Lab 2
Open Source Intelligence (OSInt) and No Tech Hacking (NTH)

The goal for this lab is to practice on the first step of pen testing: Reconnaissance. Find one technology company that you have never heard before. These can be from a news website or a simple search. Complete a thorough reconnaissance on the company. Your goal is to find:

1. Something that should not be out there and it is, such as how they perform maintenance, patches, maybe even intellectual property. You would be surprised how many companies leave important documents like these accessible through the network.
2. Something not as obvious that could get the company in trouble. For example, a job posting may ask for specific skills in a specific technology. You just found something that could make this company vulnerable to a hacker.

Write a report on your results. Show that you used sophisticated google searches and OSInt tools. Include screenshots, the exact commands that you ran, your methodology and rationale. Your report should have minimum length 500 words.

Note 1: I need you to find something substantial and not just the CEOs address or things that are obvious. I want you to think outside of the box for items 1, 2.

Note 2: Depending on the severity of what you find, we may notify the company. Remember that you have signed an ethics agreement to report vulnerabilities, not take advantage of these.


Recommended Sources:
Google hacking database: https://www.exploit-db.com/google-hacking-database/
OS Int Framework: http://osintframework.com/