# **CTF Topic: TCP/IP Hijacking**

# **Introduction**

In this Capture The Flag (CTF) challenge, we'll delve into the realm of network scanning and analysis, specifically focusing on TCP/IP hijacking and packet analysis. The challenge will test your knowledge and skills in network reconnaissance, packet manipulation, and protocol analysis.

# **Tools and requirements**

Wireshark

Python3

# **Link**

Target: <https://www.mediafire.com/file/tkpxj9ywq71wlzr/Challange.PY/file>

# **Scenario**

You are tasked with analyzing network traffic and performing a TCP/IP hijacking attack on a target network. The target network includes a server with the following details:

* Server IP: 65.61.137.117
* Destination Port for TCP Hijacking

# **Process to Perform**

Begin with Scanning the network looking for open ports

**Let’s Begin the challenge**

# **Question**

**Flag1**: what is the destination IP of the TCP hijacking?

Answer: 65. 61. 137.117

**Flag3**: what is the major tool for analyzing TCP/IP packets?

Answer: Wireshark

**Flag 4**: What is the Bank Account of Thanos?

Answer: 100192876543123

**Flag 5**: What is the Port used by Src?

Answer: 21

# **Hint**





