ARP Spoofing Challenge

ARP Spoofing is a Man in the Middle (MitM) attack that allows attackers to intercept communication between network devices.

The goal of this challenge is to intercept and decrypt messages exchanged between two hosts (from our GNS3 lab). Let's call the first host `H1` and the second one `H2`.

In this scenario we have to act as the **Attacker**. More in detail, we have to build a Python3 script able to spoof packet using **ARP Spoofing** techniques. In order to do that, we have to send (spoofed) ARP messages onto a local area network with the aim to associate our (the attacker) MAC address with the IP address of another host (in our case, `H2`). In this way, the traffic meant for our victim (`H2`) will be sent to our IP address from the default gateway.

Prerequisites

- Download and run the `packetSender.py` on host_1 `H1`
- Execute the script on `H1`

```
packetSender.py <HOST_1_SRC_IP> <HOST_2_DST_IP>
```

Hints

- In order to send ARP messages onto local area network using Python3, install `scapy` python module
- Arp messages can be sent using the following function:
  - `sendp(pkt = Ether(src='<<VICTIM_MAC_ADDRESS>>', dst='<<BROADCAST_MAC_ADDRESS>>')/ARP(op=2, hwsrc='<<VICTIM_MAC_ADDRESS>>', pdst='<<VICTIM_IP_ADDRESS>>')`
- Data can be filtered using `tshark`
- Remember that data collected from `tshark` are in byte, thus they must be converted in `base64`
- Some data are in `plaintext`, some other are crypted. Decrypt data using discovered password and encryption algorithm
  `openssl enc -a <ALGORITHM> -k <KEY> -d -pbkdf2 -base64`