Grace de Benedetti and Skyler Kessenich
Citation:
https://levelup.gitconnected.com/man-in-the-middle-attack-part-1-arp-spoofing-6f5b174dec59

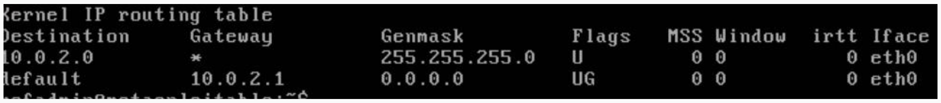
A. What is Kali's main interface's MAC address? (The main interface is probably called eth0, but check ifconfig to be sure.)
    a. eth0
B. What is Kali's main interface's IP address?
    a. 10.0.2.15
C. What is Metasploitable's main interface's MAC address?
    a. eth0
D. What is Metasploitable's main interface's IP address?
    a. 10.0.2.4
E. Show Kali's routing table. (Use "netstat -r" to see it with symbolic names, or "netstat -rn" to see it with numerical addresses.)
    a.

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         10.0.2.1        0.0.0.0         UG        0 0          0 eth0
10.0.2.0        0.0.0.0         255.255.255.0   U         0 0          0 eth0
```

F. Show Kali's ARP cache. (Use "arp" or "arp -n".)
    a.

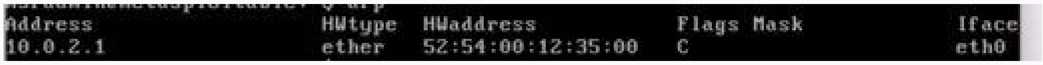
```
Address                  HWtype  HWaddress           Flags Mask            Iface
10.0.2.1                 ether   52:54:00:12:35:00   C                     eth0
```

G. Show Metasploitable's routing table.
    a.



```
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
10.0.2.0        *               255.255.255.0   U         0 0          0 eth0
default         10.0.2.1        0.0.0.0         UG        0 0          0 eth0
```

H. Show Metasploitable's ARP cache.
    a.



```
Address                  HWtype  HWaddress           Flags Mask            Iface
10.0.2.1                 ether   52:54:00:12:35:00   C                     eth0
```

I. Suppose the user of Metasploitable wants to get the CS231 sandbox page via the command "curl http://cs231.jeffondich.com/". To which MAC address should Metasploitable send the TCP SYN packet to get the whole HTTP query started? Explain why.
    a. Metasploitable should send the TCP SYN packet to 52:54:00:12:35:00 because this is the address that is connected to the network that we are

working on so it will be able to participate in the TCP handshake and deliver the webpage.

J. Fire up Wireshark on Kali. Start capturing packets for "tcp port http". On Metasploitable, execute "curl http://cs231.jeffondich.com/". On Kali, stop capturing. Do you see an HTTP response on Metasploitable? Do you see any captured packets in Wireshark on Kali?

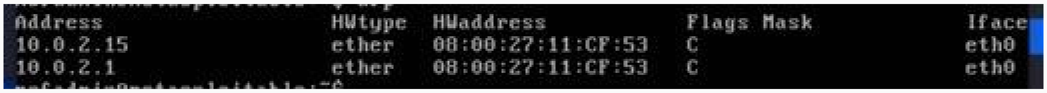
   a. We see an HTTP response written in HTML on Metasploitable but no captured packets in Wireshark on Kali

K. Now, it's time to be Mal (who will, today, merely eavesdrop). Use Ettercap to do ARP spoofing (also known as ARP Cache Poisoning) with Metasploitable as your target. There are many online tutorials on how to do this (here's one). Find one you like, and start spoofing your target. NOTE: most of these tutorials are showing an old user interface for Ettercap, which may make them confusing. The steps you're trying to take within Ettercap are:

   a. Start sniffing (*not* bridged sniffing) on eth0
   b. Scan for Hosts
   c. View the Hosts list
   d. Select your Metasploit VM from the Host List
   e. Add that host as Target 1
   f. Start ARP Poisoning (including Sniff Remote Connections)
   g. Do your stuff with wireshark and Metasploit
   h. Stop ARP Poisoning

I'll post some screenshots on Slack of how I got Ettercap to do these things. Honestly, I don't know who redesigned this user interface to make it so much harder to do things, but they did. (Common enough in the Linux UI world.)

L. Show Metasploitable's ARP cache. How has it changed?

   a. 

```
Address                  HWtype  HWaddress           Flags Mask            Iface
10.0.2.15                ether   08:00:27:11:CF:53   C                     eth0
10.0.2.1                 ether   08:00:27:11:CF:53   C                     eth0
```

   b. There is a new address 10.0.2.15 that was not there before which corresponds to the IP address of the Kali machine. Additionally, the HWaddresses have changed and they are all the same now.

M. If you execute "curl http://cs231.jeffondich.com/" on Metasploitable now, to what MAC address will Metasploitable send the TCP SYN packet? Explain why.

  a. Metasploitable would send it to 08:00:27:11:CF:53 now because that is its only option after Kali changed its ARP cache. This address is the address of the Kali machine so Metasploitable will be sending the TCP SYN packet to Kali.

N. Start Wireshark capturing "tcp port http" again.

O. Execute "curl http://cs231.jeffondich.com/" on Metasploitable. On Kali, stop capturing. Do you see an HTTP response on Metasploitable? Do you see captured packets in Wireshark? Can you tell from Kali what messages went back and forth between Metasploitable and cs231.jeffondich.com?

  a. We still see an HTTP response on Metasploitable and we now see captured packets in Wireshark. Yes, we can see the information on what messages went back and forth between Metasploitable and cs231.jeffondich.com. We see the TCP handshake, the HTTP packets being sent back and forth with get requests, and ok responses.

P. Explain in detail what happened. How did Kali change Metasploitable's ARP cache? (If you want to watch the attack in action, try stopping the PITM/MITM attack by selecting "Stop mitm attack(s)" from Ettercap's Mitm menu, starting a Wireshark capture for "arp", and restarting the ARP poisoning attack in Ettercap.)

  a. Kali changes Metasploitable's ARP cache by sending falsified messages to both Metasploitable and the access point which is their shared local area network. In the message, Kali sends information saying the location of the IP address where Metasploitable wants to send information is the MAC address associated with Kali. Kali is able to falsify the information in this message by posing as the access point by putting its IP address as the sender address in the ARP message so that Metasploitable trusts the new information. Kali does the same thing to the access point, posing as Metasploitable by using their IP address as the sender address. The ARP message says Metasploitable's IP address is located at Kali's MAC address. This way, Kali receives information from both the access point and Metasploitable. This new information is shown in the changed ARP cache for Metasploitable.

Q. If you wanted to design an ARP spoofing detector, what would you have your detector do? (As you think about this, consider under what circumstances your detector might generate false positives.)

a. If I were designing this detector, I would have it search for matching MAC addresses. As we saw in the changed ARP cache for Metasploitable, the MAC addresses are the same for both IP addresses. We can tell we have been spoofed because these addresses match and we know we would be sending all our information to the machine at that address, which is the hacker. However, there may be times when there are multiple IP addresses with the same MAC location when we are not being attacked so we could generate some false positives if that were the case. However, from research it does appear that these matching MAC addresses are a good sign you've been spoofed.