Project

You can work by groups of 2 people. The project is due on the 18/10/2024 at 17:00.

Please, send your project to eulalie.verhulst@lecnam.net and mario.patetta@lecnam.net, be sure to include [USRS78 Project] in the e-mail subject.

Attacks project

Create a Python project in which you simulate and detect DOS attacks. The detected attacks must be logged into a local csv database.

Using the database, answer the following questions on a Juptyer Notebook and illustrate your answer using a plot.

Where are the suspect IP addresses located?

What is the attack that generated more packets?

What is the attack that generated the largest traffic in terms of bytes? And in bytes per second?

DOS Attack simulation and detection

To simulate some DOS attacks, you can get help from the joint script. You can use two computers: one to launch the attacks and the other as victim. You can simulate IP addresses using a random method. Additionally, you should enrich the script with two extra features:

- specify target IP address and type of attack as arguments while launching the script;
- introducing a new parameter "attack duration" to make so that the script automatically stops after that time, and pass that as argument as well.

To detect the attacks, you can use the SniffnDetect module. The module can be found here: https://github.com/priyamharsh14/SniffnDetect. Keep in mind that open source code may contain bugs, so be sure to fix them as needed (and feel free to notify the author if you'd like to be helpful!).

Data manipulation and visualization

To answer the questions, you'll have to log the detected attacks on a local csv database. You can answer the questions using a jupyter notebook in which you'll provide a snippet of the code, a text answer and a plot to illustrate your answer.

To get the location of the suspect IP addresses, you can use a web request to ip-api.com to get the country. The data can then be plotted on an map.

Deliverable

You'll provide a copy of your python project. The project should be well commented and organized.

The project should contains all the scripts and the notebook.