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: "The Echos"

Challenge Overview:

This challenge involves analyzing a PCAP file containing thousands of packets. The flag is hidden in a pattern of packets filled with repetitive letters, and the task is to extract the flag from these patterns.

Steps to Solve:

1. **Open the PCAP File**:
    1. Use Wireshark to open the provided file.
2. **Inspect Packet Contents**:
    1. Examine the packets to identify a pattern. Many packets contain repetitive letters like AAAAAAAAAAAA.
3. **Identify the Flag**:
    1. Look for distinctive sequences, such as {{{{{{{{{{{{. The flag is located near this sequence and is revealed letter by letter.
4. **Extract the Flag**:
    1. Manually note each character in sequence, or write a script to automate this process if necessary.
5. **Decoded Flag:**
    1. STOUTCTF{fZtPEj720e1OKFrQPqouICBdgVAtD14N}

Tools and Methods:

- **Tool Used**: Wireshark for packet analysis.
- **Why This Method**: Wireshark's ability to display packet details simplifies pattern recognition.

How It Works:

Packet data often contains raw content that can be interpreted as text. In this case, a repetitive pattern hints at the presence of a hidden message. Manually or programmatically extracting the letters reconstructs the flag.