Experiment no:1

Recon-ng tool

Aim : To perform active reconnaissance using reconnaissance tool using reco-ng

Description:

Recon-ng is free and open-source tool available on GitHub. Recon-ng is based upon Open-Source Intelligence (OSINT), the easiest and useful tool for reconnaissance. Recon-ng interface is very similar to Metasploit1 and Metasploit2. Recon-ng provides a command-line interface that you can run on Kali Linux. This tool can be used to get information about our target(domain). The interactive console provides a number of helpful features, such as command completion and contextual help. Recon-ng is a Web Reconnaissance tool written in Python. It has so many modules, database interaction, built-in convenience functions, interactive help, and command completion, Recon-ng provides a powerful environment in which open-source web-based reconnaissance can be conducted, and we can gather all information.

Features of Recon-ng :

- ✓ Recon-ng is free and open-source tool this means you can download and use it at free of cost.
- ✓ Recon-ng is a complete package of information gathering modules. It has so many modules that you can use for information gathering.
- ✓ Recon-ng works and acts as a web application/website scanner.
- ✓ Recon-ng is one of the easiest and useful tool for performing reconnaissance.
- ✓ Recon-ng interface is very similar to metasploitable1 and metasploitable2 that makes is easy to use.
- ✓ Recon-ng's interactive console provides a number of helpful features.
- ✓ Recon-ng is used for information gathering and vulnerability assessment of web applications.
- ✓ Recon-ng uses shodan search engine to scan iot devices.
- ✓ Recon-ng can easily find loopholes in the code of web applications and websites.
- ✓ Recon-ng has following modules Geoip lookup, Banner grabbing, DNS lookup, port scanning, These modules makes this tool so powerful.

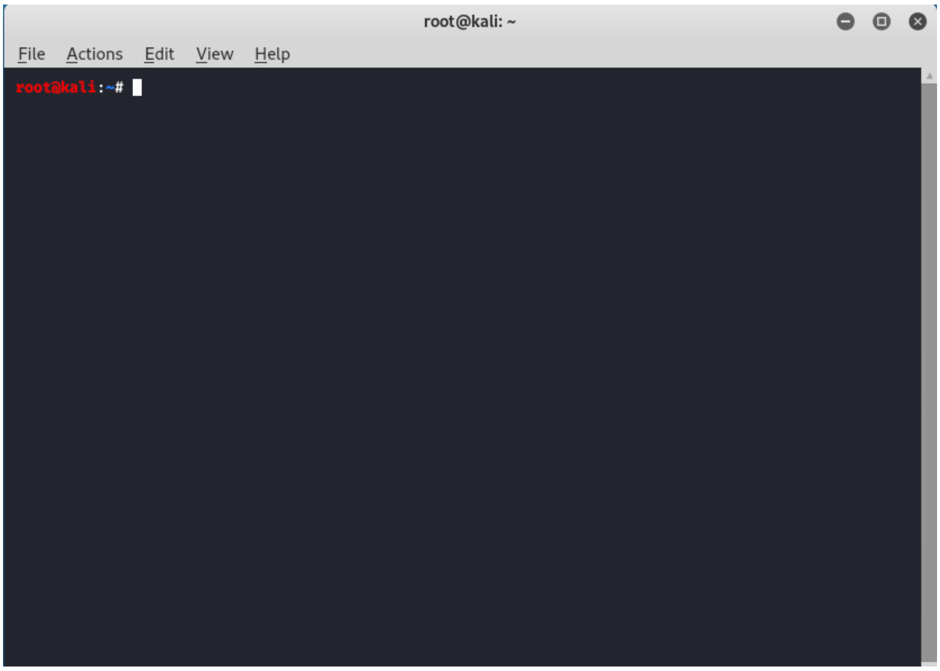
- ✓ Recon-ng can target a single domain and can found all the subdomains of that domain which makes work easy for pentesters.

Uses of Recon-ng :

- ✓ Recon-ng is a complete package of Information gathering tools.
- ✓ Recon-ng can be used to find IP Addresses of target.
- ✓ Recon-ng can be used to look for error-based SQL injections.
- ✓ Recon-ng can be used to find sensitive files such as robots.txt.
- ✓ Recon-ng can be used to find information about Geo-IP lookup, Banner grabbing, DNS lookup, port scanning, sub-domain information, reverse IP using WHOIS lookup.
- ✓ Recon-ng can be used to detects Content Management Systems (CMS) in use of a target web application,
- ✓ InfoSploit can be used for WHOIS data collection, Geo-IP lookup, Banner grabbing, DNS lookup, port scanning, sub-domain information, reverse IP, and MX records lookup
- ✓ Recon-ng is a complete package (TOOL) for information gathering. This tool is free and Open Source.
- ✓ Recon-ng subdomain finder modules is used to find subdomains of a single domain.
- ✓ Recon-ng can be used to find robots.txt file of a website.
- ✓ Recon-ng port scanner modules find closes and open ports which can be used to maintain access to the server.
- ✓ Recon-ng has various modules that can be used to get the information about target.

Procedures:

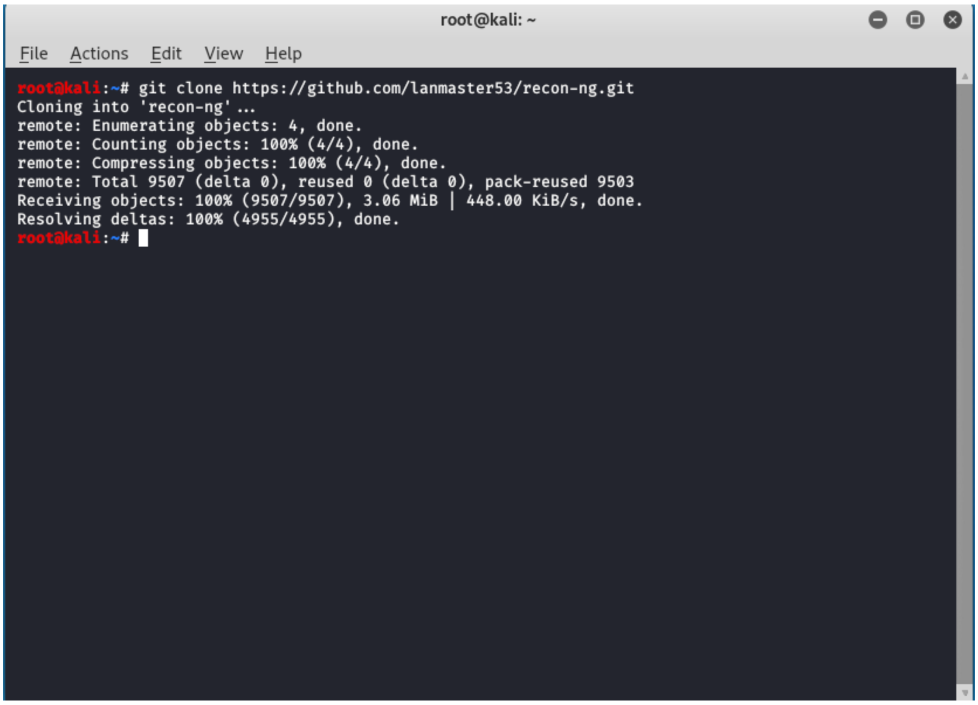
Step 1: Open Terminal of your Kali Linux



```
root@kali:~#
```

Step 2: On Terminal now type command.

git clone https://github.com/lanmaster53/recon-ng.git

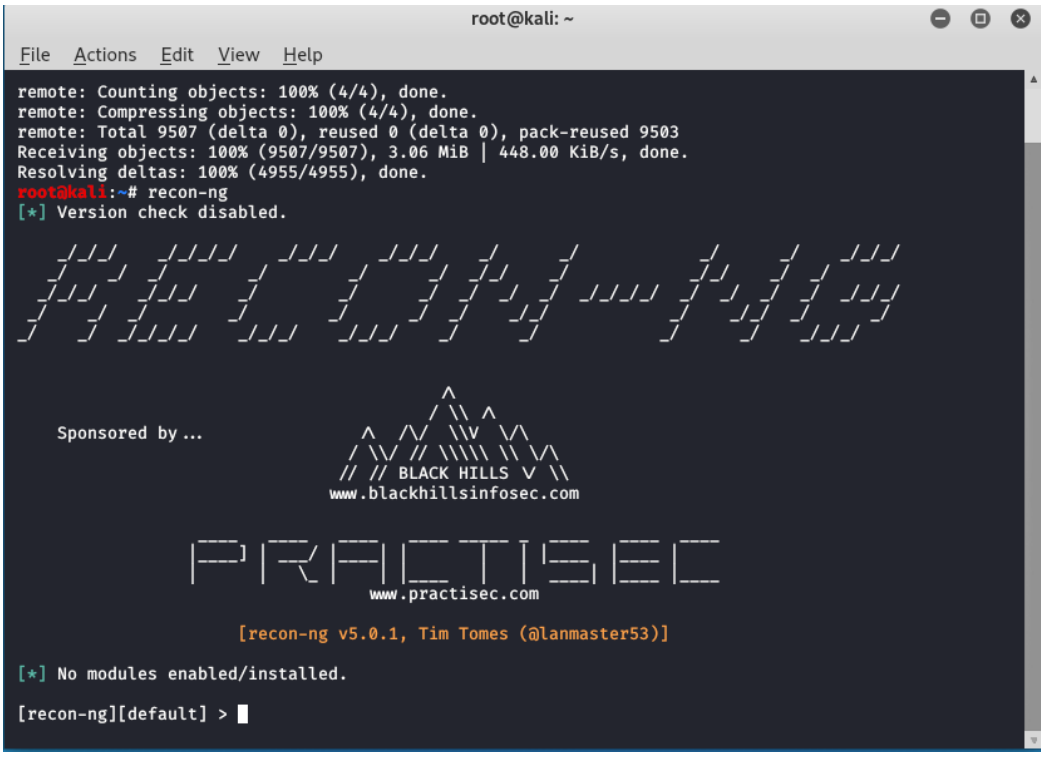


```
root@kali:~# git clone https://github.com/lanmaster53/recon-ng.git
Cloning into 'recon-ng'...
remote: Enumerating objects: 4, done.
remote: Counting objects: 100% (4/4), done.
remote: Compressing objects: 100% (4/4), done.
remote: Total 9507 (delta 0), reused 0 (delta 0), pack-reused 9503
Receiving objects: 100% (9507/9507), 3.06 MiB | 448.00 KiB/s, done.
Resolving deltas: 100% (4955/4955), done.
root@kali:~#
```

recon-ng has been installed on your Kali Linux ,now you just have to run recon-ng.

Step 3: To launch recon-ng on your kali Linux type the following the command and press enter.

recon-ng



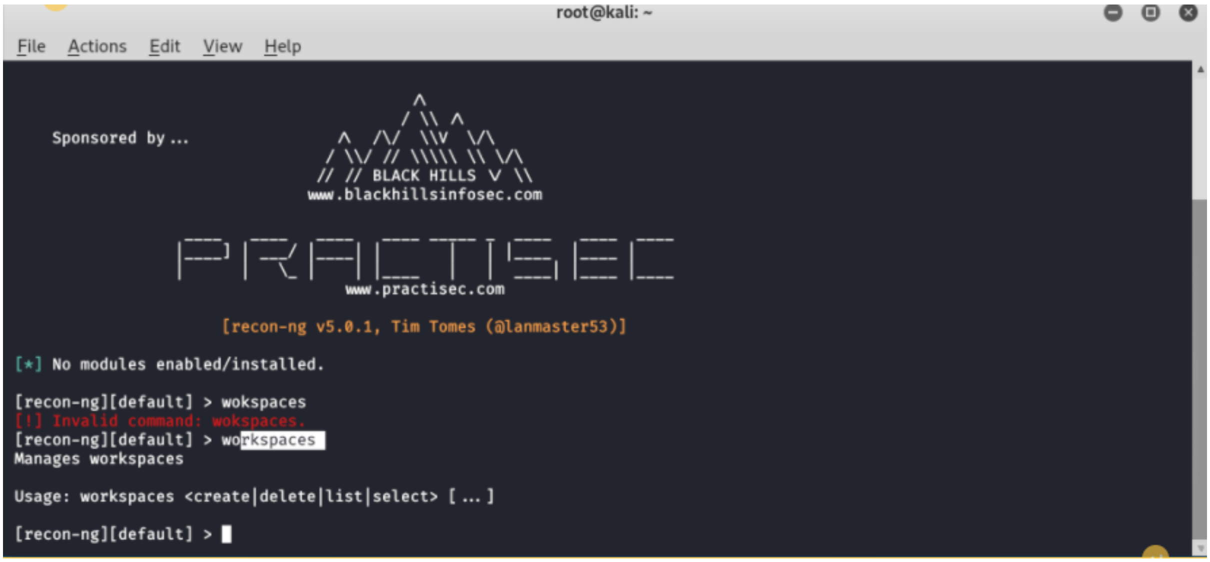
```
remote: Counting objects: 100% (4/4), done.
remote: Compressing objects: 100% (4/4), done.
remote: Total 9507 (delta 0), reused 0 (delta 0), pack-reused 9503
Receiving objects: 100% (9507/9507), 3.06 MiB | 448.00 KiB/s, done.
Resolving deltas: 100% (4955/4955), done.
root@kali:~# recon-ng
[*] Version check disabled.

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

                                     www.practisec.com

                       [recon-ng v5.0.1, Tim Tomes (@lanmaster53)]

[*] No modules enabled/installed.

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

Now Recon-ng has been downloaded and running successfully.

Step 4: Now to do Reconnaissance first you have to create a workspace for that. Basically, workspaces are like separate spaces in which you can perform reconnaissance of different targets. To know about workspaces just type the following command.

workspaces

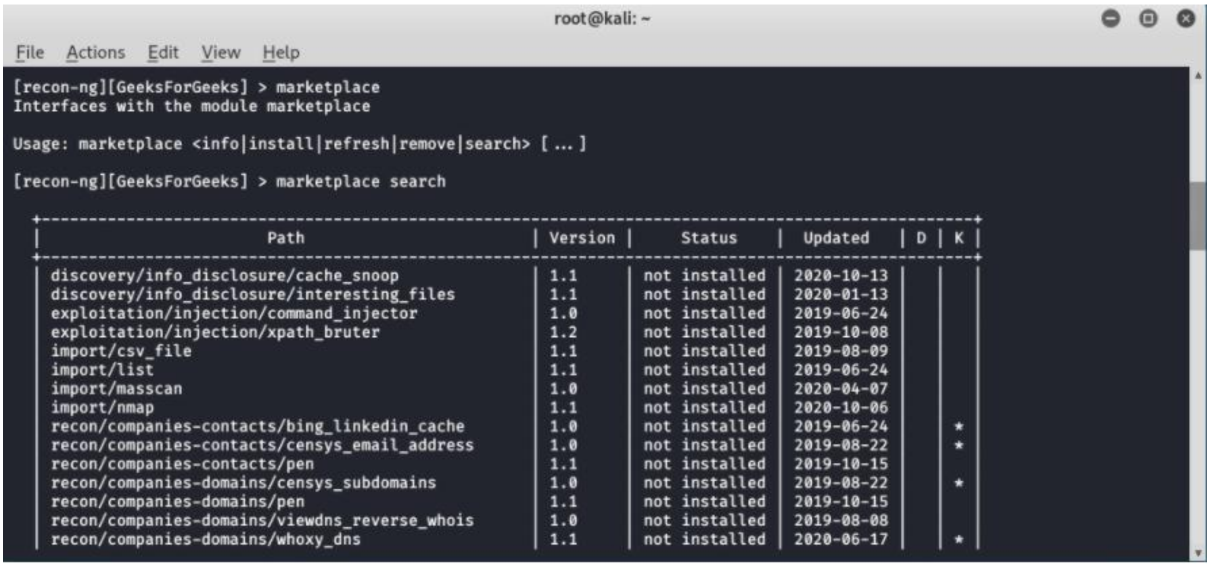
workspaces create (name)



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

                                     www.practisec.com

                       [recon-ng v5.0.1, Tim Tomes (@lanmaster53)]

[*] No modules enabled/installed.

[recon-ng][default] > wokspaces
[!] Invalid command: wokspaces.
[recon-ng][default] > workspaces
Manages workspaces

Usage: workspaces <create|delete|list|select> [ ... ]

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

Step 5: You have created workspace for you, now you have to go to marketplace to install modules to initiate your Reconnaissance here we have created a workspace called GeeksForGeeks. Now we will Reconnaissance within GeeksForGeeks workspace. Now go to marketplace and install modules.

marketplace search

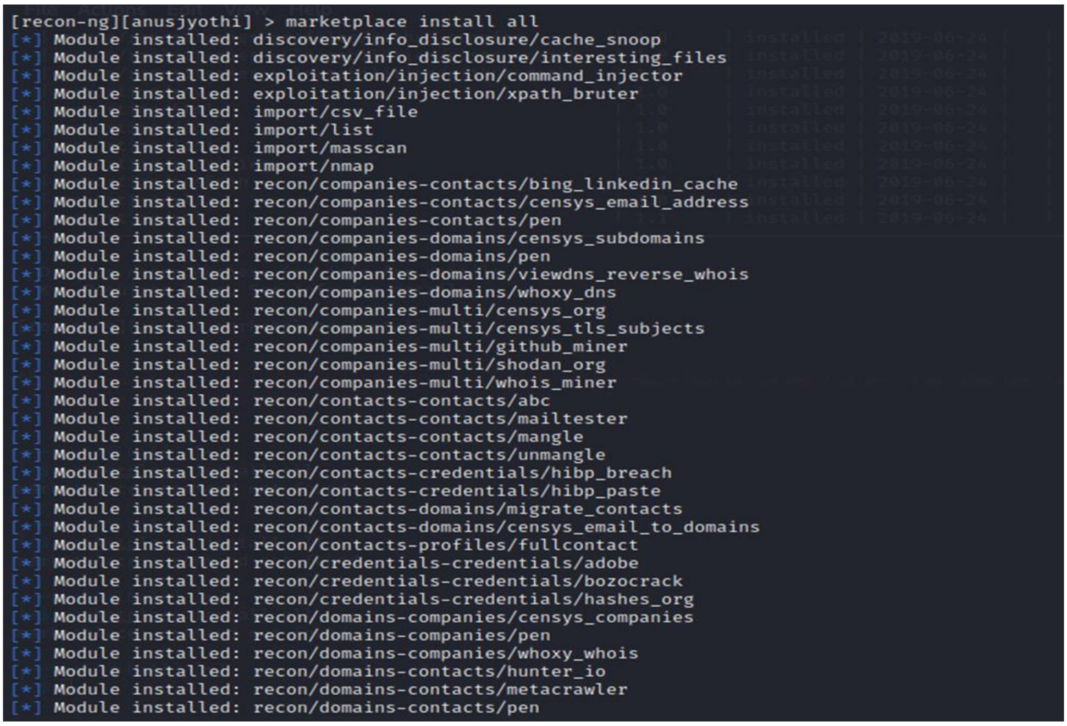


```
[recon-ng][GeeksForGeeks] > marketplace
Interfaces with the module marketplace

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

[recon-ng][GeeksForGeeks] > marketplace search

  +----------------------------------------------------------------------------------------------+
  |                       Path                        | Version |     Status    |  Updated   | D | K |
  +----------------------------------------------------------------------------------------------+
  | discovery/info_disclosure/cache_snoop             | 1.1     | not installed | 2020-10-13 |   |   |
  | discovery/info_disclosure/interesting_files       | 1.1     | not installed | 2020-01-13 |   |   |
  | exploitation/injection/command_injector           | 1.0     | not installed | 2019-06-24 |   |   |
  | exploitation/injection/xpath_bruter               | 1.2     | not installed | 2019-10-08 |   |   |
  | import/csv_file                                   | 1.1     | not installed | 2019-08-09 |   |   |
  | import/list                                       | 1.1     | not installed | 2019-06-24 |   |   |
  | import/masscan                                    | 1.0     | not installed | 2020-04-07 |   |   |
  | import/nmap                                       | 1.1     | not installed | 2020-10-06 |   |   |
  | recon/companies-contacts/bing_linkedin_cache      | 1.0     | not installed | 2019-06-24 |   | * |
  | recon/companies-contacts/censys_email_address     | 1.0     | not installed | 2019-08-22 |   | * |
  | recon/companies-contacts/pen                      | 1.1     | not installed | 2019-10-15 |   |   |
  | recon/companies-domains/censys_subdomains         | 1.0     | not installed | 2019-08-22 |   | * |
  | recon/companies-domains/pen                       | 1.1     | not installed | 2019-10-15 |   |   |
  | recon/companies-domains/viewdns_reverse_whois     | 1.0     | not installed | 2019-08-08 |   |   |
  | recon/companies-domains/whoxy_dns                 | 1.1     | not installed | 2020-06-17 |   | * |
```

Step 6: As you can now see a list of modules and so many of them are not installed so to install those modules type following command.

marketplace install (module name)

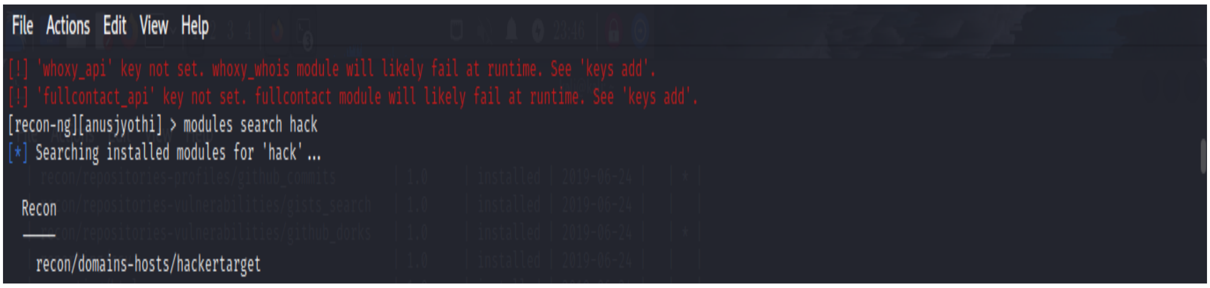
marketplace install all



```
[recon-ng][anusjyothi] > 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
[*] 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
```

Step 7: Type the command

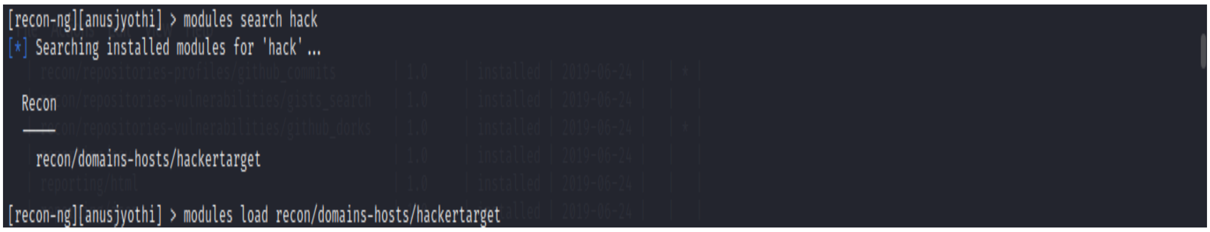
modules search hack



```
[!] 'whoxy_api' key not set. whoxy_whois module will likely fail at runtime. See 'keys add'.
[!] 'fullcontact_api' key not set. fullcontact module will likely fail at runtime. See 'keys add'.
[recon-ng][anusjyothi] > modules search hack
[*] Searching installed modules for 'hack'...

  Recon
  -----
    recon/domains-hosts/hackertarget
```

Step 8: As you can see that we have installed the module names recon/domains-hosts/hackertarget. Now we will load this module in our workspace.

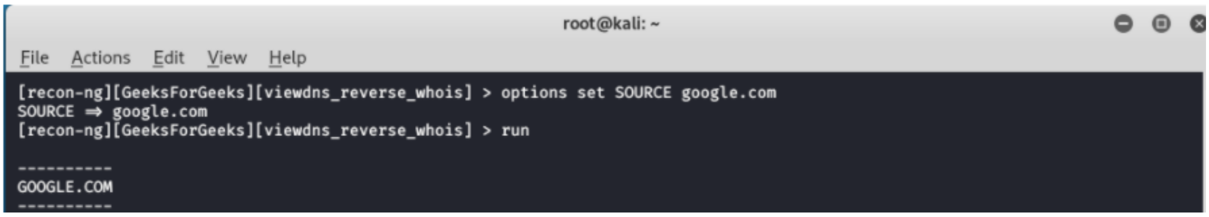
modules load (module name)



```
[recon-ng][anusjyothi] > modules search hack
[*] Searching installed modules for 'hack'...

  Recon
  -----
    recon/domains-hosts/hackertarget

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

Step 9: As you can see now we are under those modules. Now to use this module we have to set the source.

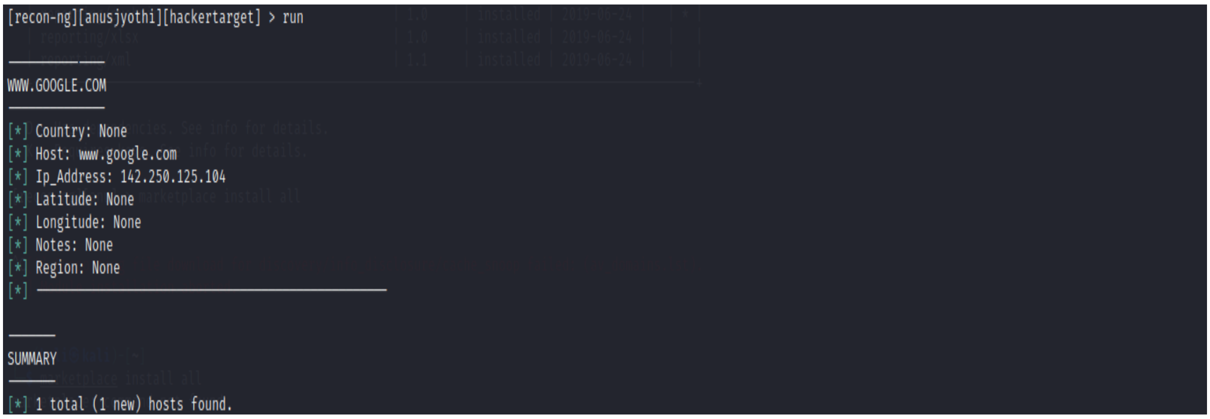
options set SOURCE (domain name)



```
[recon-ng][GeeksForGeeks][viewdns_reverse_whois] > options set SOURCE google.com
SOURCE => google.com
[recon-ng][GeeksForGeeks][viewdns_reverse_whois] > run

----------
GOOGLE.COM
----------
```

Step 10: Type the command

run



```
[recon-ng][anusjyothi][hackertarget] > run

───────────
WWW.GOOGLE.COM
───────────
[*] Country: None
[*] Host: www.google.com
[*] Ip_Address: 142.250.125.104
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ──────────────────────────────────────

──────
SUMMARY
──────
[*] 1 total (1 new) hosts found.
```

We have set google.com as a source by command options set SOURCE google.com. Recon-ng is Open-Source Intelligence, the easiest and useful tool for reconnaissance.

RESULT

Active reconnaissance using reconnaissance tool using recon-ng is performed.