

Lesson 3: ARP Spoofing

Goal: To get a high-level understanding of ARP (Address Resolution Protocol). This lesson also familiarizes students with ARP Spoofing.

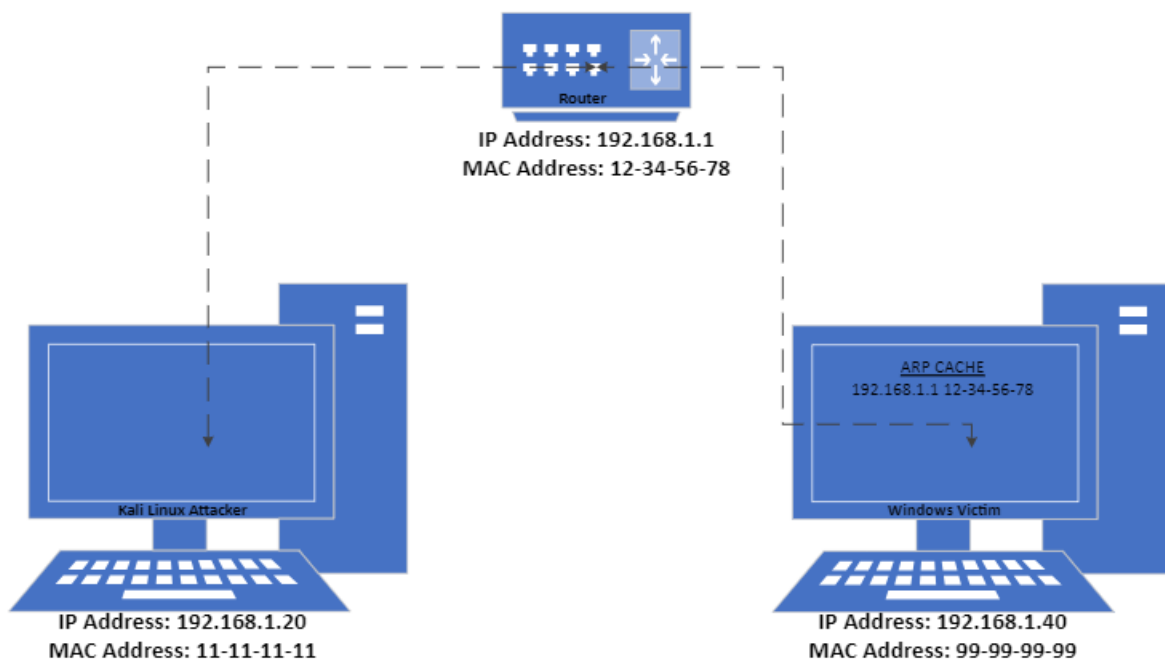
You can think of a network as a road, where regular traffic (packets of information) flows through it. In the below image, we can see that the arrows signify the road, and the traffic (information) is going through the router.

Topics Discussed:

ARP Protocol

Bettercap Tool – to perform ARP spoofing

Wireshark Tool – to see the changes made due to ARP spoofing



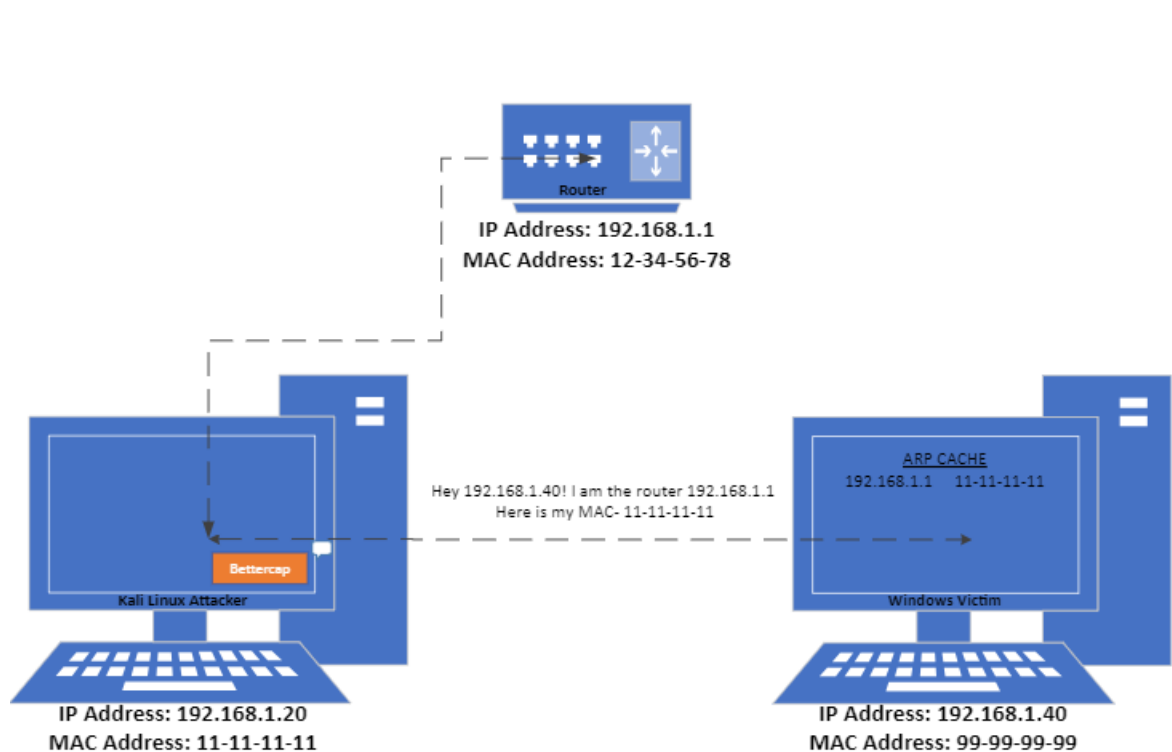
ARP or Address Resolution Protocol is what computers use to communicate the correlation between their IP address and MAC Address. IP Addresses are dynamically leased over a given time, whereas MAC Addresses are static and never change.

ARP spoofing can be used for attacks such as spying, man in the middle and denial of service attacks.

Note the ARP CACHE table within the Windows machine. This ARP cache holds a mapping of IP Addresses to MAC Addresses on a local computer, so that the computer doesn't always have to ask what everyone is before sending traffic to them. It will simply update the table and reference it. However, this does change very frequently as computers join/leave the network.

To take control of the Victims traffic, we must change the flow of traffic.

ARP Spoofing is one attack that can change the flow of traffic. Before, we mentioned that the ARP CACHE holds mapping information in a table format, so we can abuse this ARP as it is inherently insecure. By saying "Hey, Alice (Windows)! That 192.168.1.1 is my IP address, not the IP Address of the router. Here is my MAC:". The Windows computer assumes that updating the table is okay, as there is no validation built into the ARP protocol to verify if the information is correct or not.



In this image you can see that the Victim (Windows) machine has updated its ARP CACHE based on the **false** information provided by the Attacker (Ip Address of router is mapped to the MAC address of attacker).

When ARP Spoofing is done it is similar to demolishing the previous road that existed and re-paved to go through the Ubuntu Machine.

Bettercap is a tool that helps us perform ARP Spoofing, and there are many other tools (ettercap) that can do the same thing.

We will now show how ARP/ ARP Spoofing is used “under the hood”.

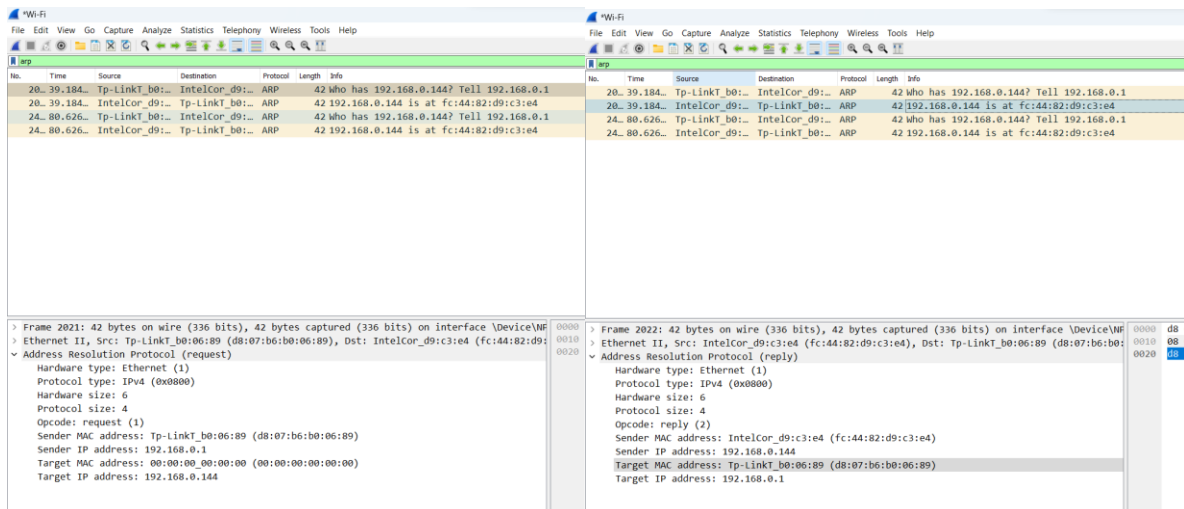
Notes

- Before
 - Show a typical ARP packet
 - Show the “Routing” aka proof that Windows is sending info to the router
- During
 - Show the ARP Spoof packet that bettercap sends
- After
 - Show the new “Routing” aka proof that Windows is now sending traffic to Kali Linux

Background:

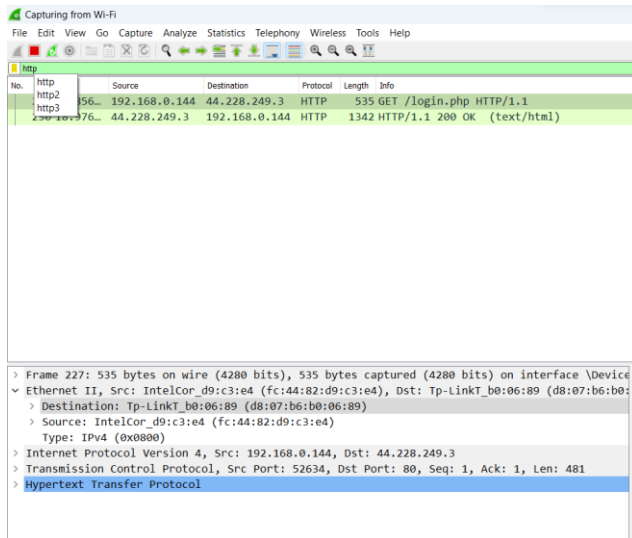
DEVICE NAME	IP ADDRESS	MAC ADDRESS
TP Link Router	192.168.0.1	d8:07:b6:b0:06:89
Windows Device	192.168.0.144	fc:44:82:d9:c3:e4
Kali Linux Device	192.168.0.224	98:48:27:3b:ec:be

Before the Attack



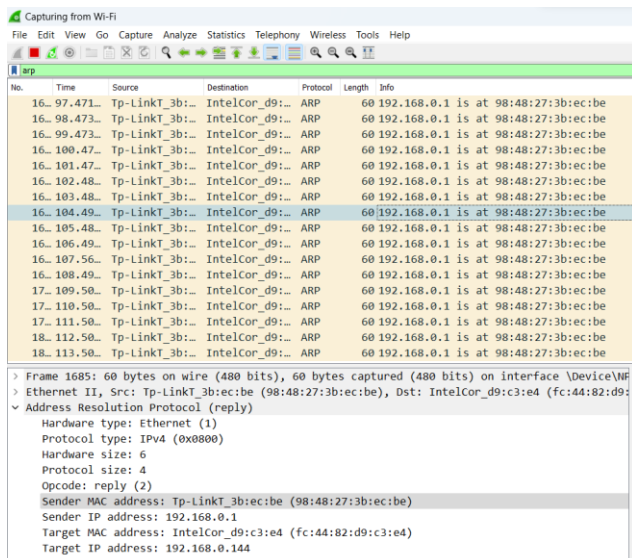
The above images show the correct ARP packets being exchanged between devices.

The left image shows the ARP request from TP Link router while the right image shows the ARP reply from the Windows computer.



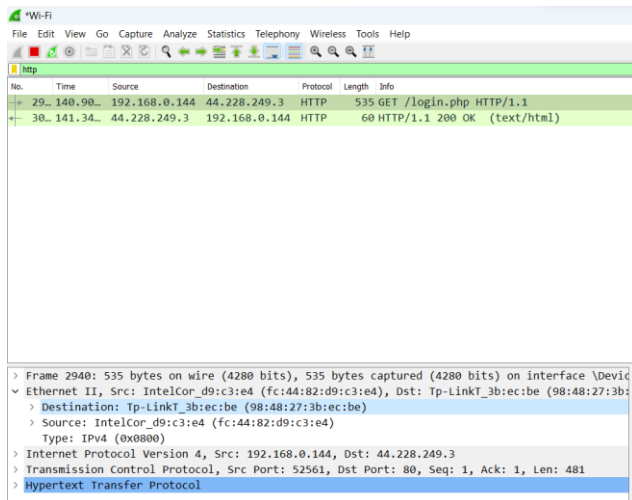
The above image shows a genuine web request to router. The destination MAC Address checks out.

During the Attack



Above image shows the Kali Linux device (sender) telling the Windows PC (receiver) that 192.168.0.1 is at a new MAC Address. Thus, Spoofing the windows computer into thinking the Attacker is the router.

After the Attack



The above image shows the ARP CACHE table of the Victim Windows device where the IP address is of the TP link router whereas the MAC Address is of the Kali Linux Device.