# **INTRODUCTION**

* In recent years, the attacks that target system availability has increased. One of the most effective availability attacks is the DOS attack (Denial of Service) which results in shutting down the server or the system by flooding the victim with traffic or sending it information that triggers a system crash.
* Systems can’t detect if the incoming heavy traffic is a normal heavy load traffic due to multiple users sending traffic at same time or it’s a DOS attack.
* So, by building a DOS classifier model, system can predict if the incoming traffic is an attack or not, and therefore they can stop it or alert the security engineers about an upcoming attack.
* Fortunately, there is an available dataset that we will use. NSL-KDD dataset which is a well-known benchmark dataset used for Intrusion Detection Systems, it contains approximately 125,000 records with 41 features and labelled as (0 – Normal, 1 – Attack).

# **TOOLS**

1. **Python Programming Language Libraries:**
   * Sklearn 🡪 To apply machine learning algorithms.
   * pandas/numpy 🡪 To read the dataset and preprocessing it.
   * matplotlib/seaborn 🡪 To make visualizations, and analysis on the data
2. **Jupyter Notebook:** 
   * An IDE to run python codes and test each code in a separate cell (mostly used for developing AI systems)