Jeremie Tordjman [redacted]
Yuval Yefet [redacted]

Arpspoof Warning + Protection

Part 1: Warning System

We have decided to implement three detection methods:

- Counting the number of ARP reply packets and ARP request packets, other than requests from other devices and replies from our device.
- Validating MAC address – we checked that he MAC address in the reply packet is actually belongs to the IP in that packet.
- We checked the ARP table for any duplicates.

There is no false positive.

Part 2: Protection (Added challenge)

First, we tried to drop all ARP replies while sniffing them in a lower level before they were dropped and then we tried to add manually packets that seemed correct. However, this implementation didn't work as expected – the dropping wasn't working properly. Therefore, we have decided to make the ARP table permanent. The protection checks the ARP table, and if there is a row that is not permanent, update it to permanent status. For each new ARP reply packet, we verify that it's correct, and only then add it to the table. In order to verify a packet, we use the same methods of detection, with a slight change in the implementation of the duplicates function.

Here we can see that once the ping runs, the ARP table shows the address in permanent status: