**Write-Up – ARP spoofing attack tool**

In this write-up we are going to show and explain main parts of our code.

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטיIn the beginning we are using the 'argparse' module to analyze the user arguments in his command:

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטיWe decided to use a class which called ArpSpoofing with relevant fields and an attack() function.

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטיNow we'll explain the constructor:

As you can see we got five arguments from the user, only 'target\_ip' is required, others get a default value via the args parser.

Target\_ip – the address we want to attack

Src\_ip – the address wh want to impersonate to. Default is the gateway.

Gw\_spoof – Boolean, if the user wants to attack the src arp table as well.

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטיYou can notice that we got MAC addresses via 'get\_mac()' function by sending arp request with the given IP:

If there isn't answer we will print a message to the user and exit the program.

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטיNow, let's understand the main function of the program – the attack() function:

Firstly, we create the spoofed-packet to the target and if the user wants a full duplex attack we'll create another packet to the src (gateway is default). We are sending the packets until the user stopped the program.

The spoofed 'is at' packets built according to the needs. Notice that the mac\_src filled by scapy when the request sent.

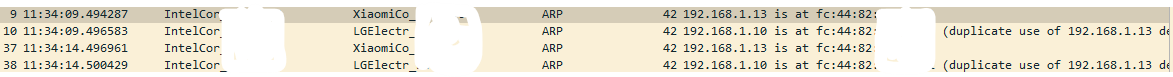
Now, we'll show a running example:

The target – my phone ip 192.168.1.10

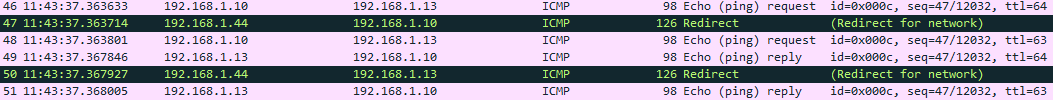
The src – my smart TV IP 192.168.1.13

We want full-duplex attack and 5 seconds delay.

The command:

Now, I will turn on wireshark and sniff WIFI interface:

You can notice the packets from my Intel to my Xiaomi and to my LG tv.

****When I send ping from my phone (via termux app) to my tv IP address, we can see in wireshark that we are a mitm and redirect the packets (by changing the IP forwarding option in the registry).

Of course, the MAC address of original request/reply is mt computer MAC.

The last thing that we want to notice is the maximum delay that inhibits the target machine from sending a 'who\_has' BROADCAST message.

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטיIn my Linux – 60 seconds

תמונה שמכילה שולחן

התיאור נוצר באופן אוטומטיIn Windows – 2 mins

**Thank you for your reading.**