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 minimise 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 organisation. Gaining valid credentials gives the attackers access to the organisation's IT system, thus circumventing most of the 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 organisation'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 the above 13 passwords out of 19 from the given data using Hashcat.exe in windows.

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

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 (message digest algorithm) is a bad password hashing algorithm because it is too fast and memory conserving. Attackers can compute the hash of a large number of passwords per second.

iii) What controls could be implemented to make cracking much harder for the hacker in the event of a password database leaking again?
Ans:
1- Enforce Strong Password Complexity: Require passwords to have a minimum length and be a combination of numbers, special characters, lowercase and uppercase alphabets. This increases the complexity and reduces the likelihood of easily guessable passwords.

2- Use Strong Hashing Algorithms: Implement high-level hashing algorithms like SHA-256 instead of weaker ones like MD5. Stronger algorithms provide better resistance against password cracking attempts**.**

3- Implement Salted Hashes: Use salts with hashes where feasible. Salting adds a random and unique value to each password before hashing, making it much harder for attackers to use precomputed tables (rainbow tables) for password cracking.

4- Utilise Slow Hashing Algorithms: Consider using slow hashing algorithms like bcrypt. These algorithms are intentionally designed to be computationally expensive, requiring more CPU cycles to authenticate a user. This significantly slows down brute-force and dictionary-based attacks.

5- Implement Multi-Factor Authentication (MFA): Require users to provide additional verification factors, such as a unique code sent to their mobile device, in addition to their password. MFA adds an extra layer of security, even if passwords are compromised.

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

Ans:

– The key length is at an average of 11
– Weak hash functions used with no salting
– Common passwords are used which can be easily guessed and cracked
– No use of capital letters, numbers and special symbols together

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

Ans:

– Minimum length of password must be 8 characters.
– Avoid common passwords like (qwerty, 123456, password) and also date of birth.
– Use a combination of numbers, special characters, lowercase and uppercase alphabets.
– An API method should be used which gives the strength of the password.
– Check your password security with password strength checker tools and websites

Thanking You
Manish kumar
Date - 15/07/2023