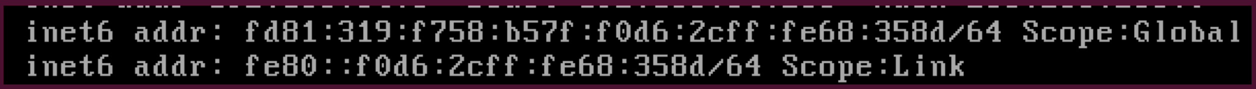
# Person-In-The-Middle Via Arp Spoofing

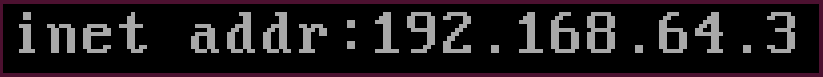
Execution

a. It is either fe80::59af:e54e:4b8e:1fd4 or fd81:319:f758:b57f:2aa2:4237:cd7d:98b6, as they're both listed.

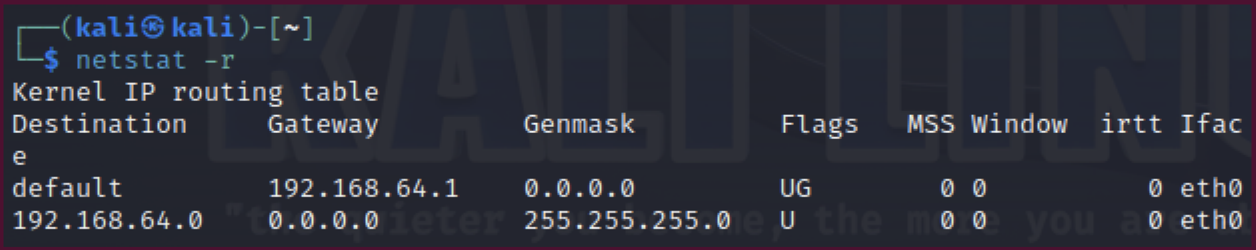
b. 192.168.64.4

c. 

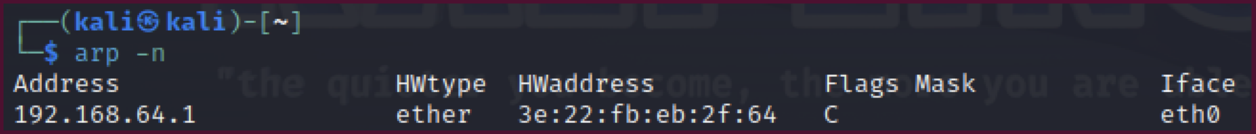
```
inet6 addr: fd81:319:f758:b57f:f0d6:2cff:fe68:358d/64 Scope:Global
inet6 addr: fe80::f0d6:2cff:fe68:358d/64 Scope:Link
```

d. 

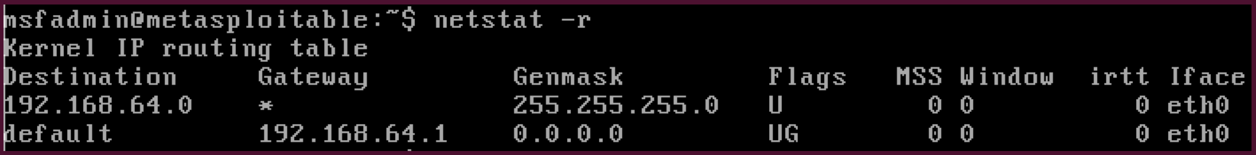
```
inet addr:192.168.64.3
```

e. 

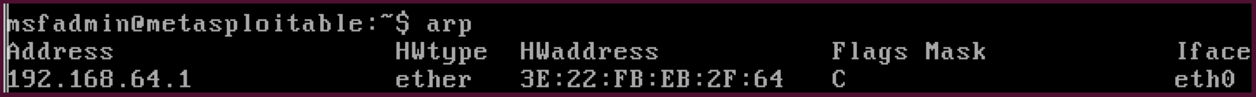
```
┌──(kali㉿kali)-[~]
└─$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Ifac
e
default         192.168.64.1    0.0.0.0         UG        0 0          0 eth0
192.168.64.0    0.0.0.0         255.255.255.0   U         0 0          0 eth0
```

f. 

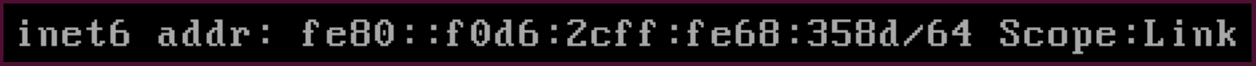
```
┌──(kali㉿kali)-[~]
└─$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.64.1             ether   3e:22:fb:eb:2f:64   C                     eth0
```

g. 

```
msfadmin@metasploitable:~$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
192.168.64.0    *               255.255.255.0   U         0 0          0 eth0
default         192.168.64.1    0.0.0.0         UG        0 0          0 eth0
```

h. 

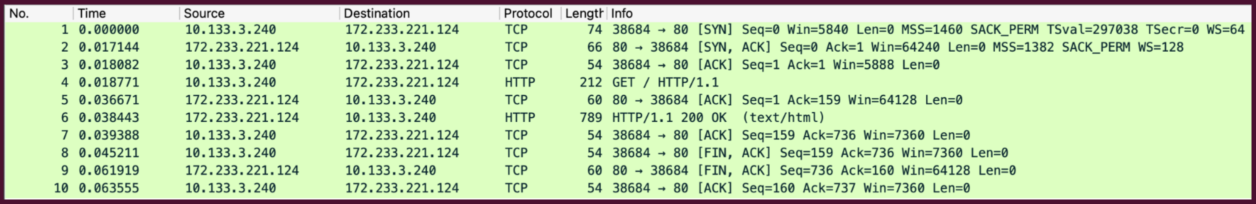
```
msfadmin@metasploitable:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.64.1             ether   3E:22:FB:EB:2F:64   C                     eth0
```

i. 

```
inet6 addr: fe80::f0d6:2cff:fe68:358d/64 Scope:Link
```

I believe we would send the TCP SYN packet to this MAC address, because it seems to be the outgoing address.

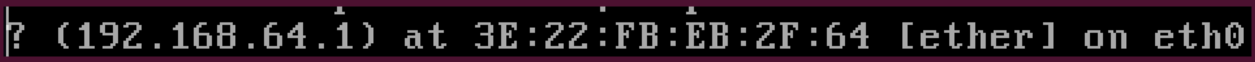
j. The HTML content of the page popped up after I executed the command. I see several captured packets in Kali



| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1 | 0.000000 | 10.133.3.240 | 172.233.221.124 | TCP | 74 | 38684 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSval=297038 TSecr=0 WS=64 |
| 2 | 0.017144 | 172.233.221.124 | 10.133.3.240 | TCP | 66 | 80 → 38684 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1382 SACK_PERM WS=128 |
| 3 | 0.018082 | 10.133.3.240 | 172.233.221.124 | TCP | 54 | 38684 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 |
| 4 | 0.018771 | 10.133.3.240 | 172.233.221.124 | HTTP | 212 | GET / HTTP/1.1 |
| 5 | 0.036671 | 172.233.221.124 | 10.133.3.240 | TCP | 60 | 80 → 38684 [ACK] Seq=1 Ack=159 Win=64128 Len=0 |
| 6 | 0.038443 | 172.233.221.124 | 10.133.3.240 | HTTP | 789 | HTTP/1.1 200 OK (text/html) |
| 7 | 0.039388 | 10.133.3.240 | 172.233.221.124 | TCP | 54 | 38684 → 80 [ACK] Seq=159 Ack=736 Win=7360 Len=0 |
| 8 | 0.045211 | 10.133.3.240 | 172.233.221.124 | TCP | 54 | 38684 → 80 [FIN, ACK] Seq=159 Ack=736 Win=7360 Len=0 |
| 9 | 0.061919 | 172.233.221.124 | 10.133.3.240 | TCP | 60 | 80 → 38684 [FIN, ACK] Seq=736 Ack=160 Win=64128 Len=0 |
| 10 | 0.063555 | 10.133.3.240 | 172.233.221.124 | TCP | 54 | 38684 → 80 [ACK] Seq=160 Ack=737 Win=7360 Len=0 |

k. I got most of this to work.

l. Metasploitable's ARP cache added the following:



```
? (192.168.64.1) at 3E:22:FB:EB:2F:64 [ether] on eth0
```

m. I suspect that it might add another line to the ARP cache. I think it will send the TCP SYN packet through the MAC address listed in l because it’s the one associated with this IP

n. Done

o. I do see captured packets and an HTTP response. It seems like the only information that was sent was the contents of the webpage in HTML.

Synthesis

a. Mal had to collect the IP and MAC addresses for both targets, then they had to set up a filtered sniffer to watch the traffic between Alice and Bob.

b. Alice can detect this attack, because it shows up in the arp cache.

c. Bob cannot detect this attack

d. Yes, they could. HTTPS prevents adversaries from being able to see the content of transmission between two parties.