Title: Password Strength Analyzer with Custom Wordlist Generator

Name: Rajnish Yadav

Internship Phase: Cyber Security Project

Date: June 25, 2025

Introduction:

In today's digital environment, strong password practices are crucial for protecting sensitive data. This project demonstrates a password strength analyzer and custom wordlist generator that simulates how hackers may use personal information to create targeted attack lists.

Abstract:

This Python-based tool allows users to:

- Analyze the strength of any password using the zxcvbn library.

- Generate a wordlist from personal details (e.g., name, birth year, pet name) that mimics common brute-force attack dictionaries.

The project emphasizes user awareness and security hygiene regarding password creation.

Tools Used:

- Python 3.13

- zxcvbn library (for password strength estimation)

- argparse (for CLI support)

- Text editor (VS Code)

- macOS terminal

Steps Involved:

1. Input Handling: Takes user password or personal information through command-line arguments.

2. Password Strength Analysis: Uses zxcvbn to assess password complexity and crack time.

3. Wordlist Generation: Based on inputs like name or birth year, it creates combinations with reversals, suffixes, and transformations.

4. Output: Prints analysis results and saves the wordlist in .txt format for educational use.

Sample CLI Usage:

$ python3 password_analyzer.py --password "MyP@ssw0rd123"

$ python3 password_analyzer.py --info Rajnish dog 2002

Conclusion:

This project demonstrates how seemingly strong passwords may still be guessable if they follow common patterns. It educates users to avoid personal data in passwords and highlights real-world brute-force methods. The custom wordlist tool gives insight into attacker strategies.

Deliverables:

- Python Script
- Wordlist output file
- PDF Report (this document)