Lab 7 - Password Cracking

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

The purpose of this lab is to learn more about passwords and password complexity. For this lab, you will use a web based password analyzing tool at <https://www.grc.com/haystack.htm> provided by Gibson Research Corporation.

If your password is the “needle” then the ability to hide your password depends on making the “haystack” as big as possible. You will also learn that some of the “truths” about passwords are myths. For example, which of the following two passwords is stronger, more secure, and more difficult to crack?

D0g…………………

PrXyc.N(n4k77#L!eVdAfp9

We have been told that clearly the second password is the better one because it is more secure. It is also impossible to remember. The Gibson Research tool, however, will show that the first password is not only easier to remember, but is 95 times more difficult to crack that the second password.

1. **Read the entire documentation on the web site, you will find it very interesting and informative. The information on this site is part of your course work and will appear on future tests.**

**Exercise 1: Using the 10 most common passwords used in the world.**

This list was compiled by PCMag.com and is something every “bad guy” has memorized. If your password is among this list, you may as well hand over your wallet or purse to bad guy right now.

1. Enter the password list below and record the Search Space Size, as a power of 10 and Offline Fast Attack Scenario. The first parameter measures the size of the haystack, and the second measures the speed of cracking based on current PC installed cracking tools. **[0.4 Marks]**

|  |  |  |  |
| --- | --- | --- | --- |
| **Rank** | **Password** | **Search Space Size (power of 10)** | **Offline Fast Attack Scenario** |
| 1 | password | 2.17 x 1011 | 2.17 seconds |
| 2 | 123456 | 1.11 x 106 | 0.0000111 seconds |
| 3 | qwerty | 3.21 x 108 | 0.000321 seconds |
| 4 | abc123 | 2.24 x 109 | 0.0224 seconds |
| 5 | letmein | 8.35 x 109 | 0.0835 seconds |
| 6 | monkey | 3.21 x 108 | 0.00321 seconds |
| 7 | myspace1 | 2.90 x 1012 | 29.02 seconds |
| 8 | password1 | 1.04 x 1014 | 17.41 minutes |
| 9 | link182 | 8.06 x 1010 | 0.806 seconds |
| 10 | Yuvraj | 3.88 x 108 | 0.00388 seconds |

**Exercise 2: Adding Complexity and Length to Password**

1. Now you will analyze how the search space and complexity influence the ability to crack the password. **[0.4 Marks]**

|  |  |  |  |
| --- | --- | --- | --- |
| **Rank** | **Password** | **Search Space Size (power of 10)** | **Offline Fast Attack Scenario** |
| 1 | 460 | 1.11 x 103 | 0.0000000111 seconds |
| 2 | 4609 | 1.11 x 104 | 0.000000111 seconds |
| 3 | 4d6A09 | 5.77 x 1010 | 0.577 seconds |
| 4 | 4d6A09 | 5.77 x 1010 | 0.577 seconds |
| 5 | 4d6A0%9 | 7.06 x 1013 | 11.76 minutes |
| 6 | SeNeCa | 2.02 x 1010 | 0.202 seconds |
| 7 | SeNeCa/ | 3.24 x 1013 | 5.41 minutes |
| 8 | SeNeCa// | 2.76 x 1015 | 7.66 hours |
| 9 | SeNeCa//// | 1.99 x 1019 | 6.33 years |
| 10 | SeNeCa//?? | 1.99 x 1019 | 6.33 years |

1. Clearly the “SeNeCa//??” password is easier to remember than “4dA0%9”. What conclusion can your draw from the above Exercise: (write 3-4 sentences to explain your conclusion) **[0.275 Marks]**

* Upon doing the above exercises, I have understood the following things:
* Passwords do not always need to be so complex in length and made up of garbage values so that nobody can guess it, also one needs to keep in mind that a 2-3 character long password isn’t good at all. Yes, it should have a certain length, but it is not true that the longer, the better. Shorter passwords can outperform the longer ones if we include different characters and use a character mixture which is explained further.
* Instead, it is a better practice to use each type of character in a password, so that a simple password like “seneca” can be written as “Seneca!2022” which is way harder to guess. Also, character mixture in the passwords can help a lot in increasing the complexity of a password.
* Lastly, including a sequence of characters in our password called padding is a good practice, where we can have our own sequence of characters in the password, this makes much much harder to crack or guess a password for the hackers.

**Exercise 3: Cracking Hashes.**

All operating systems store passwords as hash values, either MD5 or SHA-1. There are various tools designed to steal the password hash value. For these tools to work, however, the hacker needs local access to the machine. (If unauthorized people have local access to a workstation, you have a larger security problem than just passwords). Once he/she has captured the hash values, the value is compared offline to a database of hash values to find a match. If the hacker finds a match to the hash value he\she assumes that must be the password. Take the following passwords in the table below and convert to hash values.

1. Navigate to the web page <http://passwordsgenerator.net/md5-hash-generator>
2. Enter the following passwords to convert to MD5 hash values. Copy the hash value to the table below. **[0.4 Marks]**
3. Navigate to the web page <https://crackstation.net> . Read the documentation on the web site.
4. Use your phone or wrist watch to record the approximate time it takes to crack the password hash. (in seconds)
5. Enter the Captcha code and Click Crack Hashes

|  |  |  |  |
| --- | --- | --- | --- |
| **Rank** | **Password** | **MD5 Hash Value** | **Approximate Cracking Time** |
| 1 | password | 5F4DCC3B5AA765D61D8327DEB882CF99 | 0.89 seconds |
| 2 | password1 | 7C6A180B36896A0A8C02787EEAFB0E4C | 1.03 seconds |
| 3 | Passw0rd | D41E98D1EAFA6D6011D3A70F1A5B92F0 | 1.18 seconds |
| 4 | P@ssw0rd | 161EBD7D45089B3446EE4E0D86DBCF92 | 1.25 seconds |
| 5 | P@ssw0rd. | 4D934E4CDE0DCE1D9B3ECAF84F5672B2 | 1.27 seconds |
| 6 | P@ssw0rd.. | 628C98267EDFD4766DB2BE05E3B2105F | 1.39 seconds |

1. What conclusion can you make, from the above exercise, about the optimum, character mix? (write 3-4 sentences to support your answer) **[0.2 Marks]**

* What I understand by doing the above exercise is that it is very crucial to have a character mix password. Upon hash cracking the passwords which did not contain any character mix, the results just popped up almost instantly (these times that I recorded, it may be different in actual) and was having the exact match in the database. Whereas, the passwords with character mix took a little more time to crack.

1. What does padding (repetition of a character) do for the hacker and for us? (one sentence) **[0.2 Marks]**

* One thing that I noticed was upon going down the list of passwords, it was not only the time which had a little difference but, for the passwords ranking above from 1 to 4, they were having the exact match in the database whereas the P@ssw0rd.. which was having the .. padding was not found in the database or so-called (pre-computed lookup tables) which shows that it makes harder for the hacker to crack our passwords and we can be on the safer side.

**Grading:**

* **LearnName\_Lab7\_Password.docx** – complete the tables and questions
* submit the lab file using the link on MySeneca

Remember replacing learnname with your name for submission.

Submit using the Lab 7 Submission link under MySeneca\Graded Work