Recon-ng Demonstration

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 Metasploit 1 and Metasploit 2. 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.

Commands: -

1. We will use hackertarget module in order to demonstrate the Recon-ng Tool. So, firstly we have to install hackertarget module as seen below.

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

2. After installing it we have to load our module by using load command.

```
[recon-ng][default] > modules load hackertarget
```

3. Now we are ready to use this module. To have a insight of this module type help for its manual page.

```
[recon-ng][default][hackertarget] > 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
goptions        Manages the global context options
help            Displays this menu
info            Shows details about the loaded module
input           Shows inputs based on the source option
keys            Manages third party resource credentials
modules         Interfaces with installed modules
options         Manages the current context options
pdb             Starts a Python Debugger session (dev only)
reload          Reloads the loaded module
run             Runs the loaded module
script          Records and executes command scripts
shell           Executes shell commands
show            Shows various framework items
spool           Spools output to a file
```

4. Now we must set a source of our target. To do so, use show option command.

```
[recon-ng][default][hackertarget] > show options
Shows various framework items

Usage: show <companies|contacts|credentials|domains|hosts|leaks|locations|netblocks|ports|profiles|pushpins|repositories|vulnerabilities>
```

5. We have put tesla.com as our source as seen below.

```
[recon-ng][default][hackertarget] > options set SOURCE tesla.com
SOURCE => tesla.com
[recon-ng][default][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  tesla.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
```

6. Now use info command to show that current value has been change to tesla.com

```
[recon-ng][default][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  tesla.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
```

7. Use input command to see our available sources.

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

  +---------------+
  | Module Inputs |
  +---------------+
  | tesla.com     |
  +---------------+
```

8. In the end to see the result we have to run our module. To do same, use run command.

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

---------
TESLA.COM
---------
[*] Country: None
[*] Host: tesla.com
[*] Ip_Address: 104.80.228.227
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: apacvpn.tesla.com
[*] Ip_Address: 8.244.67.215
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: apacvpn1.tesla.com
[*] Ip_Address: 8.244.131.215
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: cnvpn.tesla.com
[*] Ip_Address: 103.222.41.215
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
```