Statement.md

Problem Statement:

Users commonly create weak or predictable passwords, making their accounts vulnerable to brute-force attacks, dictionary attacks, phishing, and social-engineering attempts. There is a need for an intelligent tool that can analyze password strength and provide actionable feedback to help users create secure passwords.

Scope of the Project:

This project focuses on developing a Python-based password strength checker that:

Calculates password entropy

Detects sequential, repeated, and keyboard patterns

Identifies common and weak passwords

Checks for personal information usage (username, email, name)

Scores the password and categorizes it as Weak/Moderate/Strong

Estimates expected crack time

Generates warnings and improvement suggestions

Not included in scope:

Password storage

Integration with external systems

Encryption or hashing mechanisms

Cloud or database usage

Target Users:

General users who want to test password strength

Students learning cybersecurity concepts

Developers who need a backend password-evaluation module

Organizations promoting stronger password habits

Educators teaching entropy and password model

High-Level Features:

✓ Password entropy calculation

✓ Sequential, repeated & keyboard-pattern detection

✓ Common password identification

✓ Personal information matching

✓ Strength score (0–100)

✓ Category output: Very Weak, Weak, Moderate, Strong, Very Strong

✓ Estimated crack time

✓ Warnings and improvement suggestions

✓ Clean, user-friendly terminal interface
