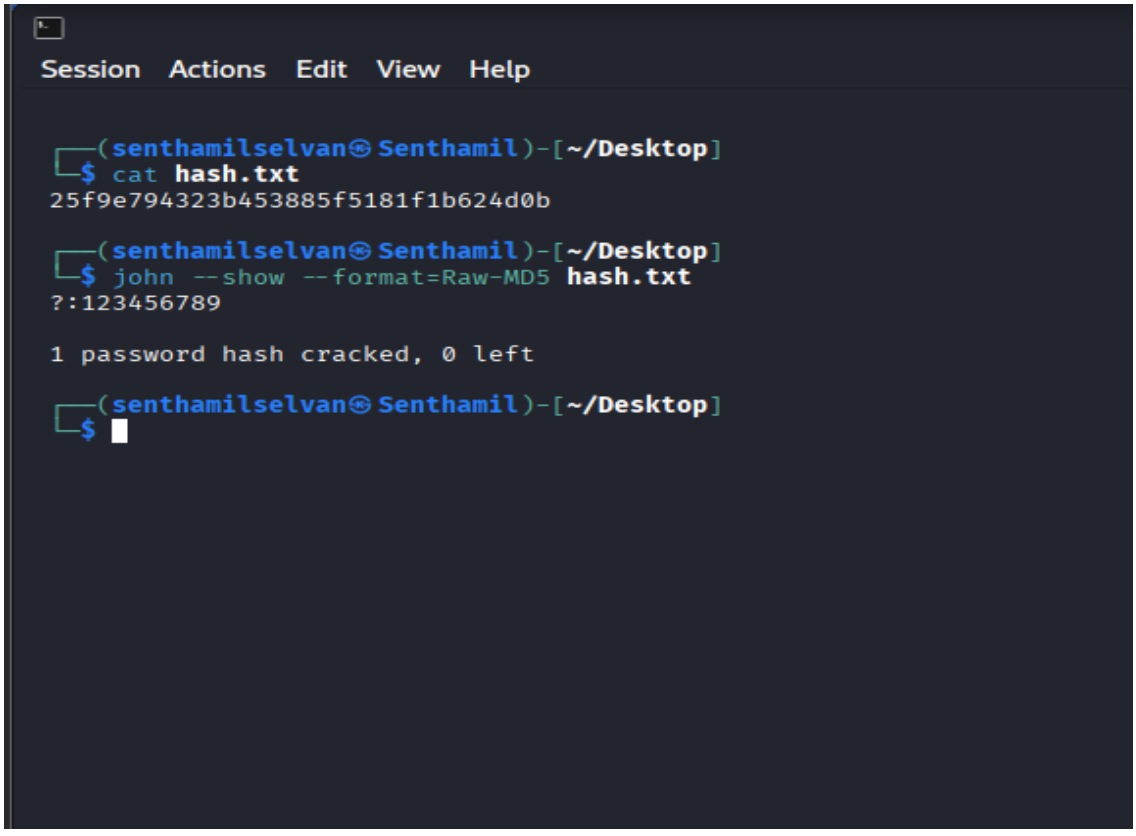
Password Security & Authentication Analysis

Hashing – Converts text into some random text. It can't be reversed into same text.
Encryption – Converts text into some random text. But it can be decrypt to same text.

Hashing has lot types like MD5, SHA-1, bcrypt.
MD5: it is a 128-bit hash. It can be easily brute forceable.
SHA-1: it is a 160-bit hash. It vulnerable for collision attacks.
bcrypt: it generates hashes slower then MD5, SHA-1. But it is more secure then MD5, SHA-1.

Password Cracking:
I generated MD5 hash for 123456789 and I used john the ripper tool for crack it.



Hash value for 123456789 in MD5- 25f9e794323b453885f5181f1b624d0b.

MFA (Multi Factor Authentication):

Multi factor authentication product our data securely. It adds extra layer on our password security. It useful when our password is cracked by attacker. Using fingerprint with pin as password is far more than using pin only as password. Using MFA can reduce the vulnerability of password cracking.

Brute Force Attack:

Tring every possible combination of characters until the correct password is found. It useful when the password rules are known like length of the password. Sometimes it takes lot of time for find the password.

Dictionary Attack:

Using a predefined list of sample common password for match the hashes. It won't take lot of time like Brute Force Attack. But, sometimes it can be fail when the password is unique or uncommon.

Weak Password:

Weak passwords like 123456789, aabbcc, are usually stored in many wordlists. Even normal human being without proper knowledge about the victim can also break this password. So weak passwords are like a human locked his home's all door but slightly opened a backdoor for the attacker.

Recommendation for strong authentication:

- Pin + Fingerprint
- Password + Eye Rays
- Pattern + Face

  I recommend to use unusual or unique password and pins. Change the password regularly as a routine. If it is not possible to change password frequently then atleast change it for 6 months once. I think this thing gives more security than usual passwords.