**Date - 07/16/2022**

**Subject – Cracking leaked passwords Database**.

The result and analysis of my finding in context to this assessment are as follows. I have cracked the some of the leaked password using the ***Hashcat*** tool.

```
experthead:e10adc3949ba59abbe56e057f20f883e
interestec:25f9e794323b453885f5181f1b624d0b
ortspoon:d8578edf8458ce06fbc5bb76a58c5ca4
reallychel:5f4dcc3b5aa765d61d8327deb882cf99
simmson56:96e79218965eb72c92a549dd5a330112
bookma:25d55ad283aa400af464c76d713c07ad
popularkiya7:e99a18c428cb38d5f260853678922e03
eatingcake1994:fcea920f7412b5da7be0cf42b8c93759
heroanhart:7c6a180b36896a0a8c02787eeafb0e4c
edi_tesla89:6c569aabbf7775ef8fc570e228c16b98
liveltekah:3f230640b78d7e71ac5514e57935eb69
blikimore:917eb5e9d6d6bca820922a0c6f7cc28b
johnwick007:f6a0cb102c62879d397b12b62c092c06
flamesbria2001:9b3b269ad0a208090309f091b3aba9db
oranolio:16ced47d3fc931483e24933665cded6d
spuffyffet:1f5c5683982d7c3814d4d9e6d749b21e
moodie:8d763385e0476ae208f21bc63956f748
nabox:defebde7b6ab6f24d5824682a16c3ae4
bandalls:bdda5f03128bcbdfa78d8934529048cf
```

**Hashing Algorithm used: MD5**

**Level of protection: MD5 (message digest algorithm) is a bad password hashing algorithm because it** is too fast and memory conserving. Attacker can compute the hash of large number of passwords per second.

**Recommendations to implement password:**

- Try using better algorithm in place of MD5. Eg.SHA256

- Always use salts with hashes where feasible.

- for better security use slow algorithm like *bcrypt*. Which make harder for attacker because it requires more CPU cycles to authenticate user.

**Observations on organization password policy**:

- weak hash functions used with no salting

- common passwords are used which can be easily guessed and cracked

- No use of capital letters, numbers and special symbols together.

**Changes to be made in password policy:**

- we can increase the password length to 12-15 because less characters length it becomes easy for hacker to crack the password using brute force attack.

- Don’ t use common phrase as password. Use of mix characters including Symbols, Special Characters and numbers.

- check your password security with password strength checker tools and websites.

Thank you<br>
Pransu Yadav