Miles Hoene-Langdon

Execution

a. Kali's main interface MAC address is ba:ed:9e:37:6a:eb.
b. Kali's main interface IP address is 192.168.64.2.
c. Metasploitable's main interface's MAC address is 3a:1c:d8:53:7f:a1.
d. Metasploitable's main interface's IP address is 192.168.64.3.
e. Kali's routing table:

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
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. Kali's ARP cache:

```
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.64.1             ether   3e:a6:f6:e3:32:64   C                     eth0
```

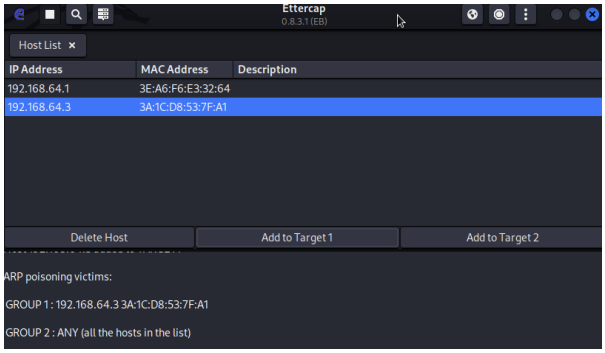
g. Metasploitable's routing table:

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
192.168.64.0    *               255.255.255.0   U         0 0          0 eth0
default         192.168.64.1    0.0.0.0         UG        0 0          0 eth0
```

h. Metasploitable's ARP cache:

```
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.64.1             ether   3E:A6:F6:E3:32:64   C                     eth0
```

i. Metasploitable should send the TCP SYN packet to 3e:a6:f6:e3:32:64. This is because plugging the IP address of http://cs338.jeffondich.com/ into Metasploitable's routing table tells us that we should send the SYN packet to 192.168.64.1 for the first hop in getting it to the desired IP. Then from our ARP cache, we know this IP address corresponds to the MAC address 3e:a6:f6:e3:32:64.
j. There is an HTTP response on Metasploitable but there are no captured packets in Wireshark on Kali.
k. I have now started ARP poisoning with Ettercap.



l. Metasploitable's ARP cache now has a different MAC address for the IP address 192.168.64. The new MAC address is Kali's MAC address. The ARP cache is shown below:

```
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.64.1             ether   BA:ED:9E:37:6A:EB   C                     eth0
```

m. If I execute "curl http://cs338.jeffondich.com/" on Metasploitable, Metasploitable will now send the SYN packet to the MAC address ba:ed:9e:37:6a:eb. This is because the Metasploitable's routing table still tells it to send the SYN packet to 192,168.64.1, however this IP address is now associated with ba:ed:9e:37:6a:eb in the ARP cache. As a result, the SYN packet will go to this MAC address.

n. Wireshark is now capturing on "tcp port http" again.

o. I do see an HTTP response on Metasploitable the same as before and now I do see the captured packets in Wireshark. I can clearly see what messages went back and forth between Metasploitable and http://cs338.jeffondich.com/ including the TCP handshake, the HTTP GET request and the HTTP response from the server.

	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.64.3	45.79.89.123	TCP	74	59291 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSva…
2	0.006787727	192.168.64.3	45.79.89.123	TCP	74	[TCP Retransmission] 59291 → 80 [SYN] Seq=0 Win=5840 Len=0 MS…
3	0.061010767	45.79.89.123	192.168.64.3	TCP	66	80 → 59291 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1386 SA…
4	0.063450278	45.79.89.123	192.168.64.3	TCP	66	[TCP Retransmission] 80 → 59291 [SYN, ACK] Seq=0 Ack=1 Win=64…
5	0.064124680	192.168.64.3	45.79.89.123	TCP	54	59291 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0
6	0.064505255	192.168.64.3	45.79.89.123	HTTP	212	GET / HTTP/1.1
7	0.070987072	192.168.64.3	45.79.89.123	TCP	54	59291 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0
8	0.071036279	192.168.64.3	45.79.89.123	TCP	212	[TCP Retransmission] 59291 → 80 [PSH, ACK] Seq=1 Ack=1 Win=58…
9	0.124613065	45.79.89.123	192.168.64.3	TCP	54	80 → 59291 [ACK] Seq=1 Ack=159 Win=64128 Len=0
10	0.124613148	45.79.89.123	192.168.64.3	HTTP	785	HTTP/1.1 200 OK (text/html)
11	0.127531501	45.79.89.123	192.168.64.3	TCP	54	80 → 59291 [ACK] Seq=1 Ack=159 Win=64128 Len=0
12	0.127561542	45.79.89.123	192.168.64.3	TCP	785	[TCP Retransmission] 80 → 59291 [PSH, ACK] Seq=1 Ack=159 Win=…
13	0.128148612	192.168.64.3	45.79.89.123	TCP	54	59291 → 80 [ACK] Seq=159 Ack=732 Win=7360 Len=0
14	0.129146382	192.168.64.3	45.79.89.123	TCP	54	59291 → 80 [FIN, ACK] Seq=159 Ack=732 Win=7360 Len=0
15	0.135554033	192.168.64.3	45.79.89.123	TCP	54	[TCP Keep-Alive] 59291 → 80 [ACK] Seq=159 Ack=732 Win=7360 Le…
16	0.135580283	192.168.64.3	45.79.89.123	TCP	54	[TCP Retransmission] 59291 → 80 [FIN, ACK] Seq=159 Ack=732 Wi…
17	0.187348067	45.79.89.123	192.168.64.3	TCP	54	80 → 59291 [FIN, ACK] Seq=732 Ack=160 Win=64128 Len=0
18	0.190361120	45.79.89.123	192.168.64.3	TCP	54	[TCP Retransmission] 80 → 59291 [FIN, ACK] Seq=732 Ack=160 Wi…
19	0.190872573	192.168.64.3	45.79.89.123	TCP	54	59291 → 80 [ACK] Seq=160 Ack=733 Win=7360 Len=0
20	0.198734776	192.168.64.3	45.79.89.123	TCP	54	[TCP Dup ACK 19#1] 59291 → 80 [ACK] Seq=160 Ack=733 Win=7360 …

p. Kali begins by cycling through all of the IP addresses 192.168.64.___ and broadcasts asking who has each address and requisition that they tell Kali. After collecting all the different hosts, ARP poisoning begins. Kali then starts sending packets to the host MAC addresses that it found, claiming that the hosts that it found are at its own MAC address. In this scenario for example, Kali sent Metasploitable a packet claiming that 192.168.64.1 is at ba:ed:9e:37:6a:eb. Metasploitable accepted this ARP packet and changed its ARP cache accordingly and became ARP poisoned.

q. My ARP spoofing detector would verify MAC addresses by asking other trusted computers on the network whether the IP matches the given MAC address. If the MAC and IP don't match the input from the trusted computer, then the detector would go off. A potential false positive for this detector could happen if IP addresses change and one trusted machine has an outdated IP address and MAC address pair that itself is unaware of.

Synthesis

a. When Alice sends information in the form of packets to Bob, Alice will begin by sending these packets to an IP on her local network that serves as the first hop in the packets' journey to Bob. This first hop IP address is determined by Alice's routing table which instructs her where to send packets intended for certain IPs. Mal's strategy for intercepting the packets Alice sends to Bob is by altering Alice's ARP cache, which consists of IP address and MAC address pairings stored by ALice. Note that MAC addresses are built into devices whereas IP addresses are not. Mal will specifically alter Alice's ARP cache so that Mal's own MAC address is the MAC address for the first hop

IP. Mal achieves this alteration through ARP poisoning. Mal begins the process of ARP poisoning by broadcasting ARP packets on Alice's local network requesting the MAC address for all the different IP addresses. Once these MAC addresses are collected, Mal then sends ARP packets to Alice telling her that the MAC address for the first hop IP is Mal's own MAC address. Alice hopefully believes Mal and changes her ARP cache so that the first hop IP is now matched with Mal's MAC address. Following this change, when Alice sends packets to Bob, they will now first go to Mal as Mal is now associated with the first hop IP for Alice. Mal will receive these packets and then send them to the actual first hop IP address. Also, Mal will receive packets from Bob that are for Alice and send them to Alice.

b. The attack is detectable from Alice's perspective. Alice will be able to broadcast an ARP packet on her local network asking what the MAC address is for the first hop IP. If the responses from different machines on the network don't match what she was told by Mal, then she will know that the information sent to Bob is being intercepted.
c. This attack is not detectable from Bob's perspective. Bob's ARP cache is specific to his local network which is not Alice's network. Bob does not know where Alice sends the packets on her local network before he receives them.
d. If Alice and Bob used HTTPS they could not detect that Mal is intercepting their packets simply by doing this but they could prevent the attack. If Alice and Bob use HTTPS then the information that they send to each other is encrypted. Even if Mal intercepts it, she cannot read or successfully alter the information in any meaningful way. Thus, the dangers of this attack are prevented through using HTTPS.