IJCCS (Indonesian Journal of Computing and Cybernetics Systems)
Vol.14, No.1, January 2020, pp. 103~112
ISSN (print): 1978-1520, ISSN (online): 2460-7258
DOI: https://doi.org/10.22146/ijccs.53265

The Analysis of Web Server Security For Multiple Attacks in The Tic Timor IP Network

Lilia E. Jeronimo Guterres*[1], Ahmad Ashari[2]
[1]Master Program of Computer Science, FMIPA UGM, Yogyakarta, Indonesia
[2]Department of Computer Science and Electronics, FMIPA UGM, Yogyakarta, Indonesia
e-mail: **[1]l.g.guterres@mail.ugm.ac.id** , [2]ashari@ugm.ac.id

Abstrak

Sistem teknologi saat ini sangat berkembang pesat, dengan kemajuan internet ini, serangan pada jaringan semakin meningkat dengan terbukanya pengetahuan hacking dan cracking dengan dukungan tools yang tersedia dengan mudah dan mendapatkan secara gratis dapat mempermudah para intruder dan attacker melakukan aksi penyusupan atau serangan, seperti mencuri data dan informasi yang bukan hak miliknya, sehingga dapat merugikan perusahaan tersebut. Lokasi untuk melakukan pengujian pada Timor Tic IP. Penelitian ini bertujuan untuk menyediakan suatu sistem keamanan terhadap server yang menggunakan rules yang dibuat untuk snort dengan fungsi memberikan pesan atau peringatan pada administrator jaringan, sehingga dengan cepat user mengetahui adanya serangan. Dengan rules yang dibuat pada snort dapat menghasilkan deteksi serangan dan menampilkan alert. Pada protokol TCP memori yang terpakai 764 Mb dengan total serangan sebanyak 4099. Untuk protokol UDP flooding dengan memori yang terpakai sebesar 9140 Mb dengan total serangan 1310 sedangkan untuk serangan protokol ICMP flooding dengan total serangan 305864 dan memakan memori sebesar 5808 Mb.

Kata kunci— *Web Server Security, Snort, BASE.*

Abstract

T*he current technology is changing rapidly, with the significant growth of the internet technology, cyber threats are becoming challenging for IT professionals in the companies and organisations to guard their system. Especially when all the hacking tools and instructions are freely available on the Internet for beginners to learn how to hack such as stealing data and information. The location of the testing was Timor Tic IP. This research was intended to make a security system on server using rules made for snort with function to give massage or warning to network administrator, so user can identify attack. Rules made on snort can detect attack and display alert. In TCP protocol it used 764 Mb memory with total 4099 attacks. For UDP flooding 9140 Mb memory was used with 1310 attacks. Meanwhile for ICMP flooding protocol there were 305864 attacks and used memory of 5808 Mb*

Keywords— *Web Server Security, Snort, BASE.*

Received January 8th,2020; Revised January 29th, 2020; Accepted January 30th, 2020

1. INTRODUCTION

The network security system is an important aspect to an organisation or company. The availability of free tools and applications in the cyber world technology has made it easier for almost any beginners in the cyber world to start an attack such as stealing data, brute-forcing a password or performing a D-DoS attack. As a result, the attacks and threats will always be increasing these days [1]. Some of the firewalls are unable to provide around the perimeter network security and some only detect attacks that are coming from the external networks. As a result, the IDS tool exists to maximize the security of the network perimeter [2]. To build a sistem of IDS in detection security for web server network traffic monitoring with the rules of snort it can be giving warning for network administrator for furthe action [3]. The measurements of snort in attack detecting based on alert implemented of the rules [4]. The Suricata, an open source-based intrusion detection system (IDS) and intrusion prevention system (IPS) on the web and database server can be utilized to detect port scanning and brute force attacks. It is a free application and sufficient tool to help network administrators to take preventive actions against these attacks [5]**.** The IDS and IPS is primary requirement to secure a network system from threats as well as helping administrators to monitor and analyze anomalies packets in the network traffic. The IDS is a security system that is able to monitor and analyze the incoming network traffics and also traffics originating from the inside [6].

TIC Timor IP is a public institution that operates and runs government's data center. With the newly established office, security system has not been well established to protect the servers such as snort-based IDS. As a result, it is essential safeguard Tic Timor IP's confidential data and protect its network system from inside and outside threats. As a matter of fact, a security system also depends on how fast responses and changes are being made during an attack. The snort-based IDS has been used by many organizations around the world to detect intrusions and most importantly it has the capability to respond quickly when an attack is taken place.

2. METHODS

This chapter will explain steps that will be done in testing attack detection. It consisted of system design analysis route, topology design and rule implementation. The snort-based is the tool that is going to be utilized in this project to identify and collect data in the form of log files [7]. Network topology is the arrangement of network elements in a certain structure to define various types of telecommunication networks, including computer networks. The IDS is a sensor device or a network application that monitors traffic for malicious or unwanted activities happening within a network [8]. It typically reports any intrusion activity to the network administrator or collecting information centrally using a security management system [9].

2.1 System Analysis

This section describes the flow analysis system activities in this report. This flow diagram analyzes the performance of network-based snort according to the standard. The process of designing an attack detection system and a data analysis system can be seen in Figure 1.

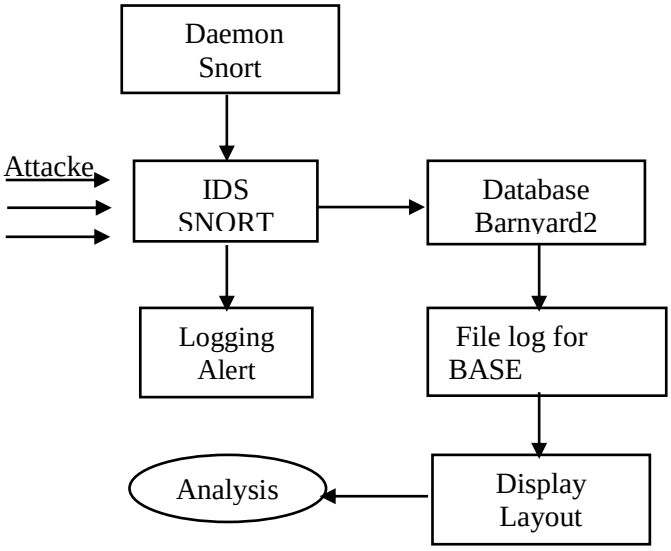

Figure 1. Analysis System Design

Figure 1 shows how the snort detects attacks. The incoming attack is detected by the snort and then the log file is taken and saved in the barnyard2 database. It is then displayed on the Basic Analysis and Security Engine (BASE), a web-based tool. And then the logs will be analyzed accordingly.

2.2. Network Simulation Design

This research experiment was conducted at the TIC Timor IP premises which is part of the government's data center. The current network topology in TIC Timor IP has 2 routers and 4 firewalls. The below diagram is the current network topology in Tic Timor IP as shown in Figure 2.

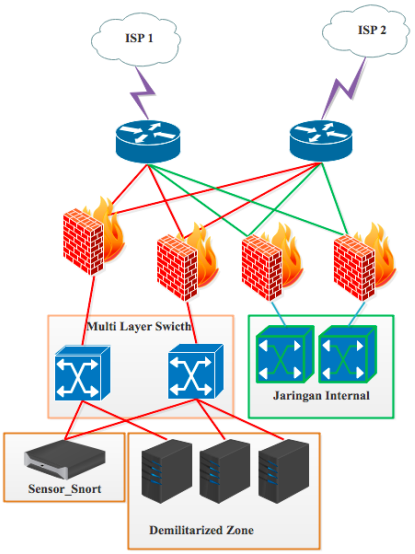

Figure 2. Exiting Network

Figure 2 is the current network architecture at TIC Timor IP which will be employed in this research project to analyze web server attacks. This research was done on Tic Timor IP that is

part of government-owned data storage. Currently network topology used star topology. This simulation analysis only focuses on the webserver and topology design as shown in Figure 3.

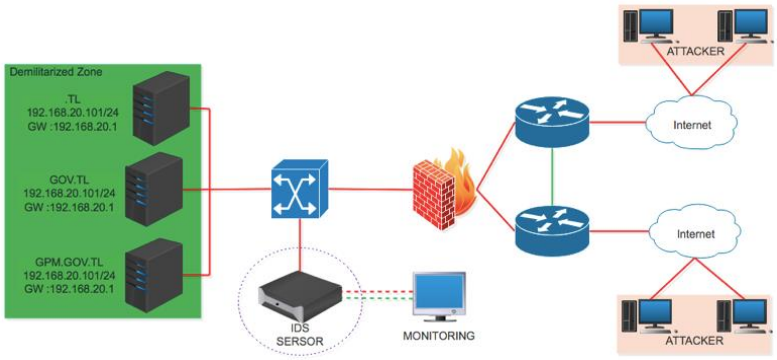

Figure 3. Network Analysis Design

Figure 3 is intended to make clearer attack architecture. In this architecture, there is attacker doing attack over server. Attacker sent attack package through internet network connected directly to router passed to firewalls. In firewall, attack package was passed to Multi Layer Switch. In the switch it was set using trunking and passed to snort. In snort, the package was analyzed whether it is attack or not. When the package is stated as an attack snort will give warning that the package is an attack. When the package is not attack the package will be passed to server.

Table 1 Detail of IP Address

No	Device	IP Address	Subnet Mask	Gateway
1	Vlan 10	192.168.0.100	255.255.255.240	192.168.0.1
2	Vlan 11	192.168.0.117	255.255.255.240	192.168.0.1
3	Vlan 12	192.168.0.133	255.255.255.240	192.168.0.1
4	Server IDS (Trunking)	192.168.0.107 192.168.0.109 192.168.0.135	255.255.255.240 255.255.255.240 255.255.255.240	192.168.0.1 192.168.0.1 192.168.0.1
5	Web Server .TL GOV.TL GMP.GOV.TL	 192.168.20.101 192.1682.20.105 192.168.20.110	 255.255.255.240 255.255.255.240 255.255.255.240	 192.168.1.2 192.168.1.6 192.168.1.10

2.3 Snort Configuration

After the installation phase, Snort needs to be configured to run as expected. There are basic settings needed to be configured to run the application as desired. One important configuration file that needs to be configured is snort.conf as shown below:

```
Ipvar HOME_NET 192.168.20.0/24
Ipvar EXTERNAL_NET !$HOME_NET

Var RULE_PATH /etc/snort/rules
Var SO_RULE_PATH /etc/snort/so_rules
Var PREPROC_RULE_PATH /etc/snort/preproc_rules

Var WHITE_LIST_PATH /etc/snort/rules
Var BLACK_LIST_PATH /etc/snort/rules
```

2.4 Configuration Rules

Snort utilizes rules to carefully examine all the packets that pass through in the network traffic. Rules have two parts, namely the *rule header* and *option*, where rule header includes action header, ICMP protocol, source IP address, destination IP address and destination ports while option consists of message option, reference, types and others. An example of the rules can be seen in the below figure 4.

```
alert icmp any any -> $HOME_NET 80 (msg:"Ping of Death"; sid:1000001; rev:001; classtype:ICMP-Event)

alert tcp any any -> $HOME_NET 139 (msg:"SQL Injection Attack"; sid:1000002; rev:001;
flow:to_server, established classtype:Attempted-user; priority:5)

alert udp any any -> $HOME_NET 68 (msg:"DHCP Attacks"; sid:1000003; rev:001)

alert tcp any any -> $HOME_NET 23 (msg:"Telnet Attacks"; sid:1000004; rev:002)

alert tcp any any -> any 25 (msg:"Trojan Jaringan Terdeteksi"; sid:1000005; rev:002;
classtype:trojan-activity; priority:2)

alert tcp any any -> $HOME_NET 443 (msg:"Web Attack Detection"; flow:to_server,established;
 classtype:web-application-activity; sid:1000006; rev:002;)
```

Figure 4 Snort Rules

Snort rules can be categorized into two parts such as [10]:

a. The Rule Header is the part in which rule actions are identified. Alerts, Logs, Passes, Activates, Dynamic, and others are among the important actions used in the configurations of snort rules.
b. The Rule Option is the part where alert messages are identified.

3. RESULTS AND DISCUSSION

3.1 System Analysis Testing

IP Scanning Testing

The first attack experiment uses Angry IP Scanner to scan active IP addresses. This attack will display all active IP address in blue color as shown in figure below. Before an attack is carried out to a webserver, it is essential to find out which IP addresses are currently active and inactive. Figure 6 shows the result of the Angry IP Scanner.

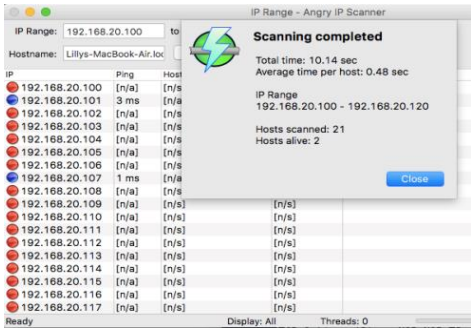

Figure 5. Process of *Scanning IP Address*

Port Scanning Testing

The next step is the port scanning which uses zenmap application. It aims to get information on the active ports. After having the knowledge of active IP addresses on the network, the next phase is to look for open ports, as shown in Figure 6.

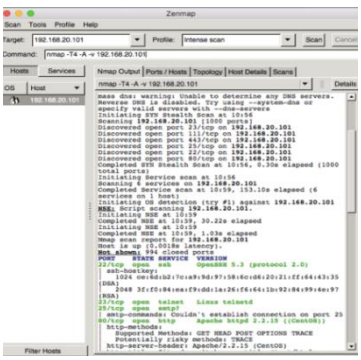

Figure 6 . Port Scanning Testing

Figure 6 is showing a successful Zenmap attack. This experiment is done by sending packets to the victim's IP address: 192.168.20.101. The result of the Zenmap scan displays a list of open ports on the victim's IP address. However, the port scanning using Nmap will end automatically as soon as ports information are captured. Meanwhile, the snort-based rules can also be configured to detect port scanning attacks. Shown in Figure 7.

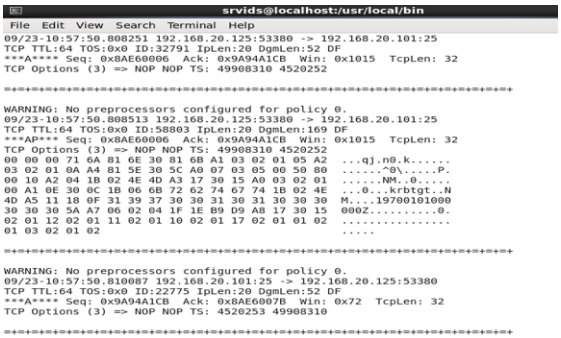

Figure 7. Traffic detect

UDP Flooding Testing

After having obtained the active IP addresses, the next step is to implement attacks the webserver. This attack is performed by using Ping Flooding. The figure shown below is UDP flooding attack experiment on the webserver directed to the IP address of 192.168.20.101, as shown in Figure 8.

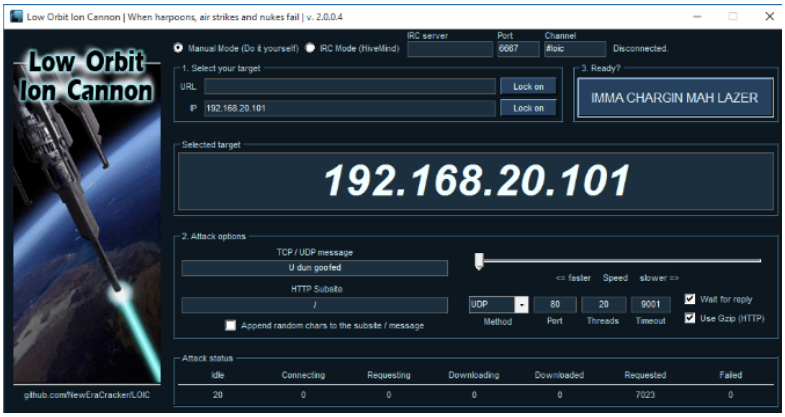

Figure 8. UDP flooding Attack

Figure 9 is an experiment of UDP flooding attack where packets are simultaneously sent to port 80 with data threads 40 and 19320 requests. This UDP flooding attack will result in traffic overloaded on the target computer as shown in Figure 9.

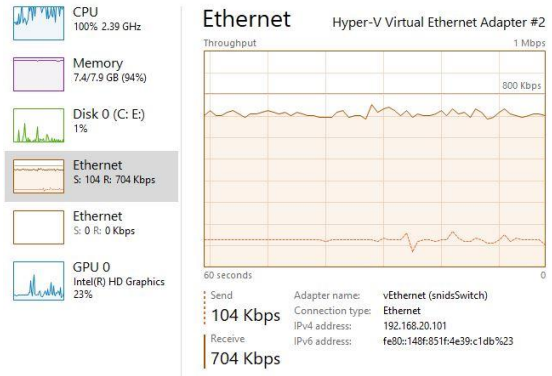

Figure 9. UDP attack occurred

In this experiment, the snort intrusion detection system will detect and send a warning to the administrator, as shown in Figure 10.

```
10/23-13:10:51.750444 192.168.20.127:58894 -> 192.168.20.101:80
UDP TTL:128 TOS:0x0 ID:24890 IpLen:20 DgmLen:40
Len: 12
55 20 64 75 6E 20 67 6F 6F 66 65 64              U dun goofed

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
10/23-13:10:51.750966 192.168.20.127:58888 -> 192.168.20.101:80
UDP TTL:128 TOS:0x0 ID:24891 IpLen:20 DgmLen:40
Len: 12
55 20 64 75 6E 20 67 6F 6F 66 65 64              U dun goofed

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
10/23-13:10:51.751016 192.168.20.127:58888 -> 192.168.20.101:80
UDP TTL:128 TOS:0x0 ID:24891 IpLen:20 DgmLen:40
Len: 12
55 20 64 75 6E 20 67 6F 6F 66 65 64              U dun goofed

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

Figure 10. Detection of udp flooding attacks

TCP Flooding Testing

The second experiment was performed using the TCP Flooding attack. This atack will be carried out on the webserver directed to port 80 with 40 threads of packet. The screenshot of the TCP flooding attack can be seen on Figure 11.

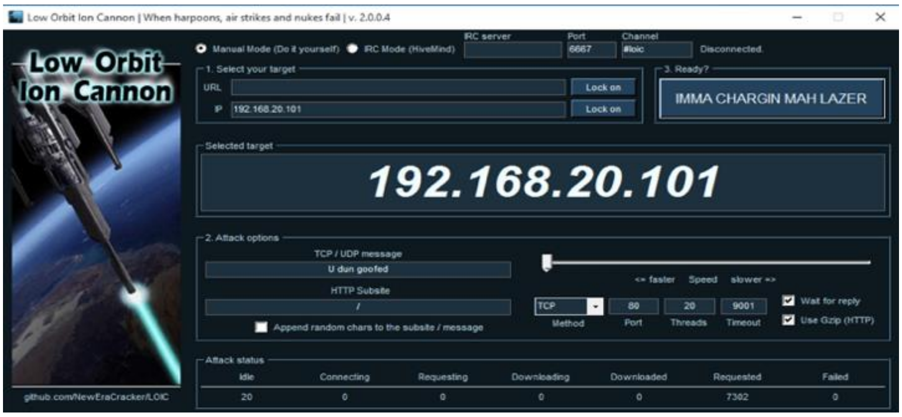

Figure 11. TCP flooding Attack

Figure 12 is showing the victim's network activites are increasing due to the TCP Flooding attack.

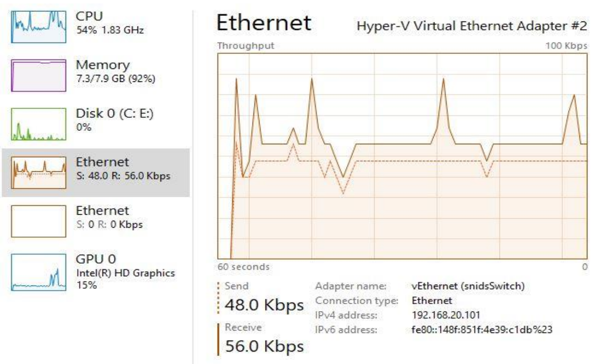

Figure 12. Network Performance monitoring

Based on the research project being carried out, the Snort tool can detect the TCP flooding attack as seen in Figure 13.

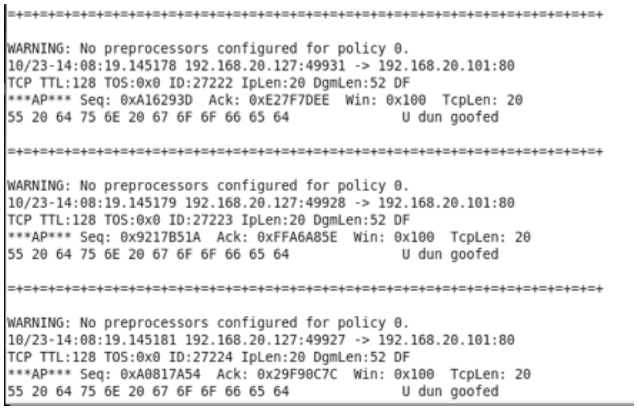

Figure 13. Detection tcp attacks

Ping of death testing

In this section, the attacker uses ICMP ping method on the terminal. This attack was carried out on 2 (two) terminals by sending large packets simultaneously. The attack is shown in Figure 14.

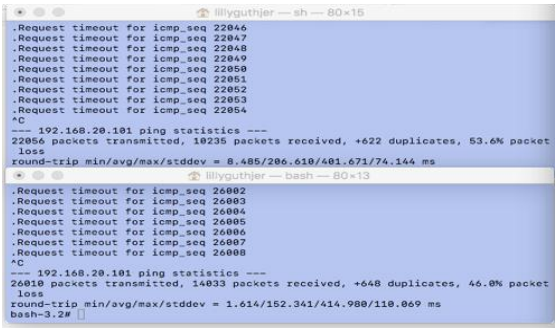

Figure 14. Ping of death

Then, while the attack is taken place on the target IP address, the suspicious activities are captured by the snort IDS server which has been configured to monitor the indicated IP address, as shown in Figure 15.

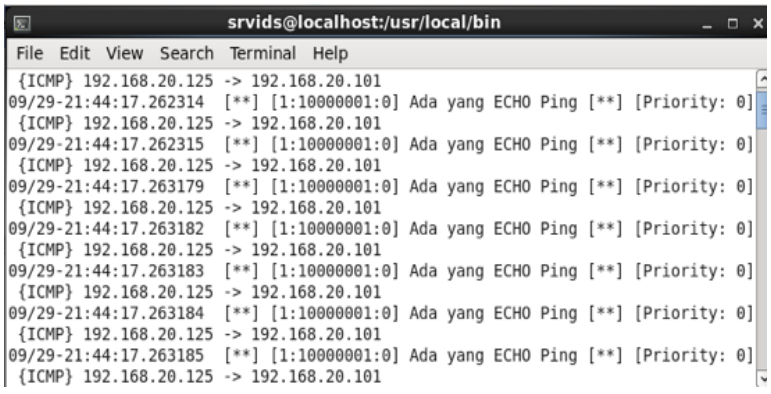

Figure 15. Ping of death Detect

From the attack experiments that have been carried out, log files generated by the Snort application and stored in a barnyard2 database can be displayed on a BASE-web based, and showing the attacks that have occurred.

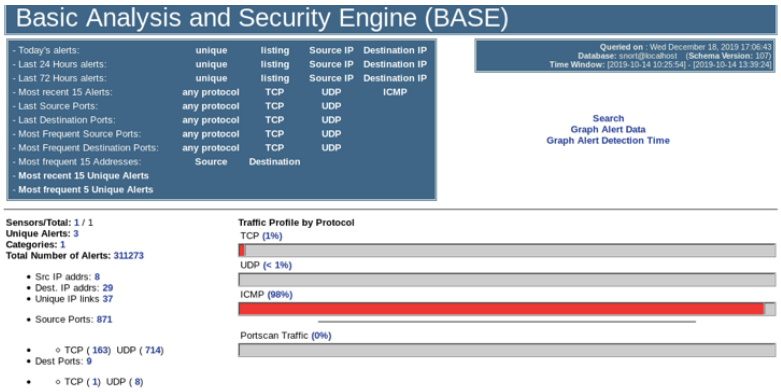

Figure 16. Output Base

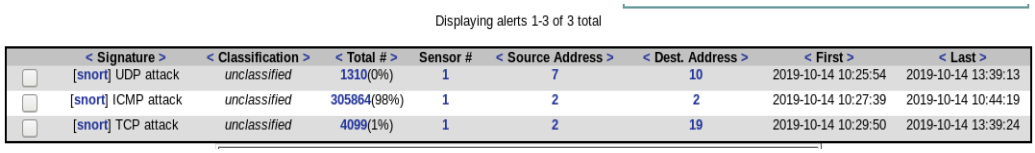

Figure 17. Total Attacks captured

3.2 Results System

The results of the penetration testing which was conducted on the TIC TIMOR IP network can be summarized as follows:

Table 2 Results of system testing

No	Attacks	Threads	Port Number	Resource		Total
				Sent	Recieved	
1	UDP Flooding	40	80	104 kbps	704 kbps	1310
2	TCP Flooding	40	80	480 kbps	560 kbps	4099
3	Ping of Death	40	80	-	-	305864

The results of attacks on the Tic Timor IP network, can be seen in Figure 18.

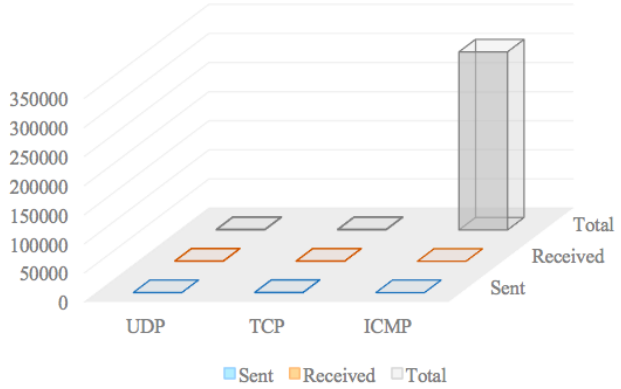

Figure 18. The result of Testing

3.3 Advantages and Disadvantages

The advantage gained from the IDS experiment on this attack can be carried out with several processes in the IDS implementation. The results obtained by the IDS system are capable of detecting and capturing all network attacks that function as sensors and events that occur within the network. However, all these experiments have only been conducted on a simulation system.

4. CONCLUSIONS

Based on the experiment results at the TIC Timor IP with the snort-based intrusion detection system (IDS) method, it is beneficial to implement the traffic rules to generate log files. The result findings of the research can be summarized as follow:

1. Security system on server with rules made for snort can detect DOS attack such as TCP flooding, UDP flooding and ICMP flooding
2. Attack on TCP protocol used memory of 764 Mb with 4099 attacks. Attack on UDP flooding protocol used 9140 Mb memory with total 1310 attacks and for ICMP flooding protocol attack there were 305864 attacks using memory of 5808 Mb

REFERENCES

[1] R. T. Gaddam and M. Nandhini, "An analysis of various snort based techniques to detect and prevent intrusions in networks: Proposal with code refactoring snort tool in Kali Linux environment," in *Proceedings of the International Conference on Inventive Communication and Computational Technologies, ICICCT 2017*, 2017, no. March 2017, pp. 10–15, doi: 10.1109/ICICCT.2017.7975177.

[2] A. Garg and P. Maheshwari, "Performance analysis of Snort-based Intrusion Detection System," in *ICACCS 2016 - 3rd International Conference on Advanced Computing and Communication Systems: Bringing to the Table, Futuristic Technologies from Arround the Globe*, 2016, vol. 01, pp. 1–5, doi: 10.1109/ICACCS.2016.7586351.

[3] N. M. Dahlan M., Latubessy A., "Analisa Keamanan Web Server Terhadap Serangan Possibility Sql Injection," *Pros. SNATIF*, vol. 0, no. 0, pp. 251–258, 2015, [online]. Available: https://jurnal.umk.ac.id/index.php/SNA/article/view/331.

[4] I. Sumaiya Thaseen and C. Aswani Kumar, "Intrusion detection model using fusion of chi-square feature selection and multi class SVM," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 29, no. 4, pp. 462–472, 2017, doi: 10.1016/j.jksuci.2015.12.004. https://doi.org/10.1016/j.jksuci.2015.12.004

[5] S. Ramadhani and Nazwita, "Analisis Sistem Keamanan Web Server Dan Database Server Menggunakan Suricata," *Semin. Nas. Teknol. Informasi, Komun. dan Ind. 9 Fak. Sains dan Teknol. UIN Sultan Syarif Kasim Riau*, pp. 308–317, 2017.

[6] M. Tiwari, "Intrusion Detection System," no. May, pp. 39–57, 2011, doi: 10.1142/9781848164482_0004.

[7] D. Ariyus, *Intrusion Detection System*, I. Yogyakarta: C.V Andi Offset, 2007.

[8] W. Park and S. Ahn, "Performance Comparison and Detection Analysis in Snort and Suricata Environment," *Wirel. Pers. Commun.*, vol. 94, no. 2, pp. 241–252, 2017, doi: 10.1007/s11277-016-3209-9.

[9] C. N. Aditya, "Pembuatan Aturan Snort Sederhana Menggunakan Automated Generation Rules Berbasis Log Honeypot untuk Mendeteksi Serangan Jaringan," Yogyakarta, 2017.

[10] R. Rahmat, *Mengganyang Hacker dengan Snort*. Yogyakarta: C.V Andi Offset, 2010.