Subject: Crack leaked password database

Dear Sir/Ma'am,

While cracking and reviewing the leaked hashes, I have found multiple loopholes and vulnerabilities in the shared password list. Please find the below suggestions and ideas to further improve the password selection process and make breaking the passwords more difficult.

All the compromised passwords are using the **MD5** cryptographic hash function which has many weaknesses, the main issue being MD5 is vulnerable to collision attacks in which the hashing algorithm takes two different inputs and produces the same hash. This property means the MD5 hash function is considered "broken" and very high-risk. This provides very poor level of protection as multiple tools such as Hashcat and free-to-use web apps can be used to crack the hashes.

I used **Hashcat** along with **CrackStation's** Human only dictionary and **MD5 Online** to crack these.

To make breaking the passwords harder, a lower-risk hash function should be implemented such as **SHA512crypt** which is resistant to collision attacks and mostly resistant to length extension attacks, or **Bcrypt** which is the standard password hash algorithm used in most systems. SHA512crypt passes the password through 5,000 hashing iterations to make decrypting harder and near impossible. Bcrypt includes a salt and is designed to withstand brute-force attacks by intentionally being slower to operate. The unsalted passwords listed below could be cracked using online websites such as CrackStation, which is very insecure.

Judging from the cracked passwords listed below, the password policy allows employees to use any combination of numbers and characters. The space character is not a valid input, and the minimum password length may be six and the maximum fourteen, although the size of the sample passwords is too small for this conclusion to be definitive. The organisation's **average password length is almost eight characters** but has multiple passwords shorter than eight and easy to guess which pose a high security risk. Their key space is smaller than modern standards.

The password policy should be changed so that passwords include the following:

- Use of number, letter, special character, capital letter
- Keeping a **threshold on length**. Set minimum length of 8.
- Employees should also avoid easy to guess passwords such as pet names and birthdates as well as avoid repeating their passwords for multiple accounts.
- **Reduce redundancy** across services such that in case of a leak out of one service doesn't make the **other passwords vulnerable**.
- **Not allowing sibling credentials to assist** the password naming, like name / user name / email / date of birth / sex.
- **Avoiding the occurrence of English verbs** like book, popular, eating, hero, life, John Wick, crack me, expert that makes the password vulnerable to brute force attacks.

Fond regards,

Pratyush Kumar

Attached Link: [PratyushKumar-0903/Goldman-Sachs-Engineering-Virtual-Program (github.com)]

User Name	Hash Type	Hash Type	Password
bandalls	bdda5f03128bcbdfa78d8934529048cf	MD5	Banda11s
blikimore	917eb5e9d6d6bca820922a0c6f7cc28b	MD5	Pa$$word1
bookma	25d55ad283aa400af464c76d713c07ad	MD5	12345678
eatingcake1994	fcea920f7412b5da7be0cf42b8c93759	MD5	1234567
edi_tesla89	6c569aabbf7775ef8fc570e228c16b98	MD5	password!
experthead	e10adc3949ba59abbe56e057f20f883e	MD5	123456
flamesbria2001	9b3b269ad0a208090309f091b3aba9db	MD5	Flamesbria2001
heroanhart	7c6a180b36896a0a8c02787eeafb0e4c	MD5	password1
interestec	25f9e794323b453885f5181f1b624d0b	MD5	123456789
johnwick007	f6a0cb102c62879d397b12b62c092c06	MD5	bluered
liveltekah	3f230640b78d7e71ac5514e57935eb69	MD5	qazxsw
moodie	8d763385e0476ae208f21bc63956f748	MD5	moodie00
ortspoon	d8578edf8458ce06fbc5bb76a58c5ca4	MD5	qwerty
popularkiya7	e99a18c428cb38d5f260853678922e03	MD5	abc123
reallychel	5f4dcc3b5aa765d61d8327deb882cf99	MD5	password
simmson56	96e79218965eb72c92a549dd5a330112	MD5	111111
spuffyffet	1f5c5683982d7c3814d4d9e6d749b21e	MD5	Spuffyffet12
nabox	defebde7b6ab6f24d5824682a16c3ae4	MD5	nAbox!1
oranolio	16ced47d3fc931483e24933665cded6d	MD5	Oranolio1994