Execution

a. 00:0c:29:55:8f:be
b. 192.168.116.128
c. 00:0c:29:fd:dc:75
d. 192.168.116.129
e.

```
┌──(kali㉿kali)-[~]
└─$ netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Ifac
e
0.0.0.0         192.168.116.2   0.0.0.0         UG        0 0          0 eth0
192.168.116.0   0.0.0.0         255.255.255.0   U         0 0          0 eth0
```

f.

```
┌──(kali㉿kali)-[~]
└─$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.116.2            ether   00:50:56:f6:c9:ce   C                     eth0
```

g.

```
msfadmin@metasploitable:~$ netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
192.168.116.0   0.0.0.0         255.255.255.0   U         0 0          0 eth0
0.0.0.0         192.168.116.2   0.0.0.0         UG        0 0          0 eth0
msfadmin@metasploitable:~$
```

h.

```
msfadmin@metasploitable:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.116.2            ether   00:50:56:F6:C9:CE   C                     eth0
msfadmin@metasploitable:~$
```

i. Metasploitable needs to access the internet, and thus exit the current network. So, it checks the IP routing table and sees the Gateway IP it wants to send to. Then, it checks the ARP cache to find the MAC address of that IP. It sends the TCP SYN packet to this MAC
j. Yes. Metasploitable gets the page back, and Wireshark on Kali sees all of the messages.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.116.129	45.79.89.123	TCP	74	44484 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSval=34230 TSecr=0 WS=32
2	0.052613719	45.79.89.123	192.168.116.129	TCP	60	80 → 44484 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
3	0.052614952	192.168.116.129	45.79.89.123	TCP	60	44484 → 80 [ACK] Seq=1 Ack=1 Win=5840 Len=0
4	0.053228707	192.168.116.129	45.79.89.123	HTTP	212	GET / HTTP/1.1
5	0.053228957	45.79.89.123	192.168.116.129	TCP	60	80 → 44484 [ACK] Seq=1 Ack=159 Win=64240 Len=0
6	0.106209771	45.79.89.123	192.168.116.129	HTTP	785	HTTP/1.1 200 OK (text/html)
7	0.106210983	192.168.116.129	45.79.89.123	TCP	60	44484 → 80 [ACK] Seq=159 Ack=732 Win=6579 Len=0
8	0.123598794	192.168.116.129	45.79.89.123	TCP	60	44484 → 80 [FIN, ACK] Seq=159 Ack=732 Win=6579 Len=0
9	0.123725426	45.79.89.123	192.168.116.129	TCP	60	80 → 44484 [ACK] Seq=732 Ack=160 Win=64239 Len=0
10	0.175690695	45.79.89.123	192.168.116.129	TCP	60	80 → 44484 [FIN, PSH, ACK] Seq=732 Ack=160 Win=64239 Len=0
11	0.175691266	192.168.116.129	45.79.89.123	TCP	60	44484 → 80 [ACK] Seq=160 Ack=733 Win=6579 Len=0

k. done

l. All IPs now route to the MAC address of kali. Additionally, several new IPs have been added.

```
msfadmin@metasploitable:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.116.2            ether   00:0C:29:55:8F:BE   C                     eth0
192.168.116.128          ether   00:0C:29:55:8F:BE   C                     eth0
192.168.116.254          ether   00:0C:29:55:8F:BE   C                     eth0
192.168.116.1            ether   00:0C:29:55:8F:BE   C                     eth0
msfadmin@metasploitable:~$
```

m. Metasploitable will send the tcp packet to Kali's MAC address, since it thinks Kali has the IP needed to leave the network. Kali will just forward it out of the network, so from Metasploitable's view it will still work correctly.
n. done
o. Yes, Metasploitable does get a response. We can see everything that went back and forth between Metasploitable and cs338.jeffondich.com since all traffic went though kali. However, we could have seen it all anyway since it's unencrypted traffic on the network.
p. Kali repeatedly sent messages claiming that it had each IP on the network, and told Metasploitable to send packets to its own (Kali's) MAC address. Since the actual owner of the IP only sends ARP messages every minute or so, Metasploitable's most recent information was the Kali had the IP. So when Metasploitable needed to send a packet outside of the network, it knew the correct IP to send it to, but thought Kali's MAC address had that IP when it didn't.
q. -Check for overly frequent arp messages
-Check for one MAC address claiming many IPs (though this could happen legitimately)
-Check ARP messages not meant for you to see if someone else is claiming your IP address
-Check network traffic to see if your messages are being redirected before leaving the network (as wireshark already tells us)

Synthesis

a. Mal told Alice (and everyone else) that all internet packets should go through Mal, by claiming to be the owner of all IPs on the network. So, when Alice decides to send TCP packets for a webpage request, she checks where to send the packets to access outside of the network (the internet). She thinks Mal owns the IP address for that, so she sent her packets to Mal's MAC address. Mal reads them before passing them on.
b. Yes. Mal was sending out ARP messages claiming IPs way more often then it usually should, and every IP on the network was being claimed by one MAC address. If Alice keeps track of recent ARP messages, she could notice something is not right. But with that said, nothing "goes wrong"--she still gets the webpage back, and if you aren't monitoring network traffic or your own ARP table then you wouldn't notice anything wrong.
c. No. The packets Bob receives won't even contain information about what MAC addresses the packet passed through, only the most recent one to touch it. Bob see's Alice's IP, which is correct, and doesn't know about Mal at all.
d. Kind of. When Alice and Bob do a DHE or similar, Mal has two options. Either they can just pass the packets along, in which case they won't be able to read future messages, or they can

be an attacker in the middle. They can interfere and get different key pairs with each of Alice and Bob, but if Alice sends a challenge to Bob with a random number R, when Bob responds with E(H(S|P_B)) where S is what Bob thinks the shared secret is, Alice will realize someone is listening, since Alice and Mal agreed on a different S than Bob and Mal.

Also, if Alice realizes Mal is ARP poisoning, she may be able to ignore ARP messages from Mal's MAC address and use what she previously thought the correct MAC to send to was.