# Crack leaked password database

Observations

I was able to crack 13 passwords from the given 19 hashcodes in the password dump file very easily.

e10adc3949ba59abbe56e057f20f883e md5 123456

25f9e794323b453885f5181f1b624d0b md5 123456789

d8578edf8458ce06fbc5bb76a58c5ca4 md5 qwerty

5f4dcc3b5aa765d61d8327deb882cf99 md5 password

96e79218965eb72c92a549dd5a330112 md5 111111

25d55ad283aa400af464c76d713c07ad md5 12345678

e99a18c428cb38d5f260853678922e03 md5 abc123

fcea920f7412b5da7be0cf42b8c93759 md5 1234567

7c6a180b36896a0a8c02787eeafb0e4c md5 password1

6c569aabbf7775ef8fc570e228c16b98 md5 password!

3f230640b78d7e71ac5514e57935eb69 md5 qazxsw

917eb5e9d6d6bca820922a0c6f7cc28b md5 Pa$$word1

f6a0cb102c62879d397b12b62c092c06 md5 bluered

What type of hashing algorithm was used to protect passwords?

Hashing algorithm are as exuberant as encryption algorithms. However, there are a few that are applied more frequently. They are MD5, SHA-1, SHA-2, NTLM, and LANMAN.

MD5: The 5th version of the Message Digest Algorithm. MD5 creates 128-bit outputs. MD5 was a very commonly used hashing algorithm.

SHA-1: The 2nd version of the Secure Hash Algorithm standard, SHA-0 being the 1st . SHA-1 is one of the main algorithms that began to replace MD5, it creates 160-bit outputs.

SHA-2: A hashing algorithms suite. It contains SHA-224, SHA-256, SHA-384, and SHA-512. Each algorithm is represented by the length of its output. SHA-2 algorithms are more secure than SHA-1 algorithms, but SHA-2 is not universally used.

LANMAN: Microsoft LANMAN is the Microsoft LAN Manager hashing algorithm. LANMAN was used by legacy windows systems to save passwords. It utilizes DES algorithms to create the hash.

NTLM: This is the NT LAN Manager algorithm. The NTLM algorithm is used for password hashing during authentication. It is the successor of the LANMAN algorithm.

What level of protection does the mechanism offer for passwords?

Hash function is a math algorithm that maps data of any size to a bit string of a defined size. With hash algorithm, it is easy to calculate the hash but nearly impossible to re-generate the original input if only the hash value is known. It is also hard to create an initial input that would match a particular desired output.

Therefore, in contrast to encryption, hashing is a one-way mechanism. The hashed data cannot be practically unhashed.

What controls could be implemented to make cracking much harder for the hacker in the event of a password database leaking again?

A min-length password rule is implemented for handling these cases.

Some special characters, numbers, lowercase and upper case alphabets should be included in the passwords.

SHA-256 and SHA-3, which provides a high level protection, can be utilized.

Password Salting concept should be applied.

What can you tell about the organization’s password policy (e.g. password length, key space, etc.)?

There is no standard rules regarding the minimum length or special characters in the password

What would you change in the password policy to make breaking the passwords harder?

A minimum length of 8 characters must be in the password.

At least 2 special characters should be used in the password, such as /, #, @, %...

To make the password strong, an external Api based tool which checks for password strength should be applied.

References:

[Hashing Algorithm - an overview | ScienceDirect Topics](https://www.sciencedirect.com/topics/computer-science/hashing-algorithm)

[How to Hash Passwords: One-Way Road to Enhanced Security (auth0.com)](https://auth0.com/blog/hashing-passwords-one-way-road-to-security/)

[ketanraj15/Goldman-Sachs-Crack-leaked-password-database: Password Controls and Security Policies (github.com)](https://github.com/ketanraj15/Goldman-Sachs-Crack-leaked-password-database)