IJCSC 0973-7391 Volume 7 • Number 2 March 2016 - Sept 2016 pp. 16-19 available online at www.csjournalss.com

Hybrid IDS System Using Snort

OKASHA ELDOW*,PUNIT LALWANI**,M.B.POTDAR**
*GTU PG SCHOOL, GANDHINAGAR
**BHASKARACHARYA INSTITUTE FOR SPACE APPLICATIONS AND GEO-INFORMATICS
**BISAG, GANDHINAGAR, GUJARAT, INDIA
okashamahi@gmail.com

Abstract: SNORT an open source system which is used very widely by so many companies ,agencies and also single users to protect their network , as snort is a signature based system so it requires regularly updating to keep our system aware about the different types of attack .anomaly detection based system are systems which is making profile for each and every attack and then try to measure to the deviation o these attacks to detect any possibility of the attacks so it is better than signature based as it could be updated automatically .

In the paper after we have been looking deeply inside snort and adding a preprocessor to the snort which it could fulfill our system , after that testing the system and showing some good results comparing to snort signature based system

Keywords: intrusion detection systems; IDS; SNORT; Anomaly detection.

I. INTRODUCTION

the intrusion detection systems has been classified into
-NIDS network based intrusion detection system
-HIDS host based intrusion detection systems

NIDS are systems which is systems that monitoring our whole network and all the packets which is possible comes in or goes out .

HIDS are systems which it has been installed into a single host so it would be possible to monitor all packets into that host or also the logs of that host and try to figure out if there any possibility of intruder to the host machine[1] .

I. INTRUSION DETECTION TECHNIQUES

There are some of techniques which has been used by IDS widely

- Misuse based or signature based
- Anomaly detection based
- Hybrid technique

Firstly Misuse based is the one of the famous IDS techniques which is used signatures o the packets and match it with the defined signatures which it has already saved in our system . it is good techniques as much as we have known types of attacks and we have set of signatures of these attacks . but the problem is the attacks types are everyday racing and increasing so it requires all the time new signatures for the new attacks so one of the circumstances is the regularly update of the signature set . secondly Anomaly detection technique which is a technique of ids systems it is duty to make a profile for each attacks and try to find out these packets or even if there is any possibility of deviation from these profiles . the good thing about these technique is it don't need any regularly updating as much as the signature based as long as it colud make a profile and count the deviations [2].

III. RELATED WORK

Intrusion Detection Systems :-
There are lots of intrusion detection systems which it has been used widely

1. SNORT
2. SURICATA
3. BRO

SNORT
Snort is an open source system which is been used very widely by so many organizations , the large user community of snort is because o the flexibility of snort . you can get snort from the snort website [3]
The components of snort

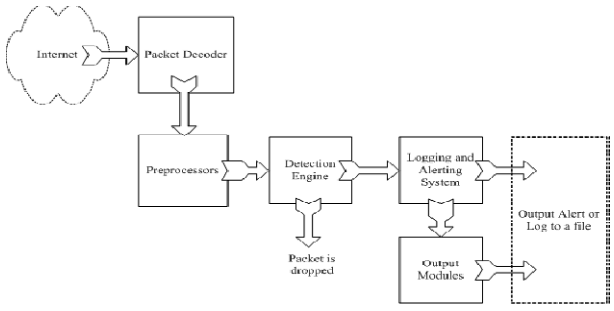

Figure III-1snort component

DOI: 10.090592/IJCSC.2016.104

the above figure is showing the component of the Snort system [4].

packet decoder :-

the packet are coming through the traffic to go to the preprocessor paret to processed or to the detection engine , it is coming through interfaces which it could be a wire or wireless traffic or whatever interface .

preprocessor part

it is the part before the detection engine which it has so many preprocessors or plugins which is making snort a flexible system , applying so many techniques for the packets make better performance to know the intruder in our systems .

Detection engine

the detection engine part is one of the most important parts of snort as the pattern matching algorithm and there are different parameters for the good detection engine

- The rules and it is possibility to fulfill our targets
- The bandwidth of the internal buses
- The performance and high configuration of the sensor which snort has been deployed

IV. PROPOSED SYSTEM

In the next figure we could see the structure of the proposed system

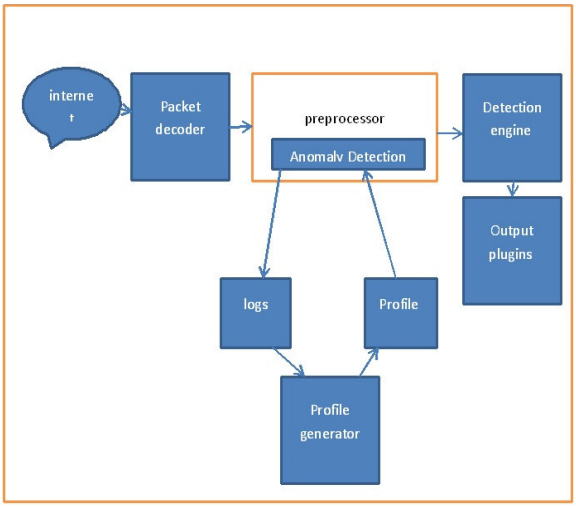

Figure 4-1.proposed system

the main idea of our system is to add a preprocessor to the snort which it could make our snort engine possible to use anomaly techniques ti find out the anomalies and intruders , but before that there are different parameters for snort anomaly techniques for writing the rules .

number of TCP packets
in TCP packets
out TCP packets
NO of TCP packets in LAN
No of UDP datagrams
in UDP datagrams
out UDP datagrams
no of UDP datagrams in LAN
No of ICMP packets
out ICMP packets
in ICMP packets
No of ICMP packets in LAN
No of TCP packets with SYN and ACK flags
out TCP packets (port 80)
in TCP packets (port 80)
out UDP datagrams (port 53)
in UDP datagrams (port 53)
out IP traffic [kB/s]
in IP traffic [kB/s]
out TCP traffic (port 80) [kB/s]
in TCP traffic (port 80) [kB/s]
out UDP traffic [kB/s]
in UDP traffic [kB/s]
out UDP traffic (port 53) [kB/s]
in UDP traffic (port 53) [kB/s]

in the coming part the proposed approach for the system which is contain two sensors , first sensor is signature based and the second sensor is snort which it has anomaly detection preprocessor .

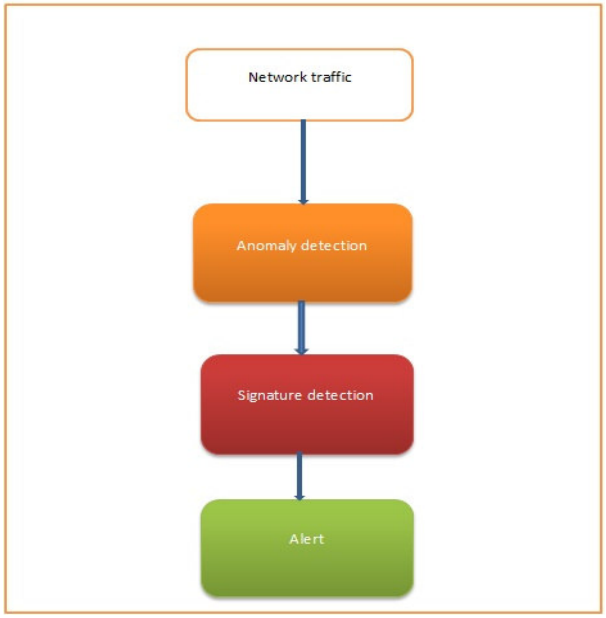

Figure 4-2.proposed approch

The work low is shown in the next figure showing the parts of our system which is containing two sensors one is signature based and other snort with anomaly detection preprocessor and , both of these systems has been tested with DARPA 1999 dataset and after that showing the results of both databases and make a comparison .

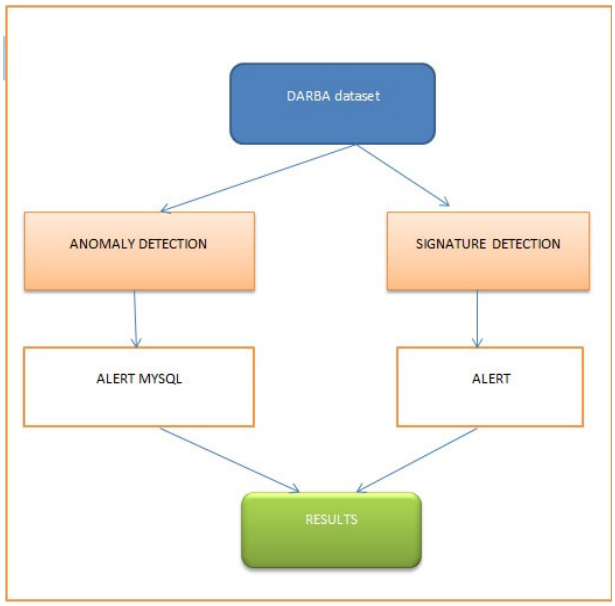

Figure4-3.work flow

Experiment (A)

Firstly we injected the sensor which it works with snort without anomaly preprocessor .
DARPA dataset
The next image showing the snort database

```
mysql> select * from signature limit 30;
+--------+-----------------------------------------+--------------+--------------+---------+----------+-----+
| sig_id | sig_name                                | sig_class_id | sig_priority | sig_rev | sig_sid  | sig |
gid |
+--------+-----------------------------------------+--------------+--------------+---------+----------+-----+
----+
|      1 | Snort Alert [1:1000001:0]               |            0 |         NULL |    NULL |  1000001 |
  1 |
|      2 | Snort Alert [1:100000160:0]             |            1 |            2 |       2 | 100000160 |
  1 |
|      3 | Snort Alert [1:100000241:0]             |            2 |            1 |       2 | 100000241 |
  1 |
|      4 | WEB-CGI redirect access                 |            3 |            2 |       7 |      895 |
  1 |
|      5 | ATTACK-RESPONSES Invalid URL            |            3 |            2 |      10 |     1200 |
  1 |
|      6 | ATTACK-RESPONSES 403 Forbidden          |            3 |            2 |       7 |     1201 |
  1 |
|      7 | WEB-FRONTPAGE /_vti_bin/ access         |            4 |            2 |       8 |     1288 |
  1 |
|      8 | WEB-IIS fpcount access                  |            4 |            2 |       9 |     1013 |
  1 |
|      9 | WEB-MISC /doc/ access                   |            4 |            2 |       6 |     1560 |
  1 |
|     10 | WEB-CGI calendar access                 |            3 |            2 |       5 |      882 |
  1 |
|     11 | WEB-MISC http directory traversal       |            3 |            2 |       5 |     1113 |
  1 |
|     12 | Snort Alert [1:100000185:0]             |            4 |            2 |       1 | 100000185 |
  1 |
|     13 | WEB-MISC search.dll access              |            4 |            2 |       6 |     1767 |
  1 |
|     14 | WEB-MISC RBS ISP /newuser access        |            4 |            2 |       9 |     1493 |
```

Image 4-IV-1snort database

Alert by protocol showing 99 signature

```
mysql> select count(distinct signature) from event as e, iphdr as i where e.cid=i.cid and ip_proto=6;
+--------------------------+
| count(distinct signature) |
+--------------------------+
|                       99 |
+--------------------------+
1 row in set (1 min 45.28 sec)
```

Image 4-IV-2alert by protocol signature sensor

Alert by dates in the next image

```
mysql> select date(timestamp),count(distinct sig_name) from event as e, signature as s where s.sig_id=e.signatu
re group by date(timestamp);
+----------------+--------------------------+
| date(timestamp) | count(distinct sig_name) |
+----------------+--------------------------+
| 1999-03-29     |                       16 |
| 1999-03-30     |                       13 |
| 1999-03-31     |                       39 |
| 1999-04-01     |                       53 |
| 1999-04-02     |                       38 |
| 1999-04-03     |                       30 |
| 1999-04-05     |                       32 |
| 1999-04-06     |                       57 |
| 1999-04-07     |                       43 |
| 1999-04-08     |                       58 |
| 1999-04-09     |                       76 |
| 1999-04-10     |                       27 |
+----------------+--------------------------+
12 rows in set (0.23 sec)
```

Image 4-IV-3alert by date signature based

Experiment (B)

The second experiment we injected the snort sensor with DARPA 1999 dataset and shown result

Alert by protocol shown 111 signatures

```
mysql> select count(distinct signature) from event as e, iphdr as i where e.cid=
i.cid and ip_proto=6;
+--------------------------+
| count(distinct signature) |
+--------------------------+
|                      111 |
+--------------------------+
1 row in set (3 hours 28 min 11.56 sec)
```

Image4-IV-4 alert by protocol anomaly sensor

Alert by date in the anomaly detection signatures

```
mysql> select date(timestamp), count(distinct sig_id) from event as e,signature
as s where s.sig_id=e.signature group by date(timestamp);
+----------------+----------------------+
| date(timestamp) | count(distinct sig_id) |
+----------------+----------------------+
| 1999-03-29      |                   26 |
| 1999-03-30      |                   22 |
| 1999-03-31      |                   47 |
| 1999-04-01      |                   61 |
| 1999-04-02      |                   47 |
| 1999-04-03      |                   37 |
| 1999-04-05      |                   41 |
| 1999-04-06      |                   65 |
| 1999-04-07      |                   51 |
| 1999-04-08      |                   66 |
| 1999-04-09      |                   85 |
| 1999-04-10      |                   37 |
+----------------+----------------------+
12 rows in set (0.01 sec)
```

Image 4-5alert by date anomaly sensor

V. RESULTS

after injecting both systems and seen the results of both ,some sort of comparison has to be done , the results we achieved we could use it to fulfill this comparison

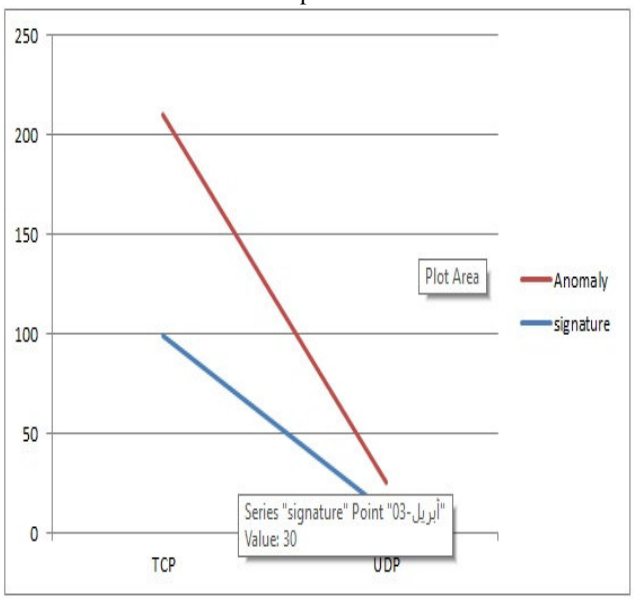

Chart 5-V-1Signature Vs Anomaly According To The Protocol

The above chart shown the number of tcp / udp protocols in both system .
now another comparison also according to the date of the a

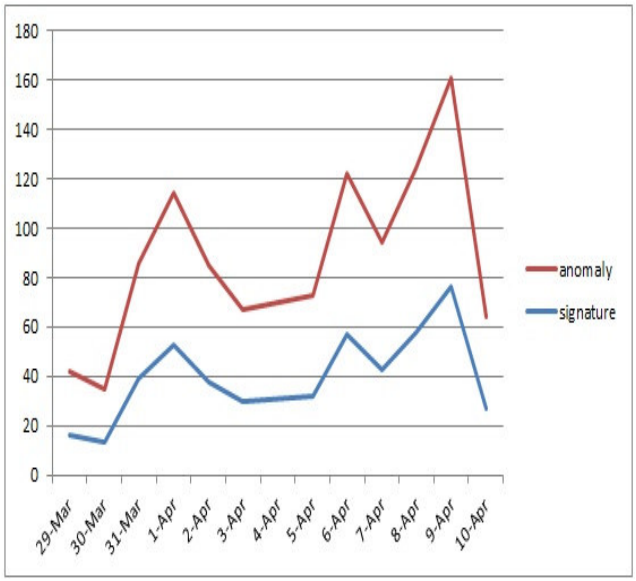

Chart 5-V-2.Signature Vs Anomaly According To The Date

The above chart shown up the comparison between both

system according to the date .

VI. CONCLOUSION

We have shown the implementation of anomaly detection preprocessor after we added it to snort preprocessor part , after that testing the system using DARPA data set . to validate the work we also injected our dataset to another system which is works under the signature based . the results showing high performance of the system which it has the anomaly detection . we have done some comparison to come up with these reults .
Future work is try to test the system using the live traffic and also using of a machine learning tool would be better to validate the results .

VII. REFERENCE

1.Karadkar, C., et al., *Review on Implementation of Intrusion Detection in Physical Network.*
2. Eldow, okasha*Computer network security ids tools and techniques (snort/suricata).*. 2016, international journal of scientific and research publications, pp. 593-597.
3. *Www.snort.org.*
4. *Rehman, r.u., intrusion detection systems with snort: advanced ids techniques using snort, apache, mysql, php, and acid. 2003: prentice hall professional.*