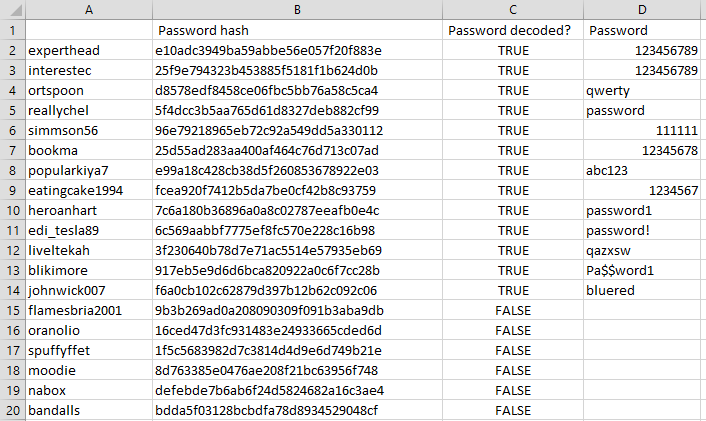
MEMORANDUM

To: Joanna Rycerz

7th September 2021

Warsaw, Masovian District, Poland

I was able to crack 14 of the 20 passwords using dictionary attack (by taking in common passwords from rockyou.txt for comparing) from the hash dump file. (<https://github.com/Guruprasad-G/Swarm-Exploration-and-Target-Searching>)



Q: What type of hashing algorithm was used to protect passwords?

Hashing algorithm used is **MD5** (Message-Digest algorithm 5).

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

MD5, produces a **128-bit hash.** It belongs to a family of one-way hash functions called message digest algorithms.

This encryption of input of any size into hash values undergoes 5 steps, and each step has its predefined task. (

MD5 is a **broken algorithm** which is still being widely used. It is mainly used for integrity check of a file. While MD5 is a generally a good checksum, it is **insecure as a password hashing algorithm** because it is simply too fast.

Q: What controls could be implemented to make cracking much harder for the hacker in the event of a password database leaking again?

* The best way could be to **use better algorithms** such as **SHA256**, SHA-512, RIPEMD-320, and Whirlpool.
* Another way in which MD5 can be used is by **making use of salt**. Adding a randomly generated salt makes sure that there is no hash collision and slows down the attacker.
* Maintain a proper password policy.
* **Reduce redundancy** across services such that in case of a leak out of one service doesn’t make the **other passwords vulnerable**.

Q: What can you tell about the organization’s password policy (e.g. password length, key space, etc.)?

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** to a set of common delimiters like ‘\_’.
* The use of **numbers increases the resistance** of password by a factor of **10 times the digit appears**.
* The **lack of capital characters** splits the password strength by half.
* **Avoid using passwords such as 123456789, “password”, etc. that are commonly known to be used.**

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

* Keeping a **threshold on length**.
* **Caution** over use of **verbs are nouns or adjectives**.
* **Mandating** minimum **3 special characters and minimum one capital letter**.
* Applying a **hashing algorithm over another**, recursively to have a strong hashing function.
* **Not allowing easily breakable or guessable nouns as passwords.**
* **Not allowing sibling credentials** **to assist** the password naming, like name / surname / date of birth / sex.