

**Inside Sherpa’s Virtual Internship**

**“CRACK LEAKED PASSWORD DATABASE”**

After analyzing, reached to a conclusion that organization is using MD5 password hashing algorithm which is more vulnerable to a breach in the password leaking event of a database. The following are the findings to the analysis over the controls currently utilized by the organization to prevent successful cracking of the passwords and proposing potential uplifts for the current controls:

* Increase the time needed for cracking the passwords by using PBKDF2, bycrypt or scrpyt hashing algorithm instead of MD5
* Incorporate password salting to defend the rainbow tables as they can help in speeding up the cracking
* The minimum password length is 6 characters at present therefor increase the minimum password length to 10 characters that will allow you too have extra time to reset the passwords
* Best practice is to avoid reused password, similar username passwords or but obvious passwords to decrease the ease of password leaking of the database
* Upgrading the password policy to long passwords that includes alpha-numeric and special characters and reset the passwords now and then. (e.g. uSasmu@Dallas7). Also enabling Multi Factor Authentication that reduces the risk of the breach and limit the number of login attempts as well.

These proposals are aligned with the best practices of the password policy in an organization that are needed to be implemented. Motivate to use password manager to enhance the efficiency without the need to memorize or writing it down without sacrificing the password policies best practices.