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