a. Kali MAC address: 00:0c:29:a3:44:78

b. Kali IP address: 192.168.52.128

c. Metasploitable MAC address: 00:0c:29:58:0d:a4

d. Metasploitable IP address: 192.168.52.129

e.

```
┌──(kali㉿kali)-[~]
└─$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         192.168.52.2    0.0.0.0         UG        0 0          0 eth0
192.168.52.0    0.0.0.0         255.255.255.0   U         0 0          0 eth0
```

f.

```
┌──(kali㉿kali)-[~]
└─$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.52.2             ether   00:50:56:e7:9b:7a   C                     eth0
192.168.52.254           ether   00:50:56:ea:ce:89   C                     eth0
192.168.52.129           ether   00:0c:29:58:0d:a4   C                     eth0
```

g.

```
msfadmin@metasploitable:~$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
192.168.52.0    *               255.255.255.0   U         0 0          0 eth0
default         192.168.52.2    0.0.0.0         UG        0 0          0 eth0
msfadmin@metasploitable:~$
```

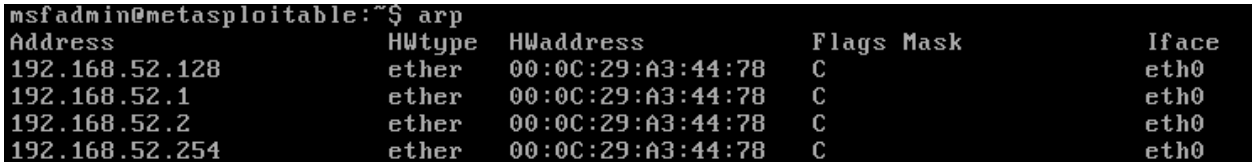
h.

```
msfadmin@metasploitable:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.52.128           ether   00:0C:29:A3:44:78   C                     eth0
192.168.52.2             ether   00:50:56:E7:9B:7A   C                     eth0
192.168.52.254           ether   00:50:56:EA:CE:89   C                     eth0
```

i. Metasploitable would send the TCP SYN packet to 00:50:56:E7:9B:7A. This is the MAC address of 192.168.52.2 which is the IP address of the first hop in the local network.

j. Metasploitable received a http response from http://cs338.jeffondich.com/ and kali was able to see all of the packages sent and received.

k.

l. 

A new IP address 192.168.52.1 has been added. Also, the MAC addresses for all 4 IP addresses are now the MAC address of IP address 192.168.52.128.

m. Now, metasploitable will probably send the TCP SYN packet to Kali as the MAC address of 192.168.52.2 has been changed to match Kali's.

n.

o. Metasploitable received the same http response as last time. Now, compared to last time, for each message sent in the conversation between Metasploitable and http://cs338.jeffondich.com/, there is an extra [TCP retransmission] packet which I'm assuming is ettercap intercepting each packet and passing it along.

p. Kali changed Metasploitable's ARP cache so that all of the MAC addresses pointed to Kali, therefore every packet that Metasploitable would send out would first go to Kali.

q. My first thought was to have a system to detect if multiple IP addresses have the same MAC address but that doesn't work since this is already allowed and used. https://www.quora.com/Can-one-MAC-address-have-multiple-IP-addresses. Another system could be to detect if the MAC address of the first hop IP address ever changes.