

Dear Sir/Ma'am

I have completed the password cracking task and have stated my findings below:

Findings:

Using a hash identifier, I found out that the hashing algorithm used to protect all the passwords was an MD5 cryptographic hash function. This has many weaknesses such as collision attacks which allow attackers to create different inputs that produce the same hash value.

To crack the passwords, I used Hashcat in combination with the rockyou.txt text wordlist which contains some of the most commonly used passwords. Through this process, I successfully identified the following passwords.

Observations on the Organisation's Password Policy:

- Minimum password length: 6 characters
- Space character: Not allowed
- Average password length: Approximately 7 characters, which significantly increases the security risk
- Additional requirements: There are no enforced rules for capital letters, numbers, or special characters, allowing users to create simple, easily guessed passwords.

Recommendations for Improving the Password Policy:

- Require a combination of numbers, uppercase and lowercase letters, and special characters.
- Increase the minimum password length to at least 8 characters.
- Enforce complexity requirements to avoid predictable passwords such as "password" or "123456".
- Prohibit the use of personal information (e.g., name, username, date of birth) in passwords.
- Encourage unique passwords for different accounts to prevent reuse across multiple platforms.

Implementing these changes should make sure that the organisations overall security would be improved and reduce the likelihood of password cracking from taking place

Kind Regards,

Neel Patkar

Hash Type:

Username	Hash	Algorithm
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
Liveltakah	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:

Username	Hash	Password
Experthead	e10adc3949ba59abbe56e057f20f883e	123456
Interestec	25f9e794323b453885f5181f1b624d0b	123456789
Ortspoon	d8578edf8458ce06fbc5bb76a58c5ca4	qwerty

Username	Hash	Password
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