ARP Spoofing

By: Sydney Nguyen

a) What is Kali's main interface's MAC address? (The main interface is probably called eth0, but check ifconfig to be sure.)

The MAC address of my kali's main interfaces 00:0c:29:90:68:2c.

b) What is Kali's main interface's IP address?

Kali's main interface's IP address 192.168.35.128.

```
msfadmin@metasploitable:~$ no
-bash: no: command not found
msfadmin@metasploitable:~$ ifcongif
-bash: ifcongif: command not found
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:f4:9f:10
          inet addr:192.168.35.130  Bcast:192.168.35.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fef4:9f10/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:226 errors:0 dropped:0 overruns:0 frame:0
          TX packets:100 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:16217 (15.8 KB)  TX bytes:12447 (12.1 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:249 errors:0 dropped:0 overruns:0 frame:0
          TX packets:249 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:97525 (95.2 KB)  TX bytes:97525 (95.2 KB)

msfadmin@metasploitable:~$ _
```

c) What is Metasploitable's main interface's MAC address?

Metasploitable's main interface's MAC address is 00:0c:29:f4:9f:10.

d) What is Metasploitable's main interface's IP address?

Metasploitable's main interface's IP address 192.168.35.130

e) Show Kali's routing table. (Use "netstat -r" to see it with symbolic names, or "netstat -rn" to see it with numerical addresses.)

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         192.168.35.2    0.0.0.0         UG        0 0          0 eth0
192.168.35.0    0.0.0.0         255.255.255.0   U         0 0          0 eth0
```

f) Show Kali's ARP cache. (Use "arp" or "arp -n".)

```
┌──(kali㉿kali)-[~]
└─$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.35.2             ether   00:50:56:e1:30:4e   C                     eth0
```

g) Show Metasploitable's routing table.

```
msfadmin@metasploitable:~$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
192.168.35.0    *               255.255.255.0   U         0 0          0 eth0
default         192.168.35.2    0.0.0.0         UG        0 0          0 eth0
msfadmin@metasploitable:~$
```

h) Show Metasploitable's ARP cache.

```
msfadmin@metasploitable:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.35.2             ether   00:50:56:E1:30:4E   C                     eth0
192.168.35.254           ether   00:50:56:F3:91:10   C                     eth0
msfadmin@metasploitable:~$ _
```

i) Suppose the user of Metasploitable wants to get the CS338 sandbox page via the command "curl http://cs338.jeffondich.com/". To which MAC address should Metasploitable send the TCP SYN packet to get the whole HTTP query started? Explain why.

> The MAC address we should send to is 00:50:56:E1:30:4E which is the default gateway for packets to be sent through we can tell because of the routing table.

j) Fire up Wireshark on Kali. Start capturing packets for "tcp port http". On Metasploitable, execute "curl http://cs338.jeffondich.com/". On Kali, stop capturing. Do you see an HTTP response on Metasploitable? Do you see any captured packets in Wireshark on Kali?

We are able to see the HTTP response on metasploitable but wireshark does not capture any packets on Kali.

k) Now, it's time to be Mal (who will, today, merely eavesdrop). Use Ettercap to do ARP spoofing (also known as ARP Cache Poisoning) with Metasploitable as your target. There are many online tutorials on how to do this (here's one). Find one you like, and start spoofing your target. NOTE: most of these tutorials are showing an old user interface for Ettercap, which may make them confusing. The steps you're trying to take within Ettercap are:
   i) Start sniffing (not bridged sniffing) on eth0
   ii) Scan for Hosts
   iii) View the Hosts list
   iv) Select your Metasploit VM from the Host List
   v) Add that host as Target 1
   vi) Start ARP Poisoning (including Sniff Remote Connections)
   vii) Do your stuff with wireshark and Metasploit
   viii) Stop ARP Poisoning

   Done, should be noted I took Jeff's route of using ettercap!

l) Show Metasploitable's ARP cache. How has it changed?
   All Mac addresses were changed into Kali's Mac address andI gained two IP addresses .1 and .128.

```
msfadmin@metasploitable:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.35.254           ether   00:0C:29:90:68:2C   C                     eth0
192.168.35.1             ether   00:0C:29:90:68:2C   C                     eth0
192.168.35.2             ether   00:0C:29:90:68:2C   C                     eth0
192.168.35.128           ether   00:0C:29:90:68:2C   C                     eth0
msfadmin@metasploitable:~$ _
```

m) Without actually doing it yet, predict what will happen if you execute "curl http://cs338.jeffondich.com/" on Metasploitable now. Specifically, to what MAC address will Metasploitable send the TCP SYN packet? Explain why.

   I think that there will be TCP SYN packets sent to Kali'smac address. This will occur because we are putting a person in the middle instead of sending to the correct location. It will just send to Kail's address.

n) Start Wireshark capturing "tcp port http" again.

Done!

o) Execute "curl http://cs338.jeffondich.com/" on Metasploitable. On Kali, stop capturing. Do you see an HTTP response on Metasploitable? Do you see captured packets in Wireshark? Can you tell from Kali what messages went back and forth between Metasploitable and cs338.jeffondich.com?

We are still able to see the HTTP response on metasploitable. Now we are able to see the captured packages in wireshark. With curl Kali can see all the TCP packets of the HTTP response that Jeff's site sends and what is sent to metasploitable. It is important to note that the packets were sent twice because we are a person in the middle so they are sent to us as well which makes snes for the duplicates.

p) Explain in detail what happened. How did Kali change Metasploitable's ARP cache? (If you want to watch the attack in action, try stopping the PITM/MITM attack by selecting "Stop mitm attack(s)" from Ettercap's Mitm menu, starting a Wireshark capture for "arp", and restarting the ARP poisoning attack in Ettercap.)

The Kali system begins by claiming or impersonating the MAC address of the desired destination. As there is no authentication system Kali is just able to answer for cs338.jeffondich Kali represents the cs338.jeffondich destination by using its Mac address. This is all being altered in metasploitable, metasploitable then things that kali's mac address is jeff. Once the Mac address of Kali is in Metasploitable arp cache. Then when Metasploitable looks up jeff in its ARP cache it will send the TCP SYN packets to Kali's MAC address rather than jeff.

q) If you wanted to design an ARP spoofing detector, what would you have your detector do? (As you think about this, consider under what circumstances your detector might generate false positives.)
   i) A simple addition to a ARP spoofing detector is to send a confirmation message to the ip address (old IP, or other contact) that there has been a change and that we take necessary precautions to be able to conclude that we are in fact talking to , sending packets to who we want to. Perhaps forcing people to do a two authentication type of change of their IP like when we often change passwords for certain accounts to get a confirmation from an email or similar type to get a confirmation that a change is indeed wanted. This can generate a lot of false

positives if people are changing their devices often meaning that their IP addresses would actually be changing often.

ii) Another option would be to set a system that flags or sends an error message to us or the clients if there are multiple MAC addresses we could just be aware to take precautions again that we are not accidently communicating with the same IP address that are lying and saying they are other IP addresses. Again this could generate false positives by people having old devices still registered as we are not keeping all the data updated IP copies may have just been used again and the old device has been destroyed.