Advances-in-Network-IDS-using-different-classifiers

This project is an implementation of Realtime Network based Intrusion Detection System using different machine learning techniques. Our proposed model is to implement the architecture of multimodel based Anomaly IDS with Neural Network (NN), Long short-term memory (LSTM) and Random Forest. We have integrated NN with Hidden Markov Model to improve our model. We have also tested our model by performing realtime attack on our model.

Dataset

We have used CIC-IDS 2017 dataset. It contains benign and the most up-to-date common attacks, which resembles the true real-world data (PCAPs). It also includes the results of the network traffic analysis using CICFlowMeter with labeled flows based on the time stamp, source, and destination IPs, source and destination ports, protocols and attack (CSV files). To download the complete Dataset Click Here. Once the download is complete, place the folder "Model_Training/Dataset/" directory.

Create python3 virtual environment using venv

```
python3 -m pip install --user virtualenv
python -m venv ids_env
source ids_env/bin/activate
```

Install CICflowmeter

```
git clone https://github.com/ayush1409/cicflowmeter-edited.git
cd cicflowmeter-edited
python setup.py install
cd ..
```

Install Network IDS Django application

```
git clone https://github.com/ayush1409/Advances-in-Network-IDS-using-different-classifiers.git
cd Advances-in-Network-IDS-using-different-classifiers
pip install -r requirements.txt
```

Usage

First capture the network flow data

Sniff packets real-time from interface to flow csv: (**need root permission**)

```
cicflowmeter -i <network-interface> -c flows.csv
```

Now run the Network IDS

```
python manage.py runserver
```

The above command will launch a django application. In the main page, upload **flows.csv** file. The result screen will look like

We have performed some realtime DoS attacks during the flow-capturing period using hping3 command. As you can see, Our application can able to capture the intentional simulated DoS attacks. You can use the following hping3 command to perform fake DoS attack

```
sudo apt-get install hping3
hping3 -c 15000 -d 120 -S -w 64 -p 80 --flood --rand-source <ip>
```

Note

To run the application, you don't need to train the models as they are already trained, the models weights are available in **saved_models** directory

For training models

Perform preprocessing

Run Model_Training/data_preprocessing.ipynb file.

For training individual models

Run Model_Training/rf.ipynb file for Random-Forest classifier
Run Model_Training/lstm.ipynb file for LSTM classifier
Run Model_Training/Anamoly_detection_with_NN.ipynb file for Neural Network classifer

For running ensemble model

Run Model_Training/clubbingnew.ipynb for ensemble model