Vanessa and Ruben

Execution

A. **What is Kali's main interface's MAC address? (The main interface is probably called eth0, but check ifconfig to be sure.)**
   a. 46:67:b1:88:d0:e0

B. **What is Kali's main interface's IP address?**
   a. 192.168.64.4

C. **What is Metasploitable's main interface's MAC address?**
   a. a6:4d:9b:67:15:26

D. **What is Metasploitable's main interface's IP address?**
   a. 192.168.64.5

E. **Show Kali's routing table. (Use "netstat -r" to see it with symbolic names, or "netstat -rn" to see it with numerical addresses.)**

```
┌──(kali㉿kali)-[~]
└─$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Ifac
e
default         192.168.64.1    0.0.0.0         UG        0 0          0 eth0
192.168.64.0    0.0.0.0         255.255.255.0   U         0 0          0 eth0
```

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

```
┌──(kali㉿kali)-[~]
└─$ arp
Address                  HWtype  HWaddress           Flags Mask            If
ace
192.168.64.1             ether   72:ae:d5:73:8a:66   C                     et
h0
```

G. **Show Metasploitable's routing table.**

```
msfadmin@metasploitable:~$ netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
192.168.64.0    0.0.0.0         255.255.255.0   U         0 0          0 eth0
0.0.0.0         192.168.64.1    0.0.0.0         UG        0 0          0 eth0
msfadmin@metasploitable:~$
```

H. **Show Metasploitable's ARP cache.**

I. **Suppose the user of Metasploitable wants to get the CS338 sandbox page via the command "curl http://cs338.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 72:AE:D5:73:8A:66. This is the only MAC address on the ARP table in Metasploitable, so it's the only option for the "next hop" that Metasploitable can take.

J. **Fire up Wireshark on Kali. Start capturing packets for "tcp port http". On Metasploitable, execute "curl http://cs338.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 do not see any captured packets on Wireshark.
    b. On Metasploitable, we see the html of the site, so we have received an HTTP response.

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:**
    L. Start sniffing (*not* bridged sniffing) on eth0
    M. Scan for Hosts
    N. View the Hosts list
    O. Select your Metasploit VM from the Host List
    P. Add that host as Target 1
    Q. Start ARP Poisoning (including Sniff Remote Connections)
    R. Do your stuff with wireshark and Metasploitable
    S. 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.)

So, to wrap up this step: start the ARP poisoning. You will keep the ARP poisoning attack active until you are done with your AITM attack. (Realistically, you will probably start and stop ARP poisoning several times as you gradually figure out what's going on while doing the steps below.)

T. Show Metasploitable's ARP cache. How has it changed?

U. Without actually doing it yet, predict what will happen if you execute "curl http://cs338.jeffondich.com/" on Metasploitable now. Specifically, to what MAC address will Metasploitable send the TCP SYN packet? Explain why.

a. Metasploitable will send the TCP SYN packet to Kali. This is because Metasploitable's arp cache says to send packets to 46:67:B1:88:D0:E0, which is the MAC address of Kali.

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

W. Execute "curl http://cs338.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 cs338.jeffondich.com?

a. Yes, we see captured packets. We can see the TCP handshake, cs338.jeffondich.com sending the html over, and we see the termination of the connection.

X. 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 AITM 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. Metasploitable doesn't know which IP to send the SYN packet to reach cs338.jeffondich.com, so it asks the local network for the machine on the local network that deals with the IP address corresponding with cs338.jeffondich.com.
b. Kali responds, telling Metasploitable that it is the computer that knows what to do with cs338.jeffondich.com's IP address.
c. Metasploitable says, "Okay, let me write that down," and puts it in their ARP cache.
d. Now Metasploitable will send the SYN packet to Kali rather than the regular path (through something like a router). Kali has now become the adversary in the middle.

Y. 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. The spoofing detector would need to be able to detect when a single MAC address has multiple IP addresses associated with it. (Is there a bad actor in the middle acting as the router/next hop in the chain of packets?)

i. This approach can create false positives because there are times when having 1 MAC address with multiple IP addresses is intended and safe (such as the [example] Jeff give's in the assignment instructions).

Synthesis

A. Explain in detail Mal's strategy for intercepting the traffic between Alice and Bob. Use any of your observations from the Execution section to clarify your explanation. But be careful not to just reiterate all the steps, and not to focus on specific tools. (For example, I would not expect you to refer to Ettercap in this explanation, since it is merely one of many available tools for generating suitable ARP messages.) Your goal here is to explain to a technical audience (e.g., other CS majors who have not studied security) what Mal is up to, and how ARP cache poisoning works.

   a. MAL sends a bunch of ARP responses quickly when Metasploitable requests for the MAC address of the computer that is responsible for the IP address it wants to send to.

      i. The router sends ARP responses slower than MAL does, so Metasploitable doesn't receive the real MAC address.

   b. It then responds to Metasploitable's request with its own MAC address.

   c.

Source	Destination	Protocol	Length	Info
46:67:b1:88:d0:e0	72:ae:d5:73:8a:66	ARP	42	192.168.64.5 is at 46:67:b1:88:d0:e0
46:67:b1:88:d0:e0	a6:4d:9b:67:15:26	ARP	42	192.168.64.1 is at 46:67:b1:88:d0:e0 (duplicate use of 1
46:67:b1:88:d0:e0	72:ae:d5:73:8a:66	ARP	42	192.168.64.5 is at 46:67:b1:88:d0:e0
46:67:b1:88:d0:e0	a6:4d:9b:67:15:26	ARP	42	192.168.64.1 is at 46:67:b1:88:d0:e0 (duplicate use of 1
46:67:b1:88:d0:e0	72:ae:d5:73:8a:66	ARP	42	192.168.64.5 is at 46:67:b1:88:d0:e0
46:67:b1:88:d0:e0	a6:4d:9b:67:15:26	ARP	42	192.168.64.1 is at 46:67:b1:88:d0:e0 (duplicate use of 1
46:67:b1:88:d0:e0	72:ae:d5:73:8a:66	ARP	42	192.168.64.5 is at 46:67:b1:88:d0:e0
46:67:b1:88:d0:e0	a6:4d:9b:67:15:26	ARP	42	192.168.64.1 is at 46:67:b1:88:d0:e0 (duplicate use of 1
46:67:b1:88:d0:e0	72:ae:d5:73:8a:66	ARP	42	192.168.64.5 is at 46:67:b1:88:d0:e0
46:67:b1:88:d0:e0	a6:4d:9b:67:15:26	ARP	42	192.168.64.1 is at 46:67:b1:88:d0:e0 (duplicate use of 1

   d. Metasploitable now has Kali/Mal's MAC address in its ARP cache for where to send its packet to next, so when Metasploitable uses this MAC address, Kali is able to intercept all the packets that Metasploitable sends (the packets with source 192.168.64.5). Kali then forwards these packets to jeffondich.com

   e.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.64.5	45.79.89.123	TCP	74	40781 → 80 [SYN] Seq=0 Win=5
2	0.005932478	192.168.64.5	45.79.89.123	TCP	74	[TCP Retransmission] 40781 →
3	0.058322993	45.79.89.123	192.168.64.5	TCP	66	80 → 40781 [SYN, ACK] Seq=0
4	0.062465470	45.79.89.123	192.168.64.5	TCP	66	[TCP Retransmission] 80 → 40
5	0.063064942	192.168.64.5	45.79.89.123	TCP	54	40781 → 80 [ACK] Seq=1 Ack=1
6	0.063608917	192.168.64.5	45.79.89.123	HTTP	212	GET / HTTP/1.1
7	0.070655261	192.168.64.5	45.79.89.123	TCP	54	40781 → 80 [ACK] Seq=1 Ack=1
8	0.070746965	192.168.64.5	45.79.89.123	TCP	212	[TCP Retransmission] 40781 →
9	0.124177890	45.79.89.123	192.168.64.5	TCP	54	80 → 40781 [ACK] Seq=1 Ack=1
10	0.124178015	45.79.89.123	192.168.64.5	HTTP	785	HTTP/1.1 200 OK (text/html)

B. From Alice's perspective, is this attack detectable? If not, why not? If so, how would Alice's setup need to change to detect the attack?

    a. No, unless Alice somehow knew the correct MAC address of the router, but if this was the case, she would never have to ask for it in the first place.
    b. If Alice wanted to detect the attack, she would need some sort of spoof detector (such as described in our answer to question Y).

C. From Bob's perspective, is this attack detectable?
    a. No. All Bob sees is that a source IP wants information, so it sends the info.

D. Could Alice or Bob detect and/or prevent this attack if the website in question was using HTTPS instead of HTTP? Explain.
    a. Yes. HTTPS uses a TLS handshake to become reasonably certain that each party in the connection is actually talking to who they think they're talking to. (That is, Bob is sure she's talking to Alice, and Alice is sure that she's talking to Bob.) This means that an AITM attack is not possible since all Mal could do here is forward the intercepted messages (act as an eavesdropper).