

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 OUpperr`
`WSCZMQHNUFBLIDEPJOYTRVXAKG`
 - The "Upper" key is: WSCZMQHNUFBLIDEPJOYTRVXAKG.

8563	0.454008	188.123.184.221	25.178.51.162	TCP	86 27256 → 48534 [SYN] Seq=0 Win=8192 Len=32
8603	5.637274	150.122.75.80	36.128.110.87	TCP	86 56783 → 22025 [SYN] Seq=0 Win=8192 Len=32
8634	3.022949	55.69.224.151	138.178.80.170	TCP	86 7844 → 52243 [SYN] Seq=0 Win=8192 Len=32
8660	6.496135	232.59.212.109	8.243.226.114	TCP	86 6382 → 37457 [SYN] Seq=0 Win=8192 Len=32
8701	1.746407	51.38.138.183	10.27.78.129	TCP	86 53164 → 10119 [SYN] Seq=0 Win=8192 Len=32
8702	1.391459	127.162.92.99	90.192.147.66	TCP	86 55033 → 39432 [SYN] Seq=0 Win=8192 Len=32
8725	1.906264	208.123.36.81	120.213.192.73	TCP	86 13205 → 32160 [SYN] Seq=0 Win=8192 Len=32
8745	5.323032	255.142.38.29	207.251.227.143	TCP	86 29540 → 36801 [SYN] Seq=0 Win=8192 Len=32
8747	6.306419	148.91.178.90	77.73.56.193	TCP	86 30269 → 17271 [SYN] Seq=0 Win=8192 Len=32
8764	722.565915	157.195.122.149	64.84.231.174	TCP	86 50198 → 57704 [PSH, ACK] Seq=1 Ack=1 Win=8192 Len=32
8775	3.218962	78.224.232.97	13.164.73.34	TCP	86 57337 → 53532 [SYN] Seq=0 Win=8192 Len=32
8807	4.908092	50.161.185.237	109.93.58.32	TCP	86 65009 → 6866 [SYN] Seq=0 Win=8192 Len=32
8808	2.783452	107.0.230.205	64.46.224.15	TCP	86 8723 → 21486 [SYN] Seq=0 Win=8192 Len=32
8832	0.095972	19.222.191.116	61.240.203.62	TCP	86 3879 → 30162 [SYN] Seq=0 Win=8192 Len=32
8849	-1.316040	222.181.237.145	178.62.250.193	TCP	86 43954 → 21464 [SYN] Seq=0 Win=8192 Len=32
8867	-0.250325	182.182.29.61	33.176.210.149	TCP	86 61716 → 49513 [SYN] Seq=0 Win=8192 Len=32
8897	4.590127	125.158.211.44	241.128.227.218	TCP	86 24084 → 27463 [SYN] Seq=0 Win=8192 Len=32
8701	1.746407	51.38.138.183	10.27.78.129	TCP	86 53164 → 10119 [SYN] Seq=0 Win=8192 Len=32
8702	1.391459	127.162.92.99	90.192.147.66	TCP	86 55033 → 39432 [SYN] Seq=0 Win=8192 Len=32
8725	1.906264	208.123.36.81	120.213.192.73	TCP	86 13205 → 32160 [SYN] Seq=0 Win=8192 Len=32
8745	5.323032	255.142.38.29	207.251.227.143	TCP	86 29540 → 36801 [SYN] Seq=0 Win=8192 Len=32
8747	6.306419	148.91.178.90	77.73.56.193	TCP	86 30269 → 17271 [SYN] Seq=0 Win=8192 Len=32
8764	722.565915	157.195.122.149	64.84.231.174	TCP	86 50198 → 57704 [PSH, ACK] Seq=1 Ack=1 Win=8192 Len=32
8775	3.218962			TCP	86 57337 → 53532 [SYN] Seq=0 Win=8192 Len=32
8807	4.908092			TCP	86 65009 → 6866 [SYN] Seq=0 Win=8192 Len=32
8808	2.783452			TCP	86 8723 → 21486 [SYN] Seq=0 Win=8192 Len=32
8832	0.095972			TCP	86 3879 → 30162 [SYN] Seq=0 Win=8192 Len=32
8849	-1.316040			TCP	86 43954 → 21464 [SYN] Seq=0 Win=8192 Len=32
8867	-0.250325			TCP	86 61716 → 49513 [SYN] Seq=0 Win=8192 Len=32
8897	4.590127			TCP	86 24084 → 27463 [SYN] Seq=0 Win=8192 Len=32
8922	6.358303			TCP	86 7902 → 8757 [SYN] Seq=0 Win=8192 Len=32
8926	-1.526688			TCP	86 13680 → 48024 [SYN] Seq=0 Win=8192 Len=32
8927	-1.185617			TCP	86 51882 → 4560 [SYN] Seq=0 Win=8192 Len=32
8928	2.394406			TCP	86 1808 → 40497 [SYN] Seq=0 Win=8192 Len=32
8937	0.948805			TCP	86 46463 → 20361 [SYN] Seq=0 Win=8192 Len=32
8956	3.108874			TCP	86 46406 → 21936 [SYN] Seq=0 Win=8192 Len=32
9007	-0.505948			TCP	86 65005 → 10683 [SYN] Seq=0 Win=8192 Len=32
9023	0.758881			TCP	86 53782 → 56076 [SYN] Seq=0 Win=8192 Len=32
9039	5.233158			TCP	86 54880 → 62198 [SYN] Seq=0 Win=8192 Len=32
9042	1.350814			TCP	86 6332 → 52167 [SYN] Seq=0 Win=8192 Len=32
9062	4.636762				q=0 Win=8192 Len=32
9079	-1.197426				q=0 Win=8192 Len=32
9093	0.386057				q=0 Win=8192 Len=32
9139	-1.534394				q=0 Win=8192 Len=32
9141	2.831675				q=0 Win=8192 Len=32
9164	5.882152				=0 Win=8192 Len=32
9176	-1.577487	140.1.57.244	72.183.89.207		q=0 Win=8192 Len=32
9208	2.850181	19.253.92.227	249.211.12.215		=0 Win=8192 Len=32
9229	2.023634	121.217.43.98	102.112.254.13		q=0 Win=8192 Len=32
9230	3.841877	6.206.184.12	116.48.243.103		q=0 Win=8192 Len=32
9244	2.921925	43.254.224.25	47.119.112.242		q=0 Win=8192 Len=32
9279	6.184524	111.119.245.200	25.246.64.17		q=0 Win=8192 Len=32
9285	1.917047	178.248.220.18	174.73.112.111		q=0 Win=8192 Len=32
9288	0.648230	73.134.22.195	103.214.104.94		q=0 Win=8192 Len=32
9291	0.376859	237.71.55.18	224.108.4.5	TCP	86 34405 → 4910 [SYN] Seq=0 Win=8192 Len=32
9293	3.681718	224.20.115.232	231.161.219.83	TCP	86 62365 → 50124 [SYN] Seq=0 Win=8192 Len=32

○ **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 1LEqhwGE
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 vndnd7Hv
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 OlcoaAx
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 d0fNB0qi
29028	4.140370	170.61.230.126	168.25.183.161	FTP	84 Request: USER ewmSDcHt

- **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{E8YrQNB6mWal2PGncYjBKGkyz3yl8lec}

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.