Dear Sir/Ma'am,

After cracking all the leaked hashes, I came to know that there is a lot of vulnerabilities in your password policy and I have summarized the result and recommendations of my analysis of the leaked hashes that I tried to break.

Secure Hash Algorithm (SHA) and Message Digest (MD5) are the common hash functions that ensure data security for authentication. All the compromised passwords used MD5 for hashing, which is a weak hash algorithm and can be easily cracked.

I used hashes.com to decrypt all the leaked hashes. Using Hashcat, these hashes can be easily cracked. That's why I would suggest to use a strong password encryption mechanism to create hashes for the password like:

1. **SHA-256**: This hash function returns a 256-bit value, which is more secure than MD's 128-bit value. It is slower than MD5, but it is more resistant to brute-force attacks and collisions.
2. **SHA-3**: This hashing function also return 256-bit value. It is slower than SHA-256 but it is more efficient for longer inputs. In terms of security, SHA-3 is more secure.
3. **Bcrypt**: This password hashing function uses a salt and a variable number of iterations to make cracking harder.

After cracking the passwords, I came to know that these are the password policy of the organization:

1. Minimum length for the password is set to 6.
2. There're no specific rules for creating password. User can use any combination of words or letter to create a password.

So, here are some of my suggestions to consider while making revising the password policy,

1. **Minimum length** of the password should be 8.
2. Password should include the combination of **Capital and small letters, numbers, special characters.**
3. Password shouldn't include any combinations of **username, actual name, data of birth.**
4. Implement **Password-strength checking bar** in login and sign-Up page near password entering field.
5. Password shouldn't contain the repetitive characters like 111111, aaaaa, @@@@ etc.

Below are the 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***

oranolio: 16ced47d3fc931483e24933665cded6d ***Oranolio1994***

spuffyffet: 1f5c5683982d7c3814d4d9e6d749b21e ***Spuffyffet12***

moodie: 8d763385e0476ae208f21bc63956f748 ***moodie00***

nabox: defebde7b6ab6f24d5824682a16c3ae4 ***nAbox!1***

bandalls: bdda5f03128bcbdfa78d8934529048cf ***Banda11s***