

## Abstract - Giuseppe Piombino s280117

The constant growth of Denial of Service (DoS) attacks stands as a significant threat in our digital and ultra-connected world. Their danger is enhanced by the difficulties in their detection. In fact, most of the various detection methods do not provide an exhausting and immediate solution to the problem. In particular, the detection of slow attack results problematic and requires a considerable human effort. Modern solutions have opted for an artificial intelligence (AI) oriented approach, which consist of creating of a model trained with a representative dataset, capable of recognising hardly detectable patterns and doing so automatically. Furthermore, the necessity to keep note of traces and proof of the attacks emerged, because they may be lost in the tentative of rebooting the system. In this environment takes application the field of the digital forensic science, that focuses on identifying, acquiring, processing, analysing and reporting on data stored electronically.

This thesis presents the development of an AI model designed to detect DoS attacks automatically within a distributed infrastructure. The experiment enlightens the traces left by the DoS attacks and demonstrate the efficiency of the AI in the field of the digital forensics. Once the data about the connections are collected, in fact, they can be analysed on the run or, more importantly, from the stored data log. The distributed system has been emulated by means of a Docker-based virtual network. The virtual network not only serves practical applications but also has a pedagogical purpose, facilitating educational exploration of network security concept, especially those that can be experimented with extended Berkeley Packet Filter (eBPF).

The data for the training and testing of the AI model were sourced from a dataset from a previous work, and the extraction of relevant information for the analysis happens by means of tools called tcpLife and tcpTracer, implemented with eBPF. The AI model employed is a Multi-Layer Perceptron (MLP), which has been compared, as a baseline, with the Random Forest classifier.

The system has been tested with several types of DoS attack simulations, such as SYN flood, HTTP flood, Slow HTTP and ICMP flood. To perform the attack, have been employed the software programs hping3, HULK and Slowhttptest. Finally, an analysis of relevant data, collected with the previously cited tools, is conducted, offering significant conclusions about the efficiency of the system.

The project contributes to the field of the network security by demonstrating the potential of AI model in recognising specific types of DoS attack, especially in the forensic practice. Furthermore, the implementation of the virtual network with Docker, underscores the practical and educational value of the developed system, offering a platform for both real-world applications and academic labs.