

Author: Kyle Machalec

Execution:

- a. What is Kali's main interface's MAC address? (The main interface is probably called eth0, but check ifconfig to be sure.)
 - i. 00:0c:29:98:6a:a8
- b. What is Kali's main interface's IP address?
 - i. 192.168.234.128
- c. What is Metasploitable's main interface's MAC address?
 - i. 00:0c:29:b1:2d:39
- d. What is Metasploitable's main interface's IP address?
 - i. 192.168.234.129
- 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)-[~/Downloads]
$ netstat -r
Kernel IP routing table
Destination        Gateway            Genmask           Flags     MSS Window  irtt Iface
default            192.168.234.2     0.0.0.0           UG        0  0        0 eth0
192.168.234.0      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)-[~/Downloads]
$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.234.254          ether    00:50:56:e8:0d:50   C                 eth0
192.168.234.2            ether    00:50:56:f4:7a:e1   C                 eth0
```

- g. Show Metasploitable's routing table.

```
msfadmin@metasploitable:~$ netstat -r
Kernel IP routing table
Destination        Gateway            Genmask           Flags     MSS Window  irtt Iface
192.168.234.0      *                  255.255.255.0     U         0  0        0 eth0
default            192.168.234.2     0.0.0.0           UG        0  0        0 eth0
```

- h. Show Metasploitable's ARP cache.

```
msfadmin@metasploitable:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.234.2            ether    00:50:56:f4:7a:e1   C                 eth0
192.168.234.128          ether    00:0c:29:98:6a:a8   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.
 - i. By checking in the Metasploitable routing table, you can find the IP address of the "gateway" to the internet, which would be 192.168.234.2 in this case. This gateway is the first destination of the TCP SYN packet. Then, in the

Metasploitable ARP cache, you can look for the MAC address associated with the IP address of the gateway, which is 00:50:56:F4:7A:E1.

- 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. I can see an HTTP response on Metasploitable, which is the HTML source code of <http://cs338.jeffondich.com/>. I do not see any 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:
 - i. Start sniffing (not bridged sniffing) on eth0
 - ii. Scan for Hosts
 - iii. View the Hosts list
 - iv. Select your Metasploit VM from the Host List
 - v. Add that host as Target 1
 - vi. Start ARP Poisoning (including Sniff Remote Connections)
 - vii. Do your stuff with wireshark and Metasploitable
 - viii. Stop ARP Poisoning

DONE

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

192.168.234.254 and 192.168.234.1 have been added to the ARP cache. All of the MAC addresses have been changed to Kali's MAC address (00:0c:29:98:6a:a8)

```
msfadmin@metasploitable:~$ arp
Address          HWtype  HWaddress      Flags Mask    Iface
192.168.234.1    ether   00:0C:29:98:6A:A8  C             eth0
192.168.234.254  ether   00:0C:29:98:6A:A8  C             eth0
192.168.234.2    ether   00:0C:29:98:6A:A8  C             eth0
192.168.234.128  ether   00:0C:29:98:6A:A8  C             eth0
```

- 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. I predict that Metasploitable will send the TCP SYN packet to Kali's MAC address (00:0c:29:98:6a:a8). This is because Metasploitable's ARP cache replaced the gateway's MAC address with Kali's MAC address, effectively letting Kali place itself in the middle between Metasploitable and the gateway.
- n. Start Wireshark capturing "tcp port http" again.
 - i. 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. I can now see packets sent between Metasploitable and cs338.jeffondich.com. I can see that Metasploitable sent an HTTP request to cs338.jeffondich.com and then cs338.jeffondich.com sent an HTTP response back to Metasploitable. I can see everything within the HTTP response (screenshot below).

http						
No.	Time	Source	Destination	Protocol	Length	Info
6	0.064052315	192.168.234.129	45.79.89.123	HTTP	212	GET / HTTP/1.1
11	0.124009930	45.79.89.123	192.168.234.129	HTTP	785	HTTP/1.1 200 OK (text/html)

▶ Frame 11: 785 bytes on wire (6280 bits), 785 bytes captured (6280 bits) on interface eth0, id 0

▶ Ethernet II, Src: VMware_f4:7a:e1 (00:50:56:f4:7a:e1), Dst: VMware_98:6a:a8 (00:0c:29:98:6a:a8)

▶ Internet Protocol Version 4, Src: 45.79.89.123, Dst: 192.168.234.129

▶ Transmission Control Protocol, Src Port: 80, Dst Port: 48888, Seq: 1, Ack: 159, Len: 731

▼ Hypertext Transfer Protocol

▶ HTTP/1.1 200 OK\r\n

Server: nginx/1.18.0 (Ubuntu)\r\n

Date: Sun, 29 Oct 2023 23:57:01 GMT\r\n

Content-Type: text/html\r\n

▶ Content-Length: 484\r\n

Last-Modified: Mon, 04 Apr 2022 14:10:51 GMT\r\n

Connection: keep-alive\r\n

ETag: "624afc6b-1e4"\r\n

Accept-Ranges: bytes\r\n

\r\n

[HTTP response 1/1]

[Time since request: 0.059957615 seconds]

[Request in frame: 6]

[Request URI: http://cs338.jeffondich.com/]

File Data: 484 bytes

▶ Line-based text data: text/html (17 lines)

- 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.)

- i. Kali sent ARP packets to the 4 different MAC addresses on Metasploitable, telling them that the IP addresses 192.168.234.1, 192.168.234.2, 192.168.234.254, and 192.168.234.128 have Kali's MAC address (00:0c:29:98:6a:a8). This can be seen in the screenshot below.

No.	Time	Source	Destination	Protocol	Length	Info
36	50.195859714	VMware_98:6a:a8	VMware_c0:00:08	ARP	42	192.168.234.129 is at 00:0c:29:98:6a:a8 (duplicate use of 192.168.234.1 detected!)
37	59.917189444	VMware_98:6a:a8	VMware_f4:7a:e1	ARP	42	Who has 192.168.234.2? Tell 192.168.234.128
38	59.918451054	VMware_f4:7a:e1	VMware_98:6a:a8	ARP	60	192.168.234.2 is at 00:50:56:f4:7a:e1
39	60.173369604	VMware_98:6a:a8	VMware_b1:2d:39	ARP	42	Who has 192.168.234.129? Tell 192.168.234.128
40	60.174576373	VMware_b1:2d:39	VMware_98:6a:a8	ARP	60	192.168.234.129 is at 00:0c:29:b1:2d:39
41	60.207131729	VMware_98:6a:a8	VMware_b1:2d:39	ARP	42	192.168.234.254 is at 00:0c:29:98:6a:a8
42	60.207517033	VMware_98:6a:a8	VMware_e8:0d:50	ARP	42	192.168.234.129 is at 00:0c:29:98:6a:a8 (duplicate use of 192.168.234.1 detected!)
43	60.218425518	VMware_98:6a:a8	VMware_b1:2d:39	ARP	42	192.168.234.2 is at 00:0c:29:98:6a:a8
44	60.218899922	VMware_98:6a:a8	VMware_f4:7a:e1	ARP	42	192.168.234.129 is at 00:0c:29:98:6a:a8 (duplicate use of 192.168.234.2 detected!)
45	60.229759608	VMware_98:6a:a8	VMware_b1:2d:39	ARP	42	192.168.234.1 is at 00:0c:29:98:6a:a8
46	60.230104311	VMware_98:6a:a8	VMware_c0:00:08	ARP	42	192.168.234.129 is at 00:0c:29:98:6a:a8 (duplicate use of 192.168.234.1 detected!)
47	63.311704803	VMware_c0:00:08	Broadcast	ARP	60	Who has 192.168.234.2? Tell 192.168.234.1 (duplicate use of 192.168.234.1 detected!)
48	64.776371912	VMware_c0:00:08	Broadcast	ARP	60	Who has 192.168.234.2? Tell 192.168.234.1 (duplicate use of 192.168.234.1 detected!)
49	65.319625352	VMware_c0:00:08	Broadcast	ARP	60	Who has 192.168.234.2? Tell 192.168.234.1 (duplicate use of 192.168.234.1 detected!)
50	66.317803324	VMware_c0:00:08	Broadcast	ARP	60	Who has 192.168.234.2? Tell 192.168.234.1 (duplicate use of 192.168.234.1 detected!)
51	67.795222090	VMware_c0:00:08	Broadcast	ARP	60	Who has 192.168.234.2? Tell 192.168.234.1 (duplicate use of 192.168.234.1 detected!)
52	68.309381684	VMware_c0:00:08	Broadcast	ARP	60	Who has 192.168.234.2? Tell 192.168.234.1 (duplicate use of 192.168.234.1 detected!)
53	69.307466907	VMware_c0:00:08	Broadcast	ARP	60	Who has 192.168.234.2? Tell 192.168.234.1 (duplicate use of 192.168.234.1 detected!)
54	70.241497402	VMware_98:6a:a8	VMware_b1:2d:39	ARP	42	192.168.234.254 is at 00:0c:29:98:6a:a8
55	70.242993506	VMware_98:6a:a8	VMware_e8:0d:50	ARP	42	192.168.234.129 is at 00:0c:29:98:6a:a8 (duplicate use of 192.168.234.254 detected!)
56	70.253117004	VMware_98:6a:a8	VMware_b1:2d:39	ARP	42	192.168.234.2 is at 00:0c:29:98:6a:a8
57	70.253470906	VMware_98:6a:a8	VMware_f4:7a:e1	ARP	42	192.168.234.129 is at 00:0c:29:98:6a:a8 (duplicate use of 192.168.234.2 detected!)
58	70.264563064	VMware_98:6a:a8	VMware_b1:2d:39	ARP	42	192.168.234.1 is at 00:0c:29:98:6a:a8
59	70.265145168	VMware_98:6a:a8	VMware_c0:00:08	ARP	42	192.168.234.129 is at 00:0c:29:98:6a:a8 (duplicate use of 192.168.234.1 detected!)
60	70.817585341	VMware_c0:00:08	Broadcast	ARP	60	Who has 192.168.234.2? Tell 192.168.234.1 (duplicate use of 192.168.234.1 detected!)
61	71.814501659	VMware_c0:00:08	Broadcast	ARP	60	Who has 192.168.234.2? Tell 192.168.234.1 (duplicate use of 192.168.234.1 detected!)
62	72.814533921	VMware_c0:00:08	Broadcast	ARP	60	Who has 192.168.234.2? Tell 192.168.234.1 (duplicate use of 192.168.234.1 detected!)
63	73.831815823	VMware_c0:00:08	Broadcast	ARP	60	Who has 192.168.234.2? Tell 192.168.234.1 (duplicate use of 192.168.234.1 detected!)

▶ Frame 54: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0

▶ Ethernet II, Src: VMware_98:6a:a8 (00:0c:29:98:6a:a8), Dst: VMware_b1:2d:39 (00:0c:29:b1:2d:39)

▶ Address Resolution Protocol (reply)

Hardware type: Ethernet (4)

Protocol type: IPv4 (0x0800)

Hardware size: 6

Protocol size: 4

Opcode: reply (2)

Sender MAC address: VMware_98:6a:a8 (00:0c:29:98:6a:a8)

Sender IP address: 192.168.234.254

Target MAC address: VMware_b1:2d:39 (00:0c:29:b1:2d:39)

Target IP address: 192.168.234.129

- 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. The detector would monitor the ARP cache to detect if more than one IP address is mapped to the same MAC address, which if true, would be a good indicator of ARP spoofing. This method could return false positives with an outdated network configuration so that there may be old devices and old IPs/MAC addresses in the cache. The detector could also look for very repetitive ARP responses from a particular source.

Synthesis:

- a. First, Mal must be on the same network as Alice. Mal then scans the network to find IP addresses within the network. Mal starts sending ARP packets that advertise that the correct MAC address for the IP addresses is Mal's MAC address. Alice then updates her ARP cache, which essentially connects her intended recipient's IP addresses (gateways, routers, etc.) to Mal's address. As a result, when Alice wants to send a packet to Bob, she tries to first get the packet to the gateway, which just so happens to be now associated with Mal's MAC address and would therefore be sent to Mal. Mal would then be able to read, edit, or do whatever she wants with this intercepted message before passing it along to the gateway (if she wants).
- b. If Alice is monitoring her ARP cache or ARP packets, this attack is very detectable. Alice could have some ARP cache poisoning protection program installed that is set up to notice if Alice is receiving a lot of repetitive ARP packets from a particular source or if Alice's ARP cache has multiple IP addresses mapped to the same MAC address.
- c. No, the attack is not detectable from Bob's perspective. Even if Bob expects some form of authentication from Alice, it wouldn't matter to Bob if Alice sends those credentials or if Mal passes on those credentials to Bob after intercepting them from Alice.
- d. Yes, it is likely that Alice and Bob could prevent this attack with HTTPS because when Alice requests a certificate from the server, Mal would have to somehow send back a valid certificate. If the certificate is invalid, the main thing Mal could do is use SSLStrip, which will still provide Alice with one notification that the certificate is invalid. However, if Alice chooses to ignore that notification, then Mal could successfully pull off the attack.