Assignment 6: Python Traceroute
CSEC141: Introduction to Cybersecurity
Assigned: Friday, March 26, 2021
Due: Monday (midnight), April 5, 2021

For this assignment, we continue with you keeping present on cybersecurity topics, as well as to have you work with writing some Python programs. Again, all written answers to the questions below MUST be written in a text-only document titled `Answers.txt` (e.g. using `Notepad++` on Windows, or `nano` on Linux, not with Word or another editor that uses some non-text formatting (for example TextEdit on a Mac writes to RTF, which is not acceptable.) You can test your final `Answers.txt` document by opening it in Kali using `nano` and making sure it really is just text. When writing an answer, you MUST write each solution on a single line, that is, do not hit a carriage return even if the line is long. Just let it wrap around. Also name the answer EXACTLY what I ask you to name it, so if I say write `Solution1:`, do not make it `solution1:` or `Solution 1:` or anything else. When I grade the assignment, your file must be `grep`-able, so that my using `grep "Solution1:" Answers.txt` should provide me with your full answer to that question. When finished with the assignment, zip up (as a .zip file) all of the screenshots, programs, and your `Answers.txt` file into a zip file called `Assignment6_DanielP.zip` (where obviously, you replace DanielP with your own first name and last initial) and submit it on Blackboard.

1. Again you are to find recent tweets that are particularly interesting to you pertaining to cybersecurity. While you will write up five tweets, you may use any of the people you follow (including any of the people I showed you or any you have added). For each of these people, post a link to a tweet that is particularly interesting, and summarize it in about two sentences each, using `Solution1A:`, `Solution1B:` etc for each. Do not just cut and paste, and do not just take the first line or two of the main content of the tweet. Actually summarize it for yourself. For example:

   ```
   Solution1A: Link: https://twitter.com/Th3G3nt3lman/status/1268832976919560193
   Shows how ServiceNow (cloud-based company offering IT services management)
   exposed information it should not.  In its Knowledge Management application, once
   an entry is created with endpoint of form KB00xxxx, they are publicly reachable and
   but should not be, leaking passwords, corporate domain tokens, and Personally
   Identifiable Information (PII) between employees.
   ```

   remembering that ALL of the above line is a single line (no carriage returns except after the final word `employees.`).

2. Again find five (5) interesting posts from any of the security blogs you wish (including those I showed you). For each, using `Solution2A:`, `Solution2B:` etc., find a post and summarize it much like you did in question 1.

3. Using the sample program, `test_traceroute.py`, modify it to do as follows. Noting that the `traceroute` manpage shows a number of options, I would like to include two of them, namely `-f first_ttl` and `-m max_ttl` where the first provides the first `ttl` which can be different from 1, and the second provides the max. Your code should default to 30 as the max unless the flag is set. To read in commandline arguments, see how the following code, called `commandline.py`, works when entering `commandline.py 1 2 3`:

   ```
   import sys
   print('length of commandline arguments = ', len(sys.argv))
   print(sys.argv[0])
   print(sys.argv)
   ```

   You will not need to error check your command line arguments. That is, I will only enter the following options without trying to trick you with something else:

   - `sudo python3 test_traceroute.py`
   - `sudo python3 test_traceroute.py -f 3`

- `sudo python3 test_traceroute.py -m 10`
- `sudo python3 test_traceroute.py -f 3 -m 10`

where of course, the 3 and 10 can be other numbers. Your code should loop through the appropriate `ttl` values once each (not 3 times like the actual traceroute code does.)