Lab 03 - Reconnaissance

# Overview

Your job is to do some initial **passive** reconnaissance of a target. You should submit only the screenshots of the results from the queries that you run. Please submit all of the screenshots in one Word document or PDF. Do not submit them as separate images.

Note: When running the following tools be very careful and if you think that the tool you’re about to run is not passive in any way **stop** and **ask**. Do not a run a tool without first understanding what it does.

**Target: DSU.EDU**

# Whois & DNS & Mail information

Perform the following using online tools of your choosing:

1. Gather DNS information
2. Gather site information
3. Gather mail information

# Recon-ng

Perform the following using recon-ng:

1. Create a workspace for your target, use your first initial + last name as the name
2. Add a company (Dakota State University)
3. Add the **dsu.edu** domain name
4. Run the following modules within Recon-ng:
	1. recon/domains-hosts/bing\_domain\_web
	2. recon/domains-hosts/google\_site\_web
	3. recon/domains-hosts/netcraft
	4. recon/hosts-hosts/resolve
	5. recon/hosts-hosts/reverse\_resolve
	6. recon/domains-contacts/pgp\_search
	7. recon/contacts-credentials/hibp\_paste
5. Create an HTML report with your name as the CREATEDBY and DSU as the CUSTOMER
6. Open the HTML report in a browser and take a screenshot of the summary pane. This should have you name at the bottom of the page.

# Discover Scripts

Install the Discover Scripts from Lee Baird on your Kali VM (<https://github.com/leebaird/discover>) and complete the following:

1. Launch the discover.sh file
2. Once it is running, choose **1. Domain** and then select **1. Passive**
3. Enter in your name as the company name and **dsu.edu** as the domain name
4. Once the discover scripts have finished, open the report in a browser and take a screenshot

# Your Choice

1. Find another tool that is used to perform information gathering and footprinting of a target
2. Install/Run the tool and collect its output
3. Explain how the information provided by the tool could be useful
4. Do not use active tools such as nmap!