Observations and Training Information

Team Name: Hawk Eyes

Problem Statement: DDOS attack

1. Training Methodology:

- First, the data is converted into per second traffic flow in the network. The following fields were taken for analysis in the **nth second**:
  - Total packets.
  - Total TCP packets.
  - Total UDP packets.
  - Total ICMP packets.
  - Total number of TCP (SYN) packets.
  - Total number of TCP (SYN-ACK) packets.
- Now we have time-series data which demonstrates the flow of network traffic.
- The next step is to break the file into chunks of 60 seconds and each chunk is labeled same as file i.e. benign or malicious.
- Now we use LSTM model to train on the dataset.
- We have a sequential model with two LSTM layers and one dense layer.

```
model = Sequential()
model.add(LSTM(256, return_sequences=True, input_shape=(seq_len, 6)))
model.add(LSTM(32, input_shape=(seq_len, 256)))
model.add(Dense(1,activation='sigmoid'))
```

2. Testing Methodology:

- During the time of testing the same pre-processing step, as in training is done. Now, even if one chunk of 60 seconds is predicted as Malicious then the whole file is labeled as malicious.

3. Results:

- We achieved 100% accuracy on the testing dataset. The spit was 75-25 between training and testing datasets.
- Total number of files used in testing = 15(benign) + 22(malicious)