Authors: Anders Shenholm and Riaz Kelly

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

   08:00:27:59:7a:bb

2. What is Kali's main interface's IP address?

   10.0.2.15

3. What is Metasploitable's main interface's MAC address?

   08:00:27:18:25:1d

4. What is Metasploitable's main interface's IP address?

   10.0.2.5

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

```
└─$ netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
0.0.0.0         10.0.2.1        0.0.0.0         UG        0 0          0 eth0
10.0.2.0        0.0.0.0         255.255.255.0   U         0 0          0 eth0
```

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

```
└─$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
10.0.2.3                 ether   08:00:27:11:d9:1f   C                     eth0
10.0.2.1                 ether   52:54:00:12:35:00   C                     eth0
```

7. Show Metasploitable's routing table.

```
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
10.0.2.0        *               255.255.255.0   U         0 0          0 eth0
default         10.0.2.1        0.0.0.0         UG        0 0          0 eth0
```

8. Show Metasploitable's ARP cache.

```
Address                  HWtype  HWaddress           Flags Mask            Iface
10.0.2.1                 ether   52:54:00:12:35:00   C                     eth0
10.0.2.3                 ether   08:00:27:11:D9:1F   C                     eth0
```

9. Suppose the user of Metasploitable wants to get the CS231 sandbox page via the command "curl http://cs231.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 initial packet to 08:00:27:18:25:1d as this MAC address corresponds to the IP address of the main interface (10.0.2.5).

10. Fire up Wireshark on Kali. Start capturing packets for "tcp port http". On Metasploitable, execute "curl http://cs231.jeffondich.com/". On Kali, stop capturing. Do you see an HTTP response on Metasploitable? Do you see any captured packets in Wireshark on Kali?

    Wireshark didn't capture anything. Metasploitable doesn't show an HTTP response, just the HTML from the page.

(Start poisoning)

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

Now the ARP cache includes another IP destination, but now all IP destinations correspond to a new, different MAC address.

```
msfadmin@metasploitable:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
10.0.2.3                 ether   08:00:27:59:7A:BB   C                     eth0
10.0.2.2                 ether   08:00:27:59:7A:BB   C                     eth0
10.0.2.1                 ether   08:00:27:59:7A:BB   C                     eth0
```

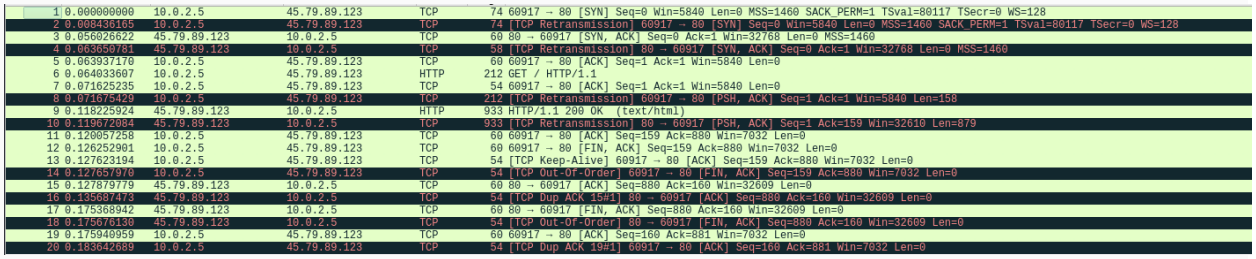
12. If you execute "curl http://cs231.jeffondich.com/" on Metasploitable now, to what MAC address will Metasploitable send the TCP SYN packet? Explain why.

Metasploitable will now send the TCP SYN packet to the MAC address of Kali's main interface (08:00:27:59:7a:bb). This is because this is where Ettercap is running.

13. Start Wireshark capturing "tcp port http" again.
14. Execute "curl http://cs231.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 cs231.jeffondich.com?

Metasploitable gave the same response as before, just a page of html.

Wireshark captured these frames. It shows TCP retransmissions between Metasploitable and cs231.jeffondich.com, indicating that packets were lost in the network connection. However, the network basically did its job and the interaction was effectively the same for Metasploitable as it returned the same result. However, we were able to eavesdrop on the interaction. We observed the TCP handshake. Also, Cs231.jeffondich.com gave an HTTP response (frame 9) though again this wasn't visible in the response Metasploitable received.



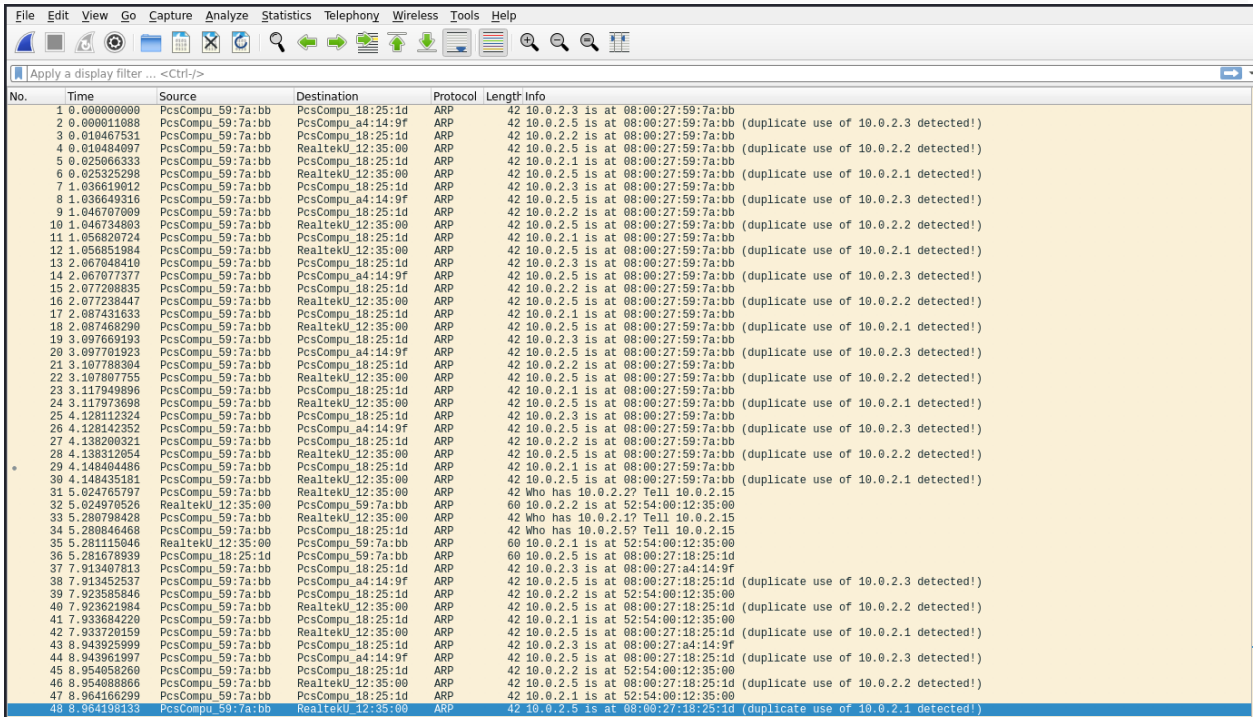
| | | | | | |
|---|---|---|---|---|---|
| 1 | 0.000000000 | 10.0.2.5 | 45.79.89.123 | TCP | 74 60917 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=80117 TSecr=0 WS=128 |
| 2 | 0.008436165 | 10.0.2.5 | 45.79.89.123 | TCP | 74 [TCP Retransmission] 60917 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=80117 TSecr=0 WS=128 |
| 3 | 0.056026622 | 45.79.89.123 | 10.0.2.5 | TCP | 60 80 → 60917 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460 |
| 4 | 0.063650781 | 45.79.89.123 | 10.0.2.5 | TCP | 58 [TCP Retransmission] 80 → 60917 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460 |
| 5 | 0.063937170 | 10.0.2.5 | 45.79.89.123 | TCP | 60 60917 → 80 [ACK] Seq=1 Ack=1 Win=5840 Len=0 |
| 6 | 0.064033607 | 10.0.2.5 | 45.79.89.123 | HTTP | 212 GET / HTTP/1.1 |
| 7 | 0.071625235 | 10.0.2.5 | 45.79.89.123 | TCP | 54 60917 → 80 [ACK] Seq=1 Ack=1 Win=5840 Len=0 |
| 8 | 0.071675429 | 10.0.2.5 | 45.79.89.123 | TCP | 212 [TCP Retransmission] 60917 → 80 [PSH, ACK] Seq=1 Ack=1 Win=5840 Len=158 |
| 9 | 0.118225924 | 45.79.89.123 | 10.0.2.5 | HTTP | 933 HTTP/1.1 200 OK  (text/html) |
| 10 | 0.119572894 | 45.79.89.123 | 10.0.2.5 | TCP | 933 [TCP Retransmission] 80 → 60917 [PSH, ACK] Seq=1 Ack=159 Win=32610 Len=879 |
| 11 | 0.120057258 | 10.0.2.5 | 45.79.89.123 | TCP | 60 60917 → 80 [ACK] Seq=159 Ack=880 Win=7032 Len=0 |
| 12 | 0.126252901 | 10.0.2.5 | 45.79.89.123 | TCP | 60 60917 → 80 [FIN, ACK] Seq=159 Ack=880 Win=7032 Len=0 |
| 13 | 0.127623194 | 10.0.2.5 | 45.79.89.123 | TCP | 54 [TCP Keep-Alive] 60917 → 80 [ACK] Seq=159 Ack=880 Win=7032 Len=0 |
| 14 | 0.127657970 | 10.0.2.5 | 45.79.89.123 | TCP | 54 [TCP Out-Of-Order] 60917 → 80 [FIN, ACK] Seq=159 Ack=880 Win=7032 Len=0 |
| 15 | 0.127879779 | 45.79.89.123 | 10.0.2.5 | TCP | 60 80 → 60917 [ACK] Seq=880 Ack=160 Win=32609 Len=0 |
| 16 | 0.135687473 | 45.79.89.123 | 10.0.2.5 | TCP | 54 [TCP Dup ACK 15#1] 80 → 60917 [ACK] Seq=880 Ack=160 Win=32609 Len=0 |
| 17 | 0.175368942 | 45.79.89.123 | 10.0.2.5 | TCP | 60 80 → 60917 [FIN, ACK] Seq=880 Ack=160 Win=32609 Len=0 |
| 18 | 0.175570130 | 45.79.89.123 | 10.0.2.5 | TCP | 54 [TCP Out-Of-Order] 80 → 60917 [FIN, ACK] Seq=880 Ack=160 Win=32609 Len=0 |
| 19 | 0.175940959 | 10.0.2.5 | 45.79.89.123 | TCP | 60 60917 → 80 [ACK] Seq=160 Ack=881 Win=7032 Len=0 |
| 20 | 0.183642689 | 10.0.2.5 | 45.79.89.123 | TCP | 54 [TCP Dup ACK 19#1] 60917 → 80 [ACK] Seq=160 Ack=881 Win=7032 Len=0 |

15. 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 PITM/MITM 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 so that every IP address was associated with the same HWaddress, which was Kali's main interface's MAC address. This change meant that the TCP handshake packets were first sent to Kali instead of Metasploitable's main interface's MAC address.

16. 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.)

To notice the version of ARP spoofing like what we did, it would have to recognize if multiple IP addresses mapped to the same hardware address. To avoid false positives of this type, it would need to have a memory of the MAC addresses which are distributed among multiple IP addresses on the local network.



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1 | 0.000000000 | PcsCompu_59:7a:bb | PcsCompu_18:25:1d | ARP | 42 | 10.0.2.3 is at 08:00:27:59:7a:bb |
| 2 | 0.000011088 | PcsCompu_59:7a:bb | PcsCompu_a4:14:9f | ARP | 42 | 10.0.2.5 is at 08:00:27:59:7a:bb (duplicate use of 10.0.2.3 detected!) |
| 3 | 0.010467531 | PcsCompu_59:7a:bb | PcsCompu_18:25:1d | ARP | 42 | 10.0.2.2 is at 08:00:27:59:7a:bb |
| 4 | 0.010484097 | PcsCompu_59:7a:bb | RealtekU_12:35:00 | ARP | 42 | 10.0.2.5 is at 08:00:27:59:7a:bb (duplicate use of 10.0.2.2 detected!) |
| 5 | 0.025066333 | PcsCompu_59:7a:bb | PcsCompu_18:25:1d | ARP | 42 | 10.0.2.1 is at 08:00:27:59:7a:bb |
| 6 | 0.025325298 | PcsCompu_59:7a:bb | RealtekU_12:35:00 | ARP | 42 | 10.0.2.5 is at 08:00:27:59:7a:bb (duplicate use of 10.0.2.1 detected!) |
| 7 | 1.036619012 | PcsCompu_59:7a:bb | PcsCompu_18:25:1d | ARP | 42 | 10.0.2.3 is at 08:00:27:59:7a:bb |
| 8 | 1.036649316 | PcsCompu_59:7a:bb | PcsCompu_a4:14:9f | ARP | 42 | 10.0.2.5 is at 08:00:27:59:7a:bb (duplicate use of 10.0.2.3 detected!) |
| 9 | 1.046707009 | PcsCompu_59:7a:bb | PcsCompu_18:25:1d | ARP | 42 | 10.0.2.2 is at 08:00:27:59:7a:bb |
| 10 | 1.046734803 | PcsCompu_59:7a:bb | RealtekU_12:35:00 | ARP | 42 | 10.0.2.5 is at 08:00:27:59:7a:bb (duplicate use of 10.0.2.2 detected!) |
| 11 | 1.056820724 | PcsCompu_59:7a:bb | PcsCompu_18:25:1d | ARP | 42 | 10.0.2.1 is at 08:00:27:59:7a:bb |
| 12 | 1.056851984 | PcsCompu_59:7a:bb | RealtekU_12:35:00 | ARP | 42 | 10.0.2.5 is at 08:00:27:59:7a:bb (duplicate use of 10.0.2.1 detected!) |
| 13 | 2.067048410 | PcsCompu_59:7a:bb | PcsCompu_18:25:1d | ARP | 42 | 10.0.2.3 is at 08:00:27:59:7a:bb |
| 14 | 2.067077377 | PcsCompu_59:7a:bb | PcsCompu_a4:14:9f | ARP | 42 | 10.0.2.5 is at 08:00:27:59:7a:bb (duplicate use of 10.0.2.3 detected!) |
| 15 | 2.077208835 | PcsCompu_59:7a:bb | PcsCompu_18:25:1d | ARP | 42 | 10.0.2.2 is at 08:00:27:59:7a:bb |
| 16 | 2.077238447 | PcsCompu_59:7a:bb | RealtekU_12:35:00 | ARP | 42 | 10.0.2.5 is at 08:00:27:59:7a:bb (duplicate use of 10.0.2.2 detected!) |
| 17 | 2.087431633 | PcsCompu_59:7a:bb | PcsCompu_18:25:1d | ARP | 42 | 10.0.2.1 is at 08:00:27:59:7a:bb |
| 18 | 2.087468290 | PcsCompu_59:7a:bb | RealtekU_12:35:00 | ARP | 42 | 10.0.2.5 is at 08:00:27:59:7a:bb (duplicate use of 10.0.2.1 detected!) |
| 19 | 3.097669193 | PcsCompu_59:7a:bb | PcsCompu_18:25:1d | ARP | 42 | 10.0.2.3 is at 08:00:27:59:7a:bb |
| 20 | 3.097701923 | PcsCompu_59:7a:bb | PcsCompu_a4:14:9f | ARP | 42 | 10.0.2.5 is at 08:00:27:59:7a:bb (duplicate use of 10.0.2.3 detected!) |
| 21 | 3.107788304 | PcsCompu_59:7a:bb | PcsCompu_18:25:1d | ARP | 42 | 10.0.2.2 is at 08:00:27:59:7a:bb |
| 22 | 3.107807755 | PcsCompu_59:7a:bb | RealtekU_12:35:00 | ARP | 42 | 10.0.2.5 is at 08:00:27:59:7a:bb (duplicate use of 10.0.2.2 detected!) |
| 23 | 3.117949896 | PcsCompu_59:7a:bb | PcsCompu_18:25:1d | ARP | 42 | 10.0.2.1 is at 08:00:27:59:7a:bb |
| 24 | 3.117973698 | PcsCompu_59:7a:bb | RealtekU_12:35:00 | ARP | 42 | 10.0.2.5 is at 08:00:27:59:7a:bb (duplicate use of 10.0.2.1 detected!) |
| 25 | 4.128112324 | PcsCompu_59:7a:bb | PcsCompu_18:25:1d | ARP | 42 | 10.0.2.3 is at 08:00:27:59:7a:bb |
| 26 | 4.128142352 | PcsCompu_59:7a:bb | PcsCompu_a4:14:9f | ARP | 42 | 10.0.2.5 is at 08:00:27:59:7a:bb (duplicate use of 10.0.2.3 detected!) |
| 27 | 4.138200321 | PcsCompu_59:7a:bb | PcsCompu_18:25:1d | ARP | 42 | 10.0.2.2 is at 08:00:27:59:7a:bb |
| 28 | 4.138312054 | PcsCompu_59:7a:bb | RealtekU_12:35:00 | ARP | 42 | 10.0.2.5 is at 08:00:27:59:7a:bb (duplicate use of 10.0.2.2 detected!) |
| 29 | 4.148404486 | PcsCompu_59:7a:bb | PcsCompu_18:25:1d | ARP | 42 | 10.0.2.1 is at 08:00:27:59:7a:bb |
| 30 | 4.148435181 | PcsCompu_59:7a:bb | RealtekU_12:35:00 | ARP | 42 | 10.0.2.5 is at 08:00:27:59:7a:bb (duplicate use of 10.0.2.1 detected!) |
| 31 | 5.024765797 | PcsCompu_59:7a:bb | RealtekU_12:35:00 | ARP | 42 | Who has 10.0.2.2? Tell 10.0.2.15 |
| 32 | 5.024970526 | RealtekU_12:35:00 | PcsCompu_59:7a:bb | ARP | 60 | 10.0.2.2 is at 52:54:00:12:35:00 |
| 33 | 5.280798428 | PcsCompu_59:7a:bb | RealtekU_12:35:00 | ARP | 42 | Who has 10.0.2.1? Tell 10.0.2.15 |
| 34 | 5.280846468 | PcsCompu_59:7a:bb | PcsCompu_18:25:1d | ARP | 42 | Who has 10.0.2.5? Tell 10.0.2.15 |
| 35 | 5.281115046 | RealtekU_12:35:00 | PcsCompu_59:7a:bb | ARP | 60 | 10.0.2.1 is at 52:54:00:12:35:00 |
| 36 | 5.281678939 | PcsCompu_18:25:1d | PcsCompu_59:7a:bb | ARP | 60 | 10.0.2.5 is at 08:00:27:18:25:1d |
| 37 | 7.913407813 | PcsCompu_59:7a:bb | PcsCompu_18:25:1d | ARP | 42 | 10.0.2.3 is at 08:00:27:a4:14:9f |
| 38 | 7.913452537 | PcsCompu_59:7a:bb | PcsCompu_a4:14:9f | ARP | 42 | 10.0.2.5 is at 08:00:27:18:25:1d (duplicate use of 10.0.2.3 detected!) |
| 39 | 7.923585846 | PcsCompu_59:7a:bb | PcsCompu_18:25:1d | ARP | 42 | 10.0.2.2 is at 52:54:00:12:35:00 |
| 40 | 7.923621984 | PcsCompu_59:7a:bb | RealtekU_12:35:00 | ARP | 42 | 10.0.2.5 is at 08:00:27:18:25:1d (duplicate use of 10.0.2.2 detected!) |
| 41 | 7.933684220 | PcsCompu_59:7a:bb | PcsCompu_18:25:1d | ARP | 42 | 10.0.2.1 is at 52:54:00:12:35:00 |
| 42 | 7.933720159 | PcsCompu_59:7a:bb | RealtekU_12:35:00 | ARP | 42 | 10.0.2.5 is at 08:00:27:18:25:1d (duplicate use of 10.0.2.1 detected!) |
| 43 | 8.943925999 | PcsCompu_59:7a:bb | PcsCompu_18:25:1d | ARP | 42 | 10.0.2.3 is at 08:00:27:a4:14:9f |
| 44 | 8.943961997 | PcsCompu_59:7a:bb | PcsCompu_a4:14:9f | ARP | 42 | 10.0.2.5 is at 08:00:27:18:25:1d (duplicate use of 10.0.2.3 detected!) |
| 45 | 8.954058260 | PcsCompu_59:7a:bb | PcsCompu_18:25:1d | ARP | 42 | 10.0.2.2 is at 52:54:00:12:35:00 |
| 46 | 8.954088866 | PcsCompu_59:7a:bb | RealtekU_12:35:00 | ARP | 42 | 10.0.2.5 is at 08:00:27:18:25:1d (duplicate use of 10.0.2.2 detected!) |
| 47 | 8.964166299 | PcsCompu_59:7a:bb | PcsCompu_18:25:1d | ARP | 42 | 10.0.2.1 is at 52:54:00:12:35:00 |
| 48 | 8.964198133 | PcsCompu_59:7a:bb | RealtekU_12:35:00 | ARP | 42 | 10.0.2.5 is at 08:00:27:18:25:1d (duplicate use of 10.0.2.1 detected!) |