Sir/Madam,

The leaked hashes use MD5 hashing algorithm, which according to my observation is providing very little protection in case of database leaking.

The hashing algorithms like MD5 and SHA-family of algorithms are the standard one's but not that strong.

After trying to crack the passwords I came across certain drawbacks of company's policy.

1. The passwords were using very common combinations and there was no specific rules on their creation.

2. The length was short which in case of cracking could be an advantage for the hackers.

3. Salting was not implemented as it creates a strong hash value.

4. Strong hashing algorithms were not used.

The changes I would suggest in the password policy are:

1. Creating combination of letters, numbers and symbols is the best approach to begin with.

2. Don't let users use common words, their username, personal information or combination of that as a password.

3. The length should be increased.

4. Hashing algorithms like bcrypt, scrypt or PBKDF2 can be used. It is ought to increase the time in cracking.

OBSERVATIONS:

Security Algorithm used : MD5

experthead:e10adc3949ba59abbe56e057f20f883e

interestec:25f9e794323b453885f5181f1b624d0b

ortspoon:d8578edf8458ce06fbc5bb76a58c5ca4

reallychel:5f4dcc3b5aa765d61d8327deb882cf99

simmson56:96e79218965eb72c92a549dd5a330112

bookma:25d55ad283aa400af464c76d713c07ad

popularkiya7:e99a18c428cb38d5f260853678922e03

eatingcake1994:fcea920f7412b5da7be0cf42b8c93759

heroanhart:7c6a180b36896a0a8c02787eeafb0e4c

edi_tesla89:6c569aabbf7775ef8fc570e228c16b98

liveltekah:3f230640b78d7e71ac5514e57935eb69

blikimore:917eb5e9d6d6bca820922a0c6f7cc28b

johnwick007:f6a0cb102c62879d397b12b62c092c06

flamesbria2001:9b3b269ad0a208090309f091b3aba9db

oranolio:16ced47d3fc931483e24933665cded6d

spuffyffet:1f5c5683982d7c3814d4d9e6d749b21e

moodie:8d763385e0476ae208f21bc63956f748

nabox:defebde7b6ab6f24d5824682a16c3ae4

bandalls:bdda5f03128bcbdfa78d8934529048cf

Cracked Passwords:

e10adc3949ba59abbe56e057f20f883e:123456

e99a18c428cb38d5f260853678922e03:abc123

d8578edf8458ce06fbc5bb76a58c5ca4:qwerty

96e79218965eb72c92a549dd5a330112:111111

3f230640b78d7e71ac5514e57935eb69:qazxsw

fcea920f7412b5da7be0cf42b8c93759:1234567

f6a0cb102c62879d397b12b62c092c06:bluered

25d55ad283aa400af464c76d713c07ad:12345678

5f4dcc3b5aa765d61d8327deb882cf99:password

8d763385e0476ae208f21bc63956f748:moodie00

Thank you

Ayushi Dangwal

B.Tech Computer Science and Engineering