Enhancing the ConTackGen Plugin for WEKA

Adan Raynaud, William Benedico, Rayan Rochdi, Frederic Dinahet

Supervised by: Nida Meddouri

EPITA, CYB 2

1 Introduction

Efficient data management is crucial in machine learning. The ConTackGen plugin was originally developed by students to automate the creation of large datasets for machine learning, especially for DDOS attacks. This automation saves time and reduces errors. However, the plugin was limited by its interface and its one and only attack. We have updated it to be more understandable for the general public, and to support an additional Man In The Middle attack.

2 Materials and Methods

We started with a student project from the previous year that works, but had some technical limitations, especially in automation and output management. Our project was divided into several parts: making the interface more pleasant and understandable, solving technical issues related to outputs and adding a new attack (MITM). First, we updated the code to make the interface more understandable. Then, we studied and updated the attack generator to implement a new type of attack, which is the Man In The Middle. Finally, we wondered about the problem concerning output management, but the lack of time and expertise made the technical problem still exist.

3 Results

With the updates, the plugin integrates a new type of attack, with a nicer GUI. The latest students have also started implementing another attack; it

is enough to distinguish real packets from attack packets.

4 Discussion

These improvements have significantly helped the plugin's ease of use, making it intuitive with two relevant attack types that have an important place in the cybersecurity field while being relevant to machine learning researchers. The ability to generate DDOS and MITM attack data is particularly valuable, as it helps develop algorithms capable of detecting and mitigating these threats.

5 Conclusion

The updated ConTackGen Plugin is now more robust, supporting a wider range of computing environments. Future work will aim to introduce more attack types and advanced features to further enhance the plugin's utility and features, and maybe get rid of Docker.