Dear Sir/Madam,

After trying to crack all the passwords in the leaked hashes file, I was able to crack 14 of the 19 hashes. This email includes all the finding and suggestions to improve password policy.

Cracked passwords:

1. e10adc3949ba59abbe56e057f20f883e: 123456
2. 25f9e794323b453885f5181f1b624d0b: 123456789
3. 5f4dcc3b5aa765d61d8327deb882cf99: password
4. fcea920f7412b5da7be0cf42b8c93759: 1234567
5. 25d55ad283aa400af464c76d713c07ad: 12345678
6. e99a18c428cb38d5f260853678922e03: abc123
7. d8578edf8458ce06fbc5bb76a58c5ca4: qwerty
8. 96e79218965eb72c92a549dd5a330112: 111111
9. 7c6a180b36896a0a8c02787eeafb0e4c: password1
10. 6c569aabbf7775ef8fc570e228c16b98: password!
11. 3f230640b78d7e71ac5514e57935eb69: qazxsw
12. f6a0cb102c62879d397b12b62c092c06: bluered
13. 917eb5e9d6d6bca820922a0c6f7cc28b: Pa$$word1
14. 8d763385e0476ae208f21bc63956f748: moodie00

The algorithm used to hash the leaked passwords of the organization was MD5. Which was easy to crack as the hashes are only 128 bits long.

The protection offered by MD5 is much lower as compared to SHA. Hashing algorithms used nowadays are SHA512, SHA3, etc. which are way more secure than MD5.

Proposed controls:

1. Use a better hashing Algorithm
2. Implement salting to prevent use of rainbow tables
3. Increase minimum password length. All passwords in this file were less than 10 characters.
4. Prevent password and username to be same. Eg: moodie
5. Spread Awareness and educate users of the company on good password practices.

The organization didn’t have a strong password policy in place:

1. The minimum password length was set to 6.
2. Numbers, letters and symbols could be used together but no compulsion was made.

No other specific requirement was made.

Proposed changes to the password policy:

1. Make a lengthier password. (at least 10 characters)
2. Use of special characters, uppercase letters, lowercase and numbers in combination should be made mandatory.
3. Avoid use of common dictionary words
4. Avoid using username, date of birth and other personal information in password.
5. Train users to adhere to these practices.

Thanking You,

Name: Maitraiyi Dandekar

B.E. Computer Engineering