Goldman Sachs Engineering Virtual Program

Sub: Task 1 - Crack leaked password database.

Respected Sir/Madam,

After cracking the passwords, I found many issues with the organization password policy, and these email summaries all the findings of issues in the passwords and suggestions to improve your password policy.

MD5 hash algorithm was used to protect the password in the given task.

MD5 is a cryptographic hash function, which produces a 128-bit hash value and it composed of 32 hexadecimal characters. Hashing the passwords provide protection for the integrity of data. MD5 is a good checksum but it is insecure as a password-protecting algorithm. Because if any collision attack happens then the MD5 hash can be easily cracked by hackers. In addition, slower and longer, the hash will be more reliable when comes to MD5 is the fastest and shortest generated hashes so that the attackers can be easily cracked it and the level of protection is low.

However, I would strongly suggest implementing other harder algorithms, which are difficult to hack the passwords such as SHA 2, SHA 3, SHA 256, bcrypt, scrypt, etc. Moreover, always use a salt value with the password's hashes so that it will make cracking of passwords much harder for the hackers.

The organization's password policy:

- The minimum length for a password is six characters.
- There is no specific requirement or rules for password creation. Users can use any combination of words and letters to create a password.

My recommendations to change in the password policy:

- Try to use longer passwords at least eight or ten characters so that it will be better and safer.
- The password should include a combination of capital letters, small letters, numbers, and special characters.
- Do not use personal information as a password such as a name, date of birth, company name, etc.
- Give proper awareness to the users about the password policy.

I hope this will be helpful and more informative to your organization.

Sincerely,
Harish Kumar R
BE – Production Engineering (Sandwich)
PSG College of Technology
Coimbatore – 641004
Mobile: 7402060193

OBSERVATIONS

Hashing algorithm used in the passwords:

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**

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**
flamesbria2001:9b3b269ad0a208090309f091b3aba9db	**Flamesbria2001**
spuffyffet:1f5c5683982d7c3814d4d9e6d749b21e	**Spuffyffet12**
moodie:8d763385e0476ae208f21bc63956f748	**moodie00**
nabox:defebde7b6ab6f24d5824682a16c3ae4	**nAbox!1**
bandalls:bdda5f03128bcbdfa78d8934529048cf	**Banda11s**