International Journal of Innovative Research in Science and Engineering
Vol. No.2, Issue 03, March 2016
www.ijirse.com
ISSN: 2454-9665

# HYBRID INTRUSION DETECTION USING SIGNATURE AND ANOMALY BASED SYSTEMS

**Apeksha Vartak[1] Darshika Pawaskar[2] Suraj Pangam[3] Tejal Mhatre[4]**

**Prof. Suresh Mestry[5]**

[1,2,3,4,5] *Department of Computer Engineering,*

*MCT Rajiv Gandhi Institute of Technology Mumbai (India)*

## ABSTRACT

*Intrusion Detection System is used to provide security for the network, but the existing IDS identifies only known attacks with low false alarm and does not work for unknown attacks that occurs on network. To overcome this, anomaly based IDS with high false alarm is used. By using SDS and ADS we have implemented HIDS with the advantage for identification of known and unknown attacks. Internet rules are used by HIDS to identify the unknown attacks in network. When server receives packets from clients in network, all the attributes of each packets are extracted. This extracted attributes are compared with the stored database to check the known attacks. For anomaly based detection, we are generating a profile with predefined rules. So, if the incoming packets do not match with this profile, then anomaly is detected. Signature will be generated for this anomaly so that in future when ever same type of attacks occur the nit will be directly identified by its signature module.*

***Keywords: Anomaly Detection System(ADS), Hybrid Intrusion Detection system(HIDS), Intrusion Detection System(IDS), Signature Detection System(SDS).***

## I. INTRODUCTION

Various attacks are designed to take advantage of the known vulnerabilities of computer systems and applications. Most of these attacks can compromise the stability of the computer system which leads to a denial of service or some sensitive information is disclosed.

The next layer after the firewall is IDS which has been termed a defense in depth strategy. When an actual attack is succeeded, it should be detected as soon as possible. The IDS creates a database of known signatures for matching those signatures against the traffic that passes through the sensors when it detects “well known attacks”.

Attackers have prior knowledge of these various defense mechanism and create new attacks to enter these systems. Now over here the signature based model of the IDS falls short. Anomaly based detection to detect unknown attacks. When signature based and anomaly based are combined, we get the HIDS. HIDS detects attacks that are present in network layer.

ISSN: 2454-9665

### 1.1 Objectives

The aim of the present work was to design and develop of Hybrid Intrusion Detection System which can detect intrusions based on behavioral patterns as well as detect through the already
existing signature database.

a) Flexibility and Extensibility: HIDS is flexible and extensible as we can detect as well as prevent known and unknown attacks on our system.

b) Performance: The response time of HIDS does not increases when during over load of traffic.

c) Simplicity and Fast Learn ability: HIDS is simple to use, learn and adapt.

### 1.2 Scope

Scope of HIDS is that it can be used in same or different networks. HIDS will increase the security of the system greatly and can be used in different organizations and well as in same LAN. When more signatures are generated, system gives good performance.

## II. LITERATURESURVEY

We have made survey of the existing papers and obtained the following information:

The data packets that may be going in or out of the system is not only checked by Host based Intrusion Detection System, but also manages the internal file system and keep slog of suspicious process. For examining the usage of LAN and to provide statistical data of uploads and downloads in a network a networking tool called Traffic monitoring tool is used. [1]

NetworktrafficinandoutofasinglecomputerischeckedbyHostbasedintrusiondetection butalsochecksttheintegrityofsystemfilesandwatchesforsuspiciousprocesses.Allmajor TCP/IPprotocolsaredecodedbymonitoringNetworktraffic.Inthesepacketmatchingis used. Packets are matched only is any suspected packet is associate with a particular file. [2]

Combination between Anomaly Detection that is based on support vector machine (SVM) and the misuse Detection is used by Intrusion Framework. Its advantage is that high range of detection is achieved with low false positive rate. A wireless sensor network (WSN) is used which consists of number of devices that operate in dividedly and communicate with each other through radio transmissions. These sensor streusel din various military and civilian applications for collection and processing of information from environment.[3]

Snort is an IDS whose functionality is extended to make it a Hybrid IDS. In these extension of Snort IDS is presented by adding a new pre-processor. But when number of elements increases
its sensitivity decreases and thus it detects fewer attacks. According to NIST, IDS is a process for monitoring various events in that occur in a computer system or a network and analyses them for instruction.[4]

Intrusion Detection System is designed using Component Based Software Engineering technique which his far better than the traditional approaches. Advantage of component based software engineering is that it takes less time and cost to develop any system and its maintenance is also easy as if any one component fails, the new component can easily replace it. [5]

ISSN: 2454-9665

Two techniques of intrusion detection are present those are Misuse detection and Anomaly detection. Some use misuse detection while some use Anomaly approach. However, misuse detection faces problems for unknown attacks while anomaly faces false alarm rate problem. An anomaly detection technique is Entropy. [6]

Intrusion Detection System is widely used to detect viler abilities and malicious activities. Research has been done on both the features of IDS that is signature based and anomaly based to design a novel and efficient hybrid IDS. Hybrid IDS has designed to detect vulner abilities on information system. [7]

Fire wall is placed between two or more computers for stopping attacks by providing various rules and policies. But fire wall is not enough for completely securing a network because some insiders also may attack the system which we could not stop. IDS help in stopping and recovering back from the attacks with minimum loss. [8]

## III. SYSTEM OVERVIEW

### 3.1 Structure

The structure of HIDS is shown below in Fig 3.1.

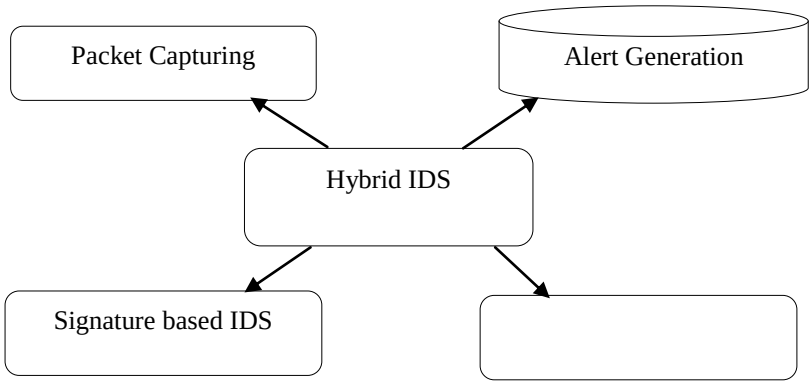


**Fig 3.1 Structure of Hybrid Intrusion Detection System**

- Packet Capturing: Packets are captured in order to get IP related information. These packets are then analyzing for detecting suspicious activities.
- Signature based IDS: A signature – based IDS analyses the network traffic and looks for patterns that matches a signature from known signatures. These signatures consist and are composed with various elements that are used for identifying the traffic.
- Anomaly based IDS: An anomaly-Based IDS looks for suspicious activities in a system. They are trained for getting an idea on ‘normal’ and ‘legitimate’ activities. And then the system will give information on suspicious activities.
- Alert Generation: Alert is indication that an attack has been detected. Alert is generated for both when known or unknown attack found. An attack detection message is display on the system when an attack found.

ISSN: 2454-9665

## IV. EXPERIMENTAL ANALYSIS

Calculation of Detection Rate for HIDS: It is ratio between the number of intrusions that are being correctly detected and the total number of intrusions.

$$DR = \frac{\text{True Positive}}{\text{False Positive + True Positive}}$$

Calculation of False Positive Rate for HIDS: It is calculated as the ratio between the numbers of normal connections that are classified incorrectly as intrusions and the total number of connections that are normal.

$$FP = \frac{\text{False Positive}}{\text{True Positive + False Positive}}$$

Brute Force Single-Keyword Matching Algorithm:

1: procedure Brute Force(x,m, y, n)

**Input:**

a =representskeyword

p =representskeyword length

b = represents text input

q = represents text length

2: for n = 0 to q − p do. For each and every possible character in b

3: m=0

4: while m< p and a[m] = b[m + n] do

5: m=m+ +, m = matching character count at and after b[n]

6: end while

7: if m>= p then

8: output n

9: end if

10: end for

11: end procedure

## V. CONCLUSION

The proposed Hybrid Intrusion detection system is a system for detecting known and unknown attacks. Signature based and anomaly based systems are integrated to form an HIDS. Signature based system detects attacks whose patterns are already present in the database. Anomaly based system detects attack whose patterns are not present in the database. Detection rate is more in HIDS then compared to signature based while false alarm rate is less then compared to anomaly based system. In HIDS as signature database increases the efficiency of signature increases.

## VI. ACKNOWLEDGEMENT

As the outset we offer our sincere thanks to our honorable guide Asst. Prof. Suresh Mastery for his guidance and also encouraging us with his knowledge and experience for the development process of the project. We also value his eagerness and enthusiasm in encouraging us to develop our technical and creative ideas, which ultimately led to success of our project. Our special thanks to faculty members of Computer Engineering Department for their great support and kind co-operation to provide us with whatever we require for our project.

## REFERENCES

[1] Prof. Naveen Kumar, Sheetal Angral, Rohan Sharma, 'Integrating Intrusion Detection System with Network monitoring', International Journal of Scientific and Research Publications, Volume4,Issue5, May2014.

[2] Prof. Radha S. Shirbhate, Prof. Pallavi A. Patil, 'Network Traffic Monitoring Using Intrusion Detection System', International Journal of Advanced Research in Computer Science and Software Engineering, Volume[2], Issue1, January 2012.

[3] Hichem Sedjelmaci and Mohamed Feham, 'Novel Hybrid Intrusion Detection System for Clustered Wireless Sensor Network', International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.4, July 2011.

[4] J.Gómez, C.Gil, N.Padilla[1], R.Banos and C.Jiménez, 'Design of a Snort-Based Hybrid Intrusion Detection System', Research Gate, January 2009.

[5] Er.MohitAngurala, Er.MaltiRani, 'Design and Develop an Intrusion Detection System Using Component Based Software Design', International Journal on Recent and Innovation Trendsin Computing and Communication Volume: 2 Issue:4, ISSN:2321-8169 854– 860

[6] Neha Chaudhary, Shailendra Mishra, 'Design and Implementation of H-IDS Using Snort, Feature Extraction, Honey pot and Rank and Reduce Alert', International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering Vol. 2, Issue 2, February 2013

[7] 7. Kanubhai K. Patel, Bharat V. Buddhadev, 'An Architecture of Hybrid Intrusion Detection System', International Journal of Information & Network Security (IJINS) Vol.2, No.2, April 2013, pp. 197-202

[8] M. Ali Aydın, A. Halim Zaim, K. Gokhan Ceylan, 'A hybrid intrusion detection system design for computer network security', Research Gate, May 2009.