

Recon-ng

Objective:

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

Purpose:

WHOIS information can consist of location, registration and expire dates, contact information (email, phone numbers, etc.) and more about domain-name. The purpose of this lab is to use recon-ng to automate the discovery of this information.

Tool:

Kali Linux

Topology:

You can use Kali Linux in a virtual machine for the purpose of this lab.

Walkthrough:

Task 1:

Begin this lab by opening Kali Linux within your virtual machine. Then, as root user, open a terminal and type:

```
recon-ng
```


Task 3:

We will begin by gathering WHOIS information about a target domain-name. Since WHOIS information is available to anyone, it is ok to do this for any domain. The domain we will be targeting is, once again, “facebook.com”, but you can do this lab for any other domain you wish.

We will need to install modules from the marketplace to search for WHOIS information. We will begin by searching WHOIS for all related information regarding a target site. To do this, we first need to install the WHOIS search module. To do this, type:

```
marketplace search whois
```

We want to install the fourth option, which is “recon/domains-contacts/whois_pocs”. To do this, type:


```
root@kali: ~  
File Actions Edit View Help  
[*] Reloading modules...  
[recon-ng][whois_recon] > modules load recon/domains-contacts/whois_pocs  
[recon-ng][whois_recon][whois_pocs] > options set SOURCE facebook.com  
SOURCE ⇒ facebook.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 facebook.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] >
```

Then, to see information about this module and how it is used, type “info” and hit enter.

We are now ready to search WHOIS for information regarding “facebook.com”. Simply type “run” and hit enter to begin the search.

As you will see, various contact and location information will show up for facebook.com. This information will be automatically saved in our workstation.

```
root@kali: ~  
File Actions Edit View Help  
[*] URL: http://whois.arin.net/rest/pocs;domain=facebook.com  
[*] URL: http://whois.arin.net/rest/poc/BST184-ARIN  
[*] Country: United States  
[*] Email: bstout@facebook.com  
[*] First_Name: Brandon  
[*] Last_Name: Stout  
[*] Middle_Name: None  
[*] Notes: None  
[*] Phone: None  
[*] Region: Chicago, IL  
[*] Title: Whois contact  
[*] _____  
[*] URL: http://whois.arin.net/rest/poc/OPERA82-ARIN  
[*] Country: United States  
[*] Email: domain@facebook.com  
[*] First_Name: None  
[*] Last_Name: Operations  
[*] Middle_Name: None  
[*] Notes: None  
[*] Phone: None  
[*] Region: Menlo Park, CA  
[*] Title: Whois contact  
[*] _____  
_____ Return to Main Menu  
SUMMARY  
_____
```

Task 4:

We will now attempt to discover as many subdomains as possible, with their IPv4 address for facebook.com, using HackerTarget.com API. We will need to import the “hackertarget” module, as we did previously for whois_pocs.

Before we do this, you should first type “back” and press enter to quit out of the whois_pocs module. We will begin by searching the marketplace for “hackertarget” modules using:

```
marketplace search hackertarget
```

Only one option should show, which is “recon/domains-hosts/hackertarget”. You can highlight this option and press ctrl + shift + c to copy the path to the module. You can paste using ctrl + shift + v. To install the module use:

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

+-----+
+ For example, you can utilize the Java Applet, Metasploit Browser, C
+ | ential Harvester Path mapping all at | Version | e wh | Status | succ | Updated |
+ D | K |
+-----+
+-----+
+ through HTA files which can be used for Windows-based PowerShell exp
+ | recon/domains-hosts/hackertarget | 1.1      | not installed | 2020-05-17 |
+ | |
+-----+
+-----+
+ asloit Browser Exploit Method
+ | ential Harvester Attack Method
+ D = Has dependencies. See info for details.
+ K = Requires keys. See info for details.
+ | Multi-Attack Web Method
[recon-ng][whois_recon] > marketplace install recon/domains-hosts/hackertarge
t
[*] Module installed: recon/domains-hosts/hackertarget
[*] Reloading modules ...
[recon-ng][whois_recon] > █
```

marketplace install recon/domains-hosts/hackertarget

We then want to load the module using:

modules load recon/domains-hosts/hackertarget

We are now ready to begin searching HackerTarget for subdomain information regarding Facebook. First, set the source by typing:

options set SOURCE facebook.com

If you want to see some information around what this module is used for and how, simply type “info” and hit enter.

```
[recon-ng][whois_recon][hackertarget] > options set SOURCE facebook.com
SOURCE ⇒ facebook.com
[recon-ng][whois_recon][hackertarget] > info
Name: HackerTarget Lookup
The Author: Michael Henriksen (@michenriksen) of attacks through the web attack
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    facebook.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] >
```

Task 5:

Once this is done, type “run” and hit enter. You will notice a list of various subdomains associated with facebook.com appearing.


```
root@kali: ~
File Actions Edit View Help
[*] Latitude: None something different.
[*] Longitude: None
[*] Notes: None Attack method was introduced by white_sheep, emgent. This method
[*] Region: None will use replacements to make the highlighted URL link to appear l
[*] _____s replaced with the mal
[*] Country: None can edit the link replacement settings in the set_config if
[*] Host: cloud-x2p-edge-http-shv-02-del2.facebook.com
[*] Ip_Address: 163.70.145.213
[*] Latitude: None method will add a combination of attacks through the web att
[*] Longitude: None e, you can utilize the Java Applet, Metasploit Browser, C
[*] Notes: None iter/Tabnabbing all at once to see which is successful.
[*] Region: None
[*] _____nd perform PowerShell i
[*] Country: None HTA files which can be used for Windows-based PowerShell exp
[*] Host: cloud-x2p-edge-http-shv-02-dfw5.facebook.com
[*] Ip_Address: 31.13.93.219
[*] Latitude: None Attack Method
[*] Longitude: None User Exploit Method
[*] Notes: None Harvester Attack Method
[*] Region: None Attack Method
[*] _____
[*] Multi-Attack Web Method
_____TA Attack Method
SUMMARY
_____return to Main Menu
[*] 501 total (501 new) hosts found.
[recon-ng][whois_recon][hackertarget] > 
```