iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** VI **Month of publication:** June 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

An Overview of Intrusion Detection System

Stephant Naorem[1], Abhishek Sharma[2]
[1,2]*M.Tech, Assistant Professor*
Department of Cse, Shri Balwant College of Engineering &Technology
Dcrust University

Abstract: With invent of new technologies and devices, Intrusion has become a major concern in businness sector as well as in research area. By monitoring the computer system and networks resources intrusion detection identify any of the unauthorized use or misuse of the information from within the organization.,and abuse of computer systems.Then it alerts and informs administrator for occurrence of an intrusion.There are several methods which can be used to detect intrusion. This paper includes an overview of intrusion detection systems, its types and then the different techniques that are commonly used.In this paper we proposed a basic knowledge of intrusion detection system.
Keywords:-Intrusion Detection, Intruders, Anomaly Detection, Misuse Detection.

I. INTRODUCTION

A. *What Is Intrusion?*

Any set of actions that attempts to compromise the confidentiality, integrity or availability of a computer resorce.

B. *What Is Intrusion Detection?*

Intrusion Detection is the process of identifying and responding to malicious activity targeted at resources.Intrusions are essentially events which are caused by intruders/attackers where an unauthorized party attempts to break into or misuse an information system for their own purposes.

C. *What Is An Intrusion Detection System?*

Intrusion Detection System is a system designed to test/analyze network system traffic/events against a given set of parameters and alert/capture data when these thresholds are met.Intrusion Detection System uses collected information and predefined knowledge –based system to reason about the possibility of an intrusion.
Intrusion Detection System also provides sevices to cop with intrusion such as giving alarms, activating programs to deal with intrusion etc. 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. It is a device or software application which monitors system or network activities for malicious activities or policy violations Intrusion Detection System monitors the operations of firewalls, routers, managementservers and files critical to other security mechanisms.

II. BACKGROUND

From last two decades, the networking of computers has been an effective field of research.In 1980 - James Anderson Published a Paper“Computer Security Threat Monitoring and Surveillance “, which was the Concept of “detecting” misuse and specific user events emerged.Between 1983 and 1984 Dr. 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. The prototype was named the “Intrusion Detection Expert System (IDES)”
In 1988 – HayStack Project at University of California Lab, released intrusion detection system for US Air force
1989 – Commercial company HayStack Labs released Stalker
1990 – UC’s Todd Heberlein introduced idea of Network Detection System”
Developed Network Security Monitor
Currently IDS is the top selling security technology

III. LITERATURE SURVEY

A. *Functions of Intrusion Detection*

Functions of intrusion detection are:
Monitoring and analysing both users and system activities.

Analyzing system configurations and vulnerabilities.
Assessing system and file integrity.
Ability to recognize patterns typical of attacks.
Analysis of abnormal activity patterns.
Tracking user policy violations
Intrusion Detection System are being developed in response to the increasing number of attacks on major sites and networks.The safeguarding of security is becoming increasingly difficult ,because the possible technologies of attack becoming ever more sophisticated;at the same time ,less technical ability is required for the novice attacker,because the proven past methods are easily assessed through the web. An Intrusion Detection System detects an attacks as soon as possible and takes appropriate action.An Intrusion Detection System does not usually take preventive measures when an attack is detected.It is a reactive rather than a pro active agent.Its plays a role of informant rather than a police officer.

B. Importance Of Intrusion Detection System (IDS)

Intrusion Detection System is important to implement in an organization for the following reasons
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. Intrusion Detection Approach

There are two basic approach which are used by Intrusion Detection Systems for detecting intruders are
Misuse Detection (also called signature based detection) and
Anomaly Detection

1) *Misuse Detection*: This detection approachss uses specifically known patterns to detect malicious code. These specific patterns are called signatures. Identifying the worms in the network is an example of signature based detection.In misuse detection, the IDS identifies illegal invasions and compares it to large database of attack signatures.This IDS possess an attacked description that can be matched to sensed attack manifestations.

Advantages
It raises fewer false alarms because they can be very specific about what it is they are looking for.

Drawbacks of Signature based IDS
Any new form of misuse is not detected
Resource consuming and slows down the throughput

2) *Anomaly Detection*: In anomaly detection, the IDS monitor the network segments and compare their state to the normal baseline to detect anomalies. Anything distinct from the noise is assumed to be an intrusion activity. E.g flooding a host with lots of packet.

Advantages
New form of attack can be detected.
It raises high false alarm
Limited by training data

Advantage
New form of attack can be detected.

D. Classification Of Intrusion Detection Systems

Intrusion detection systems are classified as
Network-based IDS

Host-based IDS

Hybrid based IDS

1) Network –Based IDS: Network based IDS identifies intrusions by examining network traffic and monitors multiple hosts. Network Intrusion Detection Systems gain access to network traffic by connecting to a hub, network switch configured for port mirroring, or network tap. An example of a NIDS is Snort.The NIDS are probably the most known systems. They are installed

on a network and act like a sniffer (stealth mode or promiscuous mode), capturing anddecoding packets to pass through his network segment. It Analyze traffic for unwanted or malicious events.

2)Host-Based IDS: Host-based systems were the first type of IDS being developed andimplemented.It differs from network-based intrusion detection the entire process is conducted on the host itself.A host-based intrusion detection system examines the activity of each individual computer or host.It Consists of sensors that are located on servers or workstations to detect attacks on that specific server or workstation.These audit information includes events like the use of identification and authentication mechanisms (logins etc.) , file opens and program executions, admin activities etc.This audit is then analyzed to detect trails of intrusion.

3) Hybrid Based IDS: In Hybrid based IDS, both host-based and network-based IDSs are used simultaneously . Hybrid intrusion detection system has flexibility and it increases the security level. It combines IDS sensor locations and reports attacks are aimed at particular segments or entire network.

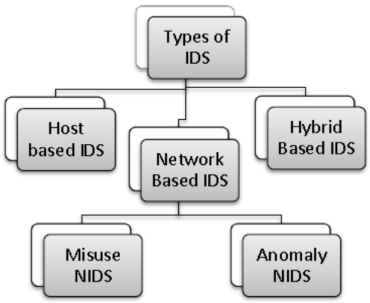


Fig. 2: Classification of IDS [19]

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

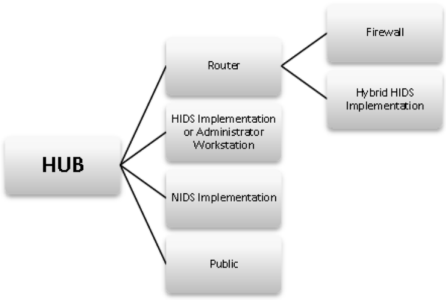


Fig. 3: Types of IDS [23]

IV. INTRUSION DETECTION TECHNIQUES

To solve the limitations of the above methods,a number of data mining techniques have been introduced:-

A. Artificial Neural Network(ANN)

Artificial Neural Network is one of the most used technique and has been sucessfully applied to intrusions detection. Artificial Neural Network (ANN) consists of base units called neurons, which are grouped, in several levels. Neurons are connected to neighbor neuronsand those connections are weighed. An ANN has input level, one or several hidden layers, and output level.

State Transition Tables:-Here, an attack is described with a set of goals and transitions that must be achieved by an intruder to compromise a system. Transitions are represented on state-transition diagrams.

B. Genetic Algorithms (GAs)

The function of Genetic Algorithms (GAs) is to copy 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. Learning Classifier System (LCS) is the related technique, in which binary rules that recognize intrusion patterns are evolved

C. 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 . This approach can handle incomplete data .

D. 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. 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

This field of intrusion Detection Technique cannot solved the problems completely.IDS donot have the capability to look at every possible security event.Its difficult to identify and evaluate the processes,procedure and tools.Lack of qualified technical staff.So ,Intruders can access the computer and networks resources very cleverly using efficient technique.So,there is a direct need to work on intrusion detection system .

VI. CONCLUSION

IDS is a technology that can be used to detect an attack,but for future capabilities in IDS can be improved.

REFERENCES

[1] 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

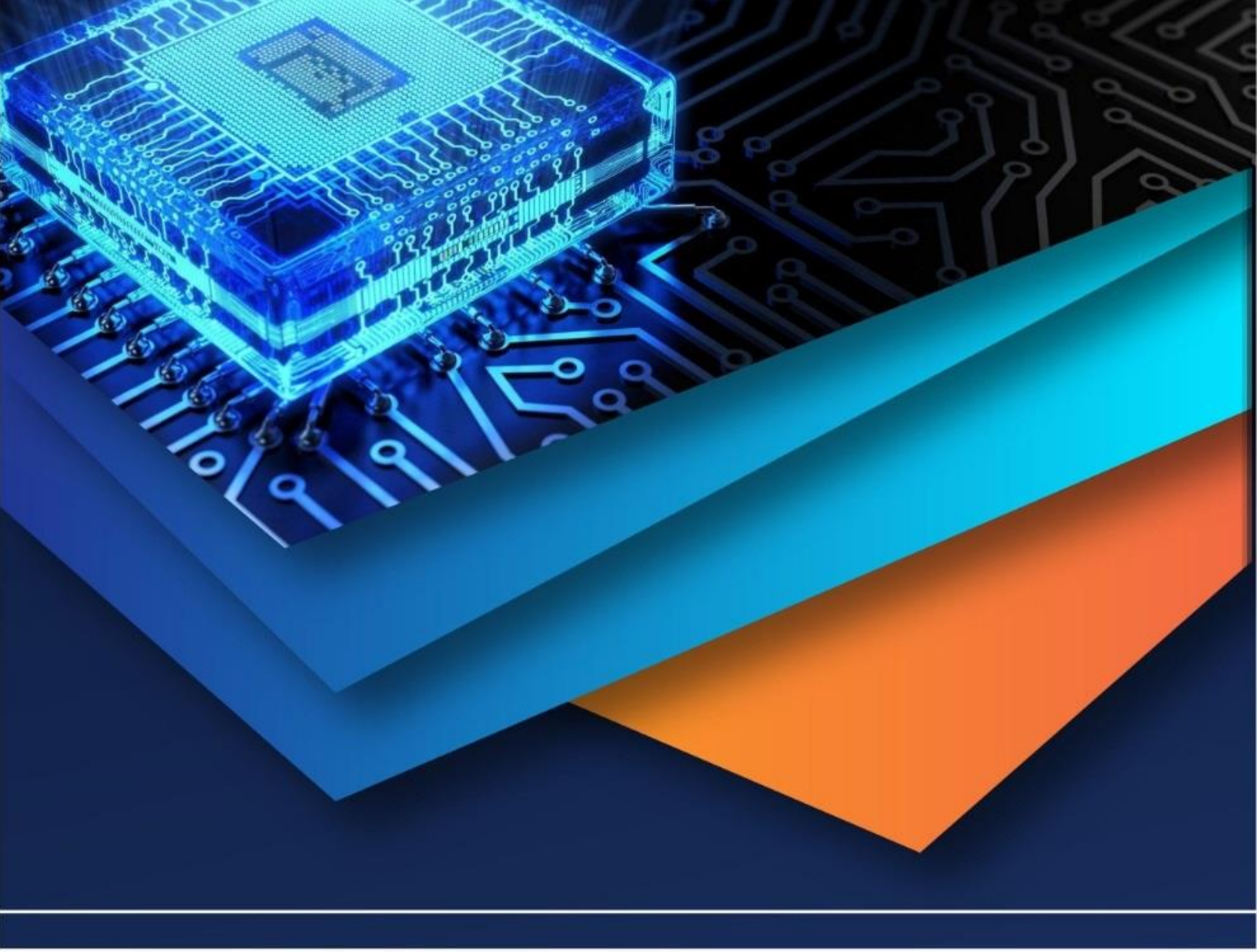
[2] John McHugh, Alan Christie, and Julia Allen (Software Engineering Institute, CERT Coordination Center), "The Role of Intrusion Detection Systems", IEEE Software September/October 2000.

[3] 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.

[4] 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.

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

[6] Vangie Beal," Intrusion Detection (IDS) and Prevention (IPS) Systems", posted 2005 [07-15-2005], last updated 2010[08-31-2010].
[7] 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.
[8] 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.
[9] M. Crosbie and E. Spafford, "Applying Genetic Programming to Intrusion Detection," GECCO '96 Proceedings of the First Annual Conference on Genetic Programming 1996.
[10] Danny Rozenblum, "Understanding Intrusion Detection Systems", SANS Institute Reading Room site.
[11] K.Rajasekhar, B.Sekhar Babu, P.Lakshmi Prasanna, D.R.Lavanya, T.Vamsi Krishna,"An Overview of Intrusion Detection System
[12] PengNing,SushilJajodia,"Intrusion Detection Techniques", http://citeseerx.ist.psu.edu/viewdoc /download?doi10.1.1.89.2492&rep=rep1&type=pdf
[13] Sandip Sonawane, Shailendra Pardeshi, Ganesh Prasad,"A survey on intrusion detection techniques",World Journal of Science and Technology 2012, 2(3):127-133.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY