Dear Sir/Ma’am,

I tried to crack all the leaked hashes, I found several vulnerabilities in your password policy and this email concludes all the findings and pieces of suggestion 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.

It was very easy to crack with hashcat.com and crackstation wordlist. I would always suggest you to 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 the organization’s password policy:

* Minimum length for a password is set to 6.
* There is no specific requirement for password creation. Users can use any combinations of characters, numbers, as well as upper- and lower-case letters.

I would like to change several new things in the password policy and I can say I would recommend these for your organization:

* Set Minimum Password Length like 8 characters is a starting point, a minimum character length of 14 characters becomes a better standard.
* Utilize Passphrases, these can be used with a 15-character minimum length that is easier to remember and type, but harder to gain access to.
* Make sure they do not reference the legal name, username, date of birth, or any other personal information while creating a password.
* Robust passwords also utilize combinations of special characters, numbers, as well as upper- and lower-case letters.
* Don’t reuse your passwords.
* Set Minimum and Maximum Password Age Limits, setting a maximum password age limit also helps with network security.
* Usually, this is set anywhere from 90 days for passwords to 180 days for passphrases.
* Instruct your users to follow these policies regularly to keep their passwords safe and secure.

Thank You Regards

Name: Aadarsh Singh

B.Tech, Computer Science & Engineering

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:

|  |  |  |
| --- | --- | --- |
| **Hash** | **Type** | **Result** |
| 25f9e794323b453885f5181f1b624d0b | md5 | 123456789 |
| e10adc3949ba59abbe56e057f20f883e | md5 | 123456 |
| d8578edf8458ce06fbc5bb76a58c5ca4 | md5 | qwerty |
| 5f4dcc3b5aa765d61d8327deb882cf99 | md5 | password |
| 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 |