Keeber 4

NahamCon CTF 2022

The Problem:

The ex-employee also left the company password database exposed to the public through GitHub. Since the password is shared throughout the company, it must be easy for employees to remember. The password used to encrypt the database is a single lowercase word somehow relating to the company. Make a custom word list using the Keeber Security Groups public facing information, and use it to open the password database The flag is in regular format.

(Hint: John the Ripper may have support for cracking .kdbx password hashes!)

The Solve:

We found the file: ksg_passwd_db.kdbx in https://github.com/keebersecuritygroup/password-manager.

We could donwload and generate hash for crack: ksg passwd db:

 $\frac{\$ keepass \$ * 2 * 58823528 * 0 * d1aa5a09ccf3f75d30ea2d548ca045d28252c90adc8bf0}{16bd444cbb3d6d5f65 * 580f6c41d95ea9407da649ee0312209f1686edf0b779458d57}{288ed7043c60ff * aec6b24ac45bf46d4b632d5e408799c7 * 4fa205b599089f79005e1}{76c9c47690ffc58492169309a47613d4269a8ef2a52 * f51a2a1f36f1ca1d10439aa78}{eccece46337274880f594f5a62a703f6007374f} > kp.hash$

Tried some common worlists, but they didn't work. So we needed to generate the company based ones from a files at this url: https://github.com/keebersecuritygroup/security-evaluation-workflow.

What achived the goal.

cewl https://raw.githubusercontent.com/keebersecuritygroup/securityevaluation-workflow/main/code_reviews.txt --lowercase -m 6 -w
keeber3

john --wordlist=keeber3 kp.hash
Using default input encoding: UTF-8
Loaded 1 password hash (KeePass [SHA256 AES 32/64])
Cost 1 (iteration count) is 58823528 for all loaded hashes
Cost 2 (version) is 2 for all loaded hashes

Cost 3 (algorithm [0=AES 1=TwoFish 2=ChaCha]) is 0 for all loaded hashes

Will run 4 OpenMP threads

Press 'q' or Ctrl-C to abort, almost any other key for status 0g 0:00:03:05 57.87% (ETA: 00:50:36) 0g/s 0.1726p/s 0.1726c/s 0.1726C/s ensures..allows

craccurrelss (ksg passwd db)

1g 0:00:04:35 DONE (2022-04-29 00:49) 0.003635g/s 0.1745p/s 0.1745c/s 0.1745C/s ensures..allows

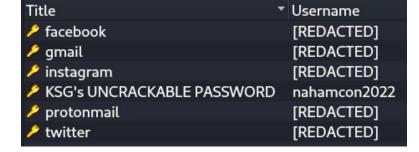
Use the "--show" option to display all of the cracked passwords reliably

Session completed.

Password is: craccurrelss what can open the kdbx file in a program

named KeePassX.

There were many other intresting content in the list.



Under the title "KSG's UNCRACKABLE PASSWORD" the nahamcon2022 user's password is the flag:

flag{9a59bc85ebf02d5694d4b517143efba6}