Goldman Sachs Engineering Virtual Experience

CRACK LEAKED PASSWORDS

KNVS SAI SNEHA | Task 1 | 8/9/2022

What type of hashing aggregate was used to protect the password

When I checked the password's security on security.org, I found all passwords to take about n octillion years to crack, because these are encrypted passwords.

Then I used Hashes.com, to find the hashing aggregate, all of the passwords Use MD5 Hashing aggregate/algorithm.

e10adc3949ba59abbe56e057f20f883e md5

25f9e794323b453885f5181f1b624d0b md5

d8578edf8458ce06fbc5bb76a58c5ca4 md5

5f4dcc3b5aa765d61d8327deb882cf99 md5

96e79218965eb72c92a549dd5a330112 md5

25d55ad283aa400af464c76d713c07ad md5

e99a18c428cb38d5f260853678922e03 md5

fcea920f7412b5da7be0cf42b8c93759 md5

7c6a180b36896a0a8c02787eeafb0e4c md5

6c569aabbf7775ef8fc570e228c16b98 md5

3f230640b78d7e71ac5514e57935eb69 md5

917eb5e9d6d6bca820922a0c6f7cc28b md5

f6a0cb102c62879d397b12b62c092c06 md5

What level of protection does the mechanism offer for the password?

For this we will use kali linux, I used ONWORKS , an online kali linux OS provider,

Then Hashcat was used to determine information about hash

What are the disadvantages of MD5?

- When compared to other algorithms like the SHA algorithm, MD5 is comparatively slow.
- It is possible to construct the same hash function for two distinct inputs using MD5.
- MD5 is less secure when compared to the SHA algorithm since MD5 is more vulnerable to collision attacks.

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

Using Hashes.com, I was able to decrypt some of the 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
flamesbria2001:9b3b269ad0a208090309f091b3aba9db
oranolio:16ced47d3fc931483e24933665cded6d
spuffyffet:1f5c5683982d7c3814d4d9e6d749b21e
moodie:8d763385e0476ae208f21bc63956f748
nabox:defebde7b6ab6f24d5824682a16c3ae4
bandalls:bdda5f03128bcbdfa78d8934529048cf
```

So there are many vulnerabilities in your password policy, to make the cracking harder, the company should follow the guidelines below.

a) Keeping a length bound on password, minimum 8 characters should work
b) Making sure that the user includes special characters, uppercase alphabets, numbers, lowercase alphabets, and knows about the strength of password on the go.
c) Using an excellent hashing algorithm, as **MD5** proves to be insecure, Google recommends using stronger hashing algorithms such as **SHA-256** and **SHA-3**. Other options commonly used in practice are **bcrypt** and **scrypt.**
d) Using an password salt, visit https://www.mcafee.com/blogs/enterprise/cloud-security/what-is-a-salt-and-how-does-it-make-password-hashing-more-secure/ For more details.

What can you tell about the organization's password policy? Like password length, key space, etc.

Currently, the password policy is weak and does not guarantee that the

Passwords are strong.

a) There are no rules regarding the length of password.
b) There is no usage of special characters.
c) The Hashing algorithm is weak and insecure.

What can you change in this password policy to make breaking the password much harder?

a) The password must be of minimum 8 characters.
b) Minimum 2 special characters (/,#,*,... etc) must be used in the password, along with Uppercase letter and number.
c) An external API based tool which checks for password strength should show that the used password is strong.