ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

A Novel Methodology to identify the Intruders and Attackers in the Network with Snort

Bathala Subbarayudu, Dr.R.China Appala Naidu, K.Meghana

Assistant Professor, Dept. of I.T., St Martin's Engineering College, Hyderabad, India

Professor, Dept. of C.S.E., St Martin's Engineering College, Hyderabad, India

M. Tech Student, VITS, Vishakapatnam, Tamil Nadu, India

ABSTRACT: Now a day's Intrusions are the most important issues in the current internet environment. The objective is to gain access to a system and steal valuable information or to increase the range of privileges accessible on a system. Attackers use system or vulnerabilities software that allow a user to execute code that opens a backdoor into the system. Gentle intruder's strength is allowable, even though they do devour resources and may slow the performance for legitimate users. However, here is no way to go forward to know whether an intruder will kind or malign. Consequently, even for systems with no mainly responsive resources, there is an inspiration to control this problem. Intruder can attack in any way. Suppose an intruder wants to access some organization valuable information. If that particular organization is fully secured, then there is no way of stealing the information. If not, the problem rises. In our proposed system the security can be provided in such a way that the organizational network contains rule sets. According to the rule sets only the connection has to be made between the organization systems and other systems and with the rule set we can identify the intruders or attackers in the network.

KEYWORDS: Intruder, IDS, Main system, Rule sets, Snort.

I.INTRODUCTION

One of the most publicized threats to security is the intruder (the other is virus) often referred to as a hacker or cracker. Intrusions are the most important issues in the current internet environment. The objective of the intruder is to gain entrée to a system or to boost the range of privileges available on a system. Most preliminary attacks use system or software vulnerabilities that allow a user to execute code that opens a backdoor into the system [2]. The techniques and performance patterns of intruders are constantly shifting, to exploit newly discovered weaknesses & to evade detection and countermeasures.

Hackers traditionally, those who hack into computers do so for the thrill of it or for status. The hacking population is a well-built meritocracy in which status is strong-minded by level of capability [3]. Thus, attackers often look for targets of break and then contribute to the information with others. A classic example is a break-in at a large financial organization reported in [RADC 04].The intruder took advantage of the fact that the commercial network was running undefended services, some of which were not even desired. In this case the key to break-in was the pcAnywhere submission. The manufacturer, Symantec, advertises this program as a remote control solution that enables source connection to remote devices. But the attacker had an easy time gaining access to pcAnywhere; the administrator used the similar 3 letter username and password for the program [6].

In this case there was no intrusion detection system on the joint business network. The intruder was only discovered when a vice president walked into her office to saw the cursor moving files around on her windows work station.
Benign intruders might be tolerable, although they do consume resources & may slow performance for legitimate users. However there is no way in advance to know whether an intruder will kind or malign. Consequently even for systems with no predominantly sensitive resources, there is an inspiration to direct this difficulty [2].

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

Intrusion detection systems are designed to counter this type of hacker threat. In addition to this such systems organizations can consider restricting remote logons to specific IP addresses and/or use virtual private network.

One of the results of the growing awareness of the intruder problem has been establishment of a number of computer emergency response teams these cooperative ventures collect in order about organization vulnerabilities and broadcast it to systems managers [7]. Hackers also routinely read CERT reports. Thus it is important for system administrator to rapidly put in all software patches to determine vulnerabilities. Unfortunately given the complexity of many IT systems, and the rate at which patches are released, this is increasingly difficult to achieve without automated updating. Even then there are problems caused by incompatibilities resulting from the updated software. Hence need for multiple layers of defense in managing security threats to IT systems.

Inevitably, the best intrusion prevention system will fail. A system next line of resistance is intrusion detection and this has been the center of much examine in modern years [5]. This awareness is motivated by an amount of considerations, including the following.

1. If an intrusion is detected speedily enough, the intruder can be recognized and expelled from the system before any harm is done or any data are compromised [8]. Even if the exposure is not sufficiently timely to anticipate the intruder, the more rapidly that recovery can be achieved.
2. A successful intrusion detection system can serve as self-possession, so acting to thwart intrusions.
3. Intrusion detection enables the group of information about intrusion detection techniques that can be used to strengthen the intrusion prevention facility.

Intrusion recognition is based on assumption that the behavior of the intruders differs from that of a genuine user in ways that can be quantified [1]. Of course, we cannot anticipate that there will be a crunchy, exact distinction between an attack by an intruder and normal use of resources by an allowed user. Rather, we must look forward to there will be some overlap.

Figure suggests, in very abstracts terms, the nature of the task confronting the fashionable of an intrusion detection system. Although the distinctive behavior of an 'I' differs from the typical behavior of an official user, there is an overlap in these behaviors.

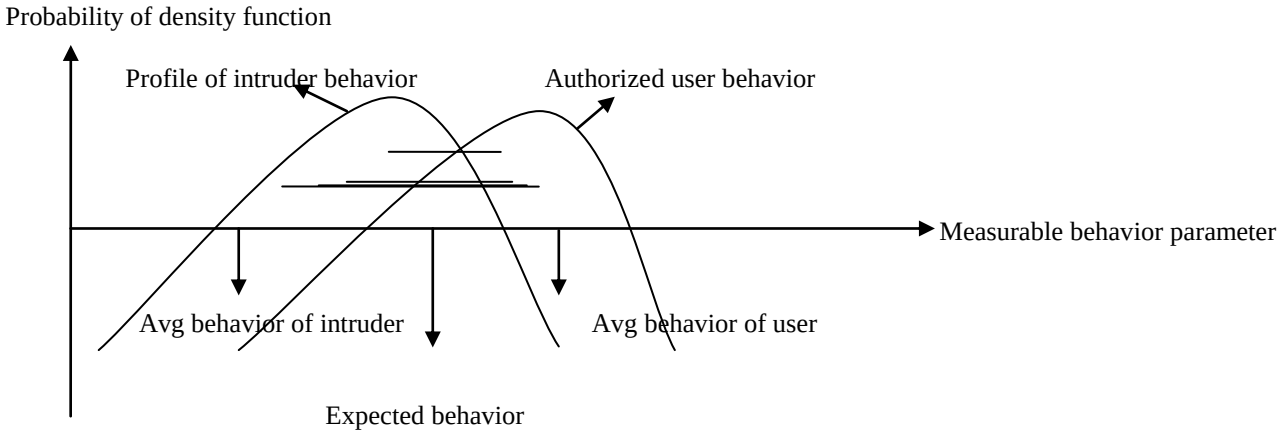

Fig 1: Profile of Behavior of Intruders and Authorized users

II.RELATED WORK

In [3] the author given intrusion detection model and how the packet sampling is done, for this he used various network security techniques in such a way that the selective sampling of packets must be compromised. In [2] the author explained about the implementation and design issues of campus intrusion detection system. In that how an organization or a campus should be protected for this intrusion detection system is responsible for authorized users'

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

entry. For providing high security he used the RSA algorithm with encryption and decryption standard and also [6] the authors given idea as how given idea as how intrusion detection system works in large scale networks. In [4] the author used artificial intelligence in intrusion detection systems for providing better security for the organization.

If an intrusion is detected speedily enough, the intruder can be recognized and expelled from the system before any harm is done or any data are compromised [8]. Even if the exposure is not sufficiently timely to anticipate the intruder, the more rapidly that recovery can be achieved. A successful intrusion detection system can serve as self-possession, so acting to thwart intrusions. Intrusion detection enables the group of information about intrusion detection techniques that can be used to strengthen the intrusion prevention facility.

III.RESEARCH METHODOLOGY

Intruder can attack in any way. For suppose an intruder wants to access some organization valuable information. If that particular organization is fully secured then, there is no way of stealing the information. If not, the problem rises. In our proposed system the security can be provided in such a way that the organizational network contains rule sets. According to the rule sets only the connection had made between the organization systems and other systems.

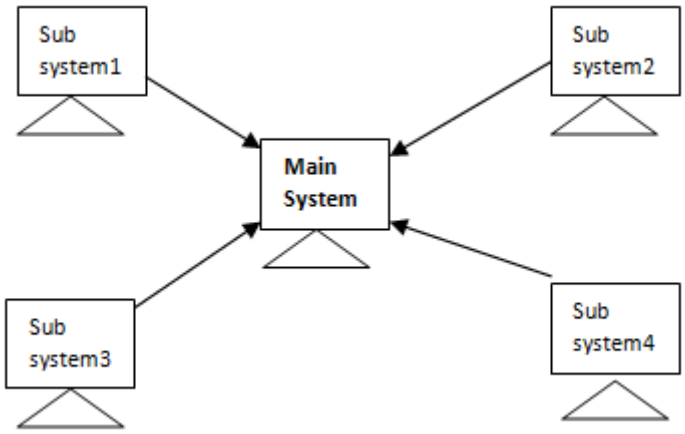

Fig 2: Main system & sub systems

If the intruder wants to access the organization information he should follow the correct rule sets defined by the organization. If it is not matched with the rule sets the main system will inform to the administrator saying that the intruder had made an attack on some specific system. The process can be shown in below diagram.

Thus a movable elucidation of intruder behavior, which will grasp more intruders, will also direct to a number of "false positives" or authorized users identified as 'I'. On the other hand, an attempt to limit false positives by a tight interpretation of intruder performance will lead to an increase in false negatives, or intruders not identified as intruders. Thus there is an element of negotiation and art in the practice of intrusion detection

This can be shown the below figure. For the intruder there is always a chance to attack the system, for that we need to provide a high level security. In this scenario we have the main system it will take care of all the organizational systems. For this we gave set of rule to follow. . According to the rule sets only the connection had made between the organization systems and other systems. i.e., if any system wants to communicate with these systems the system rule sets should match with the specific system rule sets then only the communication is possible between the systems.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

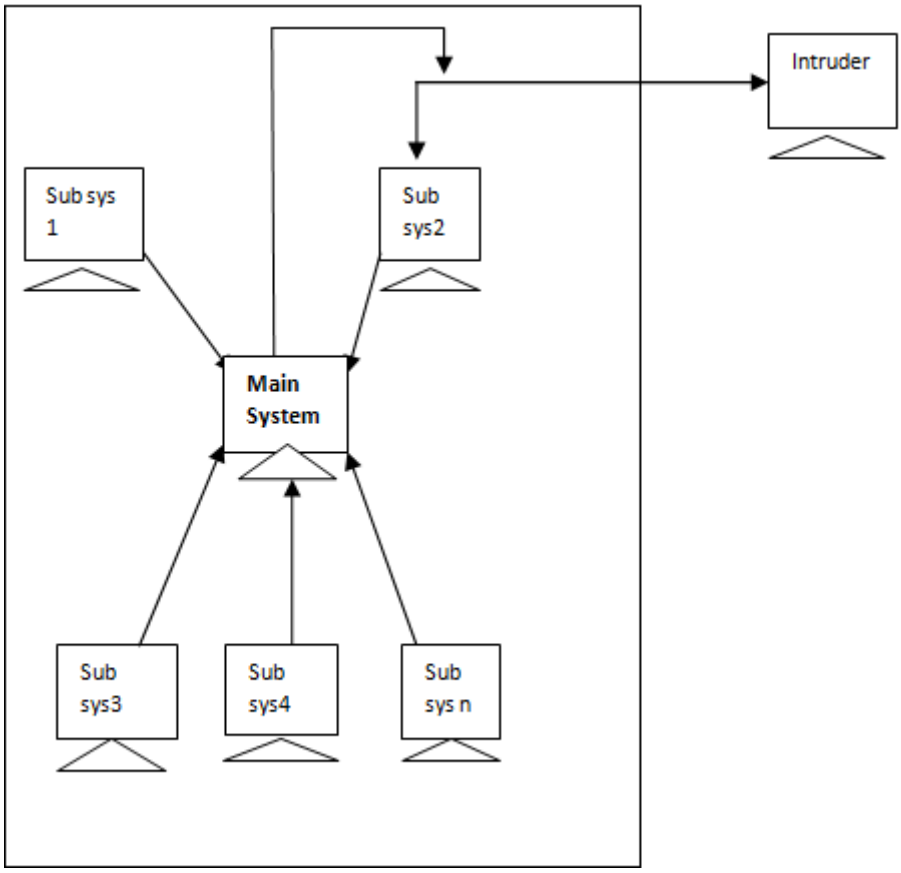

Fig: How the Intruder is identified.

Rule Sets: The TCP, HTTP rule sets will verify the system which would like to connect with the network. If any system wants to attack the any system in the network the main system will alerts and stops that system.

TCP Rule Set:

A rule is one line. A case containing rules may also contain comments: lines beginning with # are ignored.

Each rule contains an address, a colon, and a record of instructions, with no additional spaces. When tcpserver receives a connection from that address, it follows the instructions.

Addresses:

Tcpserver looks for rules with various addresses

1. $TCPREMOTEINFO@TCPREMOTEIP, if $TCPREMOTEINFO is set;
2. $TCPREMOTEINFO@=$TCPREMOTEHOST,
3. if $TCPREMOTEINFO is set and $TCPREMOTEHOST is set;
4. $TCPREMOTEIP;
5. =$TCPREMOTEHOST, if $TCPREMOTEHOST is set;
6. shorter and shorter prefixes of $TCPREMOTEIP ending with a dot;
7. shorter and shorter suffixes of $TCPREMOTEHOST starting with a dot, preceded by =, if $TCPREMOTEHOST is set;

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

8. =, if $TCPREMOTEHOST is set; and finally
9. The blank string.

tcpserver uses the first rule it finds. We should use the -p option to tcpserver if we rely on $TCPREMOTEHOST here. For example here are some rules.

joe@172.16.3.15:first
192.168.1.113: second
: Third
172.: forth.

If $TCPREMOTEIP is 192.168.0.68, tcpserver will follow the third instructions.
If $TCPREMOTEIP is 192.168.1.113, tcpserver will follow the second instructions.
If $TCPREMOTEIP is 172.16.3.15 and $TCPREMOTEINFO is bill, tcpserver will go after the fourth instructions.
If $TCPREMOTEIP is 172.16.3.15and $TCPREMOTEINFO is joe, tcpserver will follow the first instructions.
Instructions: The instructions in a rule have to begin with either allowed or deny. Deny tells tcpserver to drop the connection without running anything. For instance, the rule : deny

IV. SNORT ANALYSIS

This network intrusion detection and prevention system excels at traffic study and packet cataloguing on IP networks. During protocol analysis, content searching, and a variety of pre-processors, Snort detects thousands of worms, susceptibility make use of attempts, port scans, and other disbelieving behavior [10]. Snort uses a flexible rule-based language to describe traffic that it should gather or exceed, and a modular detection engine.
After verification made by the tcp rule set the end result also verified by the snort rules, based on snort result we can easily finds the intruder, so that the end system will be secured. This can be shown in below figure.

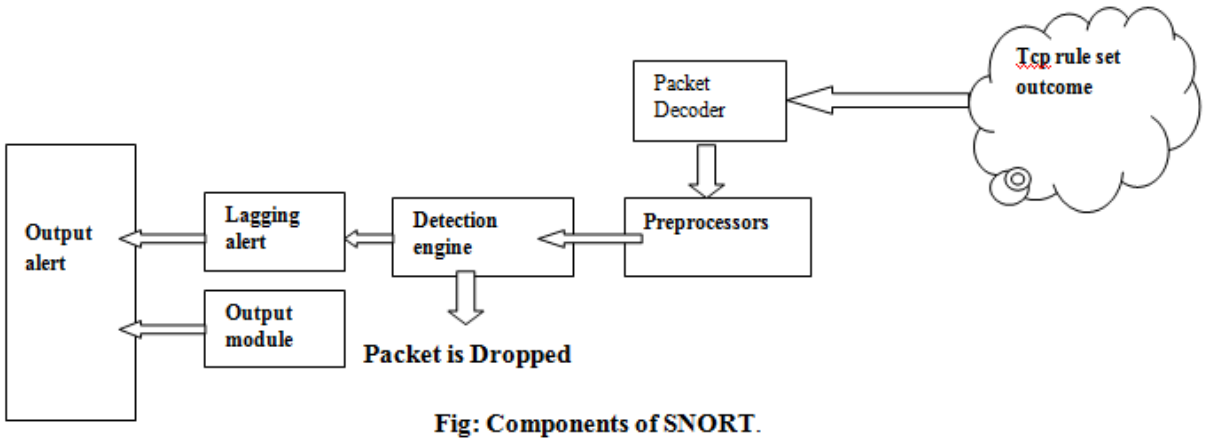

Fig: Components of SNORT.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

Table: Module Description

Name	Description
1.Packet Decoder	Prepares packets for processing
2. Preprocessors	Used to normalize protocol headers, detect anomalies, packet Reassembly and TCP stream re-assembly.
3.Detection Engine	Applies rules to packets.
4.Logging and Alerting System	Generates alert and log messages.
5.Output Modules	Process alerts and logs and generate final output

V.CONCLUSION

In this paper, we proposed a new intrusion detection mechanism. The proposed system easily detects the intruder's attack with the help of main system involvement, for this we given a certain rules to follow. If any intruder wants to attack the system the superior system will detects the attack made by the intruder.
We believe that our system could have a deterrent effect on attackers and realize the secure network environment.

REFERENCES

[1] Helio Mandes Salmon et al., "Intrusion detection system for wireless sensor networks using danger theory immune inspired techniques", International Journal of Wireless Information Networks, Vol.20(1), pp.39-66, 2013.
[2] Hu Ruipeng, "Design and Implementation of Campus Network Intrusion Detection System", International Conference on Intelligence Science and
Information Engineering, pp.507-510, 2011.
[3] Ezzat G Bakhoum, "Intrusion Detection Model based on selective packet sampling", Journal on Information Security, pp.1-12, 2011.
[4] Gulshan Kumar,Krishan Kumar, Monika Sachdeva, "The use of artificial intelligence Based techniques for intrusion detection", International Journal of Artificial Intelligence Review, Vol.34(4), pp.369-387, 2010.
[5] chun Jason xue et al., "variable length pattern matching fo hardwarenetwork intrusion detection system", International Journal of signal processing system, Vol.59(1), pp.85-93, 2010.
[6] Daxin Tian,Yanherng Liu,Yang Xiang, "Large scale network intrusion detection based on Distributed learning algorithm", International Journal of
information Security, Vol.8(1), pp.25- 35, 2009.
[7] Gerald Tripp, "A parallel string Matching engine for use in high speed Network intrusion detection systems", International Journal of Computer Virol, Vol.2(1), pp.21-34, 2006.
[8] Dong Seong Kim, Ha-Nam Nguyen, Jong Sou Park, "Genetic Algorithm to Improve SVM Based Network Intrusion Detection System", IEEE,Vol.2, pp.155-158, 2005.
[9] D. Anderson, T. Frivold, A. Valdes, "Next-generation intrusion detection expert system (NIDES)", Technical report, SRI- CSL-95-07, SRI International, Computer Science Lab, May 1995.
[10**]** http://manual.snort.org/node27.html.

BIOGRAPHY

1.**B.Subbarayudu** completed his M.Tech from JNTU Anantapur and he has 1 year of teaching experience. He is presently working in IT Dept as an Assistant Professor in St Martin's Engineering College, Hyderabad. His area of interest is Network Security, Computer Networks, Mobile Computing and Compiler Design

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

2**. Dr.R.Ch.A.Naidu** completed his M.Tech, Ph.D from University of Mysore, Mysore and Andhra University, Vishakhapatnam respectively. He has more than 13 years of teaching experience. He is presently working in CSE Dept as a Professor in St Martin's Engineering College, Hyderabad. He has life membership in professional bodies like ISTE, CSI. His area of interest is Network security, Computer networks, Digital Image processing, Data base management systems .He has life membership in professional bodies like ISTE, CSI.

3.**K.Meghana** completed her B.Tech from JNTU Kakinada in the year of 2014. Now she is doing her M.Tech in VIT, Vishakapatnam in CSE department. She published 3 papers in international journal. Her interested areas are Network security, Data management systems, Automata and Compiler design.