ISSN: 0975-766X
CODEN: IJPTFI
Available Online through *Research Article*
www.ijptonline.com

A STUDY AND ANALYSIS ON INTRUSION DETECTION BASED (IDB) TECHNIQUES

V P Krishna Anne[1, #], Dr. K Rajasekhara Rao[2], V.VenkataKoundinya[#], T Gnana Krishna Deep[#]
[1]Research Scholar, Department of Computer Science & Engineering,SCSVMV University, Enathur, Tamil Nadu.
[#]Department of Computer Science & Engineering, K L University, Guntur, Andhra Pradesh, India.
[2]Professor,Department of CSE, Usha Rama College of Engineering & Technology, Telaprolu, Andhra Pradesh, India.
Email: praveenkrishnacsi@gmail.com

Received on: 28-01-2017 *Accepted on: 02-03-2017*

Abstract

Intrusion detection resembles suite of procedures which are implemented so that it can identify attacks against computers and network infrastructures. Automatic Network Invasion Detection is one among the foremost necessary analysis domains over the previous couple of decades. To develop more efficient and productive approaches, several other alternate techniques have been proposed for improvising the process of Intrusion Detection. Those motivation behind the reason commercial enterprises don't help the exchanging interruption identification strategies could be well unwritten by accept those working efficiencies these techniques. This analysis provides a wider perspective of the Intrusion Detection approaches and can help to understand as to what Intrusion Detection techniques are being employed by the network security experts and why are they being used**.**

Keywords- Intrusion Detection System, Network based Intrusion Detection Systems, Host based Intrusion Detection Systems, Signature Based Intrusion Detection System.

1. Introduction

Automatic network invasion detection is one in every of the foremost necessary analysis domains over the previous couple of decades. An Intrusion Detection System (IDS) [1]is an approach to identify malicious activities. IDS provides methodologies that target of characteristic suspicious activity in distinctive ways that an Intrusion Detection Framework can be implemented in two different forms which include Network based IDS, shortly it is termed as NIDS and Host based Intrusion Detection System, shortly it is termed as HIDS[1] intrusion detection systems. Intrusion Identification and avoidance frameworks principally concentrate on identifying imaginable incidents, logging data about them, and

reporting attempts of intrusion. Network Intrusion Detection Systems are most proficient methods for protection against network based attacks aimed for PC frameworks. Network Intrusion Detection Systems are placed at a vital position inside the system screen activity to and from all nodes on the system. An investigation is performed for a passing traffic activity on the whole subnet, lives up to expectations in an unrestrained mode, and matches the traffic movement on the subnets to the library of known attacks. An alert is sent to the administrator when the attack is recognized.

2. Theoretical Analysis

2.1 NIDS Definition

A Network Intrusion Detection System (NIDS) isan application mechanism employed so that it can facilitate the automatic detection of the intrusions over any specified network.

2.2 NIDS Architecture

The NIDS architecture consists of several phases which are used to develop a standardized model to detect the occurrence of intrusions and to initiate responses to the detection of a malicious activity.**(Figure 1)**

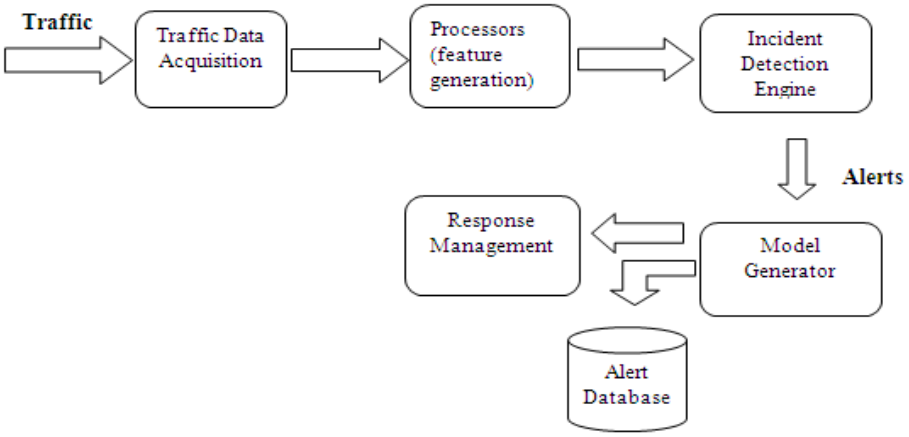

Figure 1: NIDS Architecture.

2.3 Functional Requirements of NIDS

Generally Intrusion Detection Systems consists of following parts

An Information Source: The information source provides in sequence about event records. That is whenever an event occurs the information regarding the event is handled by information source. This is also known as event generator.

An Analysis Engine: The information provided by the information source is analyzed and processed in the analysis engine where the behaviour of the intrusions is identified.

A Decision Maker: A choice maker applies some rules on the output made by the analysis engine and decides the specified action to be performed so as to mitigate the intrusion supported the outcomes of the analysis engine.

2.4 Functions of NIDS

The main functionalities of a Network Intrusion Detection System contain[2]:

Spotting attacks: NIDS should be able to detect different intrusions and possible security threats and attacks without any delay by monitoring the network continuously.

Offer information: After detecting the intrusion or attack proper data on the attack should be forwarded.

Corrective steps: If an attack is detected, different effective techniques should be implemented in order to take necessary actions to stop the intrusions.

Storage: The attack data should be stored for future usage.

2.5 Classification of Intrusion Detection Systems

The process of detecting an intrusion is classified into several categories as mentioned below[3]

Stack based Intrusion Detection System: Stack based mostly Intrusion Detection System[4] may be a recent technique. It integrates precisely with the TCP/IP, belongings packets to be seen as they navigate through the OSI layers. On seeing them to navigate permits the intrusion detection system to prevent the packet from the stack before the OS or application has probability to method the packets as has the situation of the packet at each it stage.

Network Based Intrusion Detection System (NIDS): Network based Intrusion Detection System[4] mostlyscreens the movement because it flows to different host. Screening standards are often augmented or weakened for a specific system within the network with comfort. Network based Intrusion Detection System[5] to be able to stand against large quantity of network traffic to stay effective and precise in functioning. As network traffic will increase exponentially, Network based mostly Intrusion Detection System scans whole movement and examines at specific intervals and examines in progress traffic, activities, transactions and behaviour so as to discover the prevalence of intrusions by detection Network. It works on the principle that attack behaviour differs enough from traditional user behaviour such it will be detected by cataloguing and distinguishing the variations concerned. The supervisor defines the baseline of traditional behaviour. Anomaly based mostly Intrusion Detection Systems area unit terribly liable to plenty of false positives and may cause serious process overhead on the pc system. **(Figure2)**

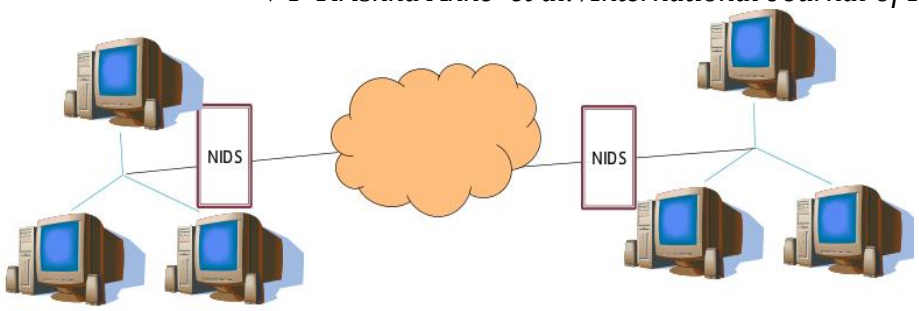

Figure 2: NIDS Architecture.

Host Based Intrusion Detection System (HIDS): Host Based Intrusion Detection System keeps record of the movement that originate or is projected to originate on a particular host. It controls privileged access to host so that it can screen definite constituents of a host which are not freely reachable for other hosts. Host Based Intrusion Detection System has partial outlook to the topology of entire network. It could not able to sense attack which can be directed to a particular system of the network which did not install the Host Based Intrusion. **(Figure 3)**

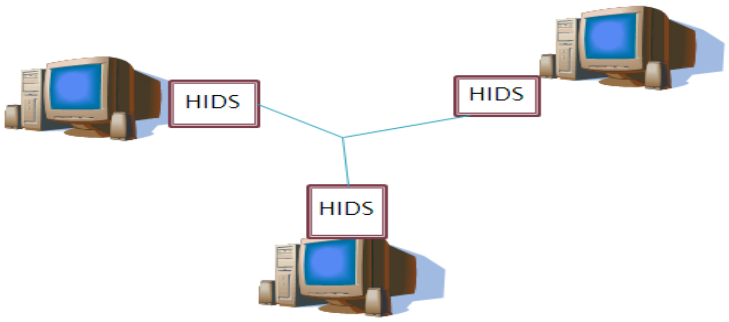

Figure 3: HIDS Architecture.

Signature Based Intrusion Detection System (**SBIDS**): It identifies intrusion by observing events and documented attacks for patterns and formulates a rule set based on the patterns. A big data base is associated with it. These databases store the signatures. Only the attacks known to its database[5] will be detected. New attacks could slide through if the database is not updated regularly. SBIDS affect the performance when several attack signatures match the intrusion pattern. There would possibly be a clear performance lag in such cases. The definitions of signatures stored in the database should be unambiguous by which the alternates of identified attacks will not be overlooked. A chunk of space can be wasted because huge databases need to be built. The intrusion detection systems can also be classified into following types on the basis of nature of action performed once an attack is detected.

Passive Intrusion Detection System: In this type of system a possible breach in the security is detected by the sensors. The breach is logged or recorded and an alert is sent to the administrator.

Reactive Intrusion Detection System: In this type of system a suspicious activity is recognized. The intrusion prevention system responds automatically by reprogramming the firewall to dam network traffic from the suspected malicious supply. The Reactive Intrusion Detection System is additionally referred to as intrusion hindrance system. The Reactive Intrusion Detection System is commonly used where both detection and prevention of an intrusion can occur involuntarily or at the order of an administrator.

2.6 NIDS and Firewalls

In spite of the fact that both NIDS and firewalls are associated with system protection, an Intrusion Detection System (IDS) contrasts from a firewall. A firewall finds external attacks or intrusions to avoid them from attacking the system. Intrusion can be prevented from occurring; the firewalls limit the admission between networks and do not flag an attack from within the system.

On the other hand an Intrusion Detection System assesses an alleged intrusion once it has occurred and gives a caution. An Intrusion Detection System additionally looks for attacks that start from inside a framework. This is mostly completed by inspecting system interchanges, distinguishing heuristics and patterns (regularly known as marks) of basic PC attacks, and making a move to alert administrators. A framework that terminates connections is called an intrusion prevention system, and is another type of an application layer firewall.

2.7. Evasion Techniques

Attackers use a number of techniques to overcome the intrusion detection systems, the subsequent are considered as the techniques which are used to elude IDS and intrude into the network:

Fragmentation: The attacker will surpass the recognition systems capability for detecting the assault signature by sending fragmented packets.

Avoiding Defaults: The port that is being used by any protocol may not always warn the protocol being implemented over the network even if there is a chance of intrusion.

Coordinated and Low-Bandwidth Attacks: Coordinating attacks are very difficult to be traced as they are coordinated among several attackers which make the administrator difficult to trace out the occurrence of intrusion.

Address Spoofing: Attackers can mask their identity by using proxy servers which makes it difficult for the network administers to actually identify the attack's source.

Pattern Change Evasion: Mostly IDS usually practices pattern similar mechanisms for detecting an occurrence of an attack. If any negligible changes are done to the script used in the attack, the IDS may not detect the intrusion as it would not match with the pattern and it may be possible to evade detection.

3. Pros and Cons of NIDS

3.1Advantages of NIDS

The major advantages of NIDS are:

- **Ease of distribution**: The Intrusion Detection systems are simple to set up and do not change the existing infrastructure of the system.
- **Small charge**: The execution and preservation of the Intrusion Detection systems is simple and is economic as it need not be deployed on every system in the network.
- **Noticing assaults**: The IDS can detect and report the occurrence of the intrusion and various techniques are implemented to improve its efficiency.
- **Hold proof**: Also these systems maintain the proof of the occurrence of attack making it difficult for the attacker.

3.2 Disadvantages of NIDS

- These systems collect enormous cautions in a day, which may overload your effort.
- The alerts can also be very high in some situations, which reduce the confidence on occurred alerts.
- If rate is cut down in order avoid false alerts, and then this can compromise NIDS reliability.
- The false alarm makes users interaction more and automatic principles disappear.

4. Unsolved for open issues

4.1 High level of human interface

Present methodologies still require ahigh level of claiming human communication throughout the model development transform. Comparative is the situation for P-BEST, for which those composing of a set of suggestion guidelines might request a respectable mankind's exertion. On the other hand, majority of the present methodologies expecting an naturally generating system movement models still requirement a large amount about mankind's pre-processing of the data information. Indeed going unsupervised approaches requires data information remains under exactly particular distribution, circumstances that might just make surety by mankind's masters. This require for mankind’s pre-processing

will be maybe a standout amongst those significant drawbacks in the sending for the individuals methodologies expecting a naturally generating movement models. The interruption identification Group will respond should this issue giving work to those alleged mixture methodologies. Mixture methodologies normally consolidate well-established NIDS such as grunt with naturally created movement models strategies. Such combinations make the sending from claiming naturally created models systems. To addition, they appear should assistance lessen the required human pre-processing.

4.2Lack of replica adjustment information

The majority of the examined methodologies utilizing programmed movement models appear to be with a chance to be mindful of the secondary system, which give routines for adapting themselves as required. However, that suitable duration of the time to performing such alterations appears to be not to a chance to be broke down sufficient. Methodologies have the ability to exchange their movements about under data that permit those system security staff with effectively assess their conceivable course of movements for further framework change.

4.3 Lack of resources consumption information

Determining the proper usage frequency for a given detection approach is crucial for analyzing its potential deployment on real networks. However, despite being a subject always present in surveys on intrusion detection, it is still difficult to establish the true usage frequency for many of the proposed approaches.

The problem is that only a few of the previously discussed intrusion detection approaches have analyzed the performance in terms of the computational resources required for generating the model as well as for evaluating a set of new network traffic records. As a result, it is difficult to establish the proper usage frequency of those approaches performing batch and real-time detection. This lack of resource consumption information could be one of the reasons why (with the exception of signature-based approaches) none of these approaches have been successfully deployed on real networks. Consequently, a better analysis about the needed computational resources could help in establishing the adequate usage frequency and therefore facilitating the deployment on real networks.

4.4Need of community network traffic data

Finally, in turn noteworthy issue viewing interruption identification may be that absence of proper open information sets to assessing the distinctive methodologies. Nowadays, a large portion regularly utilized information sets utilized for

assessment need considerable length of time, which aggravate them practically outdated. Assuming that we think about the quick advancement of the system security field present information sets is programmed to strike, Peer-to-Peer movement. However, in a lot of people cases, the investigate group proceeds assessing its interruption identification methodologies utilizing their information without giving work to data around information situated era. Circumstances that genuinely influence that standard of reliability from claiming analyses required for experimental exploration.

5. Conclusion

Network Intrusion Detection is one of the most concerned areas that needed to be taken care of while running an organization. Without proper NIDS, all the assets of the organization tend to be vulnerable. Many different approaches are being planned during the last few years in the domain of Intrusion Detection and Prevention. Different techniques have evolved based on different network phenomenon.This paper would provide a brief insight into the evolution of concept of intrusion detection, whichis addressed as interruptions. In this paper we discussed the functionalities of few Intrusion Detection approaches and also studied why or why not these technologies are being employed in today's network security practices.

References

1. Carlos A. Catania, Carlos Garcia Grain, "Automatic Network Intrusion Detection: Current Techniques and Open Issues", Computers and Electrical Engineering, 2012 Elsevier, pp.1062–1072.
2. V P Krishna Anne,et al, "Data Mining Techniques for Intrusion Detection", International Journal of Systems and Technologies, vol 3,issue1,2010, pp.75-83.
3. Siva Bala Vinod Puppala, et al, "Secure Storage Services in Multi-Cloud Environment", International Journal of Applied Engineering Research (IJAER), vol.9, issue 18, 2014, pp.4869-4876.
4. D. K. Mishra, et.al, "Knowledge Discovery and Retrieval on World Wide Web Using Web Structure Mining," 4th Asia International Conference on Mathematical/Analytical Modelling and Computer Simulation, Kota Kinabalu, Malaysia, 2010, pp. 532-537.
5. J. V. Rao, et al, "Enforcing the security within mobile devices using clouds and its infrastructure," CSI 6th International Conference on Software Engineering (CONSEG), Indore, 2012, pp. 1-4.

6. Chen C, Mabu S, Yue C, Shimada K, Hirasawa K, "Analysis Of Fuzzy Class Association Rule Mining Based on Genetic Network Programming", In: ICCAS-SICE, 2009,pp. 3480–3484.
7. Lazarevic A, Kumar V, Srivastava J, "Intrusion Detection: A Survey In Managing Cyber Threats", Massive Computing, vol. 5, US Springer, 2005, pp.19–78.
8. Mukherjee B, Heberlein L, Levitt K, "Network Intrusion Detection" Network IEEE 1994,pp.26–41.
9. Liu G, Yi Z, Yang S, "A Hierarchical Intrusion Detection Model Based on Neural Networks", Neuron Computing 2007, pp.1561–1568.