Abstract—An Intrusion can be defined as any practice or act that attempt to crack the integrity, confidentiality or availability of a resource. This may consist of a deliberate unauthorized attempt to access the information, manipulate the data, or make a system unreliable or unusable. With the expansion of computer networks at an alarming rate during the past decade, security has become one of the serious issues for computer systems. As a result of this, intrusion detection systems (IDS), which can effectively detect intrusion accesses, have gained attention. However, present time’s commercially available intrusion detection systems are signature based which are not capable of detecting unknown attacks. We are moving a step forward and using the concept of Artificial Neural Networks (ANN) in the construction of an Intrusion Detection System. The results show that our proposed system has high accuracy in attack detection as compared to the Data Mining approach and the false alarm rate is also minimum.

Keywords— Back Propagation Neural Network (BPNN) Algorithm, Training phase,

I. INTRODUCTION

Intrusion Detection System is a mechanism that is being used to protect organization from attacks from different sources. Intrusion detection is defined by the Sysadmin, Audit, Networking and Security (SANS) institute as the act of detecting actions that attempt to compromise the confidentiality, integrity or availability of a resource. It is obligatory that IDS can handle huge quantity of information without affecting performance and without loss of data and can detect intrusions reliably without giving false alarms.

IDS are broadly classified as:

A. Misuse Based System:

In misuse based IDS, detection is done by searching for the exploitation of known weak points in the system, which can be described by a specific pattern or sequence of events or data. That means these systems can detect only known attacks for which they have a defined signature.

B. Anomaly Based System:

In anomaly based IDS, detection is performed by detecting changes in the patterns of utilization or behavior of the system.

The main advantage of anomaly detection system is that they can detect previously unknown attacks. Neural networks are a form of artificial intelligence which uses many artificial neurons, networked/linked together to process information or data. This type of network or linkage has the capability to learn from patterns, and interpret results from data that has been previously entered into the network’s knowledge base. This excellent feature makes neural network applications highly valuable in intrusion detection. An artificial neuron is a computational model inspired in the natural neurons.

II. LITERATURE SURVEY

From decades till now numerous attempts have been made to build an optimal Intrusion Detection System. Misuse detection is the process which tries to identify instances of network attacks by comparing current activity against the expected actions of an intruder. Recent approaches to misuse detection involve the use of Rule-based expert systems to identify indications of known attacks. These techniques are not much successful in detecting attacks which vary from expected patterns. Artificial neural networks provide the potential & momentum to identify and classify network activity based on limited, incomplete, and nonlinear data sources. Rule-based analysis depends on sets of predefined rules that are made available by an administrator, automatically created by the system or both. Expert systems are the systems which mainly use this concept of Rule based intrusion detection. But these rule based systems suffer from an inability to detect attacks scenarios that may occur over an extended period of time or we can say after a long time span. Predictive pattern generation uses a rule base of user profiles defined as statistically weighted event sequences. This method of intrusion detection tries to predict future events based on events that have already occurred. An intrusion is detected if the observed sequence or series of events matches the left hand side of the rule but the following events significantly deviate from the right hand side of the rule. The main drawback of such system is its inability to identify some intrusions if that particular sequence of events have not been recognized and created into the rules.
Keystroke monitoring technique makes use of a user as keystrokes to detect the intrusion attempt. The main idea is to pattern match the series of keystrokes to some predefined series to detect the intrusion. The demerit with this approach is poor support from operating system to capture the keystroke sequences and also large number of ways of expressing the sequence of keystrokes for the same attack.

III. PROPOSED SYSTEM

An artificial neural network contain number of very simple processors, also called neurons, which are analogous to the biological neurons in the human brain as shown in the figure 1.

The figure 2 also shows us the layout of a neural network containing three layers, of which one is the input layer other, is the output layer and the remaining one is the hidden layer. In the figure 3, we can see that certain weights are assigned to each of the edges between every two neurons.

While computing the output, summation of these weights according to the respective neurons is calculated. This same example we can consider for understanding the operation of our IDS. Bits are assigned to the packets according to their attributes. Here if the packet is TCP, its bit is 0. This is called as Data set labeling or just Labeling. We can also see that weights are assigned to all the edges. Based on the calculations of the weights and the bits, it is predicted that the packet is an attacking packet or a non-attacking one. The architecture of our Intrusion Detection System is shown in figure 4. It is a layered architecture where each block is connected to the other in a uniform and linear fashion. All the blocks are interdependent on each other. The first block that we can see is the packet sniffer/scanner. It captures all the packets in the network which are approaching towards our system that is incoming packets. Then these packets are analyzed using packet analyzer. Analysis means knowing whether the packet is a TCP, SMTP, UDP, etc. This was only the type of packet. There are also many other attributes of packets such as header-length, flag, fragmentation offset, TTL value, etc. So recognizing all the incoming packets along with all their attributes is done by the packet analyzer and the Signature block. Now these packets along with the entire information of their attributes are stored in a Dataset.
Figure 4: System Architecture

Dataset is a form of a serialized dataset built using Java Serialization API where the packets and their information get stored. After this the Dataset Labeling takes place. Here the different attributes of packets which are to be considered are labeled that is they are assigned with the bits 0, 1, etc. The most important part of our system architecture is the Training phase. In our approach of construction of an IDS using ANN, we are considering two algorithms of ANN viz, the Back Propagation Neural Network (BPNN) algorithm and the Feed Forward (FF) algorithm. Of which we are going to implement the BPNN algorithm in the Training phase. The completion of training phase will result into the building up of a model which we call it as a Trained Model. This trained model will train our neural network for every input from the Dataset as well as for any new patterns of intrusion packets approaching our system. Now comes the final stage of the architecture which is known as Prediction. Here in this prediction phase, the Feed Forward (FF) algorithm will get implemented. After combining the results of BPNN and FF algorithms and performing mathematical operations, the Prediction phase produces output stating whether the packet is an attack packet or a non-attack packet. The outcome of this overall operation i.e an attack or a non-attack can be informed to the user via SMS or e-mail.

IV. WORKING

The attributes of packets that are stored in the dataset are labeled as 0, 1, etc. A neural network consists of three layers, viz, input layer, hidden layer and the output layer. Such labeled attributes are given as input to the neural network via input layer. From figures 2 and 3, we can observe that every layer is connected with the other through edges. So we assign some random values to these edges also called as weights. Mostly these values are of the floating point type. We already know that this packet is attacking or non-attacking. At the output layer we have two conclusions, attacking and non-attacking. We can label them 0 and 1 or vice versa. At every neuron in the hidden layer, summation of the weights of the incoming edges to that particular neuron is calculated. After that, at every neuron of the output layer, summation of the weights incoming to that neuron along with the weight of that specific neuron at the hidden layer is calculated. These results are then compared with the already known results i.e. 0 and 1. Then the difference between the actual results and the calculated results is computed.
The value thus obtained, we call it as error. It may be positive value or a negative value. So this error is now Back Propagated through the entire neural network. The weights of the edges are adjusted accordingly and again the summation operation takes place. This process continues until the calculated results matches with a specific value, known as threshold value. In other words, the neural network keeps training all the patterns repeatedly until the total error falls to some pre-determined low target value i.e. the threshold value and then it stops. On reaching the threshold value the results are concluded accordingly. This entire process is called as the learning phase or the training phase. A Back Propagation network learns by examples. When we give the algorithm, examples of what we want the network to do and it changes the network’s weights so that, when the training is finished, it will give us the required output for a particular input. The more we provide samples or examples to the neural network during its training phase the greater will be the accuracy of the neural network in determining whether the incoming packets to our system are attacking or non-attacking packets.

REFERENCES

[6] Carlos Gershenson ,’Artificial Neural Networks for Beginners’C.Gershenson@sussex.ac.uk
[8] Girish Kumar Jha, Indian Agricultural Reasearch Institute, PUSA, New Delhi,’ARTIFICIAL NEURAL NETWORKS’