Packets Primer CTF Challenge Write-up

Author: LT 'syreal' Jones
Challenge Name: Packets Primer
Platform: picoCTF
Objective: Analyze the provided packet capture (PCAP) file to find the hidden flag.

Challenge Description

In this challenge, we were provided with a packet capture file, and our task was to analyze the packets to extract a hidden flag. After loading the file into a packet analysis tool (such as Wireshark), I located the flag in **Frame 4**, hidden within the TCP payload.

The extracted flag was found in the payload but was formatted with spaces between each character. The next step was to clean up the flag by removing the spaces, which I accomplished using a simple Python script.

Packet Capture Analysis

Frame 4 Analysis:

Frame Information:

- **Frame Size:** 126 bytes
- **Source MAC Address:** `PCSSystemtec_af:39:9f (08:00:27:af:39:9f)`
- **Destination MAC Address:** `PCSSystemtec_93:ce:73 (08:00:27:93:ce:73)`

IP Information:

- **Source IP Address:** `10.0.2.15`
- **Destination IP Address:** `10.0.2.4`

TCP Information:

- **Source Port:** `48750`
- **Destination Port:** `9000 (cslistener)`
- **Sequence Number:** `1`
- **Acknowledgment Number:** `1`

TCP Payload (Data): In the TCP payload, the flag was hidden but separated by spaces:

p i c o C T F { p 4 c k 3 7 _ 5 h 4 r k _ c e c c a a 7 f }

Python Script: Removing Spaces from the Flag

After extracting the flag from the TCP payload, I wrote the following Python script to remove the spaces and format the flag correctly.

```
# Define the flag with spaces

flag_with_spaces = "p i c o C T F { p 4 c k 3 7 _ 5 h 4 r k _ c e c c a a 7 f }"



# Remove spaces

flag = flag_with_spaces.replace(" ", "")



# Print the cleaned flag

print(flag)
```

Output:

picoCTF{Redacted}