Respected Sir/Madam,

I was able to crack 19 passwords from the given 19 hashcodes in the password dump file very easily using hashmap and hashes.com

experthead:e10adc3949ba59abbe56e057f20f883e md5 123456

interestec:25f9e794323b453885f5181f1b624d0b md5 123456789

ortspoon:d8578edf8458ce06fbc5bb76a58c5ca4 md5 qwerty

reallychel:5f4dcc3b5aa765d61d8327deb882cf99 md5 password

simmson56:96e79218965eb72c92a549dd5a330112 md5 111111

bookma:25d55ad283aa400af464c76d713c07ad md5 123456789

popularkiya7:e99a18c428cb38d5f260853678922e03 md5 abc123

eatingcake1994:fcea920f7412b5da7be0cf42b8c93759 md5 1234567

heroanhart:7c6a180b36896a0a8c02787eeafb0e4c md5 password1

edi\_tesla89:6c569aabbf7775ef8fc570e228c16b98 md5 password!

liveltekah:3f230640b78d7e71ac5514e57935eb69 md5 qazxsw

blikimore:917eb5e9d6d6bca820922a0c6f7cc28b md5 Pa$$word1

johnwick007:f6a0cb102c62879d397b12b62c092c06 md5 bluered

flamesbria2001:9b3b269ad0a208090309f091b3aba9db md5 Flamesbria2001

oranolio:16ced47d3fc931483e24933665cded6d md5 Oranolio1994

spuffyffet:1f5c5683982d7c3814d4d9e6d749b21e md5 Spuffyffet12

moodie:8d763385e0476ae208f21bc63956f748 md5 moodie00

nabox:defebde7b6ab6f24d5824682a16c3ae4 md5 nAbox!1

bandalls:bdda5f03128bcbdfa78d8934529048cf md5 Banda11s

Observations:

1)What type of hashing algorithm was used to protect passwords?

Ans: Md5

2)What level of protection does the mechanism offer for passwords?

Ans: the MD5 hashing algorithm offers weak protection, making it easier for hackers to crack passwords, especially when they have access to the hashed passwords in the event of a password database leak.

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

Ans: To make it harder for hackers to crack our passwords, we need to implement the following measures:

a. Stronger Hashing Algorithm: Replace MD5 with a stronger algorithm like bcrypt, SHA-256, or Argon2. These algorithms make it much harder for hackers to crack passwords.

b. Salting: Add a unique random value (salt) to each password before hashing. This prevents hackers from using precomputed tables to crack passwords.

c. Password Complexity Policy: Enforce a strict password policy that requires longer passwords with a mix of uppercase and lowercase letters, numbers, and special characters. This makes it much harder for hackers to guess passwords.

d. Regular Password Policy Review: Review our password policy regularly to keep up with the latest security standards.

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

Ans :Password Policy Insights: From the passwords I cracked, I noticed that our current policy lacks enough complexity. Most passwords were short and lacked special characters, making them easy targets for hackers.

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

Ans: To improve password strength, we should:

a. Increase Minimum Password Length: Set a minimum password length of at least 12 characters to make it harder for hackers to guess passwords.

b. Include Special Characters: Require the use of special characters in passwords to add more complexity.

c. Educate Users: Teach employees about the importance of strong passwords and the risks of weak passwords.