

Forensics CTF 3

Platform: picoCTF 2025

Challenge Name: Ph4nt0m 1ntrud3r

Category: Forensics

Difficulty: Easy

Submitted By: Gurleen Kaur Brar

Objective

The goal of the challenge was to analyze a network packet capture (PCAP) file to identify how an intruder exfiltrated sensitive data and extract the hidden flag. This required filtering TCP traffic, inspecting packet lengths, and decoding the hidden payload.

Challenge Description

Ph4nt0m 1ntrud3r

Easy Forensics picoCTF 2025 browser_webshell_solvable

AUTHOR: PRINCE NIYONSHUTI N.

Hints ?

Description

1 2 3

A digital ghost has breached my defenses, and my sensitive data has been stolen! 🕵️💻 Your mission is to uncover how this phantom intruder infiltrated my system and retrieve the hidden flag.

To solve this challenge, you'll need to analyze the provided PCAP file and track down the attack method. The attacker has cleverly concealed his moves in well timely manner. Dive into the network traffic, apply the right filters and show off your forensic prowess and unmask the digital intruder!

Find the PCAP file here [Network Traffic PCAP file](#) and try to get the flag.

Files and Tools Used

- **File Provided:** Network Traffic PCAP file
- **Tools Used:**

- Wireshark (for PCAP analysis)
- Kali Linux

Step-by-Step Process

Step 1: Load and Rearrange Timestamps in Wireshark

Opened the PCAP file in Wireshark and rearranged the timestamp column to chronological order. This allowed for better visibility of packet sequences and retransmissions.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|-------------|-------------|----------|--------|---|
| 6 | 0.000720 | 192.168.0.2 | 192.168.1.2 | TCP | 48 | [TCP Retransmission] 20 → 80 [SYN] Seq=0 Win=8192 Len=8 |
| 18 | 0.000245 | 192.168.0.2 | 192.168.1.2 | TCP | 48 | [TCP Retransmission] 20 → 80 [SYN] Seq=0 Win=8192 Len=8 |
| 10 | 0.000000 | 192.168.0.2 | 192.168.1.2 | TCP | 48 | 20 → 80 [SYN] Seq=0 Win=8192 Len=8 [TCP PDU reassembled in 3] |
| 20 | 0.000239 | 192.168.0.2 | 192.168.1.2 | TCP | 48 | [TCP Retransmission] 20 → 80 [SYN] Seq=0 Win=8192 Len=8 |
| 150 | 0.000487 | 192.168.0.2 | 192.168.1.2 | TCP | 48 | [TCP Retransmission] 20 → 80 [SYN] Seq=0 Win=8192 Len=8 |
| 190 | 0.000735 | 192.168.0.2 | 192.168.1.2 | TCP | 48 | [TCP Retransmission] 20 → 80 [SYN] Seq=0 Win=8192 Len=8 |
| 80 | 0.000961 | 192.168.0.2 | 192.168.1.2 | TCP | 48 | [TCP Retransmission] 20 → 80 [SYN] Seq=0 Win=8192 Len=8 |
| 170 | 0.001393 | 192.168.0.2 | 192.168.1.2 | TCP | 48 | [TCP Retransmission] 20 → 80 [SYN] Seq=0 Win=8192 Len=8 |
| 120 | 0.001655 | 192.168.0.2 | 192.168.1.2 | TCP | 48 | [TCP Retransmission] 20 → 80 [SYN] Seq=0 Win=8192 Len=8 |
| 130 | 0.001882 | 192.168.0.2 | 192.168.1.2 | TCP | 48 | [TCP Retransmission] 20 → 80 [SYN] Seq=0 Win=8192 Len=8 |
| 210 | 0.002115 | 192.168.0.2 | 192.168.1.2 | TCP | 48 | [TCP Retransmission] 20 → 80 [SYN] Seq=0 Win=8192 Len=8 |
| 40 | 0.002355 | 192.168.0.2 | 192.168.1.2 | TCP | 48 | [TCP Retransmission] 20 → 80 [SYN] Seq=0 Win=8192 Len=8 |
| 90 | 0.002582 | 192.168.0.2 | 192.168.1.2 | TCP | 48 | [TCP Retransmission] 20 → 80 [SYN] Seq=0 Win=8192 Len=8 |
| 200 | 0.002821 | 192.168.0.2 | 192.168.1.2 | TCP | 48 | [TCP Retransmission] 20 → 80 [SYN] Seq=0 Win=8192 Len=8 |
| 110 | 0.003051 | 192.168.0.2 | 192.168.1.2 | TCP | 48 | [TCP Retransmission] 20 → 80 [SYN] Seq=0 Win=8192 Len=8 |
| 70 | 0.003276 | 192.168.0.2 | 192.168.1.2 | TCP | 52 | [TCP Retransmission] 20 → 80 [SYN] Seq=0 Win=8192 Len=12 |
| 220 | 0.003511 | 192.168.0.2 | 192.168.1.2 | TCP | 52 | [TCP Retransmission] 20 → 80 [SYN] Seq=0 Win=8192 Len=12 |
| 50 | 0.003740 | 192.168.0.2 | 192.168.1.2 | TCP | 52 | [TCP Retransmission] 20 → 80 [SYN] Seq=0 Win=8192 Len=12 |
| 140 | 0.004931 | 192.168.0.2 | 192.168.1.2 | TCP | 52 | [TCP Retransmission] 20 → 80 [SYN] Seq=0 Win=8192 Len=12 |
| 30 | 0.005156 | 192.168.0.2 | 192.168.1.2 | TCP | 52 | [TCP Retransmission] [Illegal Segments] |
| 100 | 0.005398 | 192.168.0.2 | 192.168.1.2 | TCP | 52 | [TCP Retransmission] 20 → 80 [SYN] Seq=0 Win=8192 Len=12 |
| 160 | 0.005617 | 192.168.0.2 | 192.168.1.2 | TCP | 44 | [TCP Retransmission] 20 → 80 [SYN] Seq=0 Win=8192 Len=4 |

Step 2: Filter Packets by Length = 12

Used Wireshark's filter to isolate TCP packets with a length of 12 bytes, a sign of possible hidden payloads or covert messages.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|-------------|-------------|----------|--------|--|
| 40 | 0.002355 | 192.168.0.2 | 192.168.1.2 | TCP | 48 | [TCP Retransmission] 20 → 80 [SYN] Seq=0 Win=8192 Len=8 |
| 90 | 0.002582 | 192.168.0.2 | 192.168.1.2 | TCP | 48 | [TCP Retransmission] 20 → 80 [SYN] Seq=0 Win=8192 Len=8 |
| 200 | 0.002821 | 192.168.0.2 | 192.168.1.2 | TCP | 48 | [TCP Retransmission] 20 → 80 [SYN] Seq=0 Win=8192 Len=8 |
| 110 | 0.003051 | 192.168.0.2 | 192.168.1.2 | TCP | 48 | [TCP Retransmission] 20 → 80 [SYN] Seq=0 Win=8192 Len=8 |
| 70 | 0.003276 | 192.168.0.2 | 192.168.1.2 | TCP | 52 | [TCP Retransmission] 20 → 80 [SYN] Seq=0 Win=8192 Len=12 |
| 220 | 0.003511 | 192.168.0.2 | 192.168.1.2 | TCP | 52 | [TCP Retransmission] 20 → 80 [SYN] Seq=0 Win=8192 Len=12 |
| 50 | 0.003740 | 192.168.0.2 | 192.168.1.2 | TCP | 52 | [TCP Retransmission] 20 → 80 [SYN] Seq=0 Win=8192 Len=12 |
| 140 | 0.004931 | 192.168.0.2 | 192.168.1.2 | TCP | 52 | [TCP Retransmission] 20 → 80 [SYN] Seq=0 Win=8192 Len=12 |
| 30 | 0.005156 | 192.168.0.2 | 192.168.1.2 | TCP | 52 | [TCP Retransmission] [Illegal Segments] |
| 100 | 0.005398 | 192.168.0.2 | 192.168.1.2 | TCP | 52 | [TCP Retransmission] 20 → 80 [SYN] Seq=0 Win=8192 Len=12 |
| 160 | 0.005617 | 192.168.0.2 | 192.168.1.2 | TCP | 44 | [TCP Retransmission] 20 → 80 [SYN] Seq=0 Win=8192 Len=4 |

[Conversation completeness: Incomplete (9)]

[TCP Segment Len: 12]

Sequence Number: 0 (relative sequence number)

Sequence Number (raw): 0

[Next Sequence Number: 13 (relative sequence number)]

Acknowledgment Number: 0

Acknowledgment number (raw): 0

0101 ... = Header Length: 20 bytes (5)

Flags: 0x002 (SYN)

Window: 8192

[Calculated window size: 8192]

Checksum: 0xfd41 [unverified]

[Checksum Status: Unverified]

Urgent Pointer: 0

[Timestamps]

[SEQ/ACK analysis]

[Bytes in flight: 12]

[Bytes sent since last PSF flag: 68]

[TCP Analysis Flags]

TCP payload (12 bytes)

Retransmitted TCP segment data (12 bytes)

0000 45 00 00 34 00 01 00 00 40 06 f8 6e c0 a8 00 02

0010 c0 a8 01 02 00 14 00 50 00 00 00 00 00 00 00

0020 50 02 20 00 fd 41 00 00 63 47 6c 6a 62 30 4e 55

0030 52 67 3d 3d

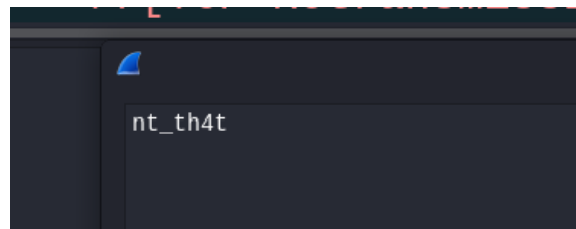
P: A: cG1jb0NU

Rg==

Step 3: Inspect Packet Bytes

Right-clicked each of these 12-byte packets → Show packet bytes. The payload revealed ASCII fragments of the flag.

The fragments were decoded and reassembled into a full string.



Flag Submitted

```
picoCTF{1t_w4snt_th4t_34sy_tbh_4r_af160980}
```

The flag was successfully submitted and marked correct.

