Network Intrusion detection based on Machine Learning algorithms (Group 1)

Context ：

With the development of the Internet, cyber-attacks are changing rapidly and the cyber security situation is not optimistic. With the increasingly in-depth integration of the Internet and social life, it exposes us to increasingly serious security threats. How to identify various network attacks, particularly not previously seen attacks, is a key issue to be solved urgently.

Objectif:

The project task is that given a set of statistic information of a network flow, identify whether this flow is benign traffic or intrusion, based on a model trained from a set of already labelled data set containing both benign and intrusion traffic

Dataset： CIC-IDS-2018

URL for downloading the Dataset : https://registry.opendata.aws/cse-cic-ids2018/

Environment

The software tool used in the project will be sklearn, numpy, and pandas. All the evaluation experiments can be carried on a DataCenter of ESME

Algorithms

The following machine learning based algorithms should be tested for training the model and predict the new network flow:
Random forest classifier
Gaussian naive bayes classifier

Performance Analysis

To measure the performance of each algorithms, the precision, recall, F1 score, and time expenses should be evaluated