IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol.-7, Issue-4, April 2019 E-ISSN: 2347-2693

Taxonomy of Intrusion Detection System –A Study

P. Kaliraj[1*], B. Subramani[2]

[1]Department of Computer Science, Kongunadu Arts and Science College, Coimbatore, India
[2]Department of Computer Science, SNMV College of Arts and Science, Coimbatore, India

Corresponding Author: pkalirajmsc@gmail.com

DOI: https://doi.org/10.26438/ijcse/v7i4.320324 | Available online at: www.ijcseonline.org

Accepted: 07/Apr/2019, Published: 30/Apr/2019

***Abstract*-**An intrusion detection system is a computer system monitors network traffic for suspicious activity, now, Computer Network is essential to give a high-level security to protect highly sensitive data and information. Network Technology and Internet related Application sector plays a essential role in today's trend. Many intrusion detection techniques, methods and algorithms help to detect these attacks, hackers use different types of attacks for getting the valuable information. Numbers of clients are being connected with the technology day by day. It's being done hacked by junction or evil intruder. A very effective tool in this is Intrusion Detection System , which detects the attacks and analysis it to take proper decision against it. Intrusion Detection System has a great impact on cyber security and network vulnerability. Once the detection is scored, the initialed can be taken by IDS. Intrusion detection system is a software and hardware device. This paper will notify us overview of IDS and to create a secure zone in the sector of networking. Numerous intrusion detection techniques, methods and algorithms assist to detect these attacks. Furthermore, appropriate problems and challenges in this field are consequently illustrated and discussed.

***Keywords*—** *Security, Intrusion detection, Network Attacks, Prevention System, Analyzer, Dos, Misuse detection, Anomaly detection.*

I. INTRODUCTION

All computer system is frequently at risk for unauthorized and interference, however, with sensitive and secret in sequence are at a high risk. IDS is a method in information security, which plays a most important role in detect various types of attacks and safeguard the network system. An Intrusion Detection System is the process of monitor and analyzing the events arising in a computer related network system to mark all security problems. NIDS supports the good number of deploy system. A Network Intrusion Detection System (NIDS) attempts to spot malicious activities such as Denial-Of-Service attacks, port scans and examine the network traffic attacks. However, they stay fully unsuccessful against those attacks that are so far unknown and these can be combated immediately once they are detect physically and a signature is produced for them [1]. Network security has received a broad attention due to the supporting security anxiety in networks.

A network-based Intrusion Detection System usually consists of a network application with a Network Interface Card (NIC). A many mixture of algorithms have been designed which can detect with security risks. With these proposal signatures based network intrusion detection system has been a commercial winner and have seen a extensive acceptance. The NIDS approaches classified into two types: Signature based system and Anomaly detection based system. These approaches increase the basis of several present intrusion detection techniques. Now approximately anybody can make use of the vulnerabilities, analyze data integrity, and more on a desktop system due to the wide accessibility of attack tools. The predictable method for securing desktop systems is to create security mechanisms, such as firewalls, verification mechanisms, 'Virtual Private Networks' (VPN) which form a protective "shield" around them.

The IDS has three functions : monitoring, detecting and generating an alert. IDS are often considered as the functionality of the firewall. A firewall must be measured as a boundary that protects the information flow and prevent intrusions where as IDS detect if the network system is under attack or if the security need by the firewall has been executed. Reciprocally firewall and IDS develop the security of the computer network. This is called intrusion detection and it is corresponding to predictable security mechanisms [2].

II. EFFICIENCY OF INTRUSION DETECTION SYSTEMS

The following uniqueness of intrusion detection systems has been recognized.

A. Prediction Performance

In IDS, easy performances are been calculated such as prediction accuracy is not sufficient. The capability to correctly recognize intrusions and the inability in identifying valid action as an intrusion results in viewing a good quality prediction performance. The predictive performance measures to evaluate IDs encompass detection rate and copied alarm rate. Generally, it is hard to calculate these two actions, as it is classically impossible to have universal data of all attacks [3]. Whereas detection rate and false alarm rate are regularly, different estimation of IDS is also executed using Receiver Operating Characteristics analysis.

B.Time Performance

The total time required for the IDS to detect an intrusion refers to the time performance of IDS. The propagation time and the processing time are also joined in this. The propagation time is the time essential to processing data to propagate to the security analyst [4]. The minimum rate of these two times permit the security analysis sufficient time for react towards an attack and to end an attacker from shifting audit data the IDS before causing much damage.

C. Fault Tolerance

An IDS must be able to provide a secure service and recover quickly from successful attacks and it must be reliable, strong and resistant to attacks. This case is very common in large DOS attacks, deliberate attacks and buffer overflow attacks which can fall down the computer network system, in turn the IDS and can shut down too. This feature plays an vital role in suitable functioning of IDS. The IDS should be alert in prevent huge number of false or confusing alarms that are caused by adversary [5].

III. INTRUSION DETECTION SYSTEM TECHNIQUES

The many different methods used to completing the preferable elements of IDS are:

A. Misuse Detection

The Misuse Detection is derived from general information of well-known attacks with mistake in a system given by the computer professional. Uses of the misuse detection are to detect the hackers that they try to execute the attacks as well as to utilize the predictable flaws of the data. It is exact and accurate in identifying recognized attacks; it cannot spot the unidentified attacks with increasing computer-generate threats to the data [6]. It is the frequent method implemented in IDS in recent days. The disadvantage is that it will spot only the identified attack.

i) Signature Based IDS

Signature based IDS uses a set of rules and regulations to recognize intrusion by inspection for model of events exactly to identified and recognized attacks.

ii) String Signatures

String signature seeks a sequence of ASCII symbols, which denote a possible attack. An example, of string signature is "cat + +" > /. rhosts" for UNIX which, carry out might cause the system turn out to be exceptionally vulnerable to set of connection attacks.

iii) Port Signatures

Port signatures often utilized for the link setup, which tries to familiar, and frequently attacked ports.

iv) Header Signatures

Header signatures examine for unsafe or illegal mixture within packet header fields. The prominent instance of packet's port field is vital pointer, Network BIOS port as well as the Out Of Band data pointer is set [7].

B. Anomaly Based

Anomaly based watches over the network congestion and contrasts it also the well-known baseline of the usual congestion profile. A key characteristics for the set of connections is basically the common bandwidth consumption for regular protocols utilized to evaluate the group of port numbers, devices, which aware the supervisor or client abnormal congestion be, noticed which to be much differed from the baseline of "normal" behavior and "anomaly".

Some Examples of Anomaly based:

1. A client turns on and off a system 30 occasions within a day as an alternative of the usual way of 2 to 4 occasions a day.
2. A computer is being used by the user around 3:00 AM, which is not of the business hours.

In designing the system deals by the accessibility of a collection of connected sets, which will be the usual type of congestion [8]. logically, the guessing which stays alive from attack-free set of information's for guidance, a detector external is used to fake the set of information's which will not give an accurate guessing. Standard set of connected systems congestion has a massive amount of scans, DOS attacks, backscatter and worm action. If it is not alert, this activity will turn out to be a part of usual state for an anomaly detector.

IV. TYPES OF INTRUSION DETECTION SYSTEM

A. Host Based IDS

Host based IDS, which is capable of working with high quality data; Host Based IDS deal with takes place on a

single server system. The information is gather from a single server system. The conclusion should depend on the guideline, which is established on the local system. These types of host-based IDS process are examine as passive component [9].

i) System Commands

Host based IDS employs functional source of information such as system commands for detect malicious user.Logged system controls examples within ps are UNIX, pstat, vmstat, get limit. The information given by these controls are about different events is extremely accurate and useful. The preprocessing of review information that is collected as informal data, which is needed before analysis.

ii) System Accounting

OS such as both 'Windows' and 'UNIX' have the availability of system accounting. There are no possible numbers of intrusion detection methods in spite of increasing attention for system accounting in windows circumstances. The common use of system accounting UNIX environment is used to gather information on system actions, which comprises of utilization of mutual assets by user of the system [10].

B. Network Intrusion Detection Systems

Network Intrusion Detection System checks whether there is any intruders in the incoming and outgoing network. NIDS are placed in the network hubs and taps. One of the disadvantages of NIDS is that it slows down the computer network speed.

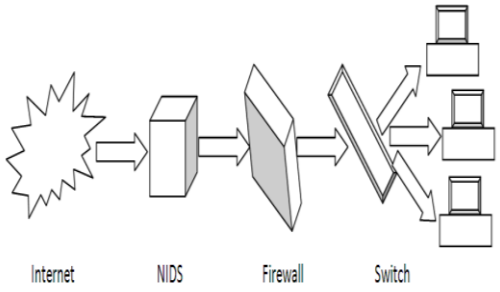

Figure 1: Network Based IDS [11]

The figure 1 illustrates that computer Network intrusion is been monitored by Network Intrusion Detection System (NIDS) are located at the key network points like routers and switches. All the traffic exceeds through the NIDS. It observes the network traffic and monitor the packets whether it holds any malicious data.

C. Distributed Intrusion Detection Systems

Distributed Intrusion Detection System contain the numerous IDS with a huge network, which interacts with each other, or a single server that provides with the advanced network monitoring. The server takes the authority and makes it at risk to the attacks. DIDS collect audit information and identify attacks from multiple hosts and possibly the network that connects the hosts [11].

V. WIRELESS NETWORKS

A Wireless Local Area Network is an easy data communication system applied as a development to or as next option for, a wired LAN. Wireless set of connected systems have turn out to be famous in recent times due to simplicity of their mechanism and protection.The overall security remains the same as with wired networks: preserving secrecy, ensuring integrity, and maintaining accessibility in cycle. Division among standard and irregular traffic is frequently not cleared in ad-hoc wireless set of connections [12].

VI. ROLE OF NIDS AND TYPES OF ATTACKS

A Network Intrusion Detection System is assigned to supervise set of connected systems on behalf of attacks otherwise intrusions are collected information of these intrusions towards the administrator in turn to get serious steps. To check every network activity, without a NIDS it results in permanent harm to an organization's Intrusion attack are those in which an attacker pass in to your network to take, break, or read your information.

A. Scanning Attack

Attackers sending a variety of packets for investigate whether a network or system is being exploited. When the analysis packets are reaching the target system, the system responds it and these replies are being examined towards finding the features of the targeted system, and there will be vulnerabilities. The scanning attack identifies a potential victim network; Port, vulnerability scanners, etc. are used to yield information [13].

B.Denial of Service Attack

A DOS attack try to collapse an objective thus to interrupt the service reject the access of genuine and certified clients. Thus, these types of attacks are usual in the Website where collections of servers, which are regularly utilized to attack WWW servers to the fake appeal. They will drastically change the financial harm to e- Commerce by rejecting the clients approach

C.Flooding DOS Attacks

An attacker delivers additional appeals to an objective than it can manage. It can also consume the processing ability or consume the network bandwidth leading to a DOS to new users. DOS (Denial of Service) attacks are difficult to conflict these do not use the data and even the most protected

system will be spotted. Bootmaster will be able to begin a DDoS attack via utilizing the vulnerability within any system, and takes command, by creating a DDoS controller [14]. The trespasser utilizes the controller to speak over with additional System.

D. Penetration Attacks

In Penetration attack, the hacker increases an illegal control and modifications of the system and reading the system information ,documents and etc., This types of attacks destroy the software, which allows the hacker to establish malware and viruses in the system.

VII. TAXONOMY OF INTRUSION DETECTION SYSTEMS

The definition of classification is "A taxonomy of organisms into groups based on similarities of structures in characteristics". The Intrusion Detection System looks for actions and/or set of actions, which are similarly predefined structure of a well-known attack, the analytical approach is known as misuse detection.

An IDS investigates the gather information simply starts from the single monitored system and DIDS which gather information from numerous monitored systems which in turn to study worldwide, spread and synchronized attacks.

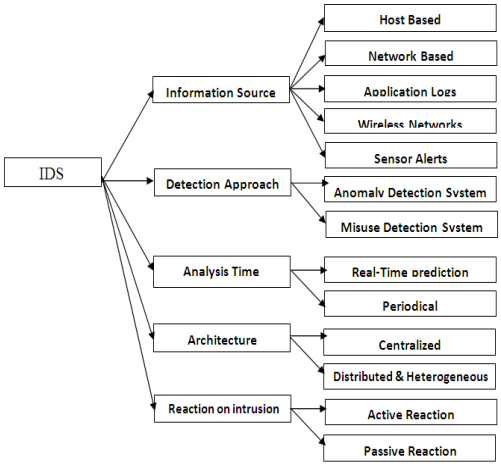

Figure 2: Characteristics classification of IDS attacks

VIII. ALERTS FROM IDS

As a result of raise in a congestion level, recent trading IDS typically lean to make an extremely huge amount of false alarms. Additionally, a huge DDOS or else scanning attack may cause several alarms while numerous network links are concerned. Additionally, it raises the amount of alarms that security analysts must study [15]. In turn to reduce amount of approach for spotting intrusions is increased, which can decrease the final detection rate.

IX.FUNCTIONS OF IDS

The Functions of IDS is classified in to Data Collection, Feature selection, Analysis and Action.

A) Data collection

Data collection passes the data as input to the IDS. The data are recorded into a file and then it is examine and analyzed. N IDS collects and alters the data packets and in host based, An IDS collect details like usage of the disk and processes of the system**.**

B) Feature Selection

This module select the particular feature large data is accessible in the network and they are usually evaluated for intrusion. For example, the Internet Protocol address of the source and target system, protocol type, header length and size could be taken as a key for intrusion [16].

C) Analysis

The Analysis is used to find the correctness. Rule based IDS analyze the data where the incoming traffic is checked against predefined signature or pattern. Another method is anomaly based IDS where the system behaviour is examine and mathematical models are employed to it [17].

D) Action

The Action defines about the attack and reaction of the computer system. It can either inform the system administrator with all the required data through email, alarm icons or message or it can play an active part in the system by dropping packets so that it does not enter the system or close the ports [18].

X.TOOLS IN INTRUSION DETECTION

An IDS products accessible today addresses a range of organizational security goal [19]. The Beloe section discusses about the security application tools.

(i) SNORT

Snort is lightweight and open source software. Snort uses a flexible rule-based language to explain the traffic .From an IP address and it records the packet in human readable format. This protocol analysis, content searching, and various pre-processors Snort detects many worms, vulnerability exploit attempts, port scans, and other doubtful behaviour.

(ii) OSSEC-HIDS

OSSEC (open source security) is freeware software. It will run on major OS and uses a Client/Server technology. OSSEC has the ability to send Operating System logs to the server for analysis and storage. It is used in powerful log analysis engine, ISPs, universities and data centers.

Authentication logs, firewalls are monitored and analyzed by HIDS.

(iii) FRAGROUTE

This is termed as fragmenting router. Here, from the attacker to the fragrouter the IP packet is sent and they are then fragmented and transformed to the party.

(iv) HONEYD

Honeyd is a tool that creates virtual hosts on the network. The services are used by the host Honeyd allows a single host to request multiple addresses on a LAN for networks simulation. It is possible to knock the virtual machines or to trace route them . Any type of service on the virtual machine can be simulated according to a simple configuration file.

XI.CONCLUSION

In this paper an overview of the lifecycle, types of IDS, various domains, types of IDS attacks and tools have been discussed. During the last decade, drastic improvement has taken place in internet. IDS are becoming essential for day today security in the world and for computer network users**.** Nowadays internet is used in all lifestyles, safe data transmission is still a vast challenge in data communication. Even though several researchers have suggested new techniques for secured data transmission, the intruders are able to break the system with ease. Therefore, a secured and efficient tool will be a big boon for data communication in today's internet world.

REFERENCES

[1] The Rebecca Bace, Peter Mell, "NIST Special Publication on Intrusion Detection Systems", 16 August **2001,** pp.**1-51**.

[2] Defeng Wang, Yeung, D.S., and Tsang, E.C., "Weighted Mahalanobis Distance Kernels for Support Vector Machines", IEEE Transactions on Neural Networks, Vol. 18, No. 5, **2007,** pp. **1453-1462.**

[3] Intrusion.com, Intrusion Secure Host, white paper available at: www.intrusion.com/products/hids.asp, **2003.**

[4] W. Jansen, P. Mell," Mobile Agents in Intrusion Detection and Response", In Proceedings of the 12th Annual Canadian Information Technology Security Symposium, Ottawa, Canada, September **2010,** pp.**77-91**.

[5] C. Kruegel, T. Toth," Distributed Pattern Detection for Intrusion Detection", In Proceedings of the Network and Distributed System Security Symposium Conference, Internet Society, Los Angeles, CA, February **2002**.

[6] E. Eskin, A. Arnold, M. Prerau, L. Portnoy and S. Stolfo,"A Geometric Framework for Unsupervised Anomaly Detection: Detecting Intrusions in Unlabeled Data, in Applications of Data Mining in Computer Security", S. Jajodia D. Barbara, "Advances In Information Security", Ed. Boston: Kluwer Academic Publishers, **2012.**

[7] M. Esmaili, R. Safavi-Naini, B. Balachandran and Pieprzyk, J." A Case Based Reasoning for Intrusion Detection System", December **1996**, pp. **214 - 223**, doi: 10.1109/CSAC.1996.569702. ISSN: 1063-9527 [In Proceedings of the 12th Annual Computer Security Applications Conference].

[8] German Florez-Larrahondo, Zhen Liu, Yoginder S. Dandass, Susan M. Bridges, and Rayford Vaughn, "Integrating Intelligent Anomaly Detection Agents into Distributed Monitoring Systems", **2006,** Vol. 1, issue 1, pp.**59–77** , ISSN 1554-1010 Dynamic Publishers, Inc.[Journal of Information Assurance and Security].

[9] C. Krugel, T. Toth," A Survey on Intrusion Detection Systems", Technical University of Vienna Technical report, April **2010,** pp.**410-417**. [Online Available: http://citeseerx.ist.psu.edu/viewdoc/summary? doi=10.1.1.72.605.

[10] Yanny Liu, "An Introduction to Intrusion Detection Systems", in ACC 626 Term Report for: Professor Malik Datardina, July 5, **2009** pp.**1-9.**

[11] Nathan Einwechter, "An Introduction to Distributed Intrusion Detection Systems", January 8, **2001. [**Online Available:http://www.symantec.com/connect/articles/introduction-distributed-intrusion-detection-systems (Accessed 30 April **2013**).

[12] Yongguang Zhang, wenkelee," Intrusion detection in Wireless ad-hoc networks", Published in Mobicom'00 Proceedings of the 6th annual international conference on Mobile computing and networking pp **275-283**

[13] Ghosh and A. Schwartzbard,"A Study in Using Neural Networks for Anomaly and Misuse Detection", In Proceedings of the Eighth USENIX Security Symposium, Washington, D.C., August **1999**, pp. **141-152.**

[14] Amrita Anand, Brajesh Patel," An Overview on Intrusion Detection System and Types of Attacks It Can Detect Considering Different Protocols", International Journal Of Advanced Research in Computer Science and Software Engineering, vol.2 Issue.8,August **2012**,ISSN: 2277 128X, pp.**94-98**.

[15] G. Helmer, J.S.K Wong, V. Honavar and L. Miller, "Intelligent Agents for Intrusion Detection", In Proceedings of the IEEE Information Technology Conference, Syracuse, NY,September **2007**, pp.**121-124**.

[16] Sriram Sundar Rajan, Vijaya Krishna Cherukuri- "An Overview of Intrusion Detection Systems".

[17] Karthikeyan .K.R and A. Indra- "Intrusion Detection Tools and Techniques a Survey"

[18] "Top 125 Network Security Tools"- SecTools.Org- http://sectools.org/tag/ids/sec

Authors Profile

Mr.P.Kaliraj has received his M.Sc degree in the year 2007 from Madurai Kamaraj University, Madurai, TamilNadu, India. Before coming to the teaching profession he has worked in a reputed software organization, Logesys Technologies ,Chennai,TamilNadu, India. He is presently working as an Assistant Professor in the Dept. of Computer Science in Kongunadu Arts and Science College, Coimbatore, TamilNadu, India. He is currently working towards his Ph.D degree in the Area of Networks. He has published several papers in International and National level journals and conferences.

Dr.B.Subramani holds a Ph.D. in Computer Application from Bharathiar University, Coimbatore. He has more than 20 years of academic experience in various positions in reputed colleges. He is a member in many Academic Bodies and Professional Societies. His interest includes Dataming, Network Security and Cloud computing. He has been recognized as a research guide in Bharathiar University and presently six students are pursuing Ph.D under his able guidance. Now he is working as a principal in SNMV college of Arts and Science, Coimbatore, TamilNadu, India. He received many awards from various universities and Professional Societies.

