International Journal of Database Theory and Application
Vol.9, No.4 (2016), pp.61-70
http://dx.doi.org/10.14257/ijdta.2016.9.4.05

A Review on Network Intrusion Detection System Using Open Source Snort

Sakshi Sharma and Manish Dixit

Department of CSE& IT
MITS
Gwalior, India
Sharmasakshi1009@gmail.com, dixitmits@gmail.com

Abstract

In the present scenario most of the organization depends on the internet for their communication, storage and protection of their valuable data and other internal resources from the unauthorized access as the importance of internet is increasing rapidly the chances of attacks also increases in the ratio. Intrusion Detection System plays a very important role in network security. Its main role in the network is to help computer system to create and deal with network attacks. An IDS acts as a key component to ensuring the safety of any network or system on which it runs. IDS works on the concept of investigating all the incoming packets for the detection of any malicious activity. This is a survey paper on the various enhancements over the decades on IDS. Snort is a lightweight and open source software which used signature based IDS. In the survey, we used BASE for providing graphical interface for displaying the result. Its used world widely in Intrusion Detection and Prevention.

Keywords*: IDS, HIDS, NIDS, Network analysis*

1. Introduction

An intrusion detection system is a solution for security to provide protection of the weaknesses which occur in computer systems during any activities.

Its work on the basis of these steps.

1. Collect data from a computer system.
2. Analyze these data.
3. Find security relevant events.
4. If there are any malicious events, then generate alarms.
5. Present the report to the admin [1].

In 1987 when Dorothy Denning published an intrusion detection model after that people start working in the field of network security. This intrusion detection system works on the real time data and motivated by four factors.

1. For fixing the most existing security flaws which present in the existing system.
2. Mainly, many attractive and secure features missing in the existing system.
3. Development of an extremely secure system is extremely difficult.
4. Most secure system is also abuses in by the insiders who misuse their privileges.

We can apply some security against the security attacks on networks its involve basically three steps.

- Prevention:- Prevent before damage.
- Detection:- Detect presence of any attack during the current.
- Mitigation:- Reacting to the attack.

Here in figure thickness of the arrow shows the amount of information to be transmitted from one system to another [4].

ISSN: 2005-4270 IJDTA

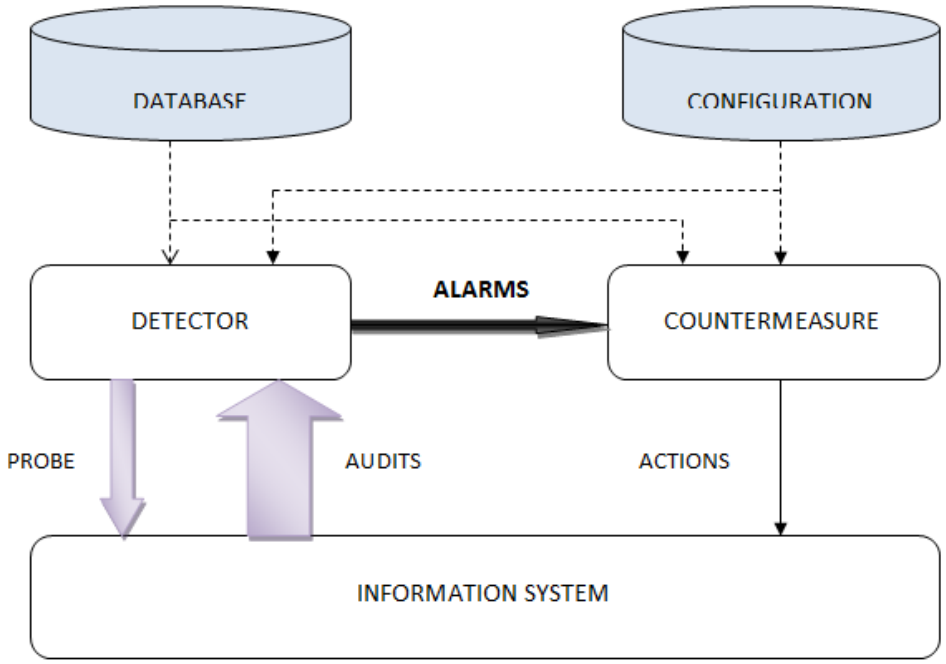


Figure 1. Working of Intrusion Detection System

2. Components of Intrusion Detection System

Intrusion detection system works on the monitoring of the events occur in the computer system or network and fetch the data for the predefined rules from the database and analyzing the events for the malicious content or signs of intrusion and maintain the integrity, confidentiality, authentication of the data. For this purpose IDS consists of the following components.

2.1 Data Preprocessor

Data pre-processor is dedicated to the collection or auditing of data from desired sources and provided these data to the next component which is responsible for further operations. It transforms the data from user access pattern to network packet level features and this formatted data used by the analyzer.

2.2 Analyzer (Intrusion Detector)

The analyzer or intrusion detector is the core component which performs analysis on the audit data and check for the attacks. Data mining, pattern matching, soft computing, machine learning and various statistical techniques used as an intrusion detector. It is one of the most researched components which determines the capability or overall strength of the system.

2.3 System Profile (DataBase/ Knowledge Base)

The system profile is used to describe the normal and abnormal user behavior. It is the database of the audit information, attacks, configuration information about the current state of the system and events that are going to happen on the system.

2.4 Response Engine

The reponse engine contains the reaction mechanism and decide how to react whenever analyzer detects an attack. Based on these mechanism system decide either to raise an alert without blocking the source of the attack or block the source address for the particular period of time. These all action depends on the predefined security rules or policy of the network.

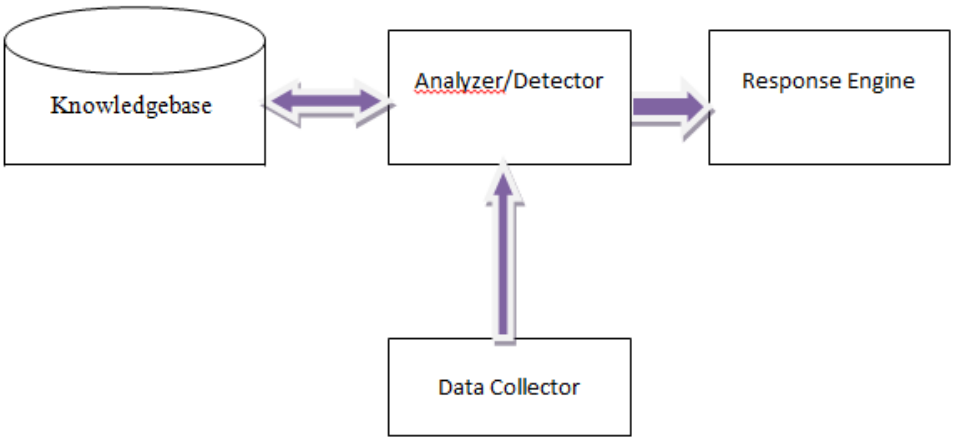
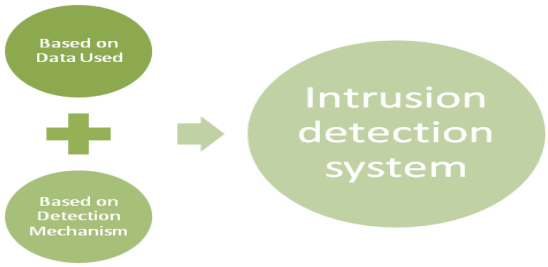


Figure 2. A Typical IDS with its Component [5]

3. Classification of Intrusion Detection System

Intrusion detection system classified in different categories based on the detection mechanism used or data source used.[5]



1. Based on Data Source Used

It classified system based on data which used as an input to the system. It classified in two sections.

I. **Host Based IDS:** Host intrusion detection system used for monitoring the host. Its consist of an agent which perform analysis for any event, host file, system registry, log files, operating system attributes for intrusive event. Its operated on host for detecting the malicious activities. [6]

II. **Network Based IDS:** Network intrusion detection system used for monitoring the network traffic for malicious activity. It works in the wide network and attempts to find any newly generated attack. Traffic on the network consist of any connectionless or connection oriented connection. Connection-oriented use TCP and connectionless use UDP protocol.[7]

Comparison between HIDS and NIDS

Host Based IDS	Network Based IDS

• Limited in scope. • Monitor host related activities. • Responds after a suspicious entry. • Host dependent. • Bandwidth independent. • Overload. • Slow down the hosts that have IDS clients installed. • Detects local attacks before they hit the network. • Well-suited for encrypted and switches environment. • A powerful tool for analyzing a possible attack because of relevant information in the database. • Low false positive rate. • Require no additional hardware. • Better for detecting attacks from inside and those that would miss by NIDS.	• Broad in scope. • Monitor network log files. • Near real-time response. • Host Independent. • Bandwidth dependent. • No overload. • Slow down the networks that have IDS clients installed. • Detects network attacks, as the payload is analyzed. • Not suitable for encrypted and switches network. • Does not perform normally detection of complex attacks. • High false positive rate. • Lower rate of ownership. • Better for detecting attacks from outside and those that would miss by HIDS.

2. Based on the Detection Mechanism [5] [8]

I. Misuse Based Intrusion Detection: It detects malicious code based on the specific known patterns (which is known as a signature). These stored patterns match against the current activity if there is a match then alarm is raised.

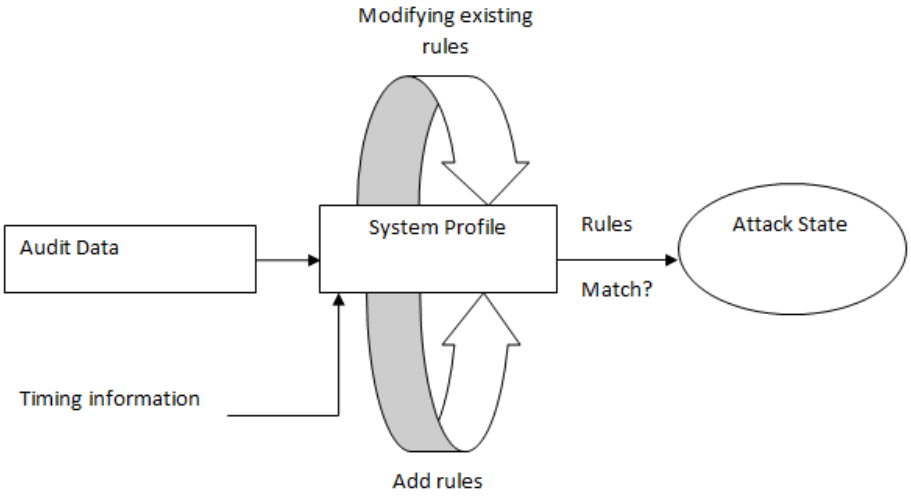


Figure 3. Typical Misuse Detection System

II. Anomaly Based Intrusion Detection: It detects the malicious code based on the "normal user profile" which used as a base line. If there is any different behaviour from base lined so alarm is raised.

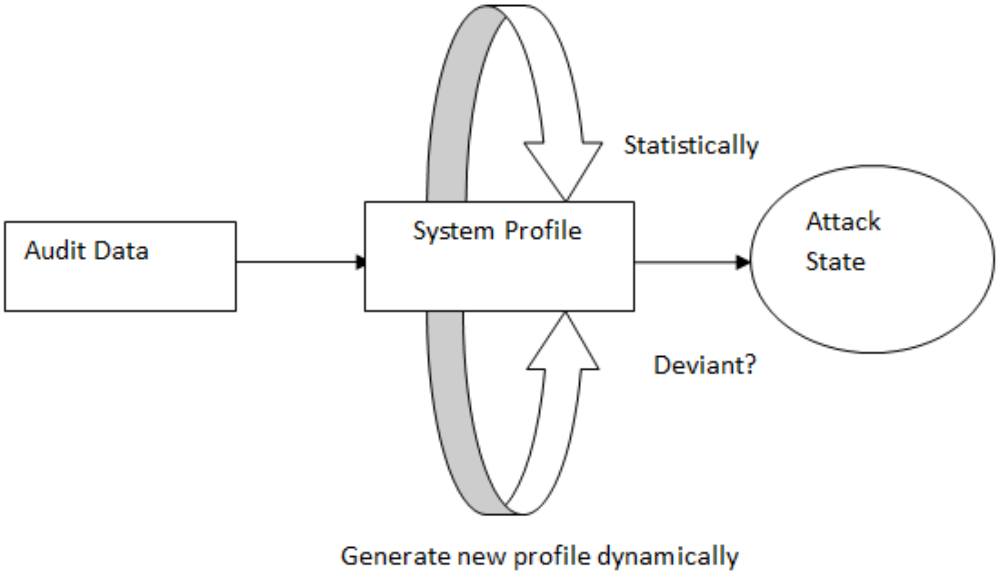


Figure 4. Typical Anomaly Detection System

I. **Hybrid Intrusion Detection System:** Hybrid system suggested the approach consisting of both misuse detection and anomaly detection. It combines the positive things of both techniques. It detects known attacks using misuse detection and detects unknown/new attacks using anomaly detection.

4. Tools For IDS Implementation

For implementing signature based IDS we need to install some network security tools, Snort, BASE, MySQL. When we used Snort for detection purpose, it matches traffic against the rule set which stored in the database. MySQL used for the Back - End Analysis of the database. BASE makes Front-End Analysis easier using Graphical representation.

4.1 Snort

Snort is a light weighted, open source network intrusion detection and prevention system used to analyze real time traffic against different types of attacks based on the rule set. Snort rule can be written in any language and easy to modify.[9] Snort is consisting of multiple components for detecting a particular attack and display the output these all components work together.[10]

- Packet Decoder
- Preprocessors
- Detection Engine
- Logging and Alerting System
- Output Modules

4.1.1. Packet Decoder

It takes packets from different types of network interfaces and prepares those packets for the preprocessing or to be sent to the detection engine. The interfaces may be Ethernet, SLIP, PPP and so on.

4.1.2. Preprocessors

These are components or plug-ins that can be combined with Snort to modify or arrange data packets before those packets reach to the detection engine perform some operation to find out if the packet is being used by an intruder.

4.1.3. The Detection Engine

The detection engine is the major component of Snort. It's used to detect if there is any malicious activity exists in a packet. The detection engine uses Snort rules for this activity.

4.1.4. Logging and Alerting System

Working of logging and altering system depends on the output of the previous component. It used to log the activity and generate the alert based on the detection engine output. Logs are kept in simple text files, tcpdump -style files or some other form.

4.1.5. Output Modules

Output modules or plug-ins performed different operations on the output generated by the logging and alerting system of Snort.

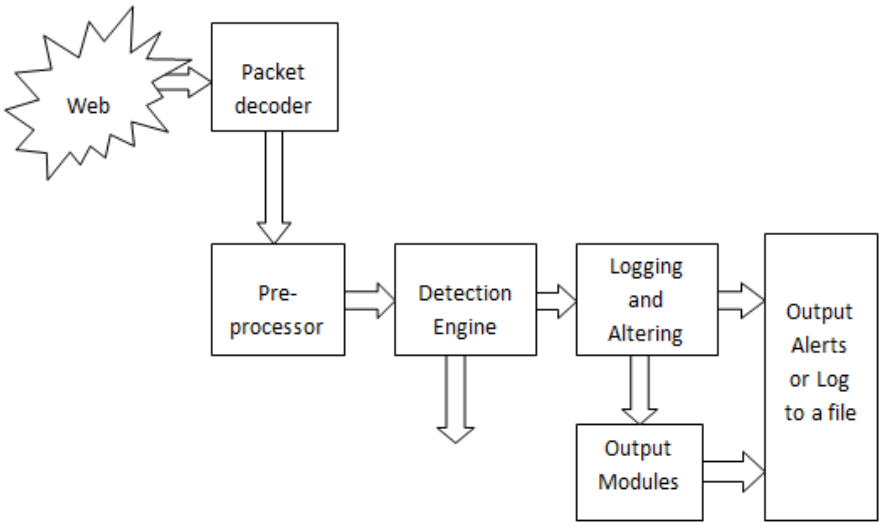


Figure 5. Component of Snort

In the figure given below shows the Running status of the Snort in the IDS mode. It provides details of network data (no. of packets, types of protocol, capture IP addresses *etc.*). By writing the command on the command prompt.

E.g. snort –c /etc/snort/snort.conf

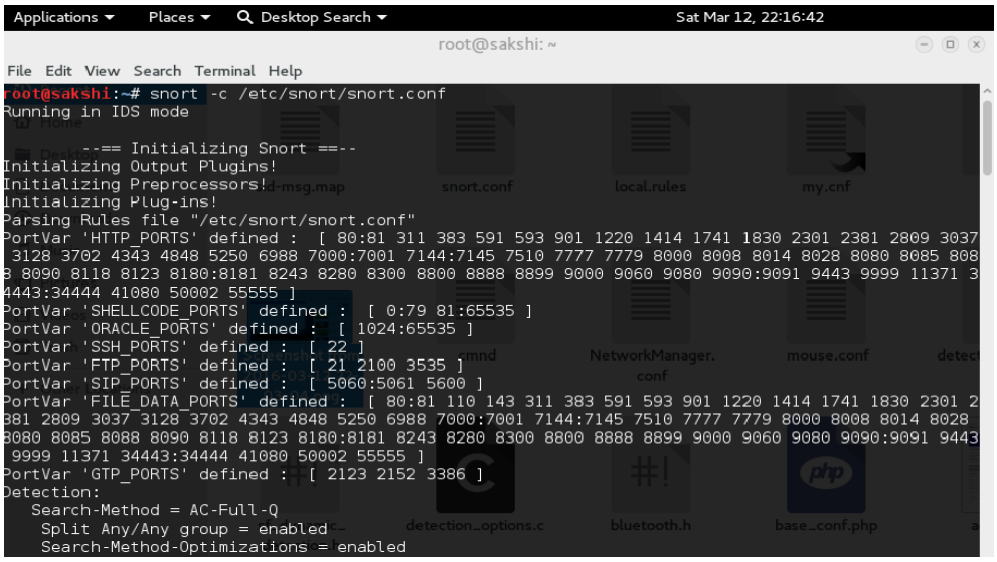


Figure 6. Snort Running in Snort Mode

4.2 BASE[10]

BASE is the Basic Analysis and Security Engine. It is based on the code from the Analysis Console for Intrusion Databases (ACID) project. This application provides a web front-end to query and analyze the alerts coming from a SNORT IDS system. It is a Graphical interface written in PHP used to display the alerts generate by SNORT.

In the given figure BASE shows the result of snort in graphical form. So user can easily analysis the output.

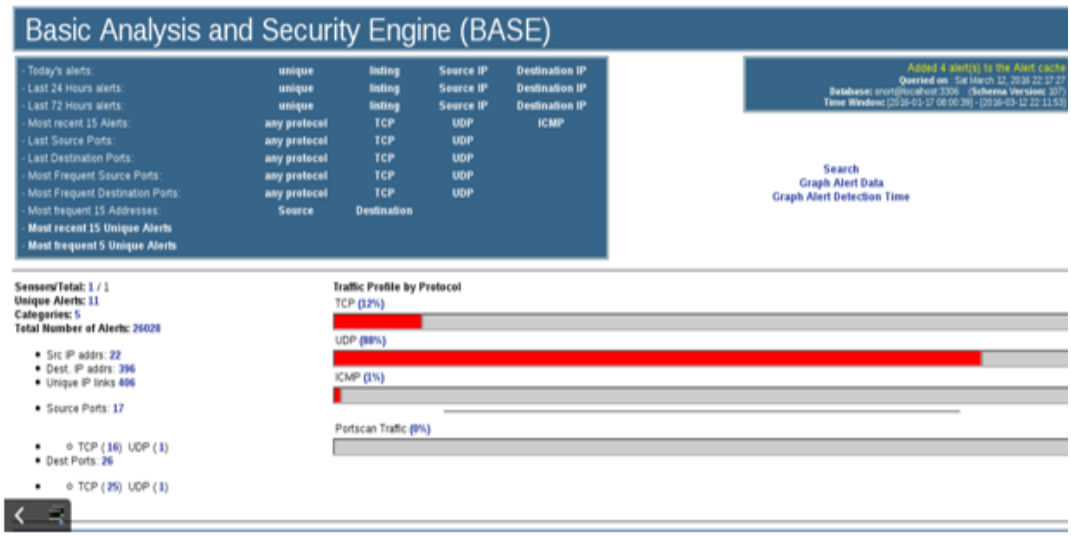


Figure 7. Results Generated by Snort on Basic Analysis Security Engine Home page

In the given figure following fields used by user for displaying result according to their needs.

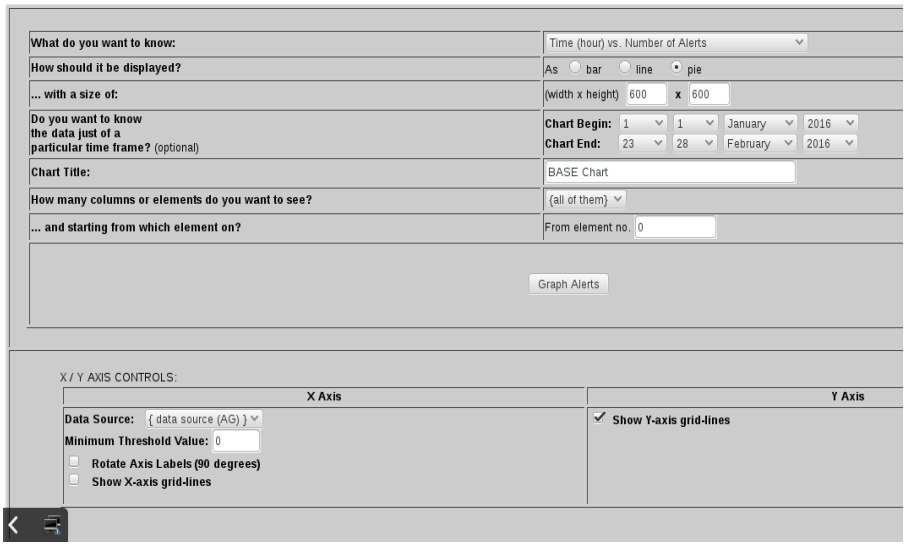


Figure 8. Report for Time vs. Number of Alerts

In the given figure pie-chart shows the details in terms of Time vs. Number of Alerts.

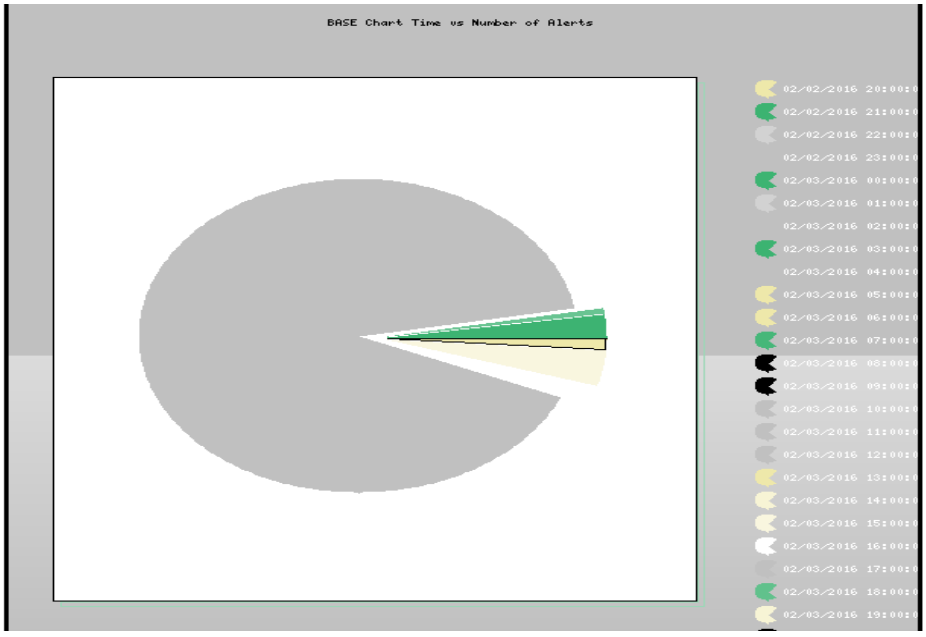
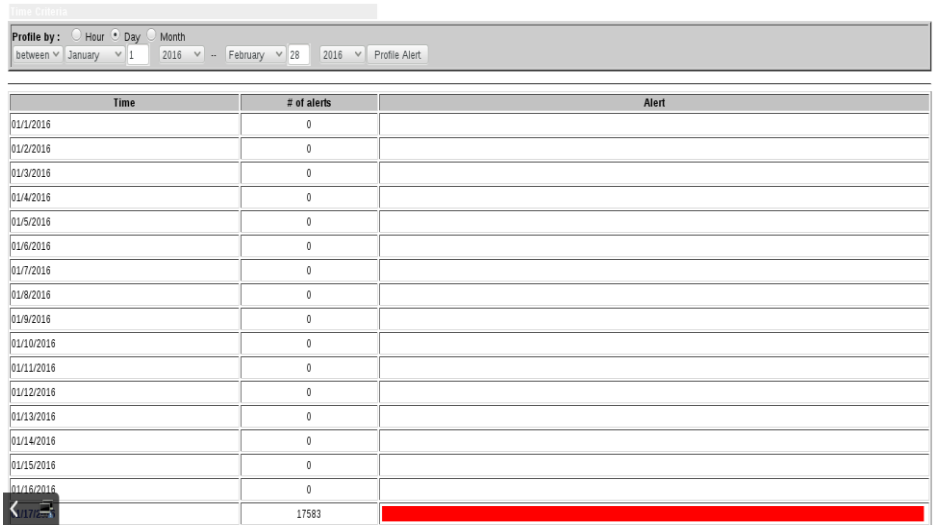


Figure 9. Pie Chart for Analysis

In the given figure shows the Report in terms of hour, day, month and Number of alerts generated with respect to time.



Time	# of alerts	Alert
01/1/2016	0	
01/2/2016	0	
01/3/2016	0	
01/4/2016	0	
01/5/2016	0	
01/6/2016	0	
01/7/2016	0	
01/8/2016	0	
01/9/2016	0	
01/10/2016	0	
01/11/2016	0	
01/12/2016	0	
01/13/2016	0	
01/14/2016	0	
01/15/2016	0	
01/16/2016	0	
	17583	

Figure 10. Report Based on Date

4.3 MySQL

MySQL is a freely available database and works perfectly on Linux and windows systems, we can use it with Snort. Some different methods for using a database with Snort are:

- You can install and run the MySQL database server on the same machine where Snort is running.
- You can also install the MySQL server on a different machine and configure Snort to log to that database.
- You can have multiple Snort sensors to log to a centralized database server running MySQL server.

5. Conclusion

Security is the basic need of any organization and Netizen. We can provide it by using snort. Snort is used to increase the security of our network against the real time traffic. It performs monitoring of network and detects malicious attack using rule set. BASE shows the result generated by the snort on the graphical console for easier understanding of the user. MySQL stored the database for logging purpose. In future work we enhance the IDS performance by creating new rules for attacks and design efficient pattern matching algorithm.

References

[1] L. Emilie and E. Jonsson, "Survey of intrusion detection research", Chalmers University of Technology, **(2002)**.
[2] E. D. Dorothy, "An intrusion-detection model", Software Engineering, IEEE Transactions, vol. 2, **(1987)**, pp. 222-232.
[3] S. Neha, P. Budhwani, S. Talekar, S. Borle and N. Jadhav, "Survey on Intrusion Detection Systems", International Journal, vol. 2, no. 1, **(2014)**.
[4] D. Herve, "An introduction to intrusion-detection systems", Proceedings of Connect, **(2000)**.
[5] T. Rajni and A. Mishra, "Introduction To Intrusion Detection System: Review".
[6] R. Suman and V. Singh, "SNORT: An Open Source Network Security Tool for Intrusion Detection in Campus Network Environment", International Journal of Computer Technology and Electronics Engineering, vol. 2, no. 1, **(2012)**, pp. 137-142.
[7] S. Gupta and R. Mamtora, "Intrusion Detection System Using Wireshark", International Journal of Advanced Research in Computer Science and Software Engineering.

[8] T. Sheetal, P. Ingle and B. B. Meshram, "IDS: Intrusion Detection System the Survey of Information Security", VJTI, Matunga, Mumbai, vol. 2, **(2012)**.
[9] K. Vinod and O. P. Sangwan, "Signature based intrusion detection system using snort", International Journal of Computer Applications & Information Technology, vol. 1, no. 3, **(2012)**, pp. 35-41.
[10] R. R. Ur, "Intrusion detection systems with Snort: advanced IDS techniques using Snort, Apache, MySQL, PHP, and ACID", Prentice Hall Professional, **(2003)**.

