Kiefer Lord
20 May 2022

a. 00:0c:29:29:c5:5e
b. 172.16.191.128
c. 00:0c:29:b7:09:c2
d. 172.16.191.129
e.
Kernel IP routing table

Destination	Gateway	Genmask	Flags	MSS	Window	irtt	Iface
default	172.16.191.2	0.0.0.0	UG	0	0	0	eth0
172.16.191.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0

f.

Address	HWtype	HWaddress	Flags	Mask	Iface
172.16.191.2	ether	00:50:56:e6:13:87	C		eth0
172.16.191.129	ether	00:0c:29:b7:09:c2	C		eth0
172.16.191.254	ether	00:50:56:f4:22:d9	C		eth0

g.

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
172.16.191.0    *               255.255.255.0   U         0 0          0 eth0
default         172.16.191.2    0.0.0.0         UG        0 0          0 eth0
```

h.

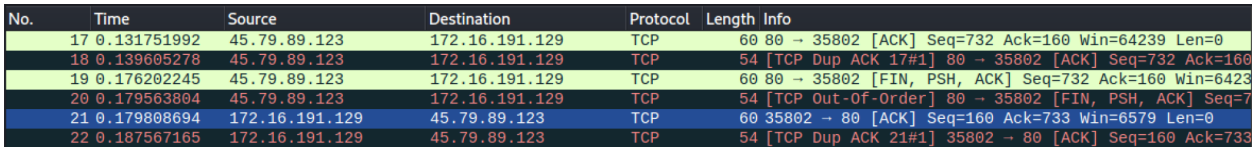
```
Address                  HWtype  HWaddress           Flags Mask            Iface
172.16.191.2             ether   00:50:56:E6:13:87   C                     eth0
172.16.191.128           ether   00:0C:29:29:C5:5E   C                     eth0
```

i. It should send the SYN packet to the gateway's MAC address, so the gateway can send the packet along to the cs338 server.
j. No packets were captured in Wireshark, but there was an HTML response.
k. Nothing to answer
l. It changed all MAC addresses to the Kali machine's MAC address

```
Address                  HWtype  HWaddress           Flags Mask            Iface
172.16.191.1             ether   00:0C:29:29:C5:5E   C                     eth0
172.16.191.254           ether   00:0C:29:29:C5:5E   C                     eth0
172.16.191.128           ether   00:0C:29:29:C5:5E   C                     eth0
172.16.191.2             ether   00:0C:29:29:C5:5E   C                     eth0
```

m. Metasploitable will send the TCP SYN packet to the Kali MAC address instead of the gateway because that is the MAC address for the gateway's IP address in the altered ARP table.
n. Nothing to answer

o. Wireshark packets:



No.	Time	Source	Destination	Protocol	Length	Info
17	0.131751992	45.79.89.123	172.16.191.129	TCP	60	80 → 35802 [ACK] Seq=732 Ack=160 Win=64239 Len=0
18	0.139605278	45.79.89.123	172.16.191.129	TCP	54	[TCP Dup ACK 17#1] 80 → 35802 [ACK] Seq=732 Ack=160
19	0.176202245	45.79.89.123	172.16.191.129	TCP	60	80 → 35802 [FIN, PSH, ACK] Seq=732 Ack=160 Win=6423
20	0.179563804	45.79.89.123	172.16.191.129	TCP	54	[TCP Out-Of-Order] 80 → 35802 [FIN, PSH, ACK] Seq=7
21	0.179808694	172.16.191.129	45.79.89.123	TCP	60	35802 → 80 [ACK] Seq=160 Ack=733 Win=6579 Len=0
22	0.187567165	172.16.191.129	45.79.89.123	TCP	54	[TCP Dup ACK 21#1] 35802 → 80 [ACK] Seq=160 Ack=733

p. The gateway does a host scan, asking every IP address for its corresponding MAC address. The Kali machine lies and says that its MAC address corresponds to every IP address, which alters the ARP caches.

q. You could detect if one MAC address is saying it corresponds to multiple IP addresses. This would prevent the Kali machine from successfully convincing other machines that it has IP addresses that it really doesn't. You would get false positives if a host truly had multiple IP addresses.