**RECON-NG**

**Lab Summary (What to expect)** - In this lab, we will be utilizing Recon-ng on Kali Linux to automate the retrieval of WHOIS information for a target domain, using the example domain "**facebook.com**." The walkthrough includes creating a dedicated workspace, installing and configuring WHOIS search modules, and discovering valuable details such as location, contact information, and registration data. Additionally, readers will learn to leverage the HackerTarget.com API to identify subdomains associated with the target domain, providing insights into potential vulnerabilities for further exploration.

**What is recon-ng** - Recon-ng is an open-source web reconnaissance framework used for automating information gathering in penetration testing and ethical hacking.

**Lab Objective** - Finding whois information on a target domain using recon-ng.

**Lab Purpose**- WHOIS details encompass location, registration and expiration dates, contact particulars (email, phone numbers, etc.), and additional data related to domain names. This lab aims to employ recon-ng for the automated exploration and retrieval of such information.

**Lab Tool** – Kali Linux.

TASK 1 –

* Fire up your kali linux as root. (Use sudo -I in the terminal).
* Type in recon-ng as shown below.   
  A screenshot of a computer

  Description automatically generated

TASK 2

* We can create our own lab and workspace using recon-ng based on our project needs. Use the command “workspaces create whois \_recon”.  
  

TASK 3

* We will begin by gathering WHOIS information about a domain. WHOIS is publicly available hence we can perform it on any domain.
* First thing we need to do is install modules from the market place. Use the command “marketplace search whois”.  
  A screenshot of a computer

  Description automatically generated

* We want to install the fourth option, which is “recon/domains-contacts/whois\_pocs”. To do this, type “marketplace install recon/domains-contacts/whois\_pocs”
* Then we load the module by using “modules load recon/domains-contacts/whois\_pocs”
* To begin searching using this module use the command “options set SOURCE facebook.com”.  
  A screenshot of a computer

  Description automatically generated

* To begin the search we simply need to write “run” and hit enter. This will display WHOIS information regarding the chosen domain(Facebook.com in this case).  
  A screenshot of a computer

  Description automatically generated

TASK 4

* Our next step is to search for any domains using ip address of facebook. We will be importing Hackertarget.com API’s module for that.
* Type back, hit enter to quit out of whois\_pocs module. Use the command “marketplace search hackertarget”. We only have one module that is recon/domains-hosts/hackertarget.
* To install it use “marketplace install recon/domains-hosts/hackertarget” and navigate to the module using “modules load econ/domains-hosts/hackertarget”.  
  A screenshot of a computer program

  Description automatically generated

* Lastly all we need to do is type “run” and hit enter. You will notice several domains from facebook.com appears.  
  A screenshot of a computer

  Description automatically generated

This information can be useful for an attacker who may be targeting Facebook. They can use this information to attack the various subdomains and their IP addresses associated with Facebook, as they may not all be equally secure, to find a way through their security.