Goldman Sachs Virtual Internship task answer

Task : Crack leaked password database

Your job is to crack as many passwords as possible with available tools (e.g. use Hashcat). Here are your Task instructions:

1. Review the links provided in the additional resources (section 4) below to gain a background understanding of password cracking
2. Try to crack the passwords provided in the 'password dump' file below using available tools
3. Assess the 5 questions in the task instructions below in relation to the passwords provided (type of hashing algorithm, level of protection, possible controls that could be implemented, password policy, changes in policy)
4. Draft an email/memo briefly explaining your findings in relation to controls used by the organization and your proposed uplifts. We recommend spending about 1.5 hours on this task and keeping it at 1 page in length.

Your answer should be provided in the form of a draft email/memo explaining your findings and conclusions of controls currently used by an organization to prevent successful cracking of passwords and potential uplifts that you would propose to existing controls with justifications.

You must determine the following:

* 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?

Answer:

After the conducted analysis it was determined that organization uses an outdated password hashing algorithm(MD5)which offers very little protection in the event of a password database leaking. It was also determined that the current password policy is not aligned with industry best practices allowing users to have short passwords (6 characters) and reuse usernames as part of passwords.

As a result of the analysis the following uplifts are proposed to increase the overall level of password protection:

* Use a dedicated password hashing algorithm bcrypt , scrypt or PBKDF2 as this will greatly increase the time needed to crack individual passwords,
* Implement salting to prevent usage of rainbow tables to speed up cracking,
* Increase the minimum password length requirement to 10 characters- this will increase the computational effort required to crack password and will give additional time to change all passwords in the event of the password database being leaked,
* Prevent passwords to be the same as usernames or reused as part of the password-such password combination is easy to check without gaining access to the password database itself.
* It is advised to educate users on creating safe and easy to remember passwords. Having a password policy requiring long passwords with a number of special characters results in user writing passwords down or constantly resetting them. The best way to create a strong and user-friendly password is using passphrases(e.g. mygrannyschairhadstaples). The best way to create such passwords is to combine a couple of completely random word. It's also advised to use some special characters and numbers as easy to remember substitutions to expand the key space(e.g. mYgrannyscha1rhadstaples)
* Educate users on the benefits of passwords managers. Having a password manager allows having very long and completely random passwords (e.g. M>?[tk6Cfep68rZ4J)KZWQ8D) without the need to remember/write down. A strong passphrase is still required as a master key for to access the password manager.