**MEMORANDUM**

To: Head of The Security Systems

From: Ian, Password Analyst

Date: September 12th, 2023

Subject: Password Analysis and Policy Recommendations

Background:

Tasked with analyzing the level of protection of implemented controls for passwords of a given database, the following areas were considered: what hashing algorithm was used to encrypt the passwords, an analysis of the level of protection and the organizations current password policy as well as recommendations for an updated password policy.

Methodology:

Given a list of leaked passwords it was noted that the passwords of the organization were encrypted using the MD5 hashing algorithm. This was derived by analyzing how many bits the encryption had which were 32 for each password of the given list.

1. experthead:e10adc3949ba59abbe56e057f20f883e -  **MD5**
2. interestec:25f9e794323b453885f5181f1b624d0b -  **MD5**
3. ortspoon:d8578edf8458ce06fbc5bb76a58c5ca4 -  **MD5**
4. reallychel:5f4dcc3b5aa765d61d8327deb882cf99 -  **MD5**
5. simmson56:96e79218965eb72c92a549dd5a330112 -  **MD5**
6. bookma:25d55ad283aa400af464c76d713c07ad –  **MD5**
7. popularkiya7:e99a18c428cb38d5f260853678922e03 –  **MD5**
8. eatingcake1994:fcea920f7412b5da7be0cf42b8c93759 -  **MD5**
9. heroanhart:7c6a180b36896a0a8c02787eeafb0e4c –  **MD5**
10. edi\_tesla89:6c569aabbf7775ef8fc570e228c16b98 - **MD5**
11. liveltekah:3f230640b78d7e71ac5514e57935eb69 -  **MD5**
12. moodie:8d763385e0476ae208f21bc63956f748 - **MD5**

In order to gain a better understanding of the password policy used by the organization the Tool Hashcat - a software used to crack passwords, was employed. The following list encompasses the passwords Hashcat was able to crack.

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. moodie:8d763385e0476ae208f21bc63956f748 -**moodie00**

Findings:

After the hashing algorithm was determined and the leaked passwords were cracked it was found that the organizations level of protection is poor. The use of the MD5 hashing algorithm is very outdated as it exposes the passwords to an array of vulnerabilities. In this case, MD5 is a relatively fast algorithm to compute, making it fairly simple to crack passwords through Brute Force and Wordlists dictionaries. Additionally, the MD5 algorithm does not support salting, which is discussed more in the recommendations section.

Secondly, it was found that organizations passwords policy is misinformed and can be easily decoded with a medium to large wordlist. For example, the user “experthead” uses the password 123456 which is a password that follows a chronological order of numbers making it easy to guess or crack.

The tool “How Secure Is My Password?” which informs how long a password would take to be cracked by a computer was used to analyze some passwords:

1. 123456 - “instantly”; this is seen as the tool hashcat cracked the password in 3 seconds
2. password! - “2 hours”
3. qazxsw - “instantly”

 Upon further look at the passwords, it can be determined that the policy allows for users to put in a set of both integers, letters and special characters as passwords of at least five characters. This policy can be improved.

Recommendations:

In order to uplift the organizations password policy to make stronger passwords against hacking, they should consider the following recommendations:

1. Employ the SHA2 or SHA3 hashing algorithm that uses more bits to encrypt the password thus making is tedious and longer to crack passwords. Additionally, the SHA2 or SHA3 algorithm employs salting which uses a random bit to per user multiplies with the hashing function to provide an encrypted password. This makes cracking the password more tedious as the hacker needs to figure out what the salt function is for the password.
2. To uplift the organizations password policy, it is strongly recommended that the organization begins to require users to put in passwords that are longer than five characters, require both integers, letters and special characters in a non chronological order. The passwords also need to be of items that are not related. For example, users name and birthday should be refused as a password as it is easy to guess but users pet name, dads birthday and specials characters such as “!,\*,&” all as one password should be accepted.
3. Lastly, if a users password is cracked, the organization can protect the user by requiring two-factor authentication to access the account.

Conclusion:

The organizations password policy is scored very poorly with the reliance on the MD5 algorithm and a lenient password policy. Immediate implementation of the SHA2 OR SHA3 algorithm is high advised as well as an updated password policy.