Lab and Homework 1
Reconnaissance

As with most assignments, pending on time, we will start working on these in class as a lab, discuss any possible questions. You will need to submit these on Oaks by the due dates.

1. (**Deadline: Jan 25**) Find three technology companies that you have never heard before. These can be from a news website or a simple search. Complete a thorough ***passive*** reconnaissance on the company with all the tools included in ch. 2 of the pen testing textbook and the site: http://www.securitysift.com/passive-reconnaissance/. Write a detailed report on your results. Include screenshots, the exact commands that you ran, your methodology and rationale. Your report should have minimum length 500 words. **(4 pts)**
2. (**Deadline: Feb. 8**) Automate the process: Write a Python or Java or C++ program to perform information gathering. *The goal of this project is not to develop the most thorough information gathering tool. It is to show you that everything that you can do manually, you may use a program to automate and perform the process faster*.

   The program may: run any command line tool that you ran manually during the first lab, or it may run searches on specific websites such as google, netcraft, and who.is (or more sites that you may find). The inputs of the program should be:

   a. The name of the company
   b. The type of information gathering you would like to perform. You need to include **at least 3 input options** such as: IP addresses, email address domains, email addresses, DNS servers, files with specific extensions, employer data, employer tweets etc. You can be creative and include additional options. No GUI is needed, just command line interface. The program may ask for example: “What kind of information do you want to gather: IPs, emails, DNS server?” or even offer more options.
   c. Then your program may either run URL searches or command line commands to gather the data or both. Your program may download raw files and post process them.
   d. Organize and save the data: save the data in a file or different files with a clean and easy to search format and names. You may have one file called: “IPs.txt”, one file called “host_names.txt” etc. If you are saving data, such as IP addresses, use a clean and easy to search format. If you are downloading files from the web you may create a folder for these files, for example: “company_files” folder. Use tabs, proper indentation, csv files, or anything else you find useful to save your data.
   e. You may print a message at the end of the search that your program has completed information gathering.
   f. Submit your code file(s) with proper comments. Include a README if your program needs specific setup of libraries or I need to run it on a specific environment such as Kali Linux.

g. Make sure to perform only OSINT and passive reconnaissance. Do not use any of the active reconnaissance tools that were discussed in ch. 2 of the textbook “Intro to pen testing”! You will lose many or all points depending on how many active recon tools you used!!

(8 pts)

Note: you may use google resources and even coding snippets as long as you cite these properly. Here are some sources that I have found and you can use (do not forget the citation as a comment in your code):

Python:

http://stackoverflow.com/questions/3898574/google-search-using-python-script
http://stackoverflow.com/questions/2376798/how-to-write-a-python-script-to-search-a-website-html-for-matching-links
http://stackoverflow.com/questions/89228/calling-an-external-command-in-python

Java:

http://stackoverflow.com/questions/3727662/how-can-you-search-google-programmatically-java-api
http://stackoverflow.com/questions/21919245/google-search-with-java
http://alvinalexander.com/java/edu/pj/pj010016

C++:

http://stackoverflow.com/questions/1397313/programatically-get-google-search-results
http://www.cplusplus.com/forum/general/46477/
http://www.cplusplus.com/reference/cstdlib/system/