Ben Hafner
CS 338 Computer Security
May 2020
ARP Spoofing

a. Kali's MAC address is: 00:0c:29:78:8f:79.
b. Kali's IP address is 172.16.227.129.
c. Metasploitable's MAC address is 00:0c:29:2b:8b:2c.
d. Metasploitable's IP address is 172.16.227.130.
e. Here's Kali's routing table:

```
┌──(kali㉿kali)-[~]
└─$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         172.16.227.2    0.0.0.0         UG        0 0          0 eth0
172.16.227.0    0.0.0.0         255.255.255.0   U         0 0          0 eth0
```

f. Here's Kali's ARP cache (I have no idea what the IP address ending in 254 is):

```
┌──(kali㉿kali)-[~]
└─$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
172.16.227.254           ether   00:50:56:f7:ba:1b   C                     eth0
172.16.227.2             ether   00:50:56:f3:e5:be   C                     eth0
```

g. Here's Metasploitable's routing table:

```
msfadmin@metasploitable:~$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
172.16.227.0    *               255.255.255.0   U         0 0          0 eth0
default         172.16.227.2    0.0.0.0         UG        0 0          0 eth0
```

h. Here's Metasploitable's ARP cache:

```
msfadmin@metasploitable:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
172.16.227.2             ether   00:50:56:F3:E5:BE   C                     eth0
172.16.227.129           ether   00:0C:29:78:8F:79   C                     eth0
```

i. Metasploitable's routing table only has two entries: one for IP addresses starting with 172.16.227 and one default for everything else. The IP address of http://cs338.jeffondich.com/ is 45.79.89.123, which falls into the default category, meaning traffic to this website should be routed to 172.16.227.2, the local gateway. According to Metasploitable's ARP cache, the MAC address for the local gateway is 00:50:56:F3:E5:BE.
j. When Metasploitable went to http://cs338.jeffondich.com/ with curl, Kali didn't see any tcp packets on port 80 because Metasploitable correctly sent all its packets straight the the local network gateway, not to Kali.
k. Done
l. Here's Metasploitable's new (poisoned) ARP cache:

```
msfadmin@metasploitable:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
172.16.227.1             ether   00:0C:29:78:8F:79   C                     eth0
172.16.227.2             ether   00:0C:29:78:8F:79   C                     eth0
172.16.227.254           ether   00:0C:29:78:8F:79   C                     eth0
172.16.227.129           ether   00:0C:29:78:8F:79   C                     eth0
```

m. I predict that Metasploitable will now send its TCP SYN packet to the MAC address 00:0c:29:78:8f:79 (Kali's MAC address)
n. Done
o. This time, when Metasploitable went to http://cs338.jeffondich.com/ with curl, Metasploitable did still get the correct response showing the website content, but Kali's Wireshark was able to see all the TCP packets that got sent back and forth.
p. When I ran ARP poisoning from Ettercap, what Ettercap did was send out a bunch of fake ARP responses. In these fraudulent responses, Kali claimed that its own MAC address was associated with the local network gateway's IP address. In fact, it actually claimed that all the IP addresses on the local network were associated with its own MAC address. That way, anyone trying to send a message over the local network will send it straight to Kali, who can then forward it to the actual intended recipient. For example, when I ask Metasploitable to go to http://cs338.jeffondich.com/ with curl, Metasploitable sends its TCP SYN packet to Kali, mistakenly believing that Kali is the gateway. Then Kali forwards this packet to the real gateway, which sends it off through the network to Jeff's web server. When Jeff's server sends back a TCP SYN ACK packet in response, the gateway directs it to Kali, who forwards it on to Metasploitable. In this way, Kali can see and control all TCP communications between Metasploitable and http://cs338.jeffondich.com/. If I wanted, I could have Kali modify or block those communications instead of just passively forwarding them on. It's a real person-in-the-middle attack!
q. Here's one way you could build an ARP spoofing detector: Make a little robot that listens to ARP requests and responses on the local network. It would keep track of which IP addresses correspond to which MAC addresses and if any IP address ever changed its MAC address, it would say "Hey! Someone's attempting ARP spoofing!" One problem with this approach it that IP addresses do need to change their MAC addresses for legitimate reasons sometimes. For instance, suppose there's a web server on the local network but the machine it's running on is getting old and needs to be replaced. If you plug a new machine into the same local network, it'd have a different MAC address, but you'd want it to run the same web server with the same IP address. The robot would wrongly flag this as ARP spoofing.