|  |
| --- |
| **Name:** Toufic Fakhry - Marcelino Keyrouz |
| **ID:** 243223 – 244064 |
| **Submitted To:** Professor Youssef El Bakouny |
|  |

****

**Machine Learning and Deep Learning – Iteration 1**

**Network Intrusion Detection System**

In this iteration we have tried to train a model to classify a network traffic as malicious or not, to help identify attacks in a network traffic log.

**Technical Description:**

We have built 2 models, using CNNs and Logistic Regression.

1. **CNNs**

Uses convolutional layers to learn spatial features automatically and hierarchically, in the context of network security, analyzing patterns in sequential data like network traffic.

1. **Logistic Regression**

Well suited for binary classification, and it helps classifying the traffic as attack or benign.

1. **Attack Types**

The models cover the below attack types:

DDos, Port Scan, Bot, infiltration, webattack|Brute force, Web attack|XSS, Web attack|SQL Injection, FTP-Patator, SSH-Patator, DoS slowris, DoS slowhttptest, DoS Hulk, DoS GoldenEye, Hearbleed

1. **Network Environment**

Online Server

1. **Performance Goal**

Desired Accuracy >= 90%

Cost of misclassification:

FPR: tolerable up to 2% with the presence of a SOC team.

|  |
| --- |
| **GitHub Repo** <https://github.com/marso16/ML-Proj> |
| **Data Source** <https://www.kaggle.com/datasets/cicdataset/cicids2017/data>  **Videos** <https://drive.google.com/drive/u/2/folders/1IQ9LdVAZXQ3VUqeFDgYW6r1Mi41NZQLH> |