TASK- CRACK LEAKED PASSWORD DATABASE

Respected Sir/Ma'am,

I have tried to crack the passwords from the leaked hashes given to me. It is to inform you that after analyzing the results, I have pointed out a number of irregularities and flaws in the organisation's password policy and listed some solutions and steps to overcome these challenges.

The passwords I found did not take a considerable amount of time. **13 out of the 19 given passwords was immediately cracked using Dictionary attack**. And after an hour or so, the **other 6 hashes were also cracked using Combinator and Masking attack** using ***Hashcat***.

The passwords which are leaked, were using ***MD5 hash algorithm***. Though MD5 is widely used but it is **considerably much weaker** because it is **prone to hash collision** i.e., it is possible to create the same hash function for two different inputs.

I consider the use of MD5 as ***Below Average***. I would recommend the usage of ***SHA-256 algorithm*** which is **much more secure than that of MD5 algorithm** and **no collision has been recorded** till today for the SHA-256. Though *MD5 is faster in comparison but security must be the first priority*.

The organisation's privacy policy is not up to the mark. I have listed below some observations-

- The **minimum length of passwords is 6** and **maximum length is 9** for the given.
- There are ***no measures to mandatory usage*** of *at least 1 special characters, 1 number, and letters* to make the passwords strong.
- There are **no restrictions to using the usernames** as a part of their respective passwords which makes the passwords vulnerable.

For the organisation to prevent their private data from being vulnerable, they should follow the below listed points. These will make the passwords hard to crack.

- A strong password must be ***minimum 8-10 characters long***.
- A strong password should **contain different types of characters**, including *uppercase letters, lowercase letters, numbers and characters.*
- They should ***discourage or prevent user to include any personal details*** while forming the password — specifically name, username, company name, DOB, etc.
- The organisation must keep **notifying the user to change his/her password after a specific amount of time**. Previous *NIST guidelines recommended forcing users to change passwords every 90 days.*
- It **should not contain any word spelled completely**.
- It's wise to **discourage or prohibit the passwords which are easy to guess** (like 'password'), a **string of numbers or letters** (like '123456'), **characters appearing adjacent to each other** in the keyboard (like '@#$%^&*'), **default or suggested passwords from any place**, even if they seem strong.

Hope this information will help in the growth of the organisation. Thanking you.

NAME - ARITRA MAZUMDAR

MASTERS IN COMPUTER APPLICATIONS (MCA)