Cybersecurity Internship Project: Development of a Password Complexity Analysis & Targeted Wordlist Tool

1. Introduction:

This project addresses the critical need for robust credential security in an era of increasing automated cyberattacks. It focuses on evaluating password complexity and understanding how targeted wordlists are created for penetration testing.

2. Abstract:

The "Password Strength Analyzer with Custom Wordlist Generator" is a Python-based security tool. It utilizes entropy-based analysis to provide realistic crack-time estimates and generates targeted wordlists by applying common patterns—such as leetspeak and suffixes—to user-provided data. This demonstrates how personal information can be leveraged in brute-force attacks.

3. Tools Used:

- **Python:** The primary programming language.
- **zxcvbn library:** Used for complex entropy calculations and realistic password strength scoring.
- **Argparse/Standard Library:** Used for creating a command-line interface and managing user input.
- **OS/File System**: For exporting wordlists in .txt format.

4. Steps Involved in Building the Project:

- **Library Integration:** Integrated the zxcvbn library to analyze user passwords for strength.
- **Input Collection**: Developed a system to allow user inputs such as names, dates, or pets.
- **Pattern Implementation**: Programmed logic to include common patterns like leetspeak and year-based suffixes.
- **Data Export**: Built a function to export the generated variations into a .txt format compatible with cracking tools.
- **Interface Development**: Created a CLI or simple GUI (using tkinter) to manage the tool.

5. Conclusion:

The project successfully meets the objective of building a tool that evaluates password strength and exports attack-specific wordlists. It provides actionable feedback to users, highlighting the vulnerability of simple passwords against targeted dictionary attacks.