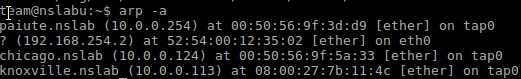
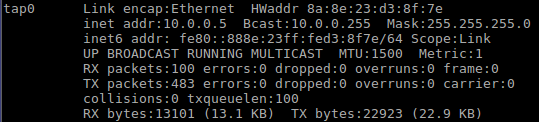
1. Send ICMP echo request to both LIN and WIN machines.

Execute command “ping –c 5 10.0.0.113”(WIN)” and “ping –c 5 10.0.0.124(LIN)” to send ICMP echo request to WIN and LIN.

run “arp –a” to get the arp cache.

Their MAC addresses go as follows:

local MAC address on tap0:

The MAC address of LIN 10.0.0.124 is at 00:50:56:9f:3d:d9

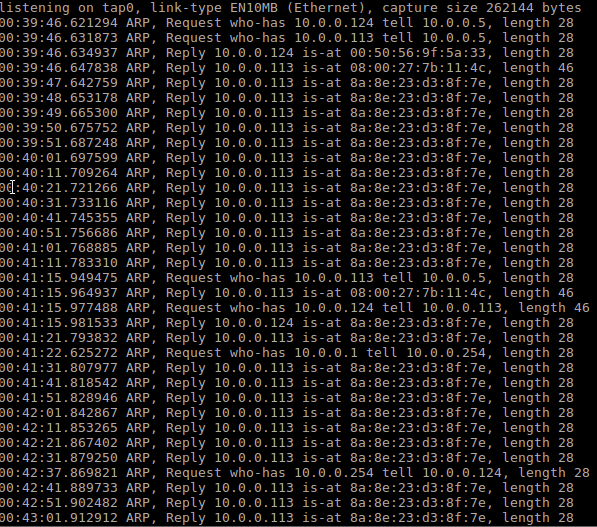
The MAC address of WIN 10.0.0.113 is at 08:00:27:7b:11:4c

The MAC address of VM is 8a:8e:23:d3:8f:7e

2. ARP data after ARP poisoning

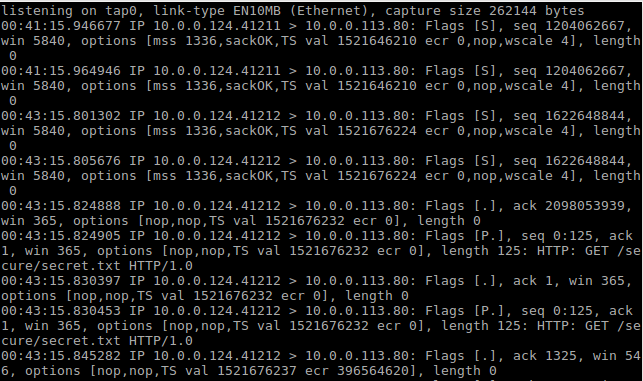
In the first terminal, run tcpdump –n –i tap0 arp to monitor the arp packets

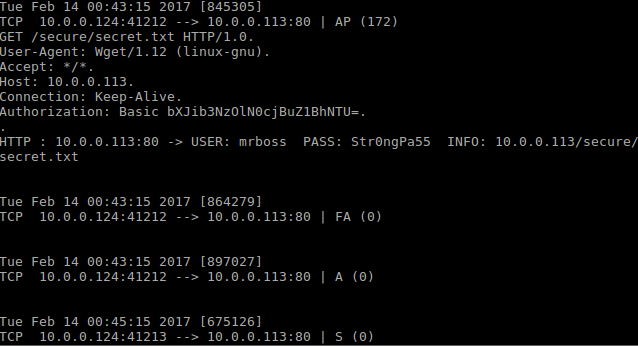
In the second terminal, run tcpdump –n –i tap0 port 80 and host 10.0.0.124

In the third terminal, run ettercap –i tap0 -T -M arp:oneway /10.0.0.124// /10.0.0.113// to start the man-in-middle attack

The graph given above is the snippet of the ARP data right after the ARP poisoning. The normal ARP replies are marked by red lines while the spoofed replies are marked by yellow lines.

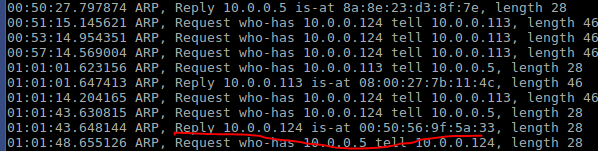
3. snippet of 10 or so lines of HTTP data between LIN and WIN

The graph given above is the HTTP data between LIN and WIN. The port used by LIN changed after several data packets, while the WIN port remain the same as 80.

4. A password line from ettercap showing the HTTP username and password.

The Password of 10.0.0.113 is marked by the red line.

5. A snippet of the ARP data right after the ARP poisoner is deactivated, showing the correct MAC address for the LIN machine



The correct reply after the poisoning deactivated is marked red.

6. What is Mallory's probability of success in the DNS cache poisoning attack against Alice?