**Advanced Password Tool – Project Report**

**Abstract**

This report presents the Advanced Password Tool, a desktop application built in Python to enhance user password security. The tool integrates entropy-based strength metrics, pattern evaluation via zxcvbn, and breach detection through the Have I Been Pwned API. It also features strongpassword generation using cryptographically secure methods, and a highly configurable wordlist builder, supporting leetspeak, casing, symbols, and year-suffix variants. A Tkinter GUI offers an intuitive multi-tab interface, theme toggling, clipboard copying, and export functionality. Packaged via PyInstaller, it delivers a single‑file executable for easy distribution. A suite of pytest unit tests ensures reliability.

### ****Introduction****

Weak or reused passwords continue to pose a major risk—studies indicate low entropy and patterns are easily guessable. The Advanced Password Tool was built to address this gap: offering both novice and security-savvy users a unified interface to assess password robustness, generate secure passwords, and build tailored wordlists for testing or educational purposes. The modular design ensures extensibility, while GUI-based interactions make security accessible without overwhelming users.

Tools Used

|  |  |
| --- | --- |
| Tool/Library | **Purpose** |
| Python 3.8+ | Core development language |
| Tkinter with ttk | GUI framework with tabbed layout and theme support |
| zxcvbn‑python | Detects intuitive patterns in passwords |
| secrets, random | Secure password and wordlist generation |
| pytest | Unit testing modules and edge case validation |
| PyInstaller | Bundle as standalone executable |

Steps Involved

1. Requirement gathering and modular design

2. Implemented core modules: analyzer (entropy + breach), generator (secure passwords), wordlist builder (transforms with combinatorial limits)

3. Built Tkinter GUI with tabbed interface and theme toggling

4. Added CLI script (cli.py) and used PyInstaller for creating a single-file executable

5. Wrote unit tests to ensure reliability

Conclusion

The Advanced Password Tool delivers functional and secure utility for password strength evaluation, generation, and tailored wordlists. Its GUI and executable packaging enhance accessibility, while future enhancements could include vault features, mnemonic generation, or CLI expansions