Trent Giever

Case Project 11-1

7/26/18

Testing Password Strength

Slightly different than current passwords

|  |  |  |  |
| --- | --- | --- | --- |
| Passwords | How secure is my password | Password checker | Password meter |
| Badhear99 | 4 Days, add tt22 158 thousand years | 49 % strength add tt22 then is 75% | Add tt22 |
| Sear9999! | 1 Month, add at33 5 million years | 50% strength, add at33 84% | Add at33 |
| Chime9999? | 10 years, add ok44 415 million years | 62% add ok44 91% | Add ok44 |

The age of hackers has made one thing clear and that is everyone hates passwords. Many people use a same password for many sites, and I do the same on sites that don’t have any real information wanted from a hacker like bank account numbers and card numbers. The idea of strong passwords is the goal of everyone, but at the same time it is hard to memorize random characters. Testing password strengths is good to know which easy to memorize pattern is a good password to use.

Password strength meters varied on the three sites very differently. The first site How Secure is my password gave helpful hints by having a pattern detection program for common traits. The downside is with computers getting faster and password cracking programs getting more complex the amount of time seemed very off from reality. The second website password checker gave the time needed by the common ways to crack including computers, GPU, and botnets, and seemed the most accurate of the three websites. But also lacked measuring the time from a pattern detection attack. The third website password meter showed the formulas it used, but a password that can be cracked in 6 days by a botnet from password checker scoring a 94% had something wrong with it and seemed more suited for the wild west days of dialup internet.

My passwords are not like “password” level of security and are stronger than most. But still follow the pattern of words then numbers that allow an attacker easy. The sites do show the average user that certain patterns are harder to detect for a pattern attack program. Another thing is that password checker websites when generating passwords are not accurate. The testers rate by how many letters, numbers, special characters without much consideration for the actual contents (Stockley, 2015). “It is evident that the commonly-used meters are highly inconsistent, fail to provide coherent feedback on user choices, and sometimes provide strength measurements that are blatantly misleading” (Stockley, 2015). What I have been doing for passwords is for websites that contain no information except my name is to use my common password to make it easy to login, and for websites like Amazon and Numerica have a unique password for just that website. With how complex password cracking is, it is not if, but how fast will the password last with the program.

Overall the best course of action is to keep unique passwords for websites with wanted information in a password book. Some believe that password storing software is secure, but it is not. My uncle (first hired at Micron, top 25 payed before retiring) was telling me a few years ago to use the one he uses, and a few days later the program got hacked exposing the programs user’s passwords. The best program is random, but also able to remember. I like a website called password generator, and it is run on the browser to create a password with letters, numbers, and special characters to help remember the random gibberish the site creates a sentence out of the password. The thing with actual password strength tests is the best password today could be the worst password tomorrow.