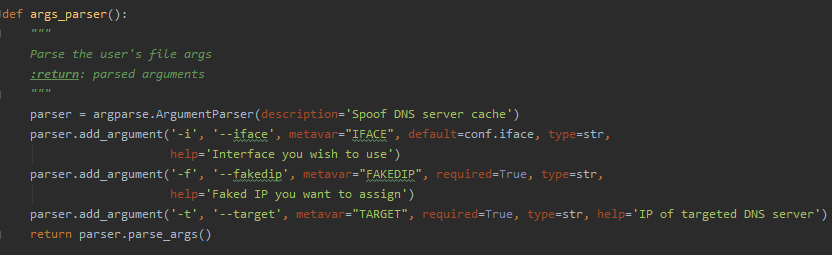
**Write-Up – DNS poisoning attack tool**

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:



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

iface – the interface that you wish to use.

faked\_ip – the faked IP address we want to assign in the faked answers.

target – the address of the DNS server we want to attack.

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

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי

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

Now, let's understand the main function of the program – the dns\_sniffer(pkt) function:



Firstly, check if this packet is a DNS query packet, if this is not a DNS query packet then exit from the function, but if this is a DNS query packet we move on.

In the next step we check whether the received packet works with ipv4 or ipv6 and according to this there are some small changes in the fields of the protocol.

Then we create the fake DNS answer with the fake address found in FAKED\_IP.

And finally, we send it to the attacked DNS server and with this we plant a fake address in it that it will send to every device in the network.

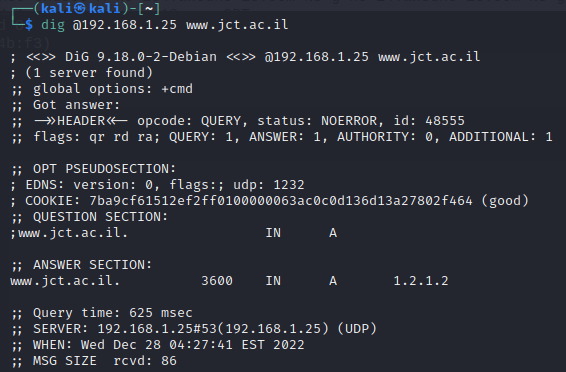
Now, we'll show a running example:

The faked ip –1.2.3.4

The target server – 192.168.1.25

The command:

Result of dig in the client:



Result of cache in the server:

****

While DNSSEC is turned on, when I'm trying to spoof **domain that uses DNSSEC as well** – it doesn’t work.

**Thank you for your reading.**