Rohan Das - 23MCAN0218

Project Title

Forensics Credential Harvester

Objective

The objective of the Forensics Credential Harvester is to develop a cross-platform tool for digital forensics professionals to extract and recover browser credentials from popular web browsers (Chrome, Firefox, Safari, Brave, and Internet Explorer). This tool aims to assist in investigations by providing a means to access stored credentials from suspects' computers and laptops in a secure and efficient manner.

Key Components

1. **Browser Credential Extraction:**
    - Mechanisms for accessing and extracting stored credentials from each supported browser.
    - Support for both encrypted and plaintext credentials.
2. **Decryption Algorithms:**
    - Implementation of algorithms to decrypt stored credentials based on the encryption methods used by each browser and operating system.
3. **Cross-Platform Compatibility:**
    - Functionality across Linux, Windows, and macOS environments to ensure broad usability in forensic investigations.
4. **Reporting Module:**
    - Generation of comprehensive reports detailing the extracted credentials, including browser type, username, and other relevant metadata.
5. **User Interface:**
    - A command-line interface (CLI) for user interaction, allowing users to specify targets and view results.

Tools & Technologies

- **Programming Language:** Python
- **Libraries:**
    - `sqlite3` for database access (Chrome, Brave, Firefox)
    - `pywin32` for Windows API interaction (DPAPI)
    - `cryptography` for handling encryption/decryption
    - `secretstorage` or `keyring` to access credentials stored in GNOME Keyring/KWallet.
    - `keyring` library or native system calls (e.g., `subprocess` with `security` command) to access Safari and Chrome passwords stored in the macOS Keychain.
- **Development Environment:** Visual Studio Code, PyCharm, or any preferred IDE
- **Version Control:** Git for source code management

Number of Lines (Code)

The estimated number of lines of code for the initial version of the Forensics Credential Harvester is expected to be approximately **500–800 lines**, depending on the complexity of the decryption logic and the number of features implemented. This estimate includes code for credential extraction, decryption, reporting, and the user interface.