The Complete Documentation of My Firewall – Ex5

Disclaimer: I omitted parts that I already explained in Ex 4 Documentation and only explained new mechanics I added in this assignment.

In this assignment, I had to implement IPS and DLP.

Since in the IPS the one im trying to protect is a server, so I had to add support for dual direction proxy, meaning that both sides now can be the "client" in the proxy connection.

To do that, I had to save another state in each connection stating the side of the client in the proxy connection. I also added support and checks for each function to ensure that the function change the right routes and everything work as intended.

I wanted to note that sending a port to the port table using the port device in the user mode, was not the same as before and I also indicated the side of the connection. As always, everything is well documented in the code.

The flow and the logics are all the same as Ex 4.

Protection – to protect from attackers in the IPS part, I striped the X-WCPAY-PLATFORM-CHECKOUT-USER header from the packet so the server will not relay on the user to determine the user ID.

More In-Depth explanation in the Presentation.

To run the ISP you have to run the python file named ISP.py

DLP – To determine if a text is C code or English text I extracted a feature vector from the text and predicted if the text is C or English using SVC model I trained with a lot of data (Mails, Wikipedia, and TONS OF C CODE).

The feature vector contained:

* Average Line length
* Fraction of C key-words in the text
* Fraction of special characters in the text
* Fraction of Lines that end with semicolons (';').

To run the DLP you have to run the python file named [protocol]DLP.py while the model in the same directory and where protocol can be smtp or HTTP.