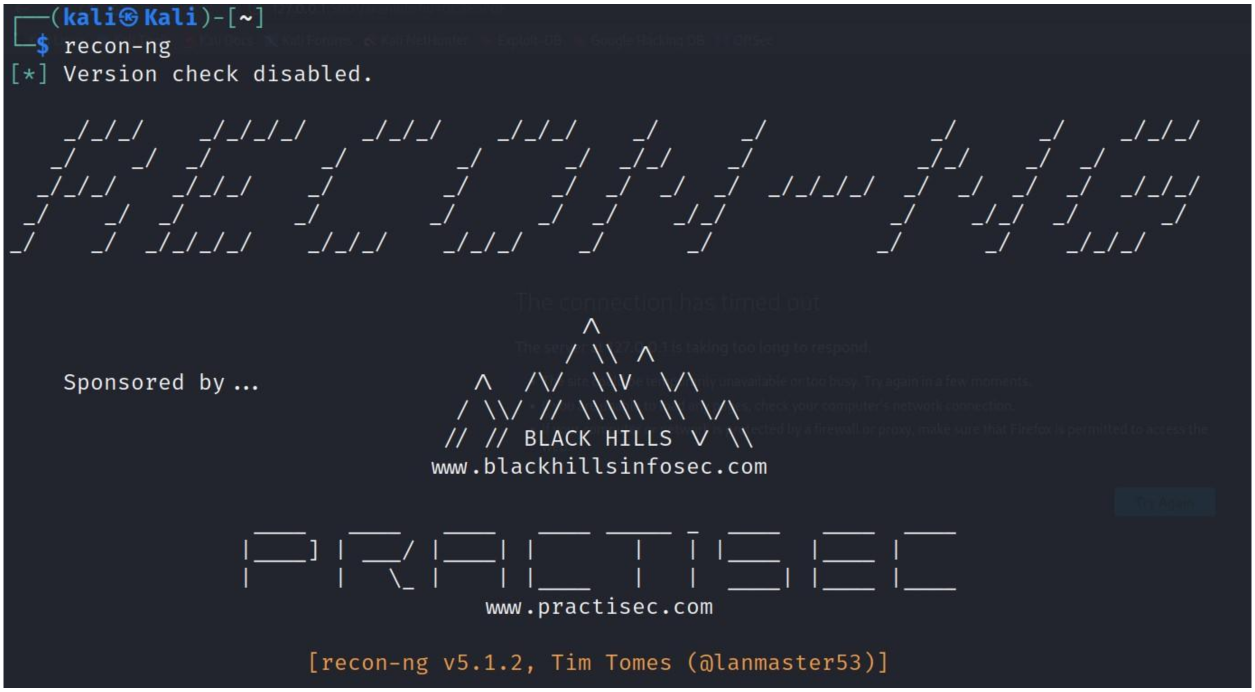
Type	Unique Data Elements	Total Data Elements	Last Data Element
Domain Name	1	1	2025-12-08 12:58:05
HTTP Headers	14	14	2025-12-08 12:59:12
HTTP Status Code	1	14	2025-12-08 12:59:12
Hash	1	1	2025-12-08 13:05:35
IP Address	1	1	2025-12-08 12:58:04
Internet Name	1	1	2025-12-08 12:58:05
Linked URL - External	2	2	2025-12-08 12:59:12
Linked URL - Internal	20	20	2025-12-08 12:59:11
Open TCP Port	6	6	2025-12-08 12:59:18
Open TCP Port Banner	2	2	2025-12-08 12:58:32
Public Code Repository	2	2	2025-12-08 13:02:50
Raw Data from RIRs/APIs	1	1	2025-12-08 12:58:34
Raw File Meta Data	5	5	2025-12-08 13:05:34
Similar Domain	17	17	2025-12-08 14:19:22
URL (Uses Javascript)	1	1	2025-12-08 13:03:13

Part 3: Investigate Recon-ng

Recon-ng is an OSINT framework that is similar to the Metasploit exploitation framework or the Social-Engineering Toolkit (SET). It consists of a series of modules that can be run in their own workspaces. The modules can be configured to run with option settings that are specific to the module. Recon-ng is used to perform a wide range of reconnaissance activities in different settings. Some modules are available with the Kali installation, and others are available for download and installation in the Recon-ng modules marketplace.

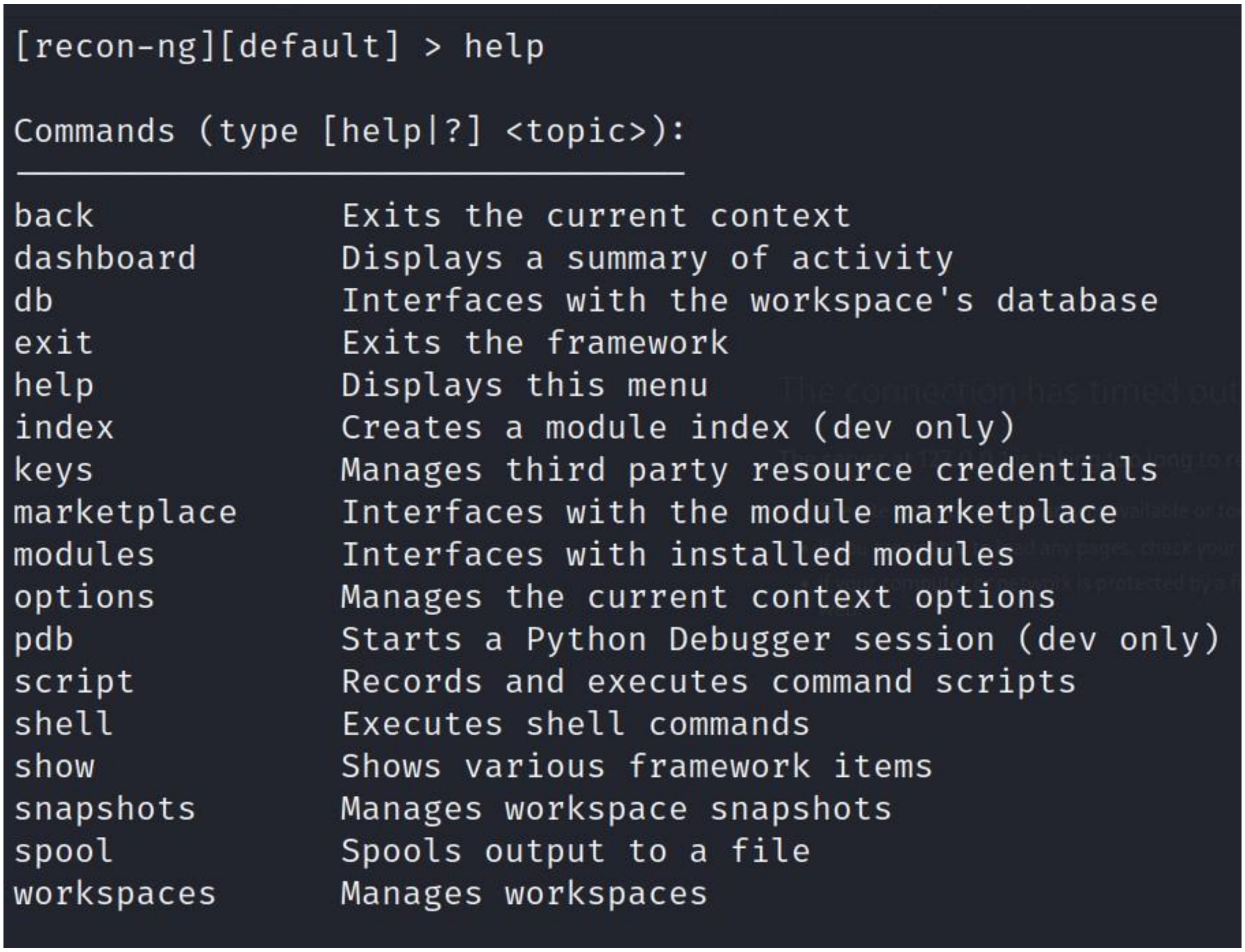
Step 1: Create a workspace.

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



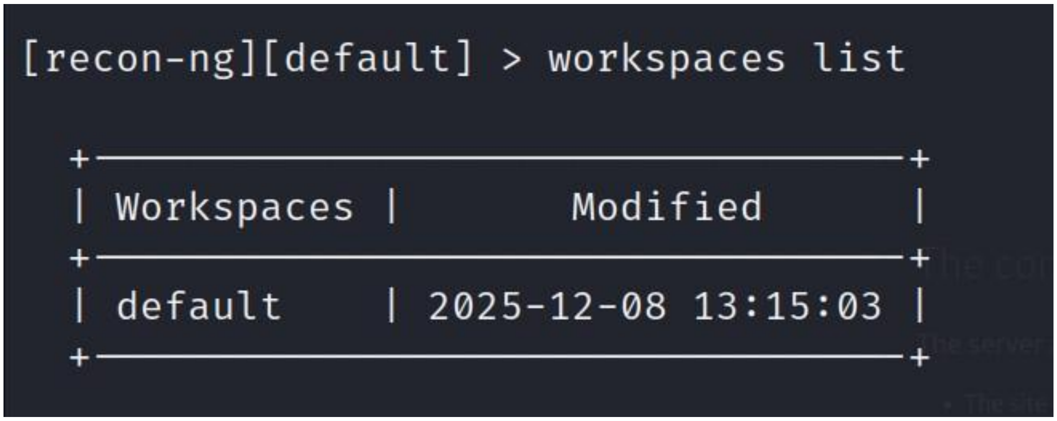
```
┌──(kali㉿Kali)-[~]
└─$ recon-ng
[*] Version check disabled.

    Sponsored by ...
                                   // // BLACK HILLS \/ \\
                                 www.blackhillsinfosec.com

                                    www.practisec.com

                      [recon-ng v5.1.2, Tim Tomes (@lanmaster53)]
```

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 available commands.



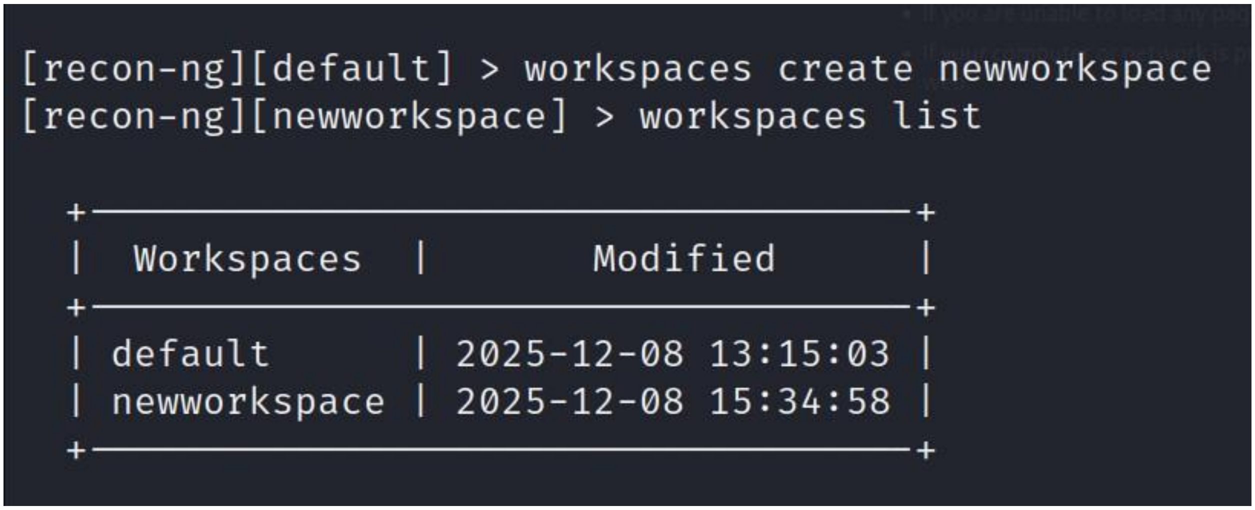
```
[recon-ng][default] > help

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
```

3. Enter the workspaces list command to display the list of workspaces.



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

  +------------------------------------+
  | Workspaces |       Modified        |
  +------------------------------------+
  | default    | 2025-12-08 13:15:03 |
  +------------------------------------+
```

4. Enter the workspace create command to create a new workspace.



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

  +--------------------------------------+
  |  Workspaces  |        Modified       |
  +--------------------------------------+
  | default      | 2025-12-08 13:15:03 |
  | newworkspace | 2025-12-08 15:34:58 |
  +--------------------------------------+
```

5. Enter the workspaces remove command to remove the workspace.

   ```
   workspaces remove [workspace_name]
   ```

6. Use the back command to exit the workspace and return to the main Recon-ng prompt.

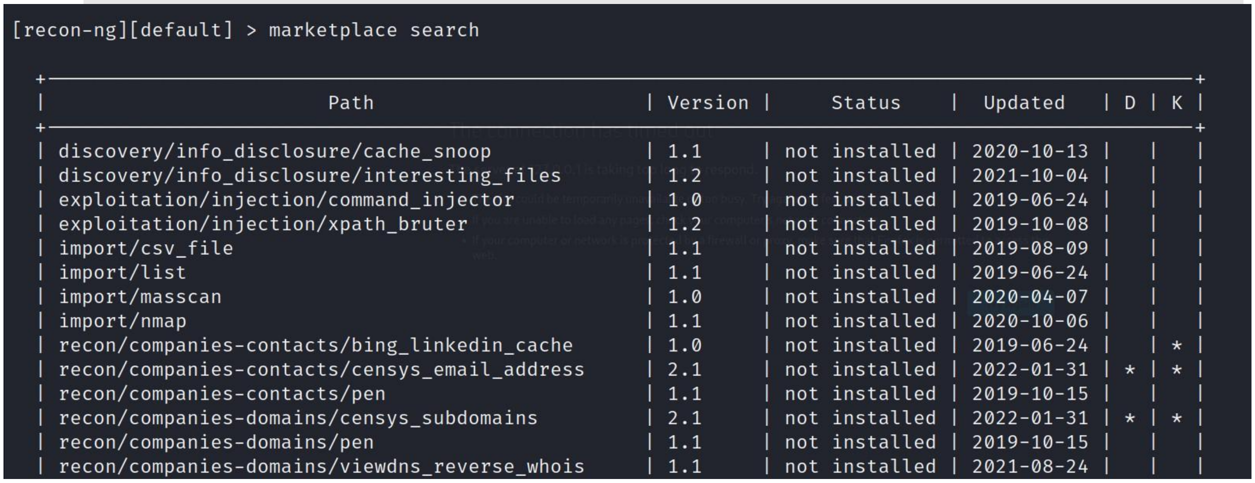
Step 2: Investigate modules.

1. Enter the **modules search** command to display the currently installed modules.

Step 3: Investigate the module marketplace.

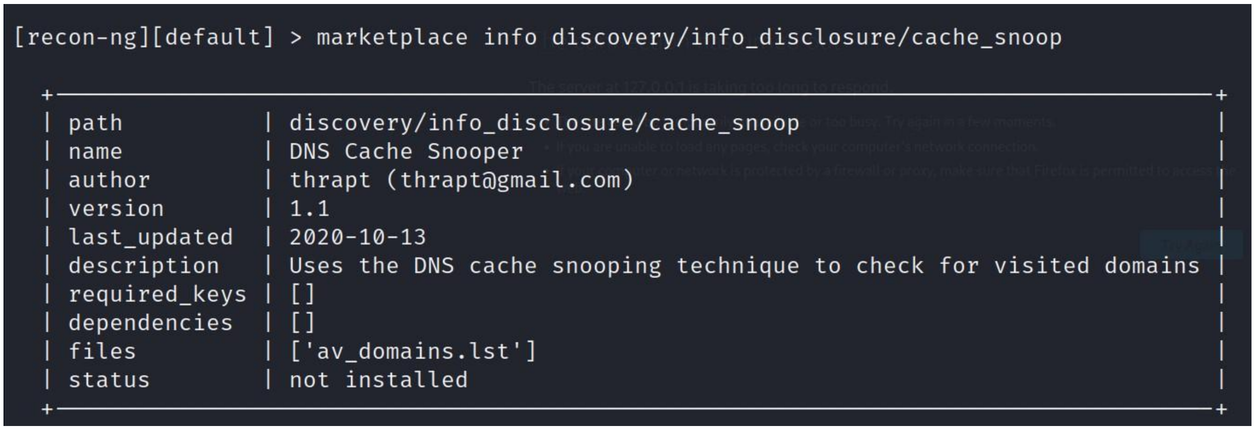
1. Use the search option to list all the modules that are currently available.

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



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

  +---------------------------------------------------------------------------------------------------------+
  |                         Path                          | Version |     Status    |  Updated   | D | K |
  +---------------------------------------------------------------------------------------------------------+
  | discovery/info_disclosure/cache_snoop                 | 1.1     | not installed | 2020-10-13 |   |   |
  | discovery/info_disclosure/interesting_files           | 1.2     | not installed | 2021-10-04 |   |   |
  | exploitation/injection/command_injector               | 1.0     | not installed | 2019-06-24 |   |   |
  | exploitation/injection/xpath_bruter                   | 1.2     | not installed | 2019-10-08 |   |   |
  | import/csv_file                                       | 1.1     | not installed | 2019-08-09 |   |   |
  | import/list                                           | 1.1     | not installed | 2019-06-24 |   |   |
  | import/masscan                                        | 1.0     | not installed | 2020-04-07 |   |   |
  | import/nmap                                           | 1.1     | not installed | 2020-10-06 |   |   |
  | recon/companies-contacts/bing_linkedin_cache          | 1.0     | not installed | 2019-06-24 |   | * |
  | recon/companies-contacts/censys_email_address         | 2.1     | not installed | 2022-01-31 | * | * |
  | recon/companies-contacts/pen                          | 1.1     | not installed | 2019-10-15 |   |   |
  | recon/companies-domains/censys_subdomains             | 2.1     | not installed | 2022-01-31 | * | * |
  | recon/companies-domains/pen                           | 1.1     | not installed | 2019-10-15 |   |   |
  | recon/companies-domains/viewdns_reverse_whois         | 1.1     | not installed | 2021-08-24 |   |   |
```

2. To learn more about individual modules, use the **marketplace info** command followed by the full name of the module.

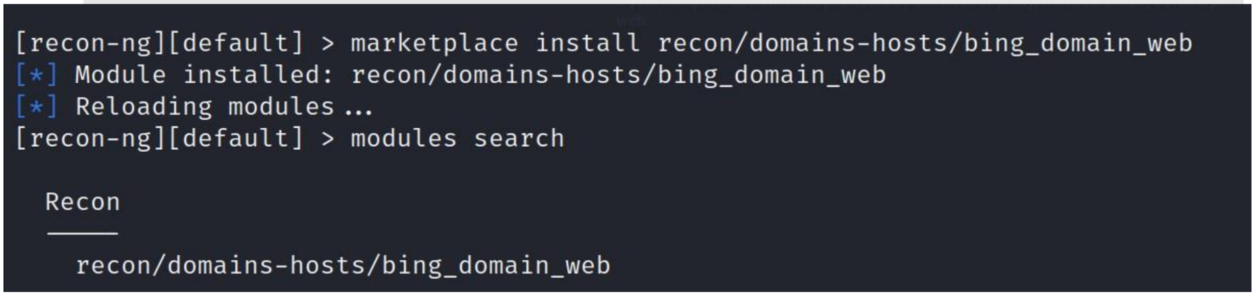


```
[recon-ng][default] > marketplace info discovery/info_disclosure/cache_snoop

  +--------------------------------------------------------------------------------------+
  | path          | discovery/info_disclosure/cache_snoop                                |
  | name          | DNS Cache Snooper                                                    |
  | author        | thrapt (thrapt@gmail.com)                                            |
  | version       | 1.1                                                                  |
  | last_updated  | 2020-10-13                                                           |
  | description   | Uses the DNS cache snooping technique to check for visited domains |
  | required_keys | []                                                                   |
  | dependencies  | []                                                                   |
  | files         | ['av_domains.lst']                                                   |
  | status        | not installed                                                        |
  +--------------------------------------------------------------------------------------+
```

Step 4: Install a new module.

1. Search the marketplace modules using Bing as a search term
2. View information for this module.
3. To install the module, copy the full name, including the path, to the clipboard.
4. Enter the marketplace install command followed by the full name of the module.

```
[recon-ng][default] > marketplace install recon/domains-hosts/bing_domain_web
```

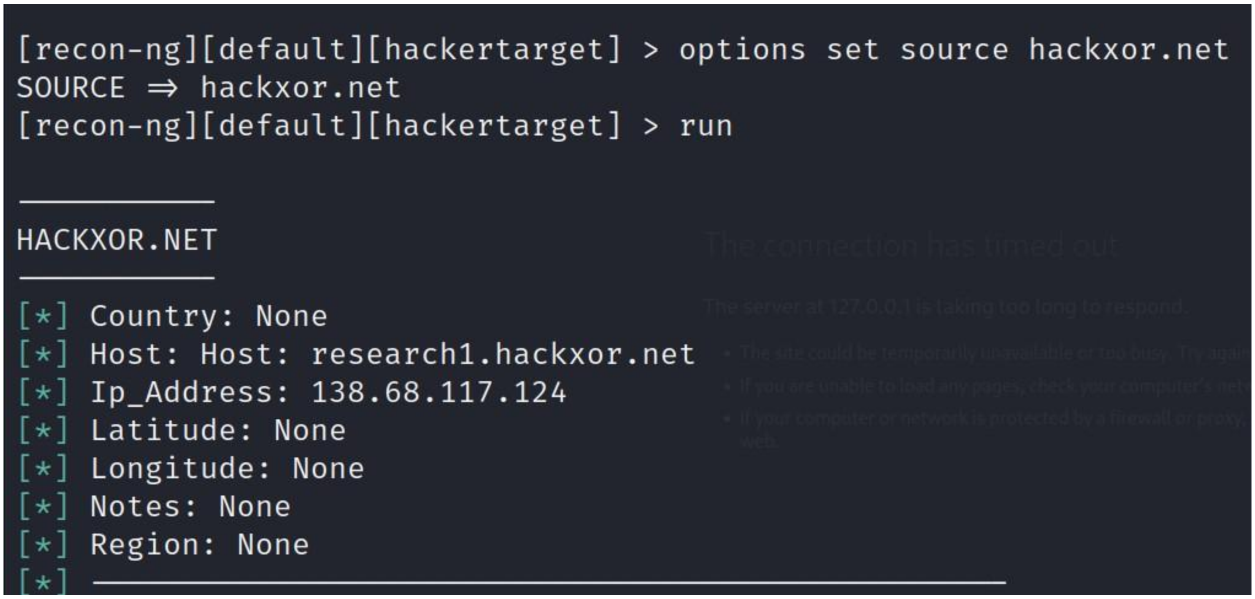


```
[recon-ng][default] > marketplace install recon/domains-hosts/bing_domain_web
[*] Module installed: recon/domains-hosts/bing_domain_web
[*] Reloading modules ...
[recon-ng][default] > modules search

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

5. After installation, enter the **modules search** command to verify that the new module is now available.
6. Repeat the process to install the **hackertarget** module.

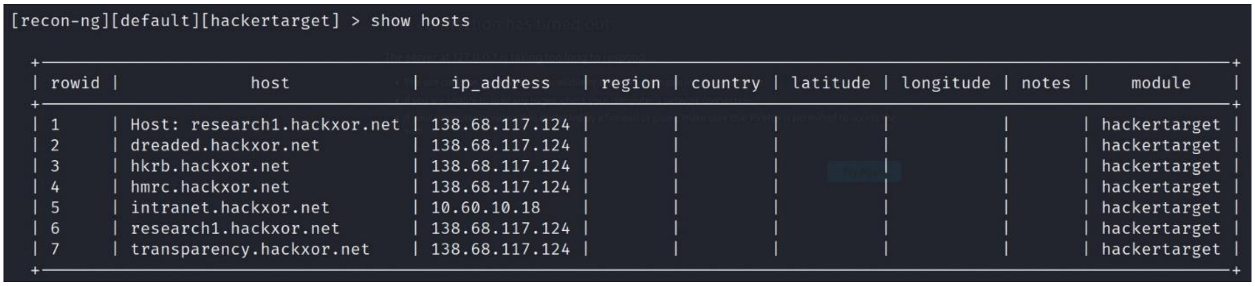
Step 5: Run the new modules

1. Enter the **modules load hackertarget** command to begin working with the module.
2. Use the **options set source** command to set the option by specifying the target as **hackxor.net**.
3. Type **run** to execute the module.



```
[recon-ng][default][hackertarget] > options set source hackxor.net
SOURCE ⇒ hackxor.net
[recon-ng][default][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
[*] ──────────────────────────────────────────────────
```

4. Enter the **dashboard** command to get a summary of the information gathered.
5. Enter the **show hosts** command to display the list of hosts that were discovered.

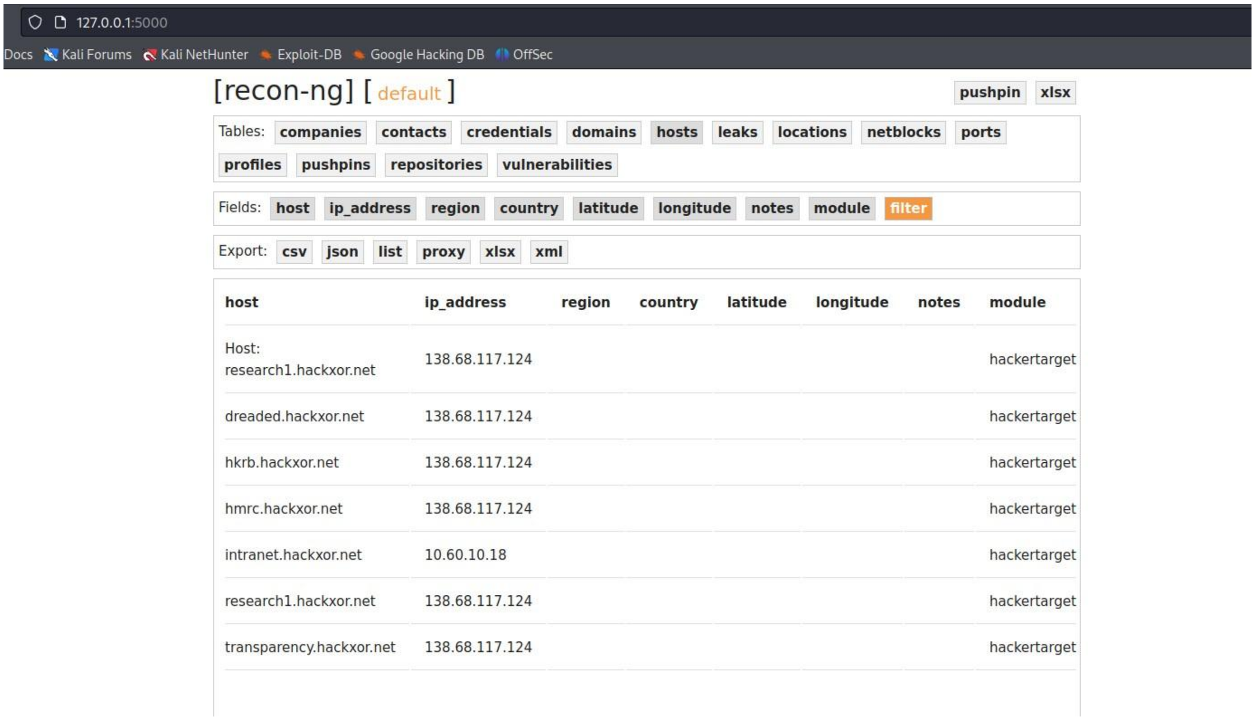


```
[recon-ng][default][hackertarget] > show hosts

  +---------------------------------------------------------------------------------------------------------------------+
  | 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 |
  +---------------------------------------------------------------------------------------------------------------------+
```

6. Repeat the process with the bing module. Compare the results with the hackertarget module.

Step 6: Investigate the web interface.

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



127.0.0.1:5000
Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec

[recon-ng] [default]

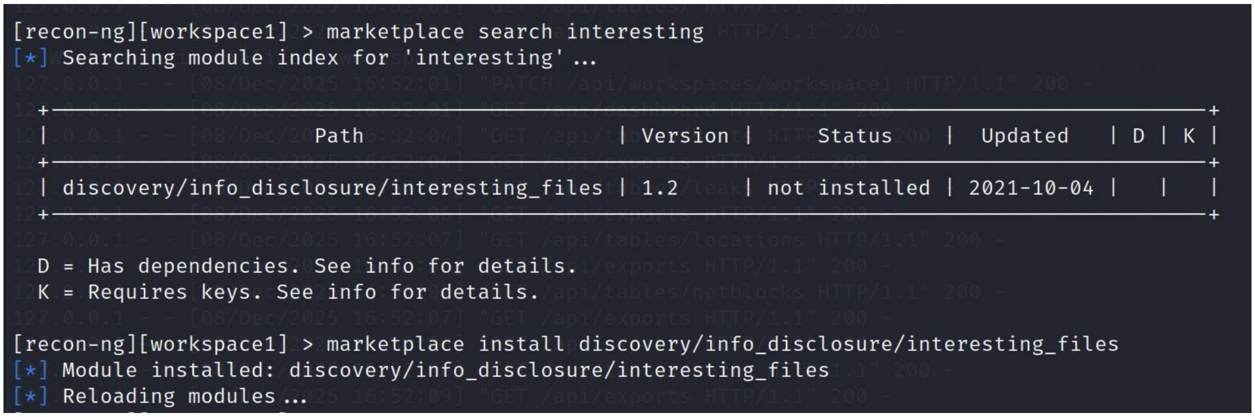
pushpin
xlsx
Tables: companies contacts credentials domains hosts leaks locations netblocks ports profiles pushpins repositories vulnerabilities
Fields: host ip_address region country latitude longitude notes module filter
Export: csv json list proxy xlsx xml

host	ip_address	region	country	latitude	longitude	notes	module
Host: research1.hackxor.net	138.68.117.124						hackertarget
dreaded.hackxor.net	138.68.117.124						hackertarget
hkrb.hackxor.net	138.68.117.124						hackertarget
hmrc.hackxor.net	138.68.117.124						hackertarget
intranet.hackxor.net	10.60.10.18						hackertarget
research1.hackxor.net	138.68.117.124						hackertarget
transparency.hackxor.net	138.68.117.124						hackertarget

5. 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

1. Search the marketplace for a module that will discover interesting files in a domain.
2. Install and load the plugin.



```
[recon-ng][workspace1] > marketplace search interesting
[*] Searching module index for 'interesting'...

  +--------------------------------------------------------------------------------------+
  |                   Path                    | Version |     Status    |  Updated   | D | K |
  +--------------------------------------------------------------------------------------+
  | discovery/info_disclosure/interesting_files | 1.2     | not installed | 2021-10-04 |   |   |
  +--------------------------------------------------------------------------------------+

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

[recon-ng][workspace1] > marketplace install discovery/info_disclosure/interesting_files
[*] Module installed: discovery/info_disclosure/interesting_files
[*] Reloading modules...
```

3. Set the source option and run the command as above.