Lab 4 – Recon-ng

**Objectives**

Our objective is to learn about and make use of Recon-ng. Sometimes with hacking we need to acquaint ourselves with tools we may not have much experience with. I am tasking you with learning about Recon-ng, our tool of the week. We have several modules to test.

It is not required to view, but if you so desire, you can find a tutorial video for recon-ng here:

* <https://www.youtube.com/watch?v=899Ls4is-ak>
* 2020 Hackerpsloit video series: <https://www.youtube.com/playlist?list=PLBf0hzazHTGOg9taK90uFjdcb8UgGfRKZ>
  + - Recon-ng developer intro to v. 5: <https://www.youtube.com/watch?v=WVEv7peHerw>

Some concepts are explained here. Some of Recon-ng is intuitive, but if you like to be shown, I strongly encourage you to watch this or other videos.

There are several others on youtube. Many web sites also contain usage information for this tool. Feel free to explore and find one that meets your needs. Some examples include the following:

* <http://null-byte.wonderhowto.com/how-to/hack-like-pro-reconnaissance-with-recon-ng-part-1-getting-started-0169854/>
* <https://hackertarget.com/recon-ng-tutorial/>
* <https://tools.kali.org/information-gathering/recon-ng>
* <https://github.com/lanmaster53/recon-ng>

**Information on Acquiring API keys**

Please note that for a number of these, you will need to acquire an API key, for services such as Bing, Flickr, etc. You can find some information here:

* <https://github.com/lanmaster53/recon-ng-marketplace/wiki/API-Keys>

Some cost money, but all the ones for this can be done with the free versions. Some of the information on this page is outdated or incomplete, so you may need to do further google searches to figure out how to obtain the necessary API keys. Please note that API keys are often used by developers for projects they are developing, so in order to obtain an API key, you may have to register as a developer or fill in placeholder information for a project that you may or may not come back to later on.

For questions 1-8, provide screenshots. Provide sufficient screenshots, so that I know you answer all parts of the question, if one is insufficient.

1. Use recon-ng to do a bing\_linkedin\_cache search for a particular car rental company. You choose. Give me the name of someone in IT?

2. Use recon-ng whois\_miner to give me possible IP addresses for NDSU.

3. Use the hibp\_breach to checked compromised accounts from breaches to see if your email address has been compromised. Check for three friends or associates.

4. Use the bing\_domain\_api to enumerate hosts for sdsu.edu. How many hosts did you find?

5. Sign up for the built with API and run it on ndsu.edu. http://api.builtwith.com/ Did you discover any other unique hosts not listed in the bing\_domain\_api search? What is its IP address?

6. Use hackertarget to enumerate hosts for ndsu.edu.

7. Sign up for flickr API: <https://www.flickr.com/services/api/misc.api_keys.html> Perform search to show images within 1 km of the DSU campus. (Hint: Use Google to find longitude and latitude coordinates.)

8. Use one other module of your choice in recon-ng to perform a search on a specific site/person/place/entity.

9. Same as #8 – find another, non-trivial module to explore.

**Deliverables**

These MUST be contained all in one PDF or DOC/DOCX.

You may select **two questions** to skip if you so desire.