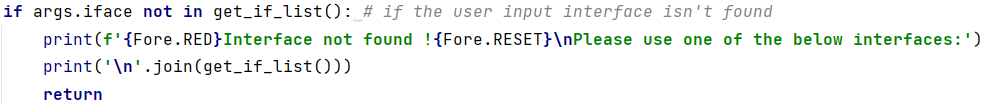
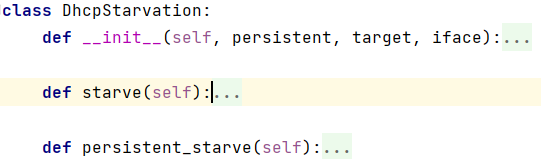
**Write-Up – DHCP starvation attack tool**

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:

As you can see there are three optional arguments.

We'll note that the decision to create a class is based on the need of maintaining the leased IP addresses in the persistent mode.

And now we can start with the DHCP starvation attack. Of course, we will start with none-persistent mode attack, just by sending DHCP-DISCOVER and a DHCP-REQUEST as a response to DHCP-OFFER.

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטיDISCOVER handling:

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטיThe discover function creates and sends the DHCP-DISCOVER packet:

If there isn't an offer after 3 discovers – the attack finished if it isn't persistent. If it's persistent attack, we will move to persistent\_starve() function.

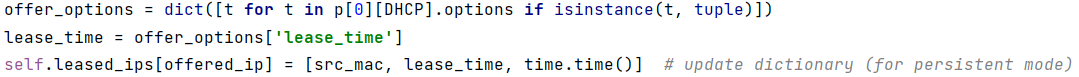
תמונה שמכילה טקסט

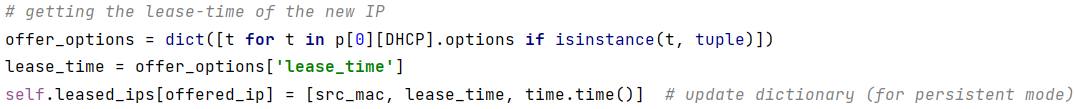
התיאור נוצר באופן אוטומטיWhile we are getting offers to the DHCP-DISCOVER we will handle the DHCP-REQUEST:

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטיThe request function creates and sends the DHCP-REQUEST packet:

We noticed that the server sends ARP-REQUEST after every DHCP-REQUEST, and we need to response with ARP-REPLY. The arp\_reply function:

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטיAfter that, we'll update our leased ip addresses dictionary:

**NOTE: in persistent mode, the starve() function called every 30 seconds to check if there are more IP addresses that released.**



Now, let's explain the persistent\_starve() function. The function loops the leased IP dictionary and checks for IP addresses that 50% of its lease-time passed (T1 expired). If one found, we are in RENEWING mode, and we'll send DHCP-REQUEST with the correct options. If we got a DHCPACK (using srp1() function in request() and return packet) the server renewed the lease and we'll update the start-lease-time in the dictionary.

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטיOf course, if 87.5% of time passed we will send broadcast DHCP-REQUEST.

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטיThe DHCP-REQUEST in RENEWING implementation:

Now I'll show you an running example (include active dhcpd.leases file):

תמונה שמכילה טקסט

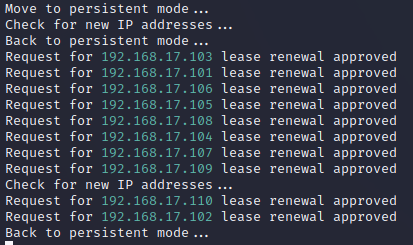
התיאור נוצר באופן אוטומטיWhite console – server. Black console – client.

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי

תמונה שמכילה שולחן

התיאור נוצר באופן אוטומטי



תמונה שמכילה שולחן

התיאור נוצר באופן אוטומטיPay attention to scanning for ne IP addresses by DISCOVER.

Above, you can pay attention to the lease renewing (valid until column).

**We tried to be sticked as we can to the RFC 2131.**

**Thank you for your reading.**