Date- 30/09/2023

Subject: Cracking Leaked passwords

The result and analysis of my findings in context to the task is explained below.

13/19 of the leaked passwords are cracked using ***Hashcat*** tool. I used rockyyou.txt as guess base, the hash mode used: MD5 and attack mode : straight.

e10adc3949ba59abbe56e057f20f883e: **123456**

25f9e794323b453885f5181f1b624d0b: **123456789**

5f4dcc3b5aa765d61d8327deb882cf99: **password**

25d55ad283aa400af464c76d713c07ad: **12345678**

e99a18c428cb38d5f260853678922e03: **abc123**

d8578edf8458ce06fbc5bb76a58c5ca4: **qwerty**

7c6a180b36896a0a8c02787eeafb0e4c: **password1**

fcea920f7412b5da7be0cf42b8c93759: **1234567**

96e79218965eb72c92a549dd5a330112: **111111**

6c569aabbf7775ef8fc570e228c16b98: **password!**

3f230640b78d7e71ac5514e57935eb69: **qazxsw**

f6a0cb102c62879d397b12b62c092c06: **bluered**

917eb5e9d6d6bca820922a0c6f7cc28b: **Pa$$word1**

Hashing Algorithm used : MD5

Level of Protection :

MD5 is not the ideal password hashing algorithm despite being memory conservant and too fast, is able to be cracked by attackers a large number of passwords per second.

Recommendation to Implement passwords:

- Use *salting*. Salting with hashing increases security against attacks

-Use a better hashing algorithm (which takes much more time to crack than MD5) instead of MD5 (eg: *SHA-512*)

- Even though memory hard, use time taking algorithms like *bcrypt*

Observations of Organisation password policy:

- Weak hash algorithm used

- No salting

- No instructions to include different cases, numbers and special characters in the same password which will make password cracking much more difficult.

- common passwords like ‘123456’ is used often

Changes to be made in Password Policy:

-Increase the minimum length of password to 10 or more to decrease the chance of getting brute force attack by attackers.

-Prohibit using common passwords.

-Make it mandatory to use different cases, numbers and special characters in the same password

Thank You,

Leeviya T S