Network intrusion detection system

Its basically a decoy server, on which when a client connects to it detcts what type of attack is happening, it detects where it is coming from ip address, mac address etc

And most importantly it gets all the logs of it which we can analyse later on to see if there is any patch which which should be done to their network or not, basically analyse all the traffic what that hacker is trying to,

There are many parts in making a network intrusion detection system but three most important components of it client, server , traffic analyser.

Tech stack we need to use and learn

Socket programming

Networking concepts and protocols

Python network programming

Bash for log analysing and automation

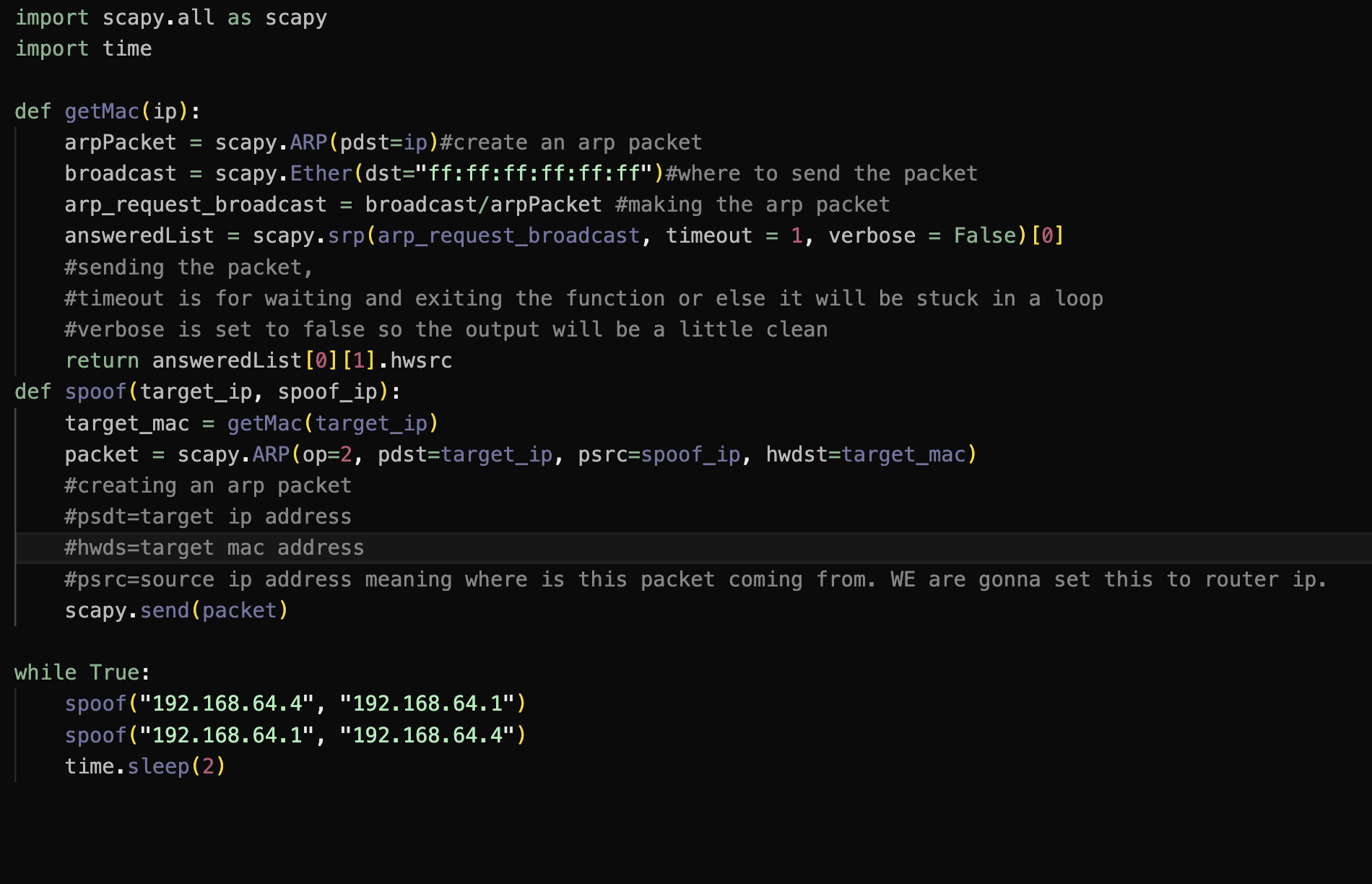
Web development for a unique dashboard

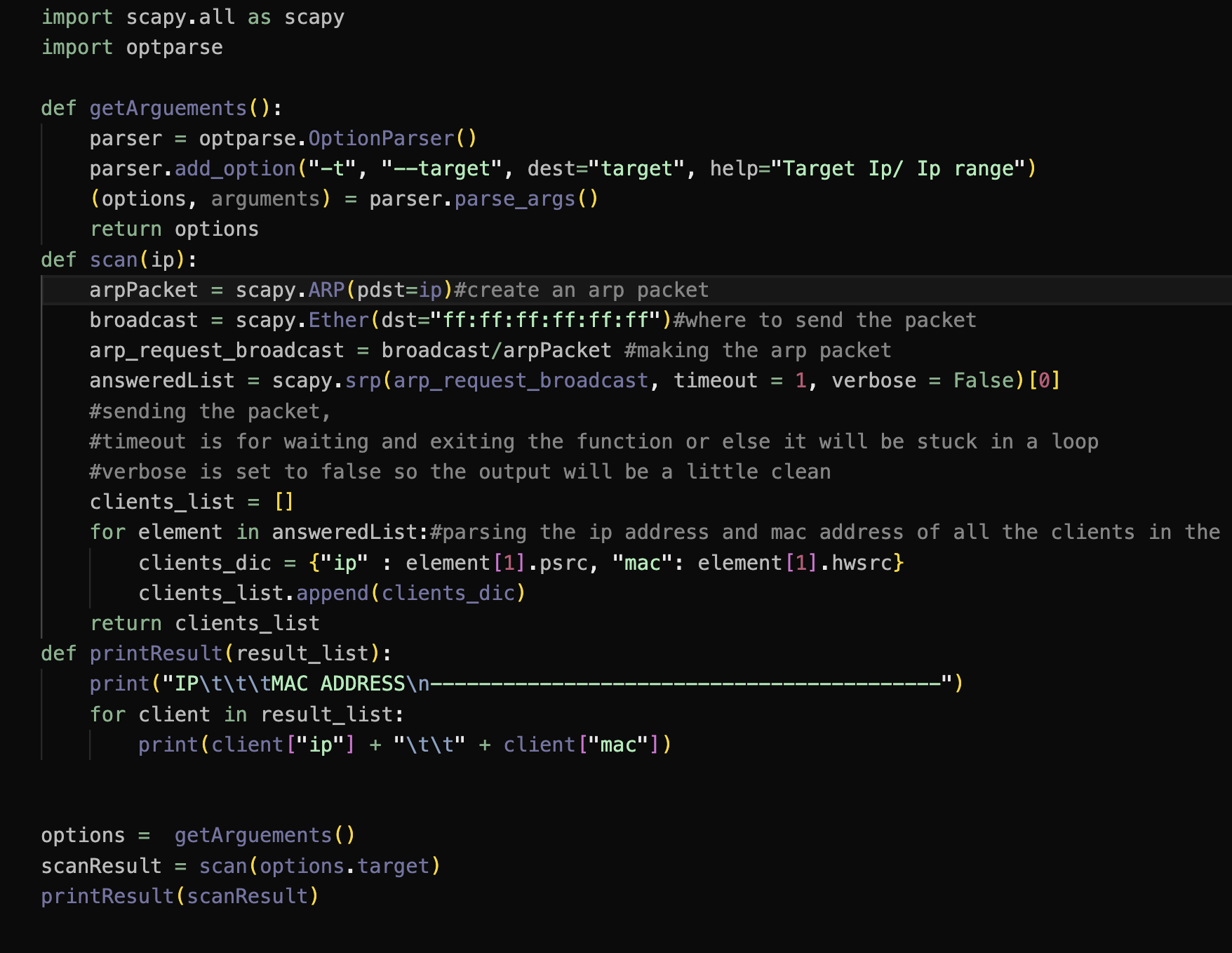
Backend to connect that dashboard

Right now we are still in learning phase and have started from networking and programming concepts in python

Module used in python

* Scapy
* Requests
* Time
* Optparse
* Os
* Sys

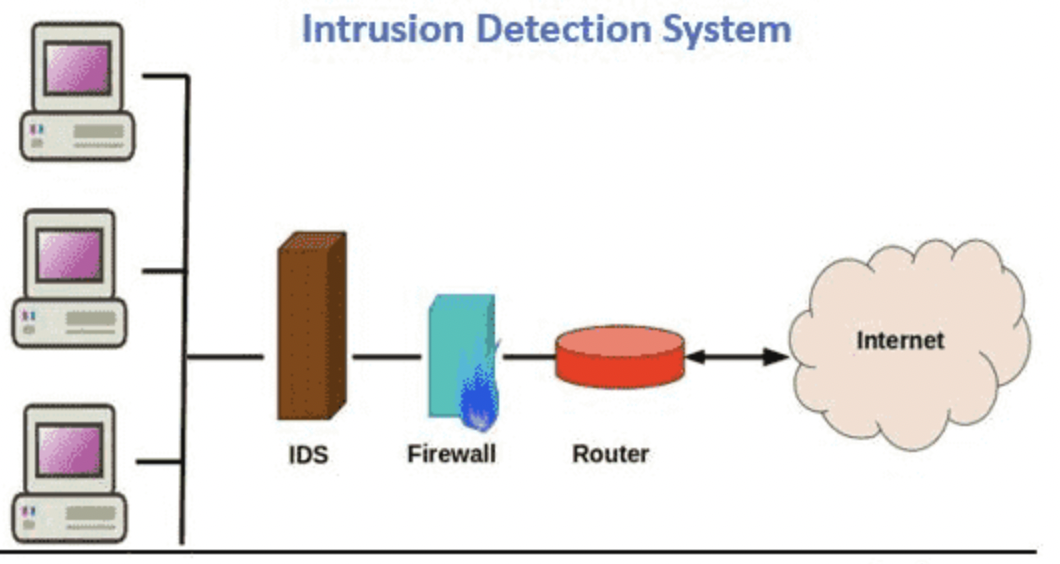




Right now we have a working model of arp spoofer and network scanner which basically puts the machiene in the middle of client and server.

After this we will work on packet sniffer in which we will redirect all the traffic to traffic analyser or log analyser.

WE are still in learning phase but this is the core concept we are gonna use in our tool.



What we learned so far is that scapy module is used for all the network protocols and communication between two networks and opt parse module is used for parsing all the data that comes from scanning the network or data that sniffed between arp spoofing.