**GOLDMAN SACHS VIRTUAL EXPERIENCE PROGRAM**

**TASK REPORT**

CRACK LEAKED PASSWORD DATABASE

Dear Sir/ Madam,

After referring to the document of hashes to be deciphered and reading the instructions, I managed to crack the hashes by using the suggested software i.e.

Hashcat and a few other tools available on the internet. After deciphering most of them, I realized that the organization to which this database belongs is highly vulnerable to password phishing attacks. Henceforth, I have come up with a few suggestions and conclusions in this report.

All the given hashes were encrypted using the **MD5** cryptographic hash functions. This function is highly susceptible to attacks and has weak encryption. It is also prone to collisions. As it is cryptologically weak, a leaked database of hashes can lead to hackers cracking almost all the passwords. As a result, my **first suggestion** would be to use **stronger encryption hash functions like SHA1 or Argon2, or salted MD5.**

On my first attempt on **Hashcat**, I was able to crack more than 70 percent of the passwords using the highly popular ‘**rockyou.txt’** wordlist and the **best64** rule.

Also, according to the link provided in the resources to check the strength of passwords, I found that almost all the cracked passwords barring two or three could be cracked instantly. This highlights the vulnerability and weaknesses in the organization’s password policy.

Here are the following conclusions that can be drawn about the organization’s password policy:

1. The minimum length of the password is of 6 characters.
2. There is no rule or restriction about the use of characters in the password. Users can use any combination of the 95 available characters. This opens them to attacks.
3. According to the deciphered list, many highly common and weak passwords are used.

Here are the suggestions to counter the problems:

1. Long passwords should be used. The minimum size should be at least 10 characters.
2. Two step-verification could be used, like an OTP after the password is entered. Also, while users set in their passwords, a real-time password strength checker should be present to inform users of how quickly their passwords could be revealed should a data breach occur.
3. Avoid repetitive words and passwords like usernames, names, or personal information.
4. Alerts should be issued to change passwords on a regular basis. Also, rules should be introduced on character usage patterns while creating the password. (Eg: One capital letter, one number, and one special character mandatory).
5. Use better encryption for the passwords. Secure the database and put it in a shadow file.

Attached below are the passwords I cracked as well as an estimation of the time it would take to crack them according to <https://www.security.org/how-secure-is-my-password/>

|  |  |  |
| --- | --- | --- |
| Hashed encryption | Deciphered Password | Estimated time to crack |
|  |  |  |
| experthead: e10adc3949ba59abbe56e057f20f883e | 123456 | Instantly |
| interestec: 25f9e794323b453885f5181f1b624d0b | 123456789 | Instantly |
| ortspoon:  d8578edf8458ce06fbc5bb76a58c5ca4 | qwerty | Instantly |
| reallychel:  5f4dcc3b5aa765d61d8327deb882cf99 | password | Instantly |
| simmson56:  96e79218965eb72c92a549dd5a330112 | 111111 | Instantly |
| bookma:  25d55ad283aa400af464c76d713c07ad | 12345678 | Instantly |
| popularkiya7:  e99a18c428cb38d5f260853678922e03 | abc123 | Instantly |
| eatingcake1994:  fcea920f7412b5da7be0cf42b8c93759 | 1234567 | Instantly |
| heroanhart:  7c6a180b36896a0a8c02787eeafb0e4c | password1 | Instantly |
| edi\_tesla89:  6c569aabbf7775ef8fc570e228c16b98 | password! | 2 hours |
| liveltekah:  3f230640b78d7e71ac5514e57935eb69 | qazxsw | Instantly |
| blikimore:  917eb5e9d6d6bca820922a0c6f7cc28b | Pa$$word1 | 3 weeks |
| johnwick007:  f6a0cb102c62879d397b12b62c092c06 | bluered | 2 hundred milliseconds |
| flamesbria2001:  9b3b269ad0a208090309f091b3aba9db | Flamesbria2001 | 9 million years |
| moodie:  8d763385e0476ae208f21bc63956f748 | moodie00 | 1 minute |
| bandalls:  bdda5f03128bcbdfa78d8934529048cf | Banda11s | 1 hour |
|  |  |  |

The report marks my conclusions, suggestions, and efforts in this task.

Thanking you for your perusal.

Amisha Sinha,

Motilal Nehru National Institute of Technology,

Bachelor of Technology, 3rd year,

Computer Science and Engineering.