**To:** [xyz\_abc@goldmansachs.com](mailto:xyz_abc@goldmansachs.com)

**Cc:**

**Bcc:**

**From:** [nambiar.rutaansh4@gmail.com](mailto:nambiar.rutaansh4@gmail.com)

**Subject:** Engineering virtual program report

Wed 14 July 2021

Respected <recipient>

I would like to thank you for giving me this enormous opportunity to showcase my abilities to perform the task provided by your esteemed firm. I had a delightful experience on learning, gaining knowledge and working on the assignment. Goldman Sachs is a firm with immense global standards and profile, it is an honour to complete this task up to the level and as a keen learner and cyber security engineer, it is my virtuous duty to report to you my findings.

PFB the points I would like to highlight about the task and an attachment to backup the same.

After analysing the given password variables in the provided text file, and using Hash-cat to crack the hashes in my device( Mac OS X with Apple silicon), I have been able to crack passwords with high efficiey . The device specifications are as to provide highly integrated computing as to which I performed this task with decent amount of processes in order to accurately determine the following:

1. The type of hashing algorithm used to protect the password strings is MD5/MD4.
2. The level of protection offered by the implemented hashing mechanism, considering present days competency , is medial. MD5 provides a 128 bit hash to a plaintext, is iterative and generally considered as foundational hashing algorithm. As a security engineer, I am obliged to report you that it is preferable that the family of MD hashes be replaced with a more secure, complex and convoluted mechanisms. Using brute force attacks and rainbow table, it is manageable for someone to decrypt the hashes.
3. In order to control and make cracking much harder for the hacker in the event of a password database leaking again, it is recommended to SHA-2/ SHA-1 or a symmetric cryptographic algorithms . With current GPUs and hash cracking tools, using MD5 is barely better than using nothing at all.
4. Analysing the password dump, what I inferred is that the password policy used by the company is primitive and out of date, the generated file obtained using hashcat containing passwords do not contain variations in upper case and lower case letters and special characters or pass-phrases, it basically consists of straightforward basic strings, It is advisable to update the password policy in order to catch up with the evolution of computing for more security.
5. In order to make password cracking much harder for a hacker, certain policy updates are required in password policy, like:

- Keeping a min count of characters, it is advisable to let a user know that his/her password is too small and simple which might generate vulnerabilities.

-Mandating minimum amount pf uppercase, lowercase and special characters

- Advisable to create pass-phrases instead of pass-words.

- Applying hashing algorithms over another recursively to generate a strong hashing function.

- Using multi factor authentications provides much more secure navigations.

- Not allowing repetitions of old passwords.

PFB Attachment to back up my implementation of the task.

