Date: 27 February 2023

Subject: Cracking Leaked Passwords Database.

I have cracked some of the leaked passwords using **Hashcat**. The results are as follows:

HASH	TYPE	RESULT
`e10adc3949ba59abbe56e057f20f883e`	MD5	123456
`25f9e794323b453885f5181f1b624d0b`	MD5	123456789
`d8578edf8458ce06fbc5bb76a58c5ca4`	MD5	qwerty
`5f4dcc3b5aa765d61d8327deb882cf99`	MD5	password
`96e79218965eb72c92a549dd5a330112`	MD5	111111
`25d55ad283aa400af464c76d713c07ad`	MD5	12345678
`e99a18c428cb38d5f260853678922e03`	MD5	abc123
`fcea920f7412b5da7be0cf42b8c93759`	MD5	1234567
`7c6a180b36896a0a8c02787eeafb0e4c`	MD5	password1
`6c569aabbf7775ef8fc570e228c16b98`	MD5	password!
`3f230640b78d7e71ac5514e57935eb69`	MD5	qazxsw
`917eb5e9d6d6bca820922a0c6f7cc28b`	MD5	Pa$$word1

f6a0cb102c62879d397b12b62c092c06	MD5	bluered

The hashing algorithm which has been used is MD5. The level of protection offered by this algorithm is too weak. Brute force attacks on MD5 hashes are quite fast. Also the combination of characters used in the passwords are alphabets (small and capital, both), digits from 0-9 and some special characters. The maximum length of the passwords is nine characters. Ignoring the passwords with special characters and taking into consideration just the digits and alphabets combined with the maximum length of 9 characters, it will take approximately 7 hours for a hacker to crack these passwords even if they resort to brute force methods. This estimate will be around 2 days if we consider the symbols and special characters as well.
(Source: https://www.hivesystems.io/password-table)

Tools such as Hashcat make it instantaneous to crack such passwords.

Observations on organization password policy:

- Most of the passwords are commonly used and can be easily cracked.
- 69.23% of the cracked passwords do not use any combination of capital letters, numbers and special symbols together.
- Salting has not been implemented in any of the cracked passwords.

Changes to be made in password policy:

- 38.46% of the cracked passwords have an easily predictable sequence of numbers (123456, 123456789, 111111, 12345678, 1234567) and another 23.07% use common words with slight variations which can be easily guessed (qwerty, password, password1). We can stop using such common phrases and instead use a mixture of various characters.
- The password length can be increased to 11 or 12 characters. Using a password of length 11 made up of numbers, uppercase and lowercase letters and symbols will take nearly 34 years to crack with brute force methods.
- Salting can be implemented to add complexity to the passwords.

Sincerely,
Saicharan Ritwik Chinni.