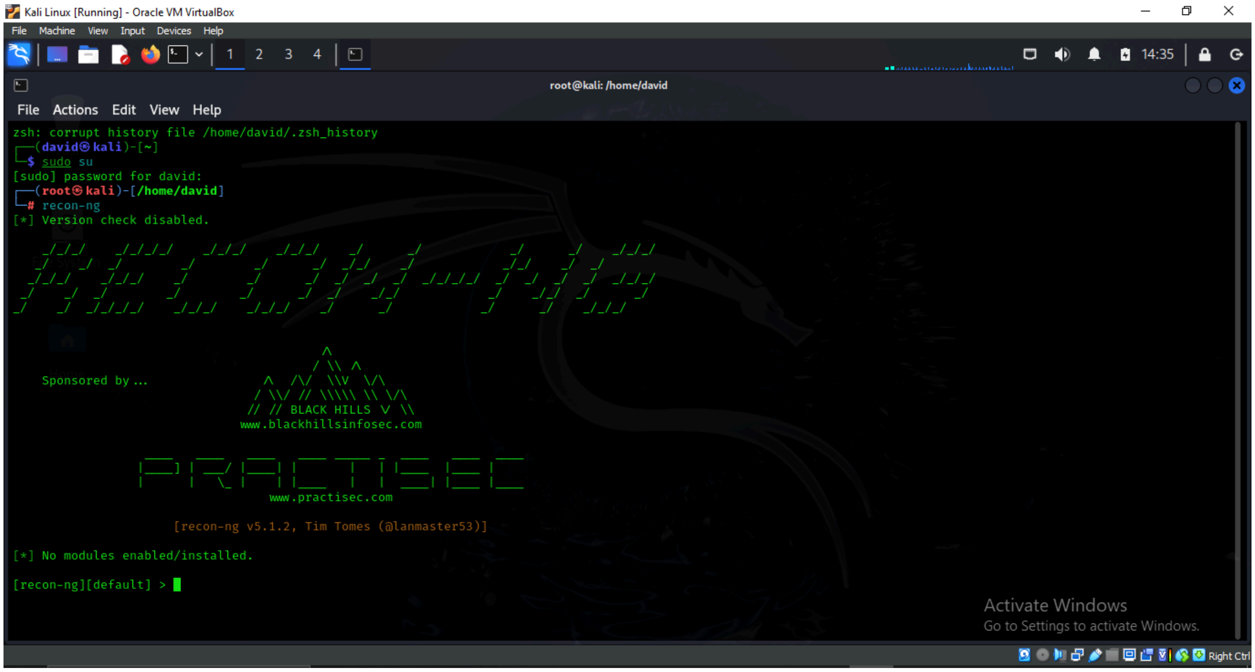
LAB 3:

RECON-NG

WHOIS information can consist of location, registration and expire dates, contact information (email, phone numbers, etc.) and more about domain-name. The purpose of this lab is to use recon-ng to automate the discovery of this information.

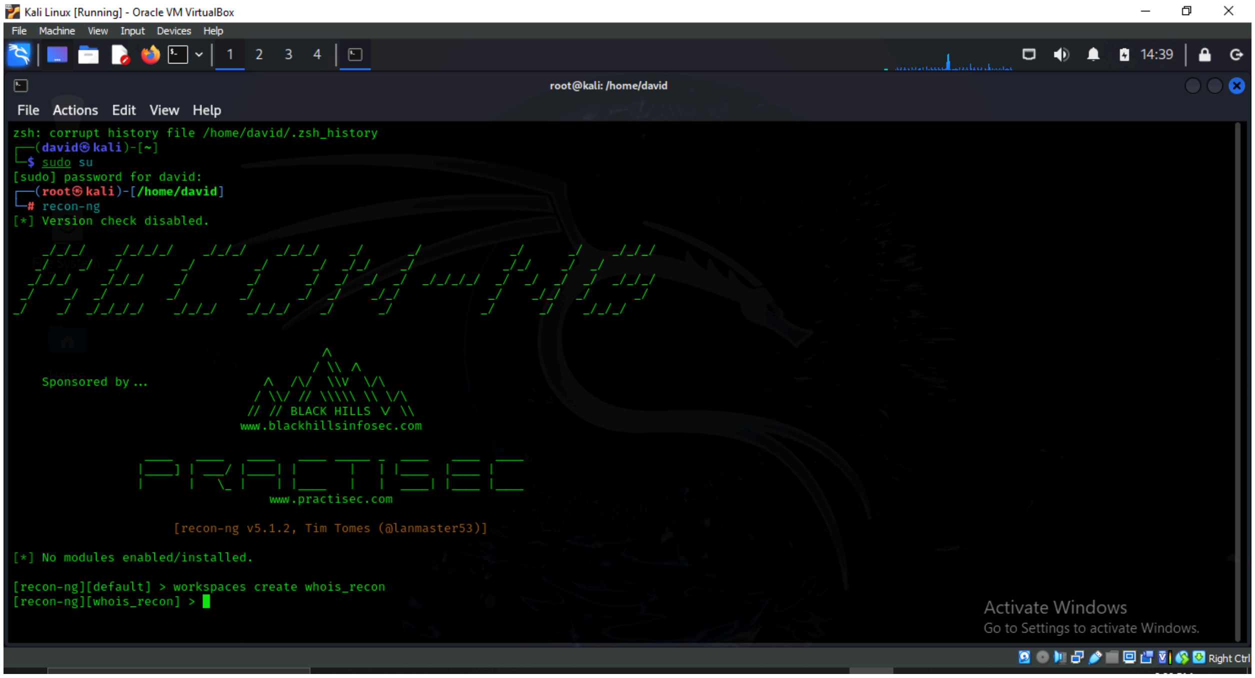
TOOL: KALI LINUX

STEP 1: Open a terminal, switch to root user with sudo su, then type recon-ng



```
zsh: corrupt history file /home/david/.zsh_history
┌──(david㉿kali)-[~]
└─$ sudo su
[sudo] password for david:
┌──(root㉿kali)-[/home/david]
└─# recon-ng
[*] Version check disabled.

    _/_/_/    _/_/_/_/    _/_/_/    _/_/_/    _/      _/            _/      _/    _/_/_/
   _/    _/  _/        _/        _/      _/  _/_/    _/            _/_/    _/  _/
  _/_/_/    _/_/_/    _/        _/      _/  _/  _/  _/  _/_/_/_/  _/  _/  _/  _/  _/_/_/
 _/    _/  _/        _/        _/      _/  _/    _/_/            _/    _/_/  _/      _/
_/    _/  _/_/_/_/    _/_/_/    _/_/_/    _/      _/            _/      _/    _/_/_/


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

                  ____   ____   ____   ____   _____ _   ____   ____   ____
                 |____] | ___/ |____| |       |   | |   |____  |____  |
                 |      |    \_ |    | |____   |   | |   ____| |____  |____
                                   www.practisec.com

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

[*] No modules enabled/installed.

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

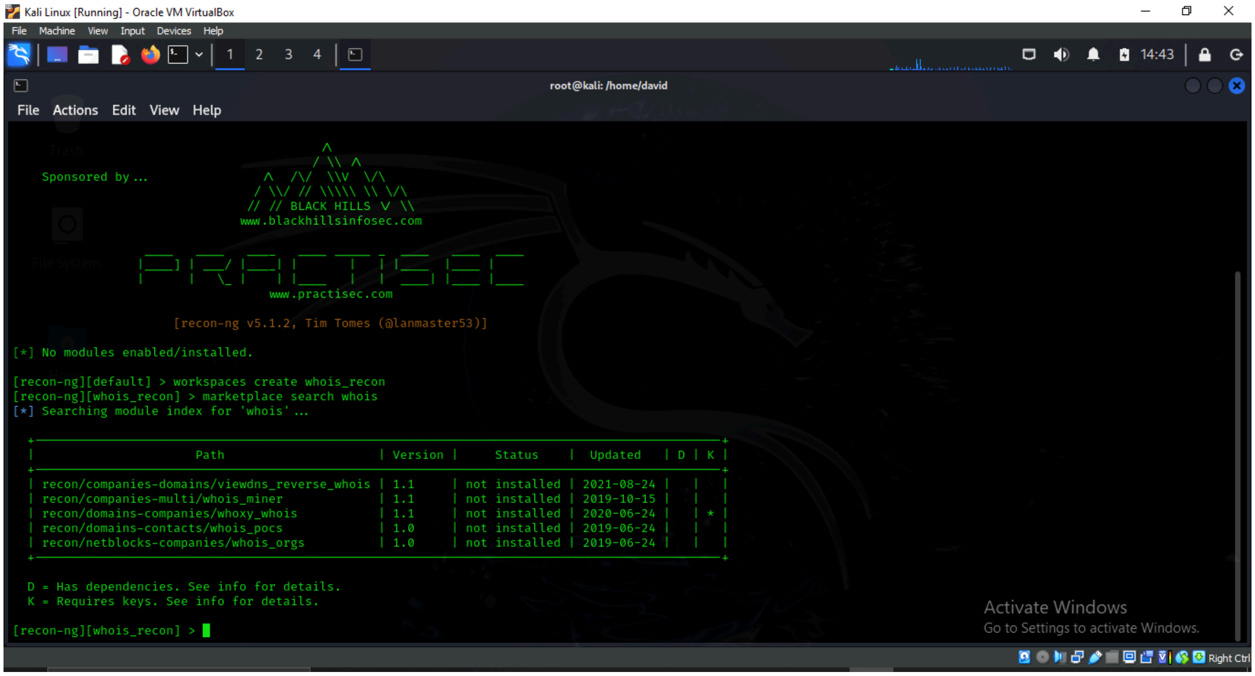
STEP 2: Create a new lab by typing the following: workspaces create whois_recon



Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/david
File Actions Edit View Help
14:39
Activate Windows
Go to Settings to activate Windows.
Right Ctrl

```
zsh: corrupt history file /home/david/.zsh_history
┌──(david㉿kali)-[~]
└─$ sudo su
[sudo] password for david:
┌──(root㉿kali)-[/home/david]
└─# recon-ng
[*] Version check disabled.

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

                             www.practisec.com

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

[*] No modules enabled/installed.

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

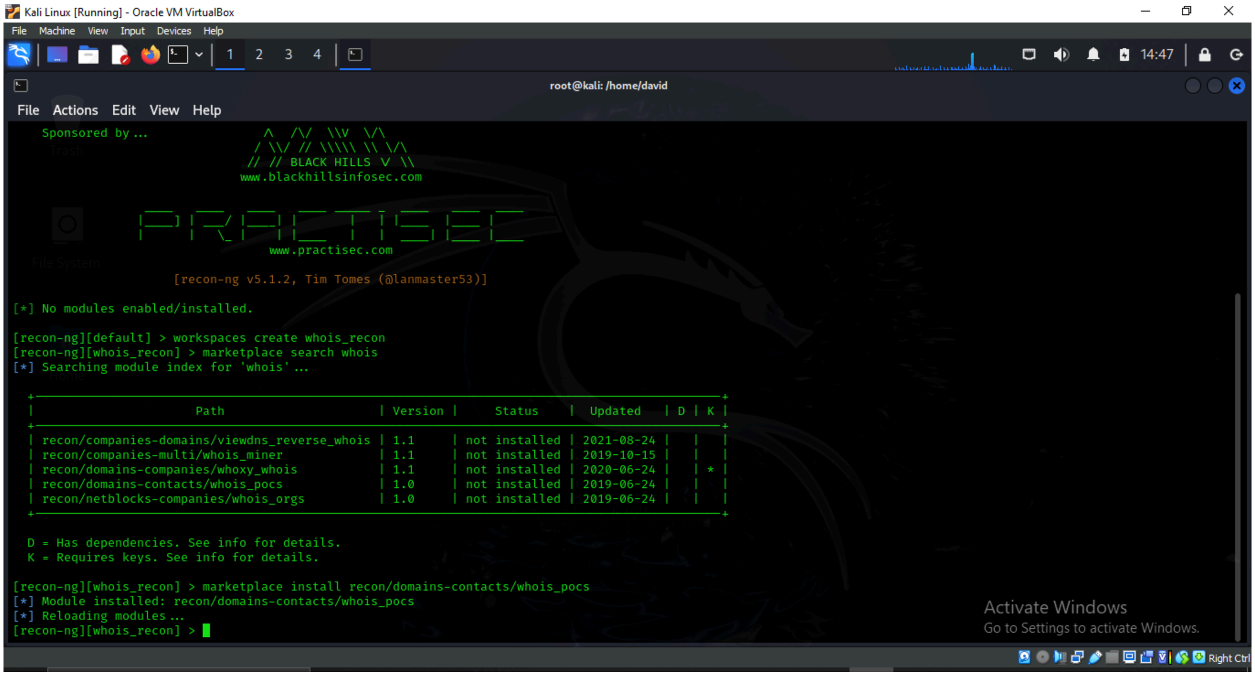
STEP 3: Install the WHOIS search module. Type : marketplace search whois



Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/david
File Actions Edit View Help
14:43
Activate Windows
Go to Settings to activate Windows.
Right Ctrl

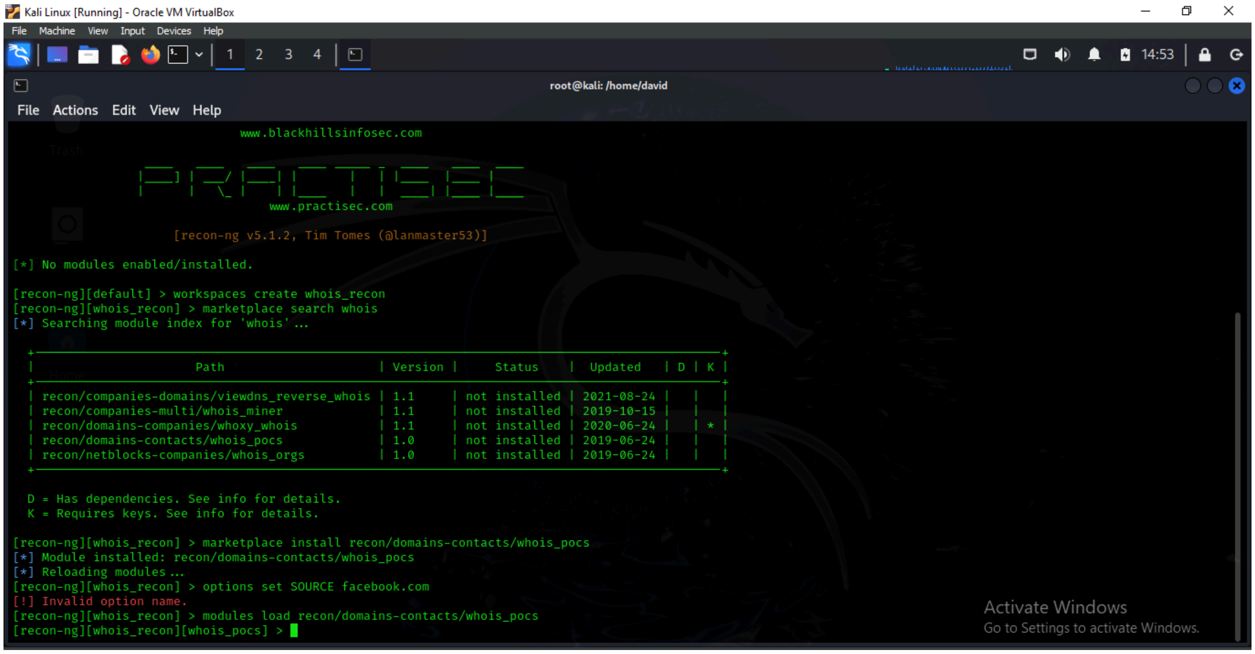
```
                                          /\
                                         / \\ /\
    Sponsored by ...         /\  /\/  \\V  \/\
                            / \\/ // \\\\\ \\ \/\
                           // // BLACK HILLS \/ \\
                          www.blackhillsinfosec.com

                             www.practisec.com

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

[*] No modules enabled/installed.

[recon-ng][default] > workspaces create whois_recon
[recon-ng][whois_recon] > marketplace search whois
[*] Searching module index for 'whois'...

  +-----------------------------------------------------------------------------------------------+
  |                        Path                          | Version |     Status    |  Updated   | D | K |
  +-----------------------------------------------------------------------------------------------+
  | recon/companies-domains/viewdns_reverse_whois | 1.1     | not installed | 2021-08-24 |   |   |
  | recon/companies-multi/whois_miner             | 1.1     | not installed | 2019-10-15 |   |   |
  | recon/domains-companies/whoxy_whois           | 1.1     | not installed | 2020-06-24 |   | * |
  | recon/domains-contacts/whois_pocs             | 1.0     | not installed | 2019-06-24 |   |   |
  | recon/netblocks-companies/whois_orgs          | 1.0     | not installed | 2019-06-24 |   |   |
  +-----------------------------------------------------------------------------------------------+

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

[recon-ng][whois_recon] >
```

STEP 4:We want to install the fourth option, which is “recon/domains-contacts/whois_pocs”. To do this, type: marketplace install recon/domains-contacts/whois_pocs


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
14:47
root@kali: /home/david
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.
Right Ctrl

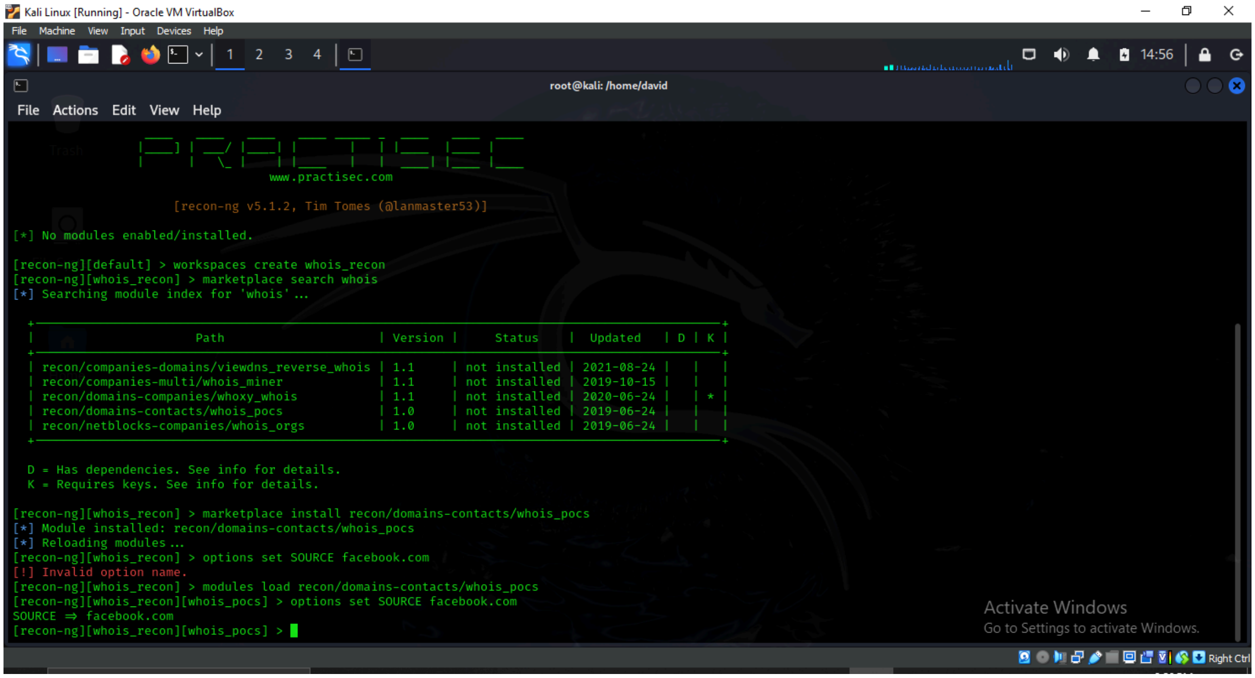
```
    Sponsored by ...                ^  /\/  \\V  \/\
                                   / \\/ // \\\\\ \\ \/\
                                  // // BLACK HILLS  V  \\
                                 www.blackhillsinfosec.com

                  ____   ____   ____   ____   _____ _  ____   ____   ____
                 |____] |___/  |____| |         |   | |____  |____  |
                 |      |   \_ |    | |____     |   | ____|  |____  |____
                                     www.practisec.com

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

[*] No modules enabled/installed.

[recon-ng][default] > workspaces create whois_recon
[recon-ng][whois_recon] > marketplace search whois
[*] Searching module index for 'whois'...

  +-----------------------------------------------------------------------------------------------+
  |                      Path                      | Version |     Status    |  Updated   | D | K |
  +-----------------------------------------------------------------------------------------------+
  | recon/companies-domains/viewdns_reverse_whois  | 1.1     | not installed | 2021-08-24 |   |   |
  | recon/companies-multi/whois_miner              | 1.1     | not installed | 2019-10-15 |   |   |
  | recon/domains-companies/whoxy_whois            | 1.1     | not installed | 2020-06-24 |   | * |
  | recon/domains-contacts/whois_pocs              | 1.0     | not installed | 2019-06-24 |   |   |
  | recon/netblocks-companies/whois_orgs           | 1.0     | not installed | 2019-06-24 |   |   |
  +-----------------------------------------------------------------------------------------------+

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

[recon-ng][whois_recon] > marketplace install recon/domains-contacts/whois_pocs
[*] Module installed: recon/domains-contacts/whois_pocs
[*] Reloading modules...
[recon-ng][whois_recon] >
```

STEP 5: To load the module for use, type: modules load recon/domains-contacts/whois_pocs


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
14:53
root@kali: /home/david
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.

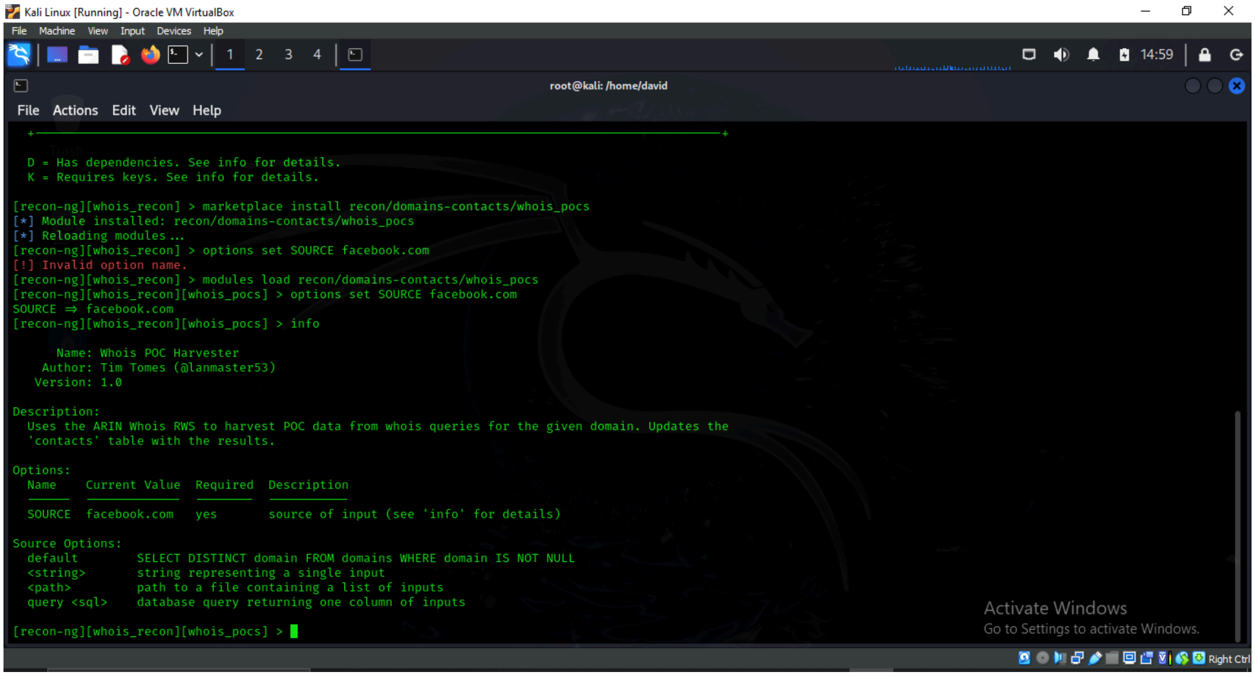
```
                    www.blackhillsinfosec.com

                         www.practisec.com

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

[*] No modules enabled/installed.

[recon-ng][default] > workspaces create whois_recon
[recon-ng][whois_recon] > marketplace search whois
[*] Searching module index for 'whois'...

  +---------------------------------------------------------------------------------------+
  |                      Path                      | Version |     Status    |  Updated   | D | K |
  +---------------------------------------------------------------------------------------+
  | recon/companies-domains/viewdns_reverse_whois | 1.1     | not installed | 2021-08-24 |   |   |
  | recon/companies-multi/whois_miner             | 1.1     | not installed | 2019-10-15 |   |   |
  | recon/domains-companies/whoxy_whois           | 1.1     | not installed | 2020-06-24 |   | * |
  | recon/domains-contacts/whois_pocs             | 1.0     | not installed | 2019-06-24 |   |   |
  | recon/netblocks-companies/whois_orgs          | 1.0     | not installed | 2019-06-24 |   |   |
  +---------------------------------------------------------------------------------------+

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

[recon-ng][whois_recon] > marketplace install recon/domains-contacts/whois_pocs
[*] Module installed: recon/domains-contacts/whois_pocs
[*] Reloading modules...
[recon-ng][whois_recon] > options set SOURCE facebook.com
[!] Invalid option name.
[recon-ng][whois_recon] > modules load recon/domains-contacts/whois_pocs
[recon-ng][whois_recon][whois_pocs] >
```

STEP 6: To begin searching, we first need to set the source by typing: options set SOURCE facebook.com


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
14:56
root@kali: /home/david
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.
Right Ctrl

```
                         www.practisec.com

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

[*] No modules enabled/installed.

[recon-ng][default] > workspaces create whois_recon
[recon-ng][whois_recon] > marketplace search whois
[*] Searching module index for 'whois'...

  +---------------------------------------------------------------------------------------+
  |                      Path                      | Version |     Status    |  Updated   | D | K |
  +---------------------------------------------------------------------------------------+
  | recon/companies-domains/viewdns_reverse_whois | 1.1     | not installed | 2021-08-24 |   |   |
  | recon/companies-multi/whois_miner             | 1.1     | not installed | 2019-10-15 |   |   |
  | recon/domains-companies/whoxy_whois           | 1.1     | not installed | 2020-06-24 |   | * |
  | recon/domains-contacts/whois_pocs             | 1.0     | not installed | 2019-06-24 |   |   |
  | recon/netblocks-companies/whois_orgs          | 1.0     | not installed | 2019-06-24 |   |   |
  +---------------------------------------------------------------------------------------+

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

[recon-ng][whois_recon] > marketplace install recon/domains-contacts/whois_pocs
[*] Module installed: recon/domains-contacts/whois_pocs
[*] Reloading modules...
[recon-ng][whois_recon] > options set SOURCE facebook.com
[!] Invalid option name.
[recon-ng][whois_recon] > modules load recon/domains-contacts/whois_pocs
[recon-ng][whois_recon][whois_pocs] > options set SOURCE facebook.com
SOURCE ⇒ facebook.com
[recon-ng][whois_recon][whois_pocs] >
```

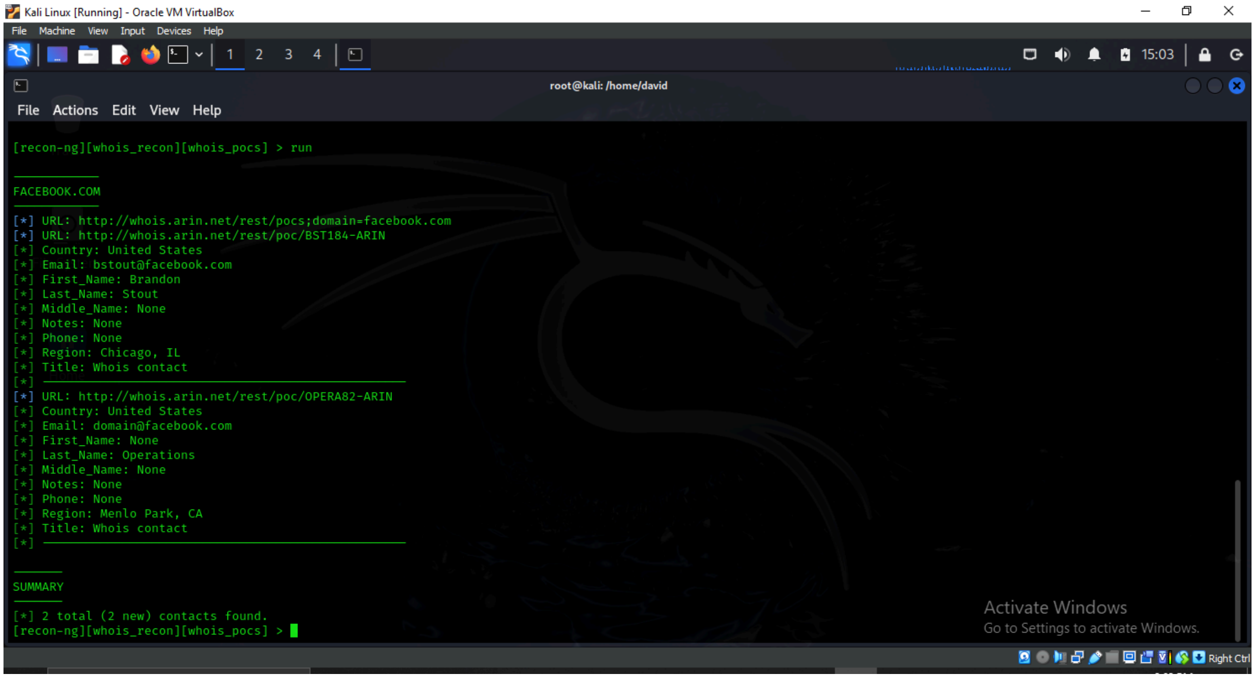
STEP 7: To see information about this module and how it is used, type “info” and hit enter.



Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
14:59
root@kali: /home/david
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.
Right Ctrl

```
  +─────────────────────────────────────────────────────────────────────────────────+

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

[recon-ng][whois_recon] > marketplace install recon/domains-contacts/whois_pocs
[*] Module installed: recon/domains-contacts/whois_pocs
[*] Reloading modules ...
[recon-ng][whois_recon] > options set SOURCE facebook.com
[!] Invalid option name.
[recon-ng][whois_recon] > modules load recon/domains-contacts/whois_pocs
[recon-ng][whois_recon][whois_pocs] > options set SOURCE facebook.com
SOURCE ⇒ facebook.com
[recon-ng][whois_recon][whois_pocs] > info

      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  facebook.com   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][whois_recon][whois_pocs] > 
```

STEP 8: To search WHOIS for information regarding “facebook.com”. Simply type “run” and hit enter to begin the search.

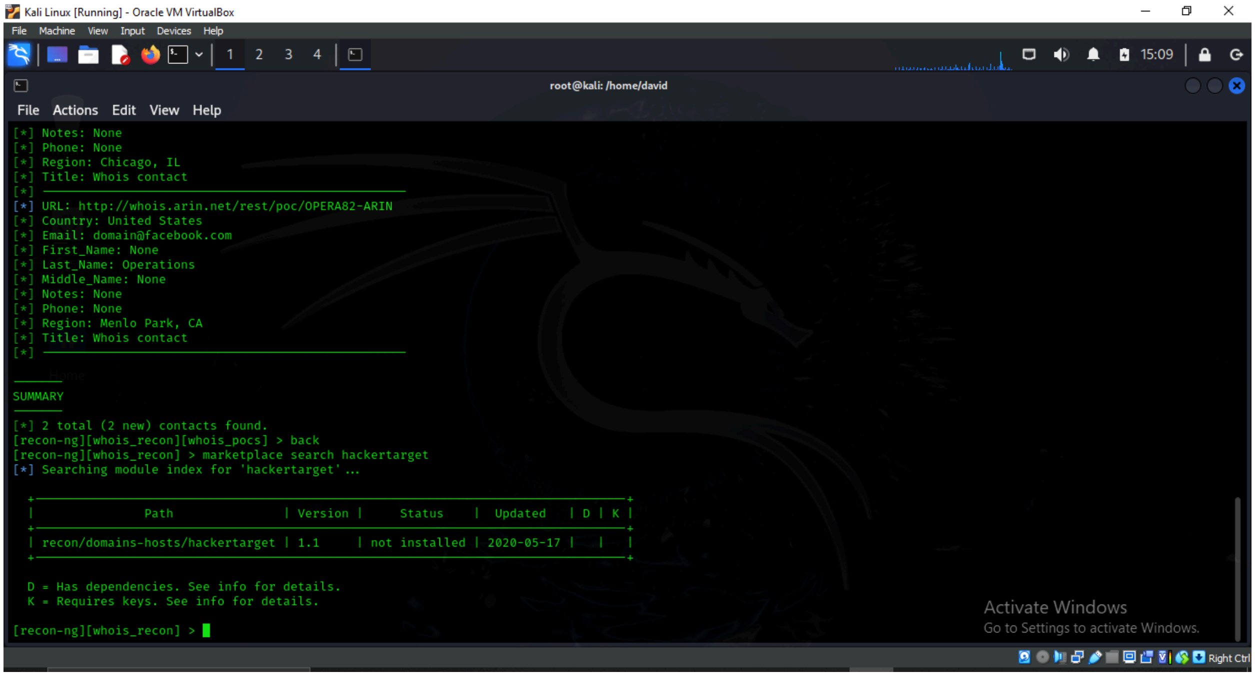


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
15:03
root@kali: /home/david
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.
Right Ctrl

```
[recon-ng][whois_recon][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
[*] Title: Whois contact
[*] ──────────────────────────────────────────────────

───────
SUMMARY
───────
[*] 2 total (2 new) contacts found.
[recon-ng][whois_recon][whois_pocs] > 
```

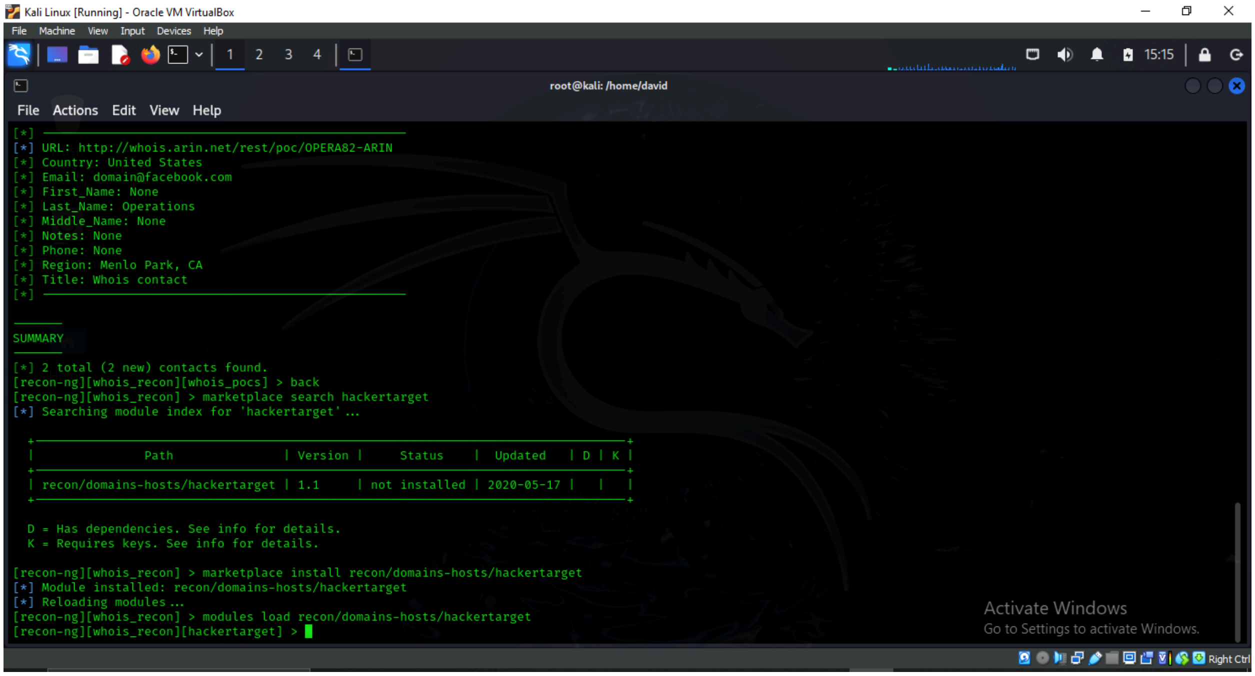
STEP 9: We will attempt to discover as many subdomains as possible, with their IPv4 address for facebook.com, using HackerTarget.com API. We will need to import the “hackertarget” module.
Before we do this, we would type “back” and press enter to quit out of the whois_pocs module.
We will begin by searching the marketplace for “hackertarget” modules using:

marketplace search hackertarget


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
15:09
root@kali: /home/david
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.
Right Ctrl

```
[*] 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
[*] Title: Whois contact
[*] ──────────────────────────────────────────────────

───────
SUMMARY
───────
[*] 2 total (2 new) contacts found.
[recon-ng][whois_recon][whois_pocs] > back
[recon-ng][whois_recon] > marketplace search hackertarget
[*] Searching module index for 'hackertarget'...

  +--------------------------------------------------------------------------------+
  |               Path                | Version |     Status    |  Updated   | D | K |
  +--------------------------------------------------------------------------------+
  | recon/domains-hosts/hackertarget | 1.1     | not installed | 2020-05-17 |   |   |
  +--------------------------------------------------------------------------------+

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

[recon-ng][whois_recon] >
```

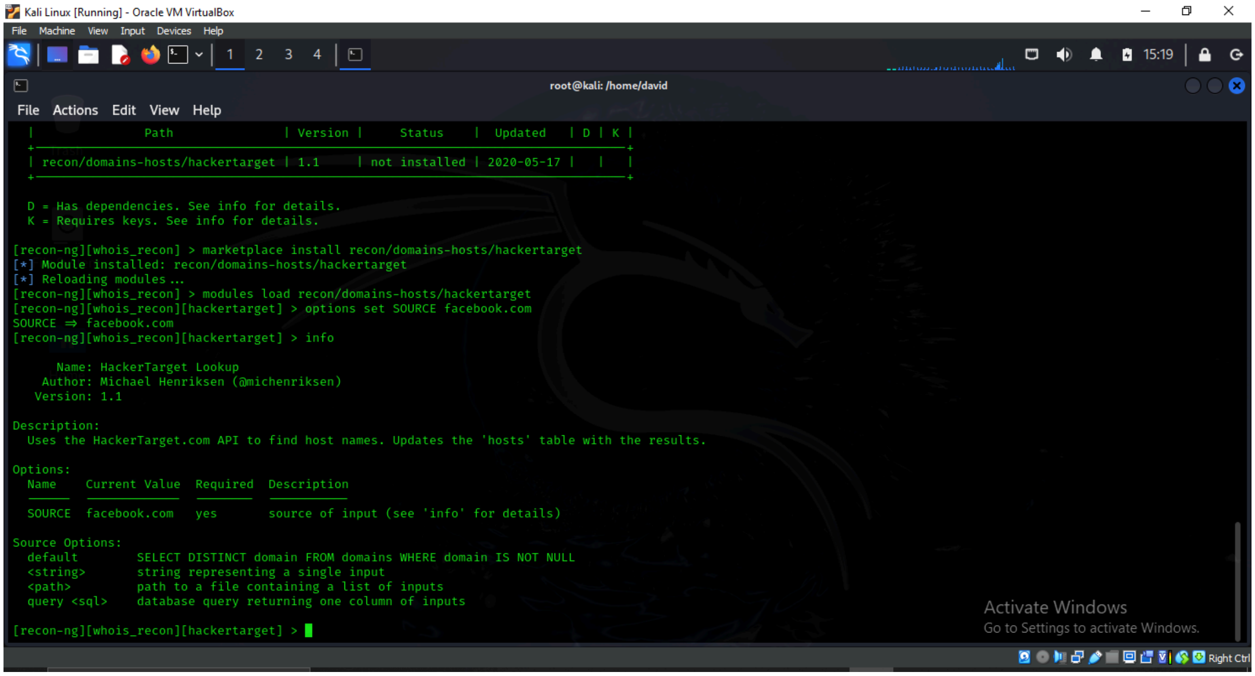
STEP 10:To install the module use: marketplace install recon/domains-hosts/hackertarget
Then load the module using: modules load recon/domains-hosts/hackertarget


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
15:15
root@kali: /home/david
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.
Right Ctrl

```
[*] ────────────────────────────────────────────────────
[*] 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
[*] Title: Whois contact
[*] ────────────────────────────────────────────────────

───────
SUMMARY
───────
[*] 2 total (2 new) contacts found.
[recon-ng][whois_recon][whois_pocs] > back
[recon-ng][whois_recon] > marketplace search hackertarget
[*] Searching module index for 'hackertarget'...

  +────────────────────────────────────────────────────────────────────────────────+
  |                Path                | Version |     Status    |  Updated   | D | K |
  +────────────────────────────────────────────────────────────────────────────────+
  | recon/domains-hosts/hackertarget | 1.1     | not installed | 2020-05-17 |   |   |
  +────────────────────────────────────────────────────────────────────────────────+

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

[recon-ng][whois_recon] > marketplace install recon/domains-hosts/hackertarget
[*] Module installed: recon/domains-hosts/hackertarget
[*] Reloading modules...
[recon-ng][whois_recon] > modules load recon/domains-hosts/hackertarget
[recon-ng][whois_recon][hackertarget] > 
```

STEP 11: We are now ready to begin searching HackerTarget for subdomain information regarding Facebook. First, set the source by typing:
options set SOURCE facebook.com

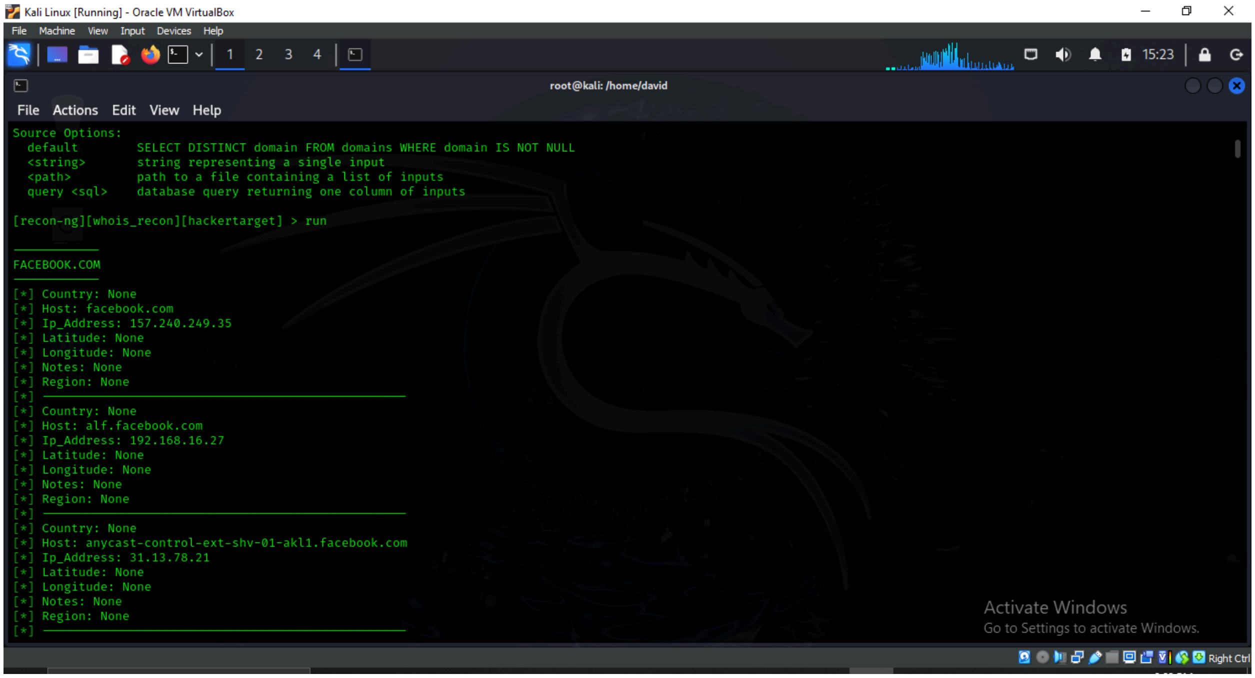
To see some information around what this module is used for and how, simply type "info" and hit enter.



Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
15:19
root@kali: /home/david
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.
Right Ctrl

```
  |               Path              | Version |     Status    |  Updated   | D | K |
  +-----------------------------------------------------------------------------------+
  | recon/domains-hosts/hackertarget | 1.1     | not installed | 2020-05-17 |   |   |
  +-----------------------------------------------------------------------------------+

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

[recon-ng][whois_recon] > marketplace install recon/domains-hosts/hackertarget
[*] Module installed: recon/domains-hosts/hackertarget
[*] Reloading modules ...
[recon-ng][whois_recon] > modules load recon/domains-hosts/hackertarget
[recon-ng][whois_recon][hackertarget] > options set SOURCE facebook.com
SOURCE ⇒ facebook.com
[recon-ng][whois_recon][hackertarget] > info

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

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

Options:
  Name    Current Value  Required  Description
  ------  -------------  --------  -----------
  SOURCE  facebook.com   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][whois_recon][hackertarget] > 
```

STEP 12: Type “run” and hit enter.



Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
15:23
root@kali: /home/david
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.
Right Ctrl

```
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][whois_recon][hackertarget] > run

------------
FACEBOOK.COM
------------
[*] Country: None
[*] Host: facebook.com
[*] Ip_Address: 157.240.249.35
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -------------------------------------------------
[*] Country: None
[*] Host: alf.facebook.com
[*] Ip_Address: 192.168.16.27
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -------------------------------------------------
[*] Country: None
[*] Host: anycast-control-ext-shv-01-akl1.facebook.com
[*] Ip_Address: 31.13.78.21
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -------------------------------------------------
```