Crack leaked password database

The Goldman Sachs Engineering Virtual Program

The passwords were protected by the MD5 hashing algorithm. This provides very poor level of protection as multiple tools such as hashcat and free-to-use web apps can be used to crack the hashes. I used hashcat along with [CrackStation’s Human only dictionary](https://crackstation.net/crackstation-wordlist-password-cracking-dictionary.htm) and [MD5 Online](https://www.md5online.org/md5-list-decrypter.html) to crack these.

Multiple controls such as reassigning randomly generated passwords to users and updating the hashed records can be executed to prevent damage in an event of a password leak.

The organisation’s average password length is almost eight characters but has multiple passwords shorter than eight which pose a high security risk. Their key space is smaller than modern standards i.e. SHA-256, SHA-128, etc.

|  |  |  |
| --- | --- | --- |
| username | md5\_hash | password |
| bandalls | bdda5f03128bcbdfa78d8934529048cf | Banda11s |
| blikimore | 917eb5e9d6d6bca820922a0c6f7cc28b | Pa$$word1 |
| bookma | 25d55ad283aa400af464c76d713c07ad | 12345678 |
| eatingcake1994 | fcea920f7412b5da7be0cf42b8c93759 | 1234567 |
| edi\_tesla89 | 6c569aabbf7775ef8fc570e228c16b98 | password! |
| experthead | e10adc3949ba59abbe56e057f20f883e | 123456 |
| flamesbria2001 | 9b3b269ad0a208090309f091b3aba9db | Flamesbria2001 |
| heroanhart | 7c6a180b36896a0a8c02787eeafb0e4c | password1 |
| interestec | 25f9e794323b453885f5181f1b624d0b | 123456789 |
| johnwick007 | f6a0cb102c62879d397b12b62c092c06 | bluered |
| liveltekah | 3f230640b78d7e71ac5514e57935eb69 | qazxsw |
| moodie | 8d763385e0476ae208f21bc63956f748 | moodie00 |
| ortspoon | d8578edf8458ce06fbc5bb76a58c5ca4 | qwerty |
| popularkiya7 | e99a18c428cb38d5f260853678922e03 | abc123 |
| reallychel | 5f4dcc3b5aa765d61d8327deb882cf99 | password |
| simmson56 | 96e79218965eb72c92a549dd5a330112 | 111111 |
| spuffyffet | 1f5c5683982d7c3814d4d9e6d749b21e | Spuffyffet12 |
| nabox | defebde7b6ab6f24d5824682a16c3ae4 | no result |
| oranolio | 16ced47d3fc931483e24933665cded6d | no result |

They should implement a minimum password length of eight characters along with a requirement of atleast one uppercase, numeric and special character. Upgrading the hashing algorithm to a better one such as SHA-256 or AES-256 is also necessary to make decrypting harder and near impossible.