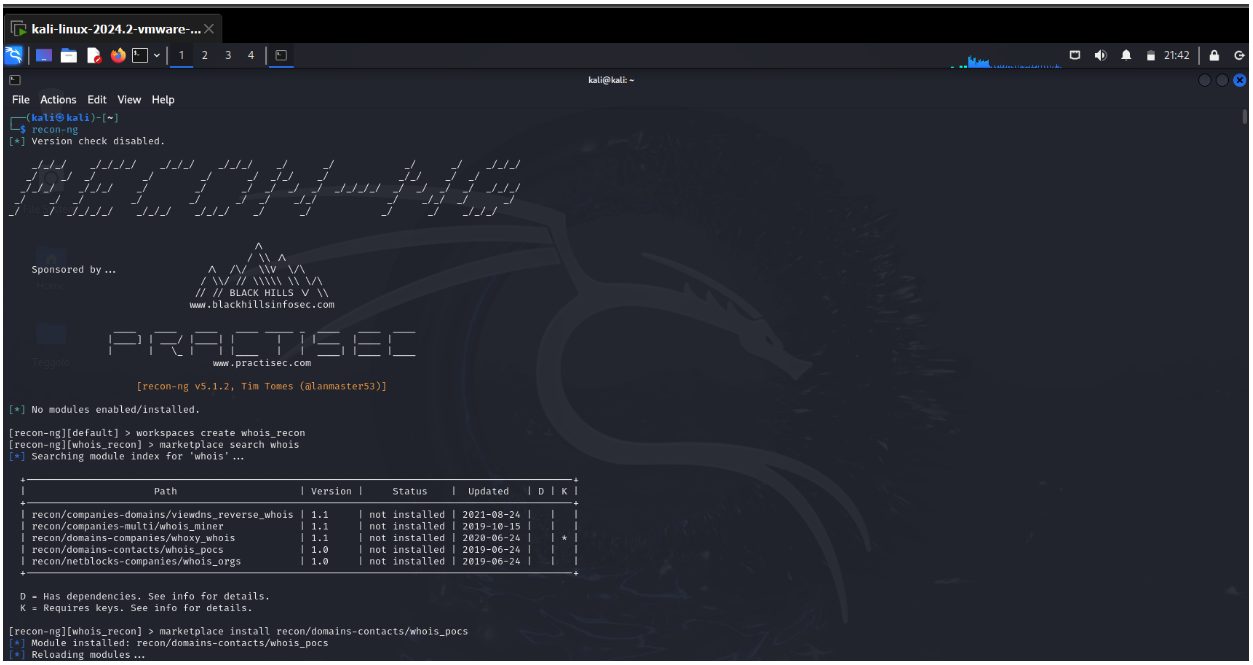
RECON-NG

Recon-ng is a web-based open source reconnaissance tool (OSINT) written in Python, often paired with the Kali Linux penetration distribution. Using Kali-Linux in a virtual machine for the purpose of this lab.

LAB WALKTHROUGH:

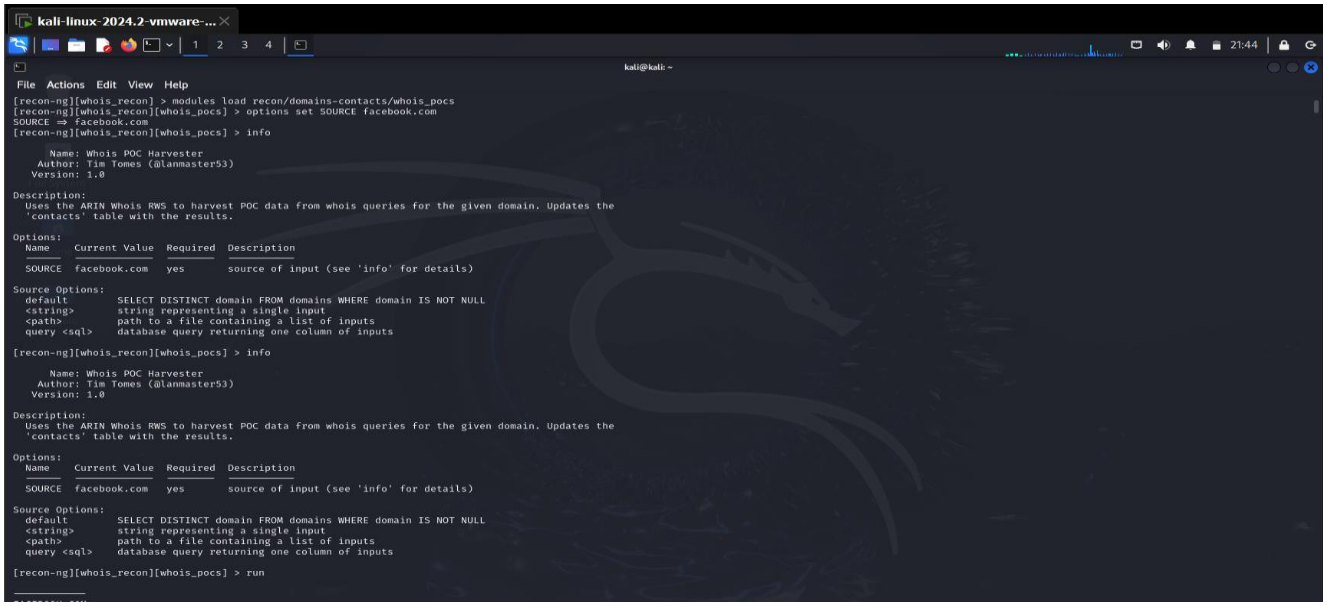
First Step: I begin the lab by opening Kali Linux within your virtual machine. Then, open terminal and type recon-ng



```
┌──(kali㉿kali)-[~]
└─$ 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] > 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...
```

Second Step: I gathered information about the target domain-name. **WHOIS** information is available to anyone, it is ok to do this for any domain. The domain I will be targeted is “facebook.com”.

I begin by searching **WHOIS information**,before commencing I installed the **WHOIS search module** by typing “marketplace search whois”. Installing the fourth option which is **“recon/domains-contacts/whois_pocs”.**

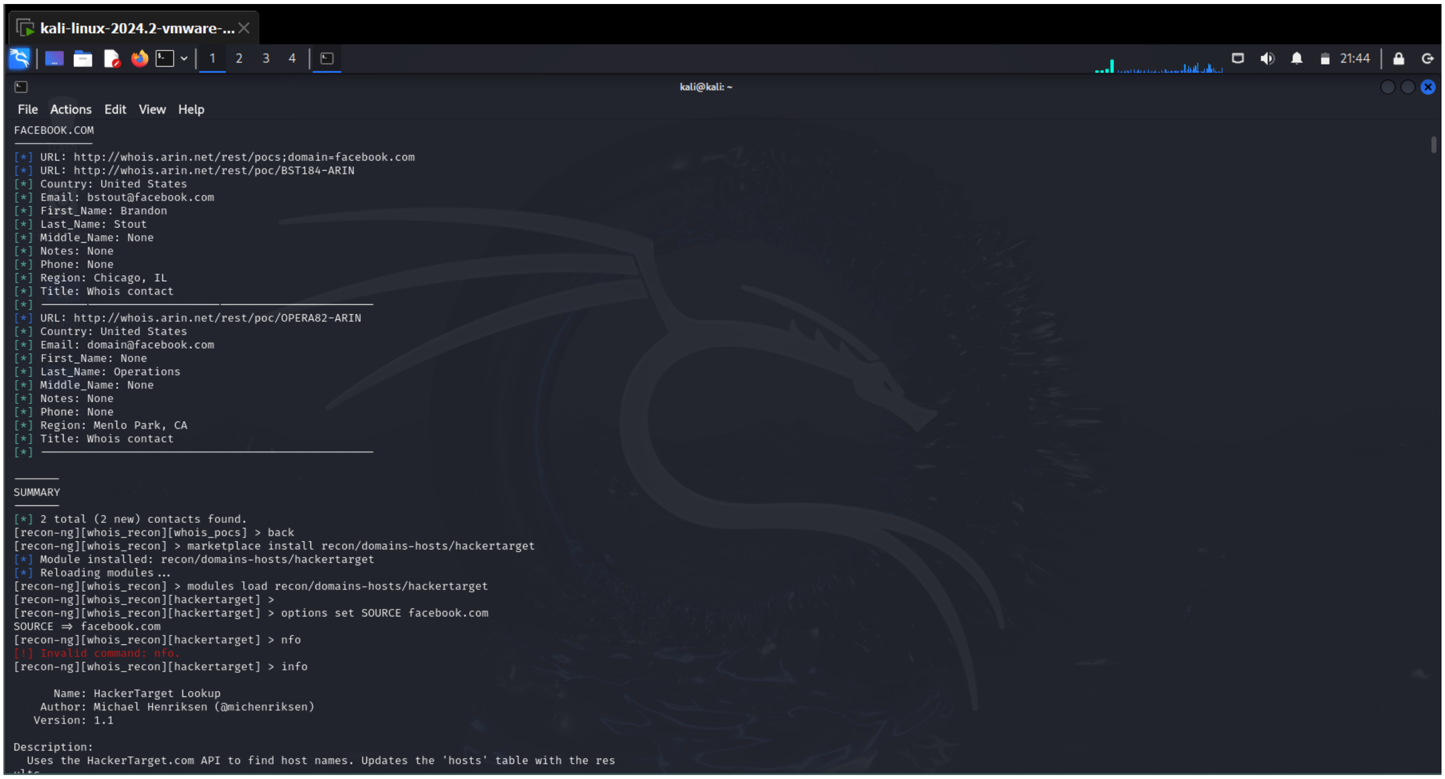


```
[recon-ng][whois_recon] > modules load recon/domains-contacts/whois_pocs
[recon-ng][whois_recon][whois_pocs] > options set SOURCE facebook.com
SOURCE ⇒ facebook.com
[recon-ng][whois_recon][whois_pocs] > info

      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] > 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] > run

-------------
```

marketplace install recon/domains-contacts/whois_pocs.

Third Step: To begin searching, I set the source by typing: options set SOURCE facebook.com. To load the module for use, type: modules load recon/domains-contacts/whois_pocs.

To see information about the module I typed "info" and hit enter. Searching for **WHOIS** for information gathering we simply type **"RUN".**

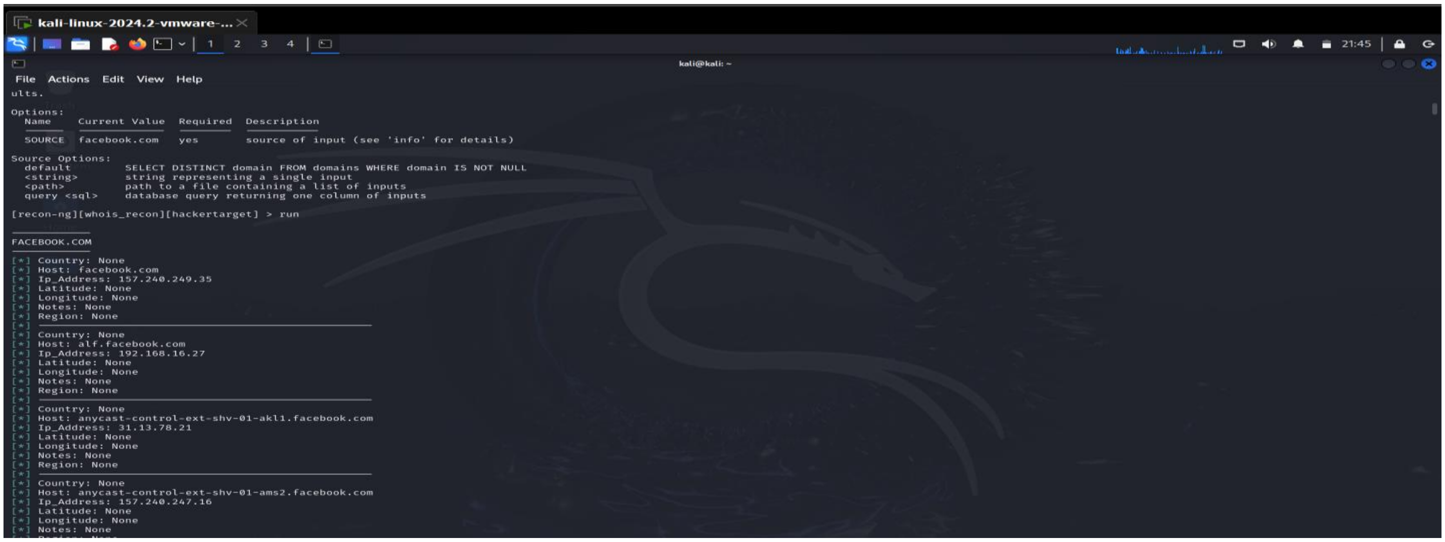


```
FACEBOOK.COM

[*] 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] > back
[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] >
[recon-ng][whois_recon][hackertarget] > options set SOURCE facebook.com
SOURCE ⇒ facebook.com
[recon-ng][whois_recon][hackertarget] > nfo
[!] Invalid command: nfo.
[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 res
```

Fourth Step: I attempted to discover as many subdomains as possible, with their IPv4 address for facebook.com, using HackerTarget.com API. I imported the "hackertarget" module, as we did previously for whois_pocs.

Before I did this, I typed "back" and enter to quit out of the whois_pocs module and begin by searching the marketplace for "hackertarget" modules using: **marketplace search hackertarget**

Only one option showed, which is **"recon/domains-hosts/hackertarget".** Following same step as above.



```
ults.

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] > 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
[*] ───────────────────────────────────────────────
[*] Country: None
[*] Host: anycast-control-ext-shv-01-ams2.facebook.com
[*] Ip_Address: 157.240.247.16
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
```