© 2016 IJSRSET | Volume 2 | Issue 1 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

A Concept on Intrusion Detection System Genetic Algorithm, Fuzzy Logic and Challenges – A Review

Anshul Atre, Rajesh Singh

Department of Computer Science and Engineering, NITM Gwalior, Madhya Pradesh, India

ABSTRACT

Intrusion Detection System (IDS) which is increasing the key element of system security is used to identify the malicious activities in a computer system there are different approaches being employed in intrusion detection systems. The prediction process may produce false alarms in many anomaly based intrusion detection systems. With the concept of fuzzy logic, the false alarm rate in establishing intrusive activities can be reduced. A set of efficient fuzzy rules can be used to define the normal and abnormal behaviors in a computer network. Research papers regarding the foundations of intrusion detection systems, the methodologies and good fuzzy classifiers using genetic algorithm which are the focus of current development efforts and the solution of the problem of Intrusion Detection System to offer a real-world view of intrusion detection. Ultimately, a discussion of the upcoming technologies and various methodologies which promise to improve the concept of IDS

Keywords: Intrusion Detection System (IDS), definition and classification and challenges, Genetic algorithm, Fuzzy logic

I. INTRODUCTION

Intrusion detection is the process of monitoring the events ([1], [2], [3]) occurring in a computer system or network and analyzing them for signs of probable incidents, which are violations or forthcoming threats of violation of computer security strategies, adequate used policies, or usual security practices. Intrusive events to computer networks are expanding because of the liking of adopting the internet and local area networks [4] and new automated hacking tools and strategy. Computer systems are evolving to be more and more exposed to attack, due to its wide spread network connectivity.

Currently, networked computer systems play an ever more major role in our society and its economy. They have become the targets of a wide array of malicious threats that invariably turn into real intrusions. This is the reason computer security has become a vital concern for network practitioner. Too often, intrusions cause disaster inside LANs and the time and cost to renovate the damage can grow to extreme proportions. Instead of using passive measures to repair and patch security hole once they have been exploited, it is more Intrusion Detection Systems (IDS) are primarily focused on identifying probable incidents, monitoring information about them, tries to stop them, and reporting them to security. IDSs have become a basic addition to the security infrastructure of almost every organization. A usual Intrusion Detection System is demonstrated in Figure A **(very simple ids system).**

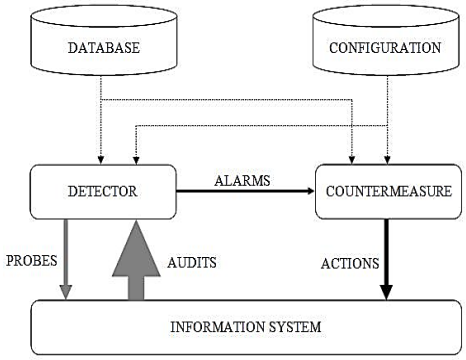


Figure 1 : Simple IDS system

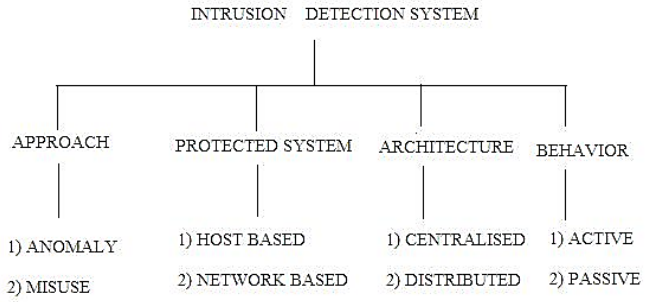
The Intrusion detection system in a similar way

complements the firewall security. The firewall protects an organization from malicious attacks from the Internet and the Intrusion detection system detects if someone tries to break in through the firewall or manages to break in the firewall security and tries to have access on any system in the trusted side and alerts the system administrator in case there is a breach in security**.**

II. METHODS AND MATERIAL

A. Classification of Intrusion Detection System

Intrusion detection system can be classified in various ways. This classification is based on data source, behavior, structure, how the system is protected and how intrusions are detected



- Approach based IDS is mainly classified into anomaly and misuse. Anomaly intrusion detection also known as behavior based system detects those attacks that are quite different from normal behavior i.e. it detects unwanted traffic that is unknown. It is able to find new attacks. The second approach misuse detection also known as signature based system only detects known attacks. Each of these techniques has their strength.
- Protection based IDS type is classified according to data source from which information is extracted. Host based IDS depends upon single host or computer system. It is implemented by placing sensor on a particular computer system. On other side network based IDS examines each and every node on network under observation. However IDS available in market are hybrid.
- IDS can also distribute or centralized. In distributed IDS numbers of IDS are present o
- The networks where they communicate with each other or to a centrally located sever. Whereas IDS can also be a standalone system.

B. Intrusion Detection Techniques

As network attacks are now and then increasing, there are many intrusion detection techniques implemented to protect computer system. These techniques differ in working, way of implementation, and many more factors. However these techniques just help to detect intrusion in network, prevention will be carried out when we will have reliable intrusion detection system. [8] The fundamentals of various techniques used to detect intrusions are described below.

Artificial intelligence (AI) is a branch of computer science that develops intelligent machines, that in includes reasoning, manipulation, logic, probability, and many others. There are various methodologies under AI that are used to implement IDS, they are artificial neural network, Fuzzy logic, Data mining, Genetic algorithm, immune system, Bayesian inference, clustering and outlier detection. These techniques are also named under machine learning method. [2] Artificial neural network works similar to human brain and is used generally for unsupervised intrusion detection

Fuzzy logic is a many valued logic which is used in intrusion detection system to distinguish data into different labels, as like normal, malicious or any other type. [2]

Data mining is used for volume data. It detects intrusion by either using associative rules, or by means of clustering.

Genetic algorithm based on chromosome like structure provides classification rules to classify incoming data. It is two step procedure including coding a program and then finding fitness function to detect intrusion. [4]

As human being has resistance power against bacteria, virus's similar systems are built to distinguish what is norm al and what is abnormal. [4]

III. RESULTS AND DISCUSSION

Challenges in IDS

There are number of challenges that impact on organization's decision to use IDS. In this section I have described a few challenges that the organizations encounter while installing an intrusion detection system. These are discussed below

1. **Human intervention** - IDS technology itself is experiencing a lot of enhancements. It is therefore very important for organizations to clearly define their prospect from the IDS implementation. Till now IDS technology has not achieved a level where it does not require human interference. Of course today's IDS technology recommends some automation like reporting the administrator in case of detection of a malicious activity,
2. **Historical analysis** - It is still very important factor to monitor the IDS logs regularly to continue on top of the incidence of events. Monitoring the logs on a Hence it is vital for an organization to have a distinct incident handling and response plan if an intrusion is detected and reported by the IDS. Also, the organization should have expert security personnel to handle this kind of situation.

3. **Deployment** - The success of an IDS implementation depends to a large degree on how it has been deployed. A lot of plan is necessary in the design as well as the implementation phase. In most cases, it is required to apply a fusion solution of network based and host based IDS to gain from both cases. In fact one technology complements the other.

IV. CONCLUSION

This paper gives us knowledge of what is an intrusion detection system, its types and in how many ways we can implement it. We are sure that this paper will be helpful to beginners those who are interested in the field of developing intrusion detection system. In this paper, I have described an overview of some of the current and past intrusion detection technologies which are being utilized for the detection of intrusive activities against computer systems or networks. The different detection challenges that affect the decision policy of the IDS employed in an organization are clearly outlined. I propose to use the new definition of the complement of fuzzy sets where the fuzzy membership value and fuzzy membership function for the complement of a fuzzy set are two different concepts.

V. REFERENCES

[1] Khattab M. Alheeti, "Intrusion Detection System and Artificial Intelligent".

[2] W. Lu & I. Traore, (2004) "Detecting New Forms of Network Intrusion Using Genetic Programming", Computational Intelligence, vol. 20, pp. 3, Blackwell Publishing, Malden, pp. 475-494

[3] J.T. Yao S.L. Zhao L. V. Saxton, "A study on fuzzy intrusion detection"

[4] Watching the Watchers: Intrusion Detection by Greg Shipley http://www.networkcomputing.com/1122/1122f3.html

[5] IJCSMC, Vol. 3, Issue. 2, February 2014, pg.700 – 703"Areview of intrusion detection system on computer network

[6] Vikas Markam, Lect. Shirish Mohan Dubey, "General Study of Associations rule mining in Intrusion Detection System", International Journal of Emerging Technology and Advanced Engineering, Volume 2, Issue 1, January 2012.

[7] Yogendra Kumar Jain and Upendra, "An Efficient Intrusion Detection based on Decision Tree Classifier Using Feature Reduction", International Journal of Scientific and Research Publication, Vol. 2 No. 1, pp:1-6, 2012.

[8] Parekh S.P., Madan B.S. And Tugnayat R.M, "Approach For Intrusion Detection System Using Data Mining", Journal of Data Mining and Knowledge Discovery, Vol. 3, No. 2, pp: 83-87, 2012.