An Overview of Intrusion Detection System in Computer Networks

Ashish Negi, Himanshu Saini

Abstract— the world has seen an era of advanced changes in networking field. This has been results in development of information exchange across all over the world. It leads to dependency on network for files transaction and valuable data. During past decades a numerous security attacks has been attempted on these networks. To ensure these networks safety Intrusion Detection System has been designed to prevent from such security attacks. Intrusion detection is a type of security management system for computer networks which gathers and analyzes information from various areas within networks to identify possible security contravention. This paper is intended to provide an overview of intrusion detection system and to give a brief idea about network protection against theft and threat.

Index Terms— Intrusion detection system, fuzzy logic, artificial intelligence.

I. INTRODUCTION

From last few decades we have seen a tremendous growth in networking technology and internet application sector. It has not only helped to carry out tasks in different sector such as financial, banking, educational, science and research etc but lead to a comfortable life. More and more users are connecting with this technology day by day. Despite, it has become an easy target to be attack by malicious and unwanted intruders. This has caused a great risk to our valuable document, software and files. Apart from it new terms such as worms, Trojans and viruses has created a fear in the minds of internet users. This resulted in a call of security and protection against these act. It can be only done if our system is able to sense and respond these attack or penetration. A helpful tool in this field is Intrusion Detection System (IDS), which not only detect the attack but also analysis it so as to take a proper action against it. This system has caused a significant prevention of cyber security and network vulnerability. Intrusion Detection was first coined by James Andersion in 1980,according to whom Intrusion is "a attack or threat to the system or network which has potential to alter, access and misuse the data and information in it ".Once the detection is marked the resistive action could be taken by it. Many reasons are there which supports the need of IDS in our networking system. One of them is the system we developed for any purpose does not contain a security system for its defense. This paper provides us an overview about intrusion detection system and various tools used under it to create a secure zone in the field of networking.

Manuscript Received on December 2014.

Ashish Negi, M.Tech Scholar, Department of Electronics & Communication Engineering, Dev Bhoomi Institute of Technology, Dehradun, India.

Himanshu Saini, Asst. Prof., Department of Electronics & Communication Engineering, Dev Bhommi Institute of Technology, Dehradun, India.

II. INTRUSION DETECTION SYSTEM & ITS SUBSYSTEMS

An Intrusion detection and response system is a powerful weapon or application which performs action and alarmed us against an act to threat, to misuse, to destroy the computer networks" In other words IDS help the system to differentiate between the right and wrong information. It filters out the undesired and danger action against our network. We can say that it's an alarm towards any theft in system [1].

Intrusion Detection provides the following:

- Monitoring and analyzing both system and user activities
- Analysis of abnormal activity pattern
- Analyzing system vulnerabilities and configurations
- Accessing file and system integrity
- Ability to recognize patterns of attacks

Fig. 1 shows different subsystem of an intrusion detection system.

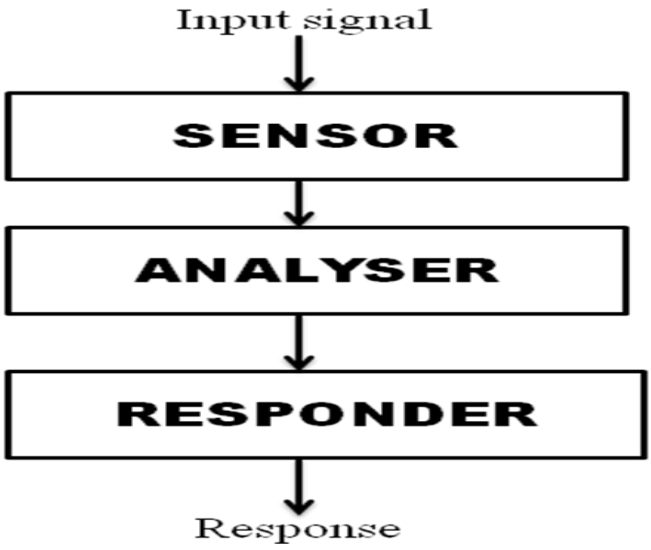

Fig. 1. Subsystems of an intrusion Detection System

1) Sensor:- A sensor is the starting subsystem of IDS which monitor and look after the information traffic in a network. In Any case of unauthorized access or attack to network it senses and sends the data to next stage of IDS.

2) *Analyzer:-*It basically collects the data from sensor and carries out calculations on it. It also makes logical and necessary decisions related to the threat.

3) *Responder:-*finally the action to be taken against the attack is performed by the responder. It not only blocks the intruder but also alarm the user about it.

III. CLASSIFICATION OF IDS

There are various ways in which we can classify IDS system. One way could be by defining the different approach such as signature and anomaly, active and passive, host and network based and centralized or distributed. Fig. 2 shows the classification of IDS system [2].

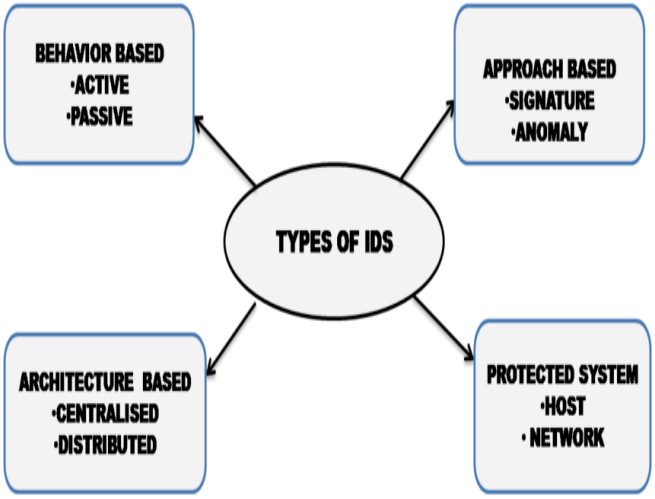

Fig. 2. Classification of Intrusion Detection System

- Approach based IDS decide the way to tackle the attacks and it is mainly of two types signature and anomaly. Signature based system also known as misuse system define the attack pattern and behavior [2]. It matches with incoming signal if matched an alarm of detection is generated. The second approach anomaly intrusion detection characterized the normal behavior of network. It detects unwanted traffic that is unknown.
- Protection based IDS can be classified on the basis information source from which information is extracted. It can provide the security either to a whole network or host. Under the category network IDS monitor whole network and its components and also checks the transactions made throughout the network, thus creating a threat free networking conditions. Host based IDS is responsible to sense information traffic related to a host. Any violating situations against the data processing protocols are reported under it.
- Behavior based IDS can also be active or passive an active IDS has a predefined response agenda based on threat. It not only generates the alarm but also takes necessary precaution against attack. A passive IDS is only made to check the system and alarm the admin about the intruder. Unlike active IDS it lacks capability to perform actions.
- The architecture of IDS to work in a networking system could be centralized or decentralized version. In centralized a single IDS unit monitors the whole system constantly viewing the network actions to find out any bug or faulty conditions. With increase in network a loading condition may arise to IDS. Hence suited to small networks such as LAN. the distributed or decentralize IDS overcome the loading condition in a central IDS it use a number of IDS are plotted among whole network which communicate with each other so called result in reliable networking safety

IV. INTRUSION DETECTION TECHNIQUES

As day by day network attacks are increasing, there are number of intrusion detection techniques implemented to protect computer systems. Some of which are discussed below [2]. These techniques just help to detect the intrusion in a network; prevention will be carried out when we will have reliable intrusion detection system.

1) Artificial intelligence

It is an engineering and scientific branch which has resulted in development of logical, conceptual and interactive machine. There are various methodologies under artificial intelligence that are used to implement IDS such as data mining, fuzzy logic and statistical approach has help to grow out an efficient IDS [8].

2) Data mining: This approach uses data volumes to evaluate the intruder attack.it is used in anamoly kind of IDS [5]. Decision tree under it are very helpful in detection of threat. Associative rules are one of its tools which can be used.

3) fuzzy logic: It is a logic related to uncertainity of natural occurring. Based on sets of conditions it is capable of using AND,OR & NOT operations.It handles the large no. of input parameters thus help in design of IDS.

4) *Genetic algorithms*: it is totally depend on biological evolution and used it as stragety against difficulties.The fitness function generated by it is very helpful in evalution of data for IDS [4] [6].

5) *Bayesian Approach:* Also known as statistical method it has various no, of nodes and arcs.It also have variable related to them and there dependency on each other .It is used for anamoly IDS in a three step process [3].

6) *Agent based:* These have self contained process and equipped with sensor to catch the intruder.these are spreaded all over networks to check threat and alarm the system about them.they are basically used in distributed type IDS.they are of two kind one is multi and other mobile kind agents[7].

V. STRENGTH AND LIMITATIONS OF IDS

In this section we will discuss what are different strength and limitations of an intrusion detection system.

A. Strength

The efficiency of IDS to check the malicious content in the input signal is much faster in comparison of men who can do the same task in days. Hence prevent extra resource utilization and time too. Hence there is no need to recruit additional networking expert to check the attacks. Apart from this it supports our firewall layer and in many case it works if firewall collapse. It can also be used in recovering the lost data in case of contaminated information analysis. It is also available in different packages at suitable cost according to the requirement of companies. Overall we can say that it's a tool with multipurpose and fits in every budget.

B. Limitations

When it's come about the limitation of IDS accuracy is the major issue which can't be neglected. It is not 100% accurate. Sometimes it generates false alarm which affects its reliability.

In many cases an error signal in IDS can lead to a significant economic and time loss. There are new ways and techniques have been developed by attackers day by day. Our IDS system is unaware of these which results an easy penetration in our databases .Until our IDS is modified these new attacks are always remain drawback of it. Though some of our IDS have learning capabilities .But still they are not automated to such a level where they can enhanced their tactics according to the situation. Another major issue in IDS is that they can't be easily modified or changed as per as need. Either you need a third team or internal experts to customize it to a specific level.

VI. CONCLUSION

This paper makes us familiar with intrusion detection system and gives us an overview of different methods to implement it so that we can protect our system in this scenario of theft and attack. It could be helpful for beginners those who are interested in the field of developing intrusion detection system.

REFERENCES

1. Khattab M. Alheeti, "Intrusion Detection System and Artificial Intelligent", ISBN 978-953-307-167-1, Published: March 22, 2011.
2. Shaik akbar, K.Nageswara Rao, J.A. Chandulal, " Intrusion Detection System Methodology Based on Data Analysis", International Journal of Computer Applications (0975-8887), Vol. 5, No. 2, Auguest 2010.
3. Peyman Kabiri, Ali A. Ghorbani, "Research on Intrusion Detection and Response: A Survey". International Journal of Network Security, Vol.1, No.2, PP.84–102, Sep. 2005.
4. Bharanidharan Shanmugam and Norbik Bashah Idris, "Hybrid Intrusion Detection Systems (HIDS) using Fuzzy Logic", ISBN 978-953-307-167-1, Published: March 22, 2011
5. Shilpa Batra, Pankaj Kumar, Sapna Sinha," Review: Soft Computing Techniques (Data-Mining) On Intrusion", International Journal of Computational Engineering Research|, vol.3, issue. 4, April 2013.
6. A.A.Ojugo, A.O.Eboka, O.E. Okonta, R.E.Yoro, F.O.Aghware," Genric Algorithm Rule Based Intrusion Detection System", journal of Emegering Trends in Computing and Information Sciences, Vol. 3, No.8, Auguest 2012.
7. Mahak Chowdhary, Shrutika Suri, Mansi Bhutani," Comparative Study of Intrusion Detection System", Journal of Computer Science International Journal of Computer Science International Journal of Computer Sciencesand Engineering and Engineering, Vol.2, No. 4, pp. (197-200), April 2014.
8. N. Puketza, K. Zhang, M. Chung, B. Mukherjee and R. A. Olsson "A methodology for testing intrusion detection systems," Proc. IEEE Transactions on Software Engineering, vol. 22, pp. 719 -729, 1996.