DoS Attack Detection using Machine Learning

Objective:

This project detects Denial-of-Service (DoS) attacks using machine learning models to classify normal vs. malicious traffic.

Methodology:

- Dataset loading

- Data preprocessing

- Train-test split

- Random Forest ML model

- Evaluation metrics

Technologies Used:

Python, Pandas, NumPy, Scikit-Learn, Jupyter Notebook

Result:

Model successfully detects DoS attacks with high accuracy.

Future Enhancement:

Integrate real-time detection using deep learning.