**Module 1: Crack Leaked password Database**

Jeenal Shah

B.Tech. Computer Science Engineering

Ahmedabad University ’ 23

Respected sir/ma’am,

I attempted to crack the passwords given in the password\_dump.txt file using the Hashcat software. I found the software easy to use.

I found out that MD5 hashing algorithm was used which is comparatively a weaker hash algorithm as it is too fast and memory-conserving. We should focus on slowing down the hacker by generating a cryptographically secure value for all the passwords. Hence, the level of protection of the passwords was compromised.

My suggestion for making password cracking much harder would be by using strong encryption method like Secure Hashing Algorithm(SHA).

About the organization password policy:

1. Minimum length of the passwords is 6.
2. It seems like there is no special requirements for creating a password i.e. no compulsion of using numbers, special characters, and capitals.
3. Users are allowed to use any combination of words, letters and symbols to create a password.
4. Such carelessness could lead to easy hacking of passwords.

My recommendations are:

1. Minimum length should be set to 8.
2. Compulsory combination of letters, numbers and special symbols must be used.
3. Capital letters should also be used.
4. There must be no reuse of the passwords.
5. Users should not be allowed to include their name, date of birth and personal information which are open to the world.
6. These restrictions should be made a compulsion.

**Cracked Passwords:**

experthead:e10adc3949ba59abbe56e057f20f883e - **123456**

interestec:25f9e794323b453885f5181f1b624d0b - **123456789**

ortspoon:d8578edf8458ce06fbc5bb76a58c5ca4 - **qwerty**

reallychel:5f4dcc3b5aa765d61d8327deb882cf99 - **password**

simmson56:96e79218965eb72c92a549dd5a330112 - **111111**

bookma:25d55ad283aa400af464c76d713c07ad - **12345678**

popularkiya7:e99a18c428cb38d5f260853678922e03 - **abc123**

eatingcake1994:fcea920f7412b5da7be0cf42b8c93759 - **1234567**

heroanhart:7c6a180b36896a0a8c02787eeafb0e4c - **password1**

edi\_tesla89:6c569aabbf7775ef8fc570e228c16b98 - **password!**

liveltekah:3f230640b78d7e71ac5514e57935eb69 - **qazxsw**

blikimore:917eb5e9d6d6bca820922a0c6f7cc28b - **Pa$$word1**

johnwick007:f6a0cb102c62879d397b12b62c092c06 - **bluered**

Thanks and Regards,

Jeenal Shah