Project Report: Strengthening Password Security Measures

Dear Sir/Madam,

I hope this message finds you well. As part of my role as a governance analyst, I have conducted an in-depth assessment of the current password protection measures within our organization. I am writing to address the vulnerabilities identified and propose comprehensive enhancements to our password policy, based on a rigorous analysis of the exposed passwords.

It is evident that the use of the Message Digest (MD5) hashing algorithm to safeguard passwords is posing a significant security risk. MD5 is now considered a weak algorithm, susceptible to breaches. Through the utilization of Hashcat.com and the "rockyou.txt" wordlist, I was able to swiftly crack passwords encrypted with MD5, underscoring its inadequacy for robust protection.

To fortify our security posture, I strongly recommend adopting the Secure Hash Algorithm (SHA), a more resilient cryptographic hash function, for generating password hashes.

Upon successful password cracking, the following insights were gleaned regarding our organization's current password policy:

* **Minimum Password Length**: The current policy mandates a minimum password length of 6 characters. This minimal requirement leaves our system susceptible to brute-force attacks.
* **Password Complexity**: Our existing policy lacks specific guidelines for password creation. Users have the liberty to utilize simple combinations of words and letters, undermining our security framework.

In light of these observations, I propose the following enhancements to our password policy:

* **Stringent Complexity Rules**: Discourage the use of common words and character combinations. Require a combination of uppercase and lowercase letters, numbers, and special characters.
* **Password Length**: Set a minimum password length of at least 12 characters. Longer passwords significantly increase the resistance against unauthorized access.
* **Prohibit Reuse**: Implement a policy to prevent users from reusing previously used passwords, thereby mitigating the risk of compromise.
* **Exclusion of Personal Information**: Disallow the inclusion of usernames, actual names, dates of birth, or any other easily guessable personal information in passwords.
* **Educational Initiatives**: Develop user training programs to educate and encourage compliance with the enhanced password policy. Well-informed users are pivotal in maintaining password security.

Incorporating these recommended uplifts will significantly bolster our organization's resilience against cyber threats and unauthorized access attempts. It is paramount that we prioritize these measures to safeguard our sensitive data and ensure the integrity of our systems.

Please feel free to reach out if you require further clarification or assistance with the implementation of these proposals.

Best Regards,

Balasubramanian PG  
Masters of Business Administration, Business Analytics

*Attachments:*



The Following were my observations after attempting to crack the passwords:

Security Algorithms used:

experthead:e10adc3949ba59abbe56e057f20f883e – MD5

interestec:25f9e794323b453885f5181f1b624d0b – MD5

ortspoon:d8578edf8458ce06fbc5bb76a58c5ca4 –MD5

reallychel:5f4dcc3b5aa765d61d8327deb882cf99 –MD5

simmson56:96e79218965eb72c92a549dd5a330112 – MD5

bookma:25d55ad283aa400af464c76d713c07ad – MD5

popularkiya7:e99a18c428cb38d5f260853678922e03 – MD5

eatingcake1994:fcea920f7412b5da7be0cf42b8c93759 – MD5

heroanhart:7c6a180b36896a0a8c02787eeafb0e4c – MD5

edi\_tesla89:6c569aabbf7775ef8fc570e228c16b98 – MD5

liveltekah:3f230640b78d7e71ac5514e57935eb69 – MD5

blikimore:917eb5e9d6d6bca820922a0c6f7cc28b – MD5

johnwick007:f6a0cb102c62879d397b12b62c092c06 – MD5

flamesbria2001:9b3b269ad0a208090309f091b3aba9db – MD5

oranolio:16ced47d3fc931483e24933665cded6d - MD5

spuffyffet:1f5c5683982d7c3814d4d9e6d749b21e - MD5

moodie:8d763385e0476ae208f21bc63956f748 - MD5

nabox:defebde7b6ab6f24d5824682a16c3ae4 - MD5

bandalls:bdda5f03128bcbdfa78d8934529048cf - MD5

Cracked Passwords:

experthead:e10adc3949ba59abbe56e057f20f883e - 123456

interestec:25f9e794323b453885f5181f1b624d0b - 123456789

ortspoon:d8578edf8458ce06fbc5bb76a58c5ca4 - qwerty

reallychel:5f4dcc3b5aa765d61d8327deb882cf99 - password

simmson56:96e79218965eb72c92a549dd5a330112 - 111111

bookma:25d55ad283aa400af464c76d713c07ad - 12345678

popularkiya7:e99a18c428cb38d5f260853678922e03 - abc123

eatingcake1994:fcea920f7412b5da7be0cf42b8c93759 - 1234567

heroanhart:7c6a180b36896a0a8c02787eeafb0e4c - password1

edi\_tesla89:6c569aabbf7775ef8fc570e228c16b98 - password!

liveltekah:3f230640b78d7e71ac5514e57935eb69 - qazxsw

blikimore:917eb5e9d6d6bca820922a0c6f7cc28b - Pa$$word1

johnwick007:f6a0cb102c62879d397b12b62c092c06 - bluered