Respected Sir/Ma’am,

As mentioned in the introduction tutorial, I utilised the Hascat password cracking tool to crack the hashes in the dump file provided. I was surprised that I was able to crack passwords using basic commands despite having no prior experience. As a result of this, there are several vulnerabilities and insecurities that must be addressed.

I cracked 14 of the 18 total hashes in a matter of moments. These are the results of my findings :

E10adc3949ba59abbe56e057f20f883e: 123456

25f9e794323b453885f5181f1b624d0b: 123456789

D8578edf8458ce06fbc5bb76a58c5ca4: qwerty

5f4dcc3b5aa765d61d8327deb882cf99: password

96e79218965eb72c92a549dd5a330112: 111111

25d55ad283aa400af464c76d713c07ad: 12345678

E99a18c428cb38d5f260853678922e03: abc123

Fcea920f7412b5da7be0cf42b8c93759: 1234567

7c6a180b36896a0a8c02787eeafb0e4c: password1

6c569aabbf7775ef8fc570e228c16b98: password!

3f230640b78d7e71ac5514e57935eb69: qazxsw

917eb5e9d6d6bca820922a0c6f7cc28b: Pa$$word1

F6a0cb102c62879d397b12b62c092c06: bluered

8d763385e0476ae208f21bc63956f748: moodie00

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

* **MD5** (message-direct-algorithm)
* What level of protection does the mechanism offer for passwords?

* **MD5** provides a very basic level of protection. It is outdated, insecure and vulnerable to several cryptographic attacks.
* What controls could be implemented to make cracking much harder for the hacker in the event of a password database leakage again?
* Enforce strong password regulations that require users to construct passwords that include uppercase and lowercase letters, digits, and special characters.
* Keep passwords safe and encrypted by using strong hashing algorithms like bcrypt, or scrypt.
* Implement salted hashes for password storage to provides an additional layer of security.
* Conduct frequent security audits and penetration testing to detect password management system flaws and shortcomings.
* Address any issues as soon as possible and keep security measures up to date.
* What can you tell about the organization’s password policy (e.g. password length, key, spaces, etc.)?
* There is no minimum length requirement for passwords.
* There are no restrictions on the use of special characters in passwords.
* Use of weak hash functions with no salting
* What would you change in the password policy to make breaking the passwords harder?

Following are my suggestions for the same :

* We can raise the password length to 10 characters or more.
* A minimum of two special characters (/,#,\*,...) must be used in the password.
* Use password strength checking tools and websites to ensure the security of your passwords.
* Never use a common phrase as a password. Use of a variety of characters.

However excessive strict password policies may lead to user frustration . Finding a proper balance between user experience and security is a must!

Thank You

Shikhar Reyya