I used hashcat on KaliLinux to crack the passwords. Was successful in cracking 13 out of the 19 hash values given.

The hashing algorithm used was MD5. By trial and error when applying MDS as the hashing algorithm parameter I was able to crack the passwords.

The current mechanism offers a relatively low level of protection for the passwords. It does hash the passwords making the hackers job a little more tedious but also MD5 hash algorithm is a known cryptographically weak algorithm, with collisions reported and has numerous vulnerabilities. More robust algorithms like SHA-256 should be utilised as it is much more difficult to compute.

The next time a password database file leaks it should be encrypted so that the hashvalues itself should not be known to the attacker. Furthermore we can add salt values(random values) to the plaintext password and then hash them further complicating the hash value and this will also create completely different hash values even if the password is the same, which is a huge advantage and will make the attackers job that much more cumbersome. The salt values however have to be random and unique everytime, as otherwise it defeats the purpose and attackets can simply append a common list of salt values to the passwords and compute the hash values.

The passwords used in this list are very short and easy and was cracked in barely 10 seconds. It is important that passwords be 8-16 charecters long and should be alpha-numeric and consists of Uppercase and lowercase letters and special charcters as well. This password policy should be enforced in all companies and organisations. This will simple rule will make our password extremely strong and take a hacker thousands of years to crack our passwords.