To:

IT Security Team

From: [Panuganti Neha], Governance Analyst

Date: [23-05-2004]

Subject: Password Security Assessment and Recommendations

Findings

1. Type of Hashing Algorithm: Upon analyzing the provided password dump, it was identified that the hashes use the MD5 hashing algorithm.

2. Level of Protection: The MD5 hashing algorithm offers minimal protection due to its susceptibility to various attack methods such as brute force and rainbow table attacks. This is evident from the ease with which many passwords were cracked using common wordlists.

3. Controls to Enhance Security: To improve security and make password cracking significantly more challenging, the following controls are recommended:

- **Adopt Stronger Hashing Algorithms:** Replace MD5 with bcrypt, Argon2, or PBKDF2, which are designed to be computationally intensive and thus harder to crack.
- **Implement Salting:** Introduce a unique salt for each password before hashing to prevent the use of rainbow tables.
- **Enforce Multi-Factor Authentication (MFA):** Implement MFA to add an extra layer of security, making it harder for attackers to gain unauthorized access even if they crack a password.

4. Current Password Policy: The password analysis indicates a lack of sufficient complexity and length in the organization’s password policy. Many passwords were simple and easily cracked. Several passwords in the list appear to be simple, such as "password" (MD5 hash: 5f4dcc3b5aa765d61d8327deb882cf99), indicating a lack of complexity and length.

5. Recommendations for Password Policy Improvements: To enhance the security of user passwords, the following policy changes are recommended:

- **Increase Minimum Password Length:** Require passwords to be at least 12-16 characters.
- **Enforce Complexity Requirements:** Mandate the inclusion of uppercase letters, lowercase letters, numbers, and special characters.
- **Implement Password Expiration:** Require users to change their passwords periodically while balancing to avoid creating frustration.
- **Password History and Reuse:** Implement rules to prevent the reuse of a certain number of previous passwords.
- **User Education:** Educate users on creating strong, unique passwords and the risks of password reuse across multiple sites.

Conclusion

The current use of the MD5 hashing algorithm provides inadequate protection for user passwords, making them vulnerable to various attack methods. By implementing stronger hashing algorithms, incorporating salts, enforcing MFA, and updating the password policy to require stronger, more complex passwords, the organization can significantly enhance its overall security posture.

Best regards, Governance Analyst