To: Joanna Rycerz

1st March, 2022

Dear Sir/Ma’am,

After trying to crack all the leaked hashes. I found several vulnerabilities in your password policy and this Email concludes all the findings and suggestions to improve your password policy.

Secure Hash Algorithm (SHA), Message Digest (MD4) and Message Digest (MD5) are the standard cryptographic hash functions to provide data security for authentication.

All the passwords which are compromised were using MD5 which is weaker and prone to brute-force attacks.

• Reduce redundancy across services such that in case of a leak out of one service doesn’t make the other passwords vulnerable.

• Use alphanumeric character with special characters.

• Reducing occurrence of an adjective on noun which is an obvious prey to brute force attacks.

It was very easy to crack with rockyou.txt or crack station wordlists. I would suggest that you use a very strong password encryption mechanism to create hashes for the password based on SHA.

After cracking the password we find following things about organization’s password policy:

* Minimum length for password is set to 6.
* The lack of capital characters splits the password strength by half.
* Not avoiding the occurrence of English verbs like book, popular, eating, hero, life, John Wick, interest, expert in turn making the password vulnerable to brute force attacks.
* There is no specific policy or standard for the password creation. Users can use and combination of word and letters to create a password.

You can include several new things in your password policy. My recommendations are:

* Maintain an 8-character minimum length requirement
* Don't require special character. For example, \*&(^%$
* Don't require mandatory periodic password resets for user accounts
* Ban common passwords, to keep the most vulnerable passwords out of your system
* Educate your users to not reuse their organization passwords for non-work related purposes
* Enforce registration for multi-factor authentication
* Enable risk-based multi-factor authentication challenges

Thanks & Regards

Vaibhav