Information Gathering

Part I

Read the section in the CEH text about “Employee and people searches”. Then, see how much information you can find about an individual (i.e. your parents, yourself, ???)

Note: I wouldn’t pay for any service like a background check. Just find what you can using publicly available tools.

See if you can answer the following questions:

- Places person has lived (addresses)
- Degrees
- People (family, friends, etc…)
- Important dates
- Employment history
- Phone numbers
- Photos (yikes…)
- Anything else that a hacker could make use of.

Create a document that has your conclusions a of the information you found. Maybe a 1 page analysis. What information surprised you? How hard was it to get the information? Summarize what you did to find information. Maybe put some samples of the information in an appendix page or something. (I don’t really care about the information. I care about what you learned as you did this reconnaissance.)

Part II - Nmap

All the following can be done using nmap. You aren’t restricted to using nmap. (See chapter 3 for help)

- Identify active machines on the network that `144.38.193.250` is attached to. The username for the machine is `it4510`, the password will be given in class. We aren’t doing any hacking yet! Just information gathering. Nmap is installed on that machine. Create a table that looks something like this: (though you will fill in only some of the columns later)

ip	hostname	ports	os	services and versions
1.2.3.4	example.com	22,33,	ubuntu	apache2.2 version 8
1.2.3.5	foo.com	22,33,	windoze	something and telnet version5 and ftp version 12
1.2.3.6	foo.com	22,33,	windoze2	

-Make a note of the ports in your document. The `-O` option of nmap does give back operating system information, but requires root. There is another way to see OS stuff, without using root).h

- What ports are open on the gateway of that network. What version of those services are running? (As much as possible) Add it to your table.

To Submit

Create one pdf with both parts above. Upload to canvas.