In the process of attempting to crack the hashes that have been provided, several detrimental vulnerabilities were identified.

The algorithms used in this case is the MD5 (Message Digest) hashing function which has caused these passwords to be compromised.

This is because MD5 is a standard but outdated algorithm that are is not recommended in today’s day and age because the level of protection offered is very miniscule as it has proven to be a weak algorithm and is very prone to hackers.

The Hashcat software or other adjacent decryption applications coupled with the rockyou.txt wordlist would have sufficed in decrypting these passwords. Controls that are to be implemented in the case of a more secure encryption would be using the SHA (Secure Hash Algorithm) encryption.

The password policy deduced by the analysis of the cracked passwords are:

* The length of a password must be 6 characters at a minimum.
* Any alphanumeric characters can be used, as well as the non-inclusion of those characters are accepted as well.

This policy, as evidently exposed in the cracking process of the passwords, is flawed and a few revisions are necessary to up the ante with regards to the security level.

A few vital changes that would improve the security conditions would be:

* The minimum length of a password must be revised to **8 characters** at a minimum.
* A combination of alphabets along with at-least one number and one character should be mandatory in creating a password. This is explained by the decryption time frame estimate of such a password on howsecureismypassword.net.
* Do not let users include their username, actual name, date of birth and other personal information in their password.
* Common words and letters are to be avoided and passwords must not be reused in the event of changing an old password.

This newly updated policy coupled with a strong encryption algorithm in the likes of SHA is recommended to upgrade the protection level of user passwords.

S. Rohith

IT Undergraduate as SSN College of Engineering.

**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**