International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 12, December 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

Distributed Intelligent Intrusion Detection System

Mrs. J.Joselin[1], Mr. A.Mohammed Yasin[2], Mr. M.Ashiq[3]

[1]Assistant Professor ,

[2,3](M.Sc. SS Student),

Department of BCA & M.Sc. SS

Sri Krishna Arts and Science College

Coimbatore

ABSTRACT

The branch of security barriers of the computer system has been always a better concern in the information technology era. The intrusions and attacks seem to come from different angles and in different types every day. It has been a critical battle to keep pace with the increasingly mounting threats to the computer systems through networks for any possible loopholes and vulnerabilities .the intruders exploit these compromising vulnerabilities to mount attacks .The existing Instruction Detection Systems (IDS) are not efficient and known type, whereas the misuse detection-based IDS produce a big cost of false alarm and still need administrator assistance. Traditional IDS are increasingly limited by their need for an up-to-date and comprehensive knowledge base. There is a need for intelligent IDS, and this paper introduces internet-based distributed IDS with the capability to learn and detect new types of attacks. This IDS focuses on overcoming the most prominent drawback of the existing IDS and may be a step forward in a new direction.

Keywords: Networks, Intrusion Detection System, Architecture and Design of the System

I.INTRODUCTION

Security for computer and internet system which contains valuable data has received the most priority due to the rapid growth of technology in all computing fields. Secured in depth will need to include firewalls installed to prevent unauthorized access, antiviral software installed to detect viruses and intrusion detection system (IDS) placed to prevent outsiders from breaking into the system or to prevent misuse of the system by an insider.

An intrusion into an information system tries to compromise the security of the system, stems either from inside the internet or outside the internet, can steal classified information or create havoc in the system and halt as well as deny access to legitimate user activities incurring big economic losses [2]. An IDS aims at detecting intrusive activities and gives warnings to the system security administrator. Based on application strategy, existing IDS can be categorized into mainly three types: host-based IDS, often referred to as HIDS; internet-based IDS; and route-based IDS, also abbreviated as NIDS. Host-based IDS are usually deployed on individual host-machines to monitor activities on the host machines. Internet-based IDS are installed in some strategic computers in the internet to monitor data packets sent between Host Router-based IDS are installed on routers to monitor data

packets passing through routers, thus trying to prevent intrusive data packets from entering the internet inside the router. Router-based IDS are similar to internet-based IDS [9].

The IDS can also be categorized based on the detected technique strategy signature based detection, anomaly detection and specification based detection. In signature based intrusion detection, the data is matched against known attack features, thus limiting the technique largely to known attacks, even excluding variants of known attacks. In anomaly detection, profiles of normal performance of systems, usually well-known through automated training, are related with the actual action of the system to flag any significant deviation. Anomaly detection can identify unknown attacks, but often at the price of a high false alarm rate. The security mechanism and detection technique used in the traditional IDS demonstration severe weakness such as robustness, scalability, intelligence, and less human interaction. The new findings also reveal that there is a variant breed of IDS emerging in the industry, joining the signature based detection and abuse detection techniques, these are named as hybrid IDS [7].

The network based distributed intelligence IDS will overcome most of the drawbacks of the present systems. It is essential to provide good IDS since security wise, the IDS faces a large number of threats. Accuracy of detection is a powerful criterion of the proposed system. In brief, the architecture and the selection of the detection algorithms play a major role in making the IDS efficient.

II. SYSTEM REQUIREMENTS

The system requirement plays a vital role here. The requirement is classified into two groups: functional and Non-functional requirements. If we take the past records, a number of different proposals have been made. Each proposal varied from one another in characteristics such as architecture, techniques used, processing methods and even deployment strategies. Nevertheless, the researchers have always focused on one primary goal that is instruction detection [3].

For IDS to be considered as quality system, it is very important the instruction system should address and present a certain cost of common quality characteristics it is pretty difficult to accommodate the entire functionalities and characteristics in one system due to difficult set of constraints.

The system is constructed with functional requirements like creating admin profile. The profiles should be uniquely local to each node, thus only authorized people who are admin will perform operation on authorized nodes. This will eliminate the unnecessary generalizing and globalizing of the admin profiles, managing vulnerability predicates and thresholds will also reduce the unnecessary produced false alarm. Further functional detection and invoke alerts. Meanwhile non-functional requirements such as accuracy, performance, scalability, security, false positive rate, fault tolerance, resilience, reliability and completeness also be incorporated to the system [6].

III.ARCHITECTURE

The IDS face a large number of threats from internal and external entities. These systems are responsible not only for the security of the internet and other system also for their own security [8]. The architecture of the systems is one of the main focus areas in improving the security. System activities are briefly described by using the use case diagram. The produced system is aimed at enhancing the accuracy of detection, detecting unknown and known attacks, reduction of false alarms and resources consumption. The novel architecture introduced self-learning capability to the proposed system [1].

There are mainly two types of detection techniques, namely, misuse detection and anomaly detection. The misuse is also called signature-based detection. The approach to instruction detection is based on the malicious behaviour in the form of signature and then monitoring it. This approach is very good at detecting attacks which are known but will miss new attack method, even if they are just minor variations on old attacks. On the other hand, in contrast to misuse detection, anomaly detection works by building a model to represent normal system usage and then monitoring anything that does not fit this model. This approach is good at detecting novel attacks that a system using misuse detection would miss [1].

The novel architecture for the proposed system takes advantage of the drawbacks of the existing architecture. The architecture enables distribution of both learning process and internet monitoring process. Mainly there are two separate components in this architecture. The architecture describes two processing unit, namely, real-time monitoring unit (RTMU) and central anomaly processing units (CAPU).

Each processing unit receives data or packets of data sniffed by the sensor from the internet and then processes in its own way. The architecture proposes two separate and parallel processing units, one performing the learning and other monitoring. If both processors operate concurrently, the RTMU can benefit from the feedback of the CAPU and can constantly improve its learning by redefining the new models or signatures [4].

The sniffed internet traffic in initially passed through a filter called data purifier. This operation is performed in order to remove insignificant data packets such as acknowledgment packets. This will greatly influence the quality of data passed to the processing units, thereby refraining from wasting time on processing insignificant data packets. When the filtered data packets are forwarded to the CAPU, the insignificant data packets are dropped off by the detection engine. The significant packets are grouped and placed on a window of arrays.

Some researches tend to group the data packets as connection-oriented packets and the data packets. And each of which is further grouped to perform detection processing. Thus the repetition of detection processing; leads an extra burden on processing power and additional resources consumption. The threshold level module is mainly focused on reducing the false alarms. When the vulnerability model is applied on the clustered data packets, it tends to give various readings for different groups of data packets depending on the matching totality of the vulnerability predicates. Nevertheless, it is necessary we should prioritize the vulnerability levels. The application of threshold levels greatly helps to understand the genuine vulnerability.

International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 12, December 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

IV.DESIGN OF SYSTEM

The intercommunication design between data sensor and processing unit describes the architecture and specifies a queuing communication model, thus allowing the internet sensor to place the packets in the queue and get ready for the next packet, while at the same time, the processing units consume the packets placed in the queue. The intercommunication design between data sensor and central anomaly processing unit is referred to as piping technology and the implementation of pipe is carried out with the help of the piping technology of PERL language.

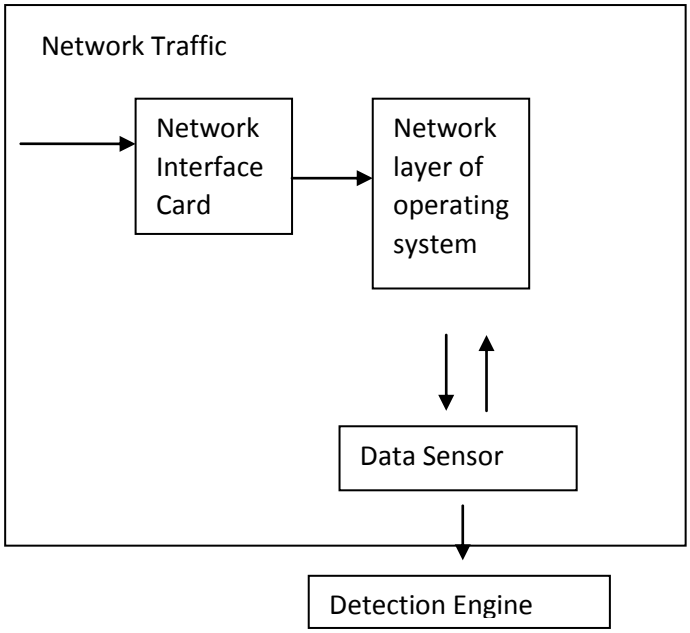

Figure 1: The Data capturing phases and the communication between the different layers of the operating system

In implementation, the practical Extraction and Reporting language (PERL) has been used to implement the prototype version of the proposed system. The proposed prototype system. The proposed prototype system has well benefited from the string manipulation capabilities of PERL. The "TK" extension module provides a path to implement contemporary Graphical User Interfaces for the front end of the systems [10] .The results of the evaluation showed that the system accurately detected any abnormal activity and generated alerts notifying the administrator. The internet IDS that are often considered by researchers demand special deployment configurations in the internet. Since most of the internet IDS that have been proposed are based on centralized architecture, this inherently creates single point of failure. We can detect attacks, either previously known or novel strategy attacks, since any attack will result in an abnormal activity. This is the philosophy behind anomaly-based IDS. Also, the denial of service attack was accurately detected by the system and notifications sent to the administrator, which is a big achievement for the project as many current system lack this detection capability [5]. The system configurations suffer that is proposed in this research can work seamlessly without modifying any part of the physical network. The proposed system has ability to collect data from any types of

internet for intrusion detection. The proposed system is good at detecting attacks. Unlike the other systems, the proposed system does not implement a database to store data; instead it uses a simple file system [11]. This system provides real time intrusion detecting and altering facility. The prototype of the proposed system is implemented with very less significant performance issues.

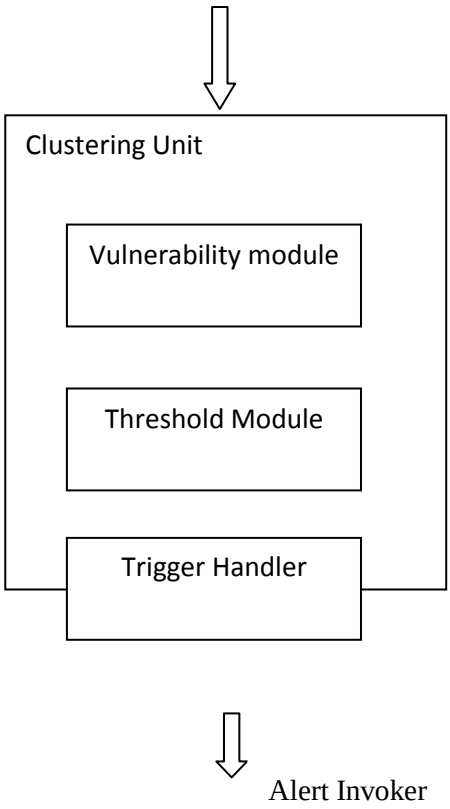

Figure 2: Interior Components of Central Anomaly Processing Unit

For example, Windows XP systems have a default configuration which allows then to give higher priority to users program as compared to certain system programs. The proposed system makes use of data clustering to identify anomalies. This system is more focused on novel attacks rather than known attacks. However, the system also has provisions for known attacks.

V.CONCLUSION

Since most of the network intrusion prevention systems that have been proposed are based on signature analysis, it inherently creates single point of failure. Since the system was proposed to networked systems, it is not necessary to have either spanning ports or tap ports. The proposed system is good at detecting attacks. The system can be easily deployed on already configured and installed wireless networks too.

REFERENCES

[1] Dr.S.Vijayarni and Ms.Maria Sylviaa.S "Intrusion Detection System-A Study " ,International Journal of security , privacy and Trust Manangement (IJSPTM), Vol 4,No 1 Feb 2015.

[2] SAIDI BEN BOUBAKER Ourida "Implementation of an Intrusion Detection System" IJCSI International Journal of computer science Issues ,Vol 9,Issue 3,No 1,May 2012.

[3] J.Antony Jeyanna , E.Indumathi , Dr.D.Shalini Punithavathani ,"A Network Intrusion Detection System Using Clustering and Outlier Detection " , International journal of innovative Research in computer and communication engineering ,Vol 3,Issue 2, Feb 2015.

[4] Andrew S Tanenbaum (2003), Computer Networks, 4th Edition, prentice Hall, ISBN; 0-13-066102-3

[5] .Bria D Foy (2007), Mastering Perl, Published by O'Reaily, ISBN: 0596527241.

[6] .Event Monitoring Enabling responses to Anomalous Live Disturbance (EMERALD), [Online] available at http://www.csl.sri.com/projects/emerald/.

[7] .Network intrusion Detection: Evasion, Traffic Normalization, and End-to-End Protocol Semantics, [Online] available at http://www.icir.org/vern/papers/normusenix-sec-01-html/index.html

[8] .Sandeep kumar (1995),Intrusion Detection In Our Time,[Online] available at http://www.cerias.purdue.edu/about/history/coast/projects/

[9] .Perl Express, [Online] available at http://www.perl-express.com/index.html

[10].Stephan Lidie and Nancy Walsh (2002). Mastering Perl/TK, published by O'Reilly ISBN:1565927168.

[11].Survey of intrusion detection Systems, [online] available at http://www.mnlab.cs.depaul.edu/seminar/spr2003/IDS.pdf