ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

Intrusion Detection Systems: A survey and Analysis of Security Issues

Dr.V.Jaiganesh[1], Mr.M.M.Karthikeyan[2]

Professor, Department of Computer Science, Dr.N.G.P Arts and Science College, Coimbatore[1]

Research Scholar, Department of Computer Science, Dr.N.G.P Arts and Science College, Coimbatore[2]

Abstract: INTRUSION DETECTION SYSTEM [IDS] are the process of identifying and responding to malicious activity targeted to computing and network resources. Intrusions are the activities that violate the security policy of system. The process used to identify intrusions. Today network securities are used in various applications like protect vital information while still allowing access to those who need Trade secrets, Medical records etc. In this paper going to see about different types of attacks, mechanisms to prevent the attacks and simulations.

Keywords: Intrusion Detection System, Methods of IDS, Protocols, Attacks.

1. INTRODUCTION

Network security involves the authorization of access to data in a network. Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor un-authorized access, misuse, modification or denial of a computer network and network-accessible resources[1]. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Fig.1 representing the performance of Intrusion Detection System [IDS] is the process of identifying and responding to malicious activity targeted to computing and network resources. Intrusions are the activities that violate the security policy of system. Intrusion Detection System [IDS] is the process used to identify intrusions and classified into Host based, Network based, Distributed based detection system. Host-based Intrusion Detection System [IDS] defined into get audit data from host audit trails and detects attacks against a single host [3]. Network-based Intrusion Detection System [IDS] is used network traffic as the auditing data source, relieving the burdens on the hosts that usually provide normal computing services and detect attacks from network [3]. Distributed Intrusion Detection System [IDS] gather audit data from multiple hosts and possibly the network that connects the hosts and detect attacks involving multiple hosts.

Intrusion Detection System [IDS] protocol types are classified into ICMP, TCP and UDP protocols [4]. Internet control message protocol is used by the IP layer to send one way messages to a host. There is no authentication in ICMP which leads to attacks using ICMP that can result in a denial of service or allowing the attacker to intercept packets. Transmission control protocol defines one application wants to communicate with another via TCP sends a communication request [4].

This TCP request must be sent to an exact address. After a hand shake between the two applications. TCP setup a full-duplex communication between the two applications. The full-duplex communications occupy the communication line between the two computers until it is closed by one of the two applications. There are security problem in TCP. User defined protocol uses a simple transmission model without implicit handshaking dialogues for providing reliability, ordering or data integrity. UDP provides an unreliable service and datagram may arrive of order, appear duplicated or go missing without notice. UDP used error checking and correction is either not necessary or performed in the application, avoiding the overhead of such processing at the network interface level [4].

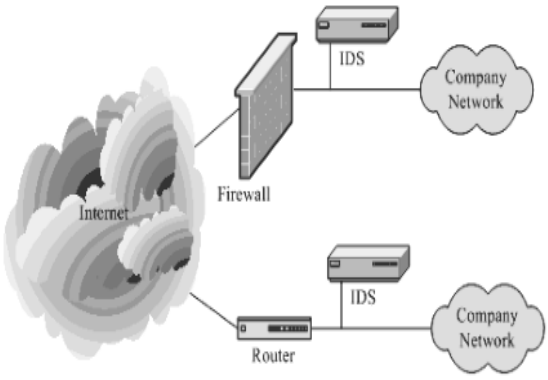

Fig.1: Intrusion Detection System

2. LITERATURE REVIEW

2.1 Efficiency of intrusion-detection systems:

Intrusion-detection systems have proposed the following five parameters:

Accuracy:

Accuracy deals with the proper detection of attacks and the absence of false alarms. Inaccuracy occurs an intrusion-detection system flags a legitimate action in the environment as anomalous or intrusive (Herv´e Debar) [8].

Performance:

Performance is the rate at which audit events are processed. If the intrusion detection system is poor, then real-time detection is not possible (Herv´e Debar) [8].

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

Completeness:

Completeness is the property of an intrusion-detection system to detect all attacks. Incompleteness occurs when the intrusion detection system fails to detect an attack. This measure is more difficult to evaluate than the others because it is impossible to have a global knowledge about attacks or abuses of privileges (Herv´e Debar) [8].

Fault tolerance:

An intrusion-detection system is resistant to attacks, especially denial-of-Service type attacks and should be designed with this goal. This is important because most intrusion detection systems run above commercially available operating systems or hardware are known to be vulnerable to attacks (Herv´e Debar) [8].

Timeliness:

An intrusion-detection system has to perform and propagate its analysis as quickly as possible to enable the security officer to react before much damage is done and also to prevent the attacker from subverting the audit source or the intrusion-detection system itself. It implies more than the measure of performance because it not only encompasses the intrinsic processing speed of the intrusion detection system, but also the time required to propagate the information and react them (Herv´e Debar) [8].

2.2Classification based on different information source:

Wei Li proposed that used the Genetic Algorithm (GA) to network Intrusion Detection Systems. Here they are describing about the Parameters and evolution process for GA [1]. And then it's useful for identification of complex anomalous behaviours during the process. There are two types of intrusion detection techniques used that is misuse detection and anomaly detection. Misuse detection refers to techniques that characterize known methods to penetrate a system. System responses are based on identified penetrations. Anomaly detection Refers to techniques that define and characterize normal or acceptable behaviours of the system [4]. Genetic algorithm considers the both temporal and spatial information of network connection during encoding problems. This is used to find the anomalous behaviours. Using this genetic algorithm with such parameters to find out the intrusion [1].

Maheshkumar Sabhnani, Gursel Serpen proposed that the machine learning algorithm within Misuse detection context.Ususally some algorithm is used to perform for some attacks but few algorithms is capable to do the more than one desired performance [2]. KDD dataset covers four major categories of attacks: Probing attacks (information gathering attacks), Denial of-Service (DoS) attacks (deny legitimate requests to a system), user-to-root (U2R) attacks (unauthorized access to local super-user or root), and remote-to-local (R2L) attacks. And then the KDD dataset is divide into two types that is labelled and unlabeled records. Each labelled record consisted of 41 attributes (features) and one target value [6]. Target value indicated the attack category name. There are around 5 million (4,898,430) records in the labelled dataset, which was used for training all classifier models discussed in this article. A second unlabelled dataset (311,029 records) is provided as testing data. It is less compare to the labelled dataset. The proposed model was able to detect 73.2% of probing attacks, 96.9% of denial of service attacks, 6.6% of U2R attacks, and 10.7% of attacks in R2L attack category. the KDD 1999 Cup data set do not offer much promise for detecting U2R and R2L attacks within the misuse detection context.

A. Kartit, A. Saidi et al, proposed that article about the security enhanced network. Many mechanisms have been developed to improve the security of computer networks. In this paper, proposed an approach based on security policy at three levels for complex computer systems. That is Strategies for External Protection, Functional Security Policies and Operational Security Policies [7]. First level is a classical so it will be placed in firewall to prevent network attacks from outside by refusing malicious connection attempts by unauthorized third parties outside And then second level is based on the tasks assigned to users in the company by the segmentation of the network to VLAN "Virtual Local Area Network" and the use of ACL "Access Control List".Atlast third level control will prevent identity usurpation from inside or from outside to the internal computer network [7].

These three levels can help the administrator to prevent intrusion and implement proactive measures to detect a possible attack.

Kiran Dhangar Prof. Deepak Kulhare Arif Khan proposed OSI layer based Intrusion Detection System [IDS].here two types of attribute find in security event log file one is login-logoff time and another is unauthorized accessing of the host [5]. Many methods have been developed by organizations and play very important roles to secure network infrastructure and communications via the Internet such as through the use of firewalls, anti-virus software packages and intrusion detection systems [5]. Intrusion Detection System[IDS] are finding layer attack or abnormality in the captured packets which is follows: in application layer attacks are finding "Back", "Buffer overflow" and "Port Scan". In Transport layer finding "TCP SYN FLOAD Attack" "Land" and "Smurf". Finally network layer attack is future work of this research. "Host based Intrusion Detection System" is proposed security analyzer to check or find attack in local host then it will detect security attack in security event log file. After completing this it is produce results. If any illegal activity find in this log file like un-authorized accessing or login failed then it will go to alarm system for information that this system is suffering from attack. In future have to work on network layers protocol and try to find attack on network layers. **Alec Yasinsac, Sachin Goregaoker** proposed that Security protocols are rules that govern such encrypted exchanges. Network Security is an important field of Computer Science [3]. With the emergence of the Internet as a medium for wide-scale exchanges of sensitive information and finance transactions, maintaining the security and integrity of messages sent over public networks is very important one for that purpose have to make a secure network exchanges.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

The classic Needham and Schroeder Conventional Key Protocol is previously used one protocol. The Secure Enclave Attack Detection System (SEADS) is a system that can detect attacks on security protocols within an enclave of valid and recognized parties that communicate using a public network. And then they implement Knowledge-Based Intrusion Detection Engine to detect attacks on security protocols executing within a secure enclave.

2.3 Classification based on different analysis method:

Misuse Detection: It catches the intrusions in terms of the characteristics of known attacks. It is based on attack actions and feature extract from known intrusions, integrate the human knowledge, finally rules are pre-defined [4]. Advantage is defined accurately and generates much fewer false alarms. Dis-advantage is can't detect novel or unknown attacks.

Anomaly Detection: It defines detect any action that significantly deviates from the normal behaviour. It is based on normal behaviour of a subject. The training audit data doesn't include intrusion data and any action that significantly deviates from the normal behaviour is considered intrusion [4]. Advantage is able to detect unknown attacks based on audit.Dis-advantage is based on audit data collected over a period of normal operation and when a noise data in the training data, it make a miss-classification. Decide the features are used and their features are usually decided by domain experts but it may be not complexity. High false alarm and limited by training data.

3. PROPOSED WORK

3.1 Machine Learning

Machine Learning is used into study of algorithms and that improve their performance at some task with more than experience. Fig.2 representing in the Machine learning techniques is preferred approaches to Speech recognition, Natural language process, Computer vision, Medical outcomes analysis, Robot control and Computational biology [2].

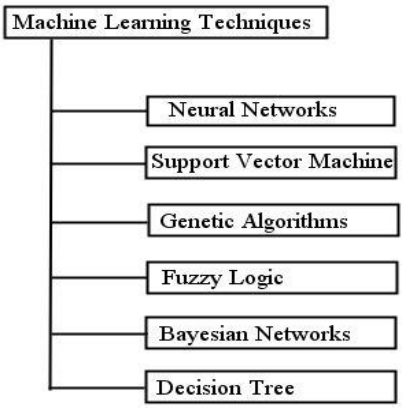

Fig.2: Machine Learning Techniques

The following is to list of common machine learning technologies are:

1. Bayesian decision theory
2. Multivariate methods
3. Clustering
4. Decision trees
5. Linear discrimination
6. Multilayer perceptions
7. Local models
8. Hidden Markov models
9. Reinforcement learning

Machine learning is typically classified into three broad categories.

Supervised Learning: Computer is presented with example inputs and their desired outputs, given by a "teacher", and the goal is to learn a general rule that maps inputs to outputs.

Unsupervised Learning: No labels are given to the learning algorithm and leaving it on its own to find structure in its input. It can be a goal in itself (discovering hidden patterns in data) or a means towards an end.

In-Reinforcement Learning: Computer program interacts with a dynamic environment in which it must perform a certain goal (such as driving a vehicle), without a teacher explicitly tell it whether has come close to its goal or not. **Example**: Learning to play a game by playing against an opponent.

3.2 Decision Tree

A decision tree is a decision support tool that uses a tree like a graph or model of decision and their possible consequence including have event out comes resource cost and utility [6]. It is one way to display our algorithm decision tree are commonly used in operations researches, specifically it decision analysis to help identify a strategy most likely to reach a goal. It is a flow chart structure which each internal node represents a test or an attribute. Each branch represented to the outcome of the test and each leaf node represents a class label.

3.2.1Decision Tree Elements:

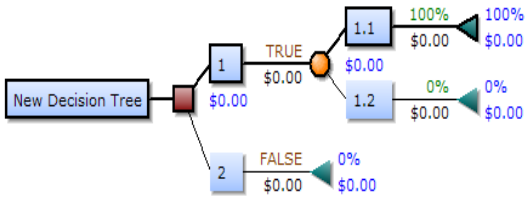

Fig.3: Default Decision Tree

Drawn from left to right, a decision tree has only burst nodes (splitting paths) but no sink nodes (converging paths)[6]. It's used manually, they can grow very big and are then often hard to draw fully by hand. Decision trees have been created manually as the aside example shows although increasingly and finally specialized software is employed.

3.2.2 Decision Rules:

The decision tree can be liberalized into decision rules where the outcome is the contents of the leaf node and the conditions along the path form a conjunction in the if case. Here fig.3 specifies the decision tree rules. In general, the rules have the form:

If cond1 and cond2 and cond3

DOI 10.17148/IJARCCE.2015.46119

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

Decision rules can also be generated by construct association rules with the target variable on the right.

3.2.3 Analysis Example:

Analysis can take into account the decision maker's (e.g., the company's) preference or utility function, for example: The basic interpretation in this situation is that the company prefers B's risk and payoffs under realistic risk preference coefficients (greater than $400K—in that range of risk aversion, the company need to model a third strategy neither "A nor B").

3.3 The Different Type of Attacks That Can Occur In an Intrusion Detection System [IDS]:

Probe:

It aims acquiring information about the target network from a source that is often external to the network. Basic connection level features such as the duration of connection and source bytes are important while features like number of files creations and number of files accessed are not expected to provide information for detecting investigation [9].

Dos:

A denial of service attack is an attack in which the attacker makes some computing or memory resource too busy or too full to handle legitimate request or denies legitimate users accessed to a machine. The Dos attacks are meant to force the target to stop the services that are provided by flooding it with probes not allowed by law or risks [9].

R2L:

One of the most difficult to detect as they involve the network level and the host level features. Select both the network level features such as the duration of connection and service requested and the host level features such as the number of login attempts among others for detecting R2L attacks [9].

U2R:

The U2R attacks involve the semantic details that are very difficult to capture at an early stage. Some attacks are often content based and target an application. Hence, for U2R attacks, features such as number of creations and number of shell prompts invoked are selected while features such as protocol and source bytes are ignored [9].

4. CONCLUSION AND FUTURE WORKS

In this paper analysed and some techniques, methods algorithms for enhance the network security. Each one method or algorithm have some performance ratio not only the advantages and also have some drawbacks within that. In future work will choose any one algorithm which is most secure and suitable to do better accuracy for network security process and then apply some enhancement within that to proof much better than the old performance.

REFERENCES

[1] Bharat S. Dhak, Shrikant Lade, "An Evolutionary Approach to Intrusion Detection System using Genetic Algorithm", International Journal of Emerging Technology and Advanced Engineering , Vol. 2, Issue 12, December 2012, ISSN 2250-2459.

[2] Maheshkumar Sabhnani, Gursel Serpen,"Why Machine Learning Algorithms Fail in Misuse Detection on KDD Intrusion Detection Data Set", Electrical Engineering and Computer Science Department the University of Toledo,OH 43606, USA.

[3] C.C. Su, K.M. Chang, Y.H. Kue, M.F. Horng, "The new intrusion prevention and detection approaches for clustering-based sensor networks", Proceedings of 2005 IEEE Wireless Communications and Networking Conference (WCNC'05), vol. 4, March-2005, pp. 1927-1932.

[4] Kiran Dhangar, Deepak Kulhare, Arif Khan, "A Proposed Intrusion Detection System", International Journal of Computer Applications, Vol. 65, No.23, March-2013, ISSN 0975 – 8887.

[5] Alec Yasinsac, Sachin Goregaoker,"An Intrusion Detection System for Security Protocol Traffic", Department of Computer Science Florida State University Tallahassee, Florida 32306-4530.

[6] I.Levin, "KDD-99 Classifier Learning Contest LLSoft's Results Overview", Jan-2000, Vol. 1 (2), pp. 67-75.

[7] R.Sekar, M.Bendre, D.Dhurjati, P.Bollineni, "A fast automaton-based method for detecting anomalous program behaviours", Proceedings of the 2001 IEEE Symposium on Security and Privacy (Washington, DC, USA), IEEE Computer Society, 2001, pp. 144--155.

[8] Herv´e Debar, "An Introduction to Intrusion-Detection Systems", IBM Research, Zurich Research Laboratory, Saumerstrasse 4, CH–8803 Ruschlikon, Switzerland.

[9] V.Jaiganesh, P.Rutravigneshwaran, P.Sumathi, "An Efficient Algorithm for Network Intrusion Detection System", International Journal of Computer Applications (0975 – 8887), Volume-90, No 12, March 2014.

BIOGRAPHIES

Dr.V.Jaiganesh is working as Professor in the Department of Computer Science**,** Dr N.G.P Arts and Science College, Coimbatore, India and he has completed Ph.D., in Manonmaniam Sundaranar University, Tirunelveli, Tamilnadu, India. He has done his M.Phil in the area of Data Mining and post graduate degrees MCA and MBA in Periyar University, Salem. He has about fourteen years of teaching and research experience and his research interests include Data Mining and Networking.

Mr.M.M.Karthikeyan is pursuing M.Phil Research Scholar, Department of Computer Science, Dr N.G.P Arts and Science College, Coimbatore, India.