**Kalyani Samoju**

**IIIT SKLM**

**3RD YEAR**

**TO,**

**Goldman Sachs**

**Crack Leaked Password Database**

**Dear Sir/Ma’am**

I devised this conclusion that your company's password policy had vulnerable flaws. Therefore I devised the following password after breaking all of the passwords using the provided hashes in the hashcat password recovery tool.

**Changes in your password policy can be handled using this solution.**

MD5 hashing algorithm was used to generate all of the passwords. MD5 is vulnerable and has been cryptographically cracked, making it insecure. If the password database is compromised, passwords encrypted using MD5 might be decrypted in a matter of minutes. Finally, more secure cryptographic hashing algorithms should be utilized, such as Secured Hashing Algorithm (SHA), Salted MD5, RIPEMD-320, and Whirlpool.

**The majority of the passwords were quickly cracked on the internet using a hacked password database.**

Using the hashcat password recovery tool, the remaining passwords were cracked in under one hour. Password strength was high, according to howsecurelsmypassword.net, yet it was still cracked in less than an hour. Finally, it is possible to determine that the organization should consider making some password modification policy.

1. A six-character password is the bare minimum.

2 There is no rule stating that symbols, capital letters, and numbers must all be used simultaneously.

3: Weak passwords that were already in the compromised password dictionary

**Password policy to make it more difficult to crack passwords**

1. Implement two-factor authentication or multiple-factor authentication. Fingerprint

When accessing a user's data, authentication can also be employed.

2. Set a minimum password length of 12 characters, change it at least twice a year, and use creative passwords.

(Special characters, spaces, upper/lowercase letters, and numeric characters are all allowed).

3. Passwords should not be reused, and usernames, DOBs, and names should not be used.

4 Avoid using the most common passwords and educate people on how to create stronger passwords.

Thanking you,

Kalyani Samoju

Computer science engineering

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **USERNAME** | **HASH** | **HASHING ALGORITH** | **PASSWORD** | **STRENGTH/REQUIRED TIME** | **ACTUALCONSUMED TIME** |
| experthead | e10adc3949ba59abbe56e057f20f883e | MD5 | 12345 | INSTANTLY | INSTANTLY |
| interestec | 25f9e794323b453885f5181f1b624d0b | MD5 | 123456789 | INSTANTLY | INSTANTLY |
| ortspoon | d8578edf8458ce06fbc5bb76a58c5ca4 | MD5 | qwerty | INSTANTLY | INSTANTLY |
| reallychel | 5f4dcc3b5aa765d61d8327deb882cf99 | MD5 | password | INSTANTLY | INSTANTLY |
| simmson56 | 96e79218965eb72c92a549dd5a330112 | MD5 | 111111 | INSTANTLY | INSTANTLY |
| bookma | 25d55ad283aa400af464c76d713c07ad | MD5 | 12345678 | INSTANTLY | INSTANTLY |
| popularkiya7 | e99a18c428cb38d5f260853678922e03 | MD5 | abc123 | INSTANTLY | INSTANTLY |
| eatingcake1994 | fcea920f7412b5da7be0cf42b8c93759 | MD5 | 1234567 | INSTANTLY | INSTANTLY |
| heroanhart | 7c6a180b36896a0a8c02787eeafb0e4c | MD5 | password1 | INSTANTLY | INSTANTLY |
| edi\_tesla89 | 6c569aabbf7775ef8fc570e228c16b98 | MD5 | password! | INSTANTLY | INSTANTLY |
| liveltekah | 3f230640b78d7e71ac5514e57935eb69 | MD5 | qazxw | INSTANTLY | INSTANTLY |
| blikimore | 917eb5e9d6d6bca820922a0c6f7cc28b | MD5 | Pa$$word1 | 3 WEEKS | INSTANTLY |
| johnwick007 | f6a0cb102c62879d397b12b62c092c06 | MD5 | bluered | 200 MILLISECONDS | INSTANTLY |
| flamesbria2001 | 9b3b269ad0a208090309f091b3aba9db | MD5 | Flamesbria2001 | 9 MILLON YEARS | 1 HOUR |
| oranolio | 16ced47d3fc931483e24933665cded6d | MD5 | Oranolio1994 | 2000 YEARS | 1 HOUR |
| spuffyffet | 1f5c5683982d7c3814d4d9e6d749b21e | MD5 | Spuffeyffet12 | 2000 EARS | 1 HOUR |
| moodie | 8d763385e0476ae208f21bc63956f748 | MD5 | moodie00 | 1 MINUTE | 1 HOUR |
| nabox | defebde7b6ab6f24d5824682a16c3ae4 | MD5 | nAbox!1 | 6 MINUTES | 1 HOUR |
| bandalls | bdda5f03128bcbdfa78d8934529048cf | MD5 | Banda11s | 1 HOUR | 1 HOUR |

**Cracked Passwords:**

experthead:e10adc3949ba59abbe56e057f20f883e - 123456

interestec:25f9e794323b453885f5181f1b624d0b - 123456789

ortspoon:d8578edf8458ce06fbc5bb76a58c5ca4 - qwerty

reallychel:5f4dcc3b5aa765d61d8327deb882cf99 - password

simmson56:96e79218965eb72c92a549dd5a330112 - 111111

bookma:25d55ad283aa400af464c76d713c07ad - 12345678

popularkiya7:e99a18c428cb38d5f260853678922e03 - abc123

eatingcake1994:fcea920f7412b5da7be0cf42b8c93759 - 1234567

heroanhart:7c6a180b36896a0a8c02787eeafb0e4c - password1

edi\_tesla89:6c569aabbf7775ef8fc570e228c16b98 - password!

liveltekah:3f230640b78d7e71ac5514e57935eb69 - qazxsw

blikimore:917eb5e9d6d6bca820922a0c6f7cc28b - Pa$$word1

johnwick007:f6a0cb102c62879d397b12b62c092c06 - bluered