International Journal of Computer Applications Technology and Research
Volume 9–Issue 02, 59-64, 2020, ISSN:-2319–8656

Network Security Monitoring System on Snort with Bot Telegram as a Notification

I Made Ari Sulistya
Departement of Information Technology
Faculty of Engineering Udayana University
Bukit Jimbaran, Bali, Indonesia

Gusti Made Arya Sasmita
Departement of Information Technologiy
Faculty of Engineering Udayana University
Bukit Jimbaran, Bali, Indonesia

Abstract: Network security in the digital era needs more attention. IDS (Intrusion Detection System) is one of the anticipation method that can be used to protect computer server. Snort IDS only comes with terminal notification or web based, this method has a weakness which to transfer information to administrator network directly. Telegram is an open source instant messaging application. Combination between those applications, produce a perfect transformation to administrator network directly through smartphone. Contrive and testing are the best methods to build this network monitoring system. The Prevention methods is added to support this network monitoring system. Penetration testing is divided by two different types such as, DDoS and port scanning. The result of those two types penetration testing show that Snort IDS is succeeded to detect those tests. The time different between Snort detection and Bot Telegram after ten times attempt in sending messages is 77,1 seconds for Snort detection and 4,05 seconds for Bot Telegram. The time different between two types of penetration after ten times attempt is 6,1 seconds for DDoS UDP and 2 seconds for Nmap portscan.
.

Keywords: IDS (Intrusion Detection System), Snort, Telegram, Penetration Testing

1. INTRODUCTION

In the last five years, cybercrime is increasing which includes identity theft, viruses, and system intrusions. Therefore, Intrusion Detection System (IDS) took an important role in detecting intrusions so that can be addressed immediately. Snort is one of the leading Network-Based IDS (Intrusion Detection System) software with nearly four hundred thousand users [2]. However, Snort does not provide a sufficient GUI (Graphical User Interface) so that the user has to install another application separately such as BASE to get a better GUI [3].

IDS alert system with web based interface like BASE cannot offer notify to the system administrator, it is possible that users may miss some attacs so that the response become too late to do [1]. The IDS (Intrusion Detection System) with real time notification system is highly needed [6].

The growing of Instant Messenger in this era, not only used in desktop. Instant Messenger has been commonly used in mobile devices. Instant Messenger also used in many platforms as real time notification system. Instant Messenger provides query facility that cannot be easily applied in other communication media [3]. System administrator are able to interact with the system to get the status and condition of the system even able to modify.

Instant Messenger only needs an internet connection to connect to the server. Meanwhile, SMS gateway requires cost of each sent message so applying SMS gateway in a system notification need no small cost. So the costs incurred when using Instant Messenger is much less [4].

Telegram Messenger is widely used instant messaging protocol with about 200 milion users that runs on many mobile operating systems such Android, iOS, and Windows phone. Telegram Messenger also can be found on desktop operation system such as Windows, Linux, aand MacOS [5]. Telegram Messenger also a platform messenger that easily to use with many modification to synchronize with any application. Based on the facts above, we utilize Telegram Messenger as an interactive interface for Snort IDS with real time notification [2]. The function of this messenger application can obtain intrusion alerts and their detail information in real time manner, also can do small prevention system to protect the system.

2. METHODOLOGY RESEARCH

The research was done based on Snort structure and integration between Telegram Messenger. The design of this system will monitor all types of suspicious data packages and the flow of data that enters the computer server through Snort. Here is a scheme of Intrusion Detection System Snort with BASE as web interface [2].

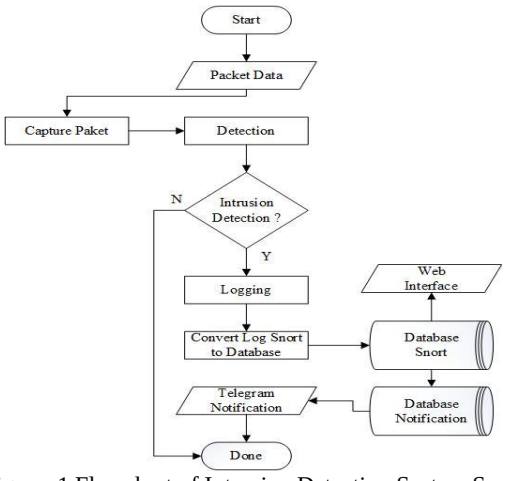

Figure. 1 Flowchart of Intrusion Detection System Snort

Figure 1 is flowchart design of Intrusion Detection System Snort with BASE as web interface. IDS console read each network packet from the target [5]. The packet is then inspected wheter the packets is a malicious packet. Each detection result will be stored into the log. The third party application called barnyard2 will convert Snort log into

database and stored to system administrator using web interface or database notification of Telegram Messenger [4].

2.1 Telegram Messenger API

Telegram Messenger provides an API (Application Program Interface) that allow developers to build application integrated to Telegram Messenger. Telegram Messenger uses bot to communicate with the system server [1]. User must registration their own bot to perform authorization to perform activities with Telegram Messenger such send messages or retrive messages. Here is a cheme flowchart design to create our own bot Telegram.

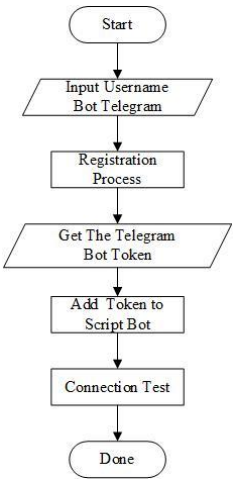

Figure. 2 Flowchart design Registration Bot Telegram

User must intall Telegram on the devices and type code to create bot on telegram. Input the username of bot application, the Telegram server will reply with bot token to connect the script of our bot to the server Telegram.

Integration between Telegram Messenger with Snort scheme can be use after this registration bot. Create database notification to accommodate Snort malicious packet information. Here is the design scheme of integrated Snort with Telegram Messenger Notification.

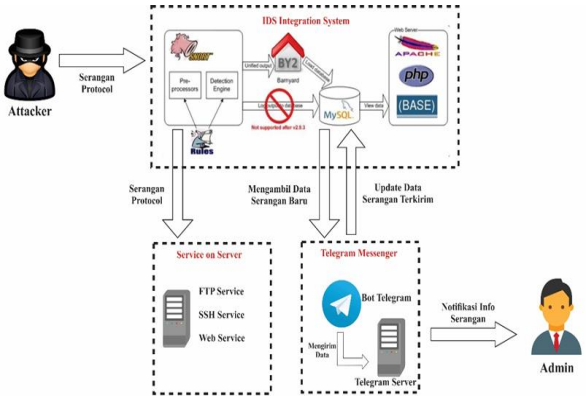

Figure. 3 Scheme design Snort with Telegram Notification

The design of the Snort with Telegram Notification is made from the detection of packages suspected by Snort and then entered into the database by a third party application called barnyard2. Telegram Messenger bot works according to the scripts to send notification to system administrator.

3. CONCEPTS AND THEORIES

Literature review contains supporting theories in the research that will be conducted. The theories including Intrusion Detection System and Telegram Messenger bot will be discussed as follows.

3.1 Intrusion Detection System

Intrusion Detection System (IDS) is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered. IDS is a software application that scans a network or a system for harmful activity or policy breaching [6].

IDS types range in scope from single computers to large networks. The most common classifications are network intrusion detection systems (NIDS) and host-based intrusion detection systems (HIDS). System that monitors important operating system files is an example of an HIDS, while a system that analyzes incoming network traffic is an example of an NIDS [3]. IDS classification it is possible too by detection approach. The most well-known variants are signature-based detection (recognizing bad patterns, such as malware) and anomaly-based detection (detecting deviations from a model of good traffic, which often relies on machine learning). Another common variant is reputation-based detection (recognizing the potential threat according to the reputation scores). Some IDS products have the ability to respond to detected intrusions. Systems with response capabilities are typically referred to as an intrusion prevention system. Intrusion detection systems can also serve specific purposes by augmenting them with custom tools, such as using a honeypot to attract and characterize malicious traffic [1].

Snort employs both signature based techniques and anomaly based techniques to detect an intrusion. Signatures are used for detecting intrusions. Snort has a rich rule set which depend upon the signatures present in either the header part of the packet or payload of the packet so as to detect intrusions [2].

3.2 Snort

Snort is a light-weight intrusion detection tool which logs the packets coming through the network and analyzes the packets. Snort checks the packets coming against the rules written by the user and generate alerts if there are any matches found. The rules are written by the user in a text file which is linked with snort.conf file where all the snort configurations are mentioned. There are few commands which is used to get snort running so that it can analyze network behavior [4]. The architecture of snort can be categorized into five basic modules namely Libcap, Packet Decoder, Preprocessors, Detection Engine and Output plugins.

The traffic comes from Internet are received by routers and passed to switch. The switch then delivers this data traffic to firewalls for first level of evaluation. After that the firewalls passed them to the Ethernet adapter of server. Here the Snort came into focus for any type of evaluation of those data packets [6].

There are different types of preprocessors included in snort 2.9.7.2 with optional options, however in this paper no preprocessor configured but for actual intrusion detection and prevention they are necessary to control [2].

3.2.1 Detection Engine

This portion of snort is principally very dynamic and unified. This module is very vital in terms of multiple rules examination in terms of their priority order. When snort use to inspect the packets multiple rules with different priorities are reported and stored in a queue. However then it only reports out the rules with highest priority. This is specially used to avoid deep evasion techniques if used by attacker. This makes the snort as a highly proficient in terms of attack identification [3].

3.2.2 Output Modules

This module design came up after Snort 1.6 version. This is the last segment of snort where packets come from detection engine and disseminated to network in different modes as per the convenience of the network administrator. The convenience of network administrator is in terms to view the real time alerts, logs and other parameters to evaluate the performance of the network of the organization. Third party tools such as mysql, a database, can also used for the same purpose. But in this paper the logs are stored into /var/log/snort directory [3].

4. RESULTS AND DISCUSSION

To determine the effectiveness of this system, we calculate the amount of delay between the occurrence of the incident until when the notification is received by the user. Testing was conducted using 10 similar attacks from single source of attack and using single client as the recipient of the notification.

4.1 Accuracy Rate of Time

The level of accuracy rate of time is calculated from the time of attack and detected. Average IDS detection rate depend on it. The rate of notification sent is also obtained from the difference in time sent with the time received by the admin, as shown in Table 1.

Table 1. Accuracy Rate of Time

No	Types	Accuracy Rate of Time (Timestamp)			
		Intruder Time (m^a,s^a)	**Snort Detection Time (m^b,s^b)**	**Telegram sent Time (m^c,s^c)**	**Admin Receive Time (m^d,s^d)**
1.	DDoS UDP	15:09:38	15:10:42	15:11:52	15:11:57
2.	DDoS UDP	15:09:49	15:10:52	15:11:54	15:11:57
3.	DDoS UDP	15:09:58	15:11:02	15:11:54	15:12:02
4.	DDoS UDP	15:10:09	15:11:12	15:11:55	15:12:02
5.	DDoS UDP	15:10:20	15:11:22	15:11:55	15:12:02
6.	DDoS UDP	15:10:28	15:11:32	15:11:55	15:12:02
7.	DDoS UDP	15:10:41	15:11:42	15:11:56	15:12:12
8.	DDoS UDP	14:48:01	14:49:04	14:49:28	14:49:30
9.	DDoS UDP	14:48:12	14:50:24	14:50:34	14:50:37
10.	DDoS UDP	14:48:22	14:50:34	14:50:39	14:50:42
11.	Nmap Portscan	11:50:51	11:53:16	11:53:19	11:53:22
12.	Nmap Portscan	11:52:28	11:55:37	11:55:41	11:55:43
13.	Nmap Portscan	11:54:31	11:56:42	11:56:45	11:56:47
14.	Nmap Portscan	11:56:11	11:57:03	11:57:06	11:57:08
15.	Nmap Portscan	11:58:02	11:58:48	11:58:50	11:58:52
16.	Nmap Portscan	12:01:22	12:02:03	12:02:05	12:02:08
17.	Nmap Portscan	12:03:05	12:03:45	12:02:48	12:02:49
18.	Nmap Portscan	12:05:35	12:06:15	12:06:18	12:06:20
19.	Nmap Portscan	12:07:46	12:08:26	12:08:29	12:08:30
20.	Nmap Portscan	12:09:17	12:10:07	12:10:10	12:10:12

Based on the Table 1. Accuracy Rate of Time measurement result above is the timestamp of two types penetration between DDoS UDP and Nmap portscan. The timestamp include of Intruder Time (m^a,s^a), Snort Detection Time (m^b,s^b), Telegram Sent Time (m^c,s^c), and Admin Receive Time (m^d,s^d). Intruder Time is timestamp that intruder start to attack the system. Snort Detection Time is timestamp that Snort detected malicious packet data. Telegram Sent Time is timestamp that bot Telegram send messages to Network administrator. Admin Receive Time is timestamp that network administrator receive all the messages of malicious packet data information.

4.2 Time Difference

Time difference between two types of penetration DDoS UDP and Nmap portscan shown in Table 2. The time difference recorded in seconds time unit. Time Difference between attacking and detection are obtained from Intruder Time (m^a,s^a), and Snort Detection Time (m^b,s^b) timestamp. Time difference between send and receive are obtained from Telegram Sent Time (m^c,s^c), and Admin Receive Time (m^d,s^d) timestamp. Here is the result of time difference shown in Table 2.

Table 2. Time Difference

No.	Types	Time Difference (Seconds)	
		Time Difference between attacking and detection (S^x)	Time Difference Between send and receive (S^y)
1.	DDoS UDP	64	5
2.	DDoS UDP	63	3
3.	DDoS UDP	64	8
4.	DDoS UDP	63	7
5.	DDoS UDP	62	7
6.	DDoS UDP	64	7
7.	DDoS UDP	61	16
8.	DDoS UDP	63	2
9.	DDoS UDP	132	3
10.	DDoS UDP	132	3
11.	Nmap Portscan	145	3
12.	Nmap Portscan	189	2
13.	Nmap Portscan	131	2
14.	Nmap Portscan	52	2
15.	Nmap Portscan	46	2
16.	Nmap Portscan	41	3
17.	Nmap Portscan	40	1
18.	Nmap Portscan	40	2
19.	Nmap Portscan	40	1
20.	Nmap Portscan	50	2
Amount of Time		**1542**	**81**
Average Time		**77,1**	**4,05**

Based on the table of Time Difference measurement result above the highest value between attacking and detection is 189 seconds on Nmap portscan type, while lowest value is 40 seconds on Nmap portscan type. The highest value between send and receive is 16 seconds on DDoS UDP type, while lowest value is 1 seconds on Nmap portscan type. Average Time of 20 penetration test with two types of attacking way between intruder and Snort detection is 77,1 seconds, while average time between send and receive is 4,05 seconds.

Time difference is obtained from timestamp result of Table 1. The formula to get the time difference is substraction between timestamp result on Table 1. Here is the formula to get time difference between attacking and detection.

$$S^x = ((m^b \times 60) + s^b) - ((m^a \times 60) + s^a)$$
$$S^x = (60m^b + s^b) - (60m^a + s^a)$$

Figure 4. Formula of Time Difference Attacking and Detection

Explanation :
S^x = Time Difference in seconds between attacking and detection
m^a = Minutes unit of time from attacking.
s^a = Seconds unit of time from attacking.
m^b = Minutes unit of time from Snort Detection.
s^b = Seconds unit of time from Snort Detection.

$$S^y = ((m^d \times 60) + s^d) - ((m^c \times 60) + s^c)$$
$$S^y = (60m^d + s^d) - (60m^c + s^c)$$

Figure 5. Formula of Time Difference Send and Receive

Explanation :
S^y = Time Difference in seconds between Send and Receive.
m^c = Minutes unit of time from Send.
s^c = Seconds unit of time from Send.
m^d = Minutes unit of time from Receive.
s^d = Seconds unit of time from Receive.

Analytical data set to see the graph of time difference data between sent and receive. Figure 6 shown the flow of Telegram messenger transformation rate to send messages information.

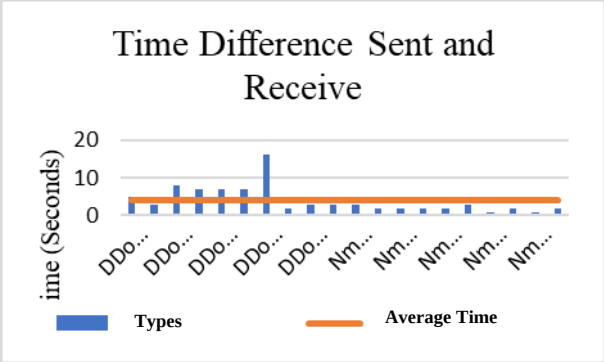

Figure 6. Analytics Chart Time Difference Sent and Receive

Figure 6 is analytical chat of time difference from send and receive messages bot Telegram. The chart shown some big difference time messages in the middle of simulation.

Analytical data set to see the graph of time difference data between Snort detection and attacking time. Figure 7 shown the flow of Snort detection rate to detected malicious packet data.

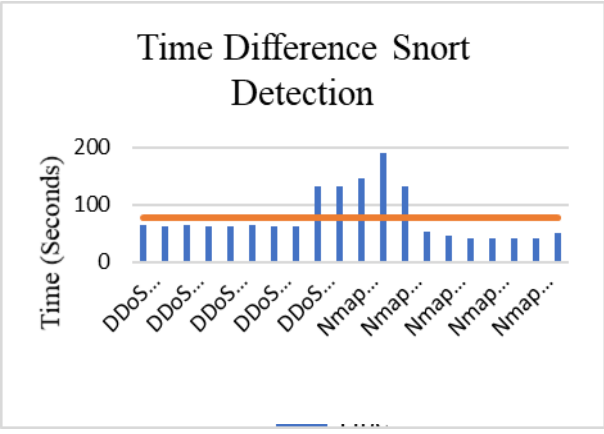

Figure 7. Analytics Chart Time Difference Snort Detection and Attacking

Figure 7 is analytical chat of time difference from Attacking and Snort Detection from detected malicious packet data. The chart shown some big difference time messages in the middle of simulation with transition betweet DDoS UDP attack to Nmap portscan attack.

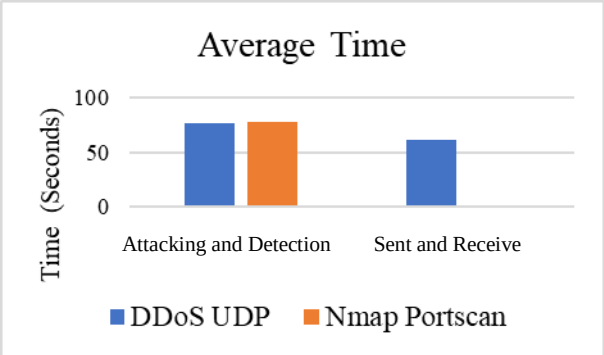

Figure 8. Analytics Chart From Average Time

Figure 8 is analytical chat from average time of attacking and detection also sent and receive with two types of penetration in seconds unit of time. The chart of attacking and detection between two penetration test shown no big difference. The chart of sent and receive between DDoS UDP and Nmap portscan penetration shown big difference that DDoS UDP have more time to send information.

4.3 System Testing

Testing system monitoring with snort has two main part from the omputer testing and the mobile testing. This feature will be explained as follows.

4.3.1 Snort Testing

Snort that already installed on computer system must be tested wether it works or not. Snort testing can be done by run the command on terminal and setting the rules of snort to detect malicious packet data like shown on Figure 9.

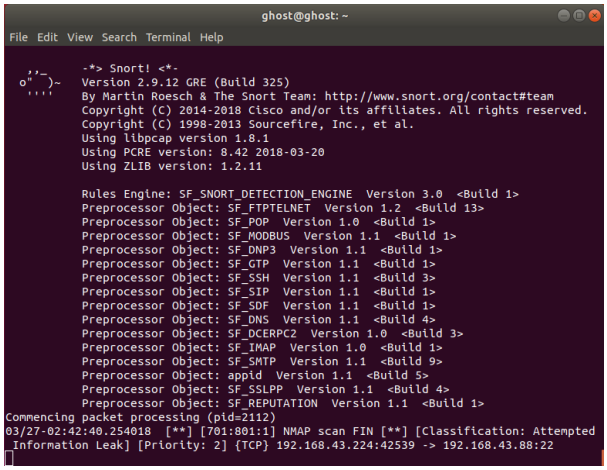

Figure 9. Snort Testing

Figure 9. Snort Testing is a display of Snort Command Line Interface (CLI). The snort display usually in the form of CLI, but there are many third parties application that support Graphic User Interface (GUI). Testing snort can be done by input command on the terminal to start the snort program and snort will commencing packet data from network interface that snort listening from. If that packet match to snort rule, snort will give notification on terminal like shown on Figure 9.

4.3.2 Penetration Testing

Penetration on snort IDS is a stage in testing the network security monitoring system to find out whether the main application is running well or not.

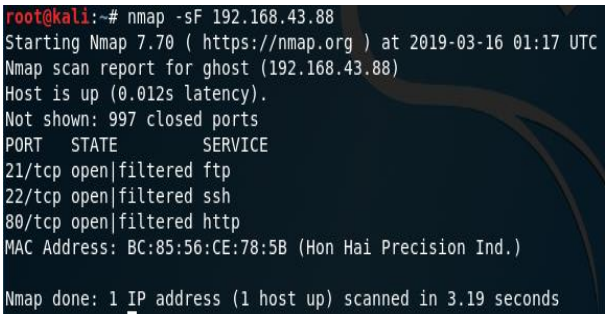

Figure 10. Penetration test using Nmap portscan

Figure 10. shown penetration test using Nmap portscan as a types of attacking from intruder computer with kali linux operation system. The intruder type nmap command and the victim IP address. The tool will start and shown what port are opened from the computer victim.

Penetration test using nmap portscan successfully launched and the bot telegram will send an information about malicious packet data who comes from nmap portscan attack like shown on Figure 11.

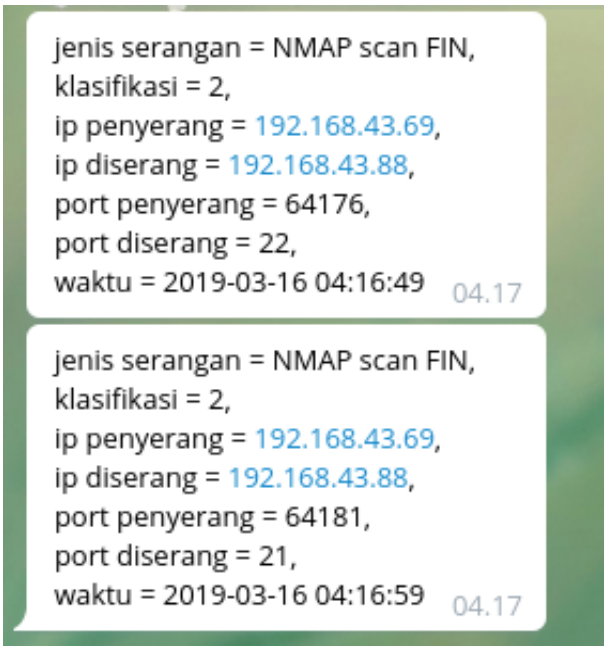

Figure 11. Telegram Information Messages

Figure 11. shown that Snort bot Telegram has receive information about malicious packet data from nmap portscan attacking. The inftomation that contains on this messages are The types of attacking, classification, Intruder IP address, victim IP address, intruder port, victim port, and time of attacking.

4.3.3 Prevention Testing

Prenvention system is a form of network security that works to prevent identified threats. Intrusion prevention systems continuously monitor your network, looking for possible malicious incidents and capturing information about them. This prevention system manually controlled by system administrator to block suspicious IP address.

Figure 11. Prevention System

Figure 11. shown that bot Telegram can be use for prevention system. This features combine linux iptables to block IP address from suspicious client. System administrator just have to type block on this bot telegram and their suspicious IP address to blocking them from the system.

4.3.4 Snort Web Based Interface

Snort has many third parties web based interface, BASE is one of many web based interface. Basic Analysis and Security Engine (BASE) is to see all snort log without open the terminal.

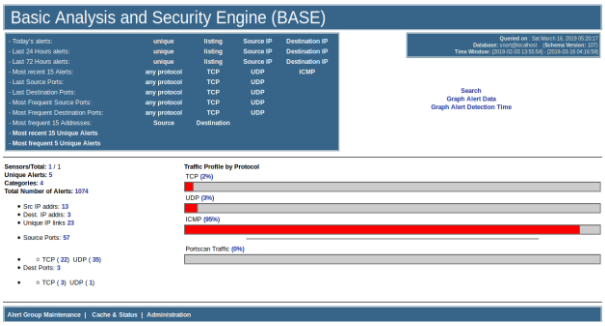

Figure 12. Snort Web Based Interface

Figure 12 shown BASE (Basic Analysis and Security Engine) this features analytics data of malicious packet data that snort detected. BASE features many analytics view such form protocol attack, even a graphic of computer system that detected suspicious packet data.

5. CONCLUSION

Snort Intrusion Detection System from testing of two types of penetration during 10 times of test successfully detected the suspicious packet data. There is delay from sending a messages from Telegram with value 4,05 seconds. Prevention system of this monitoring features can block IP address specified to port, protocol, and time during the block.

REFERENCES

[1] Ammad Uddin, Laiq Hasan, PhD, “Design and Analysis of Real-time Network Intrusion Detection and Prevention System using Open Source Tools”, University of Engineering and Technology, Peshawar, Pakistan. 2016.

[2] Parningotan Panggabean, S.Kom., M.Kom, “Analisis Network Security Snort Menggunakan Metode Intrusion Detection System (IDS) Untuk Optimasi Keamanan Jaringan Komputer”, Program Studi Sistem Informasi, STMIK GICI. 2018.

[3] Mukesh Sharma, Akhil Kaushik, Amit Sangwan, “Performance Analysis of Real Time Intrusion Detection and Prevention System using Snort”, The Technological Institute of Textile and Science,Bhiwani-127021, Haryana – India. 2012.

[4] Hargyo Tri Nugroho, Bagas Adi Wicaksono, “Utilizing Instant Messaging for Real-Time Notification and Information Retrieval of Snort Intrusion Detection System”, Department of Computer Engineering, Faculty of ICT, Universitas Multimedia Nusantara. 2013.

[5] Asep Fauzi Mutaqin, “Rancang Bangun Sistem Monitoring Keamanan Jaringan Prodi Teknik Informatika Melalui SMS Alert dengan Snort”. Universitas Tanjungpura. 2016.

[6] Bekti Maryuni Susanto, Agung Tri Guritno, “Implementasi Snort Ids Menggunakan Android Sebagai Media Notifikasi”,Politeknik Negeri Jember, 2017.Pp 1-3.