Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 2, February 2014, pg.700 – 703

REVIEW ARTICLE

A Review of Intrusion Detection System in Computer Network

Abhilasha A Sayar[1], Sunil. N. Pawar[2], Vrushali Mane[3]

[1]Electronics Dept. & BAMU, India
[2]Electronics Dept. & BAMU, India
[3]Electronics Dept. & BAMU, India
[1] abhitina29@gmail.com, [2] sunil.n.pawar@gmail.com, [3] vrushali.mane18@gmail.com

Abstract— Internet is a global network used all over by various companies, institutions, and government sectors. With the growth of internet world is coming close to an individual but at same time there is a threat of being robed. Connecting to internet can be both advantageous and disadvantageous in a sense that internet can provide as much comfort to business and also tremendous risk to end users. Increase in the speed of information data flow and also development in communication network along with many factors there is possibility of number of attacks on computer system. In order to protect computer system from these attacks and malicious activities intrusion detection system came into picture. This paper provides us overview of intrusion detection system and various techniques used to implement intrusion detection system.

Keywords— Intrusion detection system, artificial intelligence, fuzzy logic, neural network

I. INTRODUCTION

We human beings care about lot many things. It is basic nature to protect our valuable things whether they might be living or nonliving from getting damaged, or any kind of breakage. For this we put these valuable things either in safe box or provide some lock system. Similarly we also care for our personal documents, files, software present in computers from being pirated. For protecting such important files, documents and monitoring malicious action over computer network we need intrusion detection system.

The Information Assurance Technology Analysis Centre (IATAC) provides the Department of Defence (DoD) means to secure computer network and communication system. Their mission is to provide information on emerging technologies in information assurance (IA) and cyber security. With wide expansion of LAN and WAN network based technology many applications have emerged in field of business, healthcare services, financial organizations, online shopping, and internet banking that made us more dependent on computer networks. However due to open access to internet, security of computer systems data is at risk. Computer attacks are day by day increasing, detecting these attacks and securing computer systems has become priority of many researchers. This paper brings various intrusion detection techniques used to keep safe computer environment.

II. INTRUSION DETECTION SYSTEM

An intrusion can be defined as ‘‘an act of a person of proxy attempting to break into or Misuse a system in violation of an established policy’’. And intrusion detection system is a system use to detect intrusion. IDS can be a software and/or hardware System for monitoring and detecting data traffic or might be user behaviour to identify attempts of illegitimate accessing system manipulation through a network by malware and/or intruders. [1]

Intrusion detection working group (IDWG) defined a general IDS architecture based on the consideration of four types of functional modules (Fig. 1):

- E blocks (‘‘Event-boxes’’): This kind of block is composed of sensor elements that monitor the target system, thus acquiring information events to be analyzed by other blocks.
- D blocks (‘‘Database-boxes’’): These are elements intended to store information from E blocks for subsequent processing by A and R boxes.
- A blocks (‘‘Analysis-boxes’’): Processing modules for analyzing events and detecting potential hostile behavior, so that some kind of alarm will be generated if necessary
- R blocks (‘‘Response-boxes’’): The main function of this type of block is the execution, if any intrusion occurs, of a response to thwart the detected menace. [2]

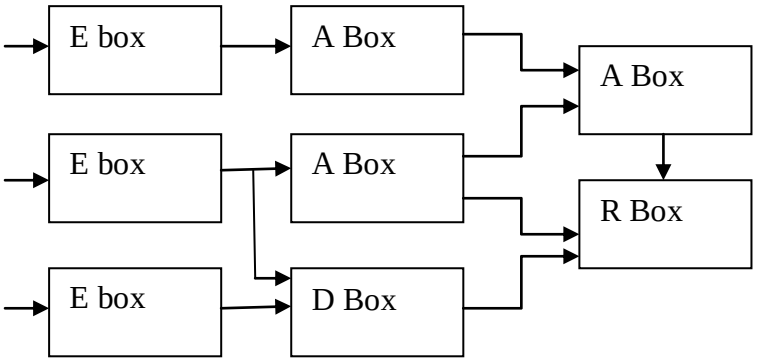
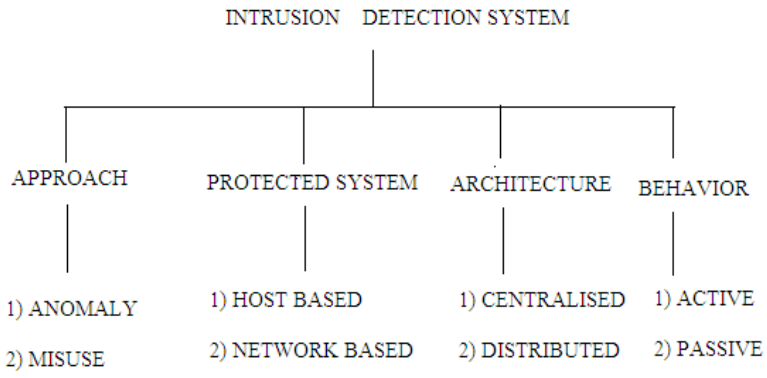


Fig 1 CIDF architecture for IDS

In other words intrusion detection system is made up of three components namely, information source, an analysis engine and a decision maker. Information source gives us information about system calls and system logs, whereas analysis engine provides approach to detect intrusion. There are mainly two types of approach misuse and anomaly. Last decision maker does the main job of applying rules as how to react based on analysis made by analysis engine. [3]

III. CLASSIFICATION OF INTRUSION DETECTION SYSTEM

Intrusion detection system can be classified in various ways. This classification is based on data source, behaviour, 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 and weakness. [5]
- 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 of NIDS and HIDS. [1][5][6][7]
- IDS can also distribute or centralized. In distributed IDS numbers of IDS are present on the network where they communicate with each other or to a centrally located sever. Whereas IDS can also be a standalone system.[1][4]
- Behavior based IDS are either active or passive. Active IDS detects and also prevents intrusion. On opposite side passive IDS only detect intrusions. Hence active IDS is also known as IDPS.

IV. **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 system. It can be an algorithm or hardware. [9]

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 and classification i.e. by extracting rules from large store of data.

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, viruses' similar systems are built to distinguish what is normal and what is abnormal. [4]

Bayesian approach uses pre and post probabilities of network attacks. By going back it finds out the cause of attack. Though this method gives the cause but at the same time it requires assumption and huge resource of data. [8]

All these methods are either implemented individually or in a combination of two or three. Implementation of these methods depends on feature space and processing time and other parameters.

- **Agent based IDS** consist of sensors located on either individual processor or on distributed system. There are two way to implement agent based IDS. In one way multi agent are used and in other mobile agent. Advantage of this method is that it detects intrusion using only required data.
- One of the **software approach** used to implement IDS is state transition analysis. Here intrusion undergoes different states. There are two states in which number of transaction takes place, these states are initial state that corresponds to the state before attack is done on system and the other state is compromised state that corresponds to the state in which the system bears attack. [11]

V. CONCLUSIONS

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.

REFERENCES

1. Khattab M. Alheeti, "Intrusion Detection System and Artificial Intelligent".
2. P. Garcı´a-Teodoro, J. Dı´az-Verdejo, G. Macia´-Ferna´ndez, E. Va´zquez, "Anomaly-based network intrusion detection: Techniques, systems and challenges".
3. J.T. Yao S.L. Zhao L. V. Saxton, "A study on fuzzy intrusion detection".
4. Bharanidharan Shanmugam and Norbik Bashah Idris, "Hybrid Intrusion Detection Systems (HIDS) using Fuzzy Logic".
5. Shaik Akbar, Dr.K.Nageswara Rao, Dr.J.A.Chandulal, "Intrusion Detection System Methodologies Based on Data Analysis". International Journal of Computer Applications (0975 – 8887) Volume 5– No.2, August 2010.
6. Marion Bogdanov, "An Approach to Developing An Information Assurance Environment".
7. Pablo Barron, Miroslav Horsky, Jonas Persson, "Intrusion Detection Systems an introduction".
8. 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.
9. Mehdi MORADI, Mohammad ZULKERNINE, "A Neural Network Based System for Intrusion Detection and Classification of Attacks".
10. Theodoros Lappas, Konstantinos Pelechrinis, "Data Mining Techniques for (Network) Intrusion Detection Systems".
Sriram Sundar Rajan, Vijaya Krishna Cherukuri, "An Overview of Intrusion Detection Systems.

