Aiden Chang

Mal Assignment

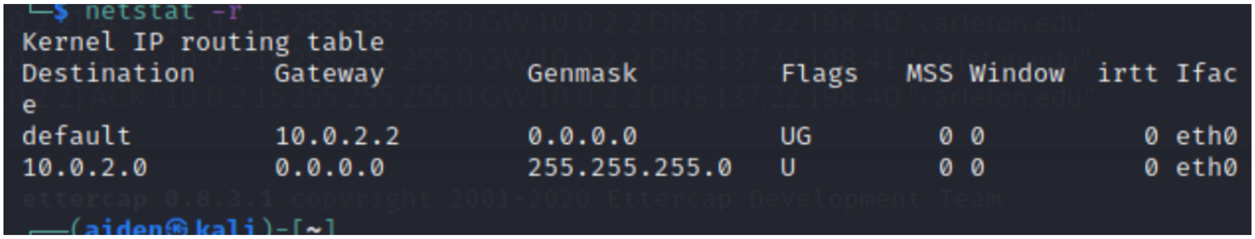
a. 08:00:27:19:60:88

b. 10.0.2.15

c. 08:00:27:1c:37:d6

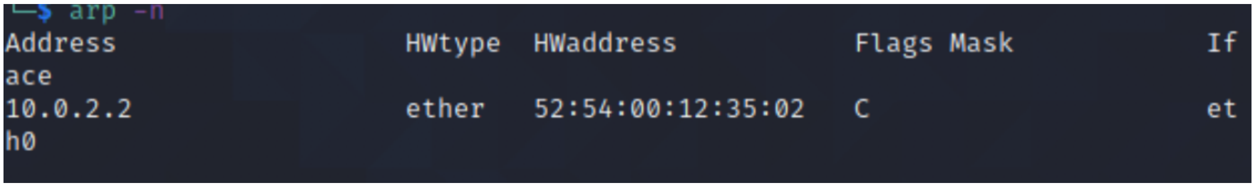
d. 10.0.2.4

E.



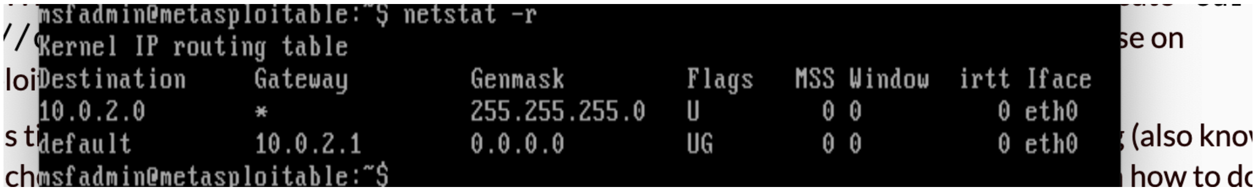
```
└─$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Ifac
e
default         10.0.2.2        0.0.0.0         UG        0 0          0 eth0
10.0.2.0        0.0.0.0         255.255.255.0   U         0 0          0 eth0

┌──(aiden㉿kali)-[~]
```

f.



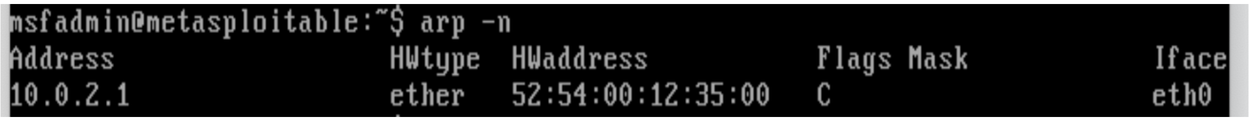
```
└─$ arp -n
Address                  HWtype  HWaddress           Flags Mask            If
ace
10.0.2.2                 ether   52:54:00:12:35:02   C                     et
h0
```

g.



```
msfadmin@metasploitable:~$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
10.0.2.0        *               255.255.255.0   U         0 0          0 eth0
default         10.0.2.1        0.0.0.0         UG        0 0          0 eth0
msfadmin@metasploitable:~$
```

h.



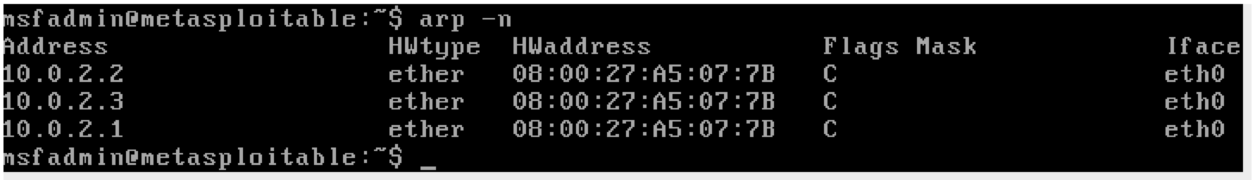
```
msfadmin@metasploitable:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.0.2.1                 ether   52:54:00:12:35:00   C                     eth0
```

I. 52:54:00:12:35:00,  it is the first mac address on my local network I will be sending my packets.

J. I don’t see a http response or any captured packets

K. **Note: I am now transitioning to the computers in Olin(since my machine is not working so the IP addresses listed above this question might be different)**

l.



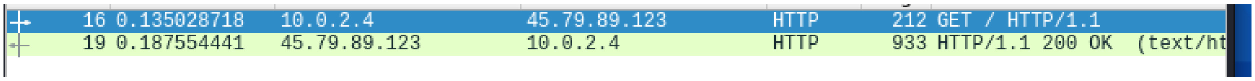
```
msfadmin@metasploitable:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.0.2.2                 ether   08:00:27:A5:07:7B   C                     eth0
10.0.2.3                 ether   08:00:27:A5:07:7B   C                     eth0
10.0.2.1                 ether   08:00:27:A5:07:7B   C                     eth0
msfadmin@metasploitable:~$ _
```

There are extra addresses, and all of them point to the same address(which is the kali MAC address)

m. I expect the TCP SYN packet to go to the Kali, since the physical MAC address of metasploitable is pointing to Kali.

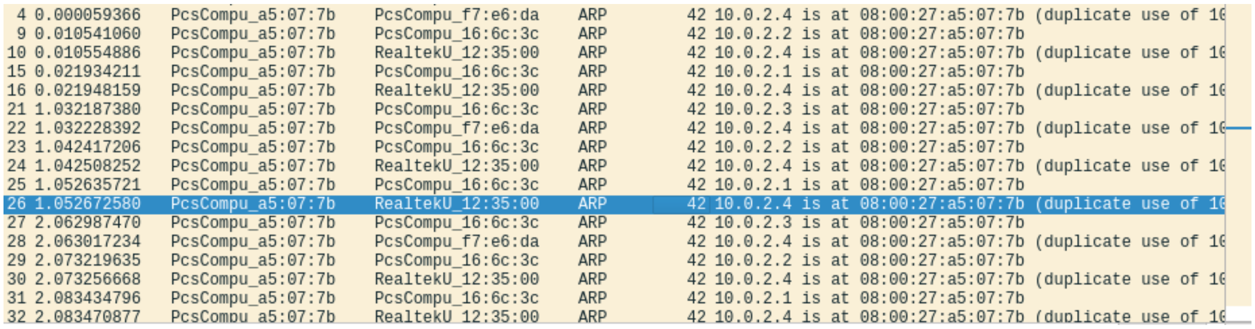
n.

o. I do see an HTTP response on Metasploitable. I can determine that a get request was issued and a text/html packet was sent back(only looking at the http packets).



```
16 0.135028718   10.0.2.4       45.79.89.123   HTTP   212 GET / HTTP/1.1
19 0.187554441   45.79.89.123   10.0.2.4       HTTP   933 HTTP/1.1 200 OK  (text/ht
```

P. It looks like the ettercap is changing metasploitable’s MAC address to Kali’s MAC address. Therefore when someone wants to send Metasploitable a packet is directed to the MAC address assigned, which is Kali’s address in this case.



```
 4 0.000059366   PcsCompu_a5:07:7b   PcsCompu_f7:e6:da   ARP       42 10.0.2.4 is at 08:00:27:a5:07:7b (duplicate use of 10
 9 0.010541060   PcsCompu_a5:07:7b   PcsCompu_16:6c:3c   ARP       42 10.0.2.2 is at 08:00:27:a5:07:7b
10 0.010554886   PcsCompu_a5:07:7b   RealtekU_12:35:00   ARP       42 10.0.2.4 is at 08:00:27:a5:07:7b (duplicate use of 10
15 0.021934211   PcsCompu_a5:07:7b   PcsCompu_16:6c:3c   ARP       42 10.0.2.1 is at 08:00:27:a5:07:7b
16 0.021948159   PcsCompu_a5:07:7b   RealtekU_12:35:00   ARP       42 10.0.2.4 is at 08:00:27:a5:07:7b (duplicate use of 10
21 1.032187380   PcsCompu_a5:07:7b   PcsCompu_16:6c:3c   ARP       42 10.0.2.3 is at 08:00:27:a5:07:7b
22 1.032228392   PcsCompu_a5:07:7b   PcsCompu_f7:e6:da   ARP       42 10.0.2.4 is at 08:00:27:a5:07:7b (duplicate use of 10
23 1.042417206   PcsCompu_a5:07:7b   PcsCompu_16:6c:3c   ARP       42 10.0.2.2 is at 08:00:27:a5:07:7b
24 1.042508252   PcsCompu_a5:07:7b   RealtekU_12:35:00   ARP       42 10.0.2.4 is at 08:00:27:a5:07:7b (duplicate use of 10
25 1.052635721   PcsCompu_a5:07:7b   PcsCompu_16:6c:3c   ARP       42 10.0.2.1 is at 08:00:27:a5:07:7b
26 1.052672580   PcsCompu_a5:07:7b   RealtekU_12:35:00   ARP       42 10.0.2.4 is at 08:00:27:a5:07:7b (duplicate use of 10
27 2.062987470   PcsCompu_a5:07:7b   PcsCompu_16:6c:3c   ARP       42 10.0.2.3 is at 08:00:27:a5:07:7b
28 2.063017234   PcsCompu_a5:07:7b   PcsCompu_f7:e6:da   ARP       42 10.0.2.4 is at 08:00:27:a5:07:7b (duplicate use of 10
29 2.073219635   PcsCompu_a5:07:7b   PcsCompu_16:6c:3c   ARP       42 10.0.2.2 is at 08:00:27:a5:07:7b
30 2.073256668   PcsCompu_a5:07:7b   RealtekU_12:35:00   ARP       42 10.0.2.4 is at 08:00:27:a5:07:7b (duplicate use of 10
31 2.083434796   PcsCompu_a5:07:7b   PcsCompu_16:6c:3c   ARP       42 10.0.2.1 is at 08:00:27:a5:07:7b
32 2.083470877   PcsCompu_a5:07:7b   RealtekU_12:35:00   ARP       42 10.0.2.4 is at 08:00:27:a5:07:7b (duplicate use of 10
```

Q. I would make my detector to scan for arp responses, to check if my ip address is getting rerouted to another MAC address. I would also raise a flag if my MAC address is redirected to somewhere else.