**Username:** Palm Beach State College IP Holder **Book:** Kali Linux – Assuring Security by Penetration Testing. No part of any chapter or book may be reproduced or transmitted in any form by any means without the prior written permission for reprints and excerpts from the publisher of the book or chapter. Redistribution or other use that violates the fair use privilege under U.S. copyright laws (see 17 USC107) or that otherwise violates these Terms of Service is strictly prohibited. Violators will be prosecuted to the full extent of U.S. Federal and Massachusetts laws.

## **Appendix A. Supplementary Tools**

This chapter will briefly describe several additional tools that can be used as extra weapons while conducting the penetration testing process. For each tool, we will describe the following aspects:

- The tool function
- The tool installation process if the tool is not included in Kali Linux
- Some examples on how to use the tool

The tools described in this chapter may not be included by default in Kali Linux. You need to download them from the Kali Linux repository as defined in the /etc/apt/sources.lst file using the apt-get command, or you can download them from each tool's website.

We will loosely divide the tools into the following categories:

- · The reconnaissance tool
- The vulnerability scanner
- · Web application tools
- The network tool

Let's see several additional tools that we can use during our penetration testing process.

## Reconnaissance tool

One of the tools that can be used to help us for reconnaissance is recon-ng. It is a framework to automate the reconnaissance and discovery processes. If you are familiar with the Metasploit interface, you should feel at home when using recon-ng—the interface is modeled after the Metasploit interface.

Kali Linux has already included recon-ng Version 1.41. If you want a newer version, you can download it from <a href="https://bitbucket.org/LaNMaSteR53">https://bitbucket.org/LaNMaSteR53</a>/recon-ng/overview.

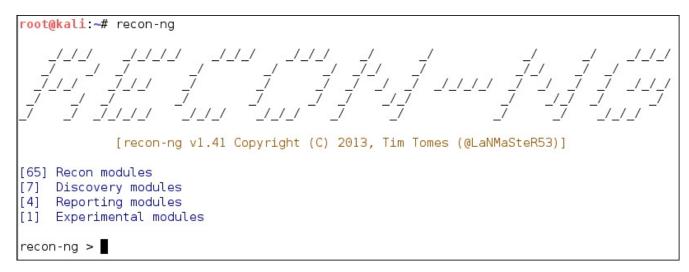
The recon-ng tool comes with modules for the reconnaissance and discovery processes. Following are the module categories included in recon-ng:

- Reconnaissance modules: In Version 1.41, Pecon-ng has 65 modules related to reconnaissance
- Discovery modules: There are seven modules in this category
- Four reporting modules
- One experimental module

To use the **recon-ng** tool, you can type the following command:

# recon-ng

After running this command, you will see the recon-ng prompt. It is very similar to the Metasploit prompt:



To find out the commands supported by recon-ng, you can type help on the prompt, the following screenshot will be displayed:

recon-ng > help	
Commands (type [help ?] <topic>):</topic>	
back banner exit help info keys load query record reload resource run search set shell show use	Exits current prompt level Displays the banner Exits current prompt level Displays this menu Displays module information Manages framework API keys Loads selected module Queries the database Records commands to a resource file Reloads all modules Executes commands from a resource file Not available Searches available modules Sets global options Executed shell commands Shows various framework items Loads selected module
use	Loads selected module

The following are several commands that you will use often:

```
• use or load : This loads the selected modules
```

reload : This reloads all the modules

• info : This displays the module information

• run : This runs the selected module

Show : This shows the various framework items

back : This exits the current prompt level

To list the available modules, you can type Show modules and it will display the available modules as shown in the following screenshot:

```
recon-ng > show modules
 Discovery
   discovery/exploitable/http/dnn fcklinkgallery
   discovery/exploitable/http/generic restaurantmenu
   discovery/exploitable/http/webwiz rte
   discovery/info disclosure/dns/cache snoop
   discovery/info disclosure/http/backup finder
   discovery/info disclosure/http/google ids
   discovery/info disclosure/http/interesting files
 Experimental
   experimental/rce
 Recon
   recon/contacts/enum/http/web/dev diver
   recon/contacts/enum/http/web/namechk
   recon/contacts/enum/http/web/pwnedlist
   recon/contacts/enum/http/web/should change password
   recon/contacts/gather/http/api/jigsaw/point usage
   recon/contacts/gather/http/api/jigsaw/purchase contact
   recon/contacts/gather/http/api/jigsaw/search contacts
   recon/contacts/gather/http/api/linkedin auth
   recon/contacts/gather/http/api/twitter
   recon/contacts/gather/http/api/whois pocs
```

To gather information about the available hosts in a target domain, you can use the Bing search engine:

```
recon-ng > load recon/hosts/gather/http/web/bing_site
recon-ng [bing_site] > set domain example.com
DOMAIN => example.com
recon-ng [bing_site] > run
[*] URL: http://www.bing.com/search?first=0&q=site%3Aexample.com
[*] www.example.com
[*] leb.example.com
[*] sos.example.com
[*] forms.example.com
[*] bankrobbers.example.com
[*] vault.example.com
[*] tips.example.com
[*] delivery.example.com
[*] omaha.example.com
[*] chicago.example.com
[*] foia.example.com
[*] 11 total hosts found.
[*] 11 NEW hosts found!
```

To see the result, we can issue the following Show hosts command:

```
recon-ng [bing_site] > show hosts
         host | ip_address | region | country | latitude |
longitude |
 | bankrobbers.example.com |
 chicago.example.com
 | delivery.example.com |
 foia.example.com
 forms.example.com
 leb.example.com
 omaha.example.com
 sos.example.com
 | tips.example.com |
 | vault.example.com
 | www.example.com |
```

This is just one of the examples of the recon-ng capabilities, you can consult the recon-ng website (https://bitbucket.org/LaNMaSteR53 /recon-ng/wiki/Home) to get more information about the other features.

[\*] 11 rows returned