
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 https://bitbucket.org/LaNMaSteR53/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, `recon-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:

```
root@kali:~# recon-ng

   _/_/_/    _/_/_/_/    _/_/_/    _/_/_/    _/      _/          _/      _/    _/_/_/
  _/    _/  _/        _/        _/        _/  _/_/    _/        _/_/    _/  _/
 _/_/_/    _/_/_/    _/        _/        _/  _/  _/  _/  _/_/_/_/  _/  _/  _/  _/  _/_/_/
_/    _/  _/        _/        _/        _/  _/    _/_/          _/    _/_/  _/      _/
_/    _/  _/_/_/_/    _/_/_/    _/_/_/    _/      _/          _/      _/    _/_/_/

            [recon-ng v1.41 Copyright (C) 2013, Tim Tomes (@LaNMaSteR53)]

[65] Recon modules
[7]  Discovery modules
[4]  Reporting modules
[1]  Experimental modules

recon-ng >
```

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

+------------------------------------------------------------------------------
--+

[*] 11 rows returned
```

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.