



Department of  
**Bachelor of Computer Applications**

**Ethical Hacking Fundamentals**  
Lab File – CA 03

**Subject Code:** 19BCA4C02L  
**Class:** II<sup>nd</sup> Year II<sup>nd</sup> Semester

Prepared By:  
Suman Garai  
20BCAR0246

## Aim :

To explore and learn Recon-ng (an open-source intelligence tool) for reconnaissance.

## Requirements :

- Virtualisation Software
- Kali Linux 2021.4a
- Basics of Maltego
- Administrator privileges
- Internet Connection

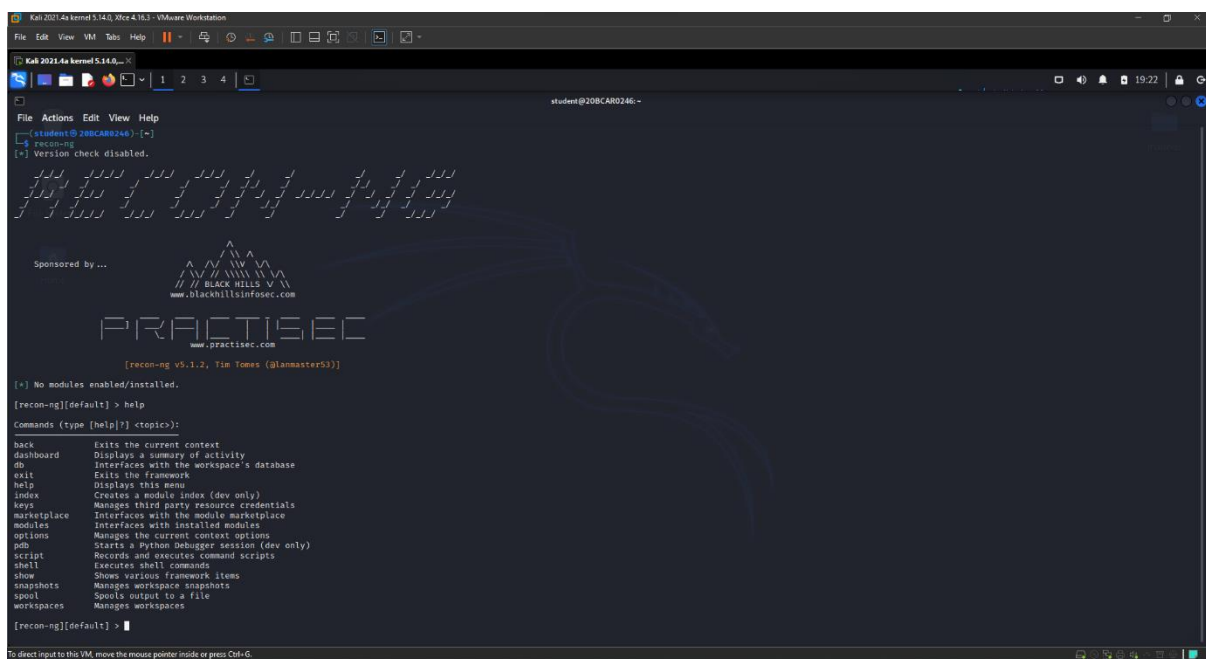
## Objectives :

To Install & Run any module any obtain desired information using it.

## Procedure :

### Basics

- 1> Open root terminal in kali linux, and run the command `recon-ng` to run recon-ng.
- 2> Type Help for getting the list of working commands in recon-ng.



```
Kali 2021.4a kernel 5.14.0, Xfce 4.16.3 - VMware Workstation
File Edit View VM Tabs Help
Kali 2021.4a kernel 5.14.0 - Xfce 4.16.3
student@208CAR0246:~$ recon-ng
[recon-ng] Version check disabled.

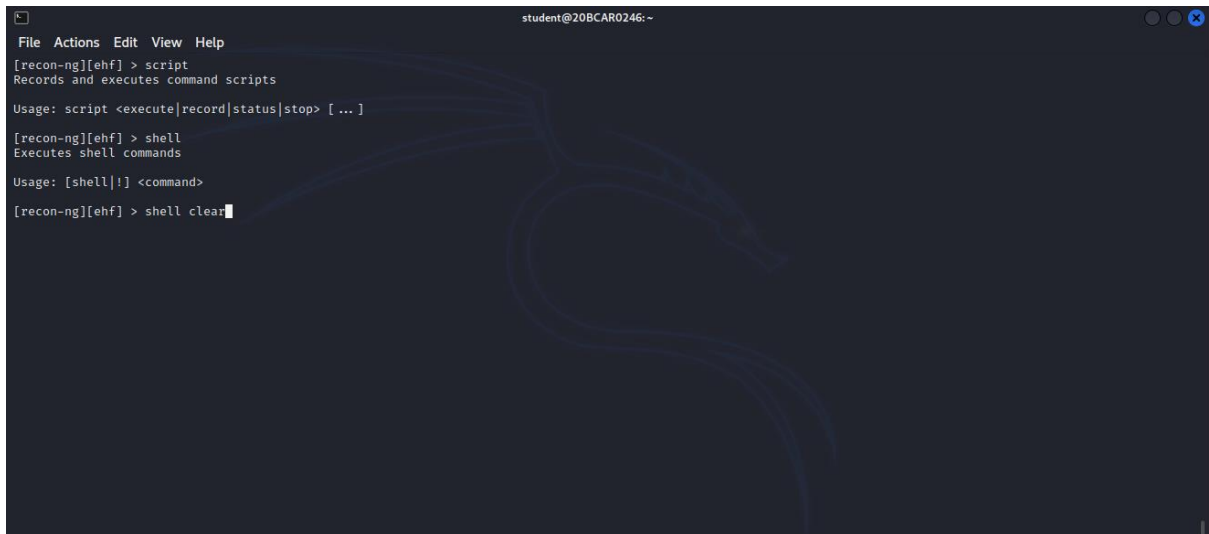
Sponsored by ...
www.blackhillsinfosec.com

PRACTISESEC
www.practisesec.com

[recon-ng v5.1.2, Tim Tomes (@lanmaster53)]
[recon-ng] No modules enabled/installed.
[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] >
```

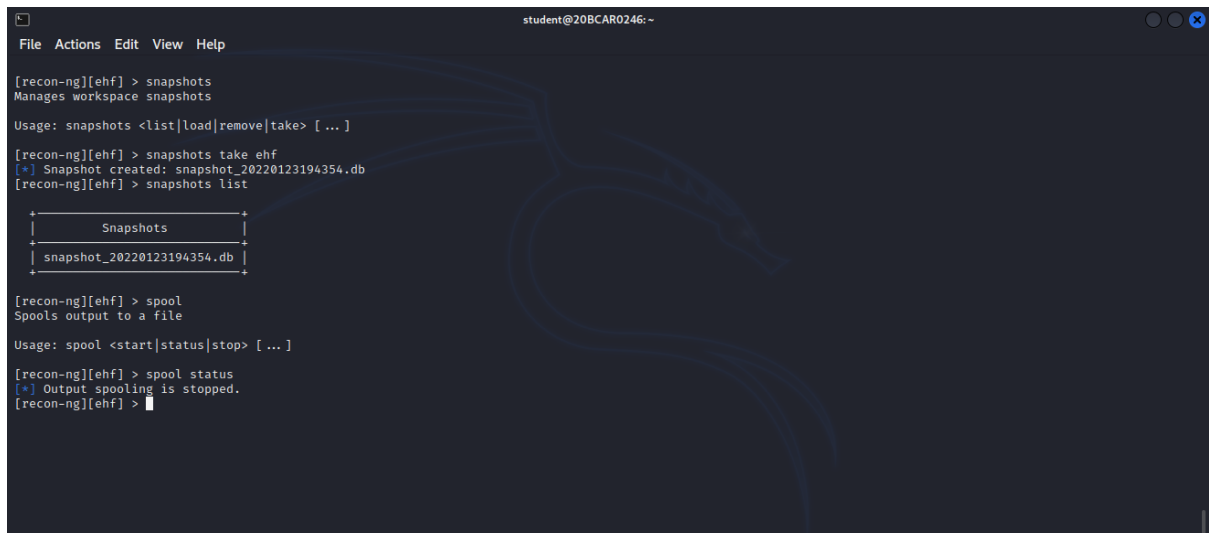
As we can see, a lot of options are present here. We are going to discuss a few of those as we proceed.

Following are the working/ output of shell, script, snapshot and spool commands in the tool.

A screenshot of a terminal window titled 'student@20BCAR0246: ~'. The terminal shows the output of the 'script' and 'shell' commands. The 'script' command is used to record and execute command scripts, with usage instructions: 'script <execute|record|status|stop> [ ... ]'. The 'shell' command is used to execute shell commands, with usage instructions: 'shell [!] <command>'. The terminal also shows the 'script clear' command being executed.

```
student@20BCAR0246: ~
File Actions Edit View Help
[recon-ng][ehf] > script
Records and executes command scripts
Usage: script <execute|record|status|stop> [ ... ]
[recon-ng][ehf] > shell
Executes shell commands
Usage: [shell|!] <command>
[recon-ng][ehf] > shell clear
```

Figure: shell & script commands

A screenshot of a terminal window titled 'student@20BCAR0246: ~'. The terminal shows the output of the 'snapshots' and 'spool' commands. The 'snapshots' command is used to manage workspace snapshots, with usage instructions: 'snapshots <list|load|remove|take> [ ... ]'. The 'spool' command is used to spool output to a file, with usage instructions: 'spool <start|status|stop> [ ... ]'. The terminal also shows the 'snapshots take ehf' command being executed, which creates a snapshot named 'snapshot\_20220123194354.db'. The 'snapshots list' command is also executed, showing a list of snapshots. The 'spool status' command is executed, showing that output spooling is stopped.

```
student@20BCAR0246: ~
File Actions Edit View Help
[recon-ng][ehf] > snapshots
Manages workspace snapshots
Usage: snapshots <list|load|remove|take> [ ... ]
[recon-ng][ehf] > snapshots take ehf
[*] Snapshot created: snapshot_20220123194354.db
[recon-ng][ehf] > snapshots list
+-----+
| Snapshots |
+-----+
| snapshot_20220123194354.db |
+-----+
[recon-ng][ehf] > spool
Spools output to a file
Usage: spool <start|status|stop> [ ... ]
[recon-ng][ehf] > spool status
[*] Output spooling is stopped.
[recon-ng][ehf] >
```

Figure: snapshot & spool

## To change NAMESERVER

- 1> While in recon-ng default workspace, without activating any module, type `options list`. We see the existing nameserver.
- 2> To change, type `options unset` and enter, to clear the existing one.
- 3> Then again type, `options set NAMESERVER <DNS>` and press enter.  
The change is displayed as follows.

```
student@20BCAR0246: ~
File Actions Edit View Help
Usage: options <list|set|unset> [ ... ]
[recon-ng][ehf] > options list

Name      Current Value  Required  Description
-----
NAMESERVER 8.8.8.8        yes       default nameserver for the resolver mixin
PROXY      no              no        proxy server (address:port)
THREADS    10             yes       number of threads (where applicable)
TIMEOUT    10             yes       socket timeout (seconds)
USER-AGENT Recon-ng/v5 yes       user-agent string
VERBOSITY  1              yes       verbosity level (0 = minimal, 1 = verbose, 2 = debug)

[recon-ng][ehf] > options unset NAMESERVER
NAMESERVER => None
[recon-ng][ehf] > options set NAMESERVER 1.1.1.1
NAMESERVER => 1.1.1.1
[recon-ng][ehf] > options list

Name      Current Value  Required  Description
-----
NAMESERVER 1.1.1.1        yes       default nameserver for the resolver mixin
PROXY      no              no        proxy server (address:port)
THREADS    10             yes       number of threads (where applicable)
TIMEOUT    10             yes       socket timeout (seconds)
USER-AGENT Recon-ng/v5 yes       user-agent string
VERBOSITY  1              yes       verbosity level (0 = minimal, 1 = verbose, 2 = debug)

[recon-ng][ehf] > █
```

As we can see, the name server is changed and set, also crosschecked.

## Working with Workspaces

- 1> To create a workspace, type `workspaces create <name>`. After it gets created, we automatically enter into the workspace, as is displayed as follows:

```
student@20BCAR0246: ~
File Actions Edit View Help
[recon-ng][default] > workspaces
Manages workspaces

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

[recon-ng][default] > workspaces create ehf
[recon-ng][ehf] > 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 settings
snapshots Manages workspace snapshots
spool     Spools output to a file
workspaces Manages workspaces

[recon-ng][ehf] > █
```

As we can see, we have entered the workspace.

## Knowing the Marketplace

- 1> While in recon-ng newly created workspace, without activating any module, type `marketplace search`. A list of modules available to install appears, displayed as follows:

```
Kali 2021.4a kernel 5.14.0, Mize 4.16.3 - VMware Workstation
File Edit View VM Tabs Help

Kali 2021.4a kernel 5.14.0
1 2 3 4 5

student@20BCAR0246:~
[recon-ng][ehf] > marketplace info
Shows detailed information about available modules
Usage: marketplace info <path>[<prefix>][all]
[recon-ng][ehf] > 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/xxpath_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/map	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	2.0	not installed	2021-05-11	*	
recon/companies-contacts/pen	1.1	not installed	2019-10-15	*	
recon/companies-domains/censys_subdomains	2.0	not installed	2021-05-10	*	
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-domains/whoxy_dns	1.1	not installed	2020-06-17	*	
recon/companies-hosts/censys_org	2.0	not installed	2021-05-11	*	
recon/companies-hosts/censys_tls_subjects	2.0	not installed	2021-05-11	*	
recon/companies-multi/github_miner	1.1	not installed	2020-05-15	*	
recon/companies-multi/shodan_org	1.1	not installed	2020-07-01	*	
recon/companies-multi/whois_miner	1.1	not installed	2019-10-15	*	
recon/contacts-contacts/abc	1.0	not installed	2019-10-11	*	
recon/contacts-contacts/mailtester	1.0	not installed	2019-06-24	*	
recon/contacts-contacts/mangle	1.0	not installed	2019-06-24	*	
recon/contacts-contacts/mangle	1.1	not installed	2019-10-27	*	
recon/contacts-credentials/hibp_breach	1.2	not installed	2019-09-18	*	
recon/contacts-credentials/hibp_paste	1.1	not installed	2019-09-18	*	
recon/contacts-domains/extract_contacts	1.1	not installed	2020-05-17	*	
recon/contacts-profiles/fullcontact	1.1	not installed	2019-07-24	*	
recon/credentials-credentials/adobe	1.0	not installed	2019-06-24	*	
recon/credentials-credentials/borocrack	1.0	not installed	2019-06-24	*	
recon/credentials-credentials/hasheer.org	1.0	not installed	2019-06-24	*	
recon/domains-companies/censys_companies	2.0	not installed	2021-05-10	*	
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_ip	1.1	not installed	2020-04-19	*	
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/ppp_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	*	

To direct input to this VM, move the mouse pointer inside or press Ctrl-G.

- 2> Type `marketplace install <module path wanted to install>` and hit enter, say, `recon/domains-contacts/wikileaker`.

```
student@20BCAR0246:~
File Actions Edit View Help

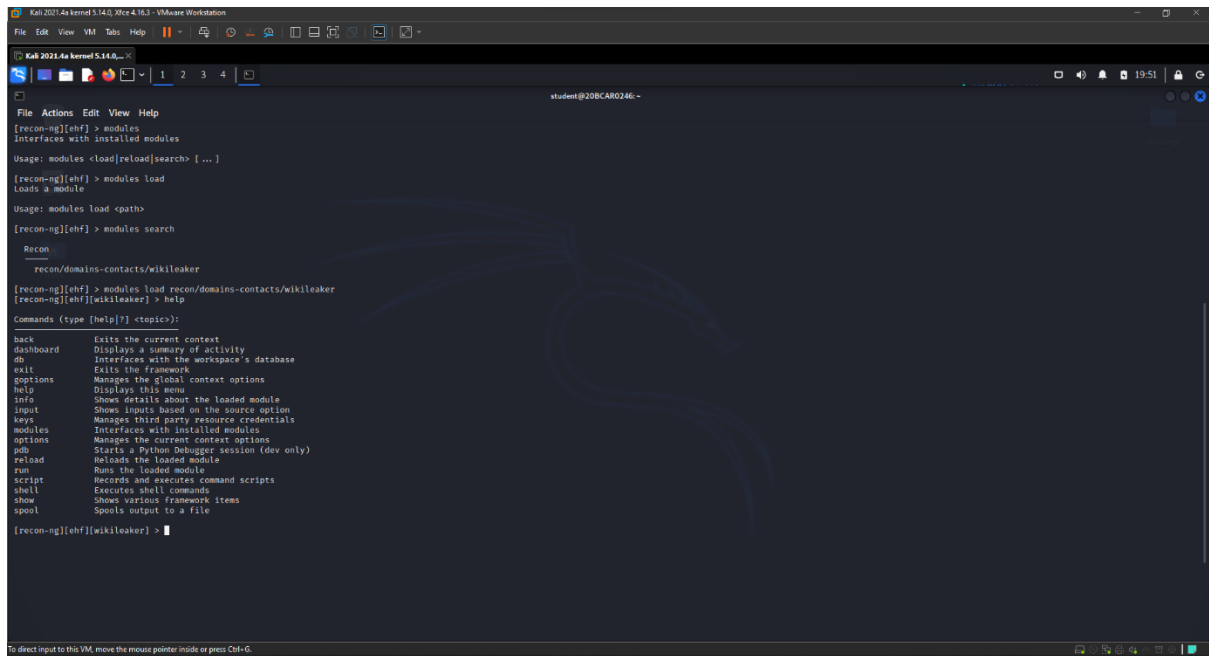
recon/ports-hosts/ssl_scan 1.1 not installed 2021-08-24 *
recon/profiles-contacts/bing_linkedin_contacts 1.2 not installed 2021-08-24 *
recon/profiles-contacts/dev_diver 1.1 not installed 2020-05-15 *
recon/profiles-contacts/github_users 1.0 not installed 2019-06-24 *
recon/profiles-profiles/namechk 1.0 not installed 2019-06-24 *
recon/profiles-profiles/profiler 1.0 not installed 2019-06-24 *
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][ehf] > marketplace install recon/domains-contacts/wikileaker
[*] Module installed: recon/domains-contacts/wikileaker
[*] Reloading modules ...
[recon-ng][ehf] >
```

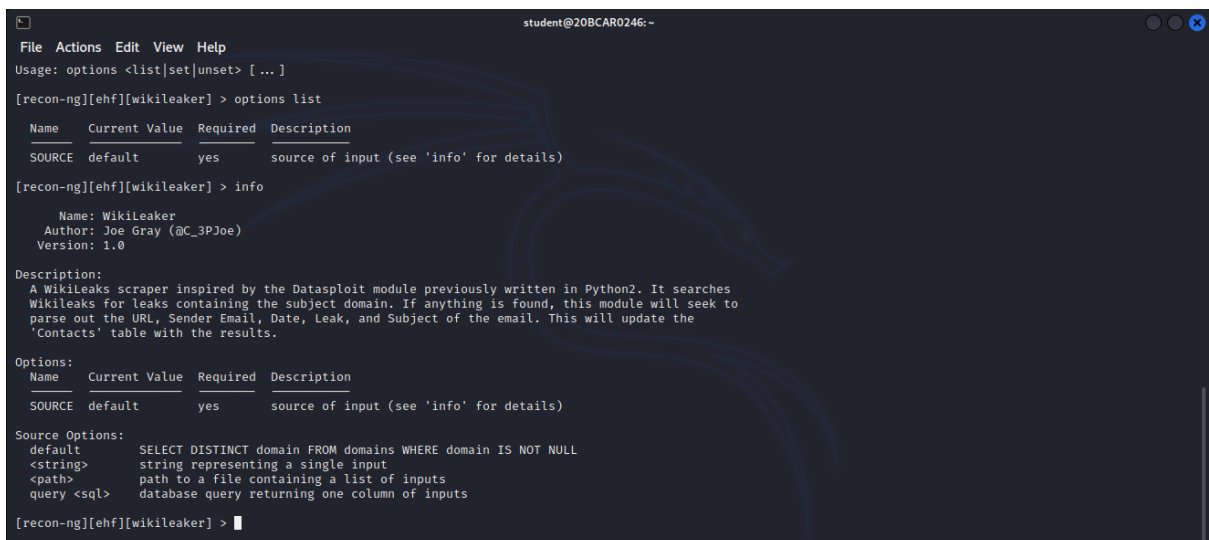
## Using the Modules

- 1> While in recon-ng newly created workspace, without activating any module, type `modules search`. A list of installed modules appears.
- 2> Type `modules load <name of the module to work with>` say, `recon/domains-contacts/wikileaker`. It should appear somewhat as follows:



```
Kali 2021.4a kernel 5.14.0_51ce 4.16.3 - VMware Workstation
File Edit View VM Tabs Help
Kali 2021.4a kernel 5.14.0_51ce 4.16.3
student@20BCAR0246:~$
[recon-ng][ehf] > modules
Interfaces with installed modules
Usage: modules <load|reload|search> [...]
[recon-ng][ehf] > modules load
Loads a module
Usage: modules load <path>
[recon-ng][ehf] > modules search
Recon
recon/domains-contacts/wikileaker
[recon-ng][ehf] > modules load recon/domains-contacts/wikileaker
[recon-ng][ehf][wikileaker] > 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
options Manage the global context options
help Displays this menu
info Shows details about the loaded module
input Shows inputs based on the source option
keys Manages third party resource credentials
modules Interfaces with installed modules
options Manage the current context options
pdb Starts a Python Debugger session (dev only)
reload Reloads the loaded module
run Runs the loaded module
script Records and executes command scripts
shell Executes shell commands
show Shows various framework items
spool Spools output to a file
[recon-ng][ehf][wikileaker] >
```

- 3> To know about the module, `info` can be used as follows:



```
student@20BCAR0246:~$
File Actions Edit View Help
Usage: options <list|set|unset> [...]
[recon-ng][ehf][wikileaker] > options list
Name Current Value Required Description
SOURCE default yes source of input (see 'info' for details)
[recon-ng][ehf][wikileaker] > info
Name: Wikileaker
Author: Joe Gray (@C_3PJoe)
Version: 1.0
Description:
A Wikileaks scraper inspired by the Datasplloit module previously written in Python2. It searches Wikileaks for leaks containing the subject domain. If anything is found, this module will seek to parse out the URL, Sender Email, Date, Leak, and Subject of the email. This will update the 'Contacts' 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][ehf][wikileaker] >
```



- The image is a screenshot of a Kali Linux desktop environment. In the foreground, a terminal window is open, displaying a series of commands and their outputs. The commands are related to setting environment variables, searching for 'bory' on WikiLeaks, and listing various framework items. The outputs show a large number of search results from WikiLeaks, including links to documents and a list of framework items. In the background, a web browser window is open, showing the WikiLeaks website. The search results for 'bory' are displayed, including a list of documents and a section for 'UPCOMING MARKETING ASSETS'. The browser also shows a sidebar with navigation links and a search bar.

## Summary of Events

```
student@20BCAR0246: ~
File Actions Edit View Help
[recon-ng][ehf][wikileaker] > dashboard

+-----+
| Activity Summary |
+-----+
| Module           | Runs |
+-----+
| recon/domains-contacts/wikileaker | 2    |
+-----+

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

[recon-ng][ehf][wikileaker] > exit

student@20BCAR0246: ~
$
```

7 | Page

## Conclusion :

Recon-ng is a powerful tool that can be further explored by looking through the list of modules. The help within the console is very clear and with a bit of playing around it won't take long to become an expert.

Once you start to become more familiar with the layout of the tool you will discover options such as workspaces that allow you to segment based on organization or network. The rise of bug bounties allows you to play with new tools and explore organizations internet-facing footprint. Have fun and don't break the rules.