Task - 6

Password Creation and Strength Evaluation

1. Let us create multiple passwords with varying complexities:
    - pass
    - pass123
    - Password0
    - PASS-word
    - PaSsWoRd_66
    - You2CAntfInd_THisONe38

2. The above passwords are arranged in order of increasing complexities and also they differ in terms of Lowercase, Uppercase, Numbers, Symbols and Length Variations.

3. Lets open the passwordmeter.com to check these created passwords

4. Scores and Feedback:
    - pass - 3 / Very Weak
    - pass123 - 35 / Weak
    - Password0 - 54 / Good
    - PASS-word - 58 / Good
    - PaSsWoRd_66 - 86 / Very Strong
    - You2CAntfInd_THisONe38 - 100 / Very Strong

5. The Best practices for creating passwords are:
    - It should be minimum 8 characters in length
    - It should contain mix of both Uppercase Letters and Lowercase Letters
    - It should contain Numbers in it
    - It also should have special characters to make it more secure

6. From these evaluations i have learned that,
    - we should use passwords of length atleast 8 characters
    - We should use more Special characters and also that should not be used more commonly
    - We should not use consecutive numbers and also we should not use consecutive lowercase and uppercase letters
    - There should also not be repetitive characters

7. Common Password attacks are:
    - Brute Force: If we use password of smaller lengths, it is easy to brute force them and crack it, for example if we use only numbers in passwords and it is of only length 4 characters then, we can break it in 9999 tries and modern computers

can break them in seconds. So we need to use mix of characters, numbers and special characters also the length should be more than 8 characters.

- Dictionary attacks: In this type of attacks, the attacker guesses the password and tries some predefined passwords which are used commonly by people. As people tend to use easier passwords for their convenience and easy remembrance, attacker uses some predefined commonly used passwords to break them. Some examples are name of the user, their birthdays, birth years, their lucky numbers and family names.
- Phishing: Attackers make users to enter their passwords themselves by pretending to be a legitimate entities or deceptive websites.
- Keylogging: A malware installed on user's system will record every keystroke made by the user, which also records their password and sends them to attackers.

8. So password complexity is important for security, as more complex your password is more secure it is else it will be easily cracked.