PLAGIARISM SCAN REPORT

Report Generation Date: 29-05-22

Words: 1500

Characters: 9513

Excluded URL : N/A

12%	88%
Plagiarism	Unique
10	**76**
Plagiarized Sentences	Unique Sentences

Content Checked for Plagiarism

1. Introduction

The world today is regarded as global village as the geographical distance and isolations have been reduced through electronic media. These electronic media includes television and internet. Most of the electronic device today uses internet to communicate with which other through which they convey the information. The medium these devices use is internet which is network of interconnected devices connected through wired and wireless links. These networks use packets for communication and typically face errors. This is where a neural network helps to improve accuracy of packets being sent and detected, what type of problem is faced in case of loss with techniques to solve the issue. Neural network is a machine learning technique. The word neural clearly gives us an idea that it depicts the human brain. Just like the human brain sends signals, the neural networks have nodes which communicate with each other and form layers. Along with improving the accuracy of packets and detecting Intrusion detection is part of the whole process.

1.1 Problem

In the modern tech era cyber-attack is the most common threat that distresses many organizations as these attack can exploit their privacy that costs millions of dollars to recover from the loss and setup defenders like software and human resource to fight against these attacks.

1.2 Significance

The intrusion detection system is required to defend against cyber-attack. An intrusion detection system (IDS) should be able to distinguish between an attack and normal data traveling across the network. One of the many benefits of an IDS is that it notifies personnel whenever a security incident is taking place. An IDS makes it easier to observe the network traffic as well as collect information about the packets like their host, and devices in a more efficient way than following traditional approaches.

1.3 Purpose of Study

Our research focuses on introducing a more efficient way for an intrusion detection system to observe the incoming packets and learn from them as well as evolve in order detect the ever evolving

cyber-attacks on the basis of the features that a malicious packet or attack consists.

2. Literature Review

2.1. Creating firewall rules with machine learning techniques

For fighting cybercrime, interruption recognition is pivotal. Network security field intrusion detection searches for attacks inside data and information packets. Packet attributes are used to decide if a packet is malicious. Firstly information is accumulated. Then features are extracted. Next model is trained to predict the type of attack. Lastly, the model is tested and results are analyzed. One method is a use of firewall that filter incoming packets on the basis of IP addresses, port numbers and protocols also known as ACL rules but these firewalls are not smart enough to catch a malicious packet as is doesn't checks the data that a network packet holds. Therefore more efficient ways should be introduced and which are using machine learning techniques like MLP, SVM, and Decision tree.

2.2. Intrusion detection using NN and SVM

Intrusion detection and audit trial reduction with the help of support vector machines and neural networks use 13 features to predict results, this enhances the accuracy. History of attacks can also be used prevent and identify attack patterns. The data set being used here is developed by DARPA. Furthermore binary classification will degrade if the data set is reduced. The model is able to classify four types of attacks, DOS, R2L, U2R and probing. We randomly select data and extract 13 features out to train our SVM. Training is done using a radical bias function. We individually train SVM and neural networks and then compare their efficiencies to check which is better. SVM outperforms neural networks in terms of training time and efficiency. Even though there is a small difference in efficiency, it matters when data is important. SVMs are fast in training, scalability and generalization which gives them an advantage in detection. Still many experiments are being carried out to introduce more efficient and cost effective methods.

2.3. NN-Based Intrusion Detection System for Critical Infrastructures

Security in control systems such as SCADA are relevant concerns. Forming an intrusion detection system would be beneficial for critical systems where security is top priority. Critical infrastructure systems are interconnected computers. Intrusion attacks mainly lead to financial loss by endangering public data. The data here is taken from already existing infrastructure. Most of the critical systems have PLCs which are used for data gathering. The header of packets carries a lot of information which are used to extract features. By analyzing data it reveals normal patterns as well as intrusion attempts. To get results here the IDS-NNM algorithm is used which has clusters to constitute data. To get more accurate results ANN is used. The model is then trained on a data set. ANN works as a classifier which directly gives results on input data. To get accurate results, detection rate and false positive rate was measured. In this way a model was made and it predicted the model's ability to

detect intrusion on any stream of packets.

2.4. Network based intrusion detection using Neural networks

When someone tries to illegally intercept your packet transmission, this is considered intrusion. Intrusion is a threat to users' data as well as privacy. There are two types of intrusion attacks, host based and network based. Here we will discuss network based. In this paper MLP neural networks are being used for intrusion detection. System uses modular detection to analyze data and traffic intensity. Model is trained with respect to any particular feature for identification. It identifies keywords and sorts problem accordingly. Clustering is carried out to group data of many time intervals. Ports are used to monitor traffic. Once a neural network is trained it can make decisions quickly at real time detection. Supervised and unsupervised learning have an upper hand in analyzing the whole scenario. The model classifies the type of attack and its intensity to alarm users prior to any further damage.

2.5. A real-time solution to network-based intrusion detection using neural networks

By this time, the rate of attacking has increased rapidly which has attracted many engineers' interest. After use of too many supervised learning methods, an unsupervised method was introduced, RT-UNNID. As our dependence on computers is increasing day by day it has become essential to develop systems for threat detection. Security refers to the importance of data and resources. Prevention systems block illegal attempts to change data while detection systems just report and notify about intrusion. Neural networks IDSs can be of four types; MLFF which is multilayer feed-forward neural net working for anomaly detection of threats, Recurrent and adaptive which are systems on CMAC and ELMAN working by getting feedback from output, Unsupervised and Hybrid which is combination of supervised and unsupervised. These all act as intelligent components. In RT-UUNID systems, a sniffer component collects all network traffic. Then extracted numerical features from packets. After this model is trained. It works better on TCP packets. The most important is the UNN engine which analyzes and detects intrusion. Data here comes from DARPA and is locally generated. The results are predicted by comparing outputs of IDSs and expected outputs of systems. The main advantage of unsupervised learning models is that capability to analyze improves over other models. They have high speed and lower response time. The system at the end is able to employ unsupervised learning for classifying and separating packets, normal vs malicious.

3. Methodology

In this project we will be using MLP classifier to filter incoming packets along with intrusion detection. MLP (multilayer perceptron) classifier is a machine learning technique also known as ANN (artificial neural network) that consists of multiples layer most commonly 3, input layer, hidden layer, and output layer. It is the simplest type of neural network, it takes dataset as input providing each feature in a dataset to a neuron in input layer and compute a numerical output for that neuron by using the formula:

$Y` = A(Y)$, where $Y = Xi * Wi$,

Here Y is the output for the neuron, W is the weight assigned to a particular neuron, X is the feature provided, whereas A() is the activation function, Y` is the predicted output for the neuron after Y is

normalized that is then passed as input to next neuron of next layer.

3.1. Procedure

Firstly we will select features from the KDD cup 99 dataset that are more suitable for our problem by doing an brief data analysis after that the dataset is split into train and test data with a ratio of 70:30 where training data is used to train MLP model and test data is used to validate and test the accuracy of model. There are two MLP models that has been used in the project, 1st model is used to filter incoming packet by predicting whether to accept or reject packet based on features i.e. protocol, service, flag etc. Whereas the 2nd model is used for intrusion detection predicting the attack that rejected packet from 1st model contains.

Matched Sources :

7.1 Electronic communication | Internet communication tools — **50%**

https://intl.siyavula.com/read/cat/grade-12-cat/internet-communication-tools/07-internet-communication-tools

Wired and Wireless Networking - GeeksforGeeks — **34%**

https://www.geeksforgeeks.org/wired-and-wireless-networking/

SVM Vs Neural Network | Baeldung on Computer Science — **4%**

https://www.baeldung.com/cs/svm-vs-neural-network

Neural Network Based Intrusion Detection System for ... — **3%**

· Neural Network Based Intrusion Detection System for Critical Infrastructures You are accessing a document from the Department of Energy's (DOE) OSTI.GOV . This site is a product of DOE's Office of Scientific and Technical Information (OSTI) and is provided as a ...

https://www.bing.com/ck/a?!

Map Data | Static Map API | Platform - HERE Technologies — **3%**

https://www.here.com/platform/map-data

Intrusion Analysis - an overview | ScienceDirect Topics — **3%**

https://www.sciencedirect.com/topics/computer-science/intrusion-analysis

Training, validation, and test data sets - Wikipedia — **3%**

https://en.wikipedia.org/wiki/Training,_validation,_and_test_data_sets

Survey of intrusion detection systems: techniques, datasets ... — **2%**

https://cybersecurity.springeropen.com/articles/10.1186/s42400-019-0038-7

A survey of emerging threats in cybersecurity - ScienceDirect **2%**

https://www.sciencedirect.com/science/article/pii/S0022000014000178

Compare identified model output and measured ... - MathWorksSimulate and Predict Identified Model Output - MathWorks **2%**

https://www.mathworks.com/help/ident/ref/compare.html