ISSN No. 0976-5697

Volume 3, No. 7, Nov-Dec 2012

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Snort Based Network Traffic Anomaly Detector to Improve the Performance of Intrusion Detection System

G.V.Nadiammai*
Department of Computer Science
Karpagam University Coimbatore, TN, India
gvnadisri@gmail.com

M.Hemalatha
Head, Department of Computer Science
Karpagam University Coimbatore, TN, India
csresearchhema@gmail.com

Abstract: Data Mining is the way of identifying the hidden patterns from large amount of data. It is commonly used in a marketing, surveillance, fraud detection and scientific discovery. Intrusion occurs when anyone tries to gain the access of normal user and even exploits attack over the network. Instruction detection deals with the concept of analyzing all sorts of illegal action towards data. IDS and IPS has equal significance in research community. Snort is a software tool that is designed to capture the network packets. It performs pre- processing by its own without the indulgence of security experts. And also it generates alarm if any anomaly packet is found with the help of in-build rules. In this paper snort is used to detect the attack from (one week data) the network packets. The number of attacks detected by misuse based IDS is compared with the enhanced IDS approach obtained by combining anomaly and misuse based IDSs and shows that the improved IDS with NETAD performs well by detecting 133 attacks out of 180 (73%) attacks after training on one week attack free traffic. KDD Cup 99 dataset is taken for the study.

Keywords: Intrusion Detection, Snort, Network Traffic Anomaly Detector (NETAD), KDD Cup99 dataset and Real time traffic data.

I. INTRODUCTION

Due to the rapid growth of internet it is very hard to handle large volumes of data. This in turn results in unauthorized access, disaster, enabling worms, viruses, etc. in this situation we need to impose a stream of security policies such as firewall, encryption, antivirus software, and etc. obviously ids serves as a defense tool against attacks/intrusion. It is software/ hardware enables to detect the user behavior over the network.

A. Intrusion Detection System:

The main task of intrusion detection systems is to protect a computer system by detecting an attack and possibly repelling it. Detecting hostile attacks depends on the number and type of appropriate actions. An Intrusion Detection System was first coined by Anderson (1980) [1] in a technical report. Intrusion prevention requires a well-selected combination of "baiting and trapping" aimed at both investigations of threats. Diverting the intruder's attention from protected resources is another task. Both the real system and a possible trap system are constantly monitored. Data generated by intrusion detection systems is carefully examined which is the main task of each IDS and detecting possible attacks.

Once an intrusion has been detected, IDS provides an alert representing administrators about the situation. The next step is carried out by the administrators or the IDS itself [2]. An IDS is an element of the security policy. Among various IDS tasks, intruder recognition is one of the fundamental tasks. It can be useful in the forensic research of incidents and installing appropriate patches to enable the detection of future attack attempts targeted on specific persons or resources. However the number of threats seems to be increasing continuously. So IDS has become an integral part of security measures within an organization [3, 4]. Intrusion detection may sometimes produce false alarms, for example as a result of malfunctioning network interface or sending attack description or signatures via email.

B. IDS Techniques

There are two basic types of IDS namely HIDS [5] and NIDS. For each of the two types, there are four basic techniques used to detect intruders: anomaly detection and misuse detection.

C. Anomaly Detection:

Designed to uncover abnormal patterns of behavior, the IDS establishes a baseline of normal usage patterns, and anything that widely deviates from it gets flagged as a possible intrusion. What is considered to be an anomaly can vary, but normally, we think as an anomaly any incident that occurs on frequency greater than or less than two standard deviations from the statistical norm. It identifies anomalies as deviations from "normal" behavior and automatically detects any deviation from it, flagging the latter as suspect. Thus these techniques identify new types of intrusion as deviations from normal usage. It is an extremely powerful and novel tool but a potential drawback is the high false alarm rate, i.e. previously unseen system behaviors may also be recognized as anomalies, and hence flagged as potential intrusions. If a user in the graphics department suddenly starts accessing accounting programs or compiling code, the system can properly alert its administrators.

D. Misuse Detection:

Here each instance in a data set is labeled as normal" or "intrusive" and a learning algorithm is trained over the labeled data. These techniques are able to automatically retrain intrusion detection models on different input data that include new types of attacks. Unlike signature-based IDS, models of misuse are created automatically and can be more sophisticated and precise than manually created signatures. They have high degree of accuracy in detecting known attacks and their variants. Their disadvantage is that they cannot detect unknown intrusions and they rely on signatures extracted by human experts. This method uses specifically known patterns of unauthorized behavior to predict and detect subsequent similar attempts. These specific patterns are called signatures. Data mining techniques such as association, classification, clustering and neural networks have been used in intrusion detection [6, 7].

E. Protecting IDS against attacks:

Once the ids are compromised, the attacker stops the working of it. To avoid this we can perform the following methods [8, 9],

a. Do not run the ids itself because through network server the attack can exploit the system.
b. If snort is performed in a particular platform then all the latest security policies must be imposed.
c. Configure the machine.
d. If we are running snort on a Linux machine then we must use filter to stop the unusual packets.
e. Snort can also run in a host without assigning the IP address by avoiding anybody from accessing it. To achieve this we need to use two interfaces one with IP and other without IP address.

Thus, high level of human interaction is needed during modeling the intrusion detection system. To solve the work load in preprocessing the snort [10] has been used to automatically analyze the traffic. Based on this technique, a hybrid IDS (Snort+NETAD) is developed according to the environment where it is deployed and validated through simulation experiments. The new signatures are generated from anomalies detected by snort based approach. This new approach automatically simulates NIDS to detect similar anomalous attacks in future. . Association rule is one among the widely used method to build IDS [11].

This paper is organized as follows: Section 2 explains the working of snort. Section 3 provides the information about the data set used and its features in detail. Sections 4 describe the performance evaluation of various snort based approach. Section 5 refers to conclusion & future enhancement.

II. METHODOLOGY

Here the misuse based and anomaly based approach has been taken for the study. Comparison is made based on its performance by analyzing the detection rate of snort of its own with the anomaly based algorithms. Here Snort requires frequent revision in order to capture new attacks from existing. Snort has predefined rules and also we can able to update any rules in future. Under anomaly based approach, we have four types of statistical methods like PHAD, NETAD, ALAD and LERAD respectively [12]. Among that NETAD is taken for the study. We can see it one by one,

A. SNORT:

Snort is developed by Martin Roesch, a software engineer [13, 14] in 1990 attempts to detect attacks occurred in his computer. It is a fast; rule based and misuse detection methods written in a specific language. It is possible to integrate new functionalities within the snort during the time of compilation. It makes use of text files or tcpdump files to store the packets. Tcpdump is a kind of tool or program that is used to capture the various hosts in a network. Snort consists of the following five components:

a. Packet Decoder:

Packet decoder captures the packets from different interfaces that are transmitted over network. Then it sends for further preprocessing. The interface may be Ethernet, Point to Point Protocol, SLIP and so on.

b. Pre- Processor:

It is a kind of component or plug-ins added with snort to sort and arrange the packet information in order to analyze the severity of the packets. It uses the packet header for checking anomalies and if any found it generates alerts.

c. Detection Engine:

Detection engine plays the vital role in snort. It performs the detection with the help of the rule specified within the snort. First, it applies the rule on the database and finds if any anomalies have been occur. If not, it keeps as such otherwise it includes appropriate rule for the anomaly packets to make the administrator to handle the situation.

d. Logging & Alerting System:

All logs are placed in a text files (tcpdump files). While packets passed over the network it has been automatically stored in the log files by default. We can even change the location of log files and alerts. Depending upon the work of detection engine with the packets, alerts will be generated.

e. Output modules:

Output plug-ins saves the output generated by logging and alerting system of snort. It controls the alarm produced by preprocessor, detection engine and logging & alerting system.

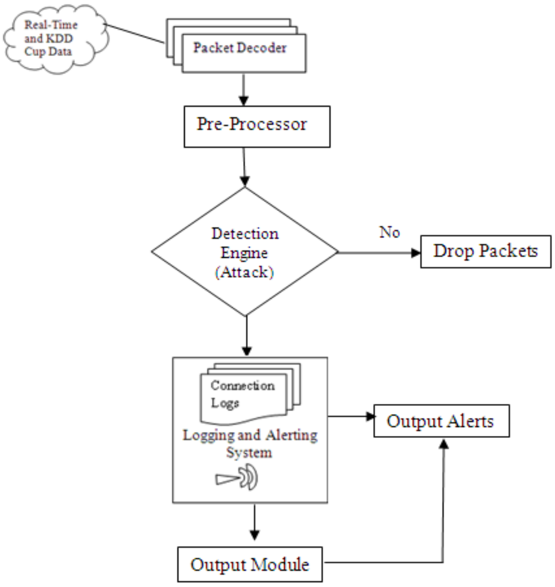


Figure 1 Architecture of SNORT

An illustration of snort rule structure is shown in the fig 2. The first field relates to the action field which may be alert, activate, log and so on. When the values matches, then the action are taken as response (alert). Alert specifies that the match is found. The next field handles the protocol such as tcp, udp and icmp. The protocol in this example is http. Fourth one holds the source address as ip address and port number. Any any implies that the packets come from any ip address and tcp port.

“**Alert** tcp any any ->[a.b.0.0/06, c.d.e.0/14] 90 (msg:"**ATTACKS** conf/httpd.conf attempt"; nocase; sid: 1384; flow: to_server, established; content:"conf/httpd.conf"; [...])”

Figure 2 Snort Rule Structure

B. Network Traffic Anomaly Detector (NETAD):

Network Traffic Anomaly Detector is the second kind of anomaly based approach. It works as that of PHAD the only difference is that, it posses two phases. First, to filter the incoming traffic sequence is filtered to differentiate the beginning of sequence. Second is the modeling phase. The filtering phase models the traffic from 98 to 99%. Then the remaining packet enters the modeling phase. The second phase models 5 types of packets [15] such as,

a. All IP packets
b. All TCP packets (if protocol= TCP (6))
c. TCP SYN (if TCP and flags =SYN (2))
d. TCP data (if TCP and flags = ACK (16))
e. TCP data for port number between 0 and 255 (if TCP and ACK and DP1 (high order bit of destination port) =0)

Anomaly score is calculated using

$$tn_a\ (1\text{-}r/256)/r+t_in(n_i+r/W) \qquad (1)$$

Where, n_a is the number of normal packets from where the last anomaly found.256 is the constant coefficient value

IV. DATASET DESCRIPTION

Both the combination of real time traffic from LAN network and KDD cup are chosen in this study. KDD cup 99 dataset [16] has been used to analyze the network intrusion detection and it is developed by Stolfo et al based upon DARPA dataset from MIT Lincoln Laboratory as an evaluation benchmark. The dataset involves approximately 4 million connection records with 41 related features & 21 attack types. All different attacks fall into 4 major categories as dos, probe, u2r and r2l attacks labeled as attack and normal type. The attack free data from the kdd cup and LAN network are taken as training set and one week attack data from kdd cup as testing set. Attacks can be described as

A. ***Dos Attack-*** It is a kind of attack where the attacker makes processing time of the resources and memory busy so as to avoid legitimate user from accessing those resources.

B. ***U2R Attack-*** Here the attacker sniffs the password or makes some kind of attack to access the particular host in a network as a legitimate user. They can even promote some vulnerability to gain the root access of the system.

C. ***R2L Attack-*** Here the attacker sends a message to the host in a network over remote system and makes some vulnerability.

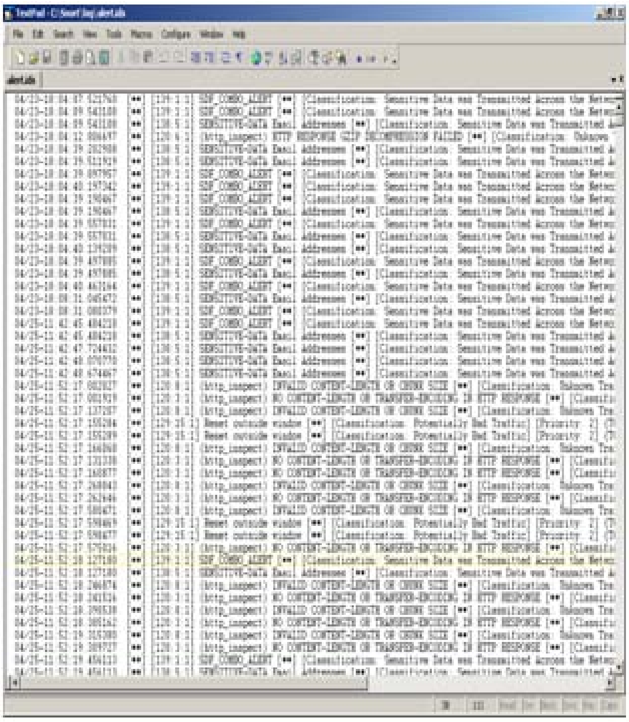
D. ***Probe Attack-*** Attacker will scan the network to gather information and would make some violation in future.

Table 1 Name Of The Attacks Classified Under 4 Groups

Denial of Service	Back, land, neptune, pod, smurf, teardrop
Probes	Satan, ipsweep, nmap, port sweep
Remote to Local	ftp_write, , imap, guess_passwd phf, spy, warezclient, multihop, warezmaster
User to Root	buffer_overflow, load module, Perl, root kit

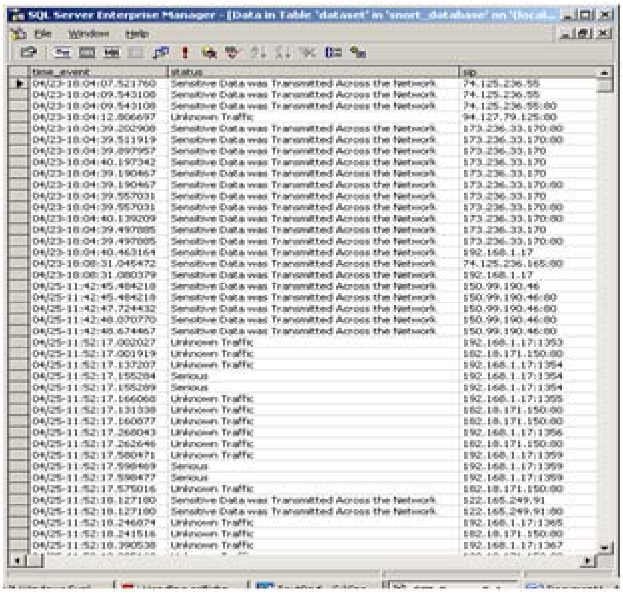
V. EXPERIMENTAL RESULTS

Hybrid IDS is developed to overcome the human interaction towards preprocessing. Most of the evaluation on intrusion detection is based on proprietary data and results are not reproducible. To solve this problem, KDD cup 99 [17] dataset has been used. Lack of public data availability is one of the major issues during evaluation of intrusion detection system. Totally out of 500 instances, 320 instances involved in training phase and remaining 180 instances are taken for testing phase. Analysis is done based on performance of Snort and performance of Snort + NETAD. Fig 3 specifies the data stored within the snort before pre processing (Captured packet over network). Fig 4 shows the data after pre processing which has been arranged in a manner as time of packets that are captured, source IP and destination addresses, etc.



```
04/23-18:04:07.521760  [**] [139:1:1] SDF_COMBO_ALERT [**] [Classification: Sensitive Data was Transmitted Across the Netw
04/23-18:04:09.543108  [**] [139:1:1] SDF_COMBO_ALERT [**] [Classification: Sensitive Data was Transmitted Across the Netw
04/23-18:04:09.543108  [**] [138:5:1] SENSITIVE-DATA Email Addresses [**] [Classification: Sensitive Data was Transmitted A
04/23-18:04:12.806697  [**] [120:6:1] (http_inspect) HTTP RESPONSE GZIP DECOMPRESSION FAILED [**] [Classification: Unknown
04/23-18:04:39.202908  [**] [138:5:1] SENSITIVE-DATA Email Addresses [**] [Classification: Sensitive Data was Transmitted A
04/23-18:04:39.511919  [**] [138:5:1] SENSITIVE-DATA Email Addresses [**] [Classification: Sensitive Data was Transmitted A
04/23-18:04:39.897957  [**] [139:1:1] SDF_COMBO_ALERT [**] [Classification: Sensitive Data was Transmitted Across the Netw
04/23-18:04:40.197342  [**] [139:1:1] SDF_COMBO_ALERT [**] [Classification: Sensitive Data was Transmitted Across the Netw
04/23-18:04:39.190467  [**] [139:1:1] SDF_COMBO_ALERT [**] [Classification: Sensitive Data was Transmitted Across the Netw
04/23-18:04:39.190467  [**] [138:5:1] SENSITIVE-DATA Email Addresses [**] [Classification: Sensitive Data was Transmitted A
04/23-18:04:39.557031  [**] [139:1:1] SDF_COMBO_ALERT [**] [Classification: Sensitive Data was Transmitted Across the Netw
04/23-18:04:39.557031  [**] [138:5:1] SENSITIVE-DATA Email Addresses [**] [Classification: Sensitive Data was Transmitted A
04/23-18:04:40.139209  [**] [138:5:1] SENSITIVE-DATA Email Addresses [**] [Classification: Sensitive Data was Transmitted A
04/23-18:04:39.497885  [**] [139:1:1] SDF_COMBO_ALERT [**] [Classification: Sensitive Data was Transmitted Across the Netw
04/23-18:04:39.497885  [**] [138:5:1] SENSITIVE-DATA Email Addresses [**] [Classification: Sensitive Data was Transmitted A
04/23-18:04:40.463164  [**] [139:1:1] SDF_COMBO_ALERT [**] [Classification: Sensitive Data was Transmitted Across the Netw
04/23-18:08:31.045472  [**] [138:5:1] SENSITIVE-DATA Email Addresses [**] [Classification: Sensitive Data was Transmitted A
04/23-18:08:31.080379  [**] [139:1:1] SDF_COMBO_ALERT [**] [Classification: Sensitive Data was Transmitted Across the Netw
04/25-11:42:45.484218  [**] [139:1:1] SDF_COMBO_ALERT [**] [Classification: Sensitive Data was Transmitted Across the Netw
04/25-11:42:45.484218  [**] [138:5:1] SENSITIVE-DATA Email Addresses [**] [Classification: Sensitive Data was Transmitted A
04/25-11:42:47.724432  [**] [138:5:1] SENSITIVE-DATA Email Addresses [**] [Classification: Sensitive Data was Transmitted A
04/25-11:42:48.070770  [**] [138:5:1] SENSITIVE-DATA Email Addresses [**] [Classification: Sensitive Data was Transmitted A
04/25-11:42:48.674467  [**] [138:5:1] SENSITIVE-DATA Email Addresses [**] [Classification: Sensitive Data was Transmitted A
04/25-11:52:17.002027  [**] [120:8:1] (http_inspect) INVALID CONTENT-LENGTH OR CHUNK SIZE [**] [Classification: Unknown Tra
04/25-11:52:17.001919  [**] [120:3:1] (http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE [**] [Classifi
04/25-11:52:17.137207  [**] [120:8:1] (http_inspect) INVALID CONTENT-LENGTH OR CHUNK SIZE [**] [Classification: Unknown Tra
04/25-11:52:17.155284  [**] [129:15:1] Reset outside window [**] [Classification: Potentially Bad Traffic] [Priority: 2] {T
04/25-11:52:17.155289  [**] [129:15:1] Reset outside window [**] [Classification: Potentially Bad Traffic] [Priority: 2] {T
04/25-11:52:17.166068  [**] [120:8:1] (http_inspect) INVALID CONTENT-LENGTH OR CHUNK SIZE [**] [Classification: Unknown Tra
04/25-11:52:17.131338  [**] [120:3:1] (http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE [**] [Classifi
04/25-11:52:17.160877  [**] [120:3:1] (http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE [**] [Classifi
04/25-11:52:17.268043  [**] [120:8:1] (http_inspect) INVALID CONTENT-LENGTH OR CHUNK SIZE [**] [Classification: Unknown Tra
04/25-11:52:17.262646  [**] [120:3:1] (http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE [**] [Classifi
04/25-11:52:17.580471  [**] [120:8:1] (http_inspect) INVALID CONTENT-LENGTH OR CHUNK SIZE [**] [Classification: Unknown Tra
04/25-11:52:17.598469  [**] [129:15:1] Reset outside window [**] [Classification: Potentially Bad Traffic] [Priority: 2] {T
04/25-11:52:17.598477  [**] [129:15:1] Reset outside window [**] [Classification: Potentially Bad Traffic] [Priority: 2] {T
04/25-11:52:17.575016  [**] [120:3:1] (http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE [**] [Classifi
04/25-11:52:18.127180  [**] [139:1:1] SDF_COMBO_ALERT [**] [Classification: Sensitive Data was Transmitted Across the Netw
04/25-11:52:18.127180  [**] [138:5:1] SENSITIVE-DATA Email Addresses [**] [Classification: Sensitive Data was Transmitted A
04/25-11:52:18.246874  [**] [120:8:1] (http_inspect) INVALID CONTENT-LENGTH OR CHUNK SIZE [**] [Classification: Unknown Tra
04/25-11:52:18.241516  [**] [120:3:1] (http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE [**] [Classifi
04/25-11:52:18.390538  [**] [120:8:1] (http_inspect) INVALID CONTENT-LENGTH OR CHUNK SIZE [**] [Classification: Unknown Tra
04/25-11:52:18.385162  [**] [120:3:1] (http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE [**] [Classifi
04/25-11:52:19.315300  [**] [120:8:1] (http_inspect) INVALID CONTENT-LENGTH OR CHUNK SIZE [**] [Classification: Unknown Tra
04/25-11:52:19.389727  [**] [120:3:1] (http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE [**] [Classifi
04/25-11:52:19.454113  [**] [139:1:1] SDF_COMBO_ALERT [**] [Classification: Sensitive Data was Transmitted Across the Netw
04/25-11:52:19.454113  [**] [138:5:1] SENSITIVE-DATA Email Addresses [**] [Classification: Sensitive Data was Transmitted A
```

Figure 3 Before Pre-Processing the data is stored in text files


SQL Server Enterprise Manager - [Data in Table 'dataset' in 'snort_database' on '(local...
File
Window
Help

time_event	status	sip
04/23-18:04:07.521760	Sensitive Data was Transmitted Across the Network	74.125.236.55
04/23-18:04:09.543108	Sensitive Data was Transmitted Across the Network	74.125.236.55
04/23-18:04:09.543108	Sensitive Data was Transmitted Across the Network	74.125.236.55:80
04/23-18:04:12.806697	Unknown Traffic	94.127.79.125:80
04/23-18:04:39.202908	Sensitive Data was Transmitted Across the Network	173.236.33.170:80
04/23-18:04:39.511919	Sensitive Data was Transmitted Across the Network	173.236.33.170:80
04/23-18:04:39.897957	Sensitive Data was Transmitted Across the Network	173.236.33.170
04/23-18:04:40.197342	Sensitive Data was Transmitted Across the Network	173.236.33.170
04/23-18:04:39.190467	Sensitive Data was Transmitted Across the Network	173.236.33.170
04/23-18:04:39.190467	Sensitive Data was Transmitted Across the Network	173.236.33.170:80
04/23-18:04:39.557031	Sensitive Data was Transmitted Across the Network	173.236.33.170
04/23-18:04:39.557031	Sensitive Data was Transmitted Across the Network	173.236.33.170:80
04/23-18:04:40.139209	Sensitive Data was Transmitted Across the Network	173.236.33.170:80
04/23-18:04:39.497885	Sensitive Data was Transmitted Across the Network	173.236.33.170
04/23-18:04:39.497885	Sensitive Data was Transmitted Across the Network	173.236.33.170:80
04/23-18:04:40.463164	Sensitive Data was Transmitted Across the Network	192.168.1.17
04/23-18:08:31.045472	Sensitive Data was Transmitted Across the Network	74.125.236.165:80
04/23-18:08:31.080379	Sensitive Data was Transmitted Across the Network	192.168.1.17
04/25-11:42:45.484218	Sensitive Data was Transmitted Across the Network	150.99.190.46
04/25-11:42:45.484218	Sensitive Data was Transmitted Across the Network	150.99.190.46:80
04/25-11:42:47.724432	Sensitive Data was Transmitted Across the Network	150.99.190.46:80
04/25-11:42:48.070770	Sensitive Data was Transmitted Across the Network	150.99.190.46:80
04/25-11:42:48.674467	Sensitive Data was Transmitted Across the Network	150.99.190.46:80
04/25-11:52:17.002027	Unknown Traffic	192.168.1.17:1353
04/25-11:52:17.001919	Unknown Traffic	182.18.171.150:80
04/25-11:52:17.137207	Unknown Traffic	192.168.1.17:1354
04/25-11:52:17.155284	Serious	192.168.1.17:1354
04/25-11:52:17.155289	Serious	192.168.1.17:1354
04/25-11:52:17.166068	Unknown Traffic	192.168.1.17:1355
04/25-11:52:17.131338	Unknown Traffic	182.18.171.150:80
04/25-11:52:17.160877	Unknown Traffic	182.18.171.150:80
04/25-11:52:17.268043	Unknown Traffic	192.168.1.17:1356
04/25-11:52:17.262646	Unknown Traffic	182.18.171.150:80
04/25-11:52:17.580471	Unknown Traffic	192.168.1.17:1359
04/25-11:52:17.598469	Serious	192.168.1.17:1359
04/25-11:52:17.598477	Serious	192.168.1.17:1359
04/25-11:52:17.575016	Unknown Traffic	182.18.171.150:80
04/25-11:52:18.127180	Sensitive Data was Transmitted Across the Network	122.165.249.91
04/25-11:52:18.127180	Sensitive Data was Transmitted Across the Network	122.165.249.91:80
04/25-11:52:18.246874	Unknown Traffic	192.168.1.17:1365
04/25-11:52:18.241516	Unknown Traffic	182.18.171.150:80
04/25-11:52:18.390538	Unknown Traffic	192.168.1.17:1367

Figure 4 After Pre-Processing the data is stored in text files (time, status, Source IP address, Destination IP Address and so on)

Snort is tested on real time traffic and simulated dataset (one week data including attack) and attacks detected are listed day by day. The files have been downloaded from [30] and LAN network. Attack detected on daily order is shown in the below figure 5. Snort has detected 77 attacks out of 180 attacks without adding any anomaly based approaches.

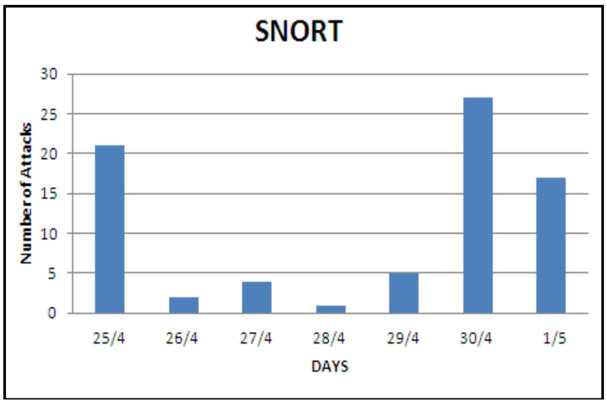
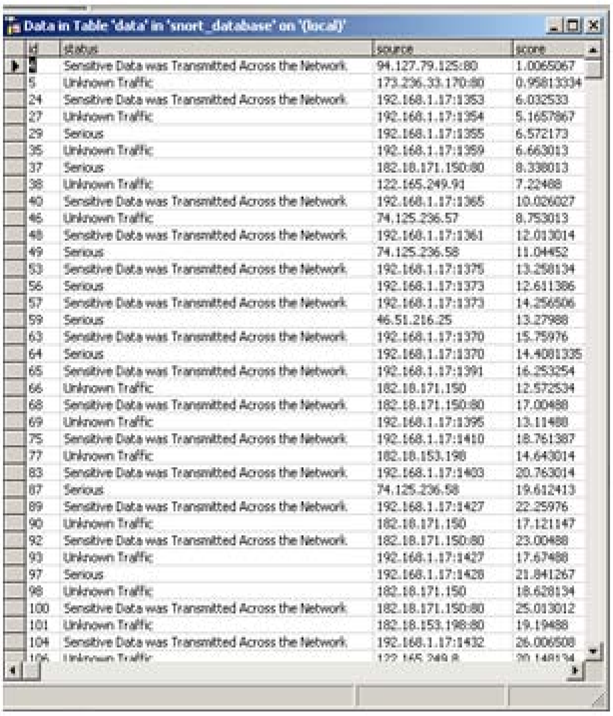


Figure 5 Attacks detected by Snort on a daily basis



id	status	source	score
[illegible]	Sensitive Data was Transmitted Across the Network	94.127.79.125:80	1.0065067
5	Unknown Traffic	173.236.33.170:80	0.95813334
24	Sensitive Data was Transmitted Across the Network	192.168.1.17:1353	6.032533
27	Unknown Traffic	192.168.1.17:1354	5.1657867
29	Serious	192.168.1.17:1355	6.572173
35	Unknown Traffic	192.168.1.17:1359	6.663013
37	Serious	182.18.171.150:80	8.338013
38	Unknown Traffic	122.165.249.91	7.22488
40	Sensitive Data was Transmitted Across the Network	192.168.1.17:1365	10.026027
46	Unknown Traffic	74.125.236.57	8.753013
48	Sensitive Data was Transmitted Across the Network	192.168.1.17:1361	12.013014
49	Serious	74.125.236.58	11.04452
53	Sensitive Data was Transmitted Across the Network	192.168.1.17:1375	13.258134
56	Serious	192.168.1.17:1373	12.611386
57	Sensitive Data was Transmitted Across the Network	192.168.1.17:1373	14.256506
59	Serious	46.51.216.25	13.27988
63	Sensitive Data was Transmitted Across the Network	192.168.1.17:1370	15.75976
64	Serious	192.168.1.17:1370	14.4081335
65	Sensitive Data was Transmitted Across the Network	192.168.1.17:1391	16.253254
66	Unknown Traffic	182.18.171.150	12.572534
68	Sensitive Data was Transmitted Across the Network	182.18.171.150:80	17.00488
69	Unknown Traffic	192.168.1.17:1395	13.11488
75	Sensitive Data was Transmitted Across the Network	192.168.1.17:1410	18.761387
77	Unknown Traffic	182.18.153.198	14.643014
83	Sensitive Data was Transmitted Across the Network	192.168.1.17:1403	20.763014
87	Serious	74.125.236.58	19.612413
89	Sensitive Data was Transmitted Across the Network	192.168.1.17:1427	22.25976
90	Unknown Traffic	182.18.171.150	17.121147
92	Sensitive Data was Transmitted Across the Network	182.18.171.150:80	23.00488
93	Unknown Traffic	192.168.1.17:1427	17.67488
97	Serious	192.168.1.17:1428	21.841267
98	Unknown Traffic	182.18.171.150	18.628134
100	Sensitive Data was Transmitted Across the Network	182.18.171.150:80	25.013012
101	Unknown Traffic	182.18.153.198:80	19.19488
104	Sensitive Data was Transmitted Across the Network	192.168.1.17:1432	26.006508
106	Unknown Traffic	122.165.249.8	20.148134

Figure 6 Anomaly score calculated for each packet

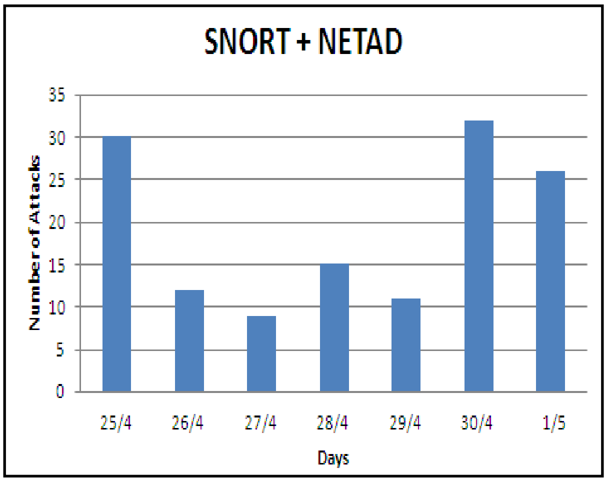


Figure 7 Attacks detected by Snort +NETAD on a daily basis

Above fig 6 represents the anomaly score that are calculated for Snort+NETAD implementation. In case of NETAD, anomaly score is calculated for each packet that is stored within snort. If the anomaly score is less than those data can be label as less severe. Data with high score is taken as attack one. Fig 7 shows the graphical representation of Snort +NETAD on their own and results in improved intrusion detection system. After adding Snort+NETAD, the ids perform better while compared with other Snort based IDS method. The number of attacks detected by Snort+NETAD increased from 77 to 133 in Snort+ NETAD version of the IDS. Instead of using Snort alone it is advisable to include the statistical algorithm along with Snort improves the accuracy level by means of detection rate.

VI. CONCLUSION & FUTURE SCOPE

In this paper, the open source snort tool has been used to detect the network attacks. Based on the application the vulnerability level varies but it cannot be solved with the help of rules. But it can be done in network security. Snort detects attacks at application layer in case of transformation of packets. It provides temporary solution for identifying malicious packets and useful in many organization. The misuse and anomaly algorithm is combined to obtain the strength of both and thereby achieving an improved intrusion detection system. It has been proven by the above result that Snort +NETAD detects 133 attacks from 180 attacks (73%).

In future, various statistical methods can be combined with snort for better performance.

VII. REFERENCES

[1]. J.P.Anderson, Computer Security Threat Monitoring & surveillance, Technical Report, James P Anderson Co., Fort Washington, Pennsylvania, 1980.

[2]. R Bace. Intrusion detection. Indianapolis, USA: Macmillan Technical Publishing; 2000.

[3]. K.Scafone, P.Mell, Guide to intrusion detection and prevention system (IDPs), NIST Special Publication, pp.800-94, 2007.

[4]. R. Bace, P.Mell, Intrusion detection systems, NIST Special Publication on intrusion detection Systems, pp. 800-831, 2001.

[5]. L.Ertoz, E.Eilertson, A.Lazarevic, P.Tan, J.Srivastava, Kumar, et al, The MINDS- Minnesota intrusion detection system, *Next* generation data mining, MIT Press, 2009.

[6]. B. Ben Sujatha., V.Kavitha, Survey on intrusion detection approaches, International Journal of Advanced Research in Computer Science, vol. 3, no. 1, pp.363-371, 2012.

[7]. Alok Ranjan, S.Ravindra Hegadi, Emerging Trends in Data Mining for Intrusion Detection, International Journal of Advanced Research in Computer Science, Vol. 3(2), pp.279-281, 2012.

[8]. G.D Kurundkar, N.A Naik and S.D Khamithar, “Network Intrusion Detection using Snort”, International Journal of Engineering Research and Application(IJERA) vol.2, issue 2, pp-1288-1296, 2012.

[9]. J.Gomez, C. Gil, N. Padilla, R. Barios and C. Jimenez, “Design of a Snort-Based Hybrid Intrusion Detection System” pp. 515–522,Springer-LNCS,2009.

[10]. M.Roesch Snort – Lightweight Intrusion Detection System for Networks, In Proceedings of the 13th LISA conference of USENIX association, 1999.

[11]. D. Barbara, J. Couto, S. Jajodia, L. Popyack, and N. Wu, ADAM: Detecting Intrusions by Data Mining, In Proceedings of IEEE Workshop Information Assurance and Security, 2001.

[12]. M.Mahoney, IDS Distribution, 2003.

[13]. Russell, Snort intrusion detection, 2.0. *Rockland, MA:* Syngress Publishing, Inc.; 2003.

[14]. Snort Users Manual 2.6.1; Available at:www.snort.org/docs/snort_manual/2.6.1/snort_manual.pdf, 2006

[15]. MA. AydIn, AH. Zaim, KG. Ceylan, A hybrid intrusion detection system design for computer network security, Computer Electrical Engineering; Vol.35:pp.517–526, 2009.

[16]. R.P. Lippmann and J. Haines, Analysis and Results of the 1999 DARPA Off-Line Intrusion Detection Evaluation, Proceedings of Third International Workshop on Recent Advances in Intrusion H. Debar, L. Me, and S.F. Wu, eds., pp. 162-182, 2000.

[17]. KDD Cup 99 intrusion Detection Data set. Available from: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html

Short Bio Data for the Author

G.V.Nadiammai completed M.C.A., and currently pursuing Ph.D in computer science at Karpagam University under the guidance of Dr.M.Hemalatha, Professor and Head, Dept. of Software System, Karpagam University, Coimbatore. Published four papers in International Journals and presented three papers in international conference. Area of research is Data Mining, Network Security and Knowledge Discovery.

Dr. M. Hemalatha completed M.Sc., M.C.A., M. Phil., Ph.D (Ph.D, Mother Terasa women's University, Kodaikanal). She is Professor & Head and guiding Ph.D Scholars in Department of Computer Science at Karpagam University, Coimbatore. Twelve years of experience in teaching and published more than hundred papers in International Journals and also presented more than eighty papers in various national and international conferences. She received best researcher award in the year 2012 from Karpagam University. Her research areas include Data Mining, Image Processing, Computer Networks, Cloud Computing, Software Engineering, Bioinformatics and Neural Network. She is a reviewer in several National and International Journals.