Goldman Sachs FinTech Engineering Virtual Experience Program

The result and analysis of finding in the context of this assessment are as follows. The passwords were cracked using the Hashcat tool.

experthead: e10adc3949ba59abbe56e057f20f883e: **123456**
popularkiya7: e99a18c428cb38d5f260853678922e03: **abc123**
ortspoon: d8578edf8458ce06fbc5bb76a58c5ca4: **qwerty**
liveltekah: 3f230640b78d7e71ac5514e57935eb69: **qazxsw**
eatingcake1994: fcea920f7412b5da7be0cf42b8c93759: **1234567**
johnwick007: f6a0cb102c62879d397b12b62c092c06: **bluered**
reallychel: 5f4dcc3b5aa765d61d8327deb882cf99: **password**
moodie: 8d763385e0476ae208f21bc63956f748: **moodie00**
interestec: 25f9e794323b453885f5181f1b624d0b: **123456789**
simmson56: 96e79218965eb72c92a549dd5a330112: **111111**
bookma: 25d55ad283aa400af464c76d713c07ad: **12345678**
heroanhart: 7c6a180b36896a0a8c02787eeafb0e4c: **password1**
edi_tesla89: 6c569aabbf7775ef8fc570e228c16b98: **password!**
blikimore: 917eb5e9d6d6bca820922a0c6f7cc28b: **Pa$$word1**
flamesbria2001: 9b3b269ad0a208090309f091b3aba9db: **Flamesbria2001**
oranolio: 16ced47d3fc931483e24933665cded6d: **No Result**
spuffyffet: 1f5c5683982d7c3814d4d9e6d749b21e: **Spuffyffet12**
nabox: defebde7b6ab6f24d5824682a16c3ae4: **nAbox!1**
bandalls: bdda5f03128bcbdfa78d8934529048cf: **Banda11s**

Q: What type of hashing algorithm was used to protect passwords?
A: **MD5** or **MD4** (Raw Hash)

Q: What level of protection does the mechanism offer for passwords?
A:

- MD5 is an iterative hash function.
- MD5 is generally a considerable mechanism for storing passwords in production.
- MD5 produces a 128-bit hash.
- MD5 is backed up by RSA's algorithm (defined in Internet RFC).
- MD5 is a utility that can generate a digital signature of a file. MD5 belongs to a family of one-way hash functions called message digest algorithms. The MD5 system was determined in RFC 1321.
- The algorithm takes stored a message of arbitrary length and produces a 128-bit "fingerprint" or "message digest" of the input as output. It is conjectured that it is computationally infeasible to produce two messages with the same message digest or any message with a given prespecified target message digest. The MD5 algorithm is intended for digital signature applications, where a large file must securely be "compressed" before being encrypted with a private (secret) key under a public-key cryptosystem such as RSA.

Goldman Sachs FinTech Engineering Virtual Experience Program

Q: What controls could be implemented to make cracking harder for the hacker if a password database leaks again?
A:

- One way of making the password hard to crack is by maintaining credentials from a multitude of services in a manager like dashlane because they tend to use various hashing algorithms & even hashing over hashed passwords [e.g., md5(md5($plaintext))] to store and keep the strength high, meeting to the rigidity of a strong case for an algorithm to process.
- Reduce redundancy across services such that in case of a leak out of one service does not make the other passwords vulnerable.
- Use alphanumeric characters with special characters.
- Reducing the occurrence of an adjective on a noun or verb is a conspicuous prey to brute force attacks.

Q: What can you tell about the organization's password policy (e.g., password length, virtual space, etc.)?
A: It can be very well determined that the organization's password policy is not up to the mark as:

- The key length is at an average of 11.
- Although they do not allow spaces, the use of special characters is probably resisted by a set of standard delimiters like '_.'
- Using numbers increases the resistance of passwords by ten times the digit that appears.
- The lack of capital characters splits the password strength by half.
- Not avoiding the occurrence of English verbs like a book, popular, eating, hero, life, John Wick, interest, and expert, in turn, makes the password vulnerable to brute force attacks.

Q: What would you change in the password policy to make breaking the passwords harder?
A:

- Keep a threshold on length.
- Caution overuse of verbs is nouns or adjectives.
- Mandate a minimum of 3 unique characters and a minimum of one capital letter.
- Applying a hashing algorithm over another, recursively to have a vital hashing function, e.g., md5(strtoupper(md5($plaintext)))
- Not allow sibling credentials to assist the password naming, like name/surname/date of birth/sex.

Refrences :

Maximum Security -- Ch 11 -- Trojans.
http://single-honeypot.sourceforge.net/libros/maxsecurity/ch11/ch11.htm

Goldman Sachs FinTech Engineering Virtual Experience Program

What is MD5 (MD5 Message-Digest Algorithm)? - SearchSecurity.
https://www.techtarget.com/searchsecurity/definition/MD5

ISO 3297:2007 Certified DOI Advanced banking transaction using secured ....
https://iarjset.com/wp-content/uploads/2022/07/IARJSET.2022.9695.pdf