Arp Spoofing

Eric Neidhart, Ankit Sanghi, Ginnie White

A. 08:00:27:11:cf:53
B. The IP address is 10.0.2.15
C. 08:00:27:1a:45:12
D. The IP address is 10.0.2.4
E. Screenshot below:

```
┌──(kali㉿kali)-[~]
└─$ netstat -r                                                          130 ×
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt If
ace
default         10.0.2.1        0.0.0.0         UG        0 0          0 et
h0
10.0.2.0        0.0.0.0         255.255.255.0   U         0 0          0 et
h0
```

F.

```
┌──(kali㉿kali)-[~]
└─$ arp
Address                  HWtype  HWaddress           Flags Mask
Iface
10.0.2.1                 ether   52:54:00:12:35:00   C
eth0
10.0.2.3                 ether   08:00:27:e2:64:43   C
eth0
```

G.

```
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
```

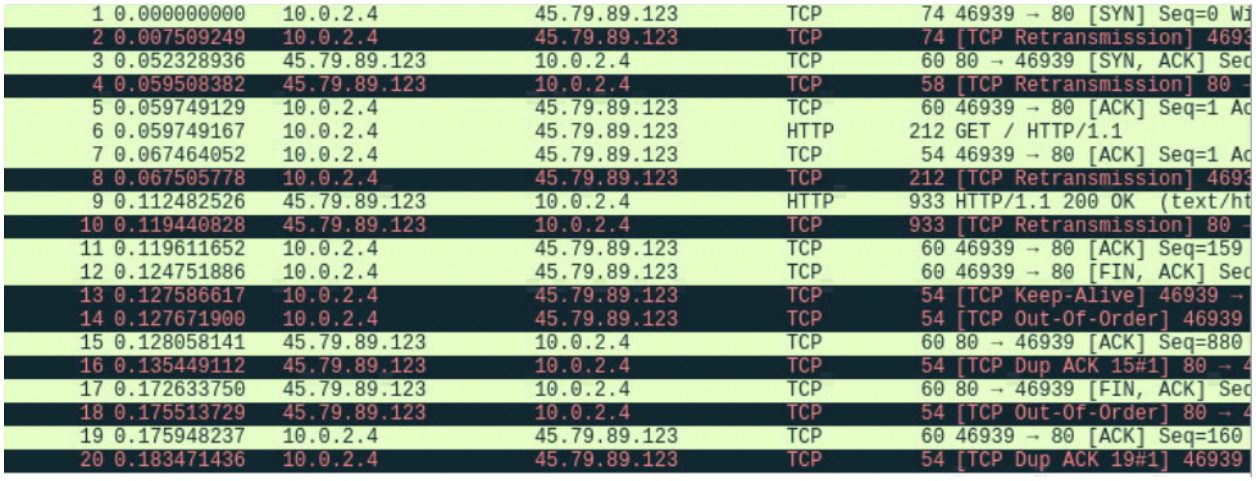
H.

```
msfadmin@metasploitable:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Ifa
10.0.2.1                 ether   52:54:00:12:35:00   C                     eth
10.0.2.3                 ether   08:00:27:E2:64:43   C                     eth
```

I. We use the MAC address 52:54:00:12:35:00 because it is the one associated with the default gateway IP address of 10.0.2.1.

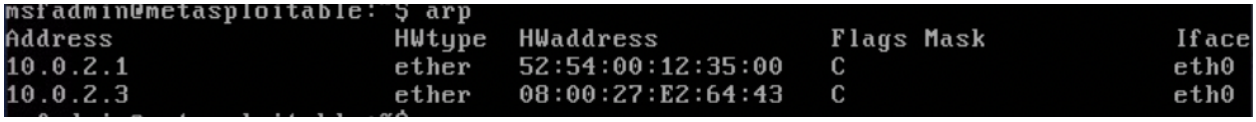
J. We do see an HTTP response in Metasploitable (the returned HTML) but we don't see any packets on Wireshark on Kali.

K.



1	0.000000000	10.0.2.4	45.79.89.123	TCP	74 46939 → 80 [SYN] Seq=0 Wi
2	0.007509249	10.0.2.4	45.79.89.123	TCP	74 [TCP Retransmission] 4693
3	0.052328936	45.79.89.123	10.0.2.4	TCP	60 80 → 46939 [SYN, ACK] Seq
4	0.059508382	45.79.89.123	10.0.2.4	TCP	58 [TCP Retransmission] 80 →
5	0.059749129	10.0.2.4	45.79.89.123	TCP	60 46939 → 80 [ACK] Seq=1 Ac
6	0.059749167	10.0.2.4	45.79.89.123	HTTP	212 GET / HTTP/1.1
7	0.067464052	10.0.2.4	45.79.89.123	TCP	54 46939 → 80 [ACK] Seq=1 Ac
8	0.067505778	10.0.2.4	45.79.89.123	TCP	212 [TCP Retransmission] 4693
9	0.112482526	45.79.89.123	10.0.2.4	HTTP	933 HTTP/1.1 200 OK (text/ht
10	0.119440828	45.79.89.123	10.0.2.4	TCP	933 [TCP Retransmission] 80 →
11	0.119611652	10.0.2.4	45.79.89.123	TCP	60 46939 → 80 [ACK] Seq=159
12	0.124751886	10.0.2.4	45.79.89.123	TCP	60 46939 → 80 [FIN, ACK] Seq
13	0.127586617	10.0.2.4	45.79.89.123	TCP	54 [TCP Keep-Alive] 46939 →
14	0.127671900	10.0.2.4	45.79.89.123	TCP	54 [TCP Out-Of-Order] 46939
15	0.128058141	45.79.89.123	10.0.2.4	TCP	60 80 → 46939 [ACK] Seq=880
16	0.135449112	45.79.89.123	10.0.2.4	TCP	54 [TCP Dup ACK 15#1] 80 → 4
17	0.172633750	45.79.89.123	10.0.2.4	TCP	60 80 → 46939 [FIN, ACK] Seq
18	0.175513729	45.79.89.123	10.0.2.4	TCP	54 [TCP Out-Of-Order] 80 → 4
19	0.175948237	10.0.2.4	45.79.89.123	TCP	60 46939 → 80 [ACK] Seq=160
20	0.183471436	10.0.2.4	45.79.89.123	TCP	54 [TCP Dup ACK 19#1] 46939

L. Now the second IP address is the same as one of the IP addresses of Kali. So now Metasploitable is now using Kali as one of it's routers.



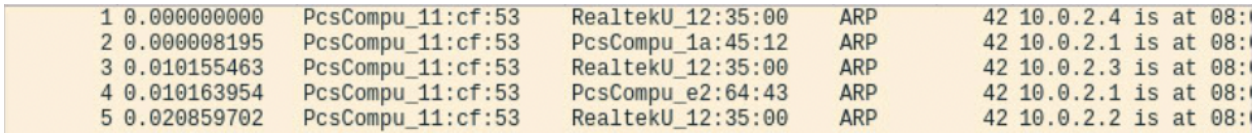
```
msfadmin@metasploitable: $ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
10.0.2.1                 ether   52:54:00:12:35:00   C                     eth0
10.0.2.3                 ether   08:00:27:E2:64:43   C                     eth0
```

M. We now send packets to the MAC address of one of Kali's routers, which is 08:00:27:e2:64:43.

N. We did this above. Refer to the screenshot in question K.

O. We can see an HTTP response on Metasploitable. As you can see from our screenshot on question K, we did detect packets using Wireshark this time. We can see the GET request that contains the request for Jeff's site, and we can also see the HTTP OK response when this goes through.

P.



1	0.000000000	PcsCompu_11:cf:53	RealtekU_12:35:00	ARP	42 10.0.2.4 is at 08:
2	0.000008195	PcsCompu_11:cf:53	PcsCompu_1a:45:12	ARP	42 10.0.2.1 is at 08:
3	0.010155463	PcsCompu_11:cf:53	RealtekU_12:35:00	ARP	42 10.0.2.3 is at 08:
4	0.010163954	PcsCompu_11:cf:53	PcsCompu_e2:64:43	ARP	42 10.0.2.1 is at 08:
5	0.020859702	PcsCompu_11:cf:53	RealtekU_12:35:00	ARP	42 10.0.2.2 is at 08:

First, Ettercap starts an ARP Poisoning attack by scanning the network for at least two other devices on the network. Ettercap sends out lots of forged ARP response packets. The forged responses advertise that the correct MAC address for both IP addresses, belonging to the two devices, is the attacker's MAC address. This fools both devices to connect to Kali instead of the router. Metasploitable then updates its ARP cache entries and from that point onwards, communicates with the attacker instead of directly with each other. The attacker is now secretly in the middle of all communications.

Q. A very basic detector would notify you if your routing addresses suddenly changed. However, you would get false positives if this happened for benevolent reasons (say, you changed

wireless networks). Another detector could detect large numbers of arp packets in a short period of time, which may indicate an ARP poisoning attack is underway.