Soren DeHaan and Carl Tankersley

a. What is Kali's main interface's MAC address? (The main interface is probably called eth0, but check ifconfig to be sure.)
    - Using command “ifconfig -a”, 08:00:27:61:6a:17 seems to be the MAC address

b. What is Kali's main interface's IP address?
    - Using command “ip -4 a”, 10.0.2.15 seems to be the IP address

c. What is Metasploitable's main interface's MAC address?
    - Using command “ifconfig -a”, 08:00:27:82:78:fc seems to be the MAC address

d. What is Metasploitable's main interface's IP address?
    - Using command “ip -4 a”, 10.0.2.4 seems to be the IP address

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         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
    ```

f. Show Kali's ARP cache. (Use "arp" or "arp -n".)
    -
    ```
    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:a3:8c:67   C                     eth0
    ```

g. Show Metasploitable's routing table.
    -
    ```
    Kernel IP 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
    ```

h. Show Metasploitable's ARP cache.
    -
    ```
    Address                  HWtype  HWaddress           Flags Mask            Iface
    10.0.2.1                 ether   52:54:00:12:35:00   C                     eth0
    ```

i. 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.
    - Metasploitable only has one MAC address stored in the ARP cache, so it oughtta be that one

j. 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?
    - Metasploitable got an HTTP response, but Wireshark didn’t catch any of it.

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.
    - Success!

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

↔

```
Address            HWtype  HWaddress           Flags Mask            Iface
10.0.2.1           ether   08:00:27:61:6a:17   C                     eth0
```

Wouldja look at that? It's Kali!

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

↔ It will again send it to the only MAC address it knows. Which just so happens to be Kali now…

n. Start Wireshark capturing "tcp port http" again.

↔ Okay.

o. 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?

↔ Yes, we can see the captured packets! And Metasploitable receives the HTTP response as normal (so they don't know what's going on…). We can see the [SYN], [SYN, ACK], [ACK] that suggests a TCP handshake, followed by the entire HTTP response. It then ends with the standard sign-off.

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 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.)

↔ First, we set up a sniffer, and request the MAC addresses for all devices on the network. Once we've identified the target IP addresses, we send messages using Kali's MAC address, but Metasploitable's/default's IP addresses. We can then send a message to Metasploitable as if coming from the default gateway, and so it will overwrite the 'outdated' ARP cache, and route traffic to Kali as well. Likewise, Kali passes a message from Metasploitable's IP address, using Kali's MAC address, so the default gateway also routes returning traffic through Kali.

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.)

↔ If a message is coming from or going to an IP address which has multiple MAC addresses, that *probably* means that there's some ARP spoofing. However, whenever a network is getting changed, it may be possible for a MAC address to tag along with an old IP address, which could create a false positive.