Date - 09/05/2022

Subject: Cracking Leaked Passwords

The results and findings to the assignment.I have found out these passwords

```
e10adc3949ba59abbe56e057f20f883e md5 123456
25f9e794323b453885f5181f1b624d0b md5 123456789
D8578edf8458ce06fbc5bb76a58c5ca4 md5 qwerty
5f4dcc3b5aa765d61d8327deb882cf99 md5 password
96e79218965eb72c92a549dd5a330112 md5 111111
25d55ad283aa400af464c76d713c07ad md5 12345678
E99a18c428cb38d5f260853678922e03 md5 abc123
Fcea920f7412b5da7be0cf42b8c93759 md5 1234567
```

Hashing Algorithm used: MD5

- Message Direct Algorithm is a bad password hashing algorithm because it is too fast and memory conserving.Attacker can compute hash of large number of passwords per second.

Recommendations to Implement Password:

- Try using better Algorithm in place of MD5 Eg:SH256
- Always use salts with hashes.
- For better Security use bcrypt.Which make harder for attacker because it requires more CPU to get access.

Observations on Organisation Password Policy:

- Weak hash functions used with no salting.
- Common passwords are used which is easy to crack
- No usage of any Capital letters , symbols and numbers as a whole.

Changes to be made in Organisation Password Policy:

- Increase the input character length to 12, or else attacker can easily brute force.
- Using of mix of characters rather than simple text(simple text).
- By maintaining the strength like weak, strong ,very strong to help users understand.

Thank you

Tejroop.B