Kyra Helmbold & Kiri Salij

EXECUTION

a. **What is Kali's main interface's MAC address? (The main interface is probably called eth0, but check ifconfig to be sure.)**

```
0x0<global>, 12:d3:45:c0:bf:d9
```

b. **What is Kali's main interface's IP address?**

```
192.168.64.2
```

c. **What is Metasploitable's main interface's MAC address?**

```
eth0 - 8a:b9:1b:b6:ab:22
```

d. **What is Metasploitable's main interface's IP address?**

```
192.168.64.3
```

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

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

```
Address                  HWtype  HWaddress           Flags Mask          Iface
192.168.64.1             ether   d2:88:0c:97:ad:64   C                     eth0
```

g. **Show Metasploitable'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
```

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

```
Address                  HWtype  HWaddress           Flags Mask          Iface
192.168.64.1             ether   D2:88:0C:97:AD:64   C                     eth0
```

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.**

   It should send it to 192.168.64.1. This is the address in the arp cache, and we want to send the TCP SYN packet to an address in the ARP Cache.

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?**

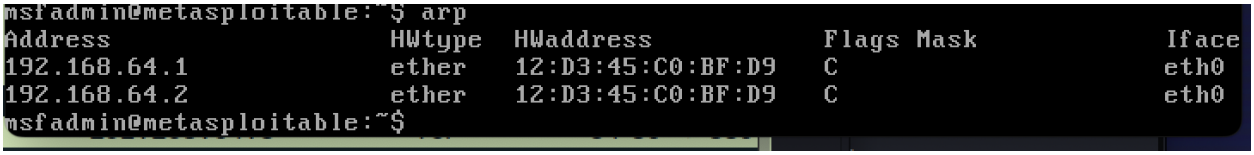
   I see an HTTP response on Metasploitable, but I do not see captured packers in Wireshark on Kali.

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:**

   done :)

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.)

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



We now have 192.2.168.64.2 in the arp cache. It thinks 192.186.64.2 has the MAC address 12:D3:45:C0:BF:D9, but it doesn't. Kali Lied. Now there are two MAC addresses with the same HWaddress.

m. **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.**

I think Metasploitable will send the TCP SYN Packet to 192.168.64.2, as this was most recently added to the ARP cache.

n. Start Wireshark capturing "tcp port http" again.
Done :)

o. 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?
I do! Yes I can.

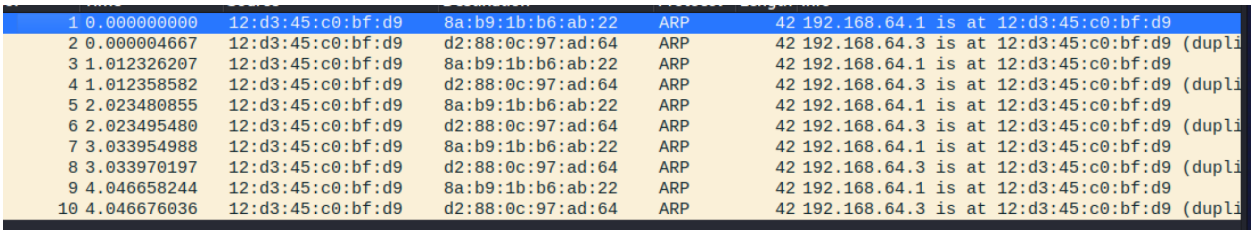
1	0.000000000	192.168.64.3	45.79.89.123	TCP	74	38979 → 80 [SYN] Seq=0 Win=5840 Len=0
2	0.006797044	192.168.64.3	45.79.89.123	TCP	74	[TCP Retransmission] 38979 → 80 [SYN]
3	0.112519036	45.79.89.123	192.168.64.3	TCP	66	80 → 38979 [SYN, ACK] Seq=0 Ack=1 Win=
4	0.118845058	45.79.89.123	192.168.64.3	TCP	66	[TCP Retransmission] 80 → 38979 [SYN,
5	0.119615859	192.168.64.3	45.79.89.123	TCP	54	38979 → 80 [ACK] Seq=1 Ack=1 Win=5888
6	0.119821308	192.168.64.3	45.79.89.123	HTTP	212	GET / HTTP/1.1
7	0.126777345	192.168.64.3	45.79.89.123	TCP	54	38979 → 80 [ACK] Seq=1 Ack=1 Win=5888
8	0.126834551	192.168.64.3	45.79.89.123	TCP	212	[TCP Retransmission] 38979 → 80 [PSH,
9	0.196381877	45.79.89.123	192.168.64.3	TCP	54	80 → 38979 [ACK] Seq=1 Ack=159 Win=64
10	0.196381919	45.79.89.123	192.168.64.3	HTTP	785	HTTP/1.1 200 OK (text/html)
11	0.198765276	45.79.89.123	192.168.64.3	TCP	54	80 → 38979 [ACK] Seq=1 Ack=159 Win=64
12	0.198822815	45.79.89.123	192.168.64.3	TCP	785	[TCP Retransmission] 80 → 38979 [PSH,
13	0.199321794	192.168.64.3	45.79.89.123	TCP	54	38979 → 80 [ACK] Seq=159 Ack=732 Win=
14	0.200804897	192.168.64.3	45.79.89.123	TCP	54	38979 → 80 [FIN, ACK] Seq=159 Ack=732
15	0.210858718	192.168.64.3	45.79.89.123	TCP	54	[TCP Keep-Alive] 38979 → 80 [ACK] Seq=
16	0.210880926	192.168.64.3	45.79.89.123	TCP	54	[TCP Retransmission] 38979 → 80 [FIN,
17	0.298988544	45.79.89.123	192.168.64.3	TCP	54	80 → 38979 [FIN, ACK] Seq=732 Ack=160
18	0.304252195	45.79.89.123	192.168.64.3	TCP	54	[TCP Retransmission] 80 → 38979 [FIN,
19	0.304773964	192.168.64.3	45.79.89.123	TCP	54	38979 → 80 [ACK] Seq=160 Ack=733 Win=
20	0.311587673	192.168.64.3	45.79.89.123	TCP	54	[TCP Dup ACK 19#1] 38979 → 80 [ACK] Se

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 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.)

Kali changed metasploitable's ARP cache, by first sending a message to all sources asking everyone to tell 192.168.64.2 (kali) who has what IP. Here, we are just scanning for hosts.

No.	Time	Source	Destination	Protocol	Length	Info
7	0.051141118	12:d3:45:c0:bf:d9	Broadcast	ARP	42	Who has 192.168.64.138? Tell 192.168.64.2
8	0.061244946	12:d3:45:c0:bf:d9	Broadcast	ARP	42	Who has 192.168.64.6? Tell 192.168.64.2
9	0.071533905	12:d3:45:c0:bf:d9	Broadcast	ARP	42	Who has 192.168.64.122? Tell 192.168.64.2
10	0.082185164	12:d3:45:c0:bf:d9	Broadcast	ARP	42	Who has 192.168.64.34? Tell 192.168.64.2
11	0.092320076	12:d3:45:c0:bf:d9	Broadcast	ARP	42	Who has 192.168.64.12? Tell 192.168.64.2
12	0.102866124	12:d3:45:c0:bf:d9	Broadcast	ARP	42	Who has 192.168.64.3? Tell 192.168.64.2
13	0.103676436	8a:b9:1b:b6:ab:22	12:d3:45:c0:bf:d9	ARP	42	192.168.64.3 is at 8a:b9:1b:b6:ab:22
14	0.113028413	12:d3:45:c0:bf:d9	Broadcast	ARP	42	Who has 192.168.64.253? Tell 192.168.64.2
15	0.123197535	12:d3:45:c0:bf:d9	Broadcast	ARP	42	Who has 192.168.64.204? Tell 192.168.64.2
16	0.133303114	12:d3:45:c0:bf:d9	Broadcast	ARP	42	Who has 192.168.64.190? Tell 192.168.64.2
17	0.143431610	12:d3:45:c0:bf:d9	Broadcast	ARP	42	Who has 192.168.64.175? Tell 192.168.64.2
18	0.153531063	12:d3:45:c0:bf:d9	Broadcast	ARP	42	Who has 192.168.64.127? Tell 192.168.64.2
19	0.163630559	12:d3:45:c0:bf:d9	Broadcast	ARP	42	Who has 192.168.64.243? Tell 192.168.64.2
20	0.173758472	12:d3:45:c0:bf:d9	Broadcast	ARP	42	Who has 192.168.64.177? Tell 192.168.64.2
21	0.183862467	12:d3:45:c0:bf:d9	Broadcast	ARP	42	Who has 192.168.64.117? Tell 192.168.64.2

Then, we poison the ARP Cache.



1	0.000000000	12:d3:45:c0:bf:d9	8a:b9:1b:b6:ab:22	ARP	42	192.168.64.1 is at 12:d3:45:c0:bf:d9
2	0.000004667	12:d3:45:c0:bf:d9	d2:88:0c:97:ad:64	ARP	42	192.168.64.3 is at 12:d3:45:c0:bf:d9 (dupli
3	1.012326207	12:d3:45:c0:bf:d9	8a:b9:1b:b6:ab:22	ARP	42	192.168.64.1 is at 12:d3:45:c0:bf:d9
4	1.012358582	12:d3:45:c0:bf:d9	d2:88:0c:97:ad:64	ARP	42	192.168.64.3 is at 12:d3:45:c0:bf:d9 (dupli
5	2.023480855	12:d3:45:c0:bf:d9	8a:b9:1b:b6:ab:22	ARP	42	192.168.64.1 is at 12:d3:45:c0:bf:d9
6	2.023495480	12:d3:45:c0:bf:d9	d2:88:0c:97:ad:64	ARP	42	192.168.64.3 is at 12:d3:45:c0:bf:d9 (dupli
7	3.033954988	12:d3:45:c0:bf:d9	8a:b9:1b:b6:ab:22	ARP	42	192.168.64.1 is at 12:d3:45:c0:bf:d9
8	3.033970197	12:d3:45:c0:bf:d9	d2:88:0c:97:ad:64	ARP	42	192.168.64.3 is at 12:d3:45:c0:bf:d9 (dupli
9	4.046658244	12:d3:45:c0:bf:d9	8a:b9:1b:b6:ab:22	ARP	42	192.168.64.1 is at 12:d3:45:c0:bf:d9
10	4.046676036	12:d3:45:c0:bf:d9	d2:88:0c:97:ad:64	ARP	42	192.168.64.3 is at 12:d3:45:c0:bf:d9 (dupli

Then, Metasploitable sent a message out saying I want to send my packet to whoever has the MAC address 12:D3:45:C0:BF:D9.

Metasploitable gets a response from Kali, and adds Kali's IP to the ARP cache.

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.)

I would have my spoofing detector search for instances where multiple addresses have the same MAC address, and flag all of them. This would detect false positives as it would flag both the real place I want to send them and the MITM, but it would detect the real positives too.

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.

Mal intercepts the traffic by:

1. Scanning for hosts (everyone on the local network): Broadcasts a message going to every IP address in the network saying tell me (Mal, 192.168.64.2) who you are.
2. Poisons the ARP cache ("Says hey, that's me" when Metasploitable asks "who has the MAC address I want?"). Normally, Alice does the following:
    a. Decides I want to send this to Bob.
    b. Realizes okay, I can't just send it to Bob, I have to send it to the router who sends it to a machine who then sends it to another machine, and somewhere down the line it gets to Bob.

    c. Now, Alice wants to send the packet to the router, so she asks hey, who has the MAC address 12:D3:45:C0:BF:D9, if she doesn't have this already in her ARP cache.
    d. Ettercap on Kali (Mal) says "hey, that's me!". Alternatively, earlier Mal can just send out a broadcast saying "hello! I have the MAC address 12:D3:45:C0:BF:D9! Add me to your ARP Cache!", and Alice will probably do so.
    e. Alice then says okay! I want to send my packets to the MAC address 12:D3:45:C0:BF:D9. Who in my ARP cache matches this? Alice finds out that Mal has this MAC address. Alice sends the packets to Mal.x
3. Mal then receives the traffic/packets.
4. Mal can then send the traffic/packets to Bob.

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?

Yes. There are two IP addresses in the ARP cache with the same MAC address, and they'll be able to listen in on the traffic from Alice until the ARP cache is updated (or they could continue poisoning the ARP cache). However, Alice might not be constantly checking the ARP cache.

c. From Bob's perspective, is this attack detectable?

No, it is not. Mal can just send the packets, and replace the source ip, source mac, and source port with the source information from Metasploitable (Alice). The packets will be the same as if Alice had sent them herself.

d. Could Alice or Bob detect and/or prevent this attack if the website in question was using HTTPS instead of HTTP? Explain.

No. Mal can always just forward the packets they received. They might not be able to alter or read them though. They will not be able to alter them because they would have to re-encrypt them using Alice's key, and they won't be able to read them because they would have to decrypt them using Bob's secret key. Mal still gets the packets, but cannot read or modify them.