Respected Sir/Madam,
Greetings of the day.

I was tasked with cracking the leaked passwords from your password database. After careful analysis, I have found several vulnerabilities in the password policy of your organization. A few suggestions to make password cracking much more complicated are included in this e-mail, along with a summary of my findings.

All the passwords that were compromised from your organisation's database were using Message Digest (MD5) algorithm for Hashing. MD5 is a weaker hashing algorithm and is prone to collisions. In this case the passwords were very easy to crack with Hashcat.com, Crackstation.net and rockyou.txt wordlist via terminal and web browsers.

It is my suggestion to use Standard Hash Algorithm (SHA) and Message Digest (MD5) which are standard cryptographic hash functions to provide data security and authentication. I would also suggest to use very strong password encryption mechanism to create hashes for the passwords based on SHA.

After cracking the passwords, I have found the following facts about the password policy of your organisation:

1. There is no specific requirement for password creation. Users can use any combination of alpha-numerals to create the password.
2. The minimum password length is 6 characters.

The above password policy does not set any solid rules, and most passwords set by users are weak and easy to crack. I would suggest a few changes that could be implemented in your organisation's password policy to make the passwords set by users stronger and harder to crack.

1. Longer passwords are harder to crack. (example: Set minimum length to 8)
2. Do not use common words or predictable dictionary words (eg: avoid words in dictionary like London19, lovedogs, wolves99 etc as passwords)
3. Do not use common patterns as passwords(example: abc123, xyz999 etc)
4. Never reuse passwords
5. Include capital letter, small letter, special characters and numbers in your password
6. Do not use personal information in passwords(eg: avoid using name, username, date of birth or phone number while creating the password)
7. Train users to follow the policy and use simple phrases that are easy to remember so they can keep their passwords safe.

I hope the above analysis and suggestions will be of some help to your organisation.

Thank you.

Warm Regards,

Srimoyee Dutta.

BE Computer Engineer.

The hashing algorithms used were:

```
experthead:e10adc3949ba59abbe56e057f20f883e     : MD5
interestec:25f9e794323b453885f5181f1b624d0b     : MD5
ortspoon:d8578edf8458ce06fbc5bb76a58c5ca4       : MD5
reallychel:5f4dcc3b5aa765d61d8327deb882cf99     : MD5
simmson56:96e79218965eb72c92a549dd5a330112      : MD5
bookma:25d55ad283aa400af464c76d713c07ad         : MD5
popularkiya7:e99a18c428cb38d5f260853678922e03   : MD5
eatingcake1994:fcea920f7412b5da7be0cf42b8c93759 : MD5
heroanhart:7c6a180b36896a0a8c02787eeafb0e4c     : MD5
edi_tesla89:6c569aabbf7775ef8fc570e228c16b98    : MD5
liveltekah:3f230640b78d7e71ac5514e57935eb69     : MD5
blikimore:917eb5e9d6d6bca820922a0c6f7cc28b      : MD5
johnwick007:f6a0cb102c62879d397b12b62c092c06    : MD5
flamesbria2001:9b3b269ad0a208090309f091b3aba9db : MD5
oranolio:16ced47d3fc931483e24933665cded6d       : MD5
spuffyffet:1f5c5683982d7c3814d4d9e6d749b21e     : MD5
moodie:8d763385e0476ae208f21bc63956f748         : MD5
nabox:defebde7b6ab6f24d5824682a16c3ae4          : MD5
bandalls:bdda5f03128bcbdfa78d8934529048cf       : MD5
```

The cracked passwords were:

```
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
```