# Cybersecurity Internship Project Report

## 1. Introduction

This report summarizes two cybersecurity tools developed during a two-week internship program. The objective of this internship was to gain hands-on experience with cybersecurity techniques and concepts, including password security, social engineering, file encryption, metadata handling, and file integrity verification. Both tools were developed using Python and are structured to simulate real-world security applications. The projects were executed individually and documented with clear modular design, functionality, and output validation.

## 2. Project 1: Password Strength Analyzer & Wordlist Generator

This project implements a GUI-based password analysis and wordlist generation tool using Python and the Tkinter framework. The goal of the project is to allow users to evaluate the strength of passwords using Dropbox’s zxcvbn algorithm and to create realistic wordlists for use in password cracking or auditing tasks.

### 2.1 Features

- Password strength analysis using zxcvbn

- Real-time feedback including crack time and password score

- Suggestions and warnings for improving passwords

- Wordlist generation from user inputs: name, DOB, pet name

- Leetspeak transformation (e.g., a -> @, e -> 3, s -> $)

- Appending common suffixes (e.g., 123, @123, 2025, etc.)

- Export of the generated wordlist to a .txt file

- Clean user interface with tabbed navigation

### 2.2 Technologies Used

- Python 3

- Tkinter for GUI

- zxcvbn for password strength estimation

- itertools for generating word combinations

## 3. Project 2: Secure File Storage System with AES Encryption

This project focuses on secure file encryption, metadata storage, and integrity verification. It allows a user to encrypt any file using a symmetric key and verify its authenticity during decryption. It was implemented in both command-line and GUI versions.

### 3.1 Features

- AES encryption using the Fernet module from the cryptography library

- Key generation and secure key storage

- File encryption and creation of .enc files

- Generation of metadata including SHA-256 file hash, timestamp, and filename

- Decryption of .enc files and verification of file integrity using hash matching

- GUI version developed using Tkinter

### 3.2 Technologies Used

- Python 3

- cryptography (Fernet) for AES encryption

- hashlib for SHA-256 hashing

- Tkinter for GUI

## 4. Conclusion

The internship project provided a strong practical foundation in cybersecurity. Through the development of two distinct but complementary tools, the intern learned how to apply password entropy analysis, simulate social engineering for wordlists, and implement strong encryption practices. The use of metadata and file integrity checks enhanced understanding of secure data handling. These tools represent key concepts and are a valuable part of the learning journey in cybersecurity.