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

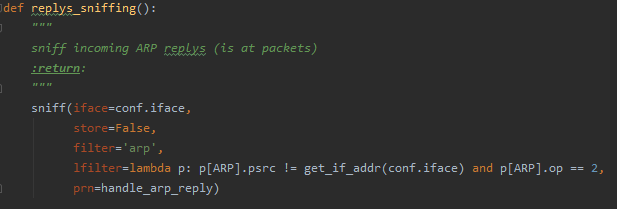
In this write-up we are going to show and explain main parts of our code.

In the beginning we are using the 'argparse' module to analyze the user arguments in his command:

תמונה שמכילה טקסט

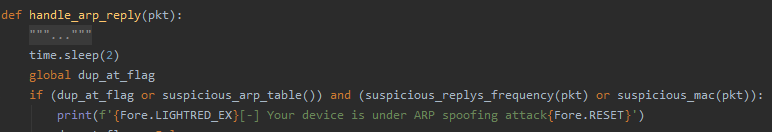
התיאור נוצר באופן אוטומטי

We begin to sniff Arp replies packets by create new thread that call to function 'replys\_sniffing' until the user stopped the program.



You can notice that in parmeter 'prn' of 'sniff' we call to function 'handle\_arp\_reply'.

In this function we check whether the 2 indicators we defined are recognized and if so, it means that the device is under attack.



The 2 indicators we defined are:

1. Checking if there is the same mac address associated with 2 or more Ip addresses.

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי

2. Comparing the received packet to a normal Arp reply packet **or** that there are 3 similar ARP replies at last 30 seconds.

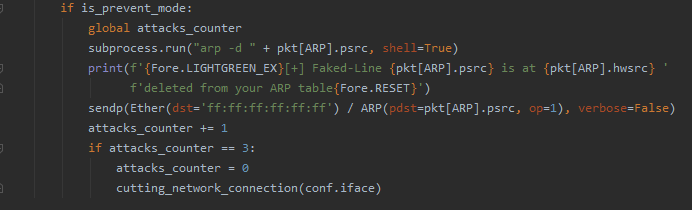
תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי

In addition, there is the prevention flag, and if it is on then we will remove the faked-line in the victim's ARP table and after three times we'll restart the network.



Now, we'll show a running example:

**Thank you for your reading.**