INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

COMPARATIVE ANALYSIS OF DIFFERENT TECHNIQUES FOR INTRUSION DETECTION

MISS SHRADDHA S. PAWAR[1], PROF. CHETAN J. SHELKE[2]

1. M.E. Scholar, Department of Computer Science & Engg., P. R. Patil College of Engineering & Technology, Amravati.
2. Assistant Professor, Department of Computer Science & Engg., P. R. Patil College of Engineering & Technology, Amravati.

Accepted Date: 15/03/2016; Published Date: 01/05/2016

Abstract: In the recent years, Intrusion Detection materializes the high network security. Thus tries to be the most perfect system to deal with the network security and the intrusions attacks. The Intrusion detection system classified into three types which is Host-base, network –base and hybrid-base. These system prevent the attack from the intruders. There is mainly two techniques which are Misuse and Anomaly Detection technique. The Anomaly technique further divided into sub type which is statistical base, knowledge-base and machine learning base technique, in which also many techniques for intrusion detection. In this paper we only showing the different techniques for intrusion detection.

Keywords: Intrusion Detection system, Anomaly Based intrusion. Neural Network, Machine Learning, statically base technique, knowledge-base techniques.

Corresponding Author: MISS SHRADDHA S. PAWAR

Access Online On:

www.ijpret.com

How to Cite This Article:

Shraddha S. Pawar, IJPRET, 2016; Volume 4 (9): 893-903

PAPER-QR CODE

INTRODUCTION

At present, The assurance of integrity and safety should be applied to computer systems and data. The Internet has made the information flow to the large extent. Also at the same time it has to face many threats and attacks. Thus the security alert is required to control the attacks and threats. The paper describes the different techniques for ID. An intrusion detection system is used to detect all types of malicious.[1]

A) What is Intrusion Detection?

Intrusions are the activities that violate the security policy of system. Intrusion detection is process used to identify the intrusion. Intrusions are usually caused by intruders/attackers, who want unauthorized and additional privileges to particular system or network for their own purposes [3]

B) What is an Intrusion Detection System?

Intrusion detection system is used for detecting the intrusion. Intrusion detection system serve three essential security function: they are monitor, detect and respond to unauthorized activity company insider and outsider intrusion.[2][3] Intrusion detection system use policies to define certain events that, if detected will issue an alert .certain intrusion detection system have capability of sending out alert, so that administration IDS receive a notification of security incident[1].

Types of Intrusion Detection System-

1) Host –Base IDS , 2)Network-Base IDS 3)Hybrid-Base ID

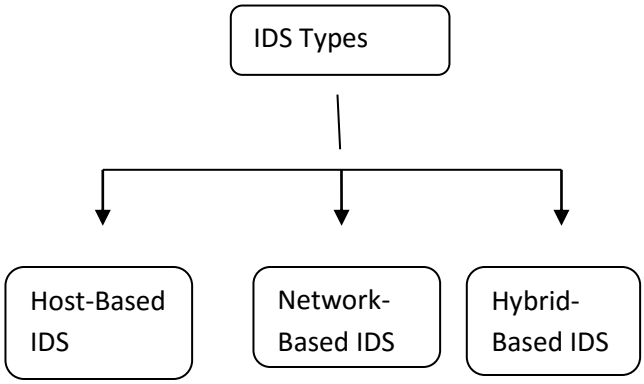


Figure.1. Intrusion Detection System – Types

Host-base system(HIDS) were the first time type of IDS to be developed and implemented. These system collect and analyze data that originate on computer that host a services, such as web server. It can either be analyze locally or sent to separate/central analysis machine.

In addition to detecting unauthorized insider activity host-base system are also effective at detecting unauthorized file modification, Network-base system(NIDS),as opposed to monitoring the activity that take place on particular network, network-base intrusion detection analyze data packet that travel over the actual network. Hybrid-base system is the combination of the host-base system and network-base system. Early research works on intrusion detection systems suggested that the intrusion detection capabilities can be improved through a hybrid approach consisting of both signature (misuse) detection as well as anomaly detection. In such a hybrid system, the signature detection technique detects known attacks and the anomaly detection technique detects novel or unknown attacks.[1]

1.1 Aim

An Intrusion Detection System is an important security feature to detect the threats to a vulnerable network. Also the different techniques involved to detect the intrusion are compared with the help of parameters like accuracy, time taken to identify the attacked, and from which we have to choose best one technique.

1.2 Objective

Intruders hack the data or use the, the access of the is unauthorized. To prevent the hacking of the for which intrusion detection system are present in which many technique is present, compaire those technique choose those technique which is best from the all Identity theft

1.3 Scope

IDS using data mining helps in protecting a network from malicious attacks from outsiders as well as insiders. It will help in Intrusion Detection in various platforms like college network, corporate network etc.

2. Related Work:

At present, The assurance of integrity and safety should be applied to computer systems and data. The Internet has made the information flow to the large extent. Also at the same time it has to face many threats and attacks. Thus the security alert is required to control the attacks and threats. The paper describes the different techniques for ID. An intrusion detection system is used to detect all types of malicious.[1]

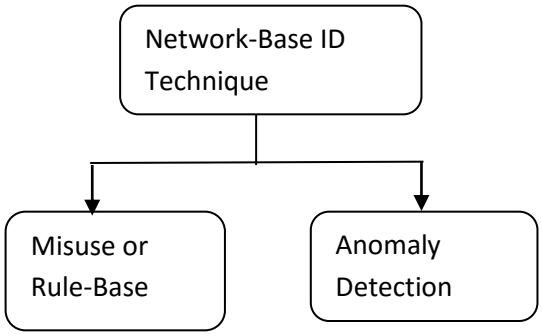
Host-base system (HIDS) were the first time type of IDS to be developed and implemented. These system collect and analyze data that originate on a computer that host a services, such as

web server. it can either be analyze locally or sent to separate/central analysis machine. In addition to detecting unauthorized insider activity, host-base system are also effective at detecting unauthorized file modification, Network-base system(NIDS),as opposed to monitoring the activity that take place on particular network, network-base intrusion detection analyze data packet that travel over the actual network. Hybrid-base system is the combination of the host-base system and network-base system.[3][5]

Network-base intrusion detection system is generally implemented using two approaches which is Rule-base detection or Misuse detection and second one is Anomaly-base detection. Rule-base detection or Misuse detection: it is based on the rate of the identifying known intrusion but it fails to detect new type of intrusion as their signature are not know. Anomaly-base: it is boundlessness of the method. It has ability to examine new or unknown intrusion.[2][3]

❖ **Anomaly detection Technique**:

It is boundlessness of the method. It has ability to examine new or unknown intrusion[2]. Profiles may be established for normal behaviour of users, which comes from the statistics of data of users. When detection is performed profile is compared with the actual users data.[3] The Anomaly detection technique are also classified into the three sub type such as statistical based, knowledge-based, and machine learning-based.



Fig(Network-Base ID technique)

I)Statistical base technique

In Statistical base technique, action and reaction of system from ergodic view point. It is based on mainly the content and time. This outline is based on metrics of basic features such as duration, protocol, source & destination ip address, source& destination port, services etc, content and time based features. It has sub types which is given as-

a)Mean and Standard Deviation:-

In this technique, by comparing even measured to profile mean and standard deviation, confidence ,internal for abnormality can be establish.[4][6]

b)Multivariate model:-

Calculating the correlation between multiple event measures, relative to the profile expectations.[4][6]

c)Markov process model:-

This model regards event types to be state variables in a state transition matrix, where an event is considered anomalous if its probability, given the previous state and associated value in the state transition matrix, is too low.[4][6]

d)Operational Model (or) Threshold Metric:-

The actions that occur over a period of time regulate the alarm. This can be visualized in Win2k lock; a user after n unsuccessful login attempt regulate the alarm. here lower limit is 0 and upper limit is n.[5]

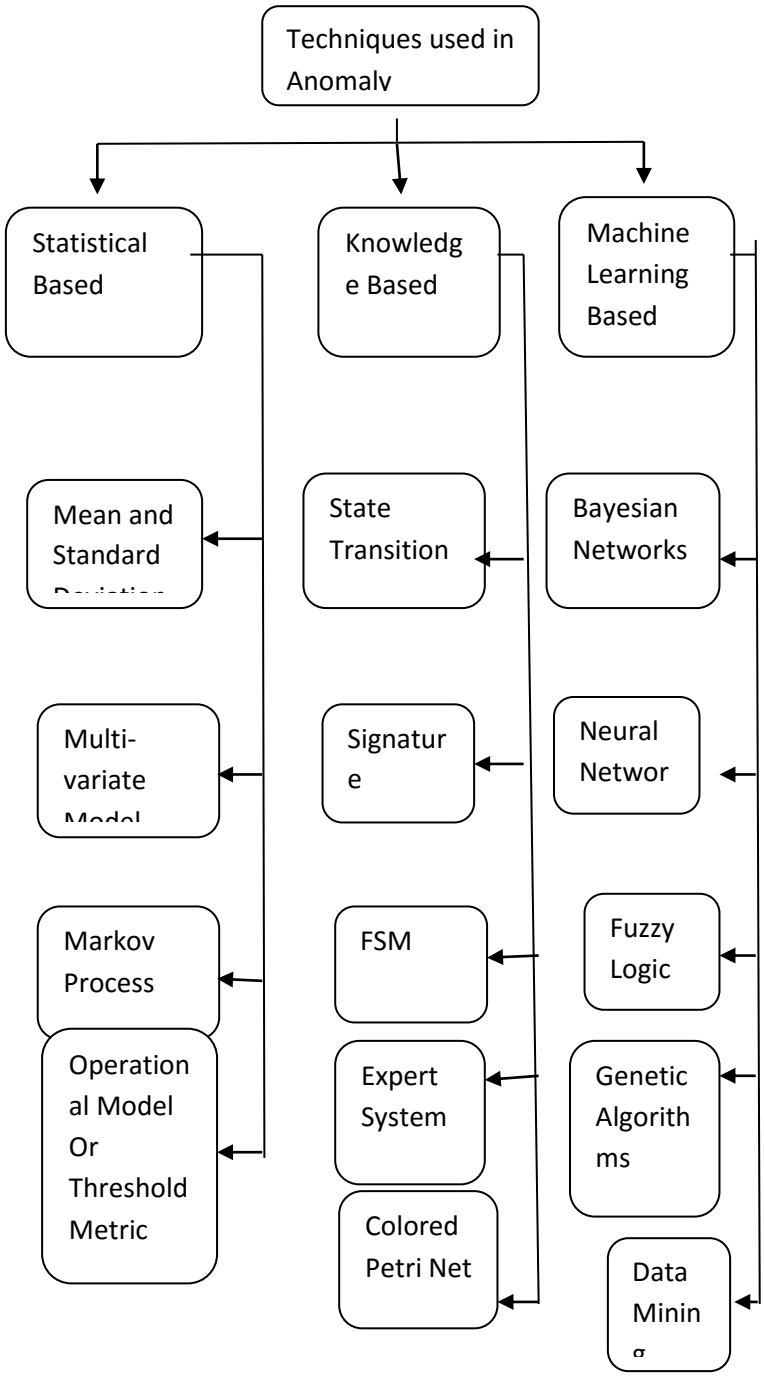


Fig: Anomaly Detection Techniques

II) Knowledge Based Technique

Knowledge based detection Technique can be used for both signature based IDS as well as anomaly based IDS. It accumulates the knowledge about specific attacks and system vulnerabilities. It uses this knowledge to exploit the attacks and vulnerabilities to generate the alarm. Their completeness requires that their knowledge of attacks be updated regularly. Knowledge based detection Technique can further be classified as:

a) State Transition Analysis:-

The monitor system is presented as state transition diagram. As data analyzed, system make transition form one state to another. Transition take map on some Boolean condition being true.[4]

b) Signature Analysis:-

This type of detection engine detect intrusion that flow well-known pattern of attack(or signature) that exploid known software. Limitation is that may not care about detecting unknown future intrusion.[7]

c) FSM:-

Finite state machine (FSM) methodology –a sequence of states and transitions among them– seems appropriate for modeling network protocols.[10]

D) Expert systems:-

The Expert Systems working principle is based on a previously defined set of rules describing an attack. All security related events incorporated in an audit trail are translated in terms of if-then else rules.[11]

e) Colored Petri Nets

This Petri Nets method is used to generalize attacks from expert knowledge bases and to represent attacks graphically. This technique is very easy and useful for system administrators to add new signatures to the system. Audit trail data may be time-consuming. This technique is not used in commercial systems.[11]

III) Machine learning-based

Machine learning based NIDS is one of the classification of anomaly based NIDS. Machine learning techniques are based on establishing an explicit or implicit model that enables the patterns analyzed to be categorized. A singular characteristic of these schemes is the need for labeled data to train the behavioral model, a procedure that places severe demands on

resources. In many cases, the applicability of machine learning principles coincides with that for the statistical techniques, although the former is focused on building a model that improves its performance on the basis of previous results. Hence, a machine learning A-NIDS has the ability to change its execution strategy as it acquires new information. Although this feature could make it desirable to use such schemes for all situations, the major drawback is their resource expensive nature. Machine Learning Based detection Technique can further be classified as:

a) 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.[3]

b)Data Mining:-

Data mining techniques have been applied to network and host audit data for building misuse detection models. In this case, intrusion detection is considered as a data analysis process, in which data mining techniques are used to automatically discover and model features of user's normal or intrusive behaviors [1].

c)Fuzzy Logic:-

It is method to computing based on degree of tsak rather than usual true or false in Boolean. with Fuzzy space fuzzy logic an object to belong to different courses at the same time. Ever fuzzy rate has following general form, If condition THEN conclusion [weight],

Where,

Condition is fuzzy defined using fuzzy logic operator like fuzzy AND and OR. Conclusion is atomic expression weight is real number in[0,1].[1][3][7].

d) Neural net:-

The idea here is to train neural network to predict a user is next action or command, given the window of n previous action. [1],[3],[6]

e)Genetic Algorithm:-

The GASSATA system (Genetic Algorithm as an Alternative tool for security audit Trail Analysis)[GASSATA] uses a genetic algorithm to search for the combination of known attacks that best event matches with observer event stream. Functioning of genetic algorithm is that

mimic natural reproduction system in nature where after certain changes, only the fittest individuals in a generation will be reproduced in subsequent generations. [1][3][8]

3. Advantages and Disadvantages of Anomaly Detection and Misuse Detection

The main disadvantage of misuse detection approaches is that they will detect only the attacks for which they are trained to detect. Novel attacks or unknown attacks or even variants of common attacks often go undetected. The main advantage of anomaly detection approaches is the ability to detect novel attacks or unknown attacks against software systems, variants of known attacks, and deviations of normal usage of programs regardless of whether the source is a privileged internal user or an unauthorized external user. The disadvantage of the anomaly detection approach is that well-known attacks may not be detected, particularly if they fit the established profile of the user. Once detected, it is often difficult to characterize the nature of the attack for forensic purposes. Finally a high false positive rate may result for a narrowly trained detection algorithm, or conversely, a high false negative rate may result for a broadly trained anomaly detection approach. [9]

Some other advantages are given bellow:

Low Rate of False Alarms: The main advantage of misuse detection systems is their ability to detect known attacks and the relatively low false alarm rate when rules are correctly defined. It is important to note that, as said above, the signatures which are used in rules must be as specific as possible to prevent false alarms.[11]

Unknown Attacks Detection: The main advantage of anomaly detection systems is that, contrary to misuse detection systems, they can detect unknown or novel attacks. They do not rely on any a priori knowledge concerning the intrusions. It is also important to note that anomaly detection systems have not for main purpose to replace misuse detection systems. The very good efficiency of misuse systems in detecting known attacks makes them a perfect complement to anomaly detection systems.[11]

Conclusion:

In this paper we discussed which type of intrusion detection system are present different technique for intrusion detection. With the help of any of the above discussed techniques\ algorithms may be designed so that network becomes safe and secure. This intrusion detection has been done

REFFERENCE

1. Rajni Tewatia, Asha Mishra "Introduction To Intrusion Detection System: Review" International Journal Of Scientific & Technology Research Volume 4, Issue 05,May 2015
2. J. Antony Jeyanna 1, E. Indumath 2, Dr. D. Shalini Punithavathani" A Network Introduction To Intrusion Detection System Using Clustering and Outlier Detection" international journal of Innovative Research In computer and communication Engineering, Vol 3,issue 2 February 2015.
3. Hussain Ahmad Madni Uppal 1,Memoona Javed 2 and M.J. Arshad 3 Department of Computer Science and Engineering, UET, Lahor, Pakistan"A Introduction To Intrusion Detection along with its commonly used Techniques and Classification" International journal of Innvoative Research in computer communication Engineering, vol 5, issue 2 february 2014.
4. Theuns Verwoerd and Ray Hunt Department of Computer Science University of Canterbury, New Zealand "Intrusion Detection Techniques and Approaches" Article in Computer Communication September 2002.
5. Dr. S. Vijayarani 1 and Ms. Maria Sylviaa, Assistant Professor, Department of Computer Science Science, Bharathiar University, Coimbatore"intrusion detection system-A study" International Journal of Security, Privacy and Trust Management (IJSPTM) Vol 4, No 1, February 2015.
6. Theuns Verwoerd and Ray Hunt, Department of Computer Science University of Canterbury, New Zealand"intrusion detection Techniques and Approach".
7. Deepika P Vinchurkar, Alpa Reshamwala M Tech student,Assistant Profesor,department of computer science"A review of Intrusion detection system using Neural network and Machine learning Technique" International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 1, Issue 2, November 2012.
8. Mahdi Zamani and Mahnush Movahedi, Department of Computer Science, University of New Mexico,"Machine Learning Techniques for Intrusion Detection", arXiv:1312.2177v2[cs.CR]9 May 2015
9. J.S Shanthini PG Scholar Jai Shri Ram Group Of Institution Avinashipalayam, Tirupur and Dr. S. RAJALAKSHMI Ph.D Head of the Department, CSE Jai Shri Ram Group of Institutions Avinashipalayam, Tirupur " Intrusion detection survey", International Journal Of Engineering Technology and Sciences – IJETS™, Volume II, Issue XI, November – 2015.
10. P. Garcı´a-Teodoroa,*, J. Dı´az-Verdejoa, G. Macia´-Ferna´ndeza, E. Va´zquezb A Department of Signal Theory, Telematics and Communications – Computer Science and Telecommunications Faculty, University of Granada, Granada, Spain B Department of Telematic Engineering - Universidad Polite´cnica de Madrid, Madrid, Spain" Anomaly-based network intrusion detection: Techniques, systems and challenges" computer security 28 (2009)1 8 – 2 8.
11. Shaik Akbar Assoc. Profr, Dept. of C.S.E, SVIET, Nandamuru, Krishna Dist, Andhra Pradesh, India Dr. K. Nageswara Rao Prof & H.O.D, Dept. of C.S.E P.V.P.S.I.T, Vijayawada, Krishna Dist, Andhra Pradesh, India Dr.J. A. Chandulal Prof, Dept. of C.S.E GITAM University, Visakhapatnam,

Andhra Pradesh, India "Intrusion Detection System Methodologies Based on Data Analysis" International Journal of Computer Applications (0975 – 8887) Volume 5– No.2, August 2010