

# Real Time Network Traffic Monitoring to Overcome Malicious Activities in Enterprise Networks

Rakshatha S<sup>1</sup>, Dr. R. Nagaraja<sup>2</sup>

<sup>1</sup>Rakshatha S, student, Department of Information Science and Engineering, Bangalore Institute of Technology, Karnataka, India.

<sup>2</sup>Dr. R. Nagaraja, Professor, PG and Research Coordinator, Department of Information Science and Engineering, Bangalore Institute of Technology, Karnataka, India.

\*\*\*

**Abstract** - Nowadays as there is a rapid expansion of computer networks, providing security has become a crucial issue. The better solution is to detect illegal use of computer network by monitoring the network traffic for both legitimate user activity and for intruder activity. The types of attacks across the network computer systems have boost the significance of computer network security. Currently the network administrators use network protocol analyzer or the packet sniffer tools such as Wireshark/Tshark for capturing the packets, inspecting and analyzing the network traffic to check out what exactly is going on and to set up a prompt feedback in case when the attack is identified. This proposed method uses the traffic data which is collected using Tshark and is pushed to ELK (Elasticsearch, Logstash, Kibana) Stack in order to learn, analyze and detect both the normal and the malicious behaviour of the network traffic. If the obtained traffic pattern doesn't match the normal behaviour of the network connection then an anomaly is detected, and furthermore, necessary action is carried out accordingly.

**Key Words:** Intruder activity, Packet Sniffer, ELK, Wireshark, Anomaly, Tshark.

## 1. INTRODUCTION

In today's networking system of an enterprise, there is a primary focus on the features of network such as security, optimization of their network bandwidth and the process of handling the network which has become the essential factor of their networking environment. The modern network monitoring incorporating several techniques to encounter the issues raised and it is very different from the basic method of monitoring the network or the network issues. These modern techniques will comfort the users to quickly diagnose the problem raised and it also prompts the malicious events occurring with respect to the network.

The organization usually consists of variety of networking devices and application in their network. Generally inside an enterprise there is an enormous usage to the internet and the intranet traffic by its employees which naturally demands for the efficient handling of its networking resources. The enterprise network should be smart enough to supervise the behaviour, security and the fault management in the network. The anomalies which are detected in network are considered as the unpredictable and transitory fluctuation from the regular operation of the network. These anomalies are purposefully created by the intruders with spiteful intent.

## 2. RELATED WORKS

The packet sniffing is one of the techniques to catch the complete data which is broadcasted over the network and it outputs the obtained data into a file which is the easy to read format by its users. These packet sniffers are properly used by the network administrator to keep track and solve the network issues raised in their network. Most of the network administrator uses the Wireshark tool to monitor their network. These tools will collect the network packets and demonstrates the acquired data packets as specific as possible. Earlier there were some tools which were efficient but they were costly. But the development of free source packet sniffing tools have made enhancement of the network security in a cost effective manner. [1]

Scrutiny of the data has become a primary consequence internet influence generation. The data storage and its recovery for inspection play a significant role. Most of the ecommerce website generates large amount of data which needs to be investigated. Elasticsearch is a free source tool and is efficient of recording and searching. Along with the Elasticsearch the Logstash is used for supervising the data and the events. Kibana is also a free source visualization tool that allows its user to discover their data in the form of graphs, heat maps and tables. [2]

### 3. PROPOSED SYSTEM

The first step of the proposed system is to collect the required network traffic information. This step is carried out using the Tshark which is one of the widely used Packet sniffer tool. Tshark lets us to capture packet data from an active network, study from earlier reserved capture file by printing a decrypted form of those packets to standard output.

Once the data is collected it is then sent to Elasticsearch for storage and analysis using Logstash pipeline as shown in figure 1. Elasticsearch is a free source search server which is based on apache lucene and is written in java. It is designed to receive data from any origins and it provides a function to search the data that is stored in real-time as it's being fed.

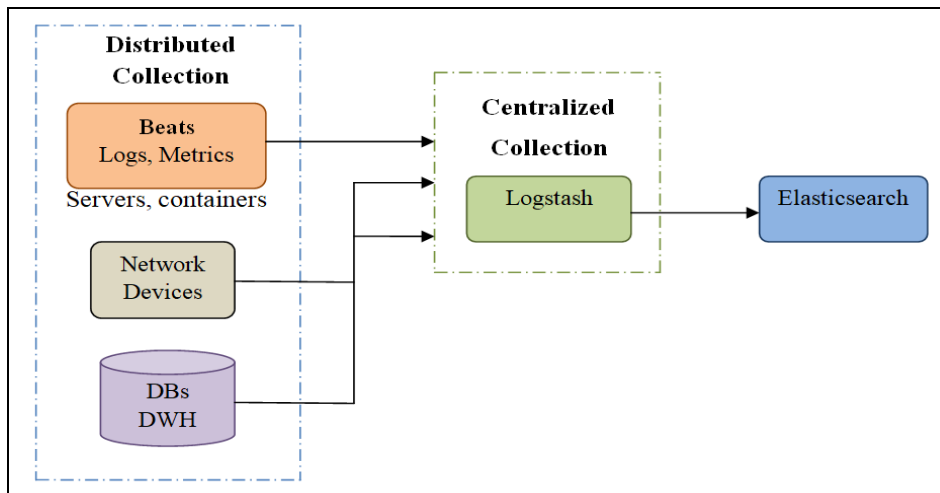
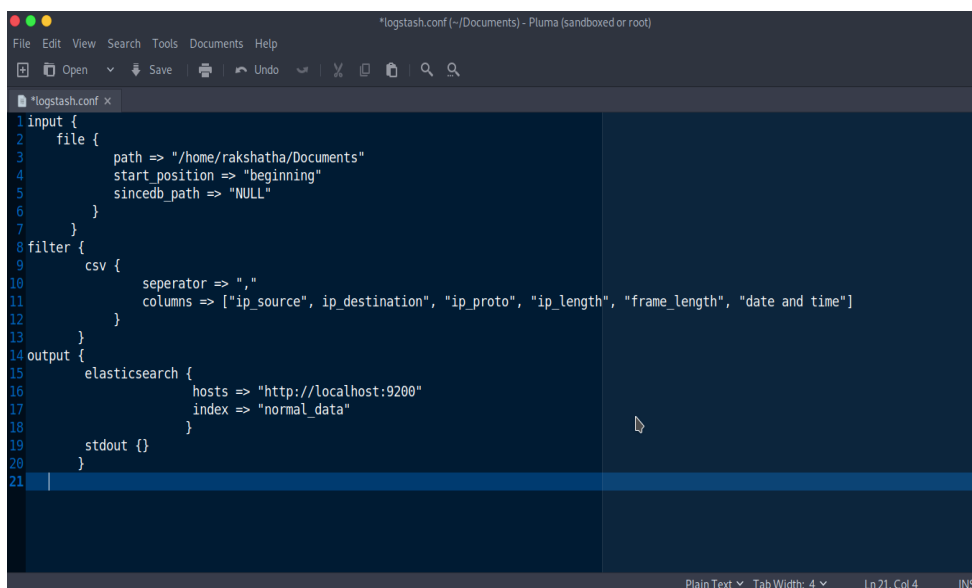


Fig -1: Data shipping to Elasticsearch using Logstash pipeline

Logstash is a data pipeline that can take data input from various origins, filter it, and output it to various sources. Logstash is very important tool in Elasticsearch as it is fundamentally used to obtain data from various sources and then push it to Elasticsearch. The Logstash works by setting up an event processing pipelines, where each pipeline consists of input, filter and the output section as shown in figure 2 respectively. The input is need for passing data to convert them into machine understandable format. Filter indicates the set of conditions to perform a particular action or an event. Output acts as a decision maker for processed event.



```
1 input {
2   file {
3     path => "/home/rakshatha/Documents"
4     start_position => "beginning"
5     since_db_path => "NULL"
6   }
7 }
8 filter {
9   csv {
10    separator => ","
11    columns => ["ip_source", "ip_destination", "ip_proto", "ip_length", "frame_length", "date and time"]
12  }
13 }
14 output {
15   elasticsearch {
16     hosts => "http://localhost:9200"
17     index => "normal_data"
18   }
19   stdout {}
20 }
21
```

Fig -2: Logstash event processing pipeline.

By creating visualizations in Kibana, it makes us easy to predict or to identify changes in tendency of errors or other powerful events of the input source. Kibana accesses the data from Elasticsearch and represents them to the user in the form of line graph, bar graph, pie charts etc. Once the data is collected using Tshark, they are sent to Elasticsearch through Logstash. These networking data which is collected is very huge, therefore Kibana allows us to easily analyse the data and make future investigations.

The IAX (Inter-Asterisk eXchange) flood which is the stressing tool is used in order to create DoS (Denial of service) attacks for the testing purpose which generates huge traffic in the enterprise network. The IAX flood is a VoIP DoS tool that transmits the required number of packets from specified source address to the destination address. Both the datasets, the normal and the data set which was collected during the IAX flooding are analysed in Kibana in order to check the differences with each of them respectively. Different graphs were created for example bar graphs, vertical graphs pie charts, tables etc to explore the obtained data set.

The last step is to send the email alert to the network administrator when the malicious activity is detected after analysing the obtained data. The python code is written to send an email to the network administrator. This code fetches the data set and analyse the data to detect the anomaly and finally sends an email to the specified email address regarding the issue.

#### 4. RESULT

The two vertical graphs shown below were created using visualization option of Kibana. The figure 3 shows the vertical graph which was created for the normal data set which does not include any anomaly. The graph shown in figure 4 was created by considering the data which was captured at the time of flooding the packets using IAX flood.

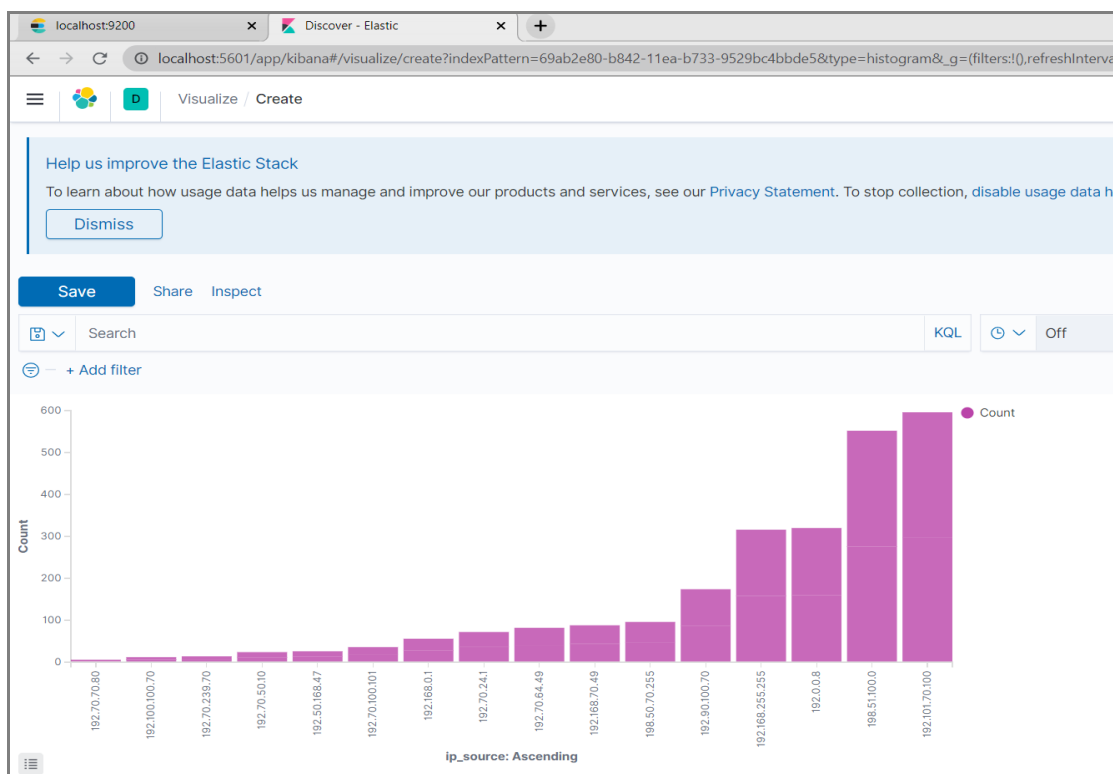


Fig-3: Vertical graph created for normal dataset

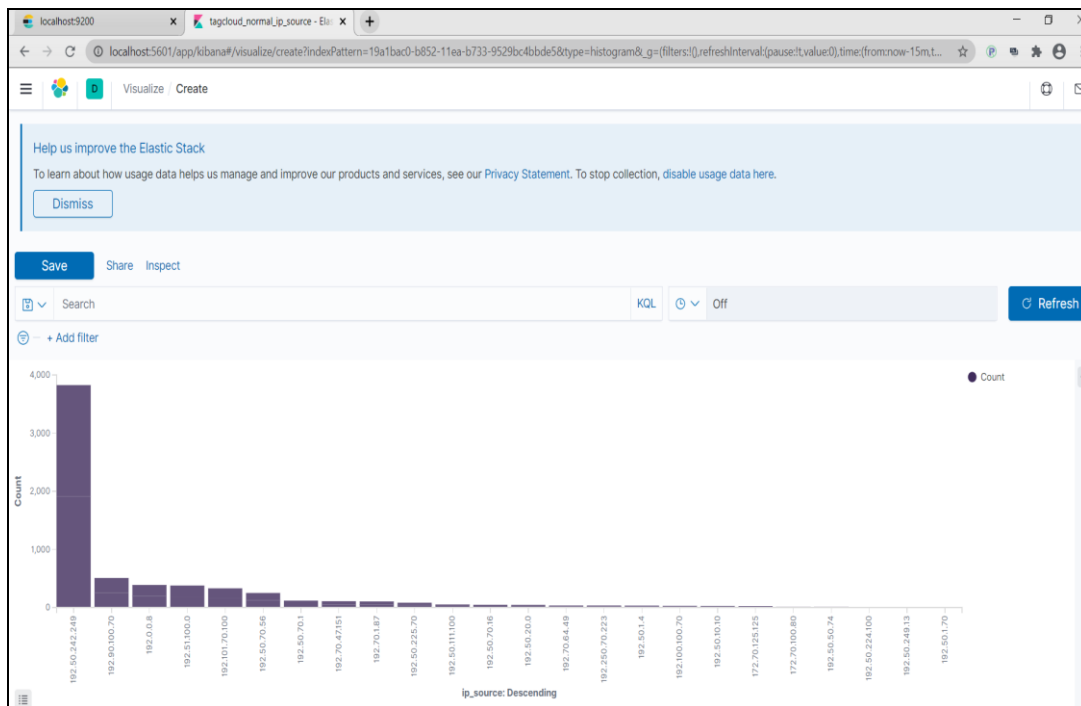
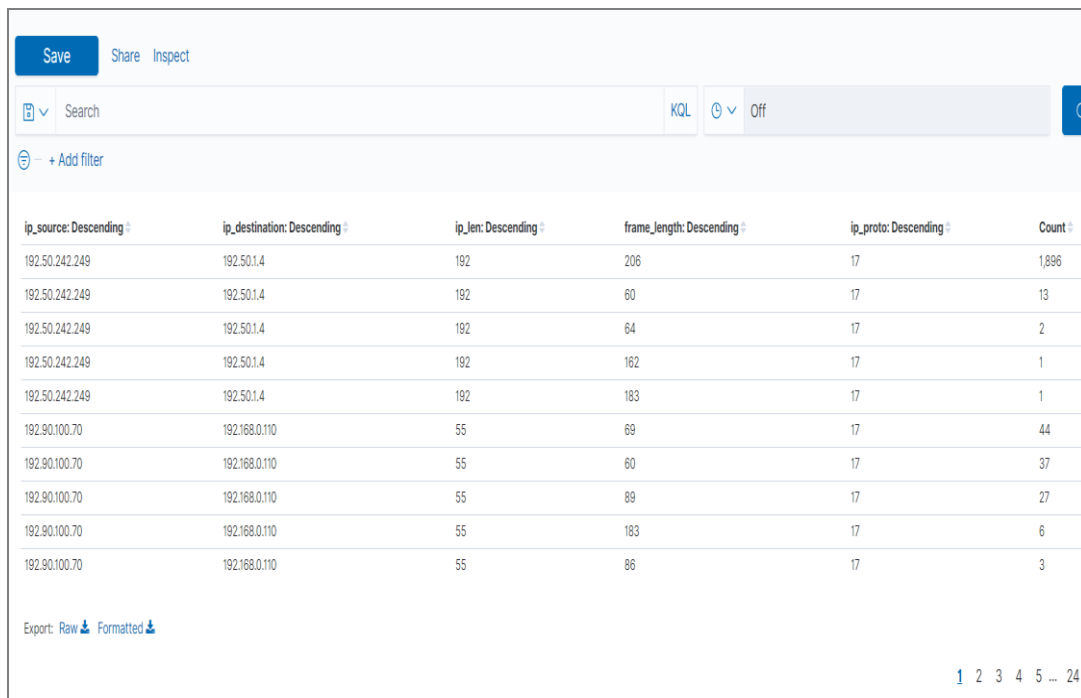


Fig- 4: Vertical graph created for malicious dataset

The two tables below were created using visualization option of Kibana. The figure 5 shows the table which is created for the normal data set and the figure 6 shows the table created for the data set where there is continuous data flooding from one source to destination.

ip_source: Descending	ip_destination: Descending	ip_len: Descending	frame_length: Descending	ip_proto: Descending	Count
192.101.70.100	198.51.100.255	78	60	17	149
192.101.70.100	198.51.100.255	78	92	17	93
192.101.70.100	198.51.100.255	78	183	17	20
192.101.70.100	198.51.100.255	78	86	17	13
192.101.70.100	198.51.100.255	78	64	17	7
192.101.70.100	198.51.100.255	78	89	17	6
192.101.70.100	198.51.100.255	78	124	17	2
192.101.70.100	198.51.100.255	78	162	17	2
192.101.70.100	198.51.100.255	78	94	17	1
192.101.70.100	198.51.100.255	78	163	17	1

Fig-5: Table created using Kibana for normal dataset



ip_source: Descending	ip_destination: Descending	ip_len: Descending	frame_length: Descending	ip_proto: Descending	Count
192.50.242.249	192.50.1.4	192	206	17	1,896
192.50.242.249	192.50.1.4	192	60	17	13
192.50.242.249	192.50.1.4	192	64	17	2
192.50.242.249	192.50.1.4	192	162	17	1
192.50.242.249	192.50.1.4	192	183	17	1
192.90.100.70	192.168.0.110	55	69	17	44
192.90.100.70	192.168.0.110	55	60	17	37
192.90.100.70	192.168.0.110	55	89	17	27
192.90.100.70	192.168.0.110	55	183	17	6
192.90.100.70	192.168.0.110	55	86	17	3

Fig-6: Table created for the data set where the flooding is detected which is considered as a malicious activity

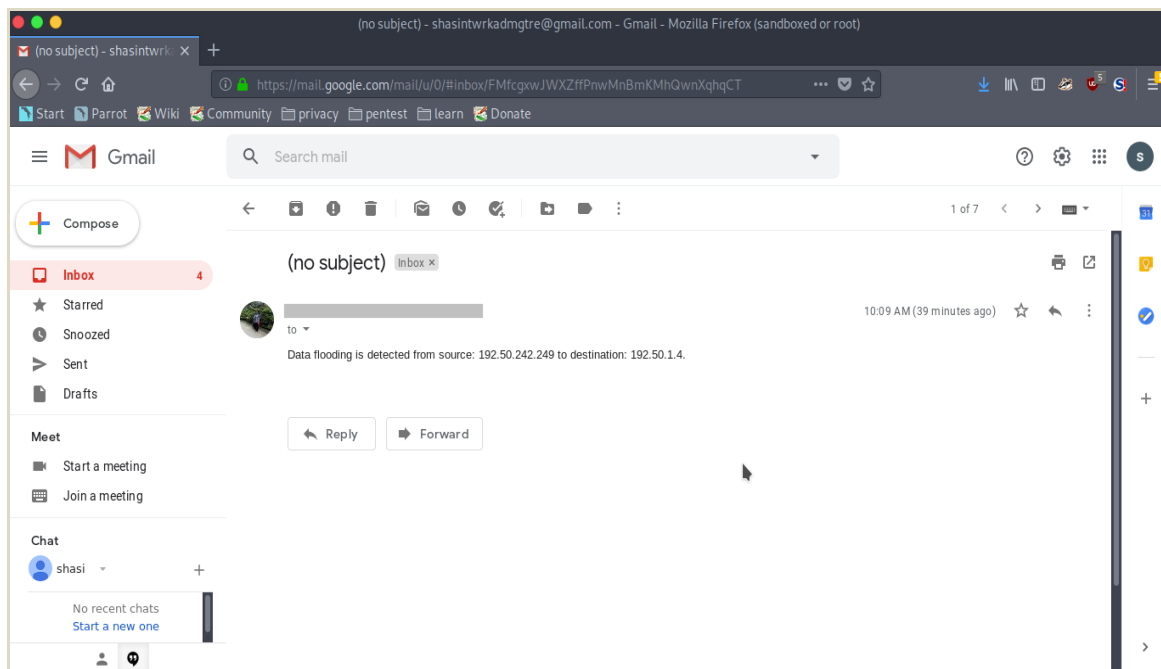


Fig-5: Email received by the network administrator

## 5. CONCLUSION

Attacking the network of an enterprise by the intruders is one of the causes for unnatural phenomena observed in the service of the network. The main aim here is to use the simple tools and methods which are available freely to monitor network traffic and to identify the anomaly effectively in the enterprise network. The method which are used for capturing the data packets, inspecting data in order to discover an anomaly and then taking the necessary action are simple and efficient. Therefore, it is highly effective and allows the administrator to gain control over the network.

## 6. FUTURE ENHANCEMENT

The method used here encounters the users to find a single type of anomaly which is the data flooding which creates Dos attack to the enterprise network. Many other anomalies such as detecting the intruders, identifying the data leakage etc., can further be discovered by adopting the same method. In this project the python coding standard are used to direct an email to the network administrator when the anomaly is discovered. Alternatively we can also use the watcher which is one among the several features that are available in Elasticsearch which creates actions based on conditions.

## REFERENCES

- [1] ApriSiswanto, Abdul Syukur, Evizal Abdul Kadir, Suratin. "Network Traffic Monitoring and Analysis using Packet Sniffer", IEEE 2019:978-1-5386-8317.
- [2] Divyesh Bhatnagar, R Jaya SubaLakshmi and Vanmathi C. "Twitter Sentiment Analysis Using Elasticsearch, Logstash and Kibana", 2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE). IEEE 2020.
- [3] Piyuh Goyal and Anurag Goyal. "Comparative study of two Most Packet Sniffing Tools – Tcpcdump and Wireshark". 2017 9<sup>th</sup> International Conference on Computational Intelligence and Communication Networks. IEEE 2017
- [4] Umesh Taware and Nuzhat Shaikh. "Heterogeneous Database System for Faster Data Querying using Elasticsearch", IEEE 2018: 978-1-5386-5257.
- [5] Vlad-Andrei Zamfir, Mihai Carabas, Costin Carabos and Nicolae Tapus. "System monitoring and big data analysis using the Elasticsearch system ". 2019 22<sup>nd</sup> International Conference on Control System and Computer Science (CSCS). IEEE 2019.
- [6] Khan, R., Khan, S. U., Zaheer, R., & Babar, M. I. "An Efficient Network Monitoring and Management System". International Journal of Information and Electronics Engineering, 3(1), 122-126. IEEE 2013.