**Goldman Sachs Crack Leaked Password Database**

**Overview:**

As a governance analyst it is part of your duties to assess the level of protection offered by implemented controls and minimize the probability of a successful breach. You often need to know the techniques used by hackers to circumvent implemented controls and propose uplifts to increase the overall level of security in an organization. Gaining valid credentials gives the attackers access to the organization’s IT system, thus circumventing most of perimeter controls in place.

**Tasks:**

* What type of hashing algorithm was used to protect passwords?
* What level of protection does the mechanism offer for passwords?
* What controls could be implemented to make cracking much harder for the hacker in the event of a password database leaking again?
* What can you tell about the organization’s password policy (e.g. password length, key space, etc.)?
* What would you change in the password policy to make breaking the passwords harder?

**Sample Data:**

**experthead:e10adc3949ba59abbe56e057f20f883e**

**interestec:25f9e794323b453885f5181f1b624d0b**

**ortspoon:d8578edf8458ce06fbc5bb76a58c5ca4**

**reallychel:5f4dcc3b5aa765d61d8327deb882cf99**

**simmson56:96e79218965eb72c92a549dd5a330112**

**bookma:25d55ad283aa400af464c76d713c07ad**

**popularkiya7:e99a18c428cb38d5f260853678922e03**

**eatingcake1994:fcea920f7412b5da7be0cf42b8c93759**

**heroanhart:7c6a180b36896a0a8c02787eeafb0e4c**

**edi\_tesla89:6c569aabbf7775ef8fc570e228c16b98**

**liveltekah:3f230640b78d7e71ac5514e57935eb69**

**blikimore:917eb5e9d6d6bca820922a0c6f7cc28b**

**johnwick007:f6a0cb102c62879d397b12b62c092c06**

flamesbria2001:9b3b269ad0a208090309f091b3aba9db

oranolio:16ced47d3fc931483e24933665cded6d

spuffyffet:1f5c5683982d7c3814d4d9e6d749b21e

moodie:8d763385e0476ae208f21bc63956f748

nabox:defebde7b6ab6f24d5824682a16c3ae4

bandalls:bdda5f03128bcbdfa78d8934529048cf

**Observations:**

I’m able to crack above bolded passwords from the given data using Hashcat.exe in windows.

|  |  |  |
| --- | --- | --- |
| **Password** | **Algorithm type** | **Cracked password** |
| experthead:e10adc3949ba59abbe56e057f20f883e | MD5 | 123456 |
| ortspoon:d8578edf8458ce06fbc5bb76a58c5ca4 | MD5 | qwerty |
| reallychel:5f4dcc3b5aa765d61d8327deb882cf99 | MD5 | password |
| simmson56:96e79218965eb72c92a549dd5a330112 | MD5 | 111111 |
| interestec:25f9e794323b453885f5181f1b624d0b | MD5 | 123456789 |
| bookma:25d55ad283aa400af464c76d713c07ad | MD5 | 12345678 |
| popularkiya7:e99a18c428cb38d5f260853678922e03 | MD5 | abc123 |
| eatingcake1994:fcea920f7412b5da7be0cf42b8c93759 | MD5 | 1234567 |
| heroanhart:7c6a180b36896a0a8c02787eeafb0e4c | MD5 | password1 |
| edi\_tesla89:6c569aabbf7775ef8fc570e228c16b98 | MD5 | password! |
| liveltekah:3f230640b78d7e71ac5514e57935eb69 | MD5 | qazxsw |
| blikimore:917eb5e9d6d6bca820922a0c6f7cc28b | MD5 | Pa$$word1 |
| johnwick007:f6a0cb102c62879d397b12b62c092c06 | MD5 | bluered |

**Conclusion:**

i) What type of hashing algorithm was used to protect passwords?

Ans: MD5

ii) What level of protection does the mechanism offer for passwords?

Ans: MD5 provides low level of protection and not recommend in the present days.

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

Ans: Below are few implementations:

1. Minimum length password should be implemented
2. Password should be a mixture of numbers, special characters, lowercase and uppercase alphabets
3. High level hashing algorithms like SHA-256 should be used
4. Salting must be done for the passwords

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

Ans: Below are the findings:

1. Minimum length of password was 6.
2. There is no mixture of numbers, special characters, lowercase and uppercase alphabets.

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

Ans:

1. Minimum length of password must be 8 characters.
2. Avoid common passwords like (qwerty, 123456, password) and also date of birth.
3. Use combination of numbers, special characters, lowercase and uppercase alphabets.
4. An API method should be used which gives the strength of the password.