# **FORAGE –GOLDMAN SACHS –TAHA QURESHI**

## TASK 1 :

What hashing algorithm was used in the Password Dump ?

Answer : MD5 – Plain : Hashing

TASK 2 :

Level of protection of that hashing used above?

Answer : MD5 is the most suffered cryptographic hash function technique to suffer the most of vulnerabilities. On 31 December 2008, the [CMU Software Engineering Institute](https://en.wikipedia.org/wiki/CMU_Software_Engineering_Institute) concluded that MD5 was essentially "cryptographically broken and unsuitable for further use"

TASK3:

How to make password cracking more complex?

Answer: “Easy to remember is not hard to guess”

Make a combination of uppercase, lowercase, numbers, special characters , and yes don’t use birthdates ,names ,etc.

Salting can also improve the security of a password. Hashing allows for later authentication without keeping and therefore risking exposure of the plaintext password if the authentication data store is compromised.

Salt is generated randomly for each password. Salts defend against attacks that use precomputed tables (e.g. rainbow tables) as they can make the size of table needed for a successful attack prohibitively large without burdening users

TASK4 : Password Tips to avoid being cracked !

* Never use phone numbers, addresses, birthdays, your SSN, your name, family members’ names, or pets’ names in your password.
* Select a combination of uppercase and lowercase letters, numbers, and symbols for your passwords.
* Never use common passwords like “123456,” “password,” or “qwerty.”
* Make sure your passwords are at least eight characters long. Passwords with more characters and symbols are more difficult to guess.
* Don’t use common words or phrases in your passwords. If you want to use them, alter the word or abbreviate the phrase. For example, if you want to use the word “eleven” you can convert it to “e13v3N.” Or if you want to use the phrase “I love to shop” you can change it to “1luv2sh0p.” Make it even stronger by adding symbols and punctuation: “#1Luv2sh0p!”

Attached photo of passwords cracked in Kali using HASHCAT:

A screenshot of a computer

Description automatically generated with medium confidence

PASSWORDS ARE:

e10adc3949ba59abbe56e057f20f883e:123456

25f9e794323b453885f5181f1b624d0b:123456789

5f4dcc3b5aa765d61d8327deb882cf99:password

fcea920f7412b5da7be0cf42b8c93759:1234567

25d55ad283aa400af464c76d713c07ad:12345678

e99a18c428cb38d5f260853678922e03:abc123

d8578edf8458ce06fbc5bb76a58c5ca4:qwerty

96e79218965eb72c92a549dd5a330112:111111

7c6a180b36896a0a8c02787eeafb0e4c:password1

6c569aabbf7775ef8fc570e228c16b98:password!

3f230640b78d7e71ac5514e57935eb69:qazxsw

f6a0cb102c62879d397b12b62c092c06:bluered

917eb5e9d6d6bca820922a0c6f7cc28b:Pa$$word1

BY TAHA QURESHI