Overview

As a governance analyst it is part of your duties to assess the level of protection offered by implemented controls and minimize the probability of a successful breach. You often need to know the techniques used by hackers to circumvent implemented controls and propose uplifts to increase the overall level of security in an organization. Gaining valid credentials gives the attackers access to the organization’s IT system, thus circumventing most of perimeter controls in place.

Project Objective

What type of hashing algorithm was used to protect passwords?

What level of protection does the mechanism offer for passwords?

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

Here is a sample data file containing hashes dumped together:

https://cdn.theforage.com/vinternsh0

After the conducted analysis it was determined that organization uses an outdated password hashing algorithm (MD5) which offers very little protection in the event of a password database leaking. It was also determined that the current password policy is not aligned with industry best practices allowing users to have short passwords (6 characters) and reuse usernames as part of passwords.

As a result of the analysis the following uplifts are proposed to increase the overall level of password protection:

• Use a dedicated password hashing algorithm bcrypt, scrypt or PBKDF2 as this will greatly increase the time needed to crack individual passwords,

• Implement salting to prevent usage of rainbow tables to speed up cracking,

• Increase the minimum password length requirement to 10 characters – this will increase the computational effort required to crack password and will give additional time to change all passwords in the event of the password database being leaked,

• Prevent passwords to be the same as usernames or reused as part of the password – such password combination is easy to check without gaining access to the password database itself.

• It is advised to educate users on creating safe and easy to remember passwords. Having a password policy requiring long passwords with a number of special characters results in user writing passwords down or constantly resetting them. The best way to create a strong and user-friendly password is using passphrases (e.g. mygrannyschairhadstaples). The best way to create such passwords is to combine a couple of completely random word. It’s also advised to use some special characters and numbers as easy to remember substitutions to expand the key space (e.g. mYgranny$cha1rhadstaples)

• Educate users on the benefits of passwords managers. Having a password manager allows having very long and completely random passwords (e.g. M>?{tk6Cfep6BrZ4J)KZWQ8j) without the need to remember/write down. A strong passphrase is still required as a master key for to access the password manager.

Project Report and Observations

Completing this task assigned by Goldman Sachs were the two algorithms that I came across. Analysing the passwords and their respective security algorithms used, I narrowed down my observations into this report.

Project Report

Dear Sir/Ma’am

After trying to crack all the leaked hashes, I found several vulnerabilities in your password policy

and this email concludes all the findings and suggestions to improve your password policy.

Secure Hash Algorithm (SHA) and Message Digest (MD5) are the standard cryptographic hash functions

to provide data security for authentication.

All the password which are compromised were using MD5 which is a weaker hash algorithm and is prone to collisions.

It was very easy to crack with Hashcat.com and rockyou.txt wordlist via terminal and web browsers.

I would suggest that you use a very strong password encryption mechanism to create hashes for the password based on SHA.

After cracking the passwords, we find the following things about organisation’s password policy:

• Minimum length for password is set to 6.

• There is no specific requirement for the password creation.

Users can use any combination of word and letters to create a password.

You can include several new things in your password policy. My recommendations are:

• Avoid common words and character combinations in your password.

• Longer passwords are better, 8 characters is a starting point.

• Don’t reuse your passwords.

• Include special character, Capital and Small letters, numbers in your password.

• Don’t let users include their username, actual name, date of birth and other personal information while creating a password.

• Train your users to follow these policies to keep their passwords safe.

Observations:

Security Algorithms used:

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

Resources

https://arstechnica.com/information-technology/2013/05/how-crackers-make-minced-meat-out-of-your-passwords/

https://howsecureismypassword.net/

https://en.wikipedia.org/wiki/Password\_cracking#Software

https://en.wikipedia.org/wiki/Salt\_(cryptography)

https://hashcat.com