**TASKS**

1. Review the links provided in the additional resources (section 4) below to gain a background understanding of password cracking – **Completed**
2. Try to crack the passwords provided in the 'password dump' file below using available tools – **I used Hashcat to do the same . PFB the cracked passwords for the given password dump.**

|  |  |  |  |
| --- | --- | --- | --- |
| Username | Hashcode | Algorithms | Cracked Passwords |
|  |  |  |  |
| experthead | e10adc3949ba59abbe56e057f20f883e | md5 | 123456 |
| interestec | 25f9e794323b453885f5181f1b624d0b | md5 | 123456789 |
| ortspoon | d8578edf8458ce06fbc5bb76a58c5ca4 | md5 | qwerty |
| reallychel | 5f4dcc3b5aa765d61d8327deb882cf99 | md5 | password |
| simmson56 | 96e79218965eb72c92a549dd5a330112 | md5 | 111111 |
| bookma | 25d55ad283aa400af464c76d713c07ad | md5 | 12345678 |
| popularkiya7 | e99a18c428cb38d5f260853678922e03 | md5 | abc123 |
| eatingcake1994 | fcea920f7412b5da7be0cf42b8c93759 | md5 | 1234567 |
| heroanhart | 7c6a180b36896a0a8c02787eeafb0e4c | md5 | password1 |
| edi\_tesla89 | 6c569aabbf7775ef8fc570e228c16b98 | md5 | password! |
| liveltekah | 3f230640b78d7e71ac5514e57935eb69 | md5 | qazxsw |
| blikimore | 917eb5e9d6d6bca820922a0c6f7cc28b | md5 | Pa$$word1 |
| johnwick007 | f6a0cb102c62879d397b12b62c092c06 | md5 | bluered |
| flamesbria2001 | 9b3b269ad0a208090309f091b3aba9db | md5 | Flamesbria2001 |
| oranolio | 16ced47d3fc931483e24933665cded6d | md5 | N/A |
| spuffyffet | 1f5c5683982d7c3814d4d9e6d749b21e | md5 | Spuffyffet12 |
| moodie | 8d763385e0476ae208f21bc63956f748 | md5 | moodie00 |
| nabox | defebde7b6ab6f24d5824682a16c3ae4 | md5 | nAbox!1 |
| bandalls | bdda5f03128bcbdfa78d8934529048cf | md5 | Banda11s |
|  |  |  |  |
|  |  |  |  |

1. Assess the 5 questions in the task instructions below in relation to the passwords provided (type of hashing algorithm, level of protection, possible controls that could be implemented, password policy, changes in policy) - **PFB the answers for all the 5 questions**
2. What type of hashing algorithm was used to protect passwords?

**The hashing algorithm used to protect passwords is MD5.**

1. What level of protection does the mechanism offer for passwords?

**After the analysis, I found that organization is using an outdated password hashing algorithm (MD5) which offers very little protection in the event of a password database leaking. MD5 has been cryptographically broken and considered insecure.**  **It was also determined that the current password policy is not aligned with industry best practices allowing users to have bad passwords.**

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

**As a result of the analysis the following uplifts are proposed to increase the overall level of password protection and to make cracking harder:**

* **Use a dedicated password hashing algorithm bcrypt 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 as 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 because `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.**
* **Organizations should set up a strong password policy like use passphrases etc.**
* **People should be advise to create passwords with a combination of couple of completely random words or use some good combinations of numbers , letters , special characters .**
* **Educate users on the benefits of passwords managers. Having a password manager allows having very long and completely random passwords without the need to remember/write down. A strong passphrase is still required as a master key for to access the password manager.**

1. What can you tell about the organization’s password policy (e.g. password length, key space, etc.)?

**I have below observations about the organization password policy:**

* **Minimum length for password looks to be set to 6.**
* **It does not look like that there are any rules or specific requirement for the password creation. Users can use any combination of word and letters to create a password.**
* **Passwords looks to be very easily guessable .**
* **It looks like many passwords are a string of numbers or letters like “12346” .**
* **Some of the password also contain the username .**

1. What would you change in the password policy to make breaking the passwords harder?

**I would like to recommend below changes in the organization password policy:**

* **Configure a minimum password length.**
* **Enforce password history policy with at least 10 previous passwords remembered.**
* **Set a minimum password age of 3 days.**
* **Enable the setting that requires passwords to meet complexity requirements. This setting can be disabled for passphrases, but it is not recommended.**
* **Reset local admin passwords every 180 days.**
* **Reset service account passwords once a year during maintenance.**
* **For domain admin accounts, use strong passphrases with a minimum of 15 characters.**
* **Track all password changes using a solution .**
* **Create email notifications for password expiration.**
* **Instead of editing the default settings in domain policy, it is recommended to create granular audit policies and link them to specific organizational units.**
* **You could also train your users to follow these policies to maintain the password guidelines.**

1. Draft an email/memo briefly explaining your findings in relation to controls used by the organization and your proposed uplifts. We recommend spending about 1.5 hours on this task and keeping it at 1 page in length – **Please find below the email with the observations on Page 4 . Also PFA the same as a separate embedded document.**



Respected Sir/Ma’am,

As I was doing this exercise for cracking all the leaked hashes, I observed several vulnerabilities in your password policy and this email explains all my findings in relation to controls used by your organization and the proposed uplifts to improve the password policy.

Secure Hash Algorithm (SHA) and Message Digest (MD5) are the standard cryptographic hash functions to provide data security for authentication. It is a major enabling technology for network security used to achieve specific security objectives.

All the listed passwords in the dump are using MD5 which is a weaker hash algorithm and so was very easy to crack using tools like Hashcat.com.

My recommendation is to switch to SHA from MD5 as not only it would provide a very strong password encryption mechanism to create hashes for the password but also SHA is more secure than MD5 due to a variety of reasons. SHA produces a larger digest, 160-bit compared to 128-bit, so a brute force attack would be much more difficult to carry out. And there are no known collisions which have been known or found for SHA.

Below are some of my observations about the organization’s password policy:

* Minimum length for password looks to be set to 6.
* It does not look like that there are any rules or specific requirement for the password creation. Users can use any combination of word and letters to create a password.
* Passwords looks to be very easily guessable .
* It looks like many passwords are a string of numbers or letters like “12346” .
* Some of the password also contain the username .

For your organization , my recommendation for you could be to include several new things in your password policy as below:

* Configure a minimum password length.
* Enforce password history policy with at least 10 previous passwords remembered.
* Set a minimum password age of 3 days.
* Enable the setting that requires passwords to meet complexity requirements. This setting can be disabled for passphrases, but it is not recommended.
* Reset local admin passwords every 180 days.
* Reset service account passwords once a year during maintenance.
* For domain admin accounts, use strong passphrases with a minimum of 15 characters.
* Track all password changes using a solution .
* Create email notifications for password expiration.
* Instead of editing the default settings in domain policy, it is recommended to create granular audit policies and link them to specific organizational units.
* You could also train your users to follow these policies to maintain the password guidelines.

Regards,

Shivani Aggarwal

MS in Software Engineering

AI developer & Project Leader at DXC.Technology