CSC436 Lab 02

Take only the screenshots of your work as indicated below and save them to a single Word or PDF document. D2L makes it really tough to grade PNG and other image files, so you must turn in a PDF or Word document.

- You may do this lab in your IA Lab VM or your own desktop. If you chose to do this in your own desktop, make sure to include your name in the screenshot (type it somewhere or whatever you need to do).
- Be EXTREMELY careful in what you are doing during these labs. If you have any questions or are unsure if what you are running is ok, please ask beforehand. It is your responsibility to remain passive in the info gathering phase and to only access systems you are authorized to do so. This is your responsibility.

Recon-Ng

Perform the following in the Recon-Ng utilitiy:

1. Create a workspace for your target, use your first-initial + last name (e.g. **cwelu**).
2. Add a company (Dakota State University)
    a. In the description, enter in “The university that (your name) attends!”
3. Add the **dsu.edu** domain name.
4. Run the following modules within Recon-ng:
    a. recon/domains-hosts/bing_domain_web
    b. recon/domains-hosts/google_site_web
    c. recon/domains-hosts/netcraft
    d. recon/hosts-hosts/resolve
    e. recon/hosts-hosts/reverse_resolve
    f. recon/domains-contacts/pgp_search
    g. recon/domains-contacts/whois_pocs
    h. recon/contacts-credentials/hibp_paste
5. Create a HTML report with your name as the CREATEDBY and DSU as the CUSTOMER fields.
6. Open the HTML report in a browser and take a screenshot of the summary pane expanded. This should have your 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). Once that is done, complete the following:

1. Launch the discover.sh file.
2. Once Discovery Scripts is up and 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 of the Passive Recon report summary (**Reports → Passive Recon**).

SpiderFoot

Install SpiderFoot (http://www.spiderfoot.net) on your Kali VM and complete the following:

1. Launch SpiderFoot and start a New Scan.
2. Enter in your name for the Scan Name.
3. For the Seed Target, enter **dsu.edu**
4. Be sure to unselect all checkboxes in the By Required Data tab and the By Module tab.
5. In the By Module tab, Checkmark only the DNS module.
6. Take a screenshot of the Browse tab of the completed scan similar to the one below:

Your Choice

1. Find another tool that is used to perform information gathering and footprinting of a target.
2. Install this tool and launch it. Take a screenshot (including your name) of your VM with the tool open. You do not need to run a scan.