Respected sir/maam

I am able to crack all the passwords by using hashcat and command prompt

All the password which are compromised were using MD5 which is a weaker hash algorithm and is prone to collisions. It was very easy to crack with Hashcat.com

The hashing algorithm that is used to protect the passwords is MD5 it uses hashes in order to encrypt the password . this MD5 hashing algorithm uses a complex mathematical formula to create a hash. It converts data into blocks of specific sizes and manipulates the data a number of times. While this is happening, the algorithm adds a unique value into the calculation and converts the result into a small signature or hash.

MD5 is insecure and provides a very low level of protection and should not be used in any application.

Controls to be implemented to make cracking harder:

i) A min-length password rule should be implemented.

ii)Passwords must contain some special characters,numbers,lowercase alphabets as well as upper case alphabets.

ii)Using a hashing algorithm which provides a high level of protection. Example:SHA-256 and SHA-3.

iv)Concept of password salting must be used.

There is no rule regarding the minimum length of the password. ii)There is no rule regarding use of special characters in the password.

The password must be of minimum 8 characters.

i) Minimum 2 special characters (/,#,\*,... etc) must be used in the password.

ii)An external Api based tool which checks for password strength should show that the used password is strong.

Thanking you

Mohammad hussain