IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 56-59

Applications of Neural Networks in Intrusion Detection

T.Sindhu, V. Safa Mehrin
Asst.Professor, Department of computer applications, Islamiah Womens Arts and Science College
Department of computer science

Abstract: *Intrusion detection systems are employed to detect the intrusion which has found its applications in securing both public data and private data. This paper deals with various aspects by providing different intrusion detection systems using neural networks for several purposes. It has various tools and databases to focus on proper intrusion detection techniques. There are several methodologies in neural networks that cause detection of intrusions using newer technologies.*

I. Introduction:

Intrusion Detection Systems are designed to improve the security of company networks. An Intrusion Detection System will have the capability to detect the real-time (attempted) intrusions and will help in execution of work to stop the attack. This paper will focus on the present state of Intrusion Detection Systems (IDS) and presents a new technique for improving the false-alarm detection using Neural Network approach. This is an upcoming approach which assures a promising future. Firstly we represent the global architecture of IDS and a few commercially available tools and then analyze new research topics in order to improve the performance of IDS and neural networks for intrusion detection.

Classification:
Intrusion Detection Systems can classified as following:

Host Based Ids:
They undergo evaluation of information which is found on either single or multiple host systems that includes contents of operating systems, system and application files.

Network Based Ids:
These systems evaluate the information which is captured from network communication thereby analyzing various streams of packets travelling across networks; packets can be captured from sensors.

Vulnerability:
Vulnerabilities on internal networks and firewall can be detected by assessment networks. The events of attacks can be analyzed by two primary models

Misuse Detection Model:
Here, the various intrusions will be detected by IDS by moving forward for the activity that contains the known signatures of various intrusions and vulnerabilities.

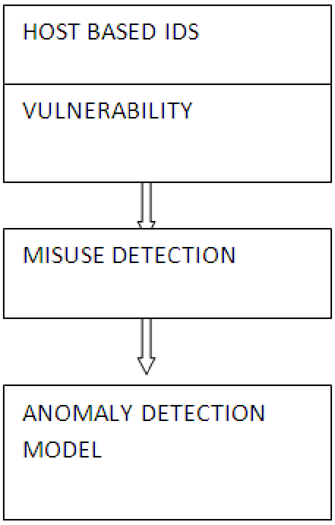

Fig : Misuse Detection Model Proces

Anomaly Detection Model:

The IDS systems here undergo detection of intrusion by searching the abnormal network traffic. Most commercial tools of IDS are misuse detection model, and signatures of intrusions which need to be updated by vendors.IDS based on anomaly detection model have the capability to detect various symptoms of attacks without having any specifications of attacks but are sensitive to false alarms.

Tools That Are Commercially Available:

1. **Suitability:** for architecture of Intrusion Detection Systems and management scheme
2. **Flexibility :** of adaptation for a specified network to be controlled
3. **Protection:** against various malicious tampering
4. **Interoperatability:** with various security tools and network managements
5. **Comprehensiveness:** to expand intrusion detection concepts thereby blocking the java applets or Active X controls, moving the email contents and blocking specific URLs
6. **Event Management:** to manage, report event trace and update attack database
7. **Active Response:** when the attack such as firewall or router recognition occurs
8. **SUPPORT for the product**

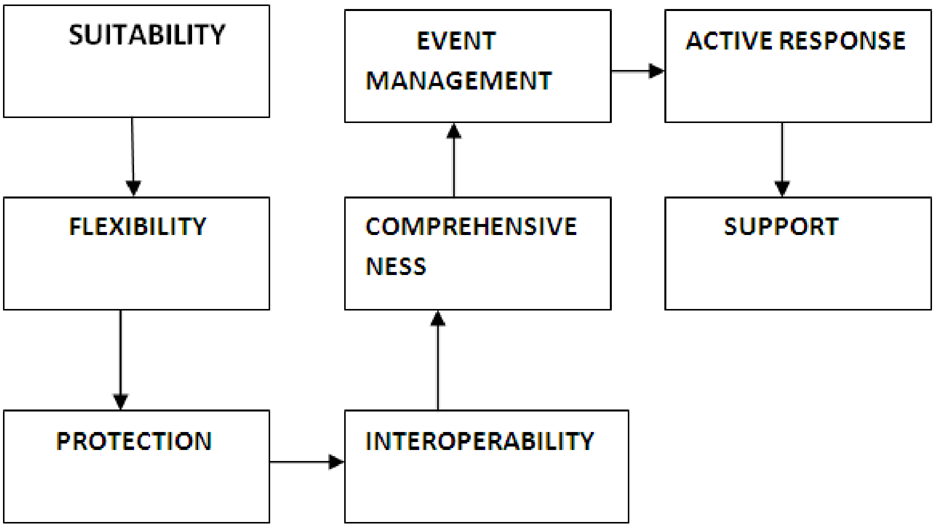

FIG.: Block Diagram for Tools

II. Samples Of Ids Tools:

Ids Tools Based On Host:

IDS tools based on host make use of system logs and operating system audit trials to detect various attacks in an individual systems.Example:Cybercops from Network Associates(NAI),Kane Security Monitor(KSM) from RSm security.Tripwrite used to detect administrative or user files changes in a server

Ids Tools Based On Network:

These system cause the detection of attacks by the process of capturing and analyzing various network packets from sensors that are placed at various places on network. Example: Real Secure from Internet Security Scanner (ISS), CiscoSecure IDS or NetRanger from Cisco Systems. The major difficulty for this kind of systems is that to process all packets in real-time for a larger network, various specific hardware solutions may be applied. Another problem is the segmentation of networks by switches that cause difficulties for capturing signals in global networks.

Ids Tools Based On Vulnerability-Assessments:

Vulnerability Assessment tools are can be most importantly called as the scanners for security which can detect operating systems configuration's vulnerabilities .Example:CyberCop Scanner from PGP security and Secure Scan NX from network viligence.

Performances Of Commercial Tools:

The various major tools that are used today are mainly designed to detect misuse, meaning that the vulnerability database need to be updated by the administrator. Then all tools are vulnerable to new signs of attacks. Tools are very sensitive to false attacks.

Application Of Neural Networks In Intrusion Detection:
Approaches For Misuse Detection:
Various approaches in the misuse detection model include:
EXPERT SYSTEMS which contain a set of rules that is used to describe attacks
SIGNATURE VERIFICATION, where attack senarios will be translated to sequences of audit events
PETRI NETS, which represents known attacks in graphical Petri nets
STATETRANSITION DIAGRAMS represents a set of goal and transition attacks
Signature Verification is one of the common approaches used for the purpose of misuse detection. This includes the process where the system can detect previously seen attacks by looking for a signature left over by attacks. These signatures can be present in audit files, in host-intrudes machines or in sniffer's looking for packets present inside or outside the attacked machine.

This approach contains various limitations because of these factors;

1. Frequent False alarms detection system
2. The need to specify and update the signature of attack on IDS tools. Discovering the signature of an attack is a difficult task
3. Discovering new stack signature require an update of the IDS

Approaches In Detecting Anomaly:
Anomaly detection in networks include the following:
THRESHOLD DETECTION that can be used for the detection of any abnormal activity that can be found on a server or network.
STATISTICAL MEASURES that is learned from historical values
RULE BASED MEASURES with expert systems
NON LINEAR ALGORITHMS such as genetic algorithm or neural networks

The most common method in anomaly detection can be said as statistical analysis which measures the behaviour of system by a number of variables that are present over a time. These variables may represent the login and logout time of each session, the amount of resources consumed or resource duration.

Darpa Intrusion Detection Database:
In order to improve the performance of IDS systems by merging with real network traffic ,a realistic and large scale intrusion detection database has been defined by US Defense Advanced Research Projects Agency (DARPA).DARPA database as designed for intrusion detection by observing the traffic for two months from US government and internet were registered the attacks against hosts.

Mit Research In Neural Network Ids:
Various tests were conducted for intrusion detection in Lippmann and Cunningham of MIT Lincoln Laboratory by the process of searching for attack specific keyword in the network traffic.MLP is used to detect UNIX host attacks. Generic keywords can be used for detecting attack preparations and actions. A two k perceptron was designed with K input nodes 2K hidden nodes, 2 output nodes. A Good detection perceptron was obtained from with 30 keywords to detect attacks.

Ubilab Laboratory:
Lui Girardin of UBILAB Laboratory employed the Self Organizing Maps (SOM) to detect the attacks by performing the grouping of network traffic .Self Organizing Maps are designed to project the image on 2-D space for visualization and are displayed with the comprehensive view for the network administrator. Intrusions can be detected from the view.

Research Of Rst Corporation:
Ghosh and Schwartbard of various reliable software technologies corps detected anomalies using neural network approach by analyzing program behaviour profile for intrusion detection. By capturing various system calls that is made by the systems the program behaviour profiles are founded.

III. Conclusion:

Intrusion detection systems are getting accomplished as the fundamental security systems. Detecting the Realtime intrusions by commercial tools has its limitations but neural network is an effective way to improve the performance of IDS systems which is based on misuse detection model and anomaly detection model.

Reference:

[1]. Cheng, B. and Titterington, D. M. (1994). Neural networks: A review from a statistical perspective. Statistical Science, 9, 2-54.

[2]. Dewolf, E.D., and Francl, L.J., (1997). Neural networks that distinguish in period of wheat tan spot in an outdoor environment. Phytopathalogy, 87, 83-87.

[3]. Dewolf, E.D. and Francl, L.J. (2000) Neural network classification of tan spot and stagonespore blotch infection period in wheat field environment. Phytopathalogy, 20, 108-113 .

[4]. Gaudart, J. Giusiano, B. and Huiart, L. (2004). Comparison of the performance of multi-layer perceptron and linear regression for epidemiological data. Comput. Statist. & Data Anal., 44, 547-70.

[5]. Hassoun, M. H. (1995). Fundamentals of Artificial Neural Networks. Cambridge: MIT Press.

[6]. Hopfield, J.J. (1982). Neural network and physical system with emergent collective computational capabilities. In proceeding of the National Academy of Science(USA) 79, 2554-2558.

[7]. Kaastra, I. and Boyd, M.(1996). Designing a neural network for forecasting financial and economic time series. Neurocomputing, 10, 215-236.

[8]. Kohzadi, N., Boyd, S.M., Kermanshahi, B. and Kaastra, I. (1996). A comparision of artificial neural network and time series models for forecasting commodity prices. Neurocomputing, 10, 169-181.

[9]. Kumar, M., Raghuwanshi, N. S., Singh, R,. Wallender, W. W. and Pruitt, W. O. (2002).

[10]. Estimating Evapotranspiration using Artificial Neural Network. Journal of Irrigation and Drainage Engineering, 128, 224-233

[11]. Masters, T. (1993). Practical neural network recipes in C++, Academic press, NewYork.

[12]. Mcculloch, W.S. and Pitts, W. (1943) A logical calculus of the ideas immanent in nervous activity. Bull. Math. Biophy., 5, 115-133

[13]. Pal, S. Das, J. Sengupta, P. and Banerjee, S. K. (2002). Short term prediction of atmospheric temperature using neural networks. Mausam, 53, 471-80

[14]. Patterson, D. (1996). Artificial Neural Networks. Singapore: Prentice Hall. Rosenblatt, F. (1958). The perceptron: A probabilistic model for information storage ang organization in the brain. Psychological review, 65, 386-408.

[15]. Rumelhart, D.E., Hinton, G.E and Williams, R.J. (1986). “Learning internal representation by error propagation”, in Parallel distributed processing: Exploration in microstructure of cognition, Vol. (1) (D.E. Rumelhart, J.L. McClelland and the PDP research gropus, edn.) Cambridge, MA: MIT Press, 318-362.

[16]. Artificial Neural Networks and its Applications V-49

[17]. Saanzogni, Louis and Kerr, Don (2001) Milk production estimate using feed forward artificial neural networks. Computer and Electronics in Agriculture, 32, 21-30.

[18]. Warner, B. and Misra, M. (1996). Understanding neural networks as statistical tools. American Statistician, 50, 284-93.

[19]. Yegnanarayana, B. (1999). Artificial Neural Networks. Prentice Hall Zhang, G., Patuwo, B. E. and Hu, M. Y. (1998). Forecasting with artificial neural networks:

[20]. The state of the art. International Journal of Forecasting, 14, 35-62.