Task: Crack leaked passwords database

Dear Sir/Madam,

This is regarding the findings of the passwords which occurred due to the database leak.

What I could make out from my findings is that the passwords make use of the MD5 hashing algorithm, which with the aid of nicely crafted wordlists are prone to be cracked by crackers. Also, the passwords does not make use of security mechanisms like salting, which if used can delay or prevent (in some cases) the passwords from getting cracked.

If there is to be a password database leak again, by all means which should not happen, then it is recommended that the company make use of security mechanisms like salting, which could be implemented to make cracking much harder for the hacker.

The company’s password policy must be rechecked and strengthened, as the strength of the passwords when checked (determines the time taken by a cracker to take it down), showed that the passwords are relatively weak, and thus, the company should refurbish their policy by increasing the complexity and length of the passwords. Thus, the passwords must make use of a mixture of Block letters, small case letters, numbers and special characters, and the policy should define the minimum limit of the passwords to be at least 8 characters long.

Also, the company must change the hashing algorithm it uses. By doing so, not only will the user passwords be more secure and complex to crack, but, the hashing algorithm will be more secure, and make it much harder for the hackers to crack the password.