TO: Goldman Sachs

FROM: Pratyakshi Gambhir

SUBJECT: Analyse results and propose uplifts to controls and policies

Having cracked the hashlist completely using a single tool (Hashcat) and rockyou wordlist, I’d like to provide your organisation with my observations regarding the level of protections offered by currently implemented controls and hoping to minimise the probability of a successful breach in future. The hashing algorithm used by your organisation is MD5, which is a one way cryptographic hash algorithm and is actually considered insecure due to it being vulnerable to cyberattacks. Due to technological advancement, MD5 has been cryptographically broken down and is susceptible to brute force, dictionary, combinator attacks which can easily crack a password produced by an MD5 algorithm nowadays.

Changing the cryptographic hash algorithm being used by the organisation with respect to technological advancement should be taken care of first and foremost. In this age, MD5 is considered an ancient algorithm for hashing password protection — Instead, I'd recommend using at best SHA-256 or SHA-512 or bcrypt or other complex hashing algorithms.

Instead of directly using a hash algorithm on a password, salting should be done in order to strengthen the protection. A strong password policy should be implemented by the organisation. The current password policy of the organisation shows:

* The Min-length rule is not applied to the password.
* There is no rule regarding using special characters or alphanumeric symbols in a single password.
* There is no rule regarding using their own username as password for easier remembrance on user’s ends.
* There is no rule regarding repeating numbers or alphanumeric or special characters that are present sequentially in their password.

Some measures or uplifts I’d like to recommend are as follows:

* Passphrase over password practice should be implemented.
* Length of a password over its complexity would increase the password entropy making it considerably harder to be cracked.
* AI generated passwords provided by the organisation itself should be implemented.
* Usage of special characters and alphanumerics should be encouraged.
* Minimum length rule should be applied in order to increase the entropy of the password.
* Time outs on passwords should be encouraged i.e user should have to create passwords at regular intervals of time.
* Previous passwords shouldn’t be allowed to be used.

[HASHLIST](https://github.com/orv3/Goldman-Sachs-Engineering-Virtual-Program/blob/b62f9452d922137b8b0617bf6d9c3079c8619925/passwd_dump.txt) // [CRACKED PASSWORDS](https://github.com/orv3/Goldman-Sachs-Engineering-Virtual-Program/blob/b62f9452d922137b8b0617bf6d9c3079c8619925/cracked_passwd.txt)