IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified

Vol. 5, Issue 10, October 2016

Intrusion Detection System with various Classification and Optimization Techniques: A Survey

Babita Kumari[1], **Piyush Singh**[2]

Department of Computer Science & Engineering, RKDFIST, Bhopal, India[1, 2]

Abstract: Various kinds of network are becoming very essential nowadays. This value is getting increase due to the more and more need of data and information sharing. Intrusion Detection Systems (IDSs) attempt to identify unauthorized use, misuse, and abuse of computer systems. In response to the growth in the use and development of IDSs, it has become more important aspect. In this paper, we identify a set of general IDS optimization techniques. This article presents the details of the methodology, including strategies for Intrusion. This article also provides background information on intrusions and IDSs to motivate our work. This article mainly deals with the various optimization and classification methods.

Keywords: Classifiers, Optimization techniques, Intrusion Detection.

I. INTRODUCTION

Intrusion detection systems (IDSs) are usually deployed along with other preventive security mechanisms, such as access control and authentication, as a second line of defense that protects information systems. There are several reasons that make intrusion detection a necessary part of the entire defense system. First, many traditional systems and applications were developed without security in mind. In other cases, systems and applications were developed to work in a different environment and may become vulnerable when deployed Intrusion detection complements these protective mechanisms to improve the system security. Moreover, even if the preventive security mechanisms can protect information systems successfully, it is still desirable to know what intrusions have happened or are happening, so that we can understand the security threats and risks and thus be better prepared for future attacks.

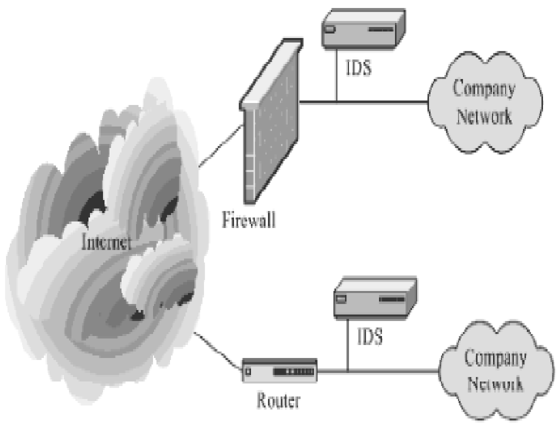

Fig 1:- IDS

The attack can be launched in term of fast attack or slow attack. Fast attack can be defined as an attack that uses a large amount of packet or connection within a few second [1]. Meanwhile, slow attack can be defined as an attack that takes a few minutes or a few hours to complete [2]. Both of the attack gives a great impact to the network environment due to the security breach decade.

As in Fig:-1, Currently IDS is used as one of the defensive tools in strengthens the network security especially in detecting the first two phases of an attack either in form slow or fast attack An intrusion detection system can be divided into two approaches which are behavior based (anomaly) and knowledge based (misuse) [3], [4]. The behavior based approach is also known as anomaly based system while knowledge based approach is known as misuse based system [5], [6].The misuse or signature based IDS is a system which contains a number of attack description or signature that are matched against a stream of audit data looking for evidence of modeled attack [7]. The audit data can be gathered from network traffic or an application log. This method can be used to detect previous known attack and the profile of the attacker has to be manually revised when new attack types are discovered.

Hence, unknown attacks in network intrusion pattern and characteristic might not be capture using this technique [8].Meanwhile, the anomaly based system identifies the intrusion by identifying traffic or application which is presumed to be normal activity on the network or host . The anomaly based system builds a model of the normal behavior of the system and then looks for anomalous activity such as activities that do not confirm to the established model. Anything that does not correspond to

DOI 10.17148/IJARCCE.2016.51093

the system profile is flagged as intrusive. False alarms generated by both systems are major concern and it is identified as a key issues and the cause of delay to further implementation of reactive intrusion detection system [9].

II. INTRUSION DETECTION SYSTEM

An intrusion detection system is a software program which helps to identify the malicious program which enter our system or in network. It helps to secure our system by responding to the malicious program. It is divided into two types. They are host based intrusion detection system and network based intrusion detection system. The active system will respond to the malicious program. But the passive system will detect only whether any malicious packets entered the system or not[7].

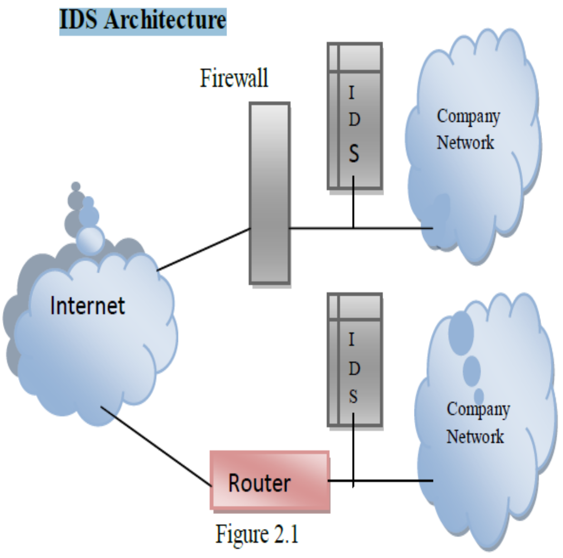

Figure 2.1

Intrusion detection system came into picture around 1980 with the publication of John Anderson's Computer Security Threat Monitoring and Surveillance, which was one of the earliest papers in the field. "An Intrusion Detection Model", published in 1987, provided a methodological framework that inspired many researchers and laid the groundwork for commercial products [10].

Intrusion Detection System (IDS) are the popular and useful tools for enhancing the security of the system and because of their value; they have now become a very important part of modern network security technology. Intrusion detection (ID) is a type of security management system for various computers as well as networks. An Intrusion Detection System collects all the information from the Host or the networks which include both anomaly and misuse intrusions. Intrusion detection functions include:

- ✓ Monitoring and analysing both user and system activities,
- ✓ Analysing system configurations and vulnerabilities,
- ✓ Assessing system and file integrity.

IDS can be categorized in two ways: one is Host based Intrusion Detection System (HIDS) and another one is Network Intrusion Detection System (NIDS).

III. VARIOUS OPTIMIZATION TECHNIQUES

IDS use several techniques, which involve the IDS stopping the attack itself, changing the security environment (e.g., reconfiguring a firewall), or changing the attack's content.

The types of IDS technologies are differentiated primarily by the types of events that they monitor and the ways in which they are deployed.

A. Network Behavior Analysis (NBA), which examines, network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service (DDoS) attacks, certain forms of malware, and policy violations (e.g., a client system providing network services to other systems). Behavior-based analysis learns the normal behavior of traffic and systems and then continually examines them for potentially harmful anomalies and for behavior that frequently accompanies incidents. This approach recognizes attacks based on what they do, rather than whether their code matches strings used in a specific past incident. ―It stops traffic that is not malicious on its face but that will do malicious things said Allan Paller [11].

B. Wireless
This technique monitors wireless network traffic and analyzes it to identify suspicious activity involving the wireless networking protocols themselves [12].

C. Host-based
It can analyze activities on the host it monitors at a high level of detail, it can often determine which processes and/or users are involved in malicious activities. Though they may each focus on a single host, many host-based IDS systems use an agent-console model where agents run on (and monitor) individual hosts but report to a single centralized console (so that a single console can configure, manage, and consolidate data from numerous hosts). Host-based IDSs can detect attacks undetectable to the network-based IDS and can gauge attack effects quite accurately [13]. Various Optimization techniques are listed below:

Table 1: Various Optimization techniques are listed below

S. No.	Techniques	Brief
1	Network Behavior	examines, network traffic to identify threats that generate unusual traffic flows
2	Wireless	technique monitors wireless network traffic and analyzes
3	Host-based	It use an agent-console model where agents run on (and monitor) individual hosts but

		report to a single centralized console (so that a single console can configure, manage, and consolidate data from numerous hosts).

IV. VARIOUS CLASSIFICATION TECHNIQUES

The following criteria will be adopted in the classification of the IPS/IDS:

Reliability: The generated alerts must be justified and no intrusion to escape.

Reactivity: An IDS/IPS must be capable to detect and to prevent the new types of attacks as quickly as possible. Thus, it must constantly self-update. Capacities of automatic update are so indispensable.

Facility of implementation and adaptability: An IDS/IPS must be easy to function and especially to adapt to the context in which it must operate. It is useless to have an IDS/IPS giving out some alerts in less than 10 seconds if the resources necessary to a reaction are not available to act in the same constraints of time.

Performance: the setting up of an IDS/IPS must not affect the performance of the supervised systems. Besides, it is necessary to have the certainty that the IDS/IPS has the capacity to treat all the information in its disposition because in the reverse case it becomes trivial to conceal the attacks while increasing the quantity of information. These criteria must be taken into consideration while classifying an IDS/IPS, as well:

- ✓ The sources of the data to analyze, network, system or application
- ✓ The behaviour of the product after intrusion passive or active
- ✓ The frequency of use, periodic or continuous
- ✓ The operating system in which operate the tools, Linux, Windows, etc.
- ✓ The source of the tools, open or private [14].

Various Optimization techniques are listed below:

Various Classifiers are listed below:

Table 2: Various Classifiers are listed below

S. No.	Techniques	Methods
1	Soft Computing Based	Neural Network
		Genetic Algorithm
		Fuzzy
2	Tree Based	J48
		ID3
		CART
3	Others	Binary, etc

V. LITERATURE REVIEW

Intrusion Detection System (IDS) has been used as a vital instrument in defending the network from this malicious or abnormal activity. it is still desirable to know what intrusions have happened or are happening, so that we can understand the security threats and risks and thus be better prepared for future attacks With the ability to analyze network traffic and recognize incoming and ongoing network attack, majority of network administrator has turn to IDS to help them in detecting anomalies in network traffic In this paper, we focus on different types of attacks on IDS this paper gives a description of different attack on different protocol such as TCP ,UDP,ARP and ICMP [15]

Web servers are ubiquitous, remotely accessible, and often misconfigured. In addition, custom web-based applications may introduce vulnerabilities that are overlooked even by the most security-conscious server administrators. Consequently, web servers are a popular target for hackers. To mitigate the security exposure associated with web servers, intrusion detection systems are deployed to analyze and screen incoming requests. The goal is to perform early detection of malicious activity and possibly prevent more serious damage to the protected site. Even though intrusion detection is critical for the security of web servers, the intrusion detection systems available today only perform very simple analyses and are often vulnerable to simple evasion techniques. In addition, most systems do not provide sophisticated attack languages that allow a system administrator to specify custom, complex attack scenarios to be detected. This paper presents WebSTAT, an intrusion detection system that analyzes web requests looking for evidence of malicious behavior. The system is novel in several ways. First of all, it provides a sophisticated language to describe multistep attacks in terms of states and transitions. In addition, the modular nature of the system supports the integrated analysis of network traffic sent to the server host, operating system-level audit data produced by the server host, and the access logs produced by the web server. By correlating different streams of events, it is possible to achieve more effective detection of web-based attacks. [16]

VI. CONCLUSION

The main objective of this paper is to provide an overview of the necessity and utility of intrusion detection system. This paper gives complete study about types of IDS, life cycle, various domains, types of attacks. IDS are becoming essential for day today security in corporate world and for network users. IPS defines about the preventing measures for the security. In the lifecycle the phases developed and the stages are illustrated. Still, there are more challenges to overcome. The techniques of anomaly detection and misuse detection are specifically illustrated and more techniques can be used. Further Work will be done on comparative analysis of some popular data mining algorithms (classier) applied to IDS and enhancing a classification based IDS by various optimization techniques.

REFERENCES

[1] Nicholas J. Puketza, Kui Zhang, Mandy Chung, Biswanath Mukherjee*, Ronald A. Olsson, "A Methodology for Testing Intrusion Detection Systems".
[2] Faizal, M.A., Mohd Zaki M., Shahrin Sahib, Robiah, Y., Siti Rahayu, S., and Asrul Hadi, Y. "Time Based Intrusion Detection on Fast Attack for Network Intrusion Detection System", Second International Conference on Network Applications, Protocols and Services, IEEE, 2010.
[3] Cuppen, F. & Miege, A. (2002). Alert Correlation in a Cooperative Intrusion Detection Framewok. In Proceeding of the 2002 IEEE Symposium on Security and Privacy. IEEE, 2002]
[4] Cabrera, J.B.D., Ravichandran, B & Mehra R.K. (2000). Statistical Traffic Modelling for Network Intrusion Detection. In Proceeding of the IEEE Conference.
[5] Yeophantong, T, Pakdeepinit, P., Moemeng, P & Daengdej, J. (2005).Network Traffic Classification Using Dynamic State Classifier. In Proceeding of IEEE Conference
[6] Farah J., Mantaceur Z. & Mohamed BA. (2007). A Framework for an Adaptive Intrusion Detection System using Bayesion Network. Proceeding of the Intelligence and Security Informatics, IEEE, 2007.
[7] Cabrera, J.B.D., Ravichandran, B & Mehra R.K. (2000). Statistical Traffic Modelling for Network Intrusion Detection. In Proceeding of the IEEE Conference.
[8] Sekar, R., Gupta, A., Frullo, J., Shanbhag, T., Tiwari, A., Yang, H. & Zhou, S. (2002). Spesification-based Anomaly Detection: A New Approach for Detecting Network Intrusions. In Proceeding of CCS ACM Conference.
[9] Karl Levitt. (2002). Intrusion Detection: Current Capabilities and Future Direction. Proceeding of IEEE Conference of the 18th Annual Computer Security Application, IEEE, 2002.
[10] Anderson, J.P., 1980. Computer Security and Threat Monitoring Surveillance. Technical report at Co. Fort Washington Pennsylvania.
[11] David Geer, Behavior-Based Network Security Goes Mainstream, IEEE,14-17, march 2006
[12] Tiwari Nitin, S. R. Singh and P. G. Singh, Intrusion Detection and Prevention System (IDPS) Technology- Network Behavior Analysis System (NBAS), International Science Congress Association , 51-56, July (2012).
[13] Karen Scarfone, Peter Mell, Guide to Intrusion detection and prevention systems (IDPS), NIST, 1 to 127, 2007.
[14] B. Santos Kumar et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 4 (1) , 2013, 77 – 82, "Intrusion Detection System- Types and Prevention".
[15] Volume 2, Issue 8, August 2012, " An Overview on Intrusion Detection System and Types of Attacks It Can Detect Considering Different Protocols".
[16] Giovanni Vigna William Robertson Vishal Kher Richard A. Kemmerer, "A Stateful Intrusion Detection System for World-Wide Web Servers".

DOI 10.17148/IJARCCE.2016.51093