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: "Fairytales"

This challenge centers around decoding a PDF file using metadata and text hints from the story itself.

Challenge Description:

- Embark on a quest into the heart of the Arctic's endless ice, where ancient mysteries await. The Eternal Navigator, a ship lost to time, holds the key to forgotten knowledge—and the cost of uncovering its secrets may be greater than you ever imagined.

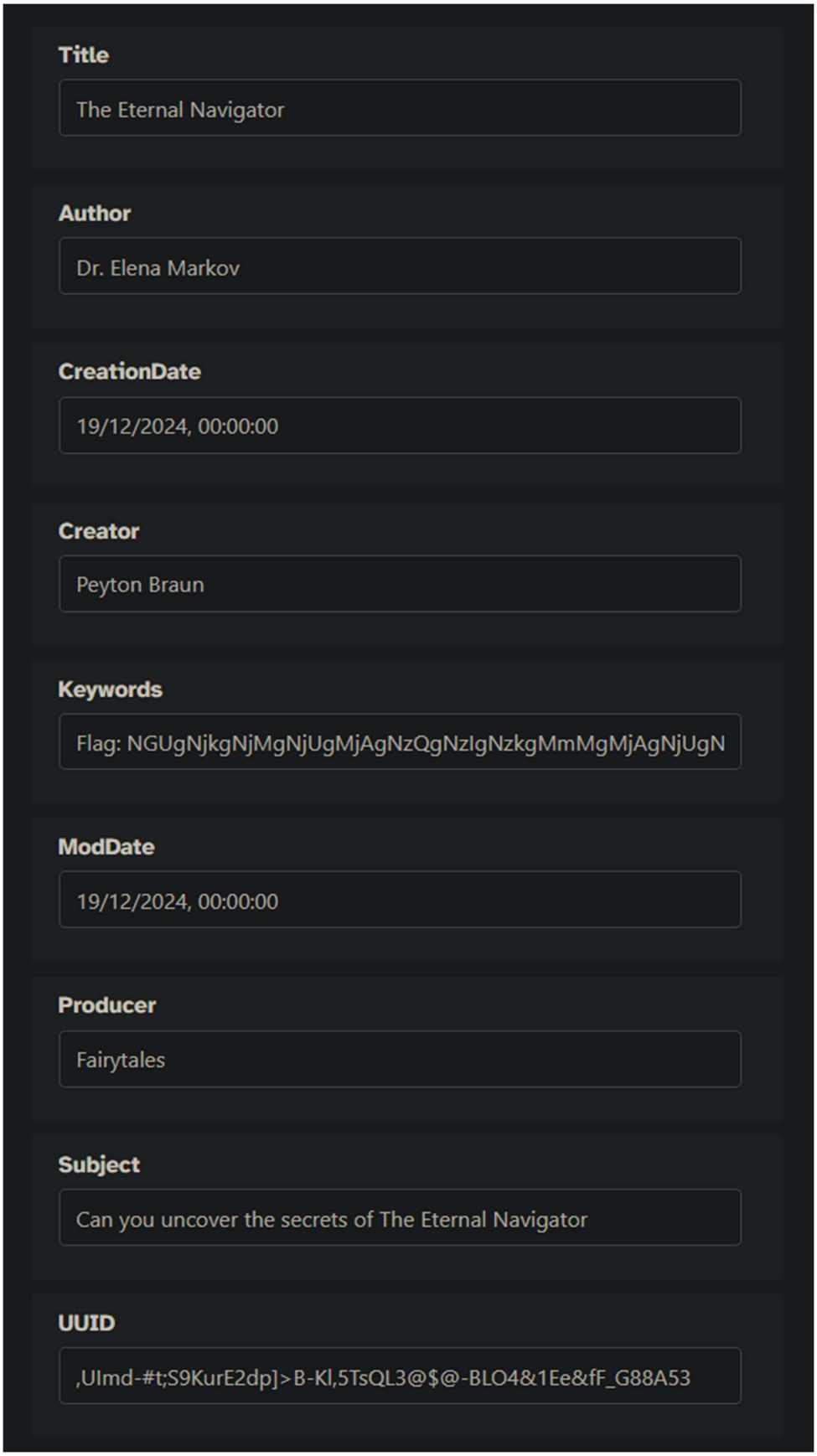
Challenge Hints:

- Like a fairytale one of the chapters has more relevant information than the rest!
- A question for you, what was it again they renamed Facebook to? Might be useful, might not, but that is for you to decide!

Steps to Solve:

1. **The PDF File:**
    - The challenge provides a 5-page PDF file containing a story. The key information is in Chapter 2, where it mentions:
        - The number 1985 which implies **Base85** decoding.
        - A cryptic reference to "ancient texts" and "shifting 47 places," which hints at **Rot47** encoding.
2. **Investigating Metadata:**

- Using a metadata viewer tool (e.g., https://www.sejda.com/edit-pdf-metadata), you can extract metadata from the PDF. One field contains:


Title
The Eternal Navigator
Author
Dr. Elena Markov
CreationDate
19/12/2024, 00:00:00
Creator
Peyton Braun
Keywords
Flag: NGUgNjkgNjMgNjUgMjAgNzQgNzIgNzkgMmMgMjAgNjUgN
ModDate
19/12/2024, 00:00:00
Producer
Fairytales
Subject
Can you uncover the secrets of The Eternal Navigator
UUID
,UImd-#t;S9KurE2dp]>B-Kl,5TsQL3@$@-BLO4&1Ee&fF_G88A53

        - flag="NGUgNjkgNjMgNjUgMjAgNzQgNzIgNzkgMmMgMjAgNjUgNzggNzAgNmMgNmYgNzIgNjUgNzIgMjEgMjAgNDIgNzUgNzQgMjAgNzQgNjggNjUgMjAgNzQgNzIgNzUgNjUgMjAgNzQgNzIgNjUgNjEgNzMgNzUgNzIgNjUgNzMgMjAgNmYgNjYgMjAgNzQgNjggNjUgMjAgNDUgNzQgNjUgNzIgNmUgNjEgNmMgMjAgNGUgNjEgNzYgNjkgNjcgNjEgNzQgNmYgNzIgMjAgNzIgNjUgNmQgNjEgNjkgNmUgMjAgNjggNjkgNjQgNjQgNjUgNmUgMmUgMjAgNGIgNjUgNjUgNzAgMjAgNzMgNjUgNjUgNmIgNjkgNmUgNjcgMmMgMjAgNjEgNmUgNjQgMjAgNzkgNmYgNzUgMjAgNmQgNjkgNjcgNjggNzQgMjAgNmEgNzUgNzMgNzQgMjAgNzUgNmUgNjMgNmYgNzYgNjUgNzIgMjAgNzQgNjggNjUgNjkgNzIgMjAgNzMgNjUgNjMgNzIgNjUgNzQgNzMgMmU="
    - This base64 string looks promising for decoding.

3. **Decoding the Metadata Field:**
    - Decode from **Base64** to get a long hexadecimal string:
        - 45 69 63 65 20 74 72 79 2c 20 65 78 70 6c 6f 72 65 72 21 20 42 75 74 20 74 68 65 20 74 72 75 65 20 74 72 65 61 73 75 72 65 73 20 6f 66 20 74 68 65 20 45 74 65 72 6e 61 6c 20 4e 61 76 69 67 61 74 6f 72 2e
    - Convert the hexadecimal string to ASCII (e.g., using https://www.rapidtables.com/convert/number/ascii-to-hex.html):
        - Nice try, explorer! But the true treasures of the Eternal Navigator remain hidden.
    - This is a **decoy message**! The real solution lies elsewhere.

4. **The UUID Clue:**
    - Another field in the metadata contains a UUID-like string:
        - ,UImd-#t;S9KurE2dp]>B-Kl,5TsQL3@$@-BLO4&1Ee&fF_G88A53
        - Since we know what a UUID should look like this should pop out as something wrong and should be looked at further.
            1. A UUID (Universally Unique Identifier) typically looks like this: "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx", where each "x" represents a hexadecimal digit (0-9, a-f), separated by hyphens, forming a 32-character string with a standard 8-4-4-4-12 grouping
    - This is the actual data to decode. Based on the story hints (Base85 and Rot47), this string needs to be decoded twice.

5. **Decoding the UUID:**
    - Use **Base85 decoding** first (e.g., CyberChef’s Base85 decoder).
    - Then apply **Rot47** to the result.

6. **Final Flag:**
    - After both decoding steps, the final flag is revealed as:
        - STOUTCTF{n2ff2B98QwhoP29hSaV9tTabPTGF94Z5}

Tools and Methods:

- **Tools:**
    - https://www.sejda.com/edit-pdf-metadata (or a similar PDF metadata viewer).
    - CyberChef for decoding and analyzing data.
    - Online Base64 and hexadecimal converters, such as https://www.rapidtables.com/convert/number/ascii-to-hex.html.
- **Methods:**
    - Base64 decoding to interpret metadata.
    - Hexadecimal to ASCII conversion for data clarity.
    - Base85 and Rot47 decoding for the final extraction.

How It Works:

1. The challenge begins with a PDF file containing hidden clues in its story and metadata.
2. Metadata reveals a field with an encoded string in Base64. Decoding this leads to a hex-encoded message.
3. The text hints and UUID-like string direct you to double decode using Base85 followed by Rot47, ultimately uncovering the flag.