Zack Johnson

a. 00:0c:29:9a:39:16 - (Kali eth0 MAC)
b. 192.168.231.128 - (Kali eth0 IP)
c. 00:0c:29:bf:21:9f - (Meta eth0 MAC)
d. 192.168.231.129 - (Meta etho IP)
e. Kali Routing Table:

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         192.168.231.2   0.0.0.0         UG        0 0          0 eth0
192.168.231.0   0.0.0.0         255.255.255.0   U         0 0          0 eth0
```

f. Kali ARP cache:

```
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.231.2            ether   00:50:56:e2:88:cb   C                     eth0
192.168.231.254          ether   00:50:56:e2:e2:2a   C                     eth0
192.168.231.129          ether   00:0c:29:bf:21:9f   C                     eth0
```

g. Meta Routing Table:

```
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
192.168.231.0   *               255.255.255.0   U         0 0          0 eth0
default         192.168.231.2   0.0.0.0         UG        0 0          0 eth0
```

h. Meta ARP cache:

```
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.231.128          ether   00:0C:29:9A:E9:16   C                     eth0
192.168.231.2            ether   00:50:56:E2:88:CB   C                     eth0
```

i. Since cs338.jeffondich.com is not on my local network it would have an IP address that is not of the form: 192.168.231.xx so metasploitable would find the default case in the Routing table. Thus, it would look for the gateway at 192.168.231.2. It would then look that IP up in the ARP Cache and find the MAC address: 00:50:56:E2:88:CB. This is where it would send its first packet.
j. We got the HTTP response containing the HTML of the web page on Metasploitble. I also see a full TCP communication on wireshark in Kali (TCP handshake, GET request, response and ACKs, and Connection closing packets).
k.
l. New ARP cache on Metasploitable:

```
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.231.128          ether   00:0C:29:9A:E9:16   C                     eth0
192.168.231.1            ether   00:0C:29:9A:E9:16   C                     eth0
192.168.231.2            ether   00:0C:29:9A:E9:16   C                     eth0
192.168.231.254          ether   00:0C:29:9A:E9:16   C                     eth0
```

All of the MAC addresses have been replaced by the address of Kali.
m. It will still (correctly) choose the IP of the gateway as the target it wishes to send to, but when it goes to lookup its MAC address it will instead get that of Kali so it will send the packet to Kali rather than the Gateway.
n.
o. I still see the HTTP response including the correct HTML contents, but now wireshark has double the packets, one set for the connection between metasploitable and kali and

another for Kali to the actual webpage. I can also read the contents through wireshark on Kali.

p. It looks like Ettercap on kali is just spamming ARP packets that all say: “this IP is at my MAC address” for all the IPs on the local network. It seems to be sending them indiscriminately to all the other machines. This eventually convinces the other machines to change their ARP caches to match this state of affairs.
q. I think the best thing would be to detect repetition in one’s own ARP cache. If there are multiple IPs mapped to the same MAC address that might be an early indication that something is up. This would trip a false positive if an IP is legitimately changed since the new and old IPs would temporarily point to the same MAC address, but it might be worth notifying an admin or some other process that would have information on if such re-configuration is going on.