Topic: Password Strength Validator Application

Information systems that are not protected with strong passwords provide the opportunity for a password-crack and unwanted access of the system.

1. Team will define the attributes of a password's "strength level" based on factors such as length, complexity, inclusion of special characters, mixed case, etc. There must be at least 3 levels.
2. Team will assess the strength of the user-supplied password based on the strength level requirements.
3. If the supplied password is not strong, provide feedback to the user that includes:
    a. Strength level of the supplied password.
    b. Why it fails to meet the strong password requirements.
    c. An estimate of how long it would take to crack their supplied password.
4. Offer suggestions for a strong password by creating a password generator capability.

Stretch goal:

1. Store username/passwords in a database.
2. After three unsuccessful attempts at login, deny further access to that user.