These writeups, authored by Peyton Braun, are designed to guide you through the process of solving all the challenges from the Inaugural University of Wisconsin – Stout Cybersecurity Capture the Flag (CTF) event.

This event was hosted by UW-Stout CyROC x CCDL

I hope these writeups help you gain a deeper understanding of each challenge and how to overcome them.

CTF Challenge Writeups

Each writeup will cover the following aspects of the challenge:

1. **Challenge Overview**: A brief description of the challenge.

2. **Steps to Solve**: Detailed steps, tools used, and reasoning behind each step.

3. **Tools and Methods**: Explanation of why specific tools and methods were chosen.

4. **How It Works**: Insight into the underlying concepts and the thinking process.

Challenge: "Iera Milpan"

Challenge Overview:

The challenge provides a file named Retak_Haiku_-_Iera_Milpan.mp3, which is deceptively labeled. The objective is to determine the actual file type and uncover the flag hidden within it.

Challenge Description:

- Waktu bahagia berkasih Muncul sesuatu tak ku duga Lilin selama ini bernyala Terpadam gelap gelita Sukarnya untuk melupakan Ikatan janji setia Di bawah pohon asmara Kau lafazkan Mentera cinta Retak hatiku hancur semua Diriku ini jiwa meronta Cinta yang sudah pudar Tenggelam di lautan kecewa Walau hati akan kekosongan Namun cintaku bukan mainan Biarlah aku bersendirian Untuk melupakanmu Biarkanlah aku Membawa diriku Semoga bahagia Walau ku berduka Walau patah tumbuh Hilangkan berganti Namun luka ini Sukar diubati Retak hatiku hancur semua Diriku ini jiwa meronta Cinta yang sudah pudar Tenggelam di lautan kecewa Walau hati akan kekosongan Namun cintaku bukan mainan Biarlah aku bersendirian Untuk melupakanmu oh Biarkanlah aku Membawa diriku Semoga bahagia Walau ku berduka Walau patah tumbuh Hilangkan berganti Namun luka ini Sukar diubati Biarkanlah dia Membawa dirinya Semoga bahagia Walau kau berduka Walau patah tumbuh Hilangkan berganti Namun luka ini Sukar diubati

Steps to Solve:

1. **Identify the File Type**:

    1. Use the file command in Kali Linux to inspect the provided file:

    2. file Retak_Haiku_-_Iera_Milpan.mp3

1. This command reveals that the file is not an MP3 but a PNG image.

2. **Rename the File**:

   1. Change the file extension to .png so it can be opened as an image:

      1. mv Retak_Haiku_-_Iera_Milpan.mp3 Retak_Haiku_-_Iera_Milpan.png

3. **Open the File**:

   1. View the image using an image viewer (e.g., eog on Linux or any other image viewer) to find the flag displayed on it.

4. **Decoded Flag:**
   1. STOUTCTF{qDtiRAwpAyR4Yg57YxzYW5p1V2dm5mwo}

Tools and Methods:

- **Command Used**: The file command identifies the actual file type by examining the file header instead of relying on the extension.

- **Methodology**: Renaming the file and using an image viewer allows for easy flag retrieval without additional tools.

How It Works:

The file header in binary data defines its actual type, regardless of the extension. The challenge tests understanding of file headers and the ability to look beyond surface-level attributes. Renaming the file enables the system to handle it correctly as a PNG image.