Avery Hall

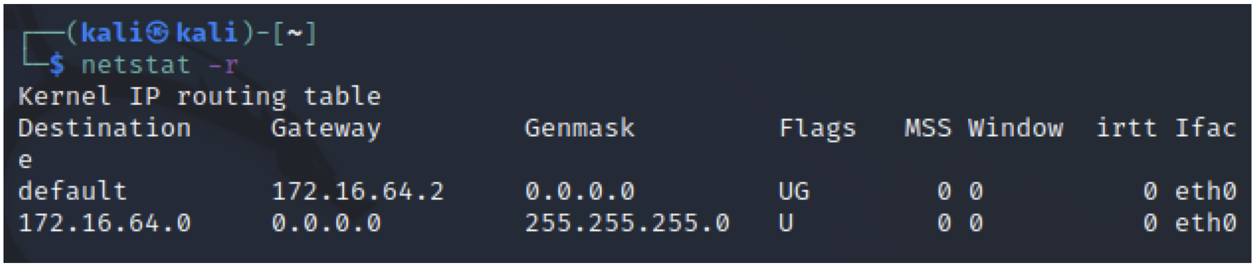
Responses for ARP Spoofing

a. 00:0c:29:a0:2e:cf

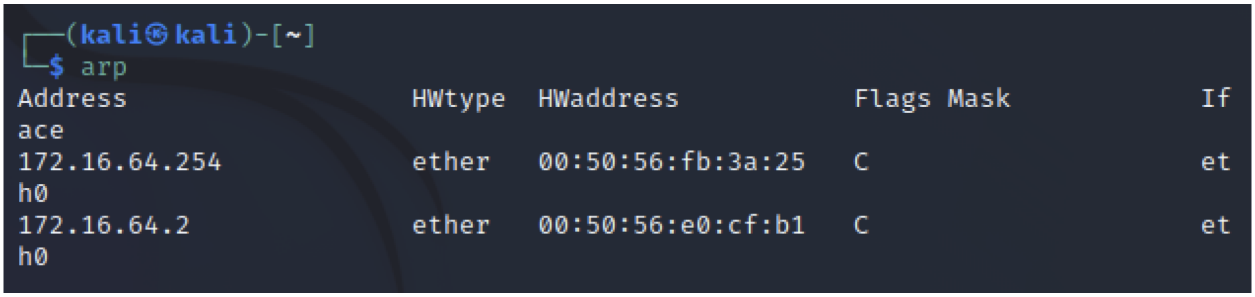
b. 172.16.64.129

c. 00:0c:29:74:4b:7c

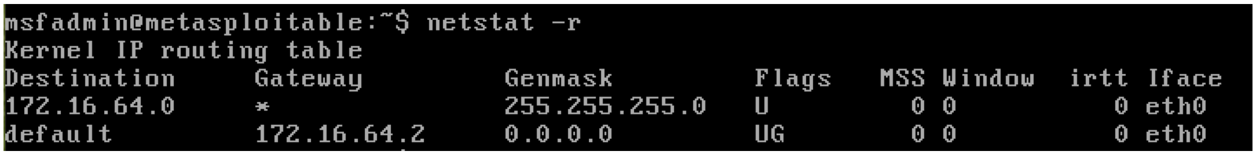
d. 172.16.64.128

e. 

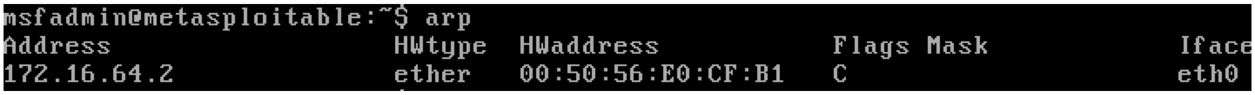
```
┌──(kali㉿kali)-[~]
└─$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Ifac
e
default         172.16.64.2     0.0.0.0         UG        0 0          0 eth0
172.16.64.0     0.0.0.0         255.255.255.0   U         0 0          0 eth0
```

f. 

```
┌──(kali㉿kali)-[~]
└─$ arp
Address                  HWtype  HWaddress           Flags Mask            If
ace
172.16.64.254            ether   00:50:56:fb:3a:25   C                     et
h0
172.16.64.2              ether   00:50:56:e0:cf:b1   C                     et
h0
```

g. 

```
msfadmin@metasploitable:~$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
172.16.64.0     *               255.255.255.0   U         0 0          0 eth0
default         172.16.64.2     0.0.0.0         UG        0 0          0 eth0
```

h. 

```
msfadmin@metasploitable:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
172.16.64.2              ether   00:50:56:E0:CF:B1   C                     eth0
```

i. You should check in the Metasploitable routing table for the IP of the gateway. In this case, this would be 172.16.64.2, and represents the first destination for the TCP SYN packet on the routing journey to Jeff's site. If we then check the ARP cache, we can see that this IP is associated with a MAC address of 00:50:56:E0:CF:B1.

j. I do see an HTTP response when executing curl. But I see no captured packets on Wireshark.

k. (done)

l. It has updated the MAC address associated with 172.16.64.2 (gateway IP) to our Kali's MAC address, effectively tricking Metasploitable into thinking that we are associated with the gateway's IP.

m. 00:0C:29:A0:2E:CF, because after starting ARP poisoning via Ettercap, this is the MAC address (ours) to which the gateway's IP has been updated.

n. (done)

o. Yes, I see an HTTP response. Yes, there are captured packets in Wireshark. Yes; there is a TCP handshake, and several communications with SYN, ACK, FIN, and PSH flags.

p. Through Ettercap's ARP poisoning, Kali was able to intercept TCP ARP packets from Metasploitable intended for the gateway by pretending that Kali's own MAC address was the one associated with that IP. So when Metasploitable received the ARP responses, they indicated that it should send messages to our MAC address, instead of the correct one associated with the actual gateway. And thus, Metasploitable updated its ARP cache with our MAC address in place of the gateway's.

q. One possible red flag that an ARP spoofing detector could be designed to notice is when multiple IP addresses are associated with the same MAC address. Although perhaps not conclusive, this is suspicious because different IP addresses should have different MAC addresses. This could also possibly generate false positives though, because in some cases it might be the case that multiple interfaces are associated with the gateway. Another potential sign for an ARP spoofing detector would be that the IP address/MAC address that it has saved in the ARP cache, or the machine that it ends up sending ARP messages to in any case, is a virtual machine, as it is in this case. Although this may be difficult to detect.