

Lesson 6: MITM Attack

Notes

- MITM Tool (MITMDump)
 - Use the infrastructure created by bettercap tool. Redirect specific cars to other places.
 - IPTables is like a Police Officer selecting specific cars in traffic and telling them to go down to a certain check point.
 - The “checkpoint” is MITMDump
- Wireshark is used to show proof

We have talked about how the typical road of traffic is going to and from the router, but with the bettercap tool, we can change the road to flow through the Ubuntu machine (attacker) using an ARP Spoofing attack. Now that we have created a new “road” for those cars to go down, we need to change the packets/ “cars” that the Windows victim is sending to the internet.

A couple of tools like MITMDump and IPTables can help us select cars that are going through the road and have those selected cars changed in some way to run malicious code for us on the victim machine.

To be more concrete, the IPTables tool will act as a Police Officer, who will select specific cars going down the road and tell them to go through a malicious toll booth. The toll booth is our MITMDump tool. This toll booth will add malicious code to the cars so that the code will be executed by the Windows victim machine.

IPTables takes that HTTP website request and gives it to MITMDump over port 8080, which MITMDump is listening on. MITMDump will send the web request that the Windows victim intended to do. All the while, bettercap is sending ARP Spoof packets to the Windows machine to keep the malicious traffic route active.

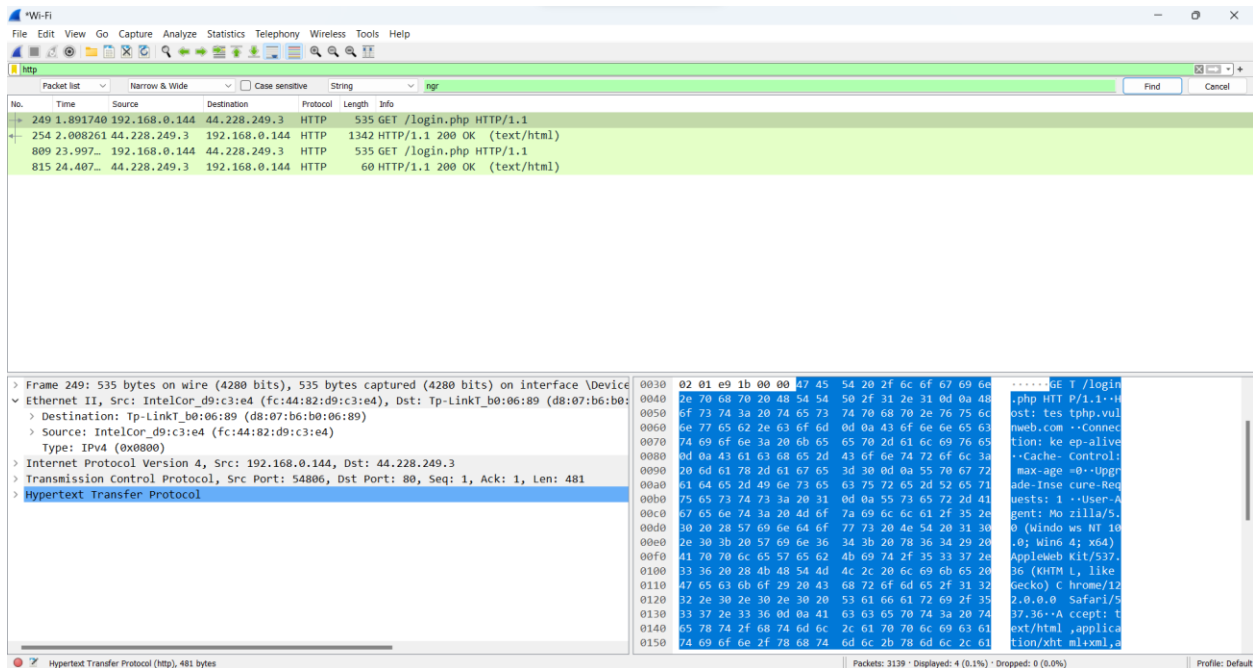
The attacker injects some malicious code that will be added to the website response. Note the “target website” has been changed due to which the victim will be forced to go to another website.

Background:

DEVICE NAME	IP ADDRESS	MAC ADDRESS
-------------	------------	-------------

TP Link Router	192.168.0.1	d8:07:b6:b0:06:89
Windows Machine	192.168.0.144	fc:44:82:d9:c3:e4
Ubuntu Machine	192.168.0.224	98:48:27:3b:ec:be

Wireshark



The above is a legit HTTP website request sent by the Windows machine to the TP Link router.

The Destination and Source MAC addresses are true.

The attacker injects some malicious code which is added to the response from the server, which will be given to the windows victim. This malicious code forces the browser on the victim's machine to open a specific website.