Goldman Sachs Engineering Virtual Program

Memo

To: Goldman Sachs
From: Samuel Waweru
Date: August 16, 2021
Subject: ***Crack leaked password database (Analysis on results and proposal on uplifts to controls and policies)***

This memo explains my finding when I attempted to crack the passwords given using hashcat and terminal.
The type of hashing algorithm used to protect the passwords is the MD5 cryptographic algorithm since the message digests are 32 digits hexadecimal numbers e.g.
experthead:e10adc3949ba59abbe56e057f20f883e

Unfortunately, MD5 Hash algorithm is weak rendering it breakable and hence the level of protection of the passwords is lower than other Hash algorithms like SHA-2.

To make cracking harder in event of a password database leakage, I would suggest the organization changes its password policies to reflect the following ;

- Requiring longer passwords that are sophisticated i.e combine alphabets, numbers and symbols.
- Adopt a two-factor authentication i.e. like a password and a temporary code delivered to a cellphone or to the email.
- Configuring the use of different and long salts on each password in storage.
- Using stronger Hashing algorithms like SHA-2 to encrypt the passwords and that also have an extremely low risk of collision.

After examining the strength of the passwords in the Password Dump document, I concluded that the organization's password policy was fairly weak and would therefore be prone to malicious attacks from hackers. I would suggest that the organization adheres to the recommendations on making cracking harder I highlighted above.

Yours sincerely;
Samuel Waweru
+254 792022398
Mechatronic Engineering Student, JKUAT 2025.

linkedin.com/in/samuelwaweru2001