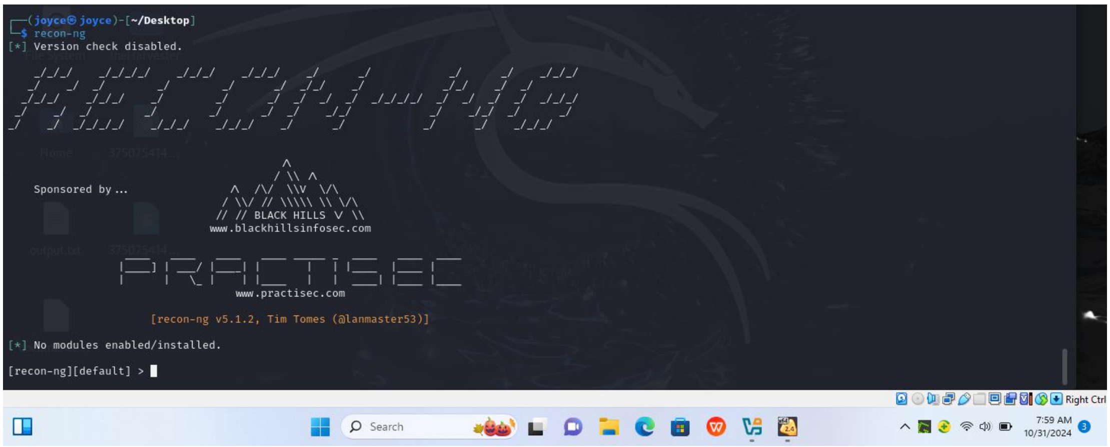
RECON-NG

Project Objective: Learn how to find WHOIS information on a target domain-name with Recon-ng.

Recon-ng is a free web based open-source reconnaissance tool(OSINT). WHOIS information consist of location, registration and expire dates, contact information(email, phone numbers,etc) about the domain. The purpose of this Lab project is to use recon-ng to automate the discovery of this information.

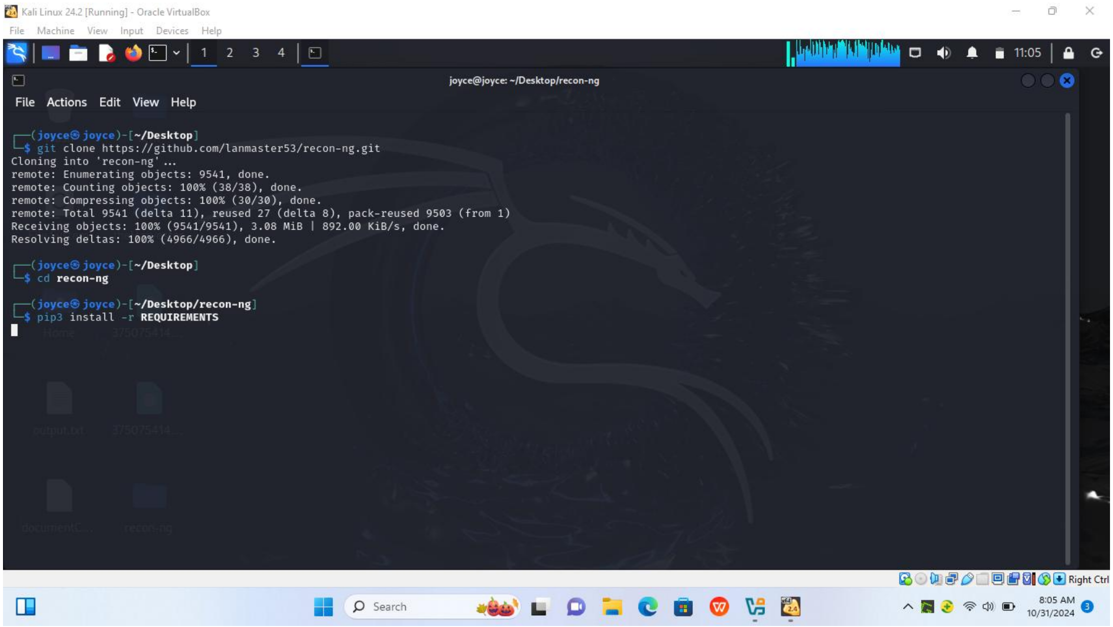
Project Tool: Kali Linux(Recon-ng, WHOIS)

Recon-ng



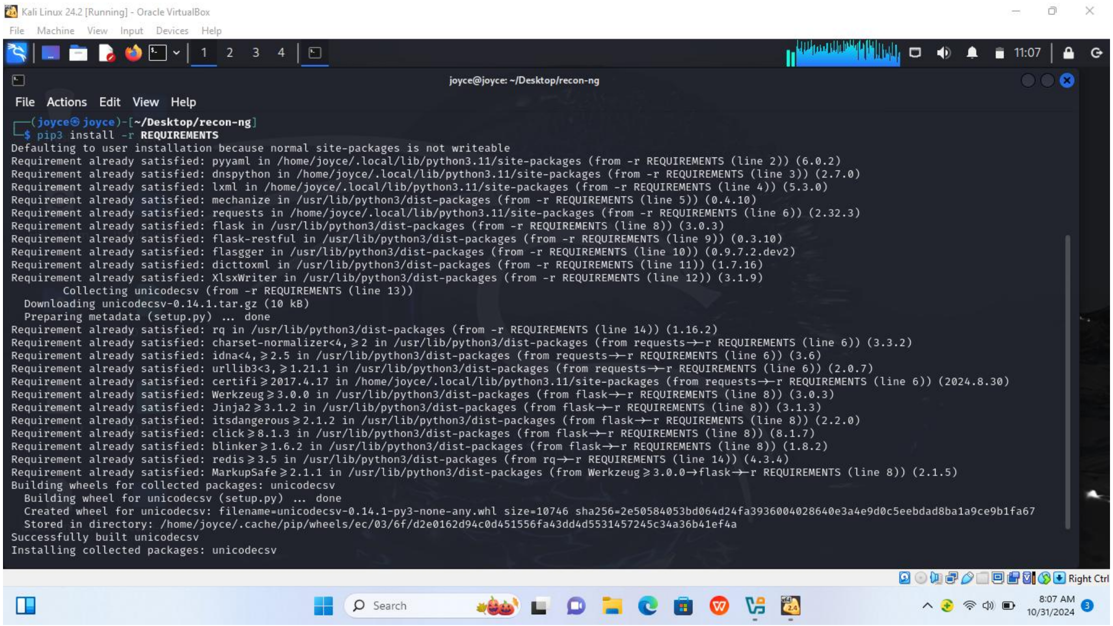
```
┌──(joyce㉿joyce)-[~/Desktop]
└─$ recon-ng
[*] Version check disabled.

    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] >
```

Git clone (Recon-ng). Installing Recon-ng



Kali Linux 24.2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
joyce@joyce: ~/Desktop/recon-ng
File Actions Edit View Help

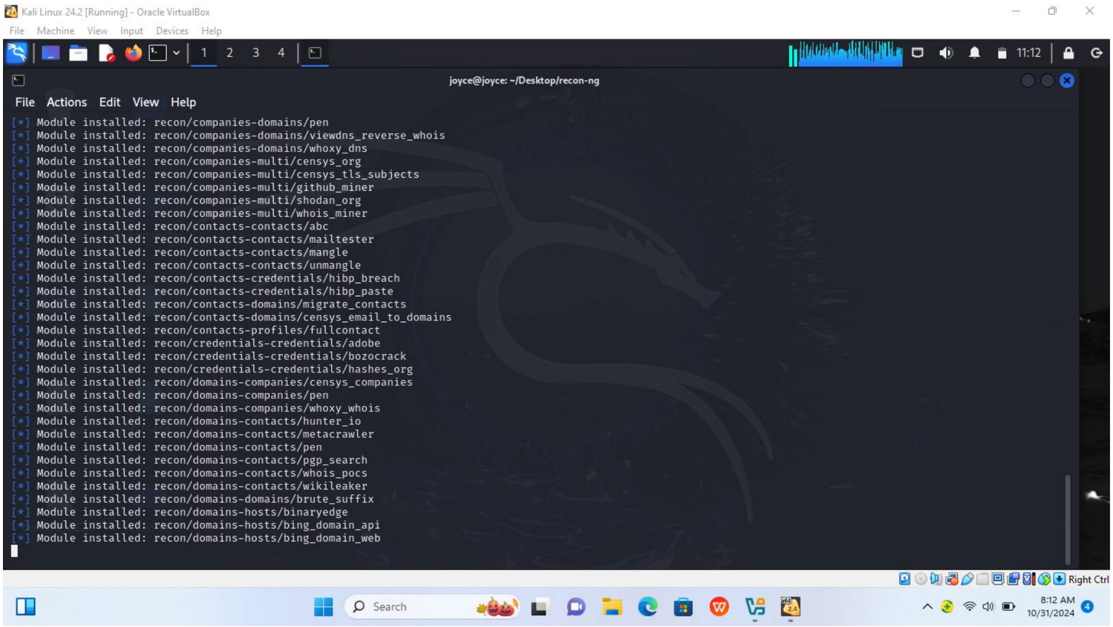
```
┌──(joyce㉿joyce)-[~/Desktop]
└─$ git clone https://github.com/lanmaster53/recon-ng.git
Cloning into 'recon-ng'...
remote: Enumerating objects: 9541, done.
remote: Counting objects: 100% (38/38), done.
remote: Compressing objects: 100% (30/30), done.
remote: Total 9541 (delta 11), reused 27 (delta 8), pack-reused 9503 (from 1)
Receiving objects: 100% (9541/9541), 3.08 MiB | 892.00 KiB/s, done.
Resolving deltas: 100% (4966/4966), done.

┌──(joyce㉿joyce)-[~/Desktop]
└─$ cd recon-ng

┌──(joyce㉿joyce)-[~/Desktop/recon-ng]
└─$ pip3 install -r REQUIREMENTS
```



Kali Linux 24.2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
11:07
joyce@joyce: ~/Desktop/recon-ng
File Actions Edit View Help
Right Ctrl
Search
8:07 AM
10/31/2024

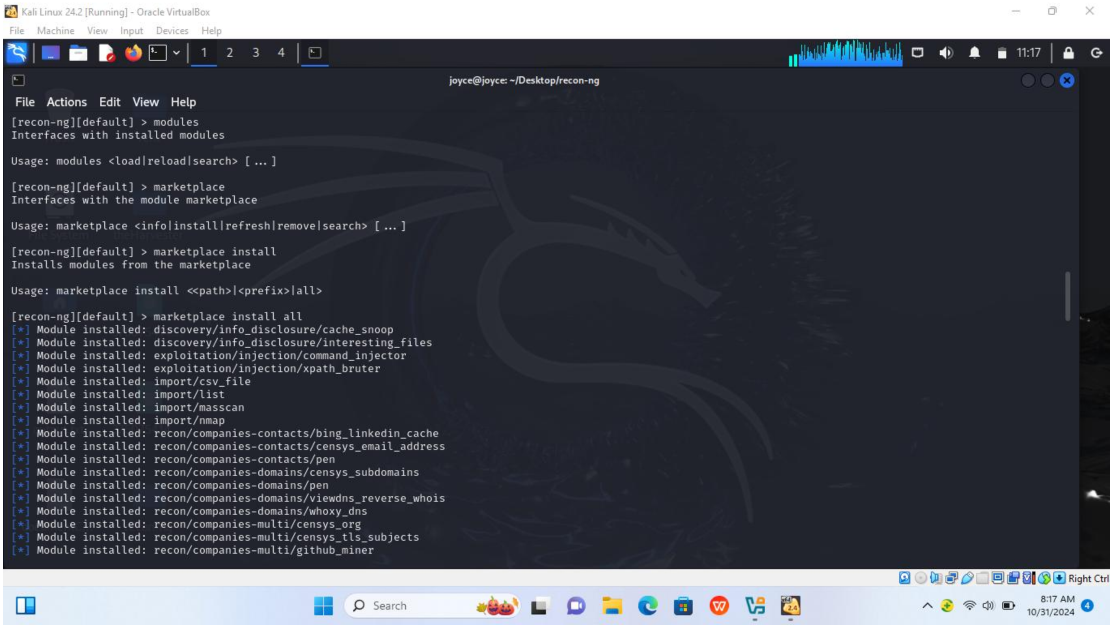
```
┌──(joyce㉿joyce)-[~/Desktop/recon-ng]
└─$ pip3 install -r REQUIREMENTS
Defaulting to user installation because normal site-packages is not writeable
Requirement already satisfied: pyyaml in /home/joyce/.local/lib/python3.11/site-packages (from -r REQUIREMENTS (line 2)) (6.0.2)
Requirement already satisfied: dnspython in /home/joyce/.local/lib/python3.11/site-packages (from -r REQUIREMENTS (line 3)) (2.7.0)
Requirement already satisfied: lxml in /home/joyce/.local/lib/python3.11/site-packages (from -r REQUIREMENTS (line 4)) (5.3.0)
Requirement already satisfied: mechanize in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 5)) (0.4.10)
Requirement already satisfied: requests in /home/joyce/.local/lib/python3.11/site-packages (from -r REQUIREMENTS (line 6)) (2.32.3)
Requirement already satisfied: flask in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 8)) (3.0.3)
Requirement already satisfied: flask-restful in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 9)) (0.3.10)
Requirement already satisfied: flasgger in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 10)) (0.9.7.2.dev2)
Requirement already satisfied: dicttoxml in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 11)) (1.7.16)
Requirement already satisfied: XlsxWriter in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 12)) (3.1.9)
        Collecting unicodecsv (from -r REQUIREMENTS (line 13))
  Downloading unicodecsv-0.14.1.tar.gz (10 kB)
  Preparing metadata (setup.py) ... done
Requirement already satisfied: rq in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 14)) (1.16.2)
Requirement already satisfied: charset-normalizer<4,≥2 in /usr/lib/python3/dist-packages (from requests→-r REQUIREMENTS (line 6)) (3.3.2)
Requirement already satisfied: idna<4,≥2.5 in /usr/lib/python3/dist-packages (from requests→-r REQUIREMENTS (line 6)) (3.6)
Requirement already satisfied: urllib3<3,≥1.21.1 in /usr/lib/python3/dist-packages (from requests→-r REQUIREMENTS (line 6)) (2.0.7)
Requirement already satisfied: certifi≥2017.4.17 in /home/joyce/.local/lib/python3.11/site-packages (from requests→-r REQUIREMENTS (line 6)) (2024.8.30)
Requirement already satisfied: Werkzeug≥3.0.0 in /usr/lib/python3/dist-packages (from flask→-r REQUIREMENTS (line 8)) (3.0.3)
Requirement already satisfied: Jinja2≥3.1.2 in /usr/lib/python3/dist-packages (from flask→-r REQUIREMENTS (line 8)) (3.1.3)
Requirement already satisfied: itsdangerous≥2.1.2 in /usr/lib/python3/dist-packages (from flask→-r REQUIREMENTS (line 8)) (2.2.0)
Requirement already satisfied: click≥8.1.3 in /usr/lib/python3/dist-packages (from flask→-r REQUIREMENTS (line 8)) (8.1.7)
Requirement already satisfied: blinker≥1.6.2 in /usr/lib/python3/dist-packages (from flask→-r REQUIREMENTS (line 8)) (1.8.2)
Requirement already satisfied: redis≥3.5 in /usr/lib/python3/dist-packages (from rq→-r REQUIREMENTS (line 14)) (4.3.4)
Requirement already satisfied: MarkupSafe≥2.1.1 in /usr/lib/python3/dist-packages (from Werkzeug≥3.0.0→flask→-r REQUIREMENTS (line 8)) (2.1.5)
Building wheels for collected packages: unicodecsv
  Building wheel for unicodecsv (setup.py) ... done
  Created wheel for unicodecsv: filename=unicodecsv-0.14.1-py3-none-any.whl size=10746 sha256=2e50584053bd064d24fa3936004028640e3a4e9d0c5eebdad8ba1a9ce9b1fa67
  Stored in directory: /home/joyce/.cache/pip/wheels/ec/03/6f/d2e0162d94c0d451556fa43dd4d5531457245c34a36b41ef4a
Successfully built unicodecsv
Installing collected packages: unicodecsv
```

INSTALLING MODULES



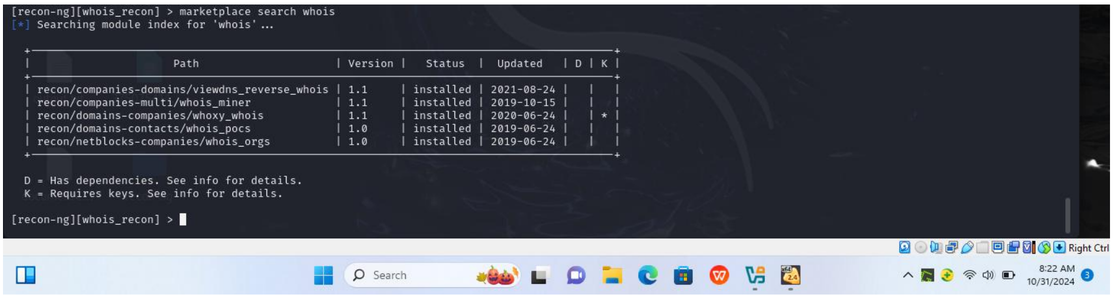
Kali Linux 24.2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
11:12
joyce@joyce: ~/Desktop/recon-ng
File Actions Edit View Help
Right Ctrl
Search
8:12 AM
10/31/2024

```
[*] 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-multi/censys_org
[*] Module installed: recon/companies-multi/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
[*] Module installed: recon/contacts-credentials/hibp_breach
[*] Module installed: recon/contacts-credentials/hibp_paste
[*] Module installed: recon/contacts-domains/migrate_contacts
[*] Module installed: recon/contacts-domains/censys_email_to_domains
[*] Module installed: recon/contacts-profiles/fullcontact
[*] Module installed: recon/credentials-credentials/adobe
[*] Module installed: recon/credentials-credentials/bozocrack
[*] Module installed: recon/credentials-credentials/hashes_org
[*] Module installed: recon/domains-companies/censys_companies
[*] Module installed: recon/domains-companies/pen
[*] Module installed: recon/domains-companies/whoxy_whois
[*] Module installed: recon/domains-contacts/hunter_io
[*] Module installed: recon/domains-contacts/metacrawler
[*] Module installed: recon/domains-contacts/pen
[*] Module installed: recon/domains-contacts/pgp_search
[*] Module installed: recon/domains-contacts/whois_pocs
[*] Module installed: recon/domains-contacts/wikileaker
[*] Module installed: recon/domains-domains/brute_suffix
[*] Module installed: recon/domains-hosts/binaryedge
[*] Module installed: recon/domains-hosts/bing_domain_api
[*] Module installed: recon/domains-hosts/bing_domain_web
▌
```

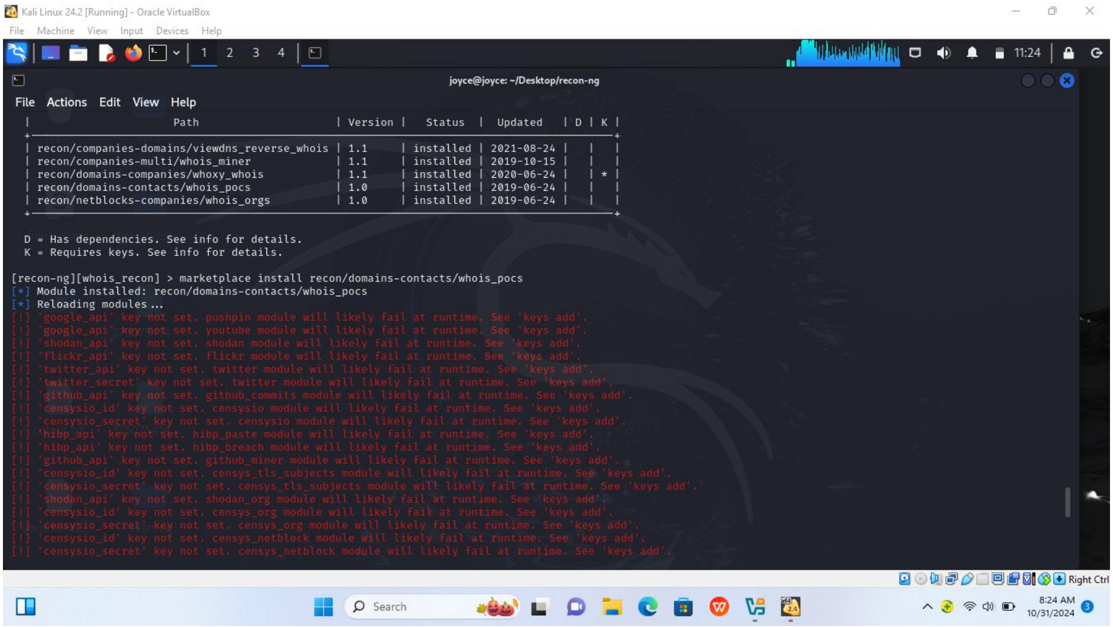

Kali Linux 24.2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
joyce@joyce: ~/Desktop/recon-ng
File Actions Edit View Help
11:17
Right Ctrl
Search
8:17 AM
10/31/2024

```
[recon-ng][default] > modules
Interfaces with installed modules

Usage: modules <load|reload|search> [ ... ]

[recon-ng][default] > marketplace
Interfaces with the module marketplace

Usage: marketplace <info|install|refresh|remove|search> [ ... ]

[recon-ng][default] > marketplace install
Installs modules from the marketplace

Usage: marketplace install <<path>|<prefix>|all>

[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-multi/censys_org
[*] Module installed: recon/companies-multi/censys_tls_subjects
[*] Module installed: recon/companies-multi/github_miner
```

Marketplace search whois

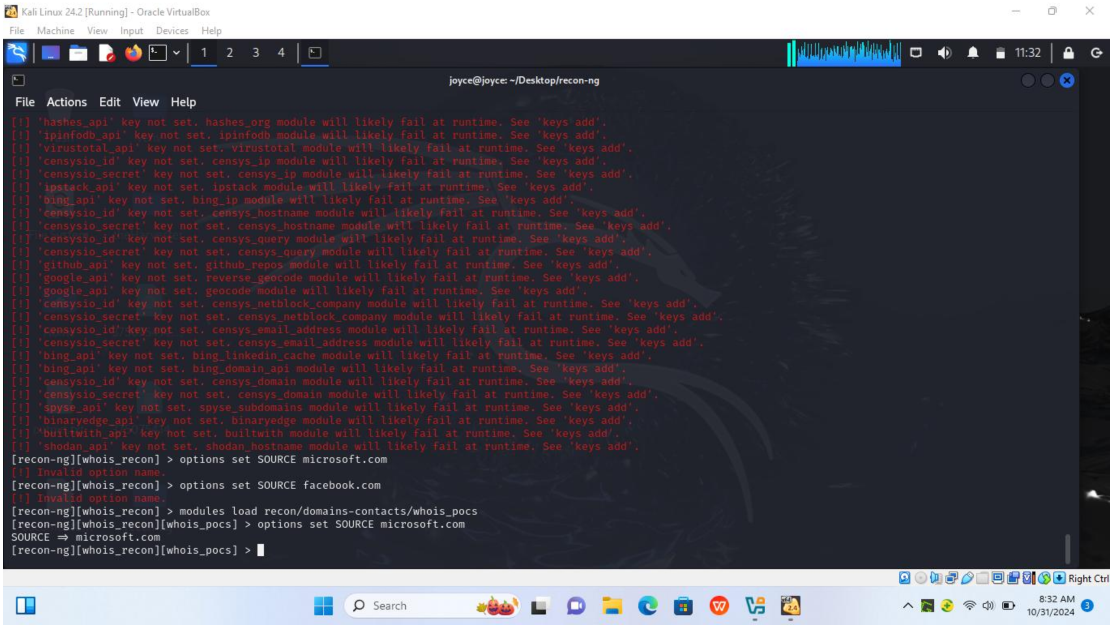


```
[recon-ng][whois_recon] > marketplace search whois
[*] Searching module index for 'whois'...

  +---------------------------------------------------------------------------------+
  |                    Path                     | Version |   Status  |  Updated   | D | K |
  +---------------------------------------------------------------------------------+
  | recon/companies-domains/viewdns_reverse_whois | 1.1     | installed | 2021-08-24 |   |   |
  | recon/companies-multi/whois_miner           | 1.1     | installed | 2019-10-15 |   |   |
  | recon/domains-companies/whoxy_whois         | 1.1     | installed | 2020-06-24 |   | * |
  | recon/domains-contacts/whois_pocs           | 1.0     | installed | 2019-06-24 |   |   |
  | recon/netblocks-companies/whois_orgs        | 1.0     | installed | 2019-06-24 |   |   |
  +---------------------------------------------------------------------------------+

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

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


Kali Linux 24.2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
joyce@joyce: ~/Desktop/recon-ng
File Actions Edit View Help
11:24
Right Ctrl
Search
8:24 AM
10/31/2024

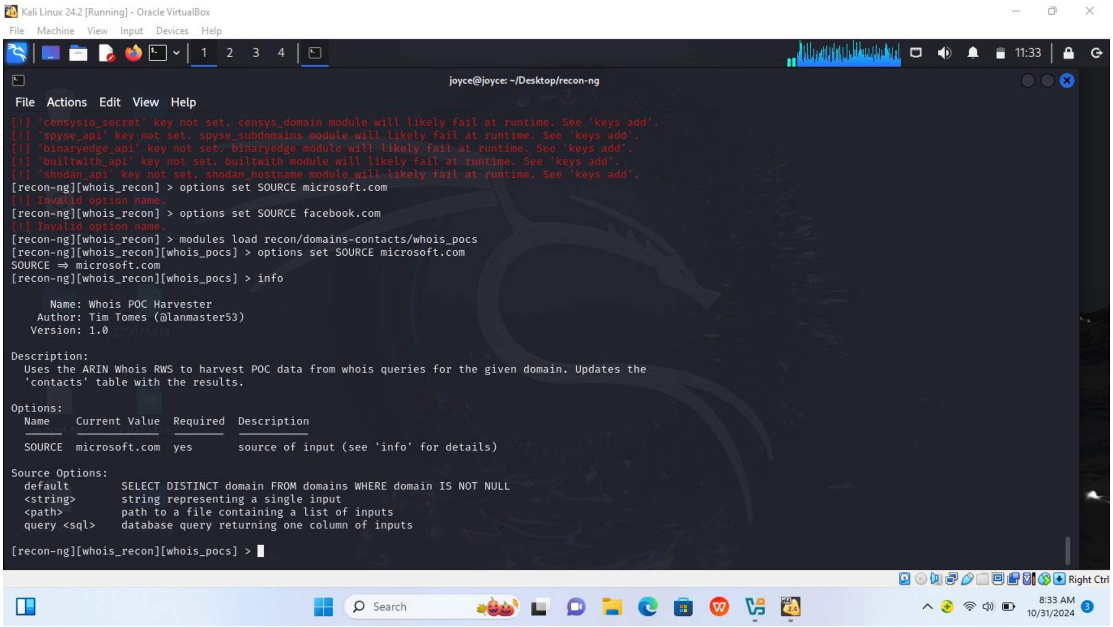
```
  |                    Path                     | Version |   Status  |  Updated   | D | K |
  +---------------------------------------------------------------------------------+
  | recon/companies-domains/viewdns_reverse_whois | 1.1     | installed | 2021-08-24 |   |   |
  | recon/companies-multi/whois_miner           | 1.1     | installed | 2019-10-15 |   |   |
  | recon/domains-companies/whoxy_whois         | 1.1     | installed | 2020-06-24 |   | * |
  | recon/domains-contacts/whois_pocs           | 1.0     | installed | 2019-06-24 |   |   |
  | recon/netblocks-companies/whois_orgs        | 1.0     | 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...
[!] 'google_api' key not set. pushpin module will likely fail at runtime. See 'keys add'.
[!] 'google_api' key not set. youtube module will likely fail at runtime. See 'keys add'.
[!] 'shodan_api' key not set. shodan module will likely fail at runtime. See 'keys add'.
[!] 'flickr_api' key not set. flickr module will likely fail at runtime. See 'keys add'.
[!] 'twitter_api' key not set. twitter module will likely fail at runtime. See 'keys add'.
[!] 'twitter_secret' key not set. twitter 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'.
[!] 'censysio_id' key not set. censysio module will likely fail at runtime. See 'keys add'.
[!] 'censysio_secret' key not set. censysio 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'.
[!] 'hibp_api' key not set. hibp_breach module will likely fail at runtime. See 'keys add'.
[!] 'github_api' key not set. github_miner module will likely fail at runtime. See 'keys add'.
[!] 'censysio_id' key not set. censys_tls_subjects module will likely fail at runtime. See 'keys add'.
[!] 'censysio_secret' key not set. censys_tls_subjects 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'.
[!] 'censysio_id' key not set. censys_org module will likely fail at runtime. See 'keys add'.
[!] 'censysio_secret' key not set. censys_org module will likely fail at runtime. See 'keys add'.
[!] 'censysio_id' key not set. censys_netblock module will likely fail at runtime. See 'keys add'.
[!] 'censysio_secret' key not set. censys_netblock module will likely fail at runtime. See 'keys add'.
```

To set the source and load the module load recon/dmains-contacts /whois_pocs



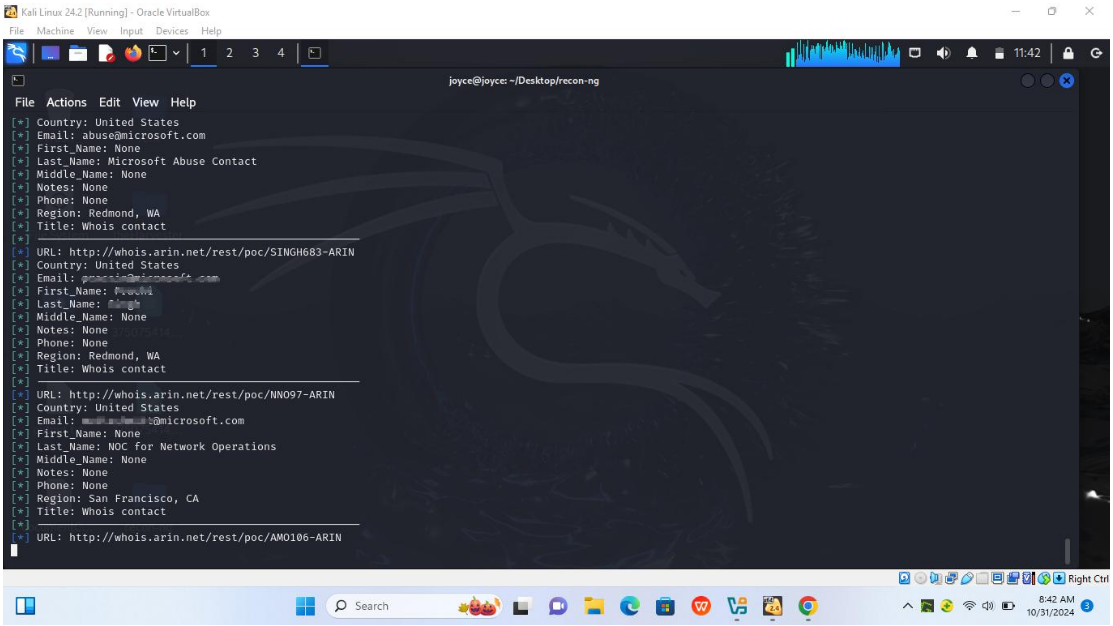
```
[!] 'hashes_api' key not set. hashes_org module will likely fail at runtime. See 'keys add'.
[!] 'ipinfodb_api' key not set. ipinfodb module will likely fail at runtime. See 'keys add'.
[!] 'virustotal_api' key not set. virustotal module will likely fail at runtime. See 'keys add'.
[!] 'censysio_id' key not set. censys_ip module will likely fail at runtime. See 'keys add'.
[!] 'censysio_secret' key not set. censys_ip module will likely fail at runtime. See 'keys add'.
[!] 'ipstack_api' key not set. ipstack module will likely fail at runtime. See 'keys add'.
[!] 'bing_api' key not set. bing_ip module will likely fail at runtime. See 'keys add'.
[!] 'censysio_id' key not set. censys_hostname module will likely fail at runtime. See 'keys add'.
[!] 'censysio_secret' key not set. censys_hostname module will likely fail at runtime. See 'keys add'.
[!] 'censysio_id' key not set. censys_query module will likely fail at runtime. See 'keys add'.
[!] 'censysio_secret' key not set. censys_query 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'.
[!] 'google_api' key not set. reverse_geocode module will likely fail at runtime. See 'keys add'.
[!] 'google_api' key not set. geocode module will likely fail at runtime. See 'keys add'.
[!] 'censysio_id' key not set. censys_netblock_company module will likely fail at runtime. See 'keys add'.
[!] 'censysio_secret' key not set. censys_netblock_company module will likely fail at runtime. See 'keys add'.
[!] 'censysio_id' key not set. censys_email_address module will likely fail at runtime. See 'keys add'.
[!] 'censysio_secret' key not set. censys_email_address module will likely fail at runtime. See 'keys add'.
[!] 'bing_api' key not set. bing_linkedin_cache module will likely fail at runtime. See 'keys add'.
[!] 'bing_api' key not set. bing_domain_api module will likely fail at runtime. See 'keys add'.
[!] 'censysio_id' key not set. censys_domain module will likely fail at runtime. See 'keys add'.
[!] 'censysio_secret' key not set. censys_domain module will likely fail at runtime. See 'keys add'.
[!] 'spyse_api' key not set. spyse_subdomains module will likely fail at runtime. See 'keys add'.
[!] 'binaryedge_api' key not set. binaryedge module will likely fail at runtime. See 'keys add'.
[!] 'builtwith_api' key not set. builtwith module will likely fail at runtime. See 'keys add'.
[!] 'shodan_api' key not set. shodan_hostname module will likely fail at runtime. See 'keys add'.
[recon-ng][whois_recon] > options set SOURCE microsoft.com
[!] Invalid option name.
[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 microsoft.com
SOURCE ⇒ microsoft.com
[recon-ng][whois_recon][whois_pocs] > 
```

Kali Linux 24.2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
joyce@joyce: ~/Desktop/recon-ng
File Actions Edit View Help
11:32
Right Ctrl
Search
8:32 AM
10/31/2024



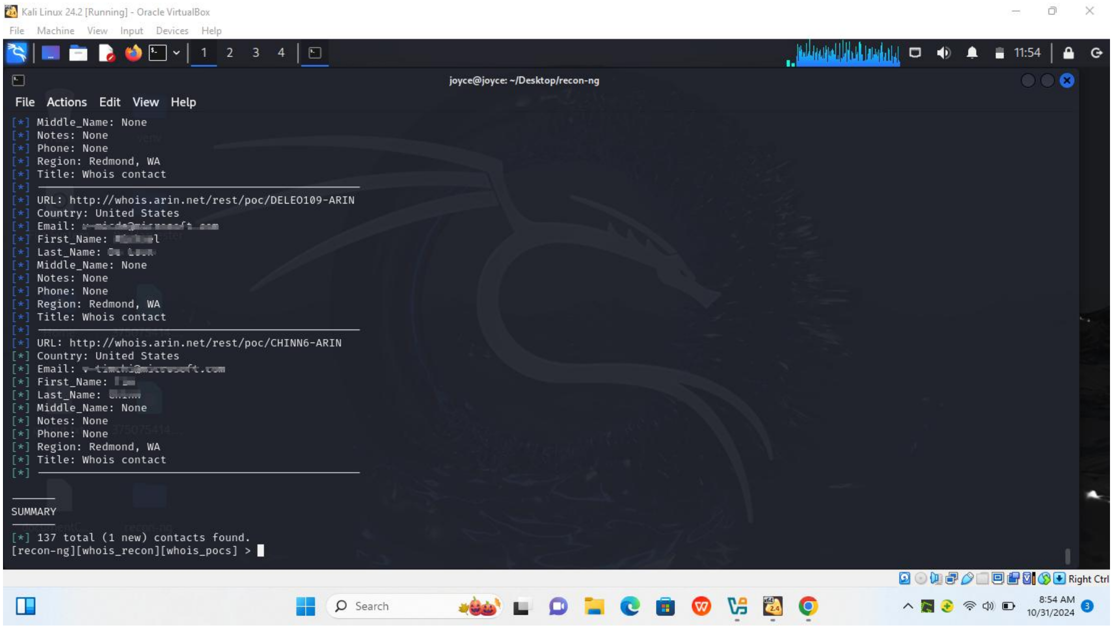
```
[!] 'censysio_secret' key not set. censys_domain module will likely fail at runtime. See 'keys add'.
[!] 'spyse_api' key not set. spyse_subdomains module will likely fail at runtime. See 'keys add'.
[!] 'binaryedge_api' key not set. binaryedge module will likely fail at runtime. See 'keys add'.
[!] 'builtwith_api' key not set. builtwith module will likely fail at runtime. See 'keys add'.
[!] 'shodan_api' key not set. shodan_hostname module will likely fail at runtime. See 'keys add'.
[recon-ng][whois_recon] > options set SOURCE microsoft.com
[!] Invalid option name.
[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 microsoft.com
SOURCE ⇒ microsoft.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  microsoft.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] > 
```

Kali Linux 24.2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
joyce@joyce: ~/Desktop/recon-ng
File Actions Edit View Help
11:33
Right Ctrl
Search
8:33 AM
10/31/2024


Kali Linux 24.2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
11:42
joyce@joyce: ~/Desktop/recon-ng
File Actions Edit View Help
Right Ctrl
Search
8:42 AM
10/31/2024

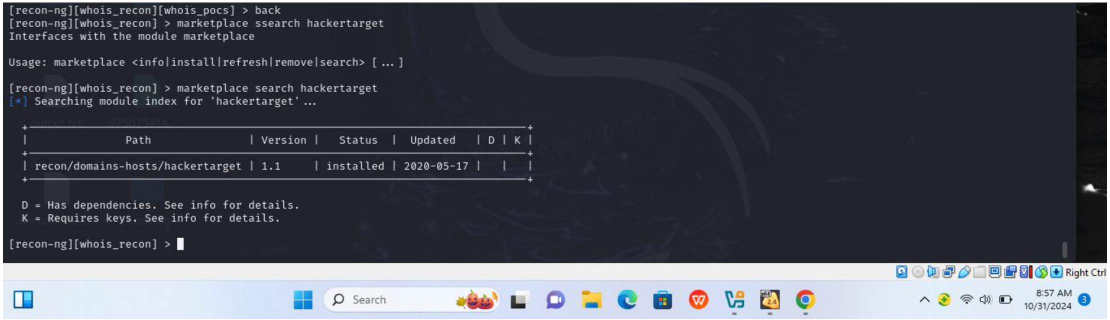
```
[*] Country: United States
[*] Email: abuse@microsoft.com
[*] First_Name: None
[*] Last_Name: Microsoft Abuse Contact
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Redmond, WA
[*] Title: Whois contact
[*] ──────────────────────────────────────────
[*] URL: http://whois.arin.net/rest/poc/SINGH683-ARIN
[*] Country: United States
[*] Email: [redacted]
[*] First_Name: [redacted]
[*] Last_Name: [redacted]
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Redmond, WA
[*] Title: Whois contact
[*] ──────────────────────────────────────────
[*] URL: http://whois.arin.net/rest/poc/NNO97-ARIN
[*] Country: United States
[*] Email: [redacted]@microsoft.com
[*] First_Name: None
[*] Last_Name: NOC for Network Operations
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: San Francisco, CA
[*] Title: Whois contact
[*] ──────────────────────────────────────────
[*] URL: http://whois.arin.net/rest/poc/AMO106-ARIN
```

WHOIS gathers open source information on the above.


Kali Linux 24.2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
11:54
joyce@joyce: ~/Desktop/recon-ng
File Actions Edit View Help
Right Ctrl
Search
8:54 AM
10/31/2024

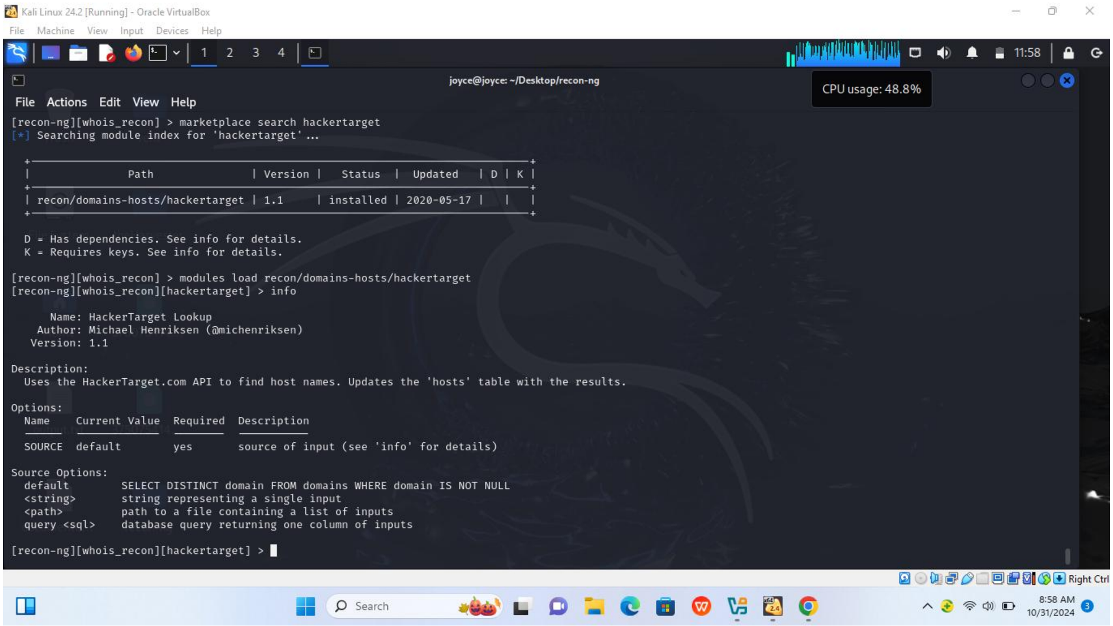
```
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Redmond, WA
[*] Title: Whois contact
[*] ──────────────────────────────────────────
[*] URL: http://whois.arin.net/rest/poc/DELEO109-ARIN
[*] Country: United States
[*] Email: [redacted]
[*] First_Name: [redacted]l
[*] Last_Name: [redacted]
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Redmond, WA
[*] Title: Whois contact
[*] ──────────────────────────────────────────
[*] URL: http://whois.arin.net/rest/poc/CHINN6-ARIN
[*] Country: United States
[*] Email: [redacted]
[*] First_Name: [redacted]
[*] Last_Name: [redacted]
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Redmond, WA
[*] Title: Whois contact
[*] ──────────────────────────────────────────

-------
SUMMARY
-------
[*] 137 total (1 new) contacts found.
[recon-ng][whois_recon][whois_pocs] >
```

Recon-ng searches the marketplace for “hackertarget”



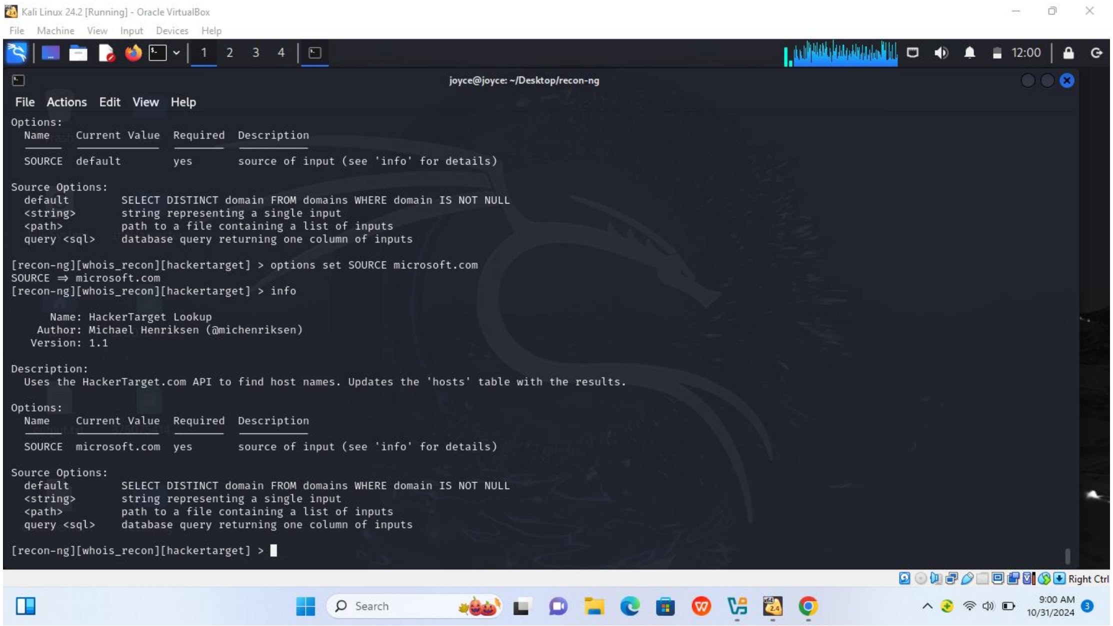
```
[recon-ng][whois_recon][whois_pocs] > back
[recon-ng][whois_recon] > marketplace ssearch hackertarget
Interfaces with the module marketplace

Usage: marketplace <info|install|refresh|remove|search> [ ... ]

[recon-ng][whois_recon] > marketplace search hackertarget
[*] Searching module index for 'hackertarget'...

  +---------------------------------------------------------------------------+
  |                Path                | Version |   Status  |  Updated   | D | K |
  +---------------------------------------------------------------------------+
  | recon/domains-hosts/hackertarget | 1.1     | installed | 2020-05-17 |   |   |
  +---------------------------------------------------------------------------+

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

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

The information for the domains-hosts.

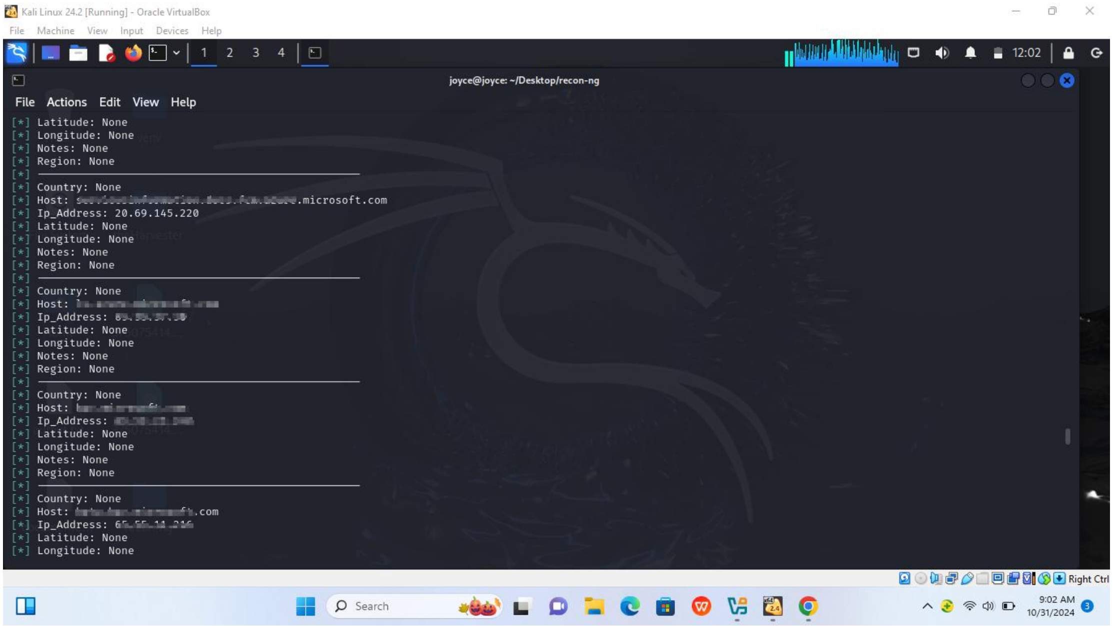

Kali Linux 24.2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
joyce@joyce: ~/Desktop/recon-ng
CPU usage: 48.8%
File Actions Edit View Help

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

  +-----------------------------------------------------------------------+
  |              Path              | Version |   Status   |  Updated   | D | K |
  +-----------------------------------------------------------------------+
  | recon/domains-hosts/hackertarget | 1.1     | installed | 2020-05-17 |   |   |
  +-----------------------------------------------------------------------+

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

[recon-ng][whois_recon] > modules load recon/domains-hosts/hackertarget
[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  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][whois_recon][hackertarget] >
```

11:58
Search
8:58 AM
10/31/2024

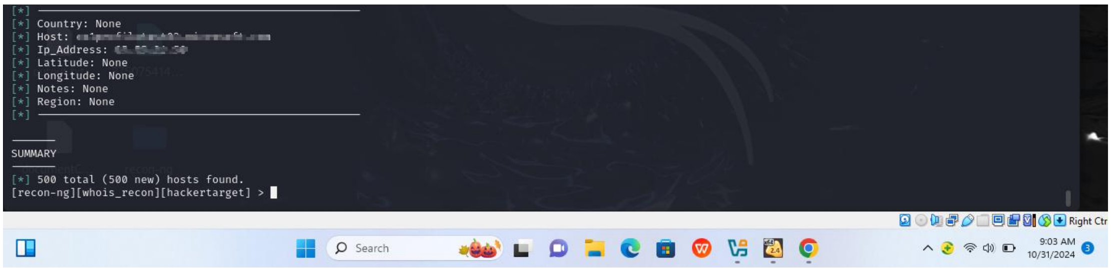

Kali Linux 24.2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
joyce@joyce: ~/Desktop/recon-ng
File Actions Edit View Help

```
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][whois_recon][hackertarget] > options set SOURCE microsoft.com
SOURCE => microsoft.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  microsoft.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] >
```


Kali Linux 24.2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
12:02
joyce@joyce: ~/Desktop/recon-ng
File Actions Edit View Help
Right Ctrl
Search
9:02 AM
10/31/2024

```
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ──────────────────────────────────────────────────
[*] Country: None
[*] Host: [redacted].microsoft.com
[*] Ip_Address: 20.69.145.220
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ──────────────────────────────────────────────────
[*] Country: None
[*] Host: [redacted]
[*] Ip_Address: [redacted]
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ──────────────────────────────────────────────────
[*] Country: None
[*] Host: [redacted]
[*] Ip_Address: [redacted]
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ──────────────────────────────────────────────────
[*] Country: None
[*] Host: [redacted].com
[*] Ip_Address: [redacted]
[*] Latitude: None
[*] Longitude: None
```

The above displays subdomains of the target site.



```
[*] ──────────────────────────────────────────────────
[*] Country: None
[*] Host: [redacted]
[*] Ip_Address: [redacted]
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ──────────────────────────────────────────────────

───────
SUMMARY
───────
[*] 500 total (500 new) hosts found.
[recon-ng][whois_recon][hackertarget] >
```