ARP Spoofing 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 [ArpSpoofingChallenge] and as body the text of the challenge decrypted.

On Attacker side you must build an ARP Spoofer 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 H1 download ARPSpoofingChallengeSender.py (available on course website) and run it with the following command:

$ sudo python3 ARPSpoofingChallengeSender.py

Hints:

- For import scapy into python script:
  - from scapy.all import *
- For sending packets with scapy
  - sendp(pkt = Ether(src='<<VICTIM_MAC_ADDRESS>>', dst='<<BROADCAST_MAC_ADDRESS>>')/ARP(op=2, hwsrc='<<VICTIM_MAC_ADDRESS>>', pdst='<<VICTIM_IP_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