Project Report

1. Introduction

The project 'Password Strength Analyzer with Custom Wordlist Generator' is aimed at helping users evaluate the strength of their passwords and generate personalized wordlists based on their details for educational and ethical hacking purposes.

2. Abstract

This tool integrates a GUI-based password strength analyzer using the zxcvbn library and a custom wordlist generator that accepts personal inputs like name, birth year, pet name, etc. The tool then produces possible password combinations using leetspeak and pattern rules. It helps in understanding weak passwords and how they can be guessed.

3. Tools Used

- Python 3.8+
- Tkinter (for GUI)
- zxcvbn (password strength estimator)
- itertools (for pattern generation)
- fpdf (to generate this PDF)

4. Steps Involved in Building the Project

1. Set up a Python environment and install dependencies from requirements.txt
2. Create separate modules: `analyzer.py`, `wordlist.py`, `utils.py`, and `gui.py`
3. Build the GUI with password input, analysis button, and wordlist generator
4. Connect analysis results with zxcvbn output
5. Implement the logic for custom wordlist generation using patterns and leetspeak
6. Add options to save analysis results and wordlists to .txt files

5. Conclusion

The project demonstrates how password security can be evaluated and personalized dictionaries can be

created for testing password robustness. It serves as an educational tool for beginners in ethical hacking, penetration testing, and cybersecurity awareness.