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: "13RottenTeRmites"

Challenge Overview:

Decode a file using base64, then apply ROT13, and search for the flag.

Steps to Solve:

1. Decode the base64 string in the file:
    1. cat 13RottenTeRmites.txt | base64 -d > decoded.txt
2. Translate the decoded text using ROT13:
    1. cat decoded.txt | tr 'A-Za-z' 'N-ZA-Mn-za-m' > translated.txt
3. Search for the flag in the translated file using Ctrl + F.
4. Retrieved flag:
    1. STOUTCTF{qKp1MOJMDaJUIJ5KybLrcfZOFQ3IN1j2}.

Tools and Methods:

- **Base64 Decoder**: Built-in Linux command to decode base64.
- **tr Command**: Efficient for applying character substitution like ROT13.

How It Works:

Base64 decoding converts the encoded data to its original format. The ROT13 cipher shifts letters by 13 places in the alphabet, effectively decrypting the text when applied again.