Project Report

Project Title: Password Strength Analyzer with Custom Wordlist Generator

Name: Shreya Deshmukh

Platform: Windows

Technology Used: Python, Tkinter GUI, zxcvbn

1. Introduction

In the digital age, weak passwords remain one of the most common vulnerabilities exploited by attackers. This project aims to help users understand the importance of strong passwords and how personal information can be used to generate attack wordlists. The tool offers two functionalities: analyzing password strength and generating custom wordlists from personal inputs.

2. Abstract

The project consists of two main features:

- A Password Strength Analyzer that uses the zxcvbn library to score passwords and estimate how long they would take to crack.

- A Custom Wordlist Generator that accepts personal keywords (like name, pet, or birthdate), applies common transformations (like leetspeak and appending years), and outputs a list of possible passwords into a `.txt` file.

Both features are integrated into a user-friendly graphical interface built using Tkinter.

3. Tools Used

- Python 3.x

- zxcvbn (password strength estimator)

- Tkinter (GUI development)

- itertools (for leetspeak combinations)

- Notepad/VS Code (for reviewing generated wordlists)

4. Steps Involved in Building the Project

1. Set up the environment by installing Python and required libraries (`zxcvbn`).

2. Created a function to analyze password strength and provide feedback using `zxcvbn`.

3. Designed a leetspeak transformation function using `itertools.product()`.

4. Built a GUI using Tkinter to accept password input and personal information.

5. Developed the logic to generate a customized wordlist by combining inputs with leetspeak and common years.

6. Exported the final wordlist to `custom_wordlist.txt`.

7. Tested the tool with different password inputs and verified the accuracy of the generated wordlist.

5. Conclusion

The tool successfully helps users understand the strength of their passwords and demonstrates how personalized information can be leveraged to simulate password attacks. The generated wordlist reflects real-world attack methods, and the intuitive GUI ensures accessibility for non-technical users. This project has educational value for both cybersecurity awareness and practical password safety.