James Tourtellotte
IT 223 - B01
6/22/2024
GMU

Password Checker Assignment

Background Information and Directions

Users will often try to create passwords using something easy to remember, such as their last name, without understanding that large datasets of pre-computed password hashes ("rainbow tables") make it very easy for a hacker to find your password if using a weak password.

1. Most operating systems hash your password to obscure the plaintext. Open https://www.fileformat.info/tool/hash.htm up in your browser and type your last name in the String hash text field - click on the Hash button to hash your last name.

2. Scroll down and copy the MD5 and SHA256 hashes of your last name into memory.

3. In a separate browser window, open https://crackstation.net/ , paste the hashes of your last name into the text box, click on the CAPTCHA box to confirm you are not a robot, and click on the "Crack Hashes" box.

4. Note the color that appears. If it is green, that hash (your last name) is located in the rainbow table (see it displayed in the "Result" column).

5. Repeat steps 1 through 3, varying your last name, until you can find a variation of your last name that is not in the table.

Answer the following questions:

1. How many attempts did it take to find a variation of your last name that was not in Crack Station's rainbow table?

I tried this and it did not work. I am in there like swimwear

2. How would "salting" defeat a rainbow table?

It makes it non-feasible, too time consuming to crack something like this as it is impossible.