ARP Storm

Name: Zeyad Salah Mohamed Fathi

ID: 120210297

**Discovering abnormalities**

The first thing we can do when we open the PCAP is to search for any abnormalities in it, if we take a look at the image below we can notice something strange, we know that the opcode can only be 0 or 1 referring to request and reply operations but in the PCAP we find that the opcode is strange it is always Unknown ARP opcode 0x…. , so from here we can start to check the abnormality we found.

A screenshot of a computer

Description automatically generated

**Searching for the way to the flag**

After we found that unusual thing, we can check all the abnormal opcodes to determine a pattern or something, after doing that we discover that they all have the same representation except for the character in the middle which change for each opcode as shown in the image below, so if we can get all those characters from the opcodes may be we can get the flag or encoded version of it.

A computer screen shot of a black screen

Description automatically generated

**First step to get the flag**

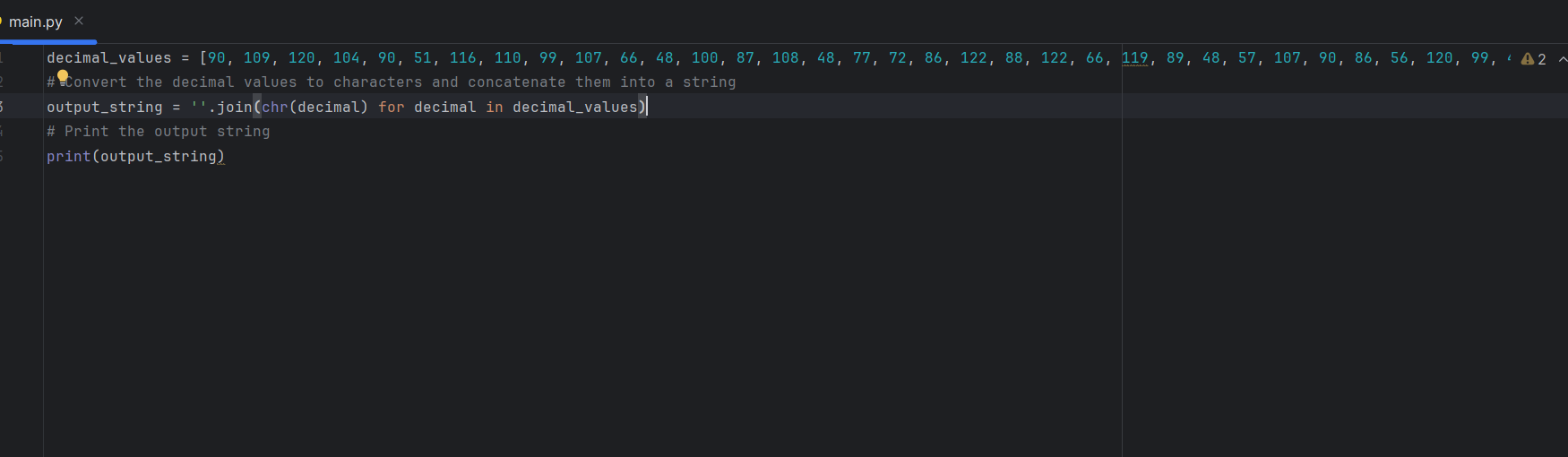
An easy way to get that character from each opcode rather than copying and pasting each one is to use tshark in command prompt to find the sequence of those characters, if we run the following command: tshark.exe -r C:\Users\Lenovo\Downloads\ARP+Storm.pcap -T fields -e arp.opcode , we will get the decimal representation for each character as shown in the image below.

A screenshot of a computer

Description automatically generated

**Second step to get the flag**

Now we want to convert from the decimal representation of each character to its actual value using ascii code, we can do that by running a python code to do that job for us. Here is the code snippet:



Then the output of that code will be our encoded flag which is: ZmxhZ3tnckB0dWl0MHVzXzBwY09kZV8xc19BbHdAeXNfQTZ1U2VkX3QwX3AwMXMwbn0

**Final step to get the flag**

It is common that if the flag is encoded and it ends by ‘=’, then that means that it is encoded by base 64, We can also run python code to decode that flag which is the following:

A screenshot of a computer

Description automatically generated

After that we will get our desired flag and the answer of our problem which is:

flag{gr@tuit0us\_0pcOde\_1s\_Alw@ys\_A6uSed\_t0\_p01s0n}