A Machine Learning Model for Network Intrusion Detection Systems (NIDS)

Domain Background

In recent years, human society has developed an increased dependency on Information and Communication Technologies. With the ever-growing use of internet, computer networks have grown leaps and bound with compounding complexities. Same time, sophisticated and diverse threats to modern computer networks and systems are also increasing. This calls for robust security mechanism and Intrusion detection systems in place to identify and combat malicious activities on computer networks.

I work for Capital One's API Platform. Cyber Security and Intrusion detection systems are my area of interest. Network Anomaly Detection is one of the Machine Learning use cases identified on the API platform. I choose this domain for my capstone project, so I can take back my learnings and research work to benefit the platform.

Problem Statement

Governments and Organizations have valuable information stored on computer networks, which has made intrusion detection the most critical focus area in every CIO's office. A variety of studies have been carried out in the field of network security, intrusion detection and resolution.

While traditional intrusion detection methods have proven to be efficient at detecting intrusions based on known parameters, they are not very effective in cases involving new types of intrusions.

Datasets and Inputs

This project will use the UNSW-NB15 dataset to build a model to detect network anomalies and intrusions. The UNSW-NB15 data set was created using an IXIA PerfectStorm tool in the Cyber Range Lab of the Australian Centre for Cyber Security (ACCS) (Australian Center for Cyber Security (ACCS), 2014) to generate a hybrid of the realistic modern normal activities and the synthetic contemporary attack behaviors from network traffic.

The details of the UNSW-NB15 data set are published in following the papers:

Moustafa, Nour, and Jill Slay. "UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). "Military Communications and Information Systems Conference (MilCIS), 2015. IEEE, 2015.

Moustafa, Nour, and Jill Slay. "The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set." Information Security Journal: A Global Perspective (2016): 1-14.

Here are some extracts from the papers:

Evaluating the efficiency of any NIDS requires a modern comprehensive data set that contains contemporary normal and attack activities. Existing benchmark data sets, especially, KDD99 and NSLKDD, were created two decades ago, and lacks modern low footprint attack fashions. The normal traffic of the existing benchmark data sets is different from the current normal traffic because of the revolution in networks speed and applications in the recent years. To address these challenges the UNSW-NB15 data set has recently been released.

This data set includes nine categories of the modern attack types and involves realistic activities of normal traffic that were captured with the change over time. In addition, it contains 49 features that comprised the flow based between hosts. It has a total of 2,540,044 records.

From the original dataset (of 2,540,044 records) a part of the data set records has been divided with an approximate 60%:40% ratio of the training and testing sets, respectively. This MLND capstone project will utilize the training and testing subset to develop the models.

The training and testing csv files of the dataset, required for this capstone project, can be downloaded from here:
https://cloudstor.aarnet.edu.au/plus/index.php/s/2DhnLGDdEECo4ys?path=%2FUNSW-NB15%20-%20CSV%20Files%2Fa%20part%20of%20training%20and%20testing%20set

Solution Statement

When an IDS uses filters and signatures to describe attack patterns, the analysis is static. This method of IDS is called signature detection (or Misuse Based Network Intrusion Detection System (MNIDS)). Signature detection is limited to the detection of known attack patterns. For the detection of unknown attacks, heuristic methods must be used. Systems that use these methods offer the possibility of detecting patterns that are not `normal'.

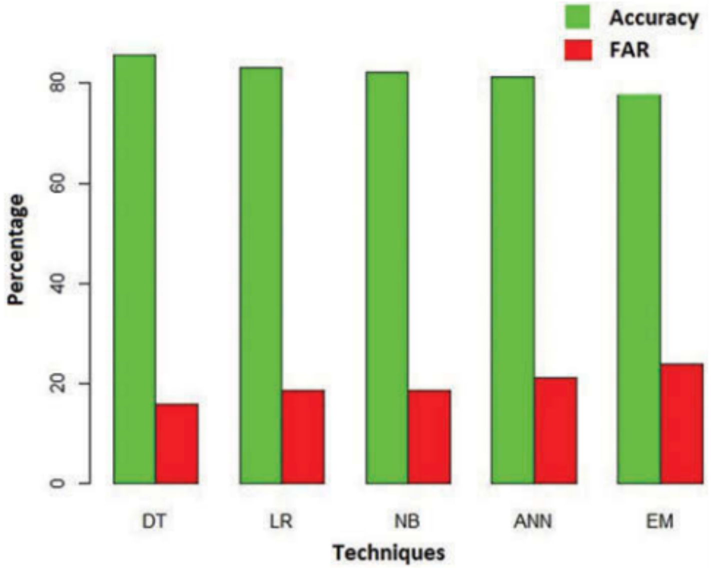
These detection methods are called anomaly detection (Anomaly Based Network Intrusion Detection System (ANIDS)).

Machine learning can be applied in ANIDS systems. One potential solution could be, self-learning systems that learns by monitoring network traffic and differentiates between normal and anomalous traffic. In addition, machine learning solutions can detect possible attacks in real time, so that combating measures can be taken in a timely manner.

The goal of this project is to train a Machine Learning Model that can be used as part of an Intrusion Detection System to identify malicious traffic at runtime.

Benchmark Models

The accompanying research paper authored by the creators of the UNSW-NB15 dataset has outlined some benchmark models and metrics. These will serve as the benchmark for this project.



	Techniques	Accuracy	FAR
1	Decision Tree	85.56	15.78
2	Logistic Regression	83.15	18.48
3	Naïve Bayes	83.07	18.56
4	Artificial Neural Networks	81.34	21.13
5	EM Clustering	78.47	23.79

Evaluation Metrics

Accuracy and FAR (False Alarm Rate) will the main evaluation metrics for this project.

Accuracy is the rate of the correctly classified records to all the records, whether correctly or incorrectly classified

Accuracy = (TP + TN) / (TP + TN + FP + FN)

False alarm rate (FAR) is the average ratio of the misclassified to classified records either normal or abnormal

FPR (False Positive Rate) = FP / (FP + TN)
FNR (False Negative Rate) = FN / (FN + TP)
FAR (False Alarm Rate) = (FPR + FNR) / 2

In addition to Accuracy and FAR, Confusion Matrix will be generated and compared.

Project Design

The project will have a typical ML Project workflow

1. Explore the Dataset
2. Preprocess data
   a. Identify features that need log transformation and apply transformation
   b. Perform minmax scaling on numerical features
   c. Identify outliers if any
   d. One hot encode categorical features
   e. Perform Feature selection / Dimensionality Reduction as required
3. Train a variety of classifiers on the given dataset. Mainly,
   a. Ensemble Methods and
   b. Deep Neural Networks
4. Compare results with the benchmark results.
5. Iterate and Fine-tune hyper-parameters to improve the accuracy and FAR.
6. Analyze confusion matrix and suggest future areas of improvements.

Citation

The details of the UNSW-NB15 data set are published in following the papers:

Moustafa, Nour, and Jill Slay. "UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set).
"Military Communications and Information Systems Conference (MilCIS), 2015. IEEE, 2015.

Moustafa, Nour, and Jill Slay. "The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set." Information Security Journal: A Global Perspective (2016): 1-14.

For more information, please contact the authors:

1. Nour Moustafa: e-mail nour.abdelhameed@student.adfa.edu.au
2. Jill Slay: e-mail j.slay@adfa.edu.au