ISSN 2047-3338

An Overview of Intrusion Detection System (IDS) along with its Commonly Used Techniques and Classifications

Hussain Ahmad Madni Uppal[1], Memoona Javed[2] and M.J. Arshad[3]
[1,2,3]Department of Computer Science and Engineering, UET, Lahore, Pakistan
[1]madni_uppal@hotmail.com, [2]memoona.javed@yahoo.com

***Abstract*– The area of intrusion detection is the central concept in overall network and computer security architecture. It is an important technology in business sector as well as in research area. By monitoring the computer and network resources, Intrusion Detection System (IDS) detects any of the misuse or unauthorized access which is basically an attack to these resources. Then it alerts and informs administrator for occurrence of an intrusion. Several methods can be used to detect an intrusion. In this paper, we have discussed the introduction of intrusion detection system, its types and then different techniques that are commonly used. This paper will be helpful for the new researchers who want to know the basic knowledge of intrusion detection systems. It will help them to understand what intrusion detection is and what are the techniques commonly used for it.**

***Index Terms*– Intrusion Detection System, Security, Resources and Techniques**

I. INTRODUCTION

A) What is Intrusion Detection?

The process of examining the events [1], [3]-[5] occurred in a computer system or network resources, then analyzing them for the indications of intrusion and probable incidents that can cause threats to security measures, is called Intrusion Detection. Intrusions are usually caused by intruders/attackers, who want unauthorized and additional privileges to particular system or network for their own purposes [1].

B) What is an Intrusion Detection System?

Intrusion Detection System (IDS) is defined as the software or hardware product, [1] which focuses and identifies probable incidents caused by attackers, monitors information about those intrusions, tries to terminate them, and produces a report for security administrators [2] in real-time environment. So, Intrusion Detection System can be considered as a security operation that complements protection, e.g., firewalls [7]. It also helps to provide security and prevention against various intrusions caused by the attackers.

This is the brief introduction of intrusion detection systems. In section II, we discussed the background of intrusion detection systems. Section III is the literature survey; in which functions, approaches and classifications of IDS are discussed. In section IV, we discussed different techniques used for intrusion detection. Some of the issues and challenges are discussed briefly in section V and conclusion is given in section VI.

II. BACKGROUND

For about two decades, intrusion detection has been an effective field of research [9]. In 1980, James Anderson published a paper, "Computer Security Threat Monitoring and surveillance", which was one of the earliest papers in the field [7], [9]. Between 1983 and 1986, Dorothy Denning and Peter Neumann began working on government project related to IDS development; they researched and developed the first model of real-time IDS [7], [10], [14]. The prototype was named the "Intrusion Detection Expert System (IDES)" [14].

In 1980s, some attacks on the internet sites were done by experienced intruders. They used automated tools and exploit scripts for the attacks. But nowadays, anyone can intrude by the use of such tools [9]. From 2006 to 2010, number of cyber incidents has increased from 5000 to 35000 as shown in Fig. 1; so there is a dire need to deploy IDS in network security model [7].

III. LITERATURE SURVEY

A) Functions of intrusion Detection

Functions of intrusion detection are:

- Observe and Monitor: Used to observe and monitor user, network and system activities for any suspicious events [7], [19].
- Recognize patterns: Has ability to recognize patterns of attacks [7].
- Reports on Intrusions: Prepare a detailed report on the captured events. Then System Administrators use these reports to analyze abnormal activity patterns, system configurations and the security setup to determine vulnerabilities [7], [19].

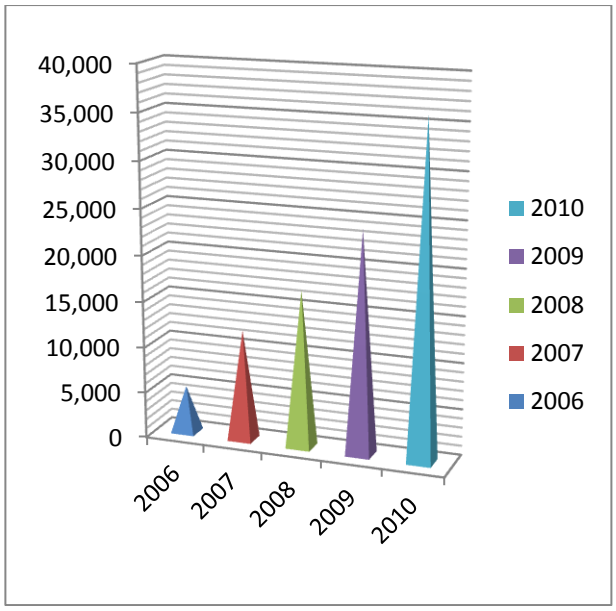

Fig. 1: Number of Cyber incidents reported to US-Cert [7]

- Track user policy violation: Used to track user policy violations, assess system and file integrity [7].
- Logging of Events: On encountering a suspicious activity, the IDS records the information related to the observed activity [7], [19], [20].
- Alerting System Administrators: IDS send alerts to the System Administrator via web pages, emails, messages etc, when any suspicious event takes place onto a database [19], [20].

B) Importance of Intrusion Detection System (IDS)

Intrusion Detection System is important to implement in an organization for the following reasons [19], [21], [22]:

- Behaves as an extra layer of protection and provides other security mechanisms.
- Detects intrusions and other suspicious events.
- Detects an attack in its initial stages when the attacker just starts to scan a port to determine vulnerable ports.
- Prepares reports about the detected activities for system administrator.
- An easy technique for analyzing the security measures.

C) Approaches of Intrusion Detection System

Approaches of intrusion detection system are:

i. Misuse Detection
ii. Anomaly Detection

1) Misuse Detection

Misuse detection is also called *signature-based* or *rule-based* detection [10], [11]. In this detection approach, user's activities are compared with the attackers' known behaviors, to penetrate a system or network [12]. In misuse detection, gathered information is analyzed and compared with large databases for attack signatures [13].

Advantage: Misuse or signature-based detection is useful, because its detection rate is high and false alarm rate is low for known attacks [7], [10].

2) Anomaly Detection

In anomaly detection approach, activities that are varied from already established patterns for users or groups of users are identified [12]. In this approach, profiles may be established for normal behavior of users, which comes from the statistics of data of users. When detection is performed, profile is compared with the actual users' data. If the threshold value is above or greater than the offset, the user's behavior is considered normal, and it is considered that he has no intention of attack. While, if the threshold value is less than the offset, user's behavior is considered abnormal and attack can occur [10]. It means that it builds a baseline of what is *normal*. Normal behavior of network should be known before its implementation [7].

Advantage: Anomaly detection can detect unknown attacks easily, but its misjudgment rate is high [10]. It can also detect previous unknown threats [7].

D) Classification of Intrusion Detection Systems

Intrusion detection systems are classified as:

i. Network-based IDS
ii. Host-based IDS
iii. Hybrid based IDS

1) Network-based IDS (NIDS)

Network-based IDS are standalone hardware appliances which include network intrusion detection capabilities [13]. They are mostly deployed on strategic point in network infrastructure [7] such as at a boundary between networks, virtual private network servers, remote access servers, and wireless networks [15]. NIDS monitors network traffic going through particular network segments or devices [15]. It can capture and analyze data to detect known attacks or illegal activities or analyze network and application protocol activity to identify anomalous and suspicious activity by traffic scanning [7], [15]. NIDS can also be referred as "packet-sniffers", because it captures and collect the data in the form of internet packets passing through communication mediums [7], [10].

2) Host-based IDS (HIDS)

In Host-Based IDS, the characteristics of a single host are monitored and the events of that host are observed for any malicious activity. They can monitor network traffic, logs, processes, operations performed by applications, file access and modification, and any configuration change in system [10], [13], [15]. The deployment of HIDS is usually done on critical hosts. Critical host includes servers or systems that are publicly accessible and have some sensitive information [15]. They are placed on one server or workstation, where data is collected from different resources and machine analyze the data locally [7].

3) Hybrid based IDS

In Hybrid based IDS, both host-based and network-based IDSs are used simultaneously [7], [15].

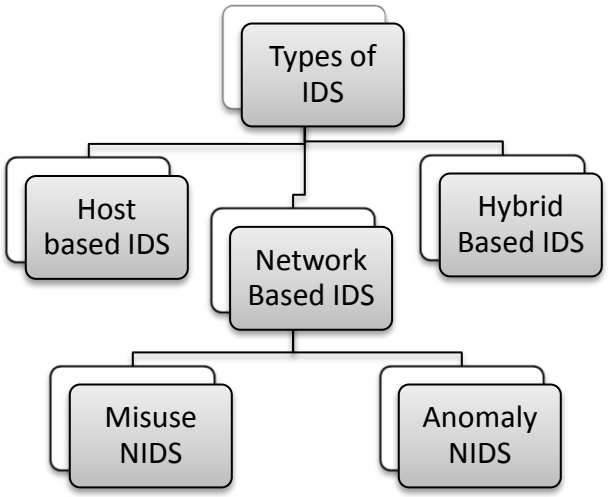

Fig. 2: Classification of IDS [19]

Fig. 2 shows that how intrusion detection system is classified. While Figure 3 shows the implementation of the types of IDS.

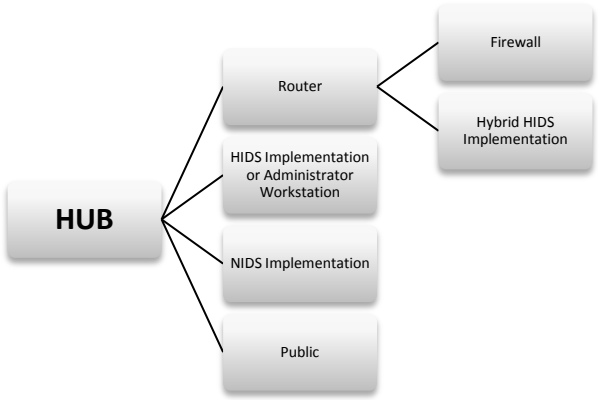

Fig. 3: Types of IDS [23]

IV. INTRUSION DETECTION TECHNIQUES

Here, we will briefly discuss the most common techniques used to detect intrusions:

Artificial Neural Networks (ANNs)

Artificial neural networks provide flexible pattern recognition capabilities. In ANNs, special kind of training is given to the system so that it can recognize various arbitrary patterns that are provided to it as input data. When system fully recognizes these patterns it is then asked to match these patterns with the output produced. By matching various input and output arbitrary patterns, it is detected that intrusion has occurred or not [6], [15].

State Transition Tables

In State Transition Table, sequence of actions performed by an intruder is described in the form of a state transition diagram and behavior of the system is observed. When it matches with identifiable compromised state and penetrated sate, an intrusion is detected [8], [15].

Genetic Algorithms (GAs)

The function of Genetic Algorithms (GAs) is to imitate or mimic the natural reproduction system in nature. After undergoing recombination and various random changes, only the fittest individual will be reproduced in subsequent generations. In 1995, the application of GAs appeared in IDS research. It involves evolving a signature that indicates intrusion [15], [16]. *Learning Classifier System (LCS)* is the related technique, in which binary rules that recognize intrusion patterns are evolved [15].

Bayesian Network

In Bayesian Network, graphical models have been introduced. These graphical models are defined by a set of transition rules, represented as probabilistic interdependencies. In this model, a conditional probability table and the state of random variables are described in each node. A conditional probability table determines the probabilities of the node in a state, given a state of its parent [15], [17]. This approach can handle incomplete data [15].

Fuzzy Logic

Fuzzy Logic is designed to handle vague and imprecise data. To indicate an intrusion, a relationship between input and output variables is defined by creating different set of rules. It uses membership functions to examine the intensity of truthfulness [15], [18].

All the above techniques are further summarized in Table 1.

Table 1: Techniques of IDS

Techniques	**Functions**
Artificial Neural Networks (ANNs)	System is trained by inserting related input/output data. This training is used afterwards to recognize arbitrary patterns, given as an input to the system.
State Transition Tables	Intrusion occurs or not is detected by comparing the behavior of the system with intruder's state transition diagram.
Genetic Algorithms (GAs)	Mimic the natural reproduction system in nature where after certain changes, only the fittest individuals in a generation will be reproduced in subsequent generations.
Bayesian Network	Graphical models are introduced and deal with incomplete data.
Fuzzy Logic	Handles vagueness and imprecision.

V. ISSUES AND CHALLENGES

In spite of all these techniques of intrusion detection, security problems cannot be solved completely. Intruders can access the computer and network resources very cleverly using some efficient techniques. So there is a dire need to work on intrusion detection systems to make them more efficient so that they can not only alert the administrator about the attack but also have the capability to detect the type of attack. Using intrusion detection with firewall, anti viruses and with other security technologies, intrusions can be avoided [9], [24].

VI. CONCLUSION

In this research paper, we have discussed that an intrusion detection system is the important part of the defensive system of computer and network resources. This system detects attacks and intrusions more accurately than any other security system and raises fewer false positive alarms. As it is an important security measure, so it becomes the need for organizations to implement this to detect the attacks and other malicious activities at preliminary stage.

REFERENCES

[1]. Mell, Peter; Bace, Rebecca, "NIST Special Publication on Intrusion Detection Systems", Standard Form 298 (Rev. 2-89) Prescribed by ANSI Std. Z39-18 298-102.

[2]. B. Abdullah, I. Abd-alghafar, Gouda I. Salama & A. Abd-alhafez, (2009) "Performance Evaluation of a Genetic Algorithm Based Approach to Network Intrusion Detection System", 13th International Conference on Aerospace Sciences and Aviation Technology (ASAT), May 26-28.

[3]. J. Gomez & D. Dasgupta, (2002) "Evolving Fuzzy Classifiers for Intrusion Detection", IEEE Proceedings of the IEEE Workshop on Information Assurance, United States Military Academy, West Point, NY.

[4]. R. H. Gong, M. Zulkernine & P. Abolmaesumi, (2005) "A Software Implementation of a Genetic Algorithm Based Approach to Network Intrusion Detection", Proceedings of the 6th International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing.

[5]. T. Xia, G. Qu, S. Hariri & M. Yousif, (2005) "An Efficient Network Intrusion Detection Method Based on Information Theory and Genetic Algorithm", Proceedings of the 24th IEEE International Performance Computing and Communications Conference, Phoenix, AZ, USA.

[6]. A. S. Mohammad and Z. Mohammad, "Efficacy of Hidden Markov Models over Neural Networks in Anomaly Intrusion Detection," 30th Annual International Computer Software and Applications Conference, Chicago, 2006, pp. 325-332.

[7]. Asmaa Shaker Ashoor (Department computer science, Pune University) Prof. Sharad Gore (Head department statistic, Pune University)," Importance of Intrusion Detection System (IDS)", International Journal of Scientific & Engineering Research, Vol. 2, Issue 1, Jan 2011.

[8]. K. Ilgun, R. A. Kemmerer and P. A. Porras, "State Transition Analysis: A Rule-based Intrusion Detection Approach," IEEE Transactions on Software Engineering, Vol. 21, No. 3, March 1995, pp. 181-199. doi: 10.1109/32.372146

[9]. John McHugh, Alan Christie, and Julia Allen (Software Engineering Institute, CERT Coordination Center), "The Role of Intrusion Detection Systems", IEEE Software September/October 2000.

[10]. Alireza Osareh, Bita Shadgar (Computer Science Department, Faculty of Engineering, Shahid Chamran University, Ahvaz, Iran), "Intrusion Detection in Computer Networks based on Machine Learning Algorithms", IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.11, November 2008.

[11]. A. Abraham, R. Jain and J. Thomas, "D-SCIDS: Distributed soft computing intrusion detection system," Journal of Network and Computer Applications, vol. 30, pp. 81-98, 2007.

[12]. James Cannady, Jay Harrell," A Comparative Analysis of Current Intrusion Detection Technologies".

[13]. Vangie Beal," Intrusion Detection (IDS) and Prevention (IPS) Systems", posted 2005 [07-15-2005], last updated 2010[08-31-2010].

[14]. SANS Institute InfoSec Reading Room, "The History and Evolution of Intrusion Detection", http://www.sans.org/reading-room/whitepapers/detection/history-evolution-intrusion-detection-344.

[15]. Indraneel Mukhopadhyay, Mohuya Chakraborty, Satyajit Chakrabarti (Department of Information Technology, Institute of Engineering & Management, Kolkata, India)"A Comparative Study of Related Technologies of Intrusion Detection & Prevention Systems", Journal of Information Security, 2011, 2, 28-38 doi:10.4236/jis.2011.21003 Published Online January 2011 http://www.SciRP.org/journal/jis.

[16]. M. Crosbie and E. Spafford, "Applying Genetic Programming to Intrusion Detection," GECCO '96 Proceedings of the First Annual Conference on Genetic Programming 1996.

[17]. F. Jemili, M. Zaghdoud and M. B. Ahmed, "A Framework for an Adaptive Intrusion Detection System using Bayesian Network," IEEE Intelligence and Security Informatics, May 2007, pp. 66-70. doi:10.1109/ISI.2007. 379535.

[18]. A. El-Semary, J. Edmonds, J. Gonzalez and M. Papa, "A Framework for Hybrid Fuzzy Logic Intrusion Detection Systems," 14th IEEE International Conference on Fuzzy Systems, May 2005, pp. 325-330, 2005.

[19]. Ratna Deepika Kannan, Dr. Martin Reed, School of Computer and Electronic Engineering University of Essex, "An Experimental Study of detecting and correlating different Intrusions (Chapter#3)".

[20]. K. Scarfone and P. Bell, "Guide to Intrusion Detection and Prevention Systems (IDPS)", in National Institute of Standards and Technology (NIST), Feb. 2007.

[21]. M. Toprak, "Intrusion Detection SystemCorrelation With Operating System Level Logs", Graduate School of Engineering and Sciences, Izmir Institute of Technology, Dec. 2009.

[22]. R. Bace and P. Mell, "Intrusion detection systems", NIST Special Publication, 2001.

[23]. V. Jaiganesh et al., "Intrusion Detection Systems: A Survey and Analysis of Classification Techniques", International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 4, April 2013.

[24]. Deris Stiawan et al., "Characterizing Network Intrusion Prevention System", International Journal of Computer Applications (0975 – 8887), Vol. 14, No.1, January 2011.