To whom this may concern,

After attempting to crack the passwords in the password dump file, I found that it was rather easy to crack them.

By using the website Hashes.com/, I found the type of Hashing algorithm used to encrypt all the passwords in the password dump using Kali Linux. To help decrypt them, I utilized rockyou.txt.gz or the ‘crackstation’ wordlist.

MD5 was the hashing algorithm used to protect the passwords, and I found that the algorithm provides a rather weak mechanism to protect user passwords.

The password policy of this organization seems to allow:

Users to have min length of 6 characters in their passwords

1. Allow users, at their own discretion, to have numbers **or** letters in their passwords.

Since the organization's password policy is rather weak, I have a few other suggestions that I think should be implemented in the organization's updated password policy.

1. Stay away from common phrases like password, qwerty, 1234, et cetera…
2. Longer passwords= harder the crack
3. Avoid reusing passwords
4. Use special characters like _!@#$%, et cetera…
5. Don’t use username or anything personal to user like birthdates, actual name be used as password
6. Utilizing the Secure Hashing Algorithm [SHA-256] to protect passwords because it is the strongest algorithm, as I write this email, that encrypts passwords the best.
7. Before a user creates a password, these 5 policies should be visible oin their screens to help them create stronger passwords.

I hope this report can be of great use to help better protect users' passwords, and I hope this email finds you well.

Sincerely,

Fatoumata Fatima Dembélé