Lab 8: Perform Footprinting using Various Footprinting Tools

Lab Scenario

The information gathered in the previous steps may not be sufficient to reveal the potential vulnerabilities of the target. There could be more information available that could help in finding loopholes in the target. As an ethical hacker, you should look for as much information as possible about the target using various tools. This lab activity will demonstrate what other information you can extract from the target using various footprinting tools.

Lab Objectives

- Footprinting a target using Recon-ng

Overview of Footprinting Tools

Footprinting tools are used to collect basic information about the target systems in order to exploit them. Information collected by the footprinting tools contains the target's IP location information, routing information, business information, address, phone number and social security number, details about the source of an email and a file, DNS information, domain information, etc.

Task 1: Footprinting a Target using Recon-ng

Recon-ng is a web reconnaissance framework with independent modules and database interaction that provides an environment in which open-source web-based reconnaissance can be conducted. Here, we will use Recon-ng to perform network reconnaissance, gather personnel information, and gather target information from social networking sites.

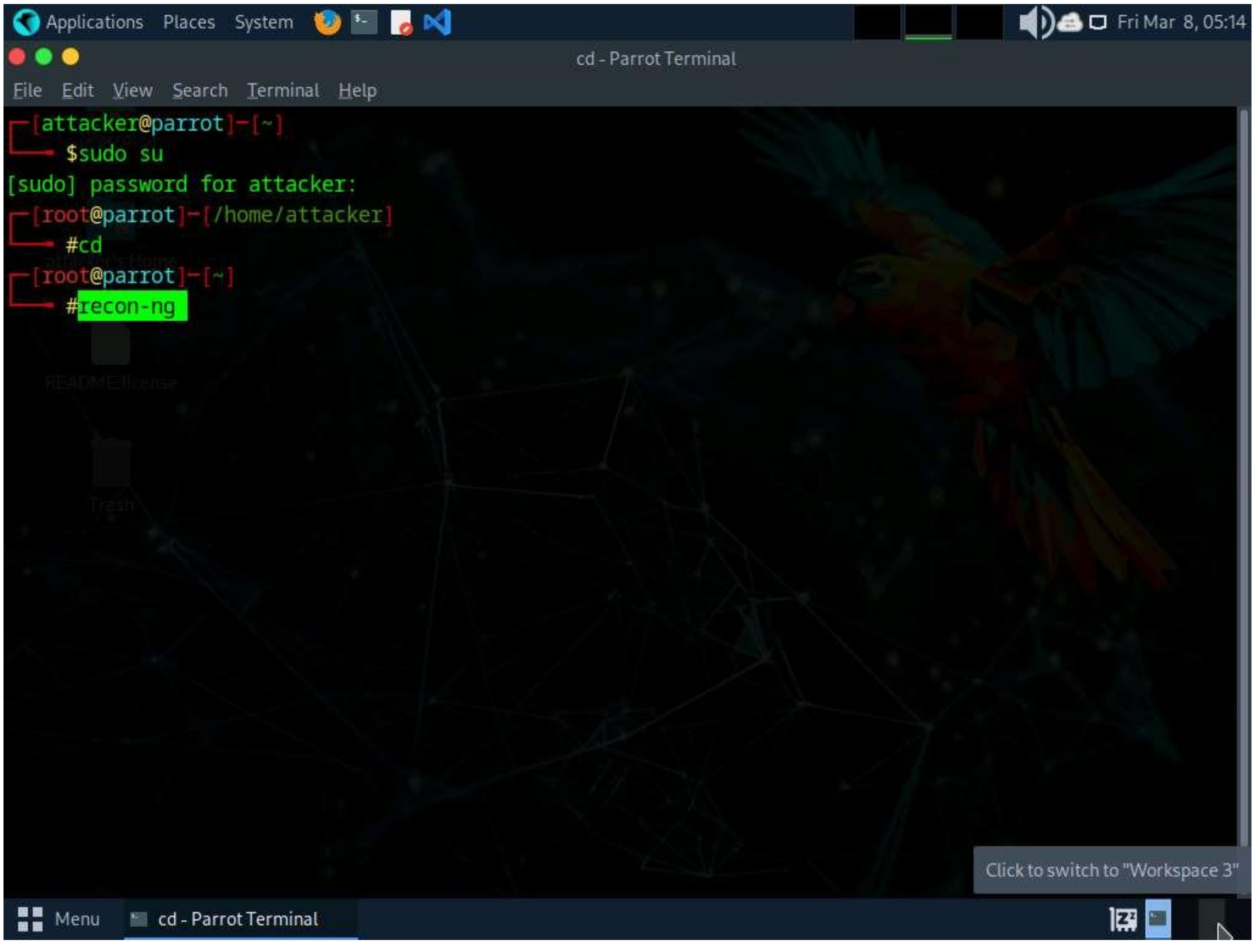
Here, we will consider **www.certifiedhacker.com** as a target website. However, you can select a target domain of your choice.

The results obtained might differ when you perform this lab task.

1. In the **Parrot Security** machine, open a **Terminal** window and execute **sudo su** to run the programs as a root user (When prompted, enter the password **toor**).

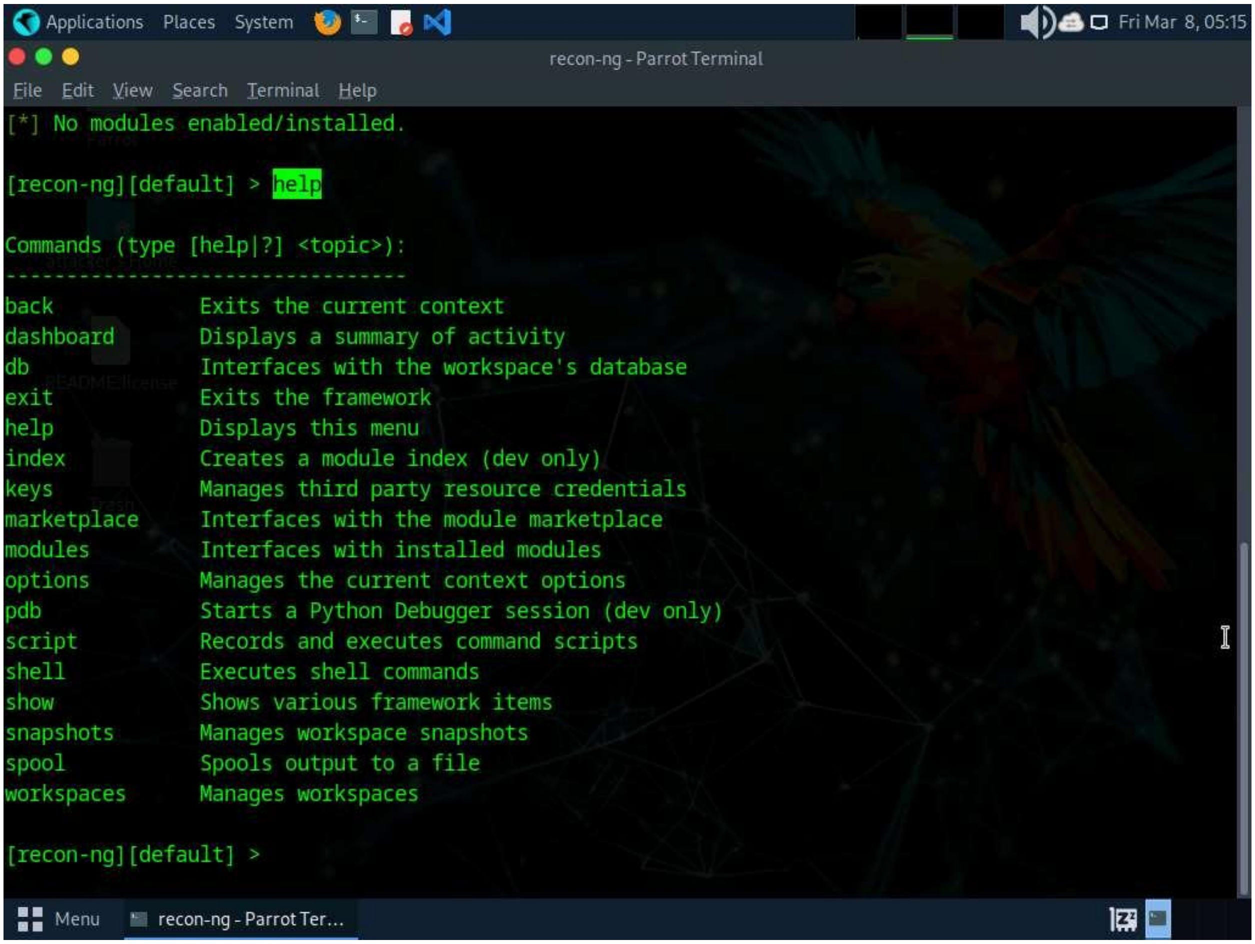
The password that you type will not be visible.

2. Now, run **cd** command to jump to the root directory and run **recon-ng** command to launch the application.



```
┌─[attacker@parrot]─[~]
└──╼ $sudo su
[sudo] password for attacker:
┌─[root@parrot]─[/home/attacker]
└──╼ #cd
┌─[root@parrot]─[~]
└──╼ #recon-ng
```

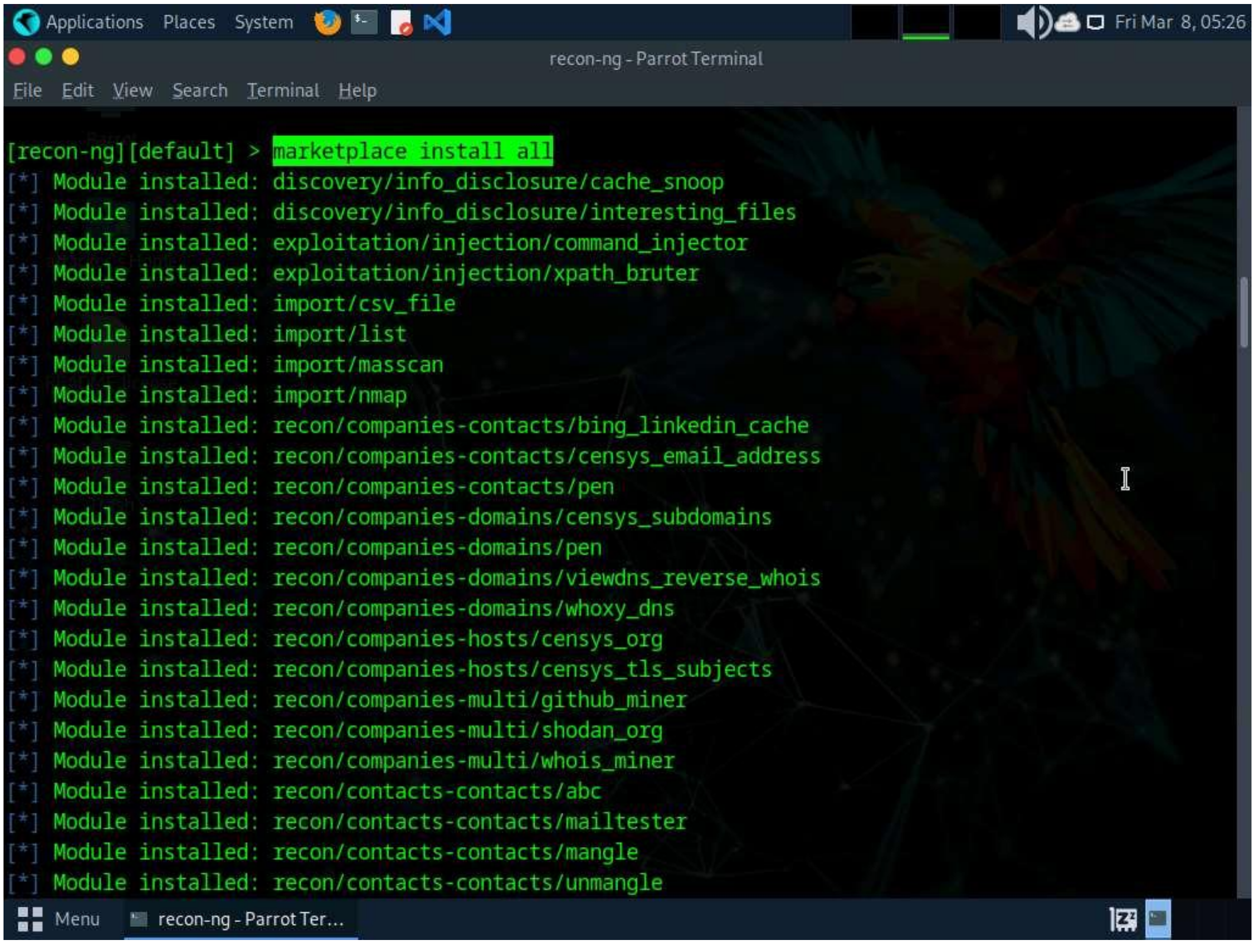
3. Run **help** command to view all the commands that allow you to add/delete records to a database, query a database, etc.



```
[*] 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] >
```

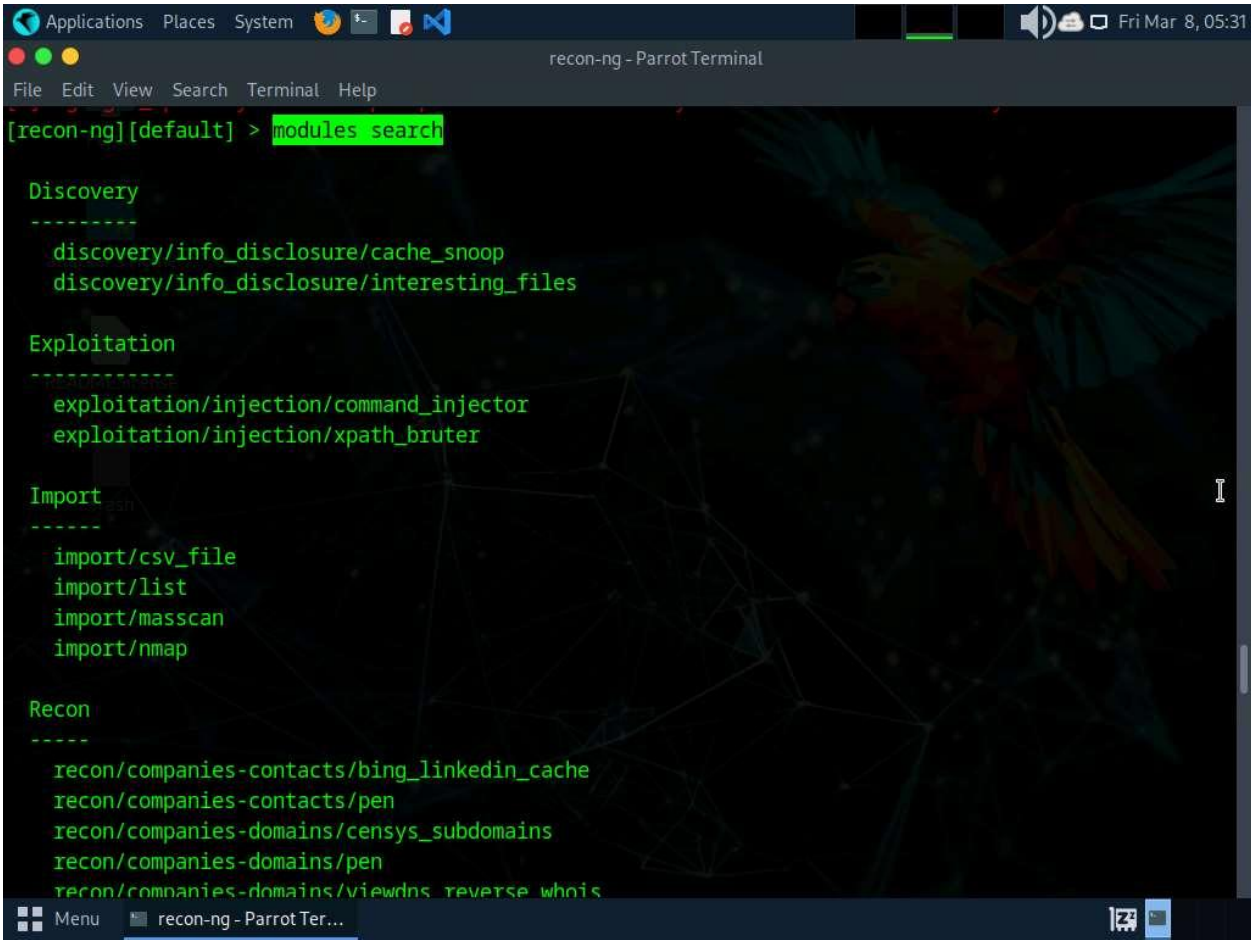
4. Run **marketplace install all** command to install all the modules available in recon-ng.

Ignore the errors while running the command.



```
[recon-ng][default] > marketplace install all
[*] Module installed: discovery/info_disclosure/cache_snoop
[*] Module installed: discovery/info_disclosure/interesting_files
[*] Module installed: exploitation/injection/command_injector
[*] Module installed: exploitation/injection/xpath_bruter
[*] Module installed: import/csv_file
[*] Module installed: import/list
[*] Module installed: import/masscan
[*] Module installed: import/nmap
[*] Module installed: recon/companies-contacts/bing_linkedin_cache
[*] Module installed: recon/companies-contacts/censys_email_address
[*] Module installed: recon/companies-contacts/pen
[*] Module installed: recon/companies-domains/censys_subdomains
[*] Module installed: recon/companies-domains/pen
[*] Module installed: recon/companies-domains/viewdns_reverse_whois
[*] Module installed: recon/companies-domains/whoxy_dns
[*] Module installed: recon/companies-hosts/censys_org
[*] Module installed: recon/companies-hosts/censys_tls_subjects
[*] Module installed: recon/companies-multi/github_miner
[*] Module installed: recon/companies-multi/shodan_org
[*] Module installed: recon/companies-multi/whois_miner
[*] Module installed: recon/contacts-contacts/abc
[*] Module installed: recon/contacts-contacts/mailtester
[*] Module installed: recon/contacts-contacts/mangle
[*] Module installed: recon/contacts-contacts/unmangle
```

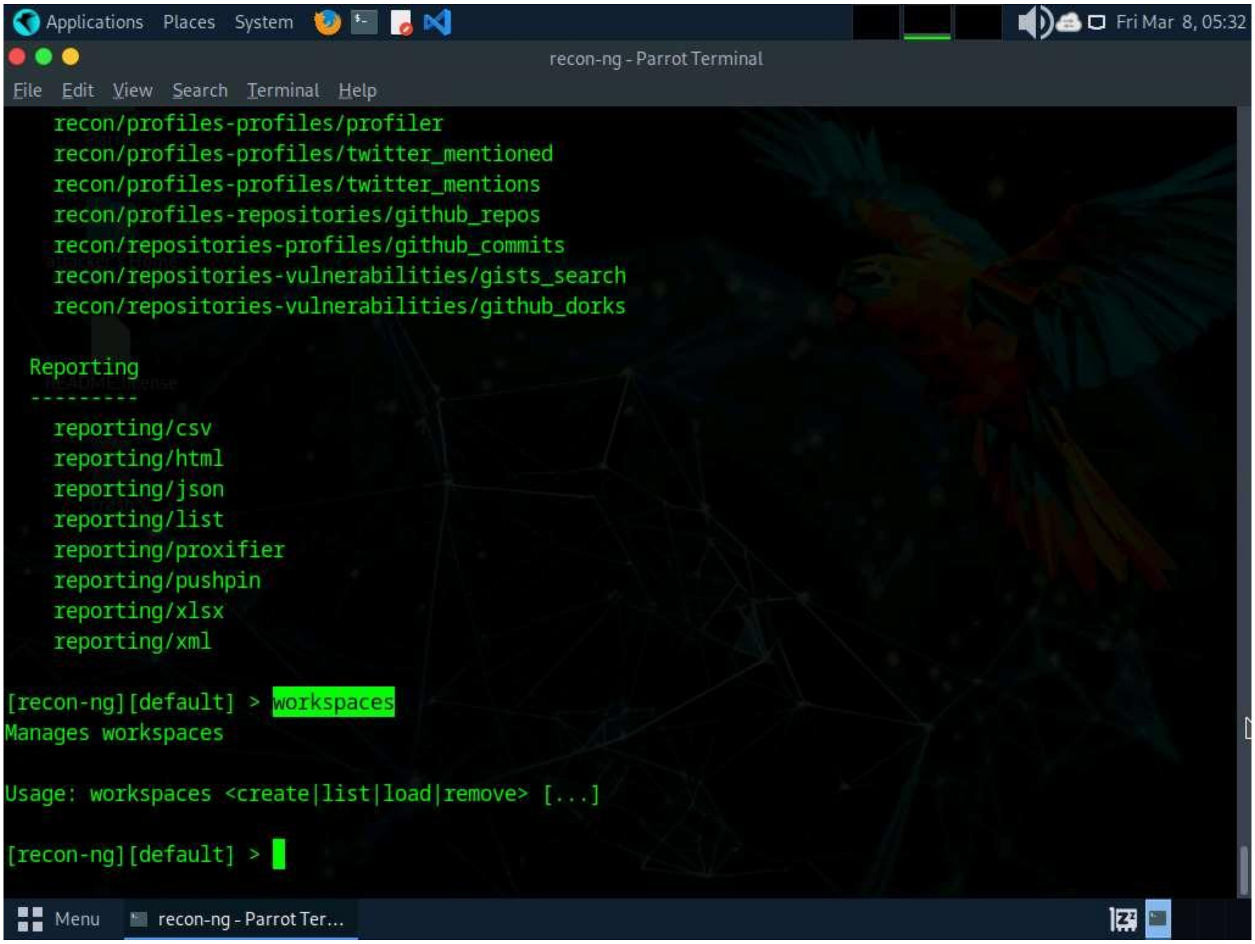
5. After the installation of modules, run **modules search** command. This displays all the modules available in recon-ng.



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

  Discovery
  ---------
    discovery/info_disclosure/cache_snoop
    discovery/info_disclosure/interesting_files

  Exploitation
  ------------
    exploitation/injection/command_injector
    exploitation/injection/xpath_bruter

  Import
  ------
    import/csv_file
    import/list
    import/masscan
    import/nmap

  Recon
  -----
    recon/companies-contacts/bing_linkedin_cache
    recon/companies-contacts/pen
    recon/companies-domains/censys_subdomains
    recon/companies-domains/pen
    recon/companies-domains/viewdns_reverse_whois
```

6. You will be able to perform network discovery, exploitation, reconnaissance, etc. by loading the required modules.

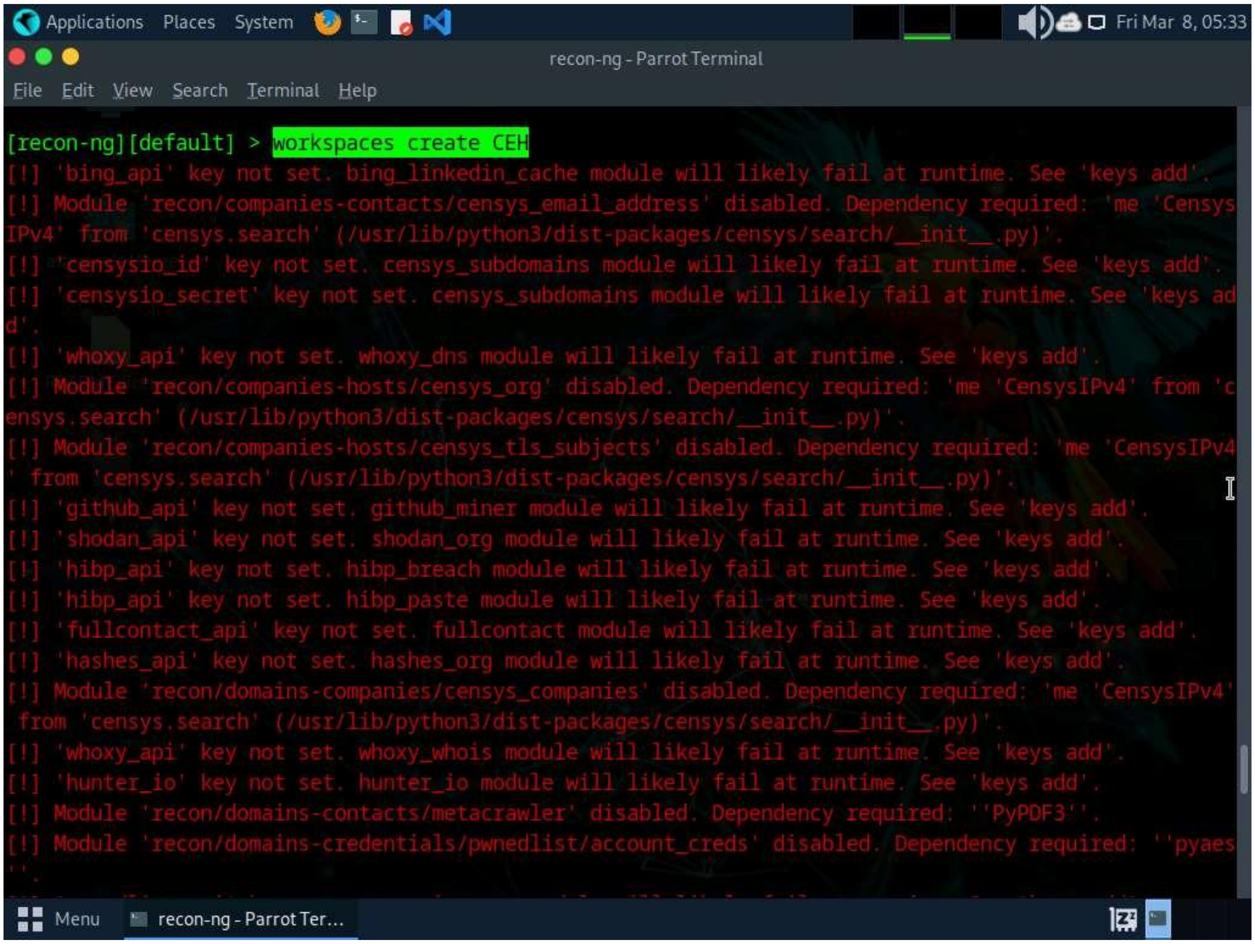
7. Run **workspaces** command to view the commands related to the workspaces.



```
    recon/profiles-profiles/profiler
    recon/profiles-profiles/twitter_mentioned
    recon/profiles-profiles/twitter_mentions
    recon/profiles-repositories/github_repos
    recon/repositories-profiles/github_commits
    recon/repositories-vulnerabilities/gists_search
    recon/repositories-vulnerabilities/github_dorks

  Reporting
  ---------
    reporting/csv
    reporting/html
    reporting/json
    reporting/list
    reporting/proxifier
    reporting/pushpin
    reporting/xlsx
    reporting/xml

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

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

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

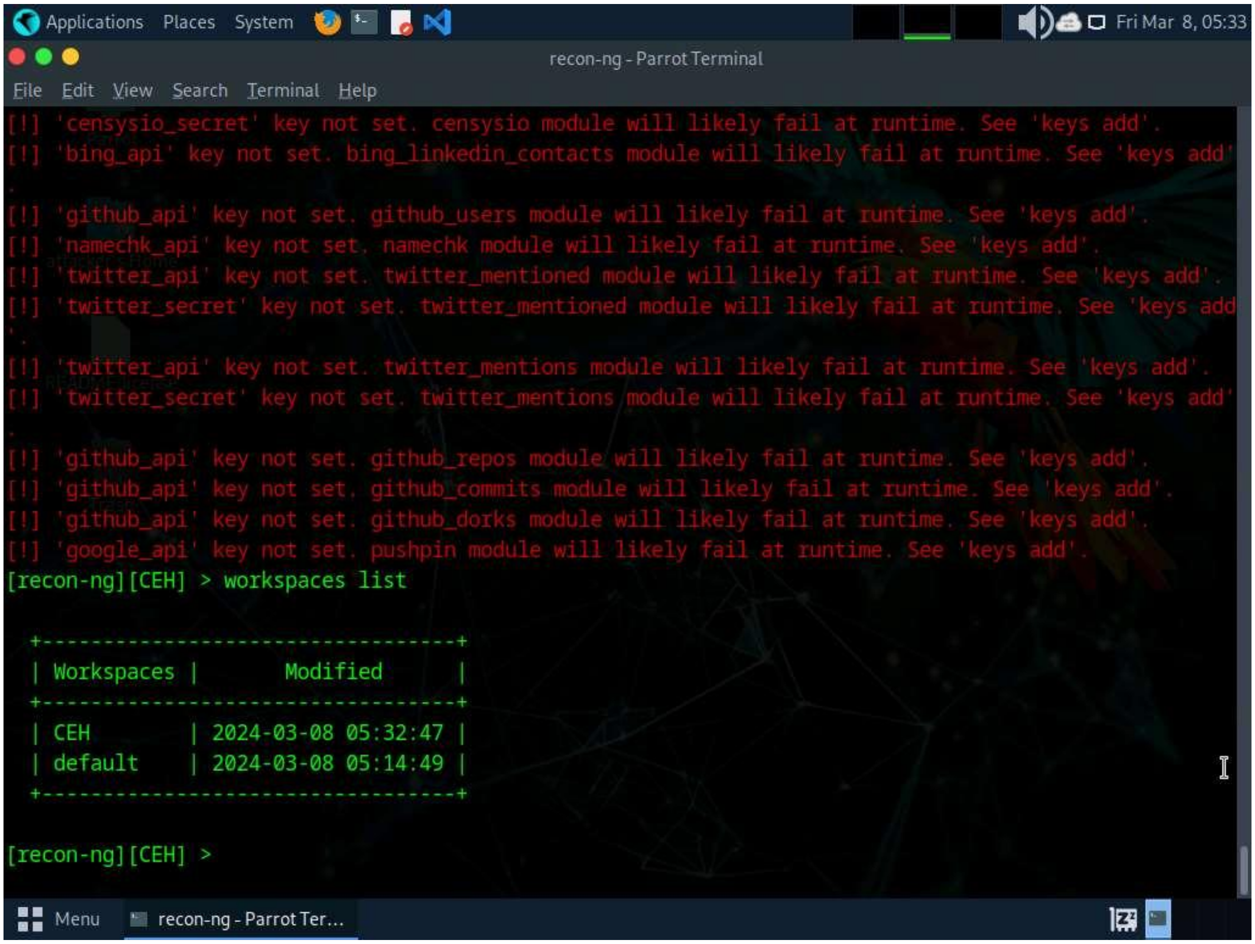
8. Create a workspace in which to perform network reconnaissance. In this task, we shall be creating a workspace named **CEH**.

9. To create the workspace, run **workspaces create CEH** command. This creates a workspace named CEH.



```
[recon-ng][default] > workspaces create CEH
[!] 'bing_api' key not set. bing_linkedin_cache module will likely fail at runtime. See 'keys add'.
[!] Module 'recon/companies-contacts/censys_email_address' disabled. Dependency required: 'me 'Censys
IPv4' from 'censys.search' (/usr/lib/python3/dist-packages/censys/search/__init__.py)'.
[!] 'censysio_id' key not set. censys_subdomains module will likely fail at runtime. See 'keys add'.
[!] 'censysio_secret' key not set. censys_subdomains module will likely fail at runtime. See 'keys ad
d'.
[!] 'whoxy_api' key not set. whoxy_dns module will likely fail at runtime. See 'keys add'.
[!] Module 'recon/companies-hosts/censys_org' disabled. Dependency required: 'me 'CensysIPv4' from 'c
ensys.search' (/usr/lib/python3/dist-packages/censys/search/__init__.py)'.
[!] Module 'recon/companies-hosts/censys_tls_subjects' disabled. Dependency required: 'me 'CensysIPv4
' from 'censys.search' (/usr/lib/python3/dist-packages/censys/search/__init__.py)'.
[!] 'github_api' key not set. github_miner module will likely fail at runtime. See 'keys add'.
[!] 'shodan_api' key not set. shodan_org module will likely fail at runtime. See 'keys add'.
[!] 'hibp_api' key not set. hibp_breach module will likely fail at runtime. See 'keys add'.
[!] 'hibp_api' key not set. hibp_paste module will likely fail at runtime. See 'keys add'.
[!] 'fullcontact_api' key not set. fullcontact module will likely fail at runtime. See 'keys add'.
[!] 'hashes_api' key not set. hashes_org module will likely fail at runtime. See 'keys add'.
[!] Module 'recon/domains-companies/censys_companies' disabled. Dependency required: 'me 'CensysIPv4'
 from 'censys.search' (/usr/lib/python3/dist-packages/censys/search/__init__.py)'.
[!] 'whoxy_api' key not set. whoxy_whois module will likely fail at runtime. See 'keys add'.
[!] 'hunter_io' key not set. hunter_io module will likely fail at runtime. See 'keys add'.
[!] Module 'recon/domains-contacts/metacrawler' disabled. Dependency required: ''PyPDF3''.
[!] Module 'recon/domains-credentials/pwnedlist/account_creds' disabled. Dependency required: ''pyaes
''.
```

10. Enter **workspaces list**. This displays a list of workspaces (along with the workspace added in the previous step) that are present within the workspaces databases.



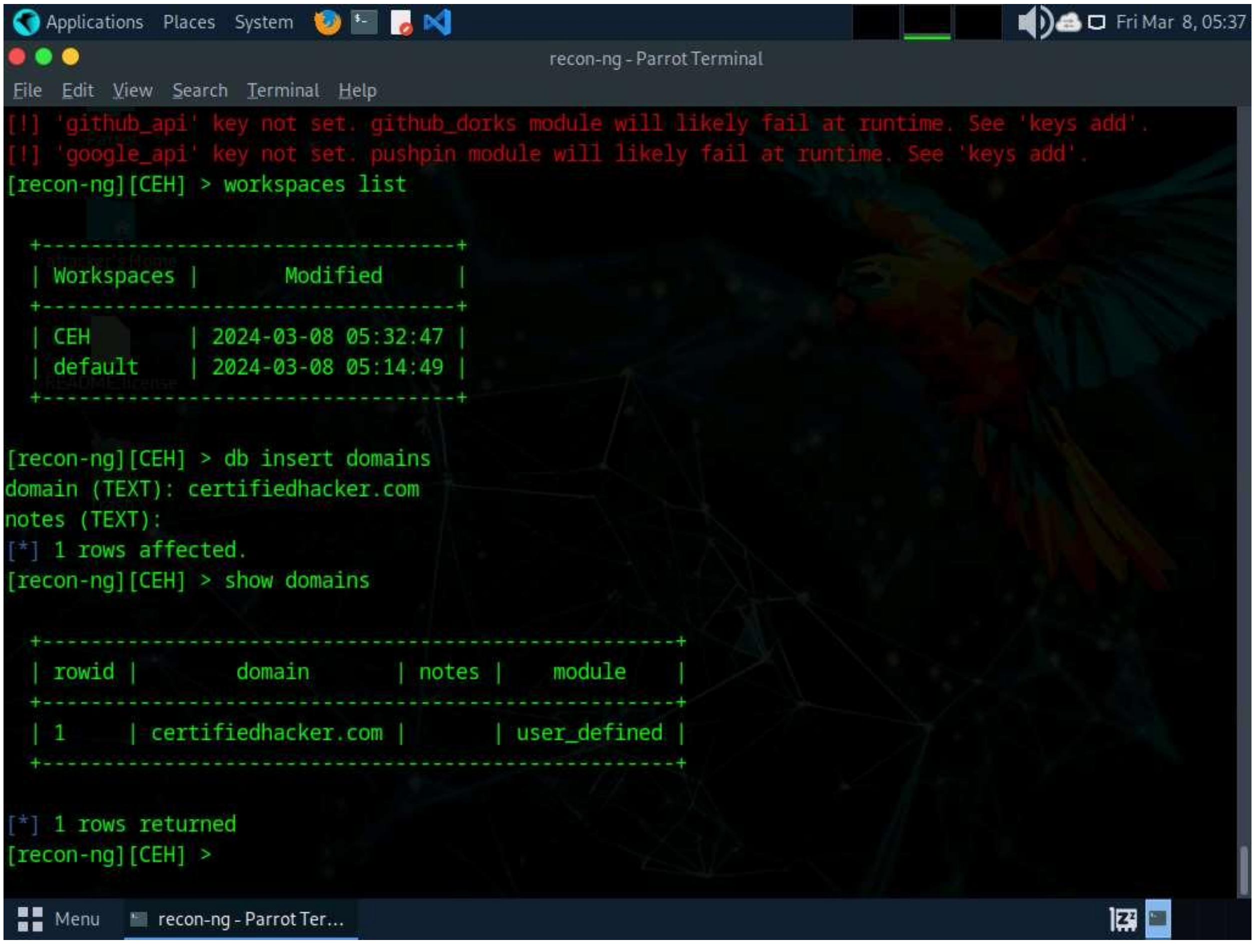
```
[!] 'censysio_secret' key not set. censysio module will likely fail at runtime. See 'keys add'.
[!] 'bing_api' key not set. bing_linkedin_contacts module will likely fail at runtime. See 'keys add'
.
[!] 'github_api' key not set. github_users module will likely fail at runtime. See 'keys add'.
[!] 'namechk_api' key not set. namechk module will likely fail at runtime. See 'keys add'.
[!] 'twitter_api' key not set. twitter_mentioned module will likely fail at runtime. See 'keys add'.
[!] 'twitter_secret' key not set. twitter_mentioned module will likely fail at runtime. See 'keys add
'.
[!] 'twitter_api' key not set. twitter_mentions module will likely fail at runtime. See 'keys add'.
[!] 'twitter_secret' key not set. twitter_mentions module will likely fail at runtime. See 'keys add'
.
[!] 'github_api' key not set. github_repos module will likely fail at runtime. See 'keys add'.
[!] 'github_api' key not set. github_commits module will likely fail at runtime. See 'keys add'.
[!] 'github_api' key not set. github_dorks module will likely fail at runtime. See 'keys add'.
[!] 'google_api' key not set. pushpin module will likely fail at runtime. See 'keys add'.
[recon-ng][CEH] > workspaces list

  +------------------------------------+
  | Workspaces |       Modified        |
  +------------------------------------+
  | CEH        | 2024-03-08 05:32:47 |
  | default    | 2024-03-08 05:14:49 |
  +------------------------------------+

[recon-ng][CEH] >
```

11. Add a domain in which you want to perform network reconnaissance.

12. Issue the command **db insert domains**.

13. Under **domain (TEXT)** option type **certifiedhacker.com** and press **Enter**. In the **notes (TEXT)** option press **Enter**. This adds certifiedhacker.com to the present workspace.

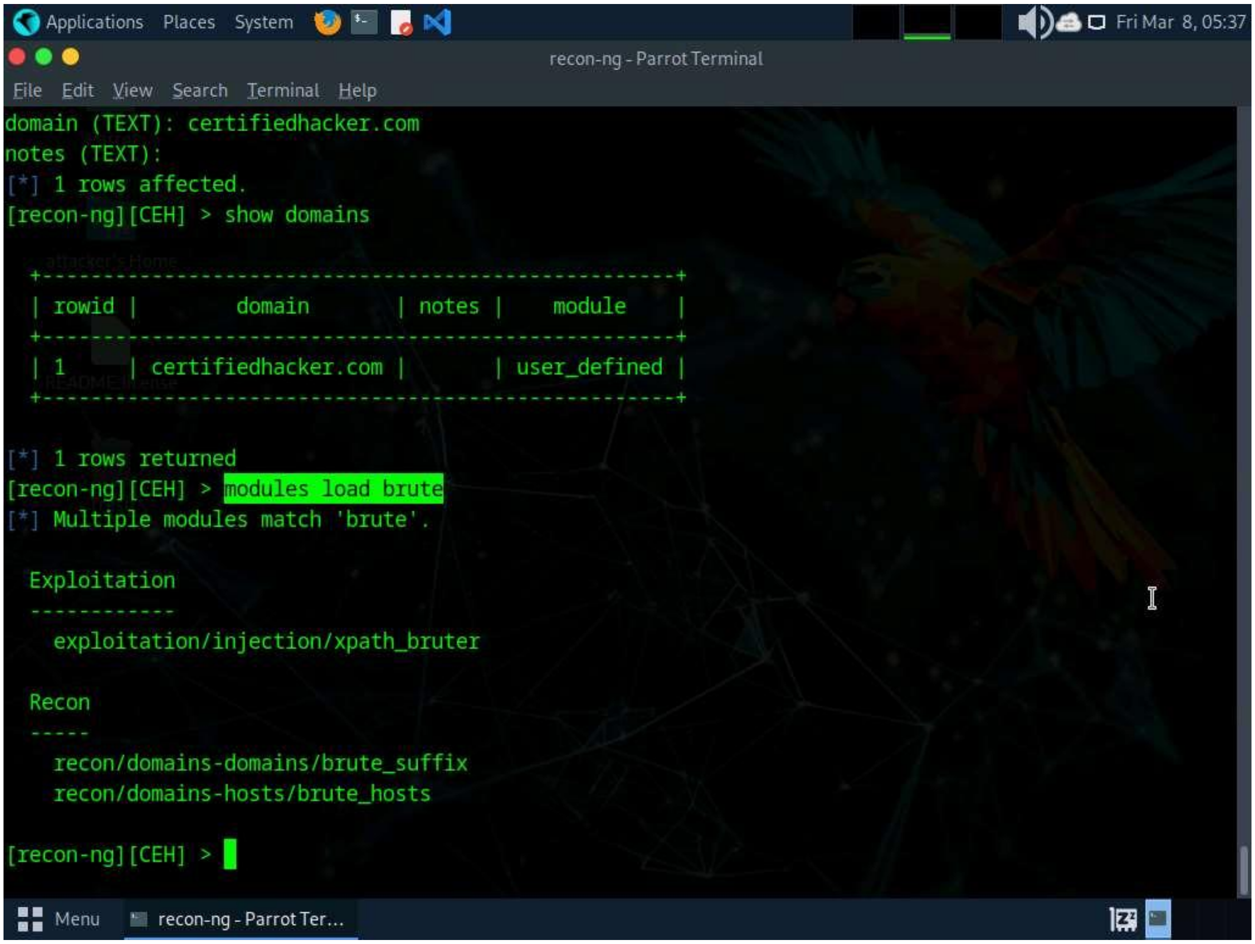
14. You can view the added domain by issuing the **show domains** command, as shown in the screenshot.



```
[!] 'github_api' key not set. github_dorks module will likely fail at runtime. See 'keys add'.
[!] 'google_api' key not set. pushpin module will likely fail at runtime. See 'keys add'.
[recon-ng][CEH] > workspaces list

  +----------------------------------+
  | Workspaces |       Modified      |
  +----------------------------------+
  | CEH        | 2024-03-08 05:32:47 |
  | default    | 2024-03-08 05:14:49 |
  +----------------------------------+

[recon-ng][CEH] > db insert domains
domain (TEXT): certifiedhacker.com
notes (TEXT):
[*] 1 rows affected.
[recon-ng][CEH] > show domains

  +-------------------------------------------------------+
  | rowid |        domain       | notes |    module    |
  +-------------------------------------------------------+
  | 1     | certifiedhacker.com |       | user_defined |
  +-------------------------------------------------------+

[*] 1 rows returned
[recon-ng][CEH] >
```

15. Harvest the hosts-related information associated with **certifiedhacker.com** by loading network reconnaissance modules such as brute_hosts, Netcraft, and Bing.

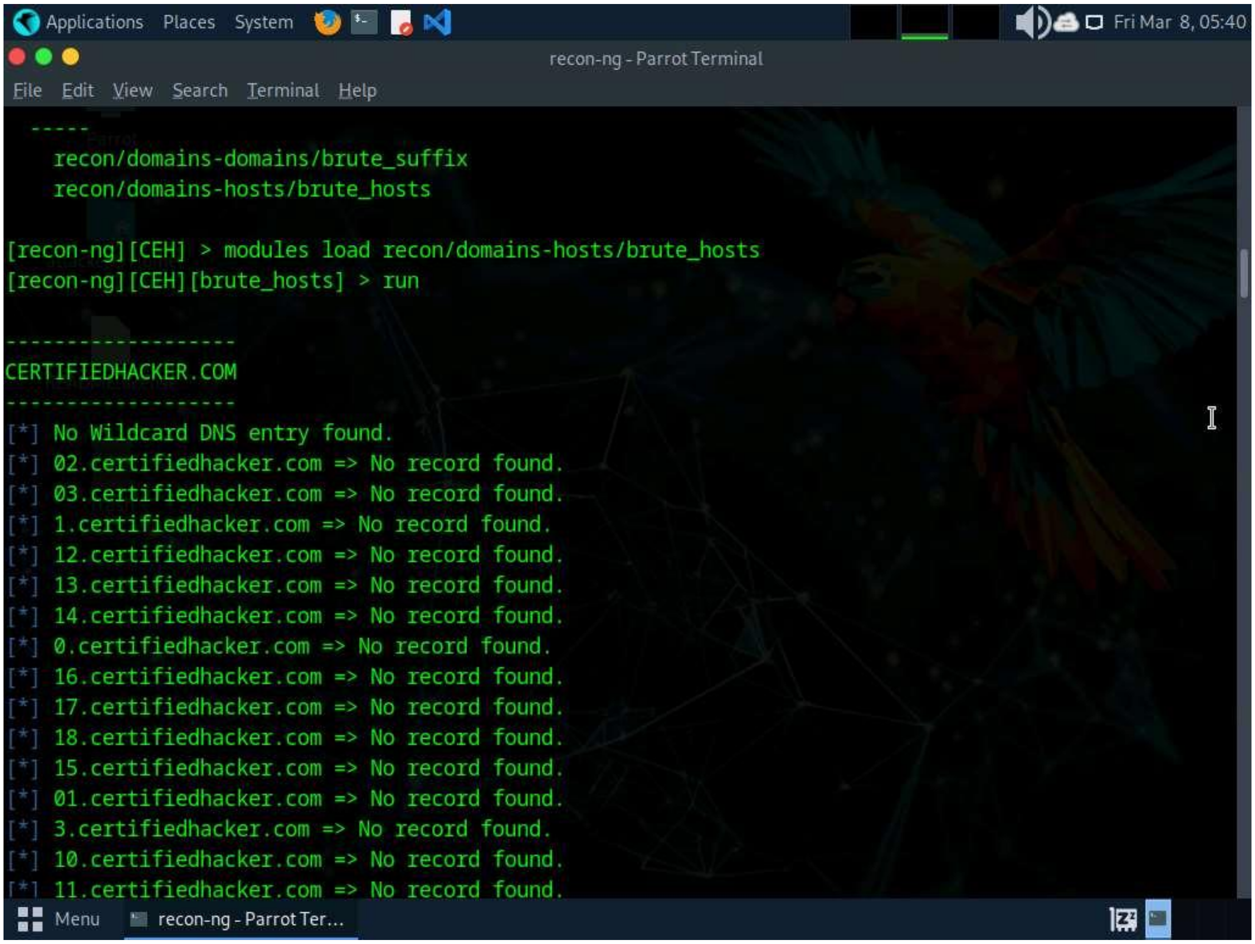
16. Issue **modules load brute** command to view all the modules related to brute forcing. In this task, we will be using the **recon/domains-hosts/brute_hosts** module to harvest hosts.


Applications Places System
Fri Mar 8, 05:37
recon-ng - Parrot Terminal
File Edit View Search Terminal Help
Menu
recon-ng - Parrot Ter...

```
domain (TEXT): certifiedhacker.com
notes (TEXT):
[*] 1 rows affected.
[recon-ng][CEH] > show domains

  +------------------------------------------------------+
  | rowid |         domain        | notes |    module    |
  +------------------------------------------------------+
  | 1     | certifiedhacker.com |       | user_defined |
  +------------------------------------------------------+

[*] 1 rows returned
[recon-ng][CEH] > modules load brute
[*] Multiple modules match 'brute'.

  Exploitation
  ------------
    exploitation/injection/xpath_bruter

  Recon
  -----
    recon/domains-domains/brute_suffix
    recon/domains-hosts/brute_hosts

[recon-ng][CEH] >
```

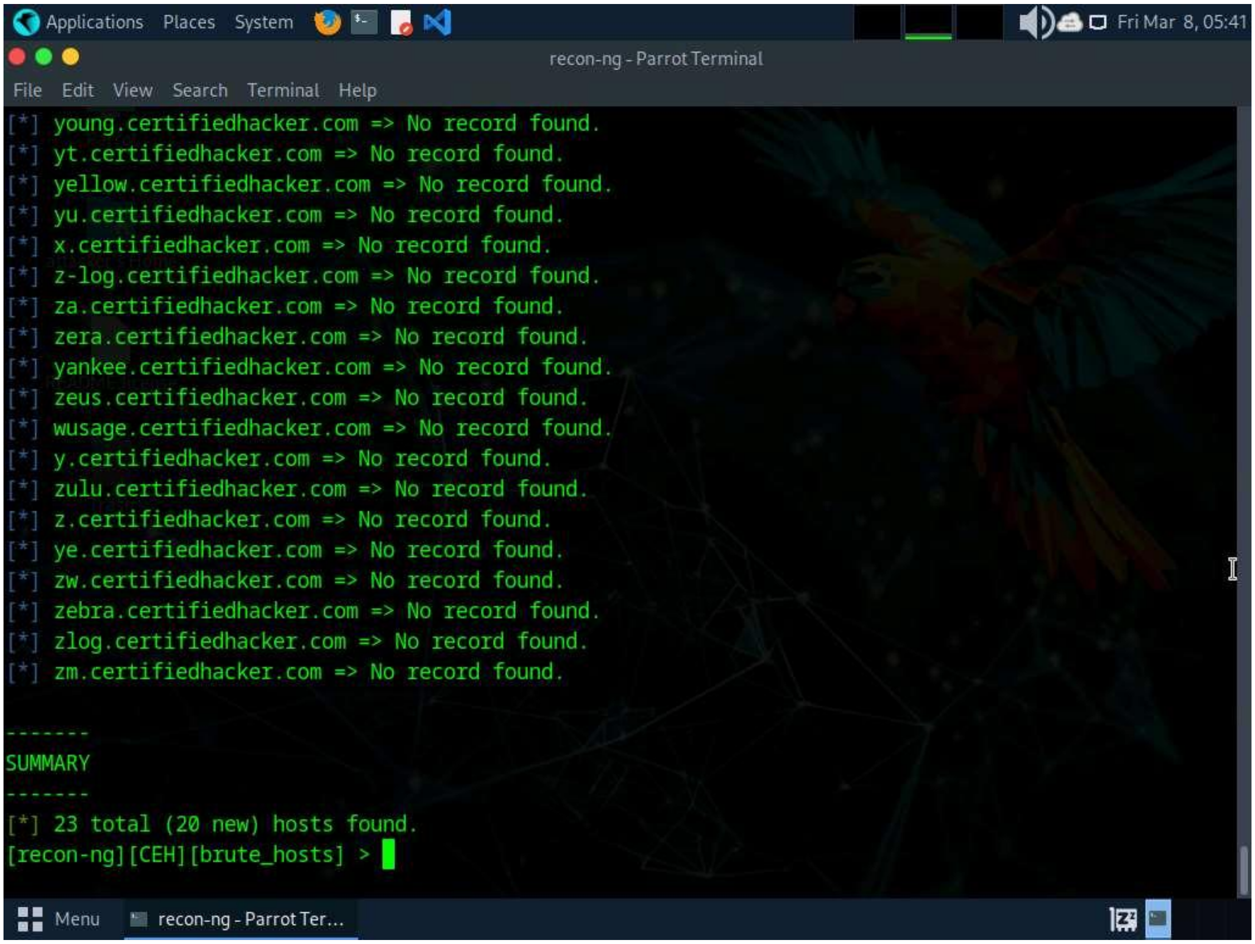
17. To load the **recon/domains-hosts/brute_hosts** module, issue **modules load recon/domains-hosts/brute_hosts** command.

18. Issue **run** command. This begins to harvest the hosts, as shown in the screenshot.



```
  -----
    recon/domains-domains/brute_suffix
    recon/domains-hosts/brute_hosts

[recon-ng][CEH] > modules load recon/domains-hosts/brute_hosts
[recon-ng][CEH][brute_hosts] > run

-------------------
CERTIFIEDHACKER.COM
-------------------
[*] No Wildcard DNS entry found.
[*] 02.certifiedhacker.com => No record found.
[*] 03.certifiedhacker.com => No record found.
[*] 1.certifiedhacker.com => No record found.
[*] 12.certifiedhacker.com => No record found.
[*] 13.certifiedhacker.com => No record found.
[*] 14.certifiedhacker.com => No record found.
[*] 0.certifiedhacker.com => No record found.
[*] 16.certifiedhacker.com => No record found.
[*] 17.certifiedhacker.com => No record found.
[*] 18.certifiedhacker.com => No record found.
[*] 15.certifiedhacker.com => No record found.
[*] 01.certifiedhacker.com => No record found.
[*] 3.certifiedhacker.com => No record found.
[*] 10.certifiedhacker.com => No record found.
[*] 11.certifiedhacker.com => No record found.
```

19. Observe that hosts have been added by running the **recon/domains-hosts/brute_hosts** module.


Applications Places System
Fri Mar 8, 05:41
recon-ng - Parrot Terminal
File Edit View Search Terminal Help
Menu
recon-ng - Parrot Ter...

```
[*] young.certifiedhacker.com => No record found.
[*] yt.certifiedhacker.com => No record found.
[*] yellow.certifiedhacker.com => No record found.
[*] yu.certifiedhacker.com => No record found.
[*] x.certifiedhacker.com => No record found.
[*] z-log.certifiedhacker.com => No record found.
[*] za.certifiedhacker.com => No record found.
[*] zera.certifiedhacker.com => No record found.
[*] yankee.certifiedhacker.com => No record found.
[*] zeus.certifiedhacker.com => No record found.
[*] wusage.certifiedhacker.com => No record found.
[*] y.certifiedhacker.com => No record found.
[*] zulu.certifiedhacker.com => No record found.
[*] z.certifiedhacker.com => No record found.
[*] ye.certifiedhacker.com => No record found.
[*] zw.certifiedhacker.com => No record found.
[*] zebra.certifiedhacker.com => No record found.
[*] zlog.certifiedhacker.com => No record found.
[*] zm.certifiedhacker.com => No record found.

-------
SUMMARY
-------
[*] 23 total (20 new) hosts found.
[recon-ng][CEH][brute_hosts] >
```

20. You have now harvested the hosts related to certifiedhacker.com using the brute_hosts module. You can use other modules such as Netcraft and Bing to harvest more hosts.

Use the **back** command to go back to the CEH attributes terminal.

To resolve hosts using the Bing module, use the following commands:

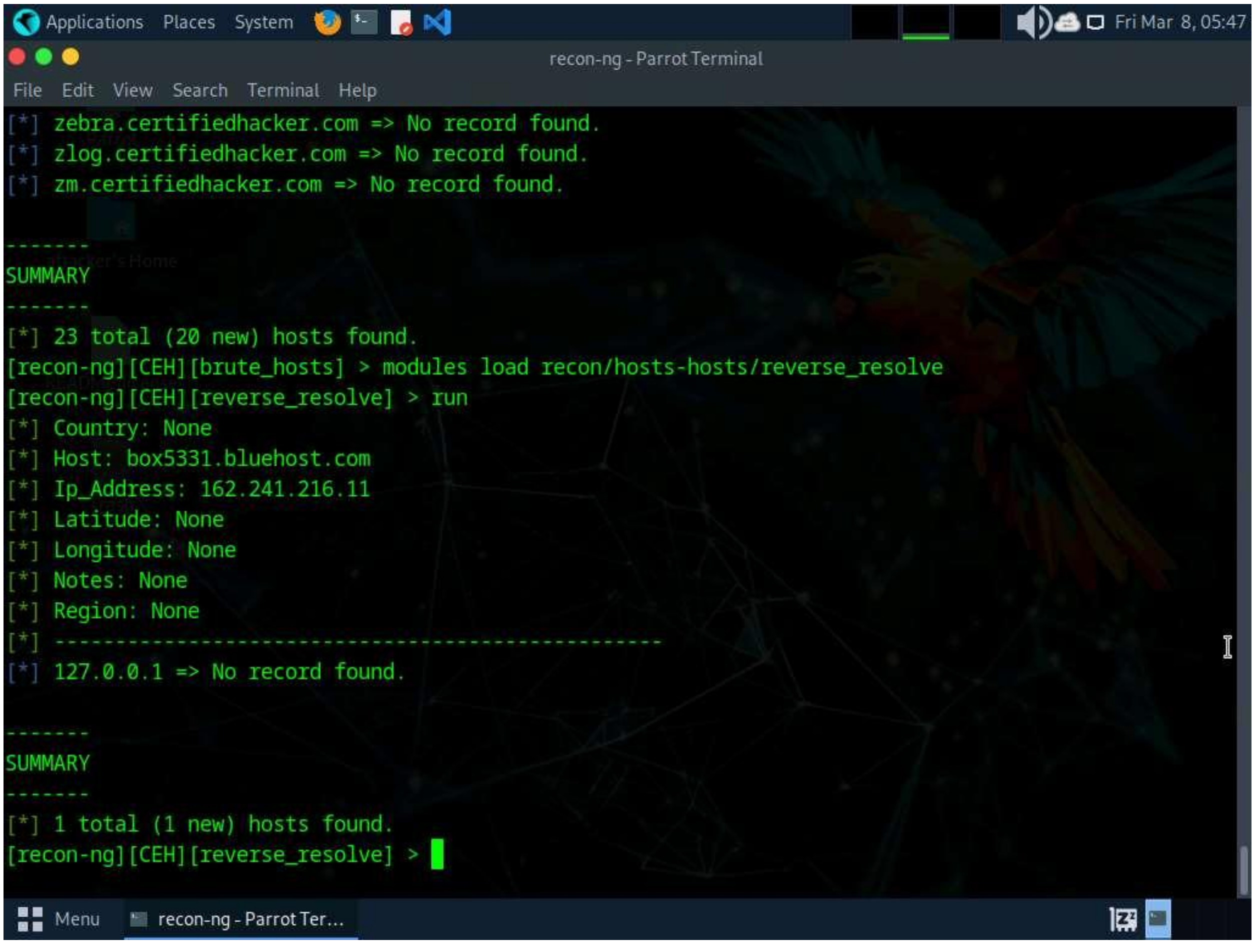
- **back**
- **modules load recon/domains-hosts/bing_domain_web**
- **run**

21. Now, perform a reverse lookup for each IP address (the IP address that is obtained during the reconnaissance process) to resolve to respective hostnames.

22. Execute **modules load reverse_resolve** command to view all the modules associated with the reverse_resolve keyword. In this task, we will be using the **recon/hosts-hosts/reverse_resolve** module.

23. Run the **modules load recon/hosts-hosts/reverse_resolve** command to load the module.

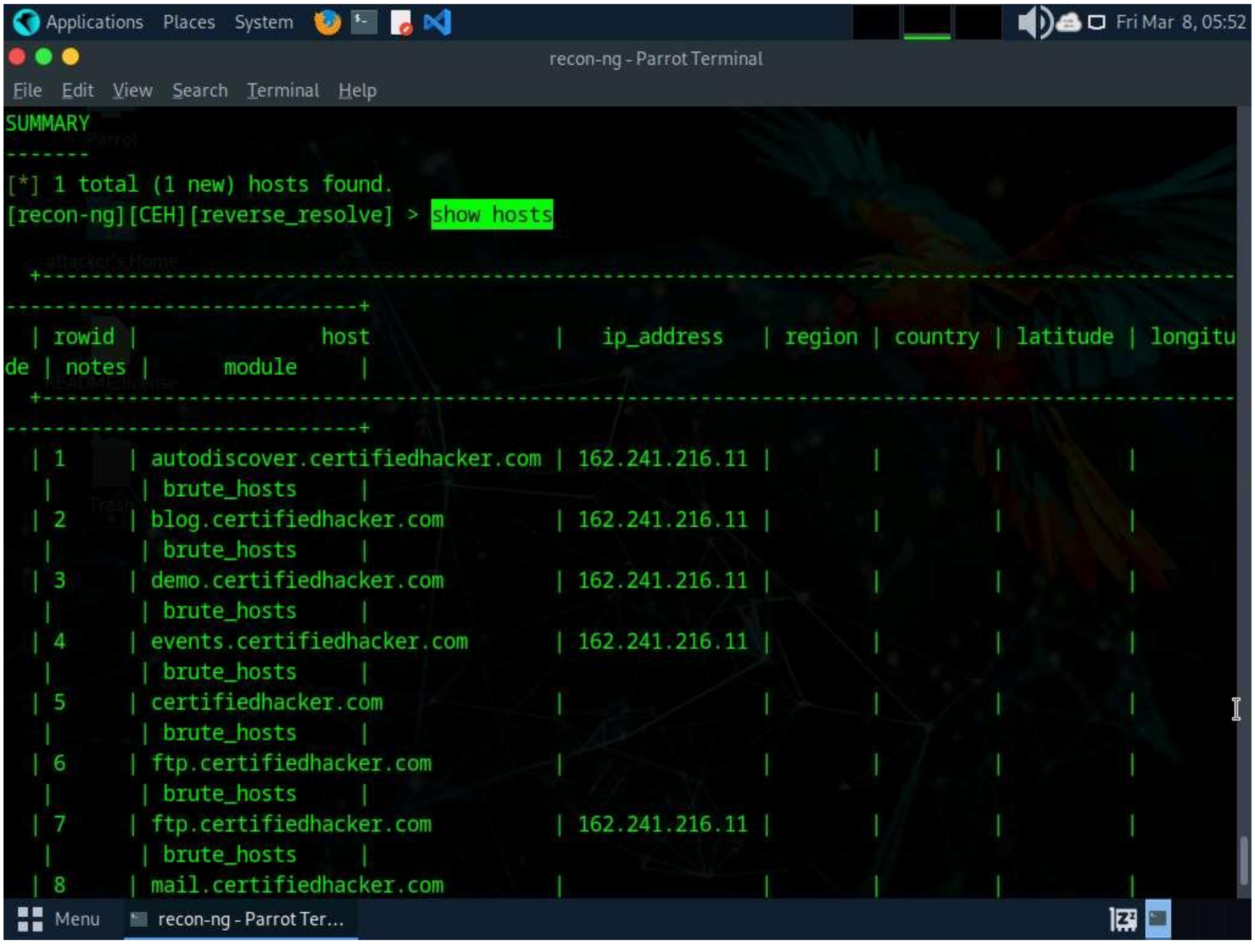
24. Issue the **run** command to begin the reverse lookup.



Applications Places System
Fri Mar 8, 05:47
recon-ng - Parrot Terminal
File Edit View Search Terminal Help
Menu
recon-ng - Parrot Ter...

```
[*] zebra.certifiedhacker.com => No record found.
[*] zlog.certifiedhacker.com => No record found.
[*] zm.certifiedhacker.com => No record found.

-------
SUMMARY
-------
[*] 23 total (20 new) hosts found.
[recon-ng][CEH][brute_hosts] > modules load recon/hosts-hosts/reverse_resolve
[recon-ng][CEH][reverse_resolve] > run
[*] Country: None
[*] Host: box5331.bluehost.com
[*] Ip_Address: 162.241.216.11
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] --------------------------------------------------
[*] 127.0.0.1 => No record found.

-------
SUMMARY
-------
[*] 1 total (1 new) hosts found.
[recon-ng][CEH][reverse_resolve] >
```

25. Once done with the reverse lookup process, run the **show hosts** command. This displays all the hosts that are harvested so far, as shown in the screenshot.



```
SUMMARY
-------
[*] 1 total (1 new) hosts found.
[recon-ng][CEH][reverse_resolve] > show hosts

  +-----------------------------------------------------------------------------------------------------
-----------------------------+
  | rowid |              host              |   ip_address    | region | country | latitude | longitu
de | notes |      module     |
  +-----------------------------------------------------------------------------------------------------
-----------------------------+
  | 1     | autodiscover.certifiedhacker.com | 162.241.216.11 |        |         |          |
  |       | brute_hosts     |
  | 2     | blog.certifiedhacker.com         | 162.241.216.11 |        |         |          |
  |       | brute_hosts     |
  | 3     | demo.certifiedhacker.com         | 162.241.216.11 |        |         |          |
  |       | brute_hosts     |
  | 4     | events.certifiedhacker.com       | 162.241.216.11 |        |         |          |
  |       | brute_hosts     |
  | 5     | certifiedhacker.com              |                |        |         |          |
  |       | brute_hosts     |
  | 6     | ftp.certifiedhacker.com          |                |        |         |          |
  |       | brute_hosts     |
  | 7     | ftp.certifiedhacker.com          | 162.241.216.11 |        |         |          |
  |       | brute_hosts     |
  | 8     | mail.certifiedhacker.com         |                |        |         |          |
```

26. Now, use the **back** command to go back to the CEH attributes terminal.

27. Now, that you have harvested several hosts, we will prepare a report containing all the hosts.

28. Execute **modules load reporting** command to view all the modules associated with the reporting keyword. In this lab, we will save the report in HTML format. So, the module used is **reporting/html**.

29. Run the **modules load reporting/html** command.

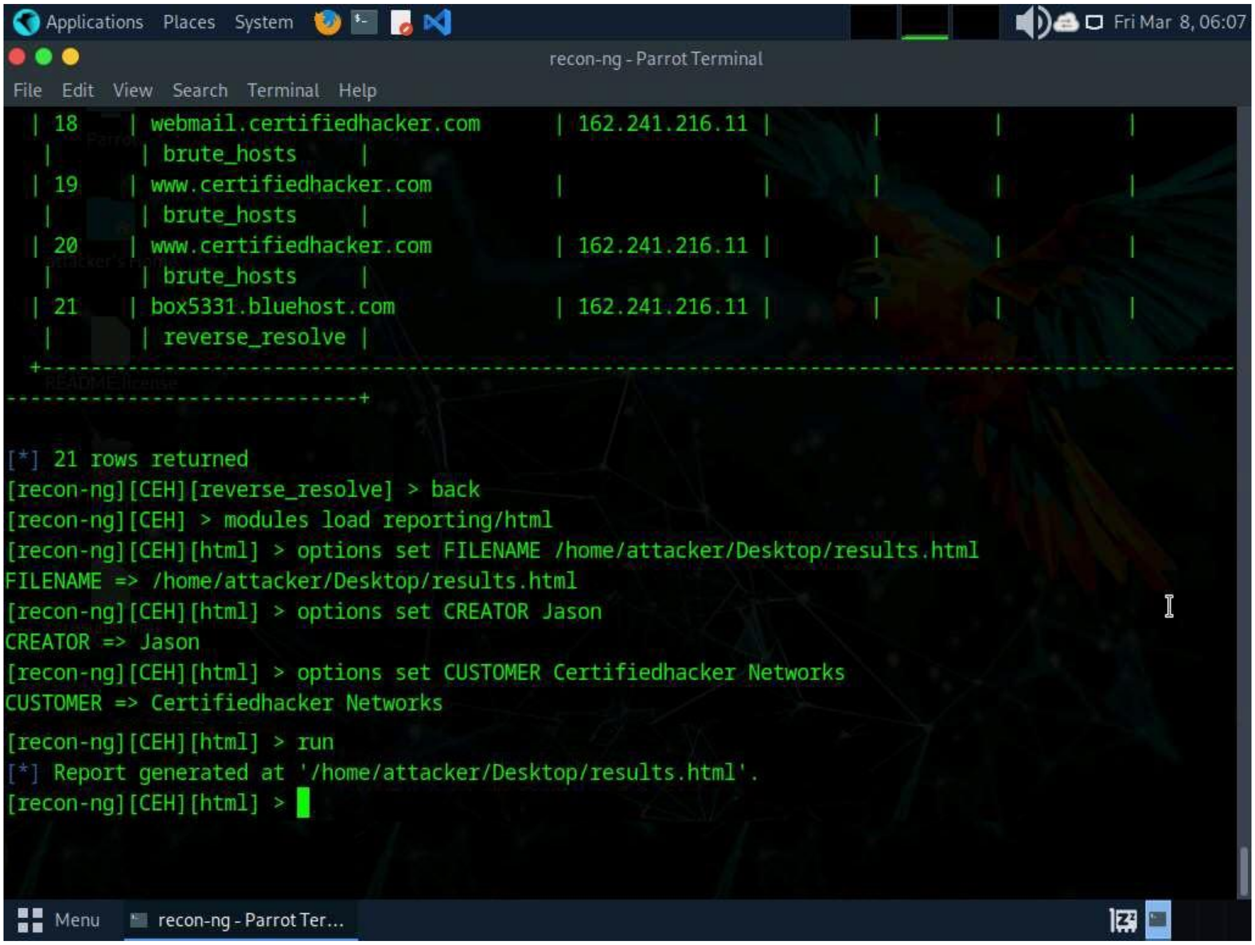
30. Observe that you need to assign values for **CREATOR** and **CUSTOMER** options while the **FILENAME** value is already set, and you may change the value if required. To do so, run the below commands:

    - **options set FILENAME /home/attacker/Desktop/results.html**. By issuing this command, you are setting the report name as **results.html** and the path to store the file as **Desktop**.

    - **options set CREATOR [your name]** (here, **Jason**).

    - **options set CUSTOMER Certifiedhacker Networks** (since you have performed network reconnaissance on **certifiedhacker.com** domain).

31. Use the **run** command and press **Enter** to create a report for all the hosts that have been harvested.

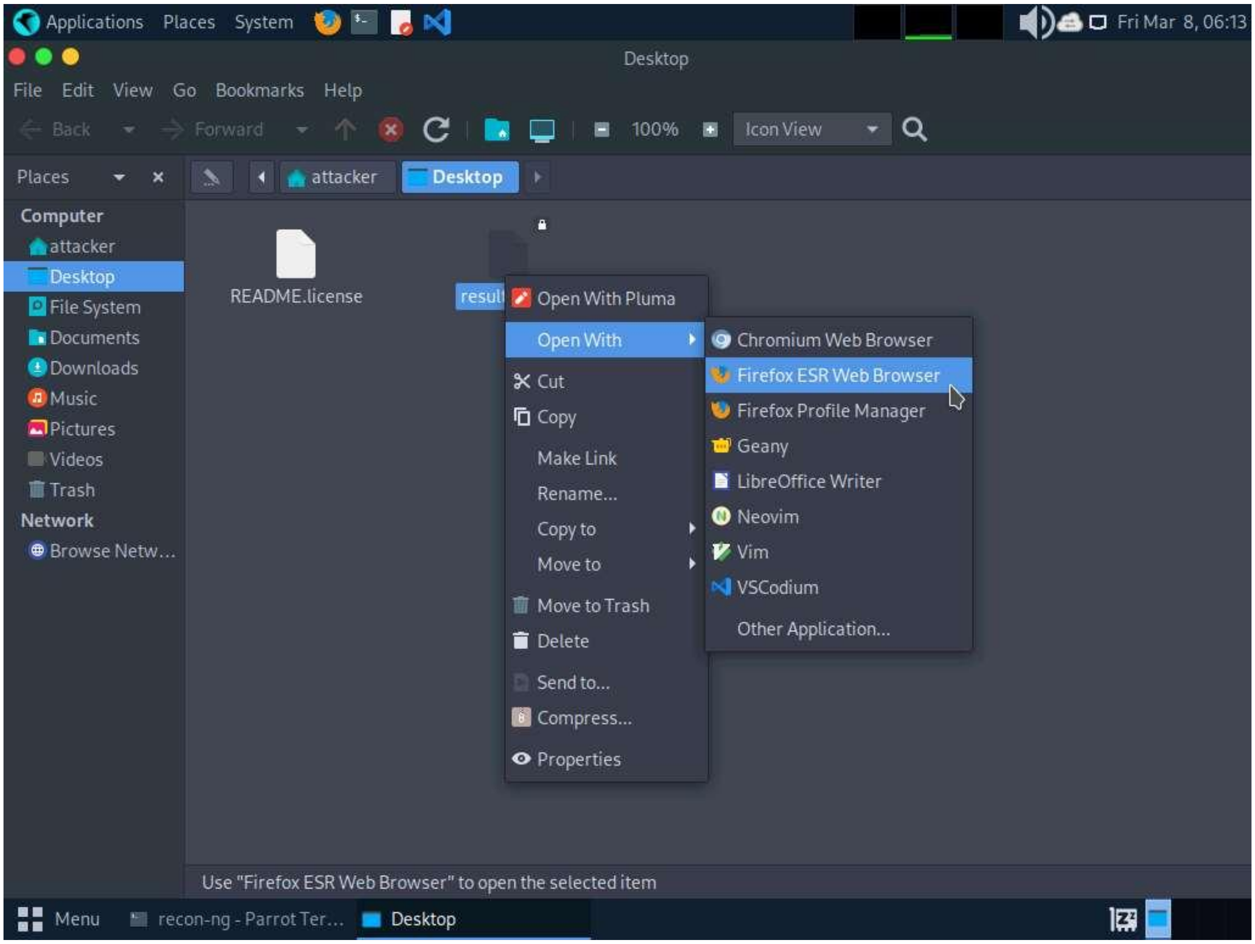


Applications Places System
Fri Mar 8, 06:07
recon-ng - Parrot Terminal
File Edit View Search Terminal Help
Menu
recon-ng - Parrot Ter...

```
  | 18    | webmail.certifiedhacker.com      | 162.241.216.11 |         |          |          |
   |       | brute_hosts      |
  | 19    | www.certifiedhacker.com          |                |         |          |          |
   |       | brute_hosts      |
  | 20    | www.certifiedhacker.com          | 162.241.216.11 |         |          |          |
   |       | brute_hosts      |
  | 21    | box5331.bluehost.com             | 162.241.216.11 |         |          |          |
   |       | reverse_resolve |
  +-----------------------------------------------------------------------------------------------------
-----------------------------+

[*] 21 rows returned
[recon-ng][CEH][reverse_resolve] > back
[recon-ng][CEH] > modules load reporting/html
[recon-ng][CEH][html] > options set FILENAME /home/attacker/Desktop/results.html
FILENAME => /home/attacker/Desktop/results.html
[recon-ng][CEH][html] > options set CREATOR Jason
CREATOR => Jason
[recon-ng][CEH][html] > options set CUSTOMER Certifiedhacker Networks
CUSTOMER => Certifiedhacker Networks
[recon-ng][CEH][html] > run
[*] Report generated at '/home/attacker/Desktop/results.html'.
[recon-ng][CEH][html] >
```

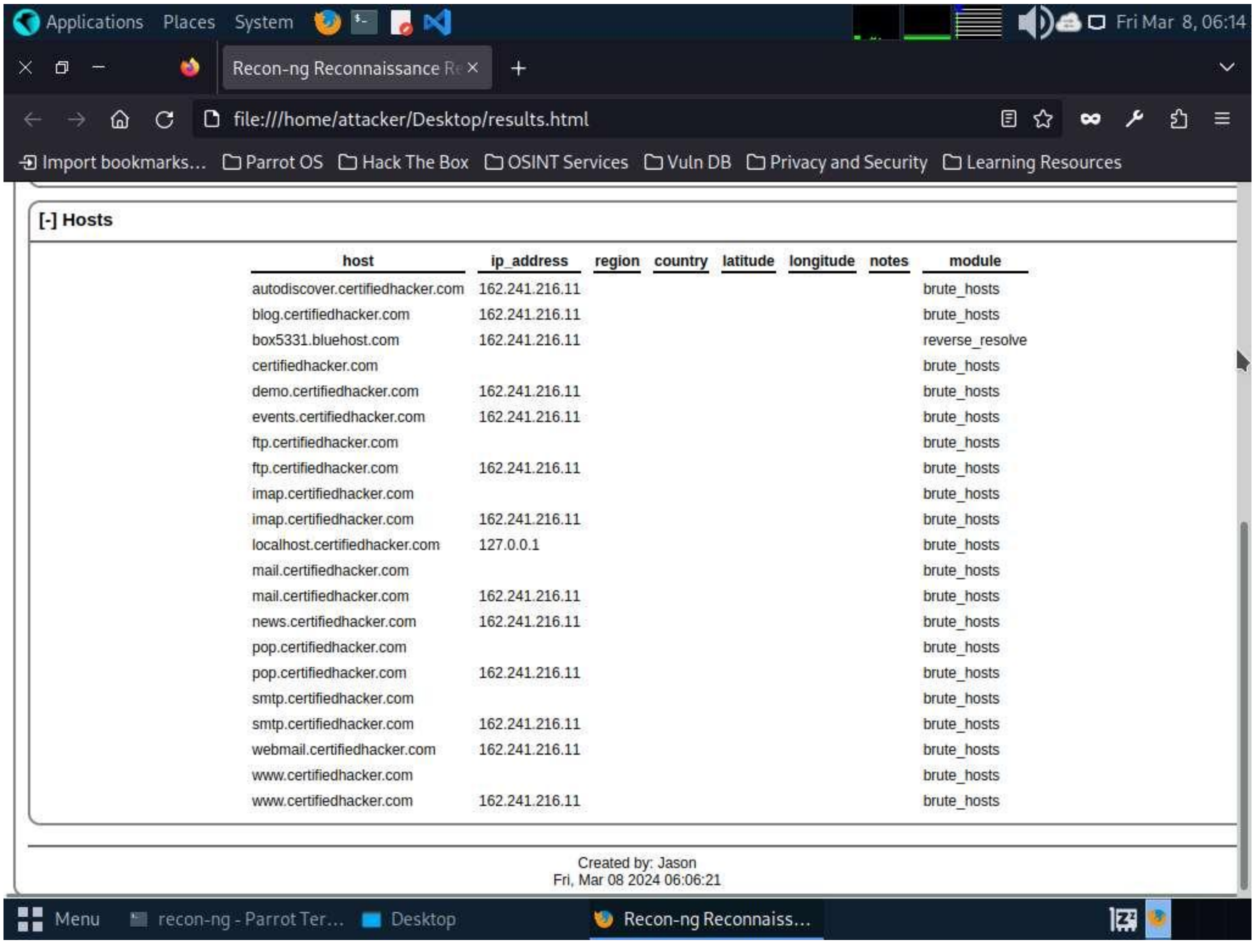
32. The generated report is saved to **/home/attacker/Desktop/**.

33. Navigate to **/home/attacker/Desktop/**, right-click on the **results.html** file, click on **Open With**, and select the **Firefox ESR Web Browser** browser from the available options.



34. The generated report appears in the **Firefox** browser, displaying the summary of the harvested hosts.

35. You can expand the **Hosts** node to view all the harvested hosts, as shown in the screenshot.



[-] Hosts

host	ip_address	region	country	latitude	longitude	notes	module
autodiscover.certifiedhacker.com	162.241.216.11						brute_hosts
blog.certifiedhacker.com	162.241.216.11						brute_hosts
box5331.bluehost.com	162.241.216.11						reverse_resolve
certifiedhacker.com							brute_hosts
demo.certifiedhacker.com	162.241.216.11						brute_hosts
events.certifiedhacker.com	162.241.216.11						brute_hosts
ftp.certifiedhacker.com							brute_hosts
ftp.certifiedhacker.com	162.241.216.11						brute_hosts
imap.certifiedhacker.com							brute_hosts
imap.certifiedhacker.com	162.241.216.11						brute_hosts
localhost.certifiedhacker.com	127.0.0.1						brute_hosts
mail.certifiedhacker.com							brute_hosts
mail.certifiedhacker.com	162.241.216.11						brute_hosts
news.certifiedhacker.com	162.241.216.11						brute_hosts
pop.certifiedhacker.com							brute_hosts
pop.certifiedhacker.com	162.241.216.11						brute_hosts
smtp.certifiedhacker.com							brute_hosts
smtp.certifiedhacker.com	162.241.216.11						brute_hosts
webmail.certifiedhacker.com	162.241.216.11						brute_hosts
www.certifiedhacker.com							brute_hosts
www.certifiedhacker.com	162.241.216.11						brute_hosts

Created by: Jason
Fri, Mar 08 2024 06:06:21

36. Close all open windows.

37. Until now, we have used the Recon-ng tool to perform network reconnaissance on a target domain

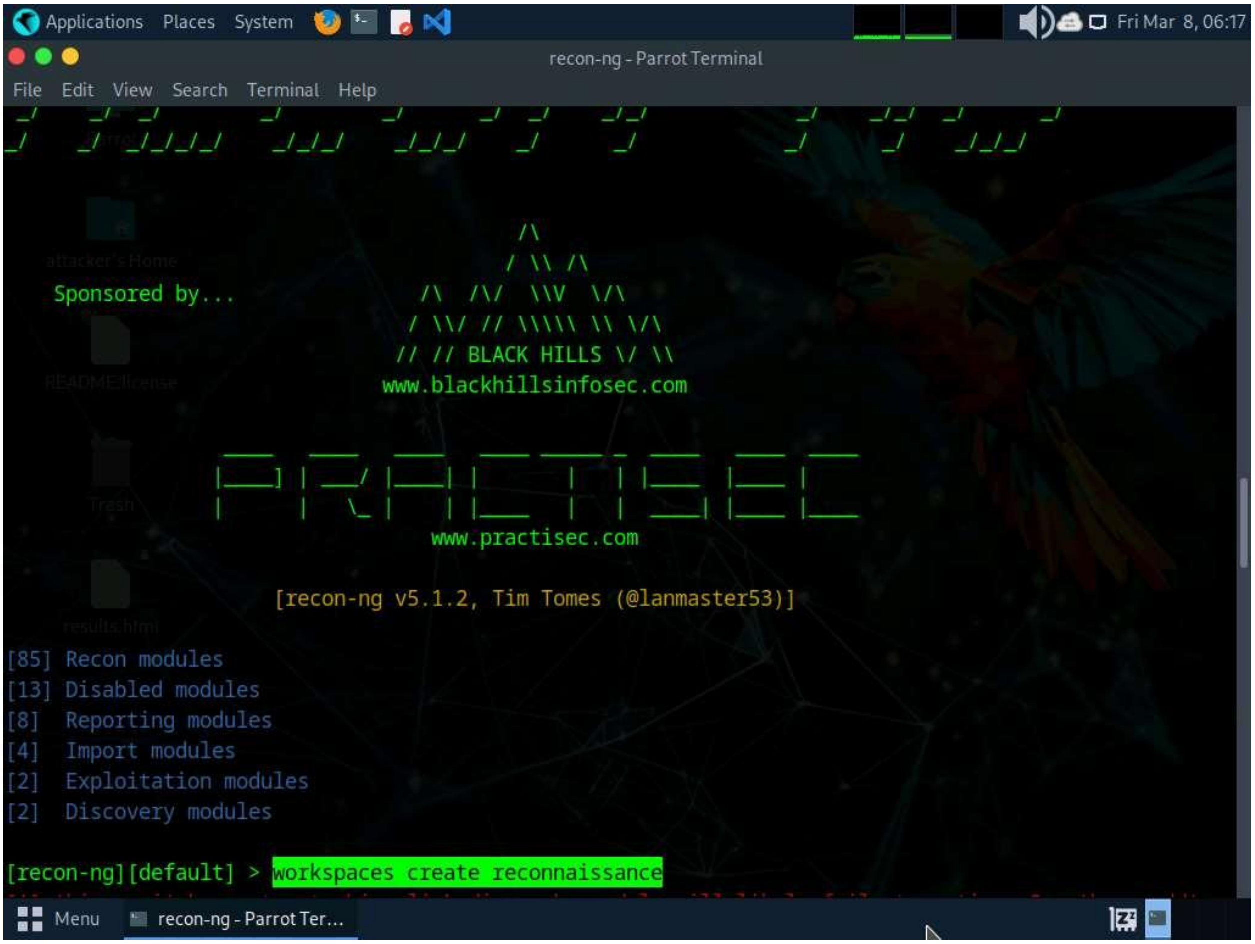
38. Now, we will use Recon-ng to gather personnel information.

39. Open a **Terminal** window and execute **sudo su** to run the programs as a root user (When prompted, enter the password **toor**).

The password that you type will not be visible.

40. Run **cd** command to jump to the root directory and run **recon-ng** command.

41. Add a workspace by issuing the command **workspaces create reconnaissance** and press **Enter**. This creates a workspace named reconnaissance.


Applications Places System
Fri Mar 8, 06:17
recon-ng - Parrot Terminal
File Edit View Search Terminal Help
Menu
recon-ng - Parrot Ter...

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

                              www.practisec.com

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

[85] Recon modules
[13] Disabled modules
[8]  Reporting modules
[4]  Import modules
[2]  Exploitation modules
[2]  Discovery modules

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

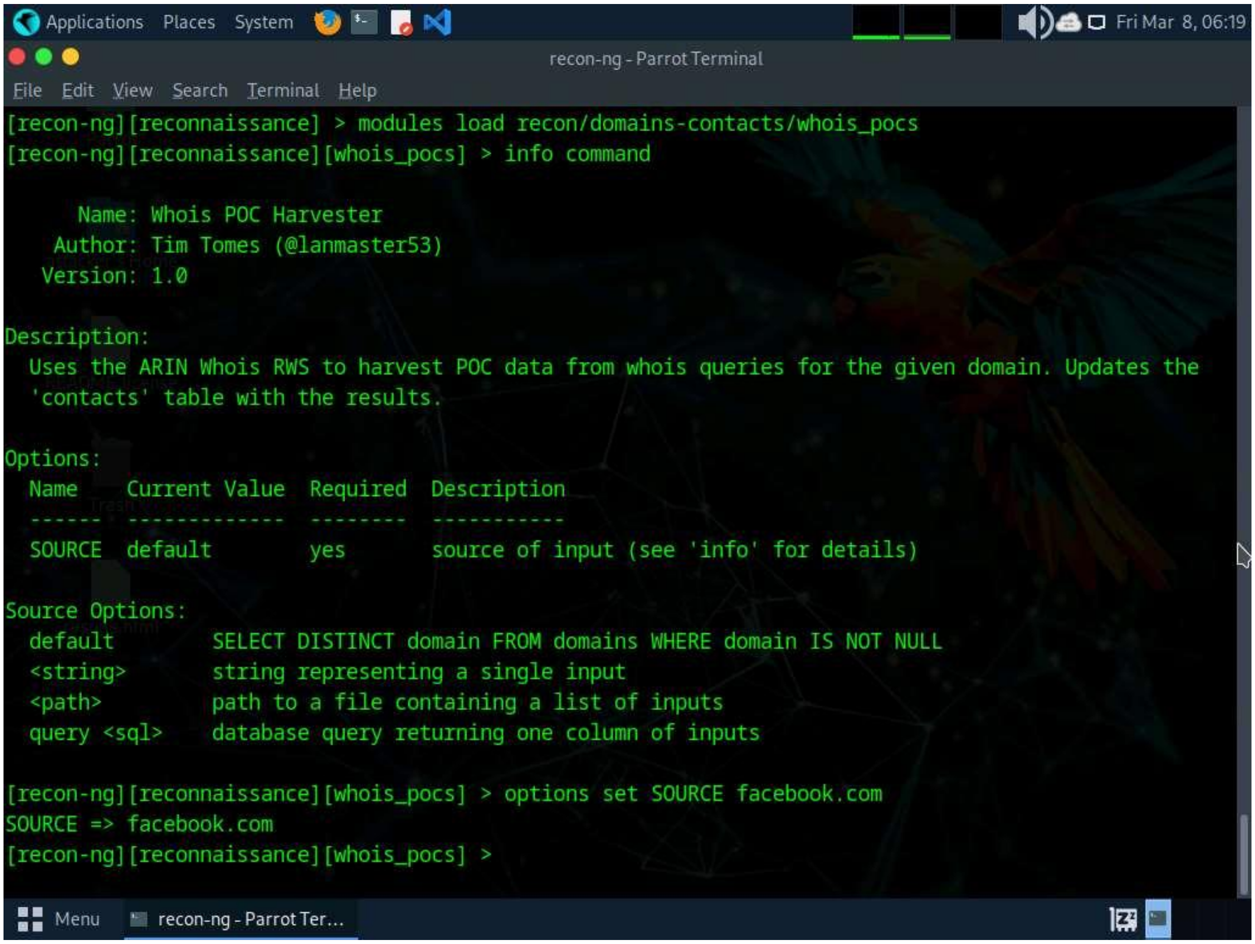
42. Set a domain and perform footprinting on it to extract contacts available in the domain.

43. Execute **modules load recon/domains-contacts/whois_pocs** command. This module uses the ARIN Whois RWS to harvest POC data from Whois queries for the given domain.

44. Run the **info command** command to view the options required to run this module.

45. Run **options set SOURCE facebook.com** command to add facebook.com as a target domain.

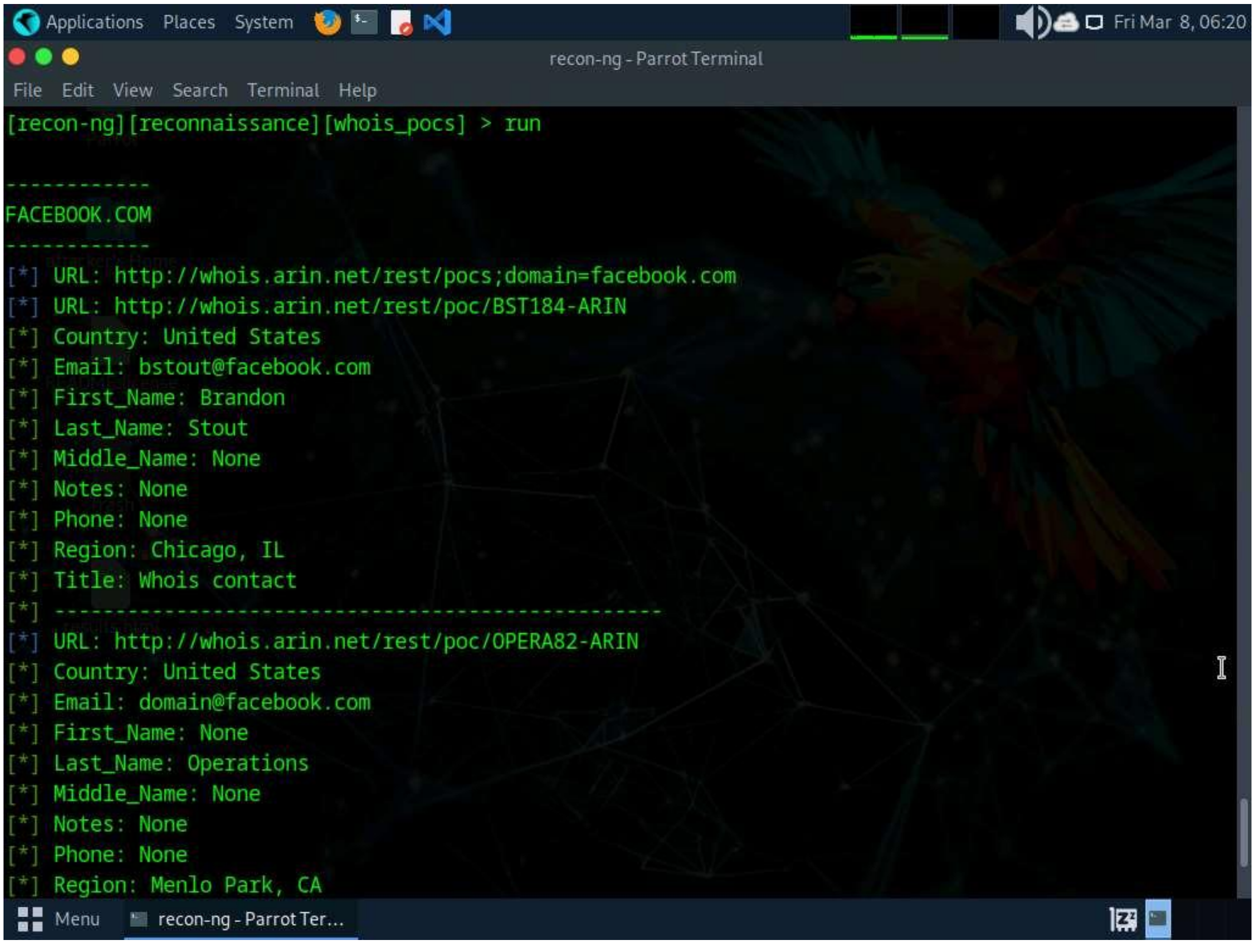
Here, we are using facebook.com as a target domain to gather contact details.



```
[recon-ng][reconnaissance] > modules load recon/domains-contacts/whois_pocs
[recon-ng][reconnaissance][whois_pocs] > info command

      Name: Whois POC Harvester
    Author: Tim Tomes (@lanmaster53)
   Version: 1.0

Description:
  Uses the ARIN Whois RWS to harvest POC data from whois queries for the given domain. Updates 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][reconnaissance][whois_pocs] > options set SOURCE facebook.com
SOURCE => facebook.com
[recon-ng][reconnaissance][whois_pocs] >
```

46. Execute the **run** command. The **recon/domains-contacts/whois_pocs** module extracts the contacts associated with the domain and displays them, as shown in the screenshot

Results might differ when you perform the lab.


Applications Places System
Fri Mar 8, 06:20
recon-ng - Parrot Terminal
File Edit View Search Terminal Help
Menu
recon-ng - Parrot Ter...

```
[recon-ng][reconnaissance][whois_pocs] > run

------------
FACEBOOK.COM
------------
[*] URL: http://whois.arin.net/rest/pocs;domain=facebook.com
[*] URL: http://whois.arin.net/rest/poc/BST184-ARIN
[*] Country: United States
[*] Email: bstout@facebook.com
[*] First_Name: Brandon
[*] Last_Name: Stout
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Chicago, IL
[*] Title: Whois contact
[*] --------------------------------------------------
[*] URL: http://whois.arin.net/rest/poc/OPERA82-ARIN
[*] Country: United States
[*] Email: domain@facebook.com
[*] First_Name: None
[*] Last_Name: Operations
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Menlo Park, CA
```

47. Until now, we have obtained contacts related to the domains. Note down these contacts' names. Close all the open windows.

48. Now, we will use Recon-ng to extract a list of subdomains and IP addresses associated with the target URL.

49. Open a **Terminal** window and execute **sudo su** to run the programs as a root user (When prompted, enter the password **toor**).

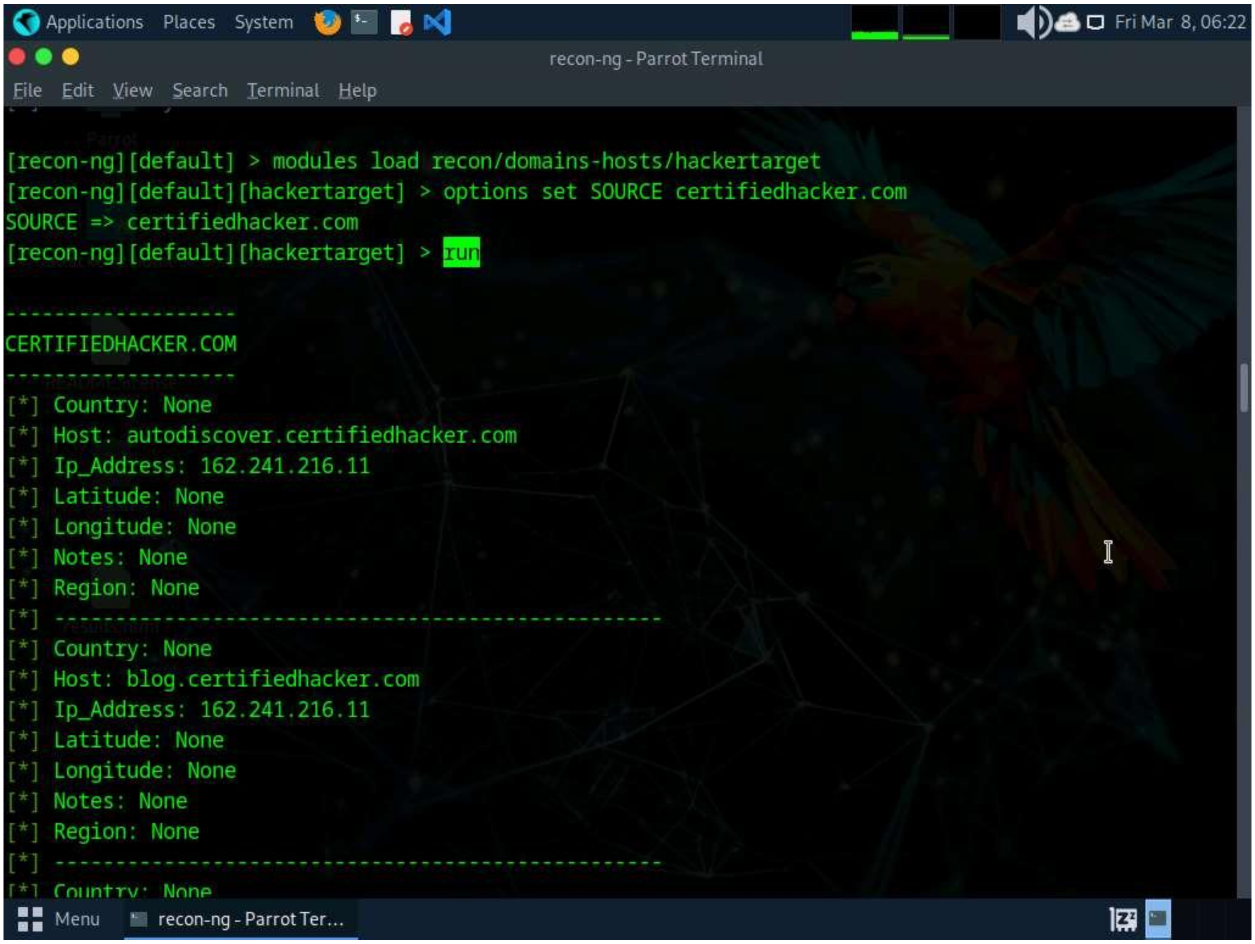
The password that you type will not be visible.

50. Now, run **cd** command to jump to the root directory and run **recon-ng** command.

51. To extract a list of subdomains and IP addresses associated with the target URL, we need to load the **recon/domains-hosts/hackertarget** module.

52. Run the **modules load recon/domains-hosts/hackertarget** command and run **options set SOURCE certifiedhacker.com** command.

53. Execute the **run** command. The **recon/domains-hosts/hackertarget** module searches for list of subdomains and IP addresses associated with the target URL and returns the list of subdomains and their IP addresses.



```
[recon-ng][default] > modules load recon/domains-hosts/hackertarget
[recon-ng][default][hackertarget] > options set SOURCE certifiedhacker.com
SOURCE => certifiedhacker.com
[recon-ng][default][hackertarget] > run

-------------------
CERTIFIEDHACKER.COM
-------------------
[*] Country: None
[*] Host: autodiscover.certifiedhacker.com
[*] Ip_Address: 162.241.216.11
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] --------------------------------------------------
[*] Country: None
[*] Host: blog.certifiedhacker.com
[*] Ip_Address: 162.241.216.11
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] --------------------------------------------------
[*] Country: None
```

54. This concludes the demonstration of gathering host information of the target domain and gathering personnel information of a target organization.

55. Close all open windows and document all the acquired information.