Execution

a What is Kali's main interface's MAC address?

ea:d3:14:4c:42:6b

---

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

192.168.64.2

---

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

fa:46:26:8b:8d:1d

---

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

192.168.64.3

---

e Show 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 Show Kali's ARP cache.

Address	HWtype	HWaddress	Flags	Mask	Iface
192.168.64.3	ether	fa:46:26:8b:8d:1d	C		eth0
192.168.64.1	ether	52:ed:3c:91:02:64	C		eth0

---

g Show 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 Show Metasploitable's ARP cache.

Address	HWtype	HWaddress	Flags	Mask	Iface
192.168.64.1	ether	52:ED:3C:91:02:64	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 the packet to the MAC address of Kali because we want to establish a connection with the Kali interface.

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 didn't get any packets captured on Wireshark, but I saw that in Metasploitable the command had returned the HTML code for the web page.

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

There is an additional entry in the cache, namely Kali's address is shown in Metasploitable's ARP cache too.

Address	HWtype	HWaddress	Flags	Mask	Iface
192.168.64.1	ether	F2:3F:6E:BF:4F:B8	C		eth0
192.168.	ether	F2:3F:6E	C		eth0

	64.2		:BF:4F:B8			

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.	It will probably go to Kali's MAC address because of the ARP spoofing and the man-in-the-middle attack as Kali's MAC address is linked with a device already on the local area network.
o	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?	In Metasploitable, I can see the code of the page containing the contents of the site. Meanwhile, on Wireshark I can see there are packets captured. On Kali, I see packets in which the source or destination match the one on Metasploitable (where IP addresses are 192.168.64.3 and 45.79.89.123).
p	Explain in detail what happened. How did Kali change Metasploitable's ARP cache?	Upon the poisoning, I saw the IP address of Kali show up in the ARP cache of Metasploitable after calling **`curl http://cs338.jeffondich.com/`** in the terminal. In other words, in Metasploitable the IP address of Kali is connected there, allowing Kali to view messages sent between Metasploitable and the site.
q	If you wanted to design an ARP spoofing detector, what would you have your detector do?	In Wireshark, the indicator that there is ARP poisoning occurring is that there are duplicates of IP addresses shown within the packets. A solution would be to detect such instances if we have access to packets. Additionally, changes to the ARP cache will occur. Maybe it would be worthwhile to check for both of these instances.

Synthesis

a. Explain in detail Mal's strategy for intercepting the traffic between Alice and Bob.

Mal is basically trying to pass herself as Alice. Under normal circumstances, Alice would communicate with Bob using their IP addresses, but in the poisoning attack, Mal can essentially connect herself with Alice's IP address, as seen in the ARP cache, so that she will have access to packets that are meant for Alice.

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, it should be if you use the command on the device "**`arp -a`**" and check for changes in the cache.

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

It should be.

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

It would make it more difficult for an ARP poisoning attack to happen if the site were to use HTTPS considering there are more security measures in place because traffic will be encrypted then.