**CHAPTER- 1.2 : NETWORK SCANNING**

* + 1. Definition:-

Network scanning is a procedure for identifying active devices on a network by employing a feature or features in the network protocol to signal devices and await a response. During a network scan, all the active devices on the network send signals, and once the response is received, the scanner evaluates the results and checks to see if there are inconsistencies.

* + 1. Purpose of Network Scanning:-

Network scanning is mainly used for security assessment, system maintenance, and also for performing attacks by hackers.

The purpose of network scanning is as follows:

* Recognize available UDP and TCP network services running on the targeted hosts.
* Recognize filtering systems between the user and the targeted hosts.
* Determine the operating systems (OSs) in use by assessing IP responses.
* Evaluate the target host's TCP sequence number predictability to determine sequence prediction attack and TCP spoofing.
  + 1. Tools Required:-

1. Kali Linux
2. Python3
3. Pycharm (Python IDE)

ARP: Address Resolution protocol is used for discovering clients on same network (link IP address with MAC address)

* + 1. PROCEDURE:-

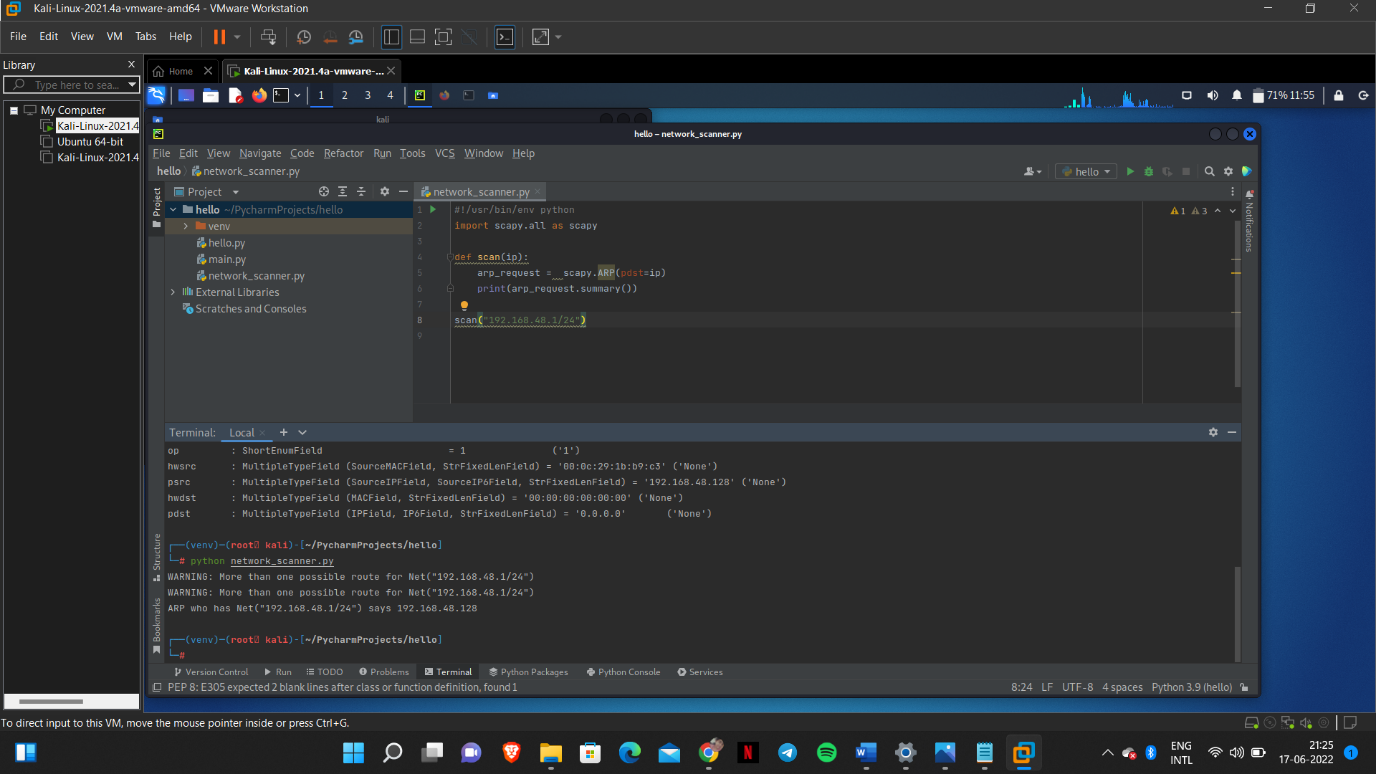
Step1: *Create an ARP request directed to the broadcast MAC address asking for IP*

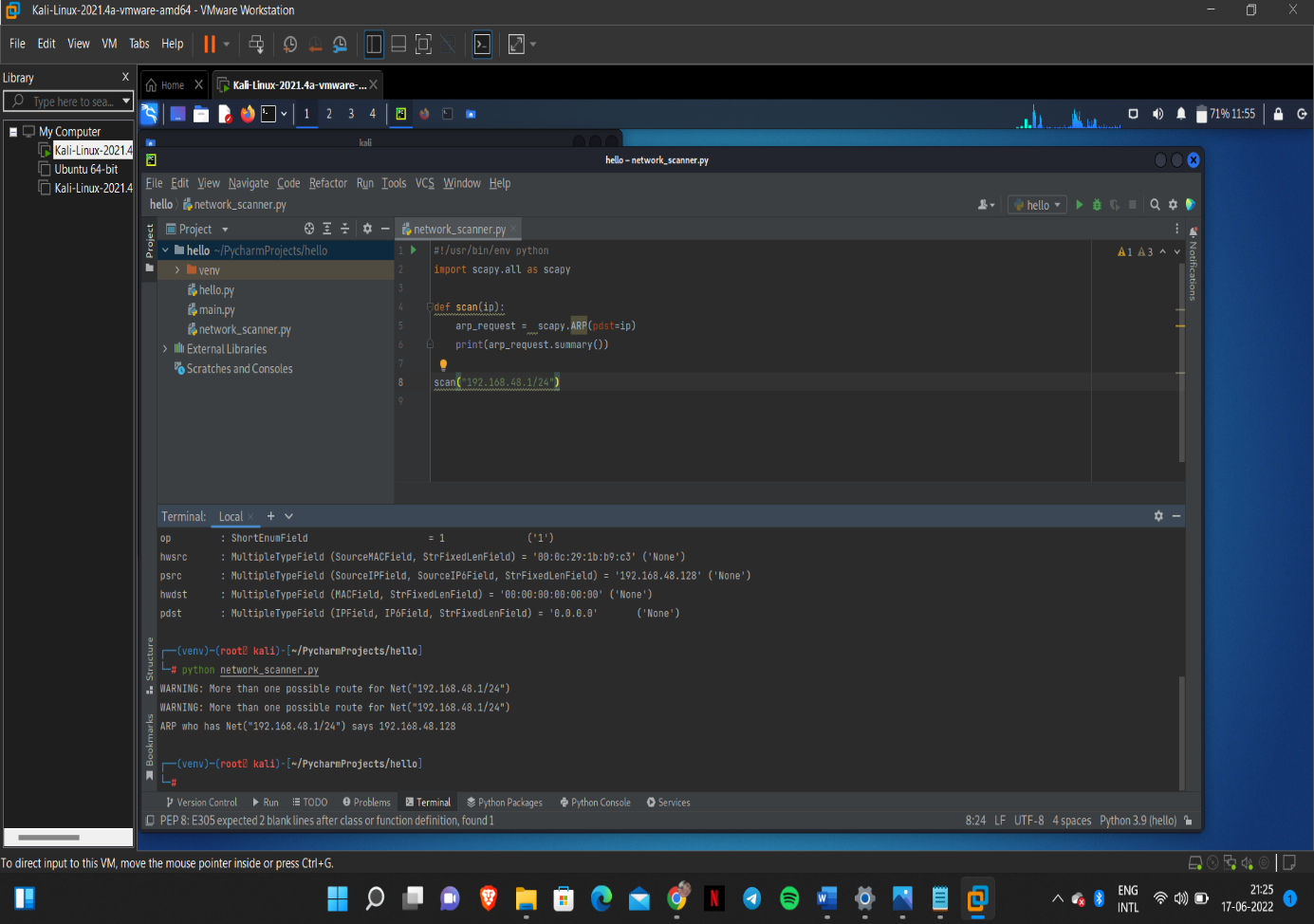
The first step of our algorithm or the first simple problem that we need to solve is being able to create packets. So, the packet that we need to create has two main features:

1. Use ARP to ask who has target IP.
2. Set destination MAC to broadcast MAC

That is, to use ARP to ask who has a specific IP and then we need to direct this packet to the broadcast MAC address so that it gets delivered to all the clients on the same network.

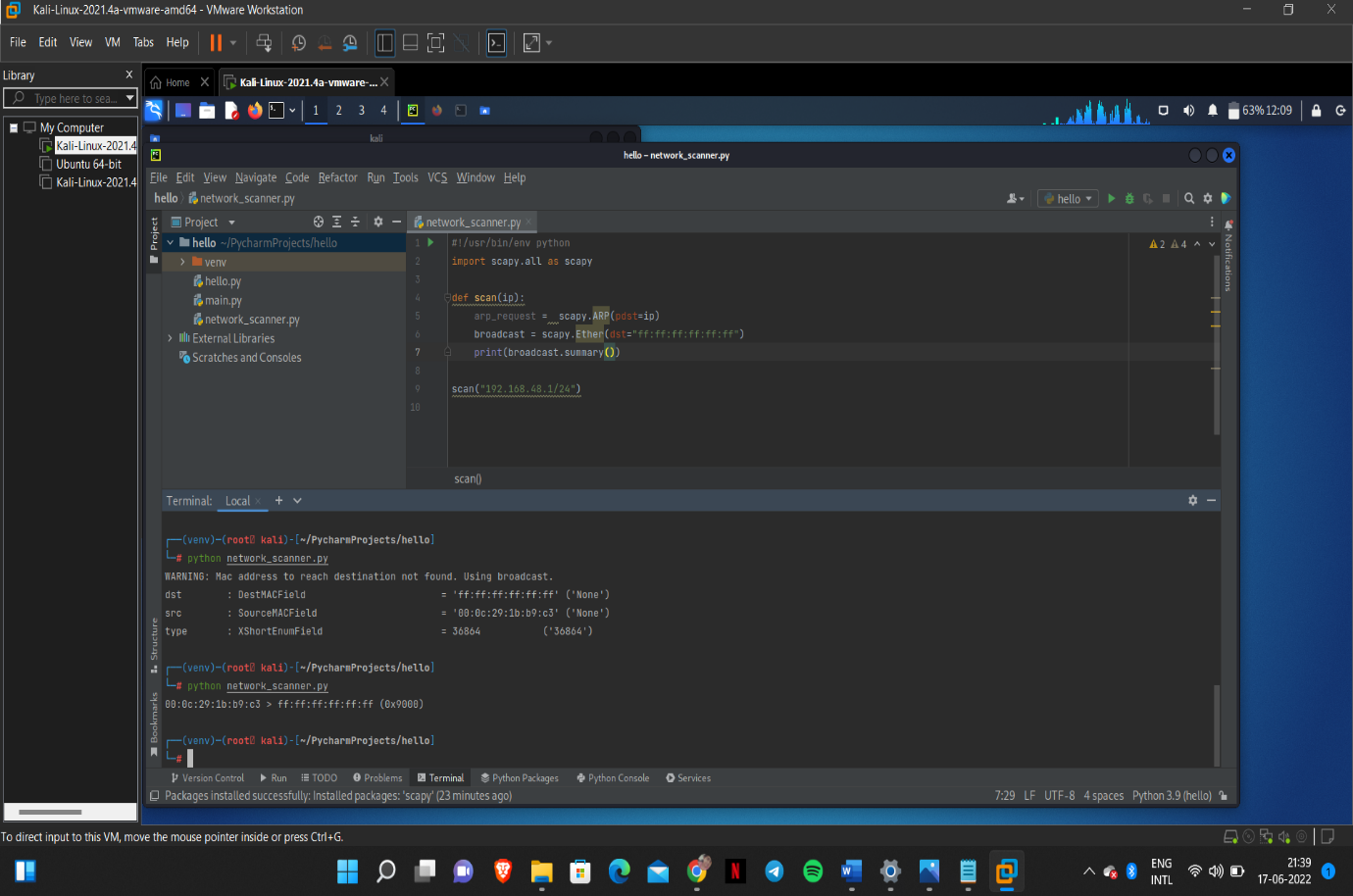
1. Use ‘’*pdst’’* whose default value is 0.0.0.0

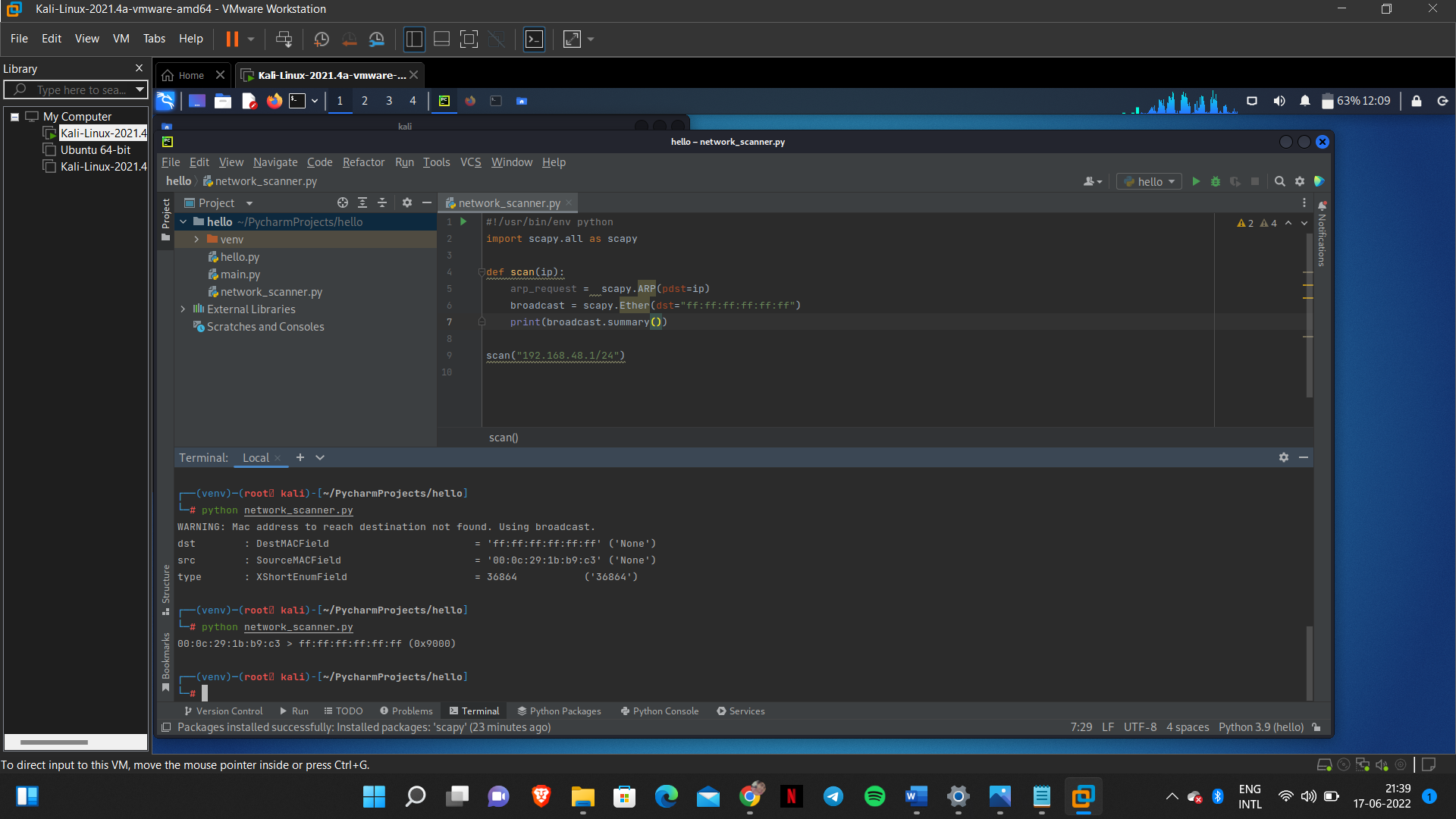




1. Now set the destination mark to the broadcast MAC address to make sure that this will be sent to all the clients on the same network.

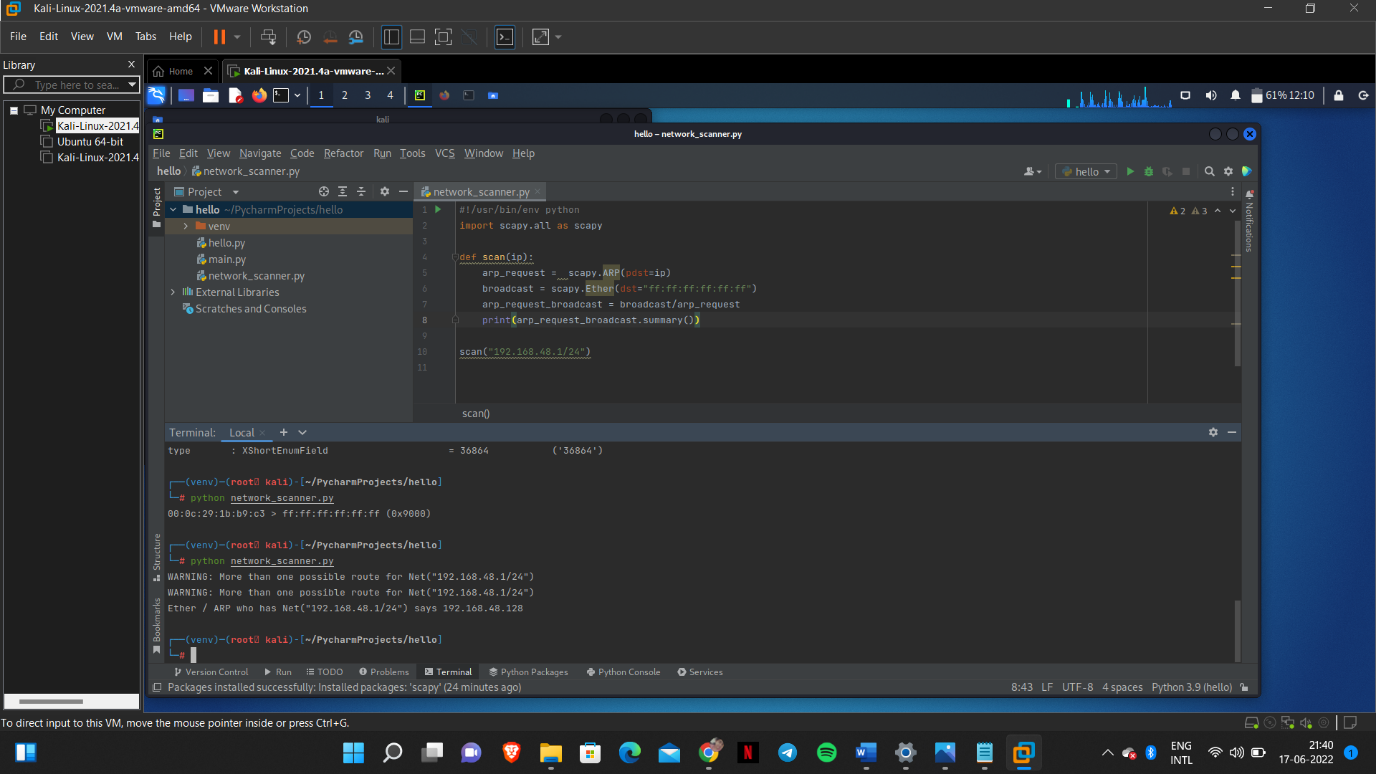
Create an Ethernet frame that will be sent to the broadcast.





Combining the above two steps, i.e; a) and b)

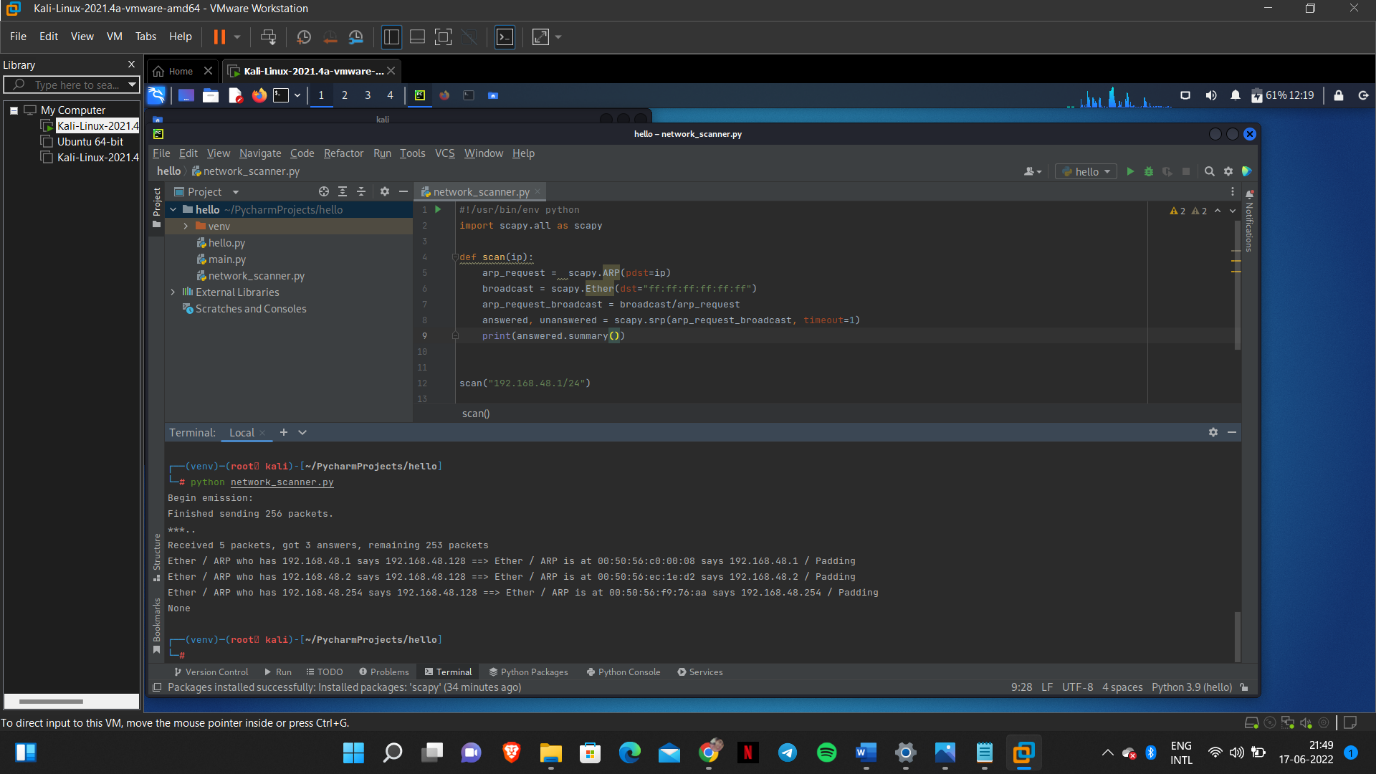


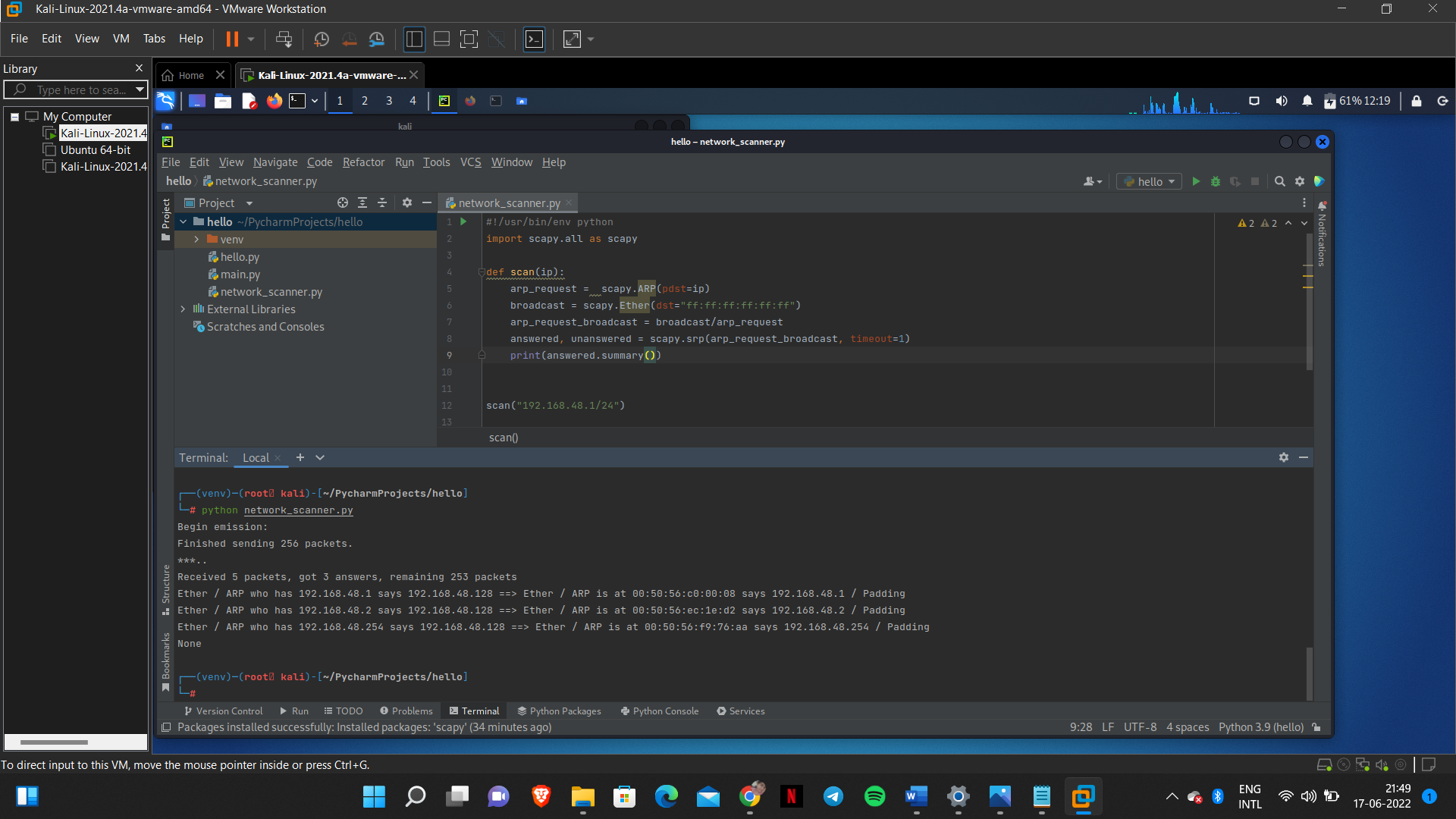


Step2:- *Send Packets and receive response*

In this step we will try to send this packet into the network and wait for the response.

So the scapy function that we'll use to send this packet is called *srp*, this will send the packet that we give it and receive the response.



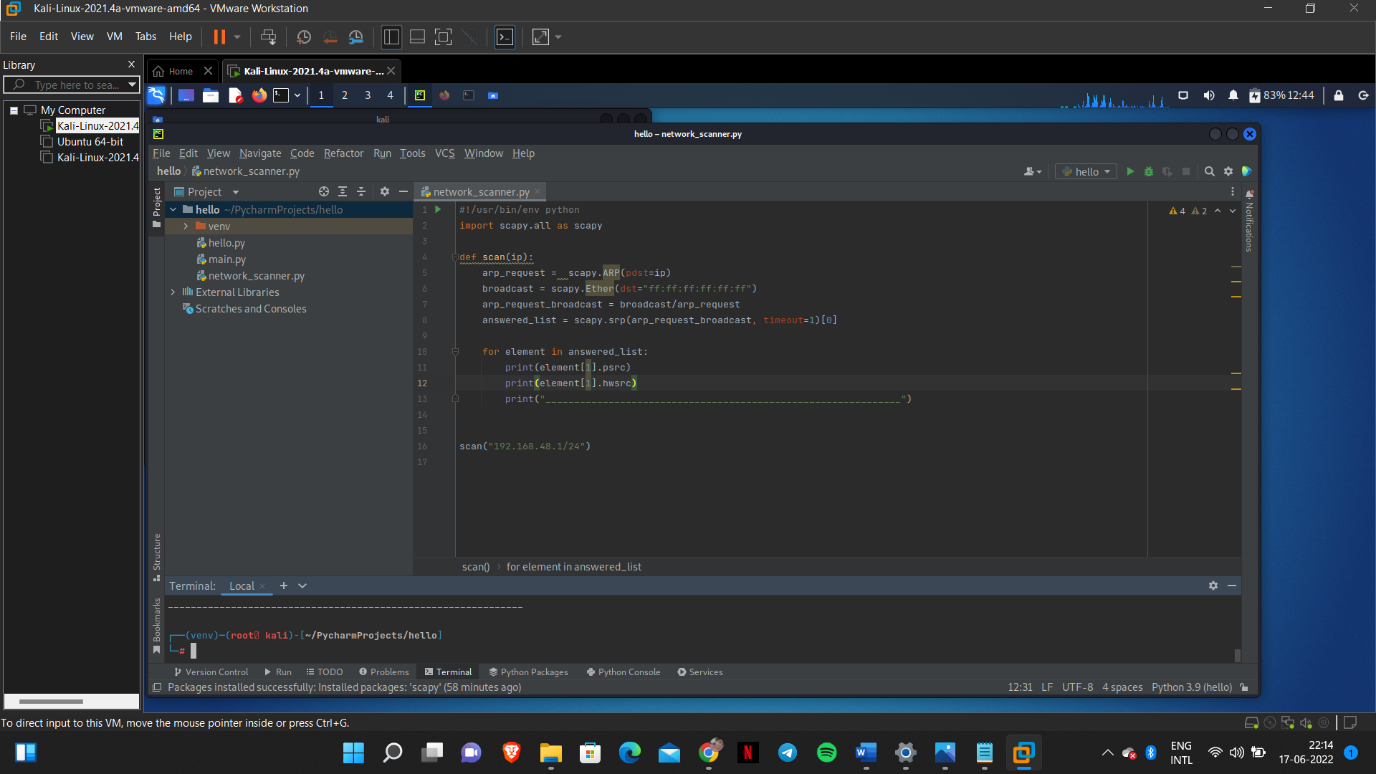


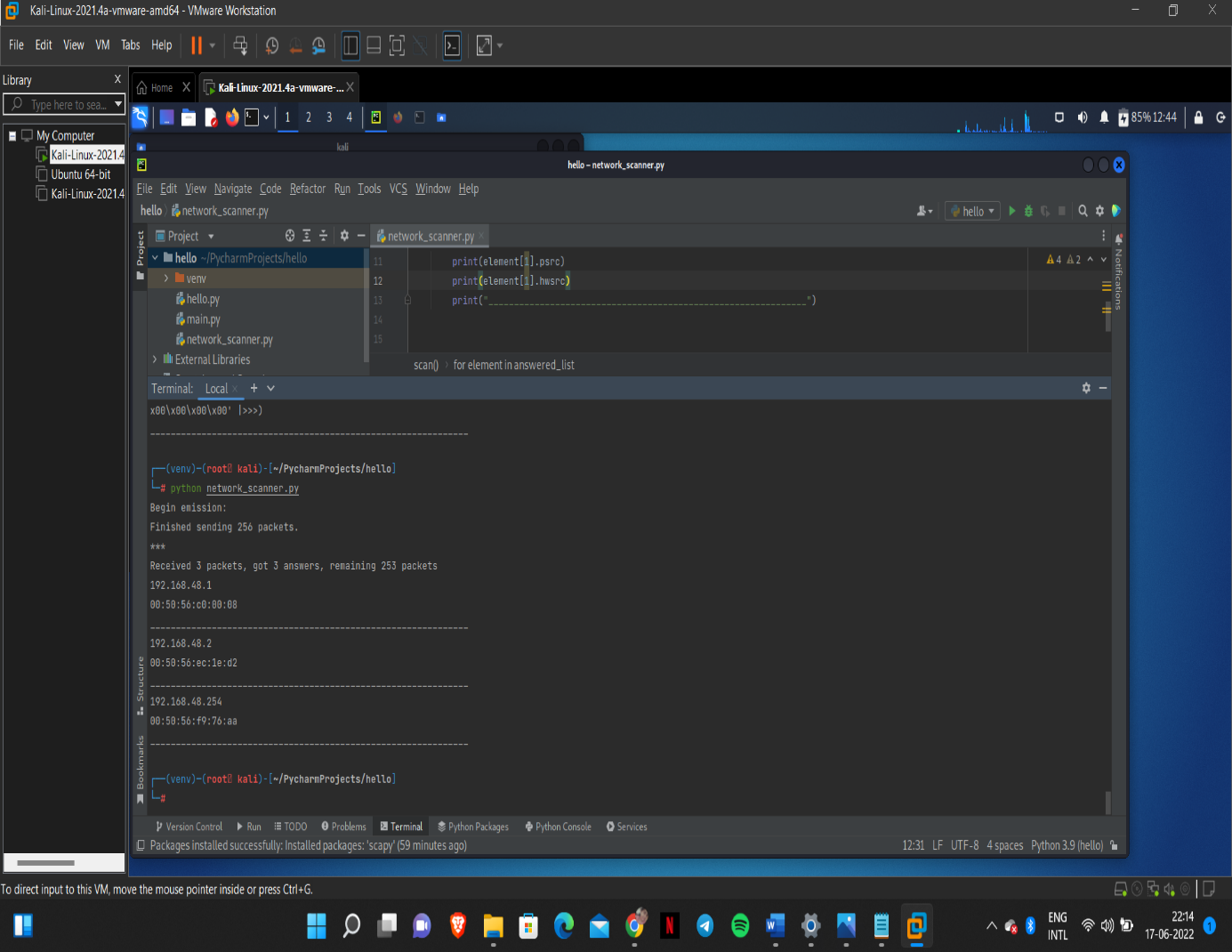
Step3 :- *Parse the response*

The next step is parsing the response that we got in step2.

There is a lot of unwanted information, so to extract the useful information we will use the ‘list’ function.

And also to make it look readable and legible we modify the code

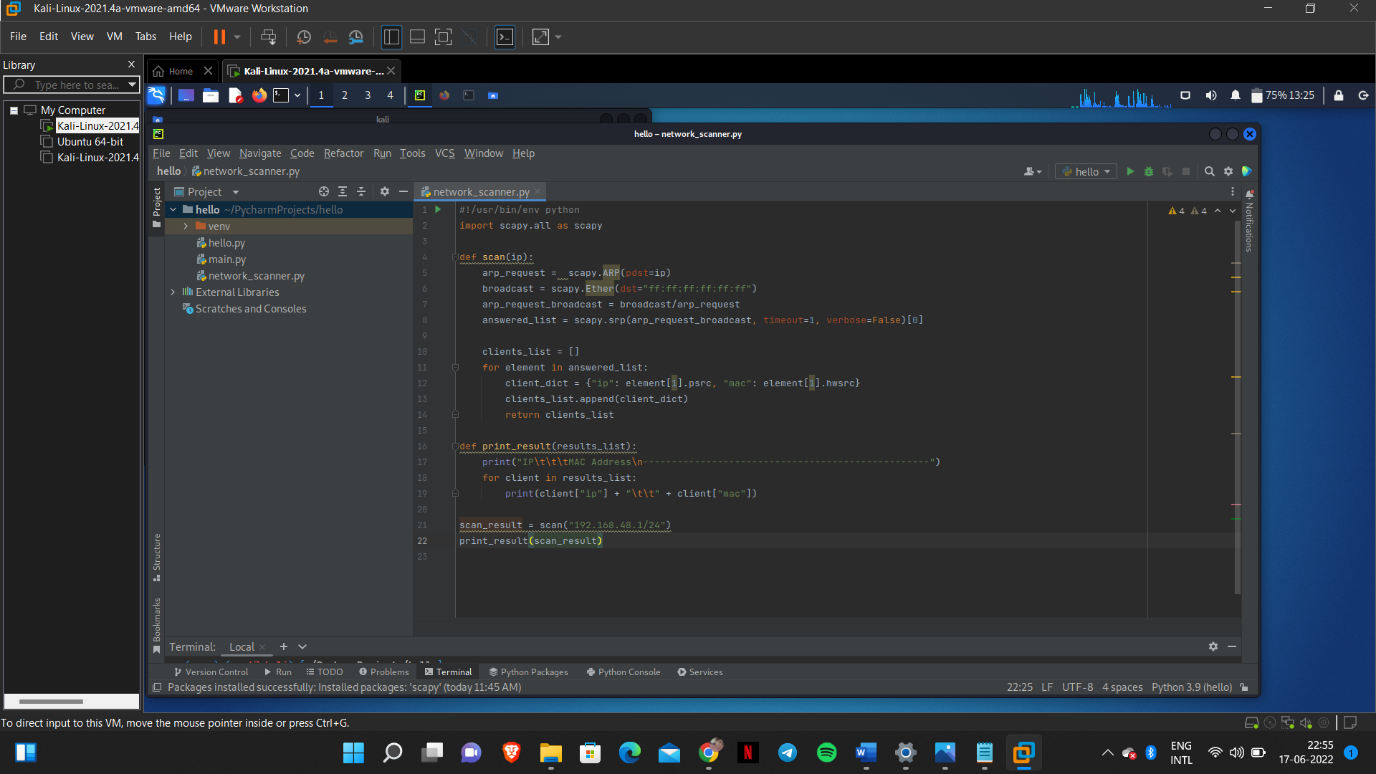




Step4 :- *Print result*

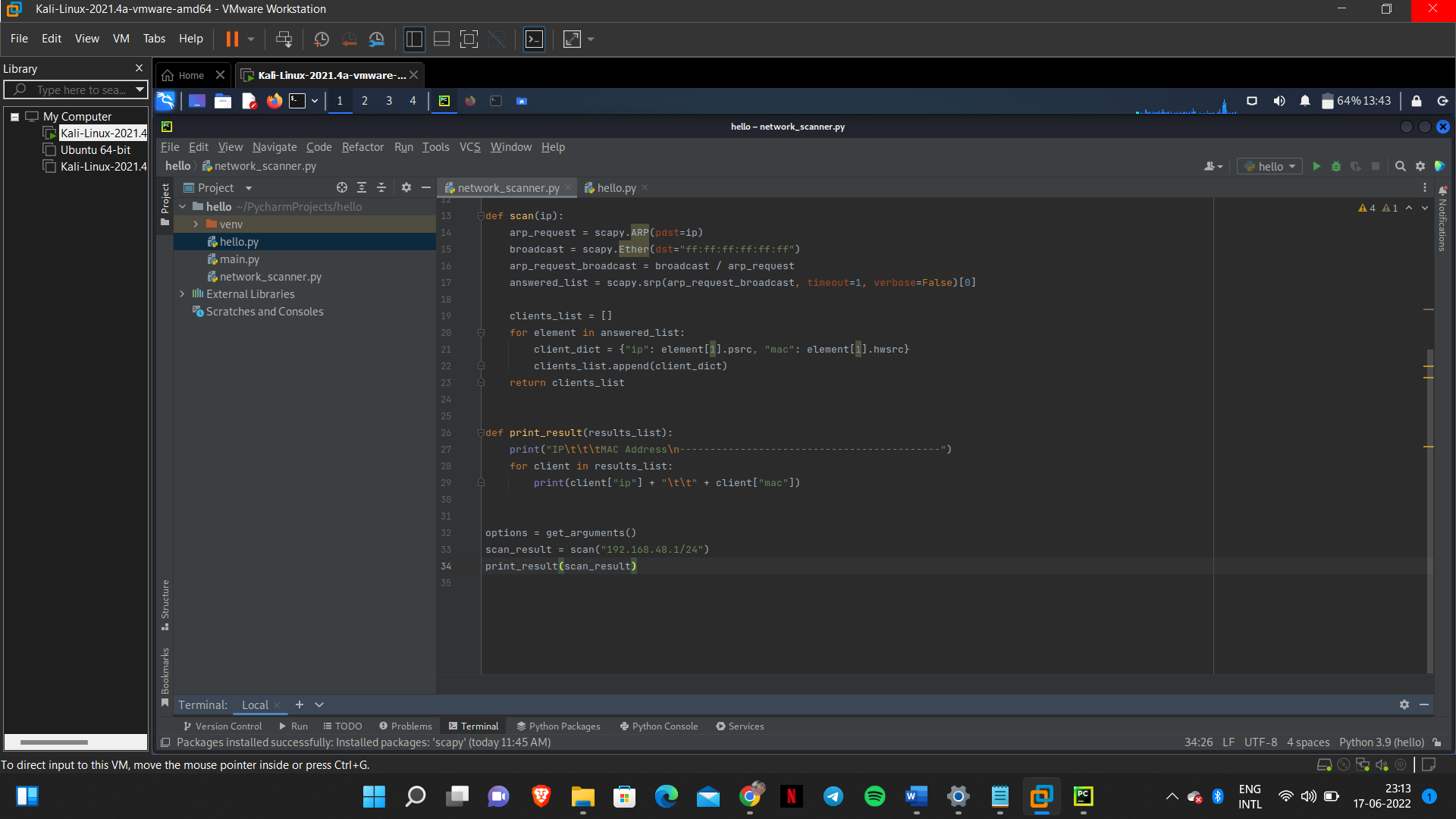
Improving the print statement to print the results in a nice table format

Trying to improve the code using a list of *dictionaries*

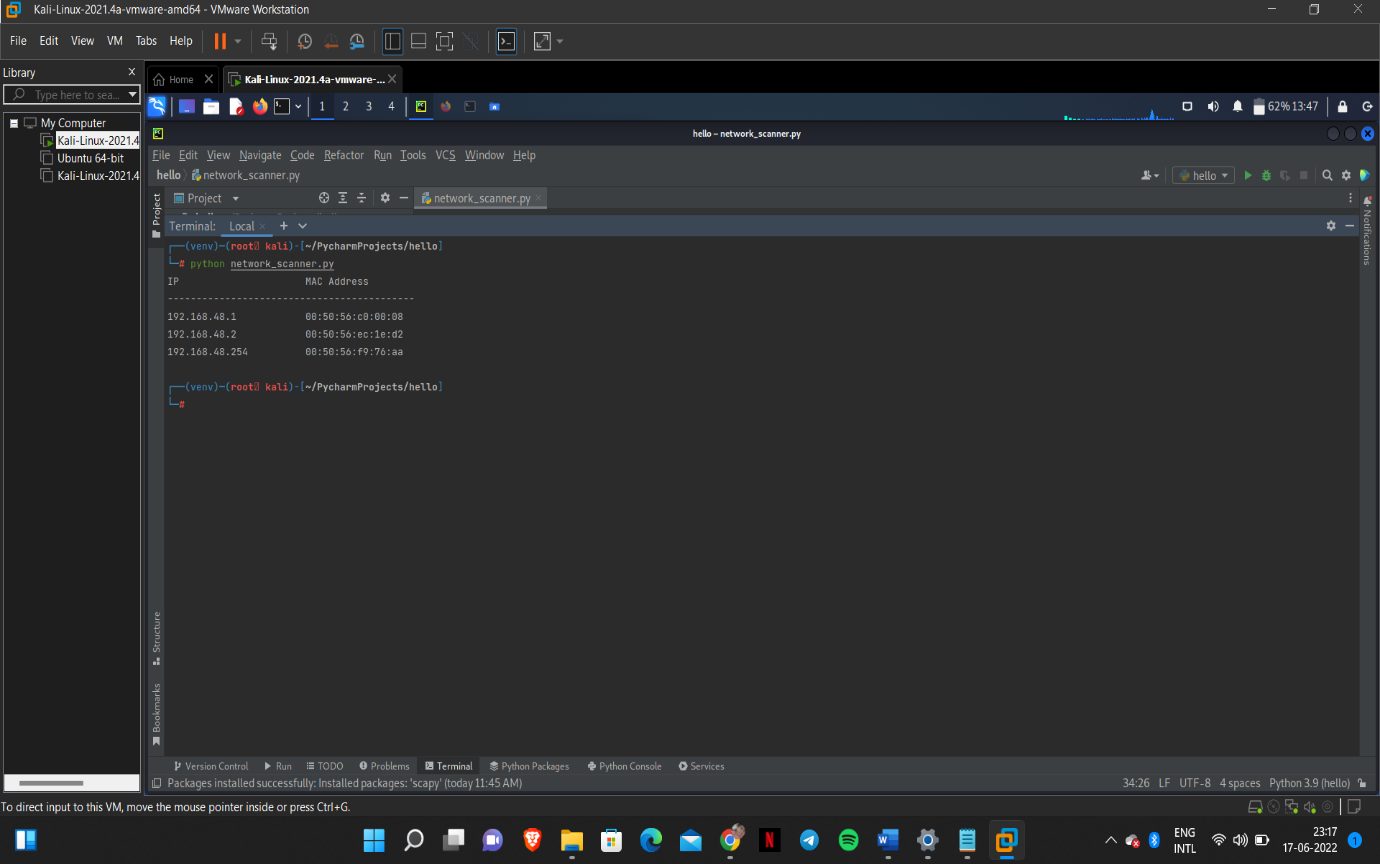


So, the final ***Python program*** for Network scanning is





***OUTPUT***:



**1.2.5** **Execution**:

*Command*:

>python3 network\_scanner.py

*Output*:

