Recon-Ng: A Full Tutorial From Noob To Pro [Updated 2024]

MOULIK / 12 SEPTEMBER 2021 / HACKING TOOLS, INFORMATION GATHERING / 2 COMMENTS

Table of Contents

Introduction

Hey, there guys, In this post, you will learn what is recon-ng and how to work with the tool from scratch and you should just follow the upcoming steps to become a pro in recon-ng. All the best my friend ????

Video

Information Gathering Using Recon ng | #recon-ng

What is recon-ng

Recon-ng is a reconnaissance tool and it is one of the powerful recon tools that exist in the modern world and I personally love this tool and do you, just comment down if you love it...

The tool has almost got every feature in it and simply we could say the tool is an all-rounder. The tool is in a command-line interface and the results can also be viewed in web format.

COOL is it

When I first worked with the tool, I said is it was a copy of Metasploit? Because the interface is much similar but not complicated as Metasploit.

Also Read: Installing custom kali is very easy

Who developed the tool ❓

The tool was written by this guy ????, His name is Tim Tomes and I should really thank him and the contributors to the tool. The author seems to be an introvert and here are his social links????????.

To download recon-ng just enter **sudo apt-get install recon-ng**

Github Download

Author's Youtube

What all the recon-ng can do

- Interactive Help
- Command Completion
- Database Interaction
- Shell Commands
- Spooling Activity
- Recording Commands
- Configuration Persistence
- Global Options
- Workspaces
- Module Marketplace
- Module Searching
- Smart Loading
- Database Snapshots
- Restricted Context
- Module Details
- Data Sources
- Third Party Modules
- Methodology Driven
- Automation
- Analysis and Reporting
- Analytics

Some use full commands in recon-ng

1. back: Exits the current context
2. dashboard: Displays a summary of activity
3. db: Interfaces with the workspace’s database
4. exit: Exits the framework
5. help: Displays this menu
6. index: Creates a module index (dev only)
7. keys: Manages third-party resource credentials
8. marketplace: Interfaces with the module marketplace
9. modules: Interfaces with installed modules
10. options: Manages the current context options

11. pdb: Starts a Python Debugger session (dev only)
12. script: Records and executes command scripts
13. shell: Executes shell commands
14. show: Shows various framework items
15. snapshots: Manages workspace snapshots
16. spool: Spools output to a file
17. workspaces: Manages workspaces

There are much more commands and if you want more familiarity just watch my youtube video on recon-ng and the video is at the top of the page.

How to use recon-ng

Follow the below steps and examples to become a noob to pro in the recon-ng tool and If you have any doubt just comment down below and I'm ready to help you...

Workspace

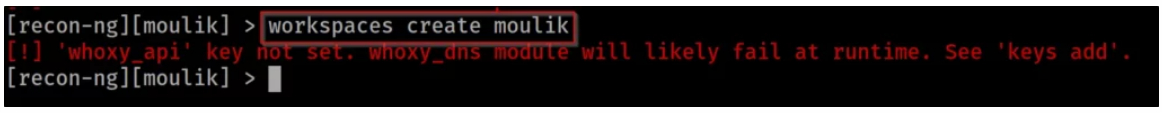
In this example let's see about workspaces. let's **create, list, load and remove** a workspace. Workspaces are where you can work on your project.

Example1:

Let's create a workspace, the command is

```
workspaces create moulik
```

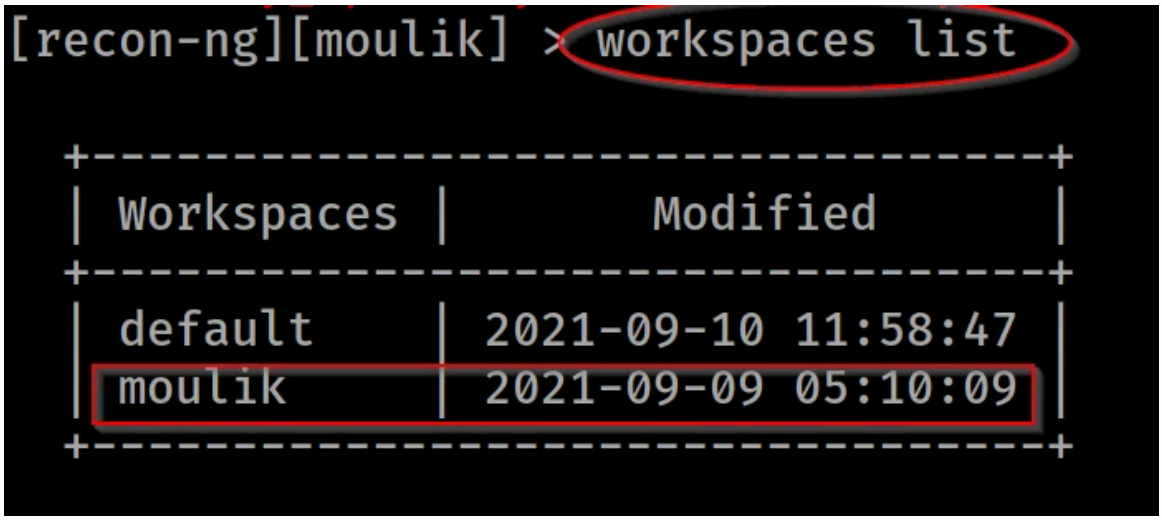
instead of moulik, you add you workspace



Example2:

Let's list the created workspaces, to list enter this command ????????

```
workspaces list
```



So here are the created workspaces and we listed them, by default there will be always a default workspace.

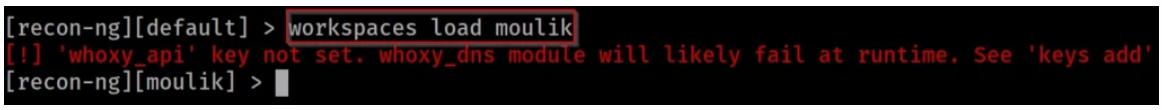
Example3:

Let's load the moulik workspace, to load any workspace enter ????????

```
workspaces load moulik
```

Instead of moulik add the workspaces name you wanna load

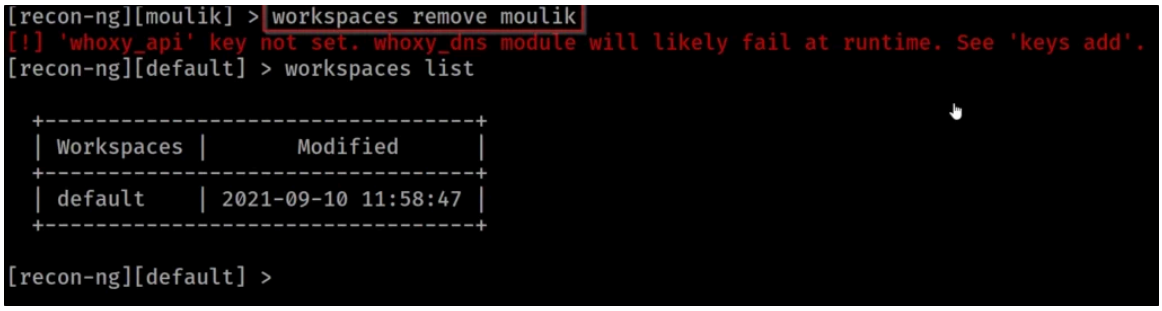
```
workspaces load moulik
```



Example4:

To remove workspaces just enter ????????

```
workspaces remove moulik
```



You see we have removed the moulik workspaces and to check we removed just do

```
workspaces list
```

Snapshots

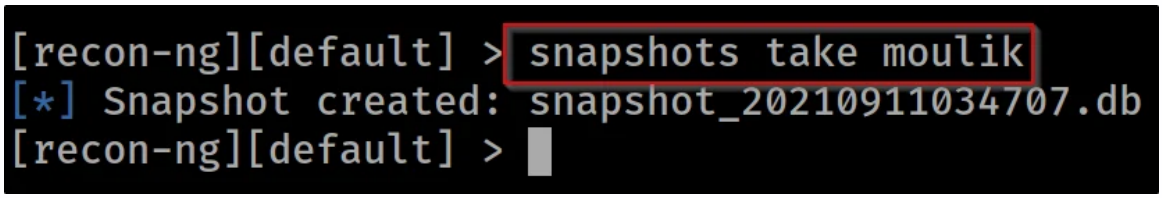
Let's do a snapshot. Snapshot is taking a snap of your work

Example1:

To do a snapshot enter this command ????????

```
snapshots take moulik
```

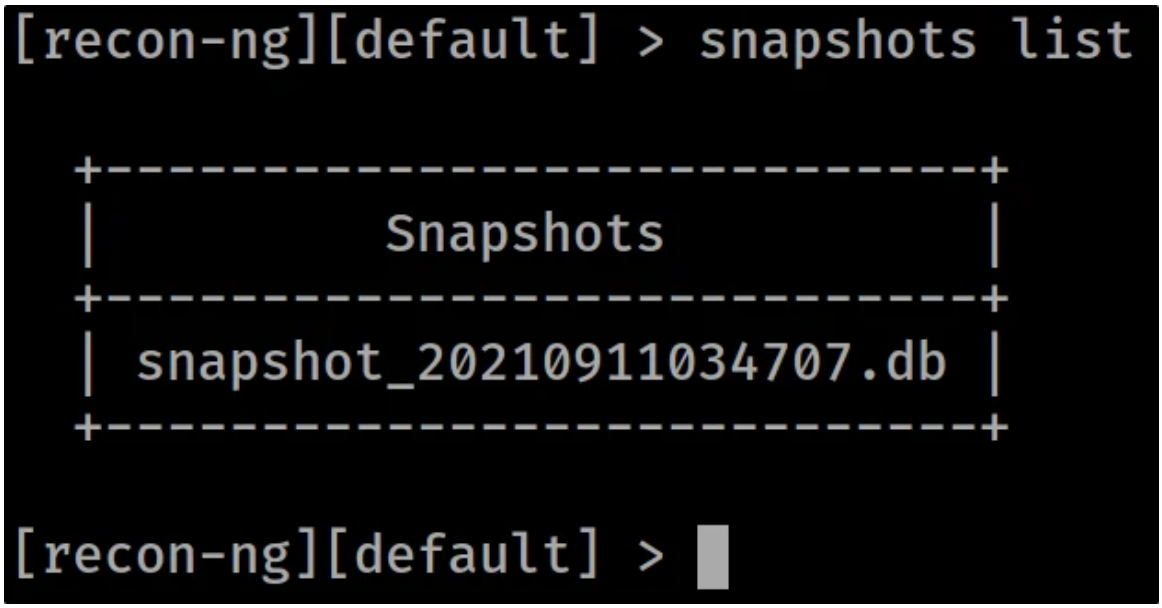
Instead of moulik keep the name you wish



Example2:

Let's list the snapshots

```
snapshots list
```



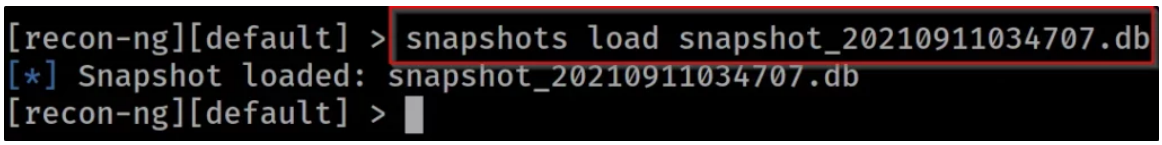
Example3:

Let's load the snapshot

To load snapshots do this command ????????

```
snapshots load snapshot_20210911034707.db
```

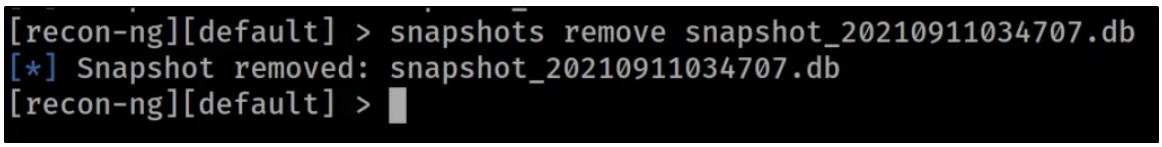
Instead of the snapshot enter the snapshot file you wanna enter



Example4:

To remove snapshots do this command

```
snapshots remove snapshot_20210911034707.db
```



Dashboards

To see a summary of your activity enter

Example1:

Here is the command to check for your work activity ????????

```
dashboard
```

Shell

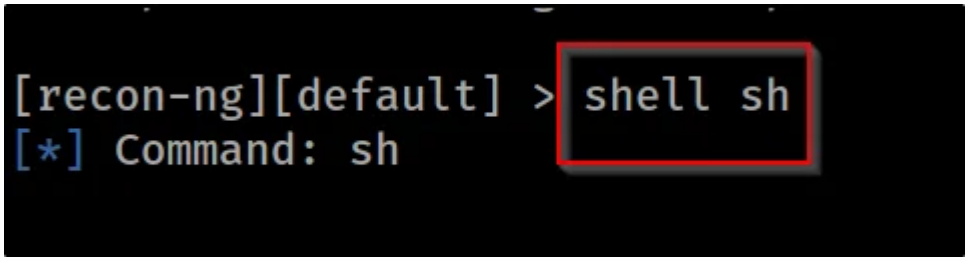
Executing a shell

Example1:

To execute a shell enter

```
shell sh
```

Instead of **sh,** you enter whatever shell you want Iam entering Bourne shell



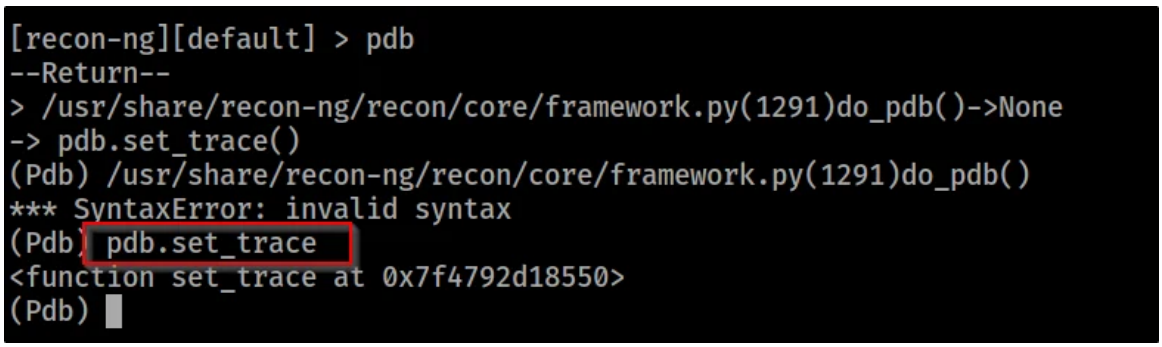
Pdb

pdb is a debugger

Example1:

To start a debugger just do this command

```
pdb.set_trace()
```



db

Interfaces with the workspace's database, Let's do a **schema, insert, delete, query, notes** etc...

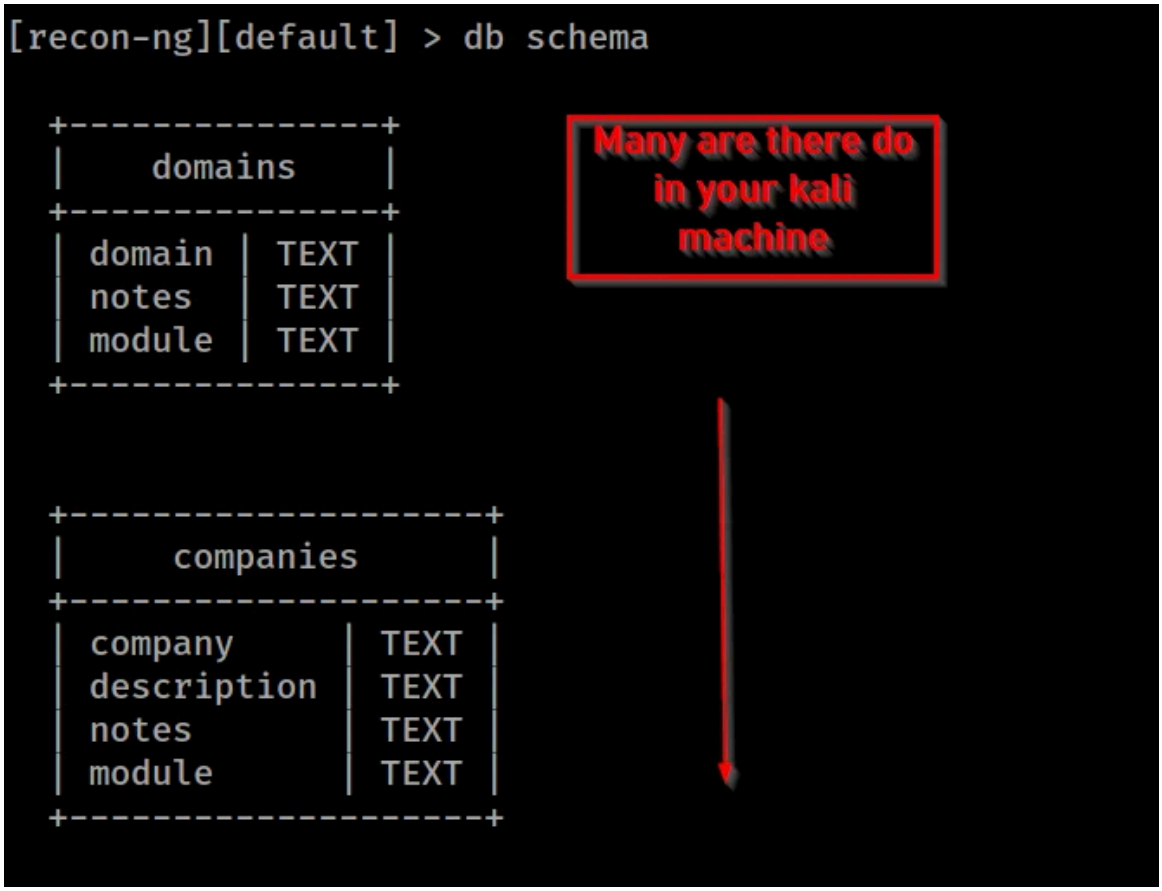
Example1:

Firstly let's enter ???????? to find the workspaces related database in a good box format

```
db schema
```

Once you do db schema you see all this information in box format

companies|contacts|credentials|domains|hosts|leaks|locations|netblocks|ports|profiles|pushpins|repositories|vulnerabilities



Example2:

Now let's add an insert port,

To insert something in db just enter

```
db insert ports
```

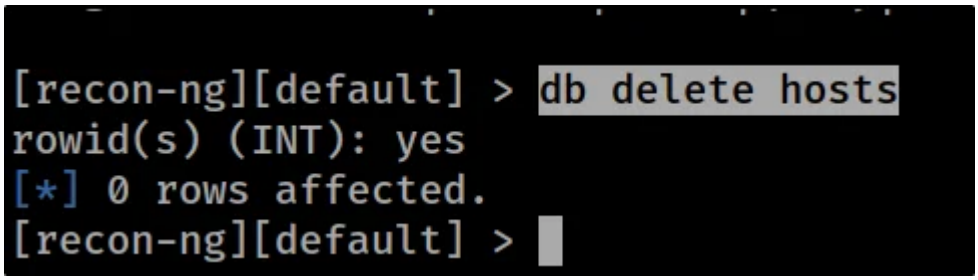
Instead of port you could enter whatever you want.

Example3:

To delete any rows enter

```
db delete hosts
```

Instead of host enter what you wanna delete and once you give this command it asks for the no of command in rows to delete like this ????????

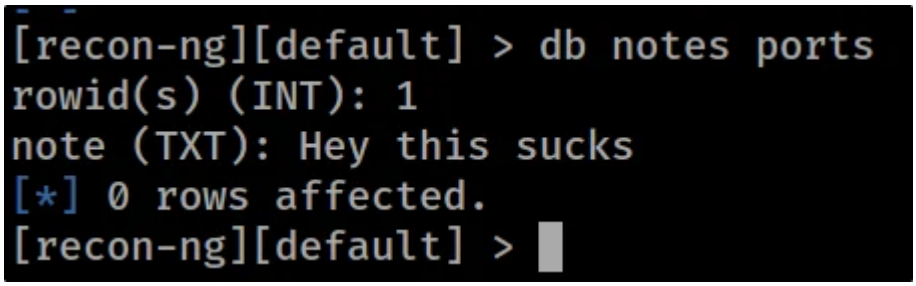


Example4:

Let's add notes in db

Do this ???????? specify the tables and then enter the rows and the enter the change

```
db notes ports
```



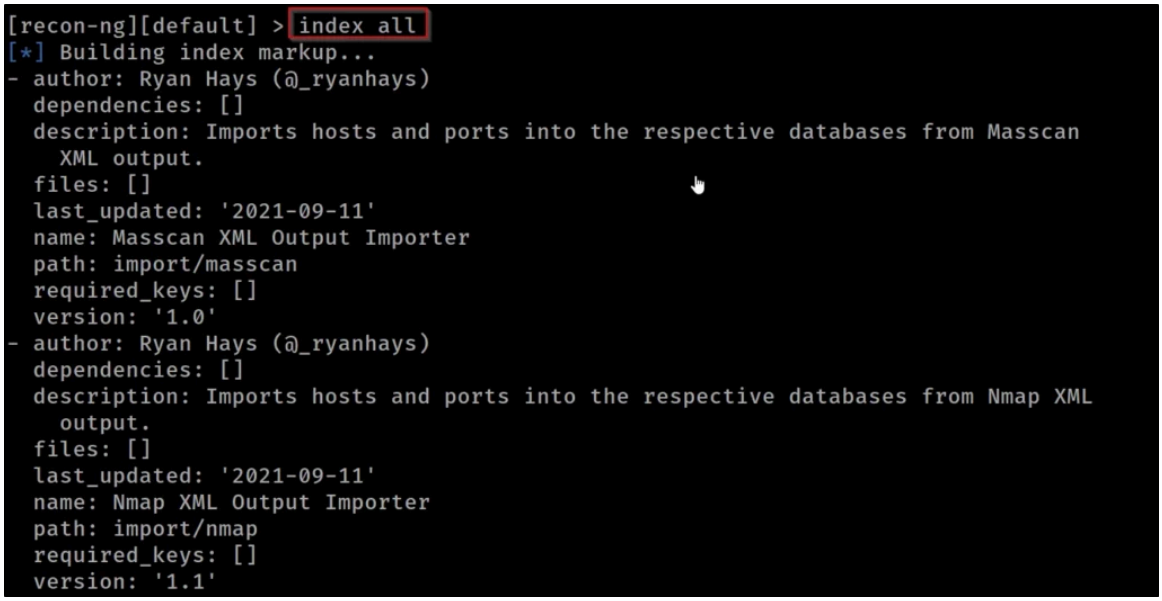
Index

Here is where we could know the information of the module.

Example1:

Gathering information on all installed modules

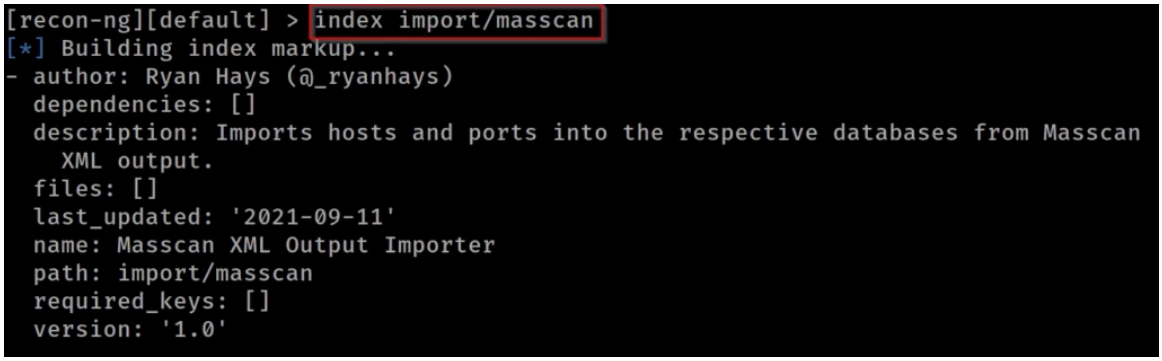
```
index all
```



Example2:

Now, let's index a specific module here it will be

```
index import/masscan
```



Marketplace

In the marketplace, we are going to install, remove, search, info, refresh and let's see about the marketplace.

In the marketplace, we can install all recon tools. Most of the recon tools are available in the marketplace but some tools will have some errors.

Example1:

Let's search for a tool, to search just enter

```
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            | 1.1     | installed     | 2020-01-13 |   |   |
  | 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     | installed     | 2020-04-07 |   |   |
  | import/nmap                                            | 1.1     | 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     | 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/unmangle                       | 1.1     | not installed | 2019-10-27 |   |   |
  | recon/contacts-credentials/hibp_breach                 | 1.2     | not installed | 2019-09-10 |   | * |
```

Example2:

Let's search for a specific tool, to search a specific tool enter this command ????????

```
marketplace search dns
```

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

  +-------------------------------------------------------------------------------------------------+
  |                          Path                          | Version |     Status    |  Updated   | D | K |
  +-------------------------------------------------------------------------------------------------+
  | 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 |   | * |
  +-------------------------------------------------------------------------------------------------+

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

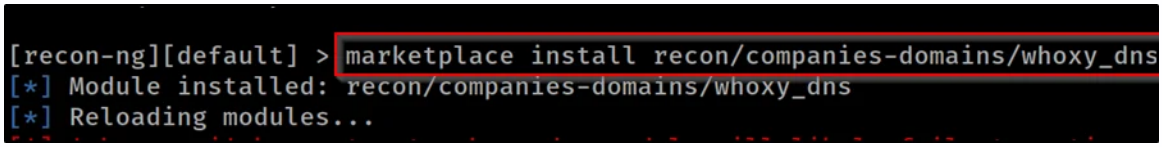
Instead of DNS you enter whatever you want, you could enter nmap, or any other tool you search for…

Example3:

Okay, now let's install the searched tool, to install any tool enter this command ????????

```
marketplace install recon/companies-domains/whoxy_dns
```

Instead of **recon/companies-domains/whoxy_dns** enter the tool you wanna install



Example4:

To remove any installed tool enter

```
marketplace remove  recon/companies-domains/whoxy_dns
```

The installed tool will be in modules, Next, let's see what is modules…

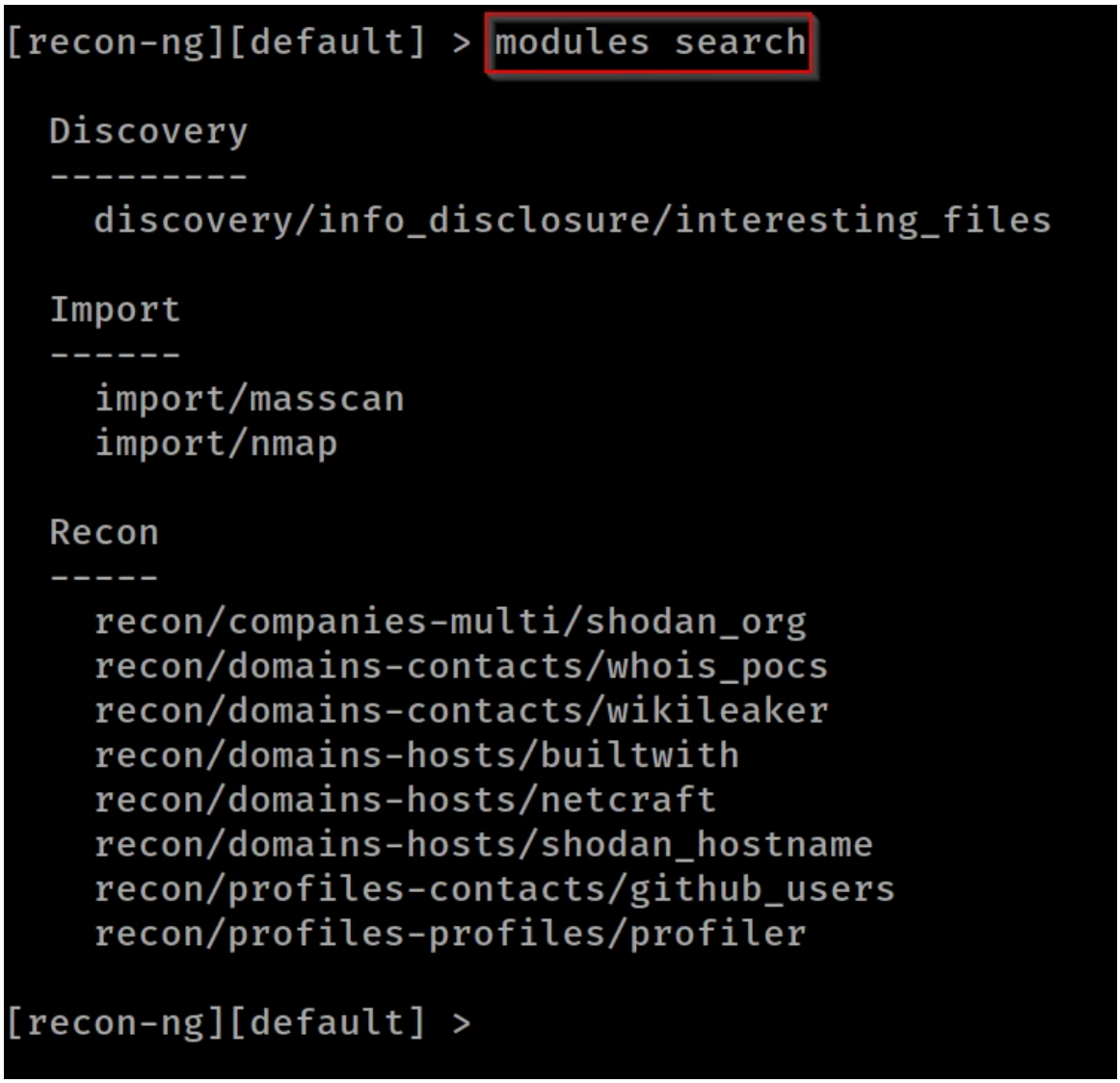
Modules

The installed tool in the marketplace will be in these modules, In modules let's see how to search, load, reload…

Example1:

Now, let's check for the installed tool in the marketplace, the tool will be saved in modules and to look for it do

```
Modules search
```

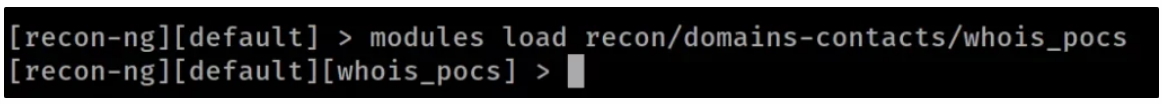


Example2:

To load the module just enter ????????

```
module load recon/domains-contacts/whois_pocs
```

Instead of **recon/domains-contacts/whois_pocs** enter the tool you wanna load

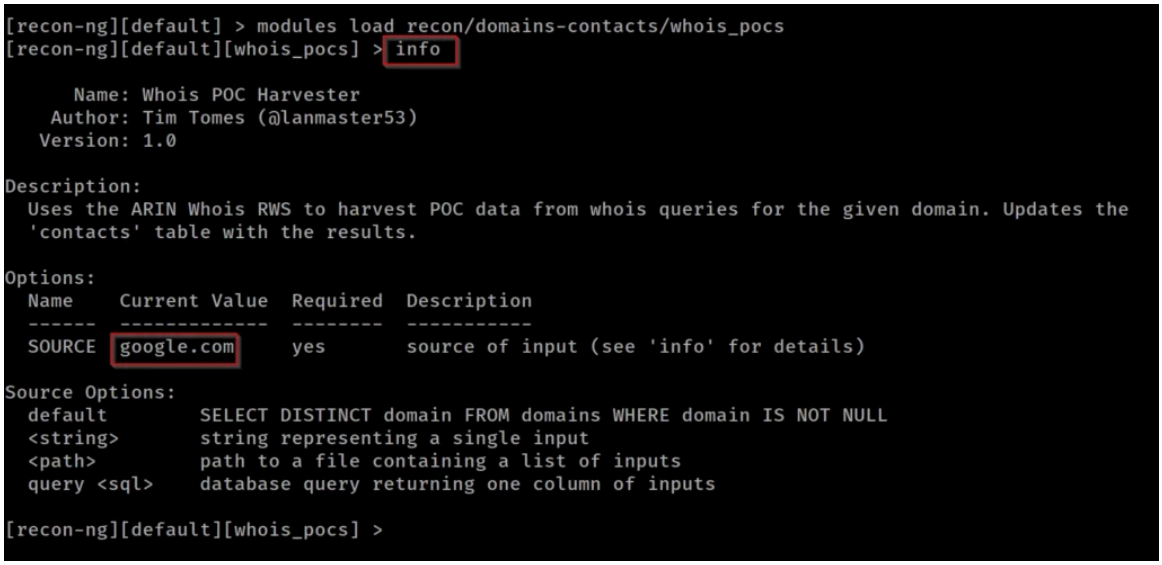


Now it is loaded, let's give **info**

Example3:

Now let's do info and look at the loaded module,

```
info
```



In the source, there is google.com, Instead of google.com we are entering bbc.com to set the SOURCE to let's enter this ????????

Example4:

Changing target

```
options unset SOURCE
```

Now we have unset the target, see the SOURCE there is nothing

Example5:

To add the target simply enter ????????

```
options set SOURCE bbc.com
```

Now the new target is set

Example6:

To run the set target just give

```
run
```

Keys

Now, we move on to keys, You should have noticed at the marketplace some tools asking for API keys.

So, to add the API key follow these steps…

Example1:

Firstly you should install a tool that has API key dependency and once installed. Do this command and see what all tools require keys

```
keys list
```

So, I have installed these tools ???? which requires API and one tool has API key.

Example2:

To add an API key just follow my steps ????????

```
keys add builtwith_api 00000000000000000000000000000000
```

Instead of buitwith_api add the tool you want, you could add whoxy_api, shodan_api and so on…

Example3:

To remove an API key do it ????????

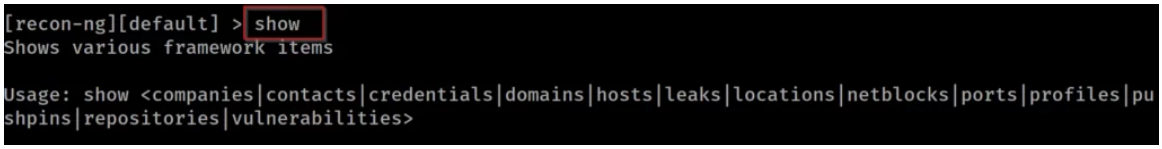
```
keys remove builtwith_api 00000000000000000000000000000000
```

Show

The show command shows the various frameworks

Example1:

The show commands show all the frameworks existing



Example2:

Now to see any framework just enter ????????

```
show companies
```

Instead of companies, you could enter the frameworks that exist there on the above pic

---

Also Read: Parsero information gathering tool

Also Read: Hping3 full tutorial

Tags

Information gathering

Share your love

You may also like

RustScan Full Tutorial | Updated 2024

3 December 2024

Feroxbuster Full Tutorial | Noob to Pro

2 December 2024

CrackMapExec in Action: Enumerating Windows Networks (Part 2)

10 March 2024