Respected Sir/Ma’am,

**My Approach:**

Running the following command in Windows PowerShell: **.\hashcat.exe -m 0 -a 3 -o cracked.txt hash.txt**

Hash type used: **MD5 (-m 0)**

Attack Mode used: **Brute Force (-a 3)**

**Following are the cracked passwords:**

johnwick007:f6a0cb102c62879d397b12b62c092c06:bluered

bookma:25d55ad283aa400af464c76d713c07ad:12345678

reallychel:5f4dcc3b5aa765d61d8327deb882cf99:password

moodie:8d763385e0476ae208f21bc63956f748:moodie00

interestec:25f9e794323b453885f5181f1b624d0b:123456789

bandalls:bdda5f03128bcbdfa78d8934529048cf:Banda11s

blikimore:917eb5e9d6d6bca820922a0c6f7cc28b:Pa$$word1

experthead:e10adc3949ba59abbe56e057f20f883e:123456

popularkiya7:e99a18c428cb38d5f260853678922e03:abc123

eatingcake1994:fcea920f7412b5da7be0cf42b8c93759:1234567

ortspoon:d8578edf8458ce06fbc5bb76a58c5ca4:qwerty

simmson56:96e79218965eb72c92a549dd5a330112:111111

edi\_tesla89:6c569aabbf7775ef8fc570e228c16b98:password!

liveltekah:3f230640b78d7e71ac5514e57935eb69:qazxsw

heroanhart:7c6a180b36896a0a8c02787eeafb0e4c:password1

**What type of hashing algorithm was used to protect passwords?**

MD5 Hashing Algorithm has been used. Which is a part of the Message Digest Algorithm family created to verify the integrity of any message or file that is hashed.

**What level of protection does the mechanism offer for passwords?**

MD5 Hashing Algorithm is a cryptographic hashing function and is considered insecure. Hence it should not be used for password protection. MD5 also has a low collision resistance.

It is a very fast algorithm and a computer will have the ability to try many combinations in just a few seconds using Brute Force attack.

**What controls could be implemented to make cracking much harder for the hacker in the event of a password database leaking again?**

* SHA-2 be used instead of MD5
* The Secure Hash Algorithm or SHA is a better alternative for MD5.
* It is equally easy to use SHA-2 in place of MD5 in any modern programming framework.
* To use MD5 effectively, we can use salts; which basically is a word added before and/or after each password to increase the length of the password which makes it harder to decrypt.

**What can you tell about the organization’s password policy(e.g. password length, key space, etc.)?**

* The minimum length of password required appears to be 6.
* The password requires a combination of uppercase letters, lowercase letters, numbers and special characters.

**What would you change in the password policy to make breaking the passwords harder?**

* Ask the user to use a complex password (a combination of uppercase letters, lowercase letters, numbers, special characters, etc.)
* Do not let the user use passwords which are predictable, for example: their name, their date of birth, passwords like: password, p@$$word, etc.
* Increase the length of the password.

Thanking You

Yours sincerely

***Aafreen Singh***

*+91 7087271954*

*7 July 2022*