Save\_class.py

This file aims at explaining how the scoring function used in the save\_class.py python file does. It will first explain how the mutability problem has been solved for the get\_os and get\_ports function.

# Get\_os:

In this function, we want to store every information we obtain on the os through nmap, to a python dictionary.

To do so, a copy of the dictionary **os\_result** (**os\_result\_copy**) is created. Then, we simply copy our original dictionary, **os\_result**, in this new dictionary. The result is we now have 2 different dictionaries, each of them pointing to a different memory slot. In other words, if one of them is modified, the other one will stay unchanged. So, the **os\_result\_copy** is then appended to **os\_copy**, which is an intermediate list. Finally, when we have finished storing data in this intermediate list, we end by adding it to **os\_list.**

Mutability problem of python is solved here: if we try to modify the dict and the list directly, it will overwrite existing entries with the new ones, when we simply need to create a copy that will point to a different memory slot and thus not be modified as the other would)

The get\_ports function got its problem solved the same way, with different variable names.

# Score\_firewall:

The goal for this function is to build a score that depends on 3 factors: during the scan, has the OS been found as a firewall-type OS? Did we find the MAC prefix of the scanned device in our list? Do the protocols found for this host fit in the 3 different lists (web\_server, mail\_server, other\_services), meaning this device has traffic from different types of devices and therefore may be a firewall?

To do so, we used IF iterations to determine which score to attribute, depending on the cases encountered:

- If all 3 counters are > 0, we have more chance of having a firewall, since it has protocols belonging to different classes (mail server, web server or other services concerning firewalls).

- If 2 out of 3 counters > 0, it has a chance of being a firewall, but since it is more uncertain, the final score added will be lower, unless we find with a second scan some protocols that weren’t found in the first one.

- If 1 or none are > 0, whether all ports are filtered / closed or we simply did not scan a firewall: the score added will be 1/2 times the protocols found (if there are some found).

For the second part, we're checking if the OS has a firewall type and if the MAC address is found in our list.

If all 3 conditions are met (meaning our 3 protocols counters are > 0, the scanned OS is a firewall and the MAC address corresponded to one in our list), an important value is added to our score. If only 2 of these conditions are met we'll add a slightly lower value. If only 1 condition is met, we will add a small value since it's more likely to not be a firewall (we do not have enough information to establish the device's nature).