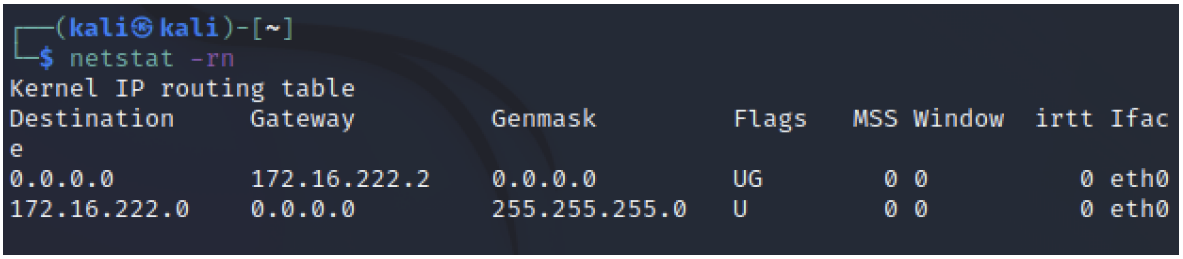
Jared Chen
5/18/2022
CS338

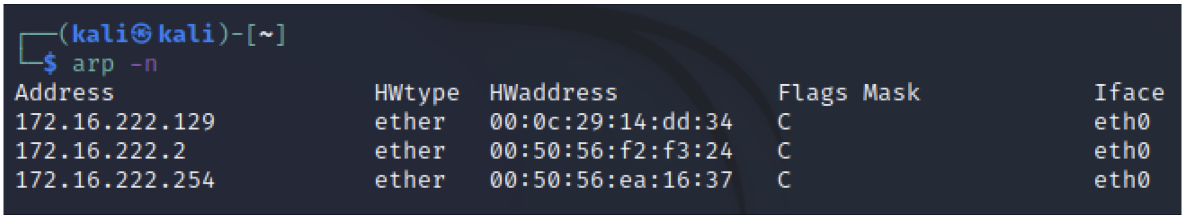
PERSON-IN-THE-MIDDLE VIA ARP SPOOFING

a. Kali MAC: 00:0c:29:38:74:c0
b. Kali IP: 172.16.222.128
c. Metasploitable MAC: 00:50:56:EA:16:37
d. Metasploitable IP: 172.16.222.129
e. Kali routing table:



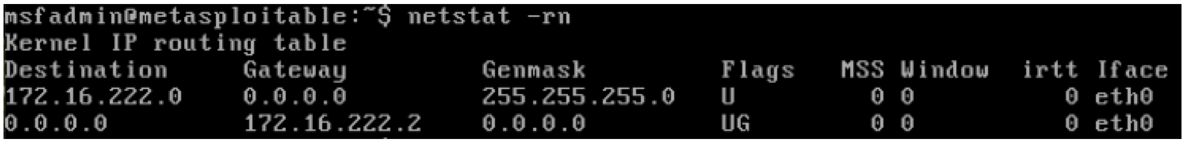
```
┌──(kali㉿kali)-[~]
└─$ netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Ifac
e
0.0.0.0         172.16.222.2    0.0.0.0         UG        0 0          0 eth0
172.16.222.0    0.0.0.0         255.255.255.0   U         0 0          0 eth0
```

f. Kali ARP cache:



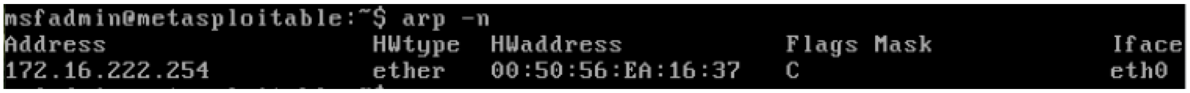
```
┌──(kali㉿kali)-[~]
└─$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
172.16.222.129           ether   00:0c:29:14:dd:34   C                     eth0
172.16.222.2             ether   00:50:56:f2:f3:24   C                     eth0
172.16.222.254           ether   00:50:56:ea:16:37   C                     eth0
```

g. Metasploitable routing table:



```
msfadmin@metasploitable:~$ netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
172.16.222.0    0.0.0.0         255.255.255.0   U         0 0          0 eth0
0.0.0.0         172.16.222.2    0.0.0.0         UG        0 0          0 eth0
```

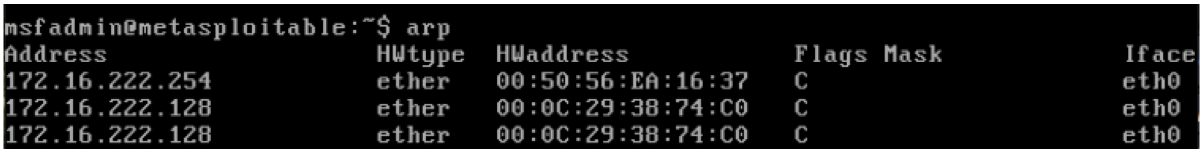
h. Metasploitable ARP cache:



```
msfadmin@metasploitable:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
172.16.222.254           ether   00:50:56:EA:16:37   C                     eth0
```

i. Metasploitable should send the TCP SYN packets to the MAC address of the machine hosting the cs338/jeffondich website. This is because the machine hosting the website is who we need to talk to in order to get that page, therefore we must send our request to that machine's MAC address.
j. While I see the HTTP response on metasploitable I do not see any captured packets in Wireshark on Kali.
k. Instruction

l. The metasploitable arp cache has changed after poisoning:



```
msfadmin@metasploitable:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
172.16.222.254           ether   00:50:56:EA:16:37   C                     eth0
172.16.222.128           ether   00:0C:29:38:74:C0   C                     eth0
172.16.222.128           ether   00:0C:29:38:74:C0   C                     eth0
```

m. Now metasploitable will send TCP SYN packets through Kali's MAC address. This is because metasploitables ARP cache has been altered such that the IP-MAC address pairing has been changed so metasploitable will send packets to Kali's MAC address instead.

n. Started wireshark

o. I see the HTTP response on metasploitable. I see the captured packets on Kali. I can inspect the packets to see what messages went between metasploitable and cs338.jeffondich.com (metasploitable request as well as server response data).

p. ARP doesn't have a way of authentication, so in our case Kali was able to answer for cs338.jeffodich and able to link the Kali MAC address to the cs338.jeffodich IP address in metasploitables ARP cache. After an IP exists within an ARP cache, the machine will look up the IP in its own cache rather than send out another ARP and wait for a reply. Therefore, metasploitable will now send its packets intended for cs338.jeffodich to Kali due to the inserted MAC address.

q. A very simple detection method would be to have some sort of notification system when the ARP cache is updated. This means potential attacks would have to be reviewed by a human, and hopefully the human wuld be able to see and deny those attacks. However this means a person needs to basically physically monitor the ARP cache whenever a change is made which isn't particularly realistic. False positives would occur when site change their IPs or MAC addresses, which can happen legitimately. Additionally, this method raises the question of how initial IP MAC parings can be added in the first place (such that we know for sure the pairing is legitimate).