Password Strength Analyzer & Wordlist Generator

Project Report

1. Introduction

Weak passwords are a leading cause of security breaches. This project develops a Python tool to:

✅ **Analyze password strength using the zxcvbn algorithm.**

✅ **Generate custom wordlists for security testing.**

Built for Windows with CLI/GUI options.

2. Tools Used

Component	Purpose
Python 3.x	Core programming language
zxcvbn	Password strength estimation
argparse / tkinter	CLI and GUI interfaces
PyInstaller	Compile to .exe (optional)

3. Implementation Steps

A. Password Analysis

Python:

```
from zxcvbn import zxcvbn

result = zxcvbn("P@ssw0rd123")

print(f"Score: {result['score']}/4   Crack Time:
{result['crack_times_display']['online_no_throttling_10_per_second']}")
```

B. Wordlist Generation

Python:

```
def generate_wordlist(names, years):

    return [name + str(year) for name in names for year in years]
```

C. CLI/GUI Integration

CLI :

bash

python analyzer.py analyze "Password123" generate "alice,bob" years "2020,2023"

GUI (optional):

python

```
import tkinter as tk
tk.Button(root, text="Analyze", command=analyze).pack()
```

D. Compilation

bash

pyinstaller onefile analyzer.py Creates standalone .exe

4. Conclusion

This tool provides:

- **Instant password feedback (strength/crack time).**
- **Custom wordlists for security audits.**
- **Flexibility (CLI for pros, GUI for beginners).**

Future Work : Add breach checking APIs and leetspeak patterns.

Appendix :

Sample Output :

Password: "hello2023"

Strength: 2/4 Crack Time: 1 hour

Warning: Predictable substitutions (e.g., 'o' → '0').