**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 me. Hint: Joseph L Francom

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 I have lived (addresses)
- Degrees
- People (family, friends, etc...)
- Important dates
- Employment history
- Phone numbers
- Photos (yikes... there is an old scary-looking one out there) (of course they are all probably scary ;-
- Approximate salary? (It’s there)
- Anything else that a hacker could make use of.

Create a document that has a summary of the information you found. I don’t want to see printscreens, just summarize what you have found. Maybe with subsections as outlined in the list above. (I am not going to read more than 2 pages)

**Part II - Nmap**

All the following can be done using nmap. You aren’t restricted to using nmap.

- Identify active machines on the network that [nitrogen.cs.dixie.edu](nitrogen.cs.dixie.edu) is attached to. 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)

<table>
<thead>
<tr>
<th>ip</th>
<th>hostname</th>
<th>ports</th>
<th>os</th>
<th>services and versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2.3.4</td>
<td>example.com</td>
<td>22,33</td>
<td>ubuntu</td>
<td>apache2.2 version 8</td>
</tr>
<tr>
<td>1.2.3.5</td>
<td>foo.com</td>
<td>22,33</td>
<td>windoze</td>
<td>something and telnet version5 and ftp version 12</td>
</tr>
<tr>
<td>1.2.3.6</td>
<td>foo.com</td>
<td>22,33</td>
<td>windoze2</td>
<td></td>
</tr>
</tbody>
</table>

- Choose 2 of those ip’s in your table and see what ports are open. One of these ip’s should be a mac, one should be a Linux machine. Make a note of the ports in your document. (Hint: I think all the macs are at one end of the network range. The \(-\) option of nmap does give back operating system information, but requires root. There is another way to see OS stuff, without using root).

  - Make sure you run a UDP scan as well. Any changes to your list?

- 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.