**Virtual Engineering Program Report - Goldman Sachs**

With the help of Crackstation platform ( URL: <https://crackstation.net/> ) I was able to crack the password of 13 hashcodes from the password dump file. Following is the list for the same with the password and hash type used.

| 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 |

After trying to crack all the passwords, I found a handful of vulnerabilities in your password policy and would like to put down my findings and suggestions so that you could update your password policy to avoid any password leak. I would suggest that you use very strong password mechanism to create hashes for the password based on Secure Hash Algorithm.

1. What type of hashing algorithm was used to protect passwords?
   * MD5 - Message Digest Algorithm
2. What level of protection does the mechanism offer for passwords?
   * MD5 is an iterative hash function. It is generally a considerable mechanism for storing passwords in production.
   * MD5 produces a 128-bit hash. MD5 is born out of RSA’s algorithm .
   * MD5 is a utility that can generate a digital signature of a file (SHA). It belongs to a family of one-way hash functions called message digest algorithms.
   * The algorithm takes as input a message of arbitrary length and produces as output a 128-bit "fingerprint" of the input called Secure Hash Algorithm. It is conjectured that it is computationally infeasible to produce two messages having the same message digest, or to produce any message having a given prespecified target message digest.
   * The MD5 algorithm is intended for digital signature applications, where a large file must be "compressed" in a secure manner before being encrypted with a private (secret) key under a public-key cryptosystem such as RSA.
3. What controls could be implemented to make cracking much harder for the hacker in the event of a password database leaking again?
   * A constant minimum-length password rule should be implemented.
   * Passwords must contain some special characters, numbers, lowercase alphabets as well as upper case alphabets.
   * Using a hashing algorithm which provides a high level of protection. Example: SHA-256 and SHA-3.
   * Concept of password salting must be used, since salting help us mitigate hash table attacks by forcing attackers to re-compute them using the salts for each user.
4. What can you tell about the organization’s password policy (e.g. password length, key space, etc.)?

Organization needs to work on it’s Password policy since:

* + A strong password must be at least 8 characters long.
  + It should not contain any of your personal information specifically your real name, user name, or even your company name.
  + It must be very unique from your previously used passwords.
  + It should not contain any word spelled completely.
  + It should contain characters from the four primary categories - uppercase letters, lowercase letters, numbers, and characters.

1. What would you change in the password policy to make breaking the passwords harder?
   * Your password should be easy for you to remember but difficult for others to guess.
   * Your password should be different than the passwords you use to log into other accounts, like your email or bank account.
   * Longer passwords are usually more secure.
   * Your password should not be your email, phone number or birthday.

Thank you,

Avani Vaish

[500082636@stu.upes.ac.in](mailto:500082636@stu.upes.ac.in)