An Integrated Model of Intrusion Detection Based on Neural Network and Expert System

ZhiSong PAN[1] Hong LIAN[2] GuYu HU GuiQiang NI
Institute of Command Automation, PLA Univ. of Science & Technology, Nanjing 210007, P.R.China[1]
hotpzs@hotmail.com
GuiZhou Radio & TV University, Guiyang 550004 P.R.China[2]

Abstract

Intrusion detection technology is an effective approach to dealing with the problems of network security. In this paper, it presents an intrusion detection model based on neural network and expert system. The key idea is to aim at taking advantage of classification abilities of neural network for unknown attacks and the expert-based system for the known attacks. We employ data from the third international knowledge discovery and data mining tools competition (KDDcup'99) to train and test the feasibility of our proposed neural network component. According to the results of our experiment, our model achieves 96.6 percent detection rate for DOS and Probing intrusions, and less than 0.04 percent false alarm rate. Expert system can detect R2L and U2R intrusions more accurately than neural network. Therefore, Hybrid model will improve the performance to detect intrusions.

1. Introduction

This paper describes an integrated neural network and expert system model for intrusion detection. Firstly, we build the expert system to improve the detection rate for known attacks. Then, we use BP network to detect the unknown intrusions. Therefore, the integrated model improves the performance to detect all intrusions. Our experiment results demonstrate efficiency and accuracy of the detector.

2. An integrated IDS model

With the combination of the misuse detection and anomaly detection, can IDS have an effective detection on the known attack and the capabilities of monitoring the unknown attacks. To improve the identification rate of the IDS and put it into use, an intrusion detection model based on integrated neural network and expert system has been designed. The model consists of the following three important parts: the rule-based detector, the statistical analyzer, the neural network component [1].

The workflow of the model introduction is as following. First of all, the model captures the network sniffing data which processed by the protocol analyzer. The engine of intrusion detection and rule-based detector match the decoded data based on each protocol fields to the rules in the attack signature database. If the result of match is true, the detective engine will alarm. This module belongs to misuse detection. Meanwhile, the decoded data also feed to the Data Formatting Module which can make data numerical so as to be dealt with Artificial Neural Network (ANN) component [1][2]. The ANN component executes anomaly detection with its output processed by the engine of intrusion detection.

As the host-based intrusion detection method, the statistical analysis module can compare statistical data about the characteristics on security of the host and system logs with those expected features under the normal situation. The statistical analysis module will carry on measurement at regular time. If the data exceed the predicted threshold, the engine will alarm. In the following part, the rule-based detector and the neural network component will be introduced.

2.1. The rule-based detector

[1] Supported by the Jiangsu Planned Projects for Postdoctoral Research Funds, natural science foundation of Jiangsu (NO.BK2005009) and natural science foundation of china(NO.60303023)

Proceedings of the 17th IEEE International Conference on Tools with Artificial Intelligence (ICTAI'05)
1082-3409/05 $20.00 © 2005 IEEE

The rule-based detector uses the freely available packet capture library winpcap to capture the network packets and the packets will be decoded in the protocol analyzer. The rule-based detector detects the known behaviors of attackers by rules of Database of attack signatures. The rules which come from a famous IDS named snort is simple to write, yet powerful enough to detect a wide variety of hostile. The rules are divided into six sections, action(DC:disconnect, Lo:log, or AL:alert), protocol(TCP, UDP,ICMP, IGMP), source and destination IP addresses and netmasks, the source and destination port numbers, alert messages and flag value of the malicious packet.

2.2. The neural network Component

The neural network Component was designed to build the detective module based on the pattern recognition. The component reads Tcpdump data and first sends them to Features Extractor which converts the raw data into 41 features data form. The process also involves the creation of relational tables for each of the data type and assigning number to each unique type of element. Therefore, the data of uniform representation can be processed by the neural network. In the study, the neural network Component utilized a 3-layer network, consisting of 70 neurons in first hidden layer,14 neurons in second hidden layer and 6 neurons in the output layer, resulting to a 41-70-14-6 feed-forward neural network. Each of the hidden nodes and the output node applied a Sigmoid transfer function to the various connection weights.

To illuminate the performance of the model, we employ data from the third international knowledge discovery and data mining tools competition (KDDcup'99)[3] to train and test the feasibility of our proposed model. We select normal dataset, Neptune attack, Portsweep attack, satan attack, buffer_overflow and guess_passwd datasets to train and test our IDS prototype. The complete description of features is found in [3]. The normal and 5 attack categories are numbered as follows:1-normal,2-neptune,3-satan,4-portsweep,5-buffer_overflow,6-guess_passwd. We get 29313 train data patterns from 10% training set and 13112 test data patterns from Test set which has attack patterns that are not present in the training data. Therefore Problem is more realistic.

The training of the neural networks was conducted using feed forward back propagation algorithm using scaled conjugate BP network structure for IDS gradient decent for learning. The network was set to train until the desired mean square error of 0.001 was met or 1500 epochs was reached. During the training process, the performance of BP network is 0.00157434 at 1500 epochs.

We put 13112 data into the TESTSET for BP network. The classified results, the false positive and detect rate are obtained as the follows:

The test result indicates that in total 99.6% of the actual "normal" examples were recognized correctly. For DOS and Probing intrusion (2-neptune,3-satan,4-portsweep) ,we can obtain the average detect rate of 96.6% and the false positive rate of 0.049%. Because all buffer_overflow and guess_passwd attacks fail to be classified by BP network, we only obtain the average detect rate of 64.9% and the false positive rate is 26.7% for all the five kinds of attacks.

However, these two kinds of attacks can be accurately detected by rule-based detector. Expert system can detect the R2L and U2R intrusions more accurately than neural network. For example, Using the detect rules: ALERT UDP ENET any <-> HNET 31337 MESSAGE:"BO access" DATA: |ce63 d1d2 16e7 13cf 3ca5 a586|", the buffer_overflow will be detected. Thus, taking advantage of the performance of each module for various attacks, the model improves the detection rate for all intrusions.

3. Conclusion

This paper presents an integrated neural network and expert system model for intrusion detection. Firstly, we build the expert system to improve the detection rate for known attacks. Then, we use BP network to detect the unknown intrusions. Therefore, Hybrid model improves the performance to detect all intrusions. Our experiment results demonstrate efficiency and accuracy of the detector. Specially, the neural network could provide significant benefits to intrusion detection through data reduction, classification, clustering the unlabeled system log data, and the each process of identifying intruders.

References

[1] A.Bivens, C.Palagiri, R.Smith, B.Szymanski, "Network-Based Intrusion Detection Using Neural Networks", 2002

[2] J Cannady, "Artificial Neural Networks for Misuse Detection", National Information Systems Security Conference (NISSC'98), Arlington.VA, Oct.1998, pp. 443-456.

[3] S.J. Stolfo, et al. "KDD cup 1999 dataset". UCI KDD repository. http://kdd.ics.uci.edu, 1999