Cracked Passwords from the given passwd\_dump.txt file:

1. experthead:e10adc3949ba59abbe56e057f20f883e - 123456
2. interestec:25f9e794323b453885f5181f1b624d0b - 123456789
3. ortspoon:d8578edf8458ce06fbc5bb76a58c5ca4 - qwerty
4. reallychel:5f4dcc3b5aa765d61d8327deb882cf99 - password
5. simmson56:96e79218965eb72c92a549dd5a330112 - 111111
6. bookma:25d55ad283aa400af464c76d713c07ad - 12345678
7. popularkiya7:e99a18c428cb38d5f260853678922e03 - abc123
8. eatingcake1994:fcea920f7412b5da7be0cf42b8c93759 - 1234567
9. heroanhart:7c6a180b36896a0a8c02787eeafb0e4c - password1
10. edi\_tesla89:6c569aabbf7775ef8fc570e228c16b98 - password!
11. liveltekah:3f230640b78d7e71ac5514e57935eb69 - qazxsw
12. blikimore:917eb5e9d6d6bca820922a0c6f7cc28b - Pa$$word1
13. johnwick007:f6a0cb102c62879d397b12b62c092c06 - bluered
14. flamesbria2001:9b3b269ad0a208090309f091b3aba9db - Flamesbria2001
15. oranolio:16ced47d3fc931483e24933665cded6d - Oranolio1994
16. spuffyffet:1f5c5683982d7c3814d4d9e6d749b21e - Spuffyffet12
17. moodie:8d763385e0476ae208f21bc63956f748 - moodie00
18. nabox:defebde7b6ab6f24d5824682a16c3ae4 - nAbox!1
19. bandalls:bdda5f03128bcbdfa78d8934529048cf - Bandalls
20. Hashing algorithm used: MD5.
21. Level of protections offered to the passwords:

After going through the provided password dump file and decrypting them, it has been found that all those hash values are the result of using MD5 algorithm to decrypt the password and following is what I found on my own research about MD5.

MD5 creates 512-bit blocks that contains 16 words of 32-bit each resulting in 128-bit message. Protection is provided in different stages.

1. Message digest value is initialized using hexadecimal numerical values.
2. In every individual stage, four message digest is passed through those changes the current data block along with the values passed from the previous block.
3. The value obtained from the final block is then MD5 digest for current block.
4. No two-password ca have same hash value.

So, this must be practically not decryptable. But this is not always the case like in Flame malware in 2012. If anyone got the hash value from any password database leakage, then it can be decrypted in few seconds or a minute.

1. To make cracking much harder for the hacker in the event of a password database leaking again we can do:
2. We can use hashing with salt to slow down the password cracking from the obtained rainbow table. No methods to prevent password cracking is safe but this is a lot of work.
3. We are using MD5 algorithm. We can do better. We can use algorithms like bcrypt – specify complexity that affects the speed at which hashing and guessing occurs, scrypt – prevents parallel cracking.
4. Above two takes lot of resources to authenticate one user and for that we can use Server-relief that uses browser or user’s system for the required resources.
5. Required length of the password can be set to least 16 that increases the cracking time.
6. No username and password similarity and not even similarity with the brand.
7. Advising users not to use dictionary word instead use letters characters, numbers all jumbled.
8. Promote use of password generator tool that generates and saves the password.
9. Upon inspecting and cracking password from the given dump file this is what I have:
10. The least password length is 6 and maximum is 14.
11. All the passwords are mostly letter and numbers and only 3 got characters.
12. Only passwords are hashed using MD5 algorithm.
13. No password is hashed + salted.
14. Company accepts any type of password like all number, all letter, all character that are easily crack able.
15. There are some preventive measures that the organization can use to make password cracking harder.
16. Using more secure hashing algorithm like SHA, bcrypt, scrypt instead of MD5.
17. Length of password be at least 16.
18. No dictionary password acceptable.
19. Password should contain capital letter, number, symbols, and non-dictionary.
20. All the password encryption to be done using salt and hash.
21. Even suggest passwords with own password generator tool.

Dear Ma’am/Sir,

After obtaining the leaked hashes I tried to crack the password, which was not even hard, I have found some vulnerabilities in the password policy of the organization. The purpose of this email is to present you my findings on the organization’s current password policy and my recommendation to prevent cracking of the password and increase the time involved in cracking it.

All the passwords cracked shows that the organization is using the MD5 algorithm for the security of user data authentication. This is an outdated and easily compromise able hashing algorithm.

There are even online tools that can crack the obtained hashed file like <https://crackstation.net/> and <https://www.dcode.fr/md5-hash> . We can enter the hash from the obtained passwd\_dump.txt file into the provided text field and upon selecting decrypt button, respective passwords are generated in fraction of second.

From the cracked password,

* minimum length of the password is found to be 6
* no password requirements, hence, any kind of password is accepted.
* All passwords are hashed with MD5 algorithm.
* No password is salted along with hash.

From above findings, here are some of my recommendations to strengthen the authentication and prevent the password cracking for the better password policy:

* Not accepting dictionary password, no username, date of birth, organization name in the password
* Length of the password to be at least 16 that contains minimum 1 capital letter, small letter, number, and symbols.
* Providing strong password generator for the users with the option to set their own password
* Suggesting user to use password generator/manager tools.
* Using better algorithm for encrypting password like bcrypt, scrypt, SHA (Secured Hashed Algorithm).
* Using Salt along with the hash.

These are my findings and recommendations. Hope this helps the organization to strengthen the authentication of user and prevent password cracking in the future.

Thank you,

Regards,

Bishal Budhathoki,

Master of Information Technology

References:

<https://crackstation.net/>

<https://en.wikipedia.org/wiki/Hash_function_security_summary>

<https://searchsecurity.techtarget.com/definition/digital-signature>

<https://searchsecurity.techtarget.com/definition/MD5>

<https://www.dcode.fr/md5-hash>

<https://onlinetoolweb.com/md5-salt-decrypt-online-tool/>

<https://www.wordfence.com/learn/how-passwords-work-and-cracking-passwords/>