# Mac Flooding Challenge

The scope of this challenge is to capture and decrypt the flags that H1 and H2 are exchanging and send it to the email abaffa94@servizimicrosoft.unical.it using the subject [MacFloodingChallenge] and as body the text of the challenge decrypted.

On Attacker side you must build a Mac Flooder script using Python and the packet forger SCAPY, sniff the data with tshark and decrypt it with openssl enc command.

It is important to have the following IP Address

H1: 10.0.0.2

H2: 10.0.0.3

Attacker: 10.0.0.4

On the H1 and the attacker some tools are required, you can install using the following commands:

Python3 → $sudo apt install python3 python3-pip

Scapy → $sudo su
$pip3 install scapy

On H1 download MacSpoofingChallengeSender.py (available on course website) and run it with the following command:

$ sudo python3 MacSpoofingChallengeSender.py

Hints:

- For import scapy into python script:
  - from scapy.all import *
- For sending packets with scapy
  - sendp(Ether(src=<<MAC_ADDRESS>>,dst=<<MAC_ADDRESS>>)/ARP(op=2, psrc="<<IP_ADDRESS(Or subnet)>>", hwdst="<<BROADCAST_MAC_ADDRESS>>"), loop=1)
- For generate Random Mac Address on scapy
  - RandMAC() → inside scapy for generating random mac address
- Filter data using Tshark
  - sudo tshark -Y '<<FILTER>>' -Tfields -e data > raw.txt
- Decode data to base64 (data collected from tshark are in byte and must converted in base 64)
  - xxd -r -p > output.txt
- Decrypt using openssl enc
  - openssl enc -<<CYPHER>> -d -k <<KEY>>-base64