Respected Sir/Ma’am,

I am Kushagra Singh, participated in an internship “Crack Leaked Password database” and engaged in all resources available.

I have found following:

1. MD5 (Message Digest algorithm 5) is weak and insecure. It can be easily cracked by hackers; hence, it is recommended to use latest hashing techniques like SHA (Secure Hash Algorithm) to minimise the risk.
2. From the “Anatomy of a hack” as provided in resource, it is very clear that a weak password is a piece of cake for hackers and crackers and if MD5 is used is a boon. It describes how various techniques like brute-force attack can be used to hack such passwords using premade combinations of passwords.
3. A **salt** is random data that is used as an additional input to a one-way function that hashes data, a password  or passphrase Salts are used to safeguard passwords in storage. It is used in SHA-256.
4. A hash function is used to generate a unique hash code for each combination of characters in alpha-numeric form. It is used to secure potential data and information, for example, in blockchain.
5. Password cracking tools are used to recover the password of the encrypted file or system.
6. Password Strength checker can be used to check the password strength, how strong or weak is the password.

From the password dump file as provided, after trying to crack and recover the passwords, following conclusions are made:

1. The password policy used is not up to the mark. The passwords used are too weak.
2. MD5 algorithm makes the storage of passwords even worse, and were easily cracked using cracking tools in kali-linux like hashcat or online hash decrypt tools.

Following Measures can be taken to make strong passwords and password storage:

1. The password length should be of minimum 6 to 8 characters long.
2. Passwords should be alphanumeric in nature i.e., at least one combination of alphabet and a numeric.
3. The password should contain at least one special character like $, @, # etc.
4. Password re-use should be avoided.
5. Do not use any personal information like name, parent’s name, date of birth etc., in passwords.
6. Use latest hashing algorithms to store passwords, which uses latest and updated security measures.

Thank you!