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: "NormalImage"

Challenge Overview:

Extract an image from a zip file and uncover the hidden flag using steganography.

Steps to Solve:

1. Extract the image from the provided zip file.
2. Use a steganography analysis tool, such as Aperisolve, to analyze the image for hidden data.
    - Upload the image to Aperisolve and review the results.
3. Retrieved flag:
    - STOUTCTF{1ywHGox1ZRNcAftHt1CWP9YT1PKT1inR}.

Tools and Methods:

- **Aperisolve**: Online platform that automates steganographic analysis.
- **zsteg**: Alternative command-line tool for steganography analysis.

How It Works:

Steganography hides information within digital files. Tools like Aperisolve and zsteg scan images for embedded data and reveal hidden content.