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.

We can use the following hashing algorithms to protect the passwords:

- Secure Hashing Algorithm (SHA)
- Message Digest (MD5)

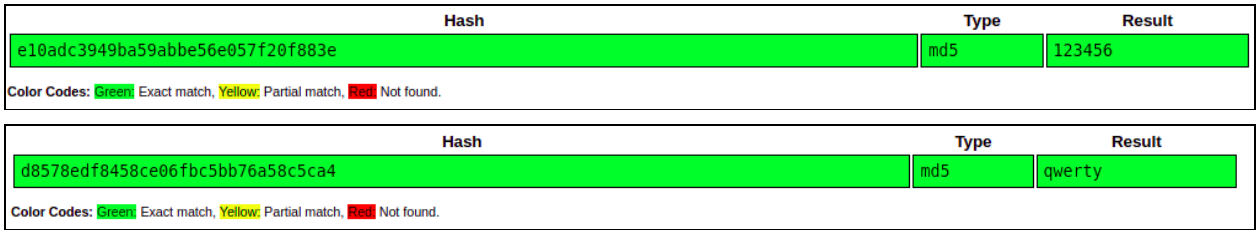
Both the algorithms are standard cryptographic functions and used to provide data security for the authentication purposes.

The shared password list is using MD5 which is weaker and more prone to crack passwords easily using crackstation or hashcat. However, SHA is the modified version of MD5 and is more secure. My suggestion is to use the SHA algorithm to create hashes for the passwords.

I have found the following details about the organizations password policy:

- Minimum length is set to 6.
- Combination of words and letters.

Attached screenshot for your reference:



Hash	Type	Result
e10adc3949ba59abbe56e057f20f883e	md5	123456

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Hash	Type	Result
d8578edf8458ce06fbc5bb76a58c5ca4	md5	qwerty

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

We can include the below points to make the passwords more secure:

- Smaller passwords are easy to crack, we can set the length to at least 8 characters.
- Try to avoid the most commonly used passwords (e.g 123456).
- Must include special characters in the passwords.
- Use the combination of letters, characters and special characters.
- Avoid your name, date of birth, email-id in your passwords.
- Avoid common words and character combinations.
- Longer passwords are less likely to crack.

I hope the above suggestions are helpful and beneficial to your organization’s password policy.

Thank you
Regards,
Alka Bharti