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) and Message Digest (MD5) are the standard

cryptographic hash functions to provide data security for authentication.

All the password which are compromised were using MD5 which is weaker

hash algorithm and is prone to collisions.

It was very easy to crack with Hashcat.com and rockyou.txt wordlist via terminal and web browsers. I would suggest that you use a very strong password encryption mechanism to create hashes for the password based on SHA.

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

 Minimum length for password is set to 6.

 There is no specific requirement for the password creation. Users can use

any combination of word and letters to create a password.

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

recommendations are:

 Avoid common words and character combinations in your password.

 Longer passwords are better; 8 characters is a starting point.

 Don’t reuse your passwords.

 Include special character, Capital and Small letters, numbers in your

password.

 Don’t let users include their username, actual name, date of birth and

other personal information while creating a password.

 Train your users to follow these policies to keep their passwords safe.

**OBSERVATIONS:**

1. What type of hashing algorithm was used to protect passwords?

It was a MD5. The MD5 (message-digest algorithm) hashing algorithm is a one-way cryptographic function that accepts a message of any length as input and returns as output a fixed-length digest value to be used for authenticating the original message.

2. What level of protection does the mechanism offer for passwords?

Using salted md5 for passwords is a bad idea. Not because of MD5's cryptographic weaknesses, but because it's fast. This means that an attacker can try billions of candidate passwords per second on a single GPU. It concludes that the MD5 provides very low security for password.

3. What controls could be implemented to make cracking much harder for the hacker in the event of a password database leaking again?

* Make every password unique.
* Make it long. This is the most critical factor. Choose nothing shorter than 15 characters, more if possible.
* Use a mix of characters. The more you mix up letters (upper-case and lower-case), numbers, and symbols, the more potent your password is, and the harder it is for a brute force attack to crack it.
* Avoid common substitutions. Password crackers are hip to the usual substitutions. Whether you use DOORBELL or D00R8377, the brute force attacker will crack it with equal ease.
* Don’t use memorable keyboard paths. Much like the advice above not to use sequential letters and numbers, do not use sequential keyboard paths either (like qwerty). These are among the first to be guessed.
* Use two-factor authentication. Even hackers that have stolen your passwords aren’t going to easily access your accounts if you follow this tip. Two-factor authentication requires you to know something (your

password), and to have something (a phone with a code, for instance).

4. What can you tell about the organization’s password policy (e.g., password length, key space, etc.)?

* Minimum length of the password should be 6 characters or more than that.
* There is no rule regarding use of special characters in the password.

5. What would you change in the password policy to make breaking the passwords harder?

* The password must be of minimum 8 characters.
* Minimum 2 special characters (/,#,\*, etc.) must be used in the password.
* An external API based tool which checks for password strength should show that the used password is strong.

**Security Algorithms used:**

experthead:e10adc3949ba59abbe56e057f20f883e – MD5 interestec:25f9e794323b453885f5181f1b624d0b – MD5 ortspoon:d8578edf8458ce06fbc5bb76a58c5ca4 –MD5 reallychel:5f4dcc3b5aa765d61d8327deb882cf99 –MD5 simmson56:96e79218965eb72c92a549dd5a330112 – MD5 bookma:25d55ad283aa400af464c76d713c07ad – MD5 popularkiya7:e99a18c428cb38d5f260853678922e03 – MD5 eatingcake1994:fcea920f7412b5da7be0cf42b8c93759 – MD5 heroanhart:7c6a180b36896a0a8c02787eeafb0e4c – MD5 edi\_tesla89:6c569aabbf7775ef8fc570e228c16b98 – MD5 liveltekah:3f230640b78d7e71ac5514e57935eb69 – MD5 blikimore:917eb5e9d6d6bca820922a0c6f7cc28b – MD5 johnwick007:f6a0cb102c62879d397b12b62c092c06 – MD5 flamesbria2001:9b3b269ad0a208090309f091b3aba9db – MD5 oranolio:16ced47d3fc931483e24933665cded6d - MD5 spuffyffet:1f5c5683982d7c3814d4d9e6d749b21e - MD5 moodie:8d763385e0476ae208f21bc63956f748 - MD5 nabox:defebde7b6ab6f24d5824682a16c3ae4 - MD5 bandalls:bdda5f03128bcbdfa78d8934529048cf - MD5

**Cracked Passwords:**

experthead:e10adc3949ba59abbe56e057f20f883e - 123456 interestec:25f9e794323b453885f5181f1b624d0b - 123456789 ortspoon:d8578edf8458ce06fbc5bb76a58c5ca4 - qwerty reallychel:5f4dcc3b5aa765d61d8327deb882cf99 - password simmson56:96e79218965eb72c92a549dd5a330112 - 111111 bookma:25d55ad283aa400af464c76d713c07ad - 12345678 popularkiya7:e99a18c428cb38d5f260853678922e03 - abc123 eatingcake1994:fcea920f7412b5da7be0cf42b8c93759 - 1234567 heroanhart:7c6a180b36896a0a8c02787eeafb0e4c - password1 edi\_tesla89:6c569aabbf7775ef8fc570e228c16b98 - password! liveltekah:3f230640b78d7e71ac5514e57935eb69 - qazxsw blikimore:917eb5e9d6d6bca820922a0c6f7cc28b - Pa$$word1 johnwick007:f6a0cb102c62879d397b12b62c092c06 - bluered