ISSN No:-2456 –2165

Survey on Network Intrusion Detection and Prevention System

Hemangni Mehta
Information Technology Department, SVMIT
Bharuch, India

Jignasa Patel
Information Technology Department, SVMIT
Bharuch, India

Abstract— The network systems of the world are insecure, and can come under attack from any source. The attack can be a denial-of-service state or another type of threat. The intrusion detection and prevention systems (IDPS) keep the networks safe. Intrusion detection and prevention systems (IDPS) are essentially a security measure to protect networks from both external and internal attacks. They constantly monitor network by using of different Techniques. Traffic and if a malicious threat is detected, the threat is blocked and reported for further analysis. Intrusion is critical and very major issue for Hybrid computing method. This paper gives the idea about intrusion, intrusion type, intrusion detection system, and earlier work according intrusion detection system. Hybrid detection system is higher detection accuracy providing system. The key purpose of this paper is give to idea about Hybrid intrusion detection system and how it is detect intrusion in a Hybrid Network. Software which used for prevent the system from this type of threat is called as intrusion prevention system. There are different types of Prevention system including in this paper.

Keywords*:*-Intrusion Detection System, Hybrid Computing, Hybrid in Detection System, Prevention System.

I. INTRODUCTION

An increasing number of organizations use information systems to conduct their core business activities. As a result, the frequency and magnitude of intrusion incidents have increased significantly. Intrusion attacks have many causes, such as malware (e.g., worms, spyware), unauthorized access to systems and misuse of privileges or attempt to gain additional privileges. While some incidents are malicious in nature, others are not. To reduce the exposure to both types of intrusion threats, organizations need intrusion detection systems (IDS) and intrusion prevention systems (IPS). Network-based IDS are directed toward "network-based attacks that come from outside and inside the organization" and use network adapters running in promiscuous mode to monitor network activities in real time. Promiscuous mode makes it very difficult for attackers to detect and locate it. Network-based IDS are not scalable.

AES encryption approach to prevent the intrusion in database of the any network system. Also detects and prevents the intrusion attacks like SQL injection. It provides an additional layer of security in database management system (DBMS).It can be considered as generic approach for any database and overcomes the limitations of the existing database security mechanisms [1].process of monitoring does not give guarantee the appropriate assurance and protection[3]. Hybrid Intrusion Detection system has been implemented using .Net framework as front end and SQL Server as back end to store the information. The Hybrid Intrusion Detection system has been deployed in Hybrid environment. The Dynamic characteristic of Hybrid Intrusion Detection System is achieved by building a simple and informative User Interface. Scalability and Self adaptive property of a Hybrid Intrusion Detection System is achieved by running the system both in network and in all the host of the network [2].

II. ISSUE IN HYBRID COMPUTING SYSTEM

A new hybrid intrusion detection system combines the advantages of low false-positive rate of a signature-based IDS and the ability of an anomaly-based IDS to "detect novel unknown attacks". The hybrid system extracts signatures from the output of the anomaly-based system and adds them to the signature database for accurate and efficient intrusion detection .It was shown that the hybrid IDS had a 60 percent detection rate in comparison to 30 percent and 22 percent for SNORT and Bro systems, respectively. This was obtained with less than 3 percent false alarms. This method thus achieves a "higher detection accuracy, lower false alarms, and, thus, a raised level of "cyber trust" through the automated data mining and signature generation process over Internet connection episodes. Hybrid Computing can also be called as On Demand Computing. Another interesting fact about Hybrid computing is that, Hybrid computing is like an elephant, for those who see this elephant in front will say it as snake, for those whose see in the side will say it as wall etc, yet few are able to say it is an elephant. There is no proper definition or none has defined Hybrid computing in a standardized manner [2].

III. HYBRID INTRUSION DETECTION SYSTEM

In now days all services provide via Internet. Therefore Intrusion threat is a biggest issue in Hybrid computing network. When any unauthorized person or system entering in the other system and that was harmful for any system then it simply defined as Intrusion. No proper Authentication provides in network and it damages the network system by attacking or hacking in network. For prevent the network system from this kind of Intrusion must be Detect the Intrusion. There are various kind of system used for detecting the Intrusion. Proposal of Hybrid computing Intrusion Detection system is provide standard security from threat.

There are three categories of Intrusion Detection system

a) Anomaly-based Intrusion Detection Systems.
b) Pattern-matching(or Signature-based) Intrusion Detection Systems.
c) Hybrid Intrusion Detection Systems.

A. Anomaly-Based Intrusion Detection Systems

Statistical anomaly detection model identifies intrusions by observation for activities that deviate from a user's traditional behaviour. Baselines of traditional l behaviour are established through identification explicit users or network connections then the IDS appearance for activities that are completely different from the baseline. They will find attacks that haven't been seen before as a result of they appear for uncommon behavior. They generate an oversized volume of false positives as results of unpredictable nature of behavior of users and networks. They typically need in depth coaching systems and event records to spot traditional behavior patterns. Careful hackers will disable such detection systems.

B. Pattern-Matching (Signature-Based) Intrusion Detection Systems

Pattern-matching (or signature-based) IDS examine network traffic and look for documented patters of attack. The system examines “every packet on the network segment for a defined pattern of activity that indicates an attempt to access a vulnerable script on a web server”. Implementation of patter-matching IDS takes a shorter period of time than anomaly IDS, provided that there is a pattern-matching engine It is easy to implement, deploy, update and understand pattern-matching IDS.They produce less false positives than do anomaly-based IDS. They are vulnerable to hacking. They cannot detect unknown attacks. Constant updating is required in this type of Detection system. They are easier to “fool by sending fragmented packets across the network”[3].

C. Hybrid Intrusion Detection Systems

This section includes the design of hybrid intrusion prevention approach, and describes its basic concepts from previously research work. Hybrid Detection and prevention system overcome the Problem of above both intrusion detection system. Hybrid approaches have been proposal to combine this advantage of both signature-based and anomaly-based. Both systems have advantages and disadvantages. Hybrid Intrusion detection system overcome the problem of both system [2]. Hybrid IDS consists of six components viz., i) Data acquisition module, ii) Signature database, iii) Analyser, iv) Anomaly detector, v) Signature generator, and vi) Counter-measure module[9].

D. Related Works

In the earlier works on intrusion detection system, Hasina A. Razzak. [2] has proposed a Methodological Approach given form implement Intrusion Detection System in Hybrid Network. In this paper main key issue of Hybrid Detection in network will be discussed.

Rana Aamir Raza Ashfaq Xi-ZhaoWang [3]defined theFuzziness based semi-supervised learning approach for intrusion detection system in paper. Hybrid Insnd truction Detection system has been implemented using .Net framework as front end and SQL server as back end to store the information. Anomaly Intrusion and misuse Intrusion used for detect Intrusion in network.

Komal Dhok[4] work done on Implementation of Pattern Matching Algorithm to Defend SQL Injection Attack. In this implementation needed Graphical passwords for login, and with the objective that it will in like manner not get hacked by attacker and can give more secure approval.

Nilesh B. Nanda[7]also work done on classification method of Intrusion Detection system.In this paper limitation of Anomaly based system defined. And it also classify the Hybrid NIDS and alert to the administrator.

Kanubhai K. Patel[9]has also proposed to work on Intrusion Detection system implementation. In this paper Architecture of Hybrid Intrusion Detection system consist for more information according Hybrid computing structure.

E. Architecture of our Hybrid IDS

Hybrid IDS consists of six components viz., i) Data acquisition module, ii) Signature database, iii) Analyser, iv) Anomaly detector, v) Signature generator, and vi) Counter-measure module (see Fig-1). Data acquisition module has multiple sensors. Sensors are placed either on individual host or in particular network segment. Sensors that are placed on individual hosts observe packets as they enter and leave that host. Sensors that are placed on a particular network segment read packets as they pass into and out of each segment. The sensors need to be positioned in locations where they will be able to capture all of the packets entering and leaving a host or network segment. Sensors that are placed on network segments do not always have the ability, if the traffic level becomes too heavy, to capture every packet. Repositioning the sensors on each network host will improve accuracy even though the effort of installing them can be considerable. The important thing is to be able to capture all packets so that none can potentially circumvent the IDS. For our purposes we use Snort on the Windows operating system using WinPcap. The Signature database records enable the IDS to have a set of signature, criteria or rules against which they can compare packets as they pass through the sensor. The database of signatures needs to be installed along with the IDS software and hardware itself. After the Signature database is in place, sensors of the Data acquisition module gather data by reading packets from the network and reassemble them. As packets from network can arrive out of order, or can be duplicated. Moreover, packets arrive at a high speed therefore the Data storage is required to store the packets. The Analyzer module compares the packets it observes with the signatures or rules of normal patterns of behaviour stored in Signature database using pattern-matching algorithm. We use the well-known Aho-Corasick algorithm for performing pattern matching. If analyzer finds any match then sends appropriate alert message for known attack to the Counter-measure module. Also it enters entry in log file about the event that caused the alert. If analyzer does not find any match then sends data to Anomaly detector for finding anomaly using pattern mining technique. If Anomaly detector finds any anomaly then send appropriate message to Signature generator. Here Signature generator creates rule or signature and make new entry in Signature database. When Counter-measure module receives the alert message of known attack from Analyzer, it notifies the administrator in one of several ways that the administrator has configured beforehand. The module might display a pop-up window or sends an e-mail message to the designated individual, for example. Besides the automated response sent to the administrator, this module can be configured to take action at the same time that an alert message is received. Typical actions are: i) Alarm, in which an alarm is sent to the administrator, ii) Drop, in which the packet is dropped without an error message being sent to the originating computer; and iii) Reset, which instructs the IDS to stop and restart network traffic and thus stop especially severe attacks. This module is also used by network administrator to evaluate the alert message and to take proper actions such as dropping a packet or closing a connection. The administrator can anticipate having to fine-tune the signature database to account for situations that seem to the IDS to be intrusions but that are actually legitimate traffic.

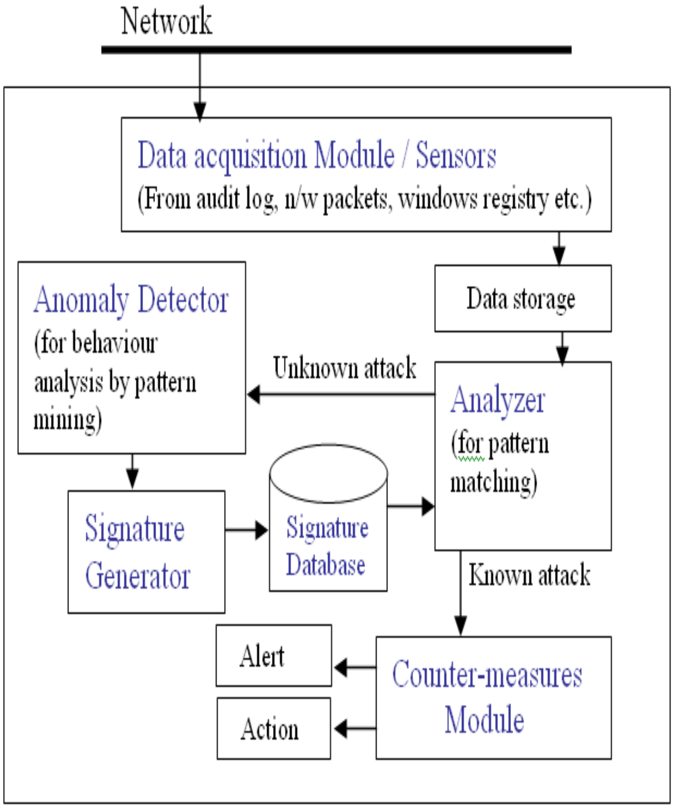

Figure1. Systematic Diagram of Hybrid IDS [9]

For example, an adjustment might be made to enable traffic that might otherwise be seen by the firewall as suspicious, such as a vulnerability scan performed by a scanning device located at a particular IP address. The IDS could be configured to add a rule that changes the action performed by the IDS in response to traffic from that IP address from Alarm to Drop.

IV. CONCLUSION

The proposed of Hybrid model is Detect malicious packets within network traffic and stop intrusions dead, blocking the aberrant traffic automatically before it does any damage in Hybrid network rather than simply giving an alert as, the malicious load has been delivered. It were invented independently to resolve ambiguities in network monitoring by placing prevention. The proposed model can be implemented in very low cost and within short time.

REFERENCES

[1]. Yashashree Dawle, Manasi Naik,Sumedha Vande,Nikita Zarkar ,"Reserch of Database Security Using Intrusion Detection System" International Journal of Latest Engineering Research and Applications (IJLERA) ISSN: 2455-7137 Volume – 02, Issue – 03, March – 2017, PP – 01-06.

[2]. Hasina A. Razzak. A. Karim, S.S Handa, M.V. Ramana Murthy" A Methodical Approach to Implement Intrusion Detection System in Hybrid Network" IJESC 2017, Volume 7 Issue No.3.

[3]. Komal Dhok, Vrushali Wadibhasme, Vaishnavi Maske, Saylee Shrirame, Vishesh Gaikwad" Reserch of Implementation of Pattern Matching Algorithm to Defend SQL Injection Attack" IJESC 2017, Volume 7 Issue No.3.

[4]. Haiqa Fayaz"Reserch of Cloud Security Enhancement Through Intrusion Detection System" International Journal of Advanced Research in Computer Science, Volume 8, No. 2, March 2017.

[5]. Parveen Sadotra, Dr. Chandrakant Sharma"Research of Intrusion Detection in Networks Security: A New Proposed Min-Min Algorithm" International Journal of Advanced Research in Computer Science,Volume 8, No. 3, March – April 2017.

[6]. Nilesh B. Nanda ,Dr. Ajay Parikh H"Reserch of Classification and Technical Analysis of Network Intrusion Detection Systems "International Journal of Advanced Research in Computer Science, Volume 8, No. 5, May-June 2017.

[7]. Janu Gupta, Jasbir Singh" Detecting Anomaly Based Network Intrusion Using Feature Extraction and Classification Techniques" International Journal of Advanced Research in Computer Science,volume 8, No. 5, May – June 2017.

[8]. Atmaja Sahasrabuddhe, Sonali Naikade, Akshaya Ramaswamy, Burhan Sadliwala , Prof.Dr.Pravin Futane," Survey on Intrusion Detection System using Data Mining Techniques, International Research Journal of Engineering and Technology (IRJET)Volume:04 Issue: 05 May -2017.

[9]. Kanubhai K. Patel, Bharat V. Buddhadev"Research of An Architecture of Hybrid Intrusion Detection System" International Journal of Information & Network Security (IJINS) Vol.2, No.2, April 2013, pp. 197~202.

[10]. Amaan Anwar & Syed Imtiyaz Hassan," Applying Artificial Intelligence Techniques to Prevent Cyber Assaults "International Journal of Computational Intelligence Research ISSN 0973-1873 Volume 13, Number 5 (2017), pp.