Doug Pham

A. Kali's main interface's MAC address: 00:0c:29:4b:27:27
B. Kali's main interface's IP address: 192.168.133.128
C. Metasploitable's main interface's MAC address: 00:0c:29:87:a9:d4
D. Metasploitable's main interface's IP address: 192.168.133.129
E.

```
┌──(kali㉿kali)-[~]
└─$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         192.168.133.2   0.0.0.0         UG        0 0          0 eth0
192.168.133.0   0.0.0.0         255.255.255.0   U         0 0          0 eth0
```

F.

```
└─$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.133.2            ether   00:50:56:f9:21:75   C                     eth0
192.168.133.129          ether   00:0c:29:87:a9:d4   C                     eth0
192.168.133.254          ether   00:50:56:e4:31:42   C                     eth0
```

G.

```
msfadmin@metasploitable:~$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
192.168.133.0   *               255.255.255.0   U         0 0          0 eth0
default         192.168.133.2   0.0.0.0         UG        0 0          0 eth0
```

H.

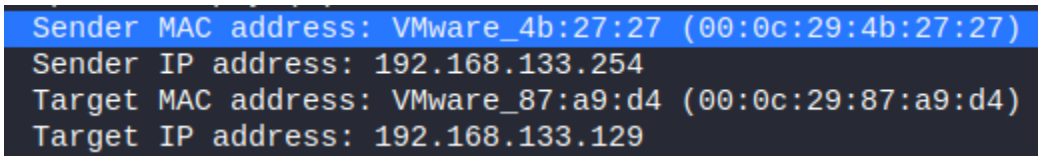
```
msfadmin@metasploitable:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.133.2            ether   00:50:56:F9:21:75   C                     eth0
192.168.133.254          ether   00:50:56:E4:31:42   C                     eth0
```

I. Metasploitable should send the packet to would be 00:50:56:F9:21:75 which is the first and MAC address on my local network
J. Yes we do see an HTTP response with the HTML of http://cs338.jeffondich.com/ and we also see the captured packets on Kali from Wireshark
L.

```
msfadmin@metasploitable:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.133.1            ether   00:0C:29:4B:27:27   C                     eth0
192.168.133.254          ether   00:0C:29:4B:27:27   C                     eth0
192.168.133.2            ether   00:0C:29:4B:27:27   C                     eth0
```

We see there are now extra addresses in the ARP cache, all of which point to the same address which is the kali MAC address.
M. I expect the TCP SYN packet to go to Kali because the MAC addresses we see in Metasploitable all point to Kali.
O. Yes we do see an HTTP response on Metasploitable. We see a lot of different captured packets in Wireshark and we see a lot of TCP protocols happening between Metasploitable and cs338.jeffondich.com.
P. We see in the image that the sender IP address is the address of Bob but then we look at the MAC address, it is Kali's MAC address. How this happens is ettercap sends ARP

messages to Metasploitable making it think it is the default gateway. This is why when we run arp on Metasploitable, we see these other addresses but they all point to Kali's MAC address.



Q. If I were designing an ARP spoofing detector, I would probably keep a legit ARP cache stored somewhere that is built over time that monitors the typical network behavior, so that if anything out of the ordinary pops up, it would know not send any data to that. The downside to this is new legit devices on the network may be detected as out of the ordinary and be excluded.

===== SYNTHESIS =====

A. Alice sends a request to the entire network asking the IP address of Bob to send its MAC address. Since the entire network gets this, typically the devices who do not have the IP address ignore it but Mal being malicious as is, can send messages to Alice making them think that Mal is the default gateway. This is where the name arp poisoning comes from as Mal poisons Alice's ARP cache and makes Alice think that Mal's MAC address is the default gateway. Hence as we saw earlier of Metasploitable's (Alice's) ARP cache was changed and all the gateways were to Kali (Mal). Now if Alice wants to send data to Bob, they send it but now Mal receives it and can do whatever with the data before sending it to Bob.

B. From Alice's perspective this is not detectable because Alice just sends the message to whatever the default gateway is which regardless if Mal gets the data or not, Bob will end up with the data. How Alice can help prevent this is by utilizing some ARP spoofing detection tools that monitor the ARP traffic and identify any potential attacks.

C. From Bob's perspective this also is not detectable since ARP spoofing typically happens on the network layer and Bob is on a higher layer than where this occurs.

D. Yes this could be detected/prevented using HTTPS because they would have that level of encryption so Mal would have more of a challenge to getting the data. Even is Mal were to successfully get in the middle of the connection, having the messages being encrypted would make it a lot more difficult to manipulate the data.