To: IT Security Team
From: Sunil Roshan A, Governance Analyst
Date: 2024-04-22
Subject: Password Security Assessment and Recommendations

Analysis:

25d55ad283aa400af464c76d713c07ad:12345678

25f9e794323b453885f5181f1b624d0b:123456789

3f230640b78d7e71ac5514e57935eb69:qazxsw

5f4dcc3b5aa765d61d8327deb882cf99:password

6c569aabbf7775ef8fc570e228c16b98:password!

7c6a180b36896a0a8c02787eeafb0e4c:password1

917eb5e9d6d6bca820922a0c6f7cc28b:Pa$$word1

96e79218965eb72c92a549dd5a330112:111111

d8578edf8458ce06fbc5bb76a58c5ca4:qwerty

e10adc3949ba59abbe56e057f20f883e:123456

e99a18c428cb38d5f260853678922e03:abc123

f6a0cb102c62879d397b12b62c092c06:bluered

fcea920f7412b5da7be0cf42b8c93759:1234567

16ced47d3fc931483e24933665cded6d:Oranolio1994

1f5c5683982d7c3814d4d9e6d749b21e:Spuffyffet12

8d763385e0476ae208f21bc63956f748:moodie00

9b3b269ad0a208090309f091b3aba9db:Flamesbria2001

defebde7b6ab6f24d5824682a16c3ae4:nAbox!1

bdda5f03128bcbdfa78d8934529048cf:Banda11s

This assessment identified that password hashes were generated using MD5, a weak hashing algorithm susceptible to brute-force attacks. Additionally, the analysis revealed a concerning number of weak passwords among the samples provided.

Recommendations:

->Strong Hashing: Implement a well-regarded hashing algorithm like bcrypt, scrypt, or PBKDF2. These slow down brute-force attacks significantly.

->Robust Password Policy: Enforce a policy requiring:

- Minimum 12 character length.
- Focus on length over complex requirements.
- Ban on dictionary words and common phrases.
- Periodic password changes (e.g., 6 months).

->Multi-Factor Authentication (MFA): Implement MFA for an extra layer of security beyond passwords.

->User Education: Regularly educate users on password hygiene best practices.

Implement salting to prevent usage of rainbow tables to speed up cracking.

Justification:

Stronger hashing algorithms significantly increase password cracking time and resources. Robust password policies ensure users create unique, strong passwords. MFA adds a crucial second layer of defense. User education empowers informed security choices.

Conclusion:

Implementing these recommendations strengthens the organization's password security posture, deterring unauthorized access and minimizing breach risks.