Lab 7 - Password Cracking

Pavneet kaur

128287216

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

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.

Note that this lab is largely based on metrics and methods presented by the Gibson Research Tool and may not reflect the real-world “security” environment in which we use passwords. Use of passwords generated following these guidelines are not guaranteed to be more secure (more difficult to guess), they simply serve to illustrate how an algorithm (such as the Gibson Research Tool) would approach such a password or series of passwords. Someone with intent may focus their efforts in ways that the algorithm does not account for and render the attack scenario timeline invalid.

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. (20 Marks)**

This list was compiled by PCMag.com as well-known weak passwords. If your password is among this list, consider changing it.

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.

|  |  |  |  |
| --- | --- | --- | --- |
| **Rank** | **Password** | **Search Space Size (power of 10)** | **Offline Fast Attack Scenario** |
| 1 | 123456 | 1.11 x 106 | 0.0000111 seconds |
| 2 | password | 2.17 x 1011 | 2.17 seconds |
| 3 | 123456789 | 1.11 x 109 | 0.0111 seconds |
| 4 | 12345 | 1.11 x 105 | 0.00000111 seconds |
| 5 | 12345678 | 1.11 x 108 | 0.00111 seconds |
| 6 | qwerty | 3.21 x 108 | 0.00321 seconds |
| 7 | abc123 | 2.24 x 109 | 0.0224 seconds |
| 8 | tiffany | 8.35 x 109 | 0.0835 seconds |
| 9 | password1 | 1.04 x 1014 | 17.41 minutes |
| 10 | <your first name> | 1.05 x 1012 | 10.48 seconds |

**Exercise 2: Adding Complexity and Length to Password (20 Marks)**

1. Now you will analyze how the search space and complexity influence the ability to crack the password.

|  |  |  |  |
| --- | --- | --- | --- |
| **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) **(5 Marks)**

* Although “4dA0%9” password is difficult to remember, but it does not mean that it is strong password. This is because the length of the password plays a vital role in the strength of the password and if the length of the password is small, it can be easily created using padding with a simple password which is easy to remember. This will make it hard to guess or hack the password but easy for the user to remember. We should never create a password which is made using difficult and forgettable words, special characters and numerical values. Instead of that to make password easy to remember we should create a password of memorable word using uppercase, lowercase and some special characters which are meaningful for us. This kind of passwords are easy to remember but hard to crack.

**Exercise 3: Cracking Hashes. (12 Marks for Table)**

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.
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 | DC647EB65E6711E155375218212B3964 | 0.5 second |
| 2 | password1 | 7C6A180B36896A0A8C02787EEAFB0E4C | 0.5 second |
| 3 | Passw0rd | D41E98D1EAFA6D6011D3A70F1A5B92F0 | 0.5 second |
| 4 | P@ssw0rd | 161EBD7D45089B3446EE4E0D86DBCF92 | 0.5 second |
| 5 | P@ssw0rd. | 4D934E4CDE0DCE1D9B3ECAF84F5672B2 | 0.5 second |
| 6 | P@ssw0rd.. | 628C98267EDFD4766DB2BE05E3B2105F | Not found |

1. What conclusion can you make, from the above exercise, about the optimum, character mix? (write 1-2 sentences to support your answer) **(2 Marks)**

* **After doing the above exercise I came to know that strong passwords does not mean complex words that are hard to remember, but are mixture of uppercase, lowercase and special characters. Password in only lower case, only special characters are considered as weak passwords which will be hacked and guessed easily by the hacker. So password should be of a word and symbol combination which is easy to remember but hard to guess.**

1. What does padding (repetition of a character) do for the hacker and for us? (one sentence) **(2 Marks)**

* **Padding can be considered as a negative thing for hackers, because it makes it harder for them to guess the password. But on the other hand a positive thing for us, which makes our password easy to remember and more secure.**

There are many approaches to understanding password complexity in the real world, where brute-force cracking attempt is more than simply trying every combination of characters. One of the better explanations comes from this comic: <https://m.xkcd.com/936/> (explained in more detail here <https://explainxkcd.com/wiki/index.php/936:_Password_Strength>). Choose your passwords carefully!

**Grading:**

* **LearnName\_Lab7\_Password.docx** – complete the tables and questions
* submit the lab file using the link on MySeneca
* Lab is marked out of 61, worth 1.875% of your final grade.