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: "Substitute Teacher"

This is the most complex challenge in the CTF, requiring multiple decoding methods, careful analysis of a PCAP file, and a substitution cipher.

Challenge Description:

- The year is 1992, a few weeks after the fall of the Soviet Union. Amidst the chaos, a group of 45 rogue operatives known as "The Teachers" were tasked with safeguarding classified files. Their mission? To ensure these secrets stayed hidden from prying eyes. To achieve this, they devised a series of intricate steps to obscure their plans.
- Your mission is to recover the hidden flag from their encrypted communication. The operatives left all the tools you need in the provided file, but they didn't make it easy. They relied on meticulous precision, where every detail—big or small, uppercase or lowercase—could hold the key to unlocking their secrets.
- Can you decipher their layers of secrecy and reveal the hidden truth?

Challenge Hints:

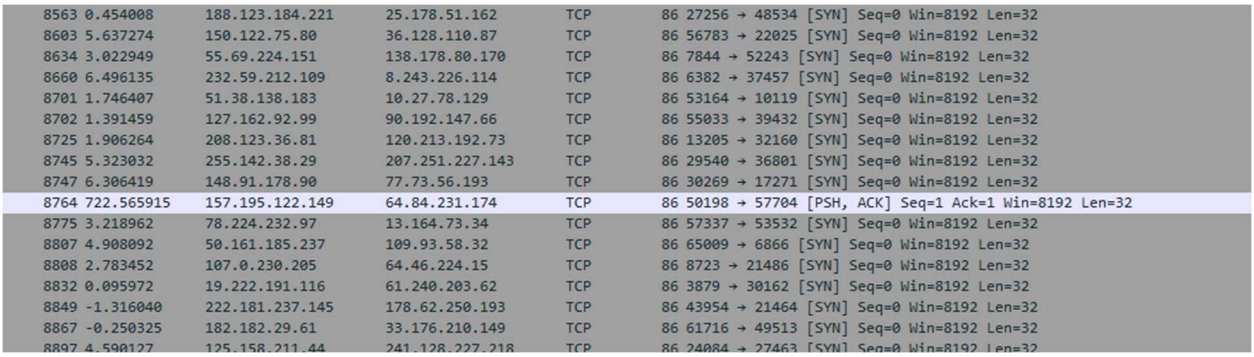
- You are looking for 1 of each of the following: HTTP, FTP, TCP, UDP. You need all 4 to solve.
- For sanity, there are 4 steps to get to the file. Then you can start looking for the flag. The flag is INSIDE the file its not hiding anywhere that you need tools to find. The 4 you need are plaintext.
- Use a tool like Cyberchef for the first couple parts of the challenge. gzip -d doesn't work for some reason. Entropy is your friend! There are 4 steps before you get a pcap file. Don't forget you have more information at your disposal, it might help to look at it ;)

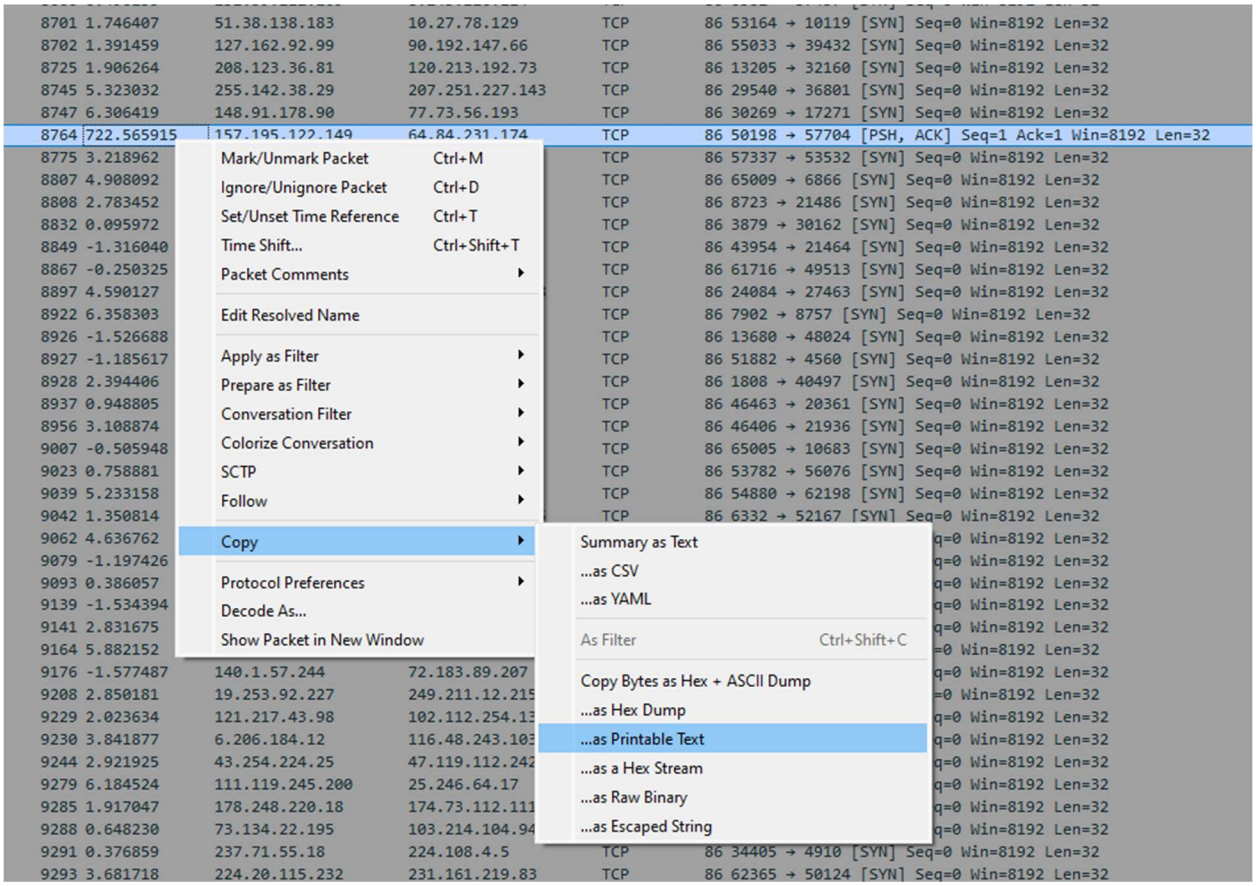
Steps to Solve:

1. **Initial File:**
    - You are provided with a .gz file. Normally, this can be decompressed using gzip -d, but in this case, it needs to be decompressed in **CyberChef**.
2. **First Layer of Decoding:**
    - Once decompressed, the file reveals another encoded layer. Use the hints from the challenge description:
        - "The year is 1992" = **Base92**.
        - "45 rouge operatives" = **Base45**.
    - Decode the file using **Base92** first, followed by **Base45**.
3. **Second Compression:**
    - After Base92 and Base45 decoding, analyze the output's entropy (in CyberChef) to discover it's compressed again. Use gzip to decompress.
4. **Resulting pcap File:**
    - The final output is a pcap file. Open it in **Wireshark** to begin analysis.
5. **Clues in Wireshark:**
    - In the challenge description, "The Teachers" implies **substitution cipher**, and "precision" means upper/lowercase and numbers are treated distinctly.
    - Look for anomalies in the pcap file, focusing on TCP, FTP, and UDP packets.

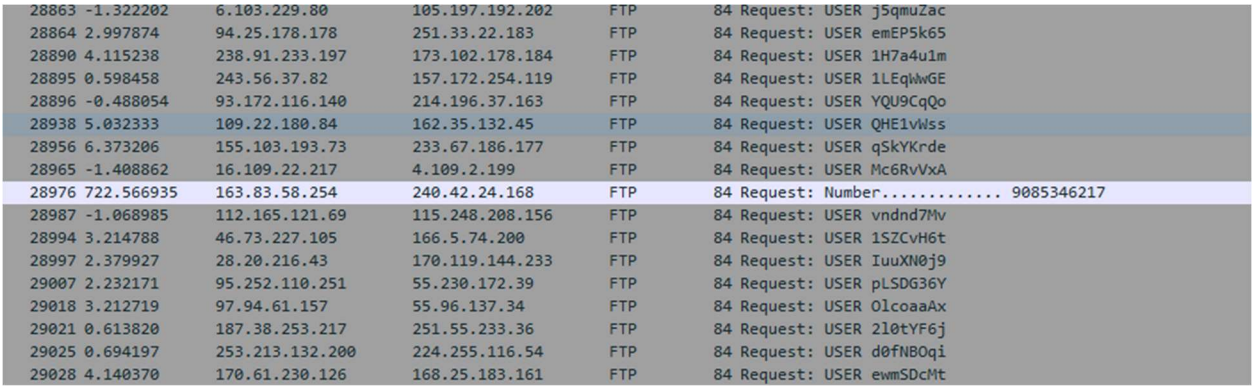
Findings:

- **HTTP Packet:** Contains:
    - **Searching for "Teacher"** in **CyberChef** as indicated by the name "Substitute Teacher" leads you to a flag embedded in a HTTP Post request.
    - **The encoded flag:** YTERTCTQ{M1KyJDS6fXaU8PHzuKjSBHrgs5gt1Uhu}
- **TCP Packet:** Contains:
    - è½¬´KÖ/ZEH@:TÃz@Tç®Äáhé÷P OUpper WSCZMQHNUFBLIDEPJOYTRVXAKG
    - The "Upper" key is: WSCZMQHNUFBLIDEPJOYTRVXAKG.





- **FTP Packet:** Contains:
  - Number..... 9085346217
  - The “Number” key is: 9085346217.



28863	-1.322202	6.103.229.80	105.197.192.202	FTP	84 Request: USER j5qmuZac
28864	2.997874	94.25.178.178	251.33.22.183	FTP	84 Request: USER emEP5k65
28890	4.115238	238.91.233.197	173.102.178.184	FTP	84 Request: USER 1H7a4u1m
28895	0.598458	243.56.37.82	157.172.254.119	FTP	84 Request: USER 1LEqWwGE
28896	-0.488054	93.172.116.140	214.196.37.163	FTP	84 Request: USER YQU9CqQo
28938	5.032333	109.22.180.84	162.35.132.45	FTP	84 Request: USER QHE1vWss
28956	6.373206	155.103.193.73	233.67.186.177	FTP	84 Request: USER qSkYKrde
28965	-1.408862	16.109.22.217	4.109.2.199	FTP	84 Request: USER Mc6RvVxA
28976	722.566935	163.83.58.254	240.42.24.168	FTP	84 Request: Number..... 9085346217
28987	-1.068985	112.165.121.69	115.248.208.156	FTP	84 Request: USER vndnd7Mv
28994	3.214788	46.73.227.105	166.5.74.200	FTP	84 Request: USER 1SZCvH6t
28997	2.379927	28.20.216.43	170.119.144.233	FTP	84 Request: USER IuuXN0j9
29007	2.232171	95.252.110.251	55.230.172.39	FTP	84 Request: USER pLSDG36Y
29018	3.212719	97.94.61.157	55.96.137.34	FTP	84 Request: USER OlcoaaAx
29021	0.613820	187.38.253.217	251.55.233.36	FTP	84 Request: USER 2l0tYF6j
29025	0.694197	253.213.132.200	224.255.116.54	FTP	84 Request: USER d0fNBOqi
29028	4.140370	170.61.230.126	168.25.183.161	FTP	84 Request: USER ewmSDcMt

- **UDP Packet:** Search for "Lower" in CyberChef to locate:
  - After finding Number and Upper we can reasonably assume we are searching for “Lower” using Cyberchef makes this easy to search for using (Ctrl + f) to find Lower inside the UDP packet, as it isn’t easily shown inside the PCAP file.
  - Lower amuphvibojrtfzwnqyeclxkdgs
  - The “Lower” key is: amuphvibojrtfzwnqyeclxkdgs.

6. **Substitution Cipher:**
   - Combine the three keys:
     - Upper: WSCZMQHNUFBLIDEPJOYTRVXAKG
     - Lower: amuphvibojrtfzwnqyeclxkdgs
     - Numbers: 9085346217
   - Substitute each character in the encoded flag using its corresponding key.
7. **Encoded Flag:**
   - Encoded flag from the challenge:
     - YTERTCTQ{M1KyJDS6fXaU8PHzuKjSBHrgs5gt1Uhu}
8. **Final Flag:**
   - After substitution, the decoded flag is:
     - STOUTCTF{E8YrQNB6mWaI2PGncYjBKGkyz3yl8Iec}

Tools and Methods:

- **Tools:**
  - CyberChef for decompression and decoding.
  - Gzip for handling compressed files.

    - Wireshark for analyzing the PCAP file.
    - Substitution cipher decoders for the final flag extraction.
- **Methods:**
    - Base92 and Base45 decoding based on challenge clues.
    - Packet analysis in Wireshark to identify encoded keys.
    - Key substitution (Uppercase, Lowercase, Numbers) to decode the flag.

How It Works:

1. Start with a .gz file and decompress it to reveal an encoded layer.
2. Decode the layers sequentially (Base92, Base45) and decompress again to obtain a PCAP file.
3. Analyze the PCAP file in Wireshark to uncover substitution cipher keys (Upper, Lower, Numbers).
4. Use the keys to decode the final encoded flag, yielding the solution.