# ANALYSIS INTRUSION PREVENTION SYSTEM (IPS) ON COMPUTER NETWORKING

Tamsir Ariyadi<sup>1)</sup>, Aan Restu Mukti<sup>2)</sup>

<sup>1,2)</sup> Faculty of Computer Science, Bina Darma University, Jl. A. Yani No. 3 Palembang Email: tamsir.ariyadi@gmail.com, aanrestu1@gmail.com

Abstract. The development of computer network technology as a medium of communication of the data to date. Intrusion Detection System (IDS) is a system of detection of disorder that is a software application or hardware device that works automatically to monitor events on the network computer and analyse network security problems. IDS is the first signal giver if the intruders trying to break someone's computer security system. In general, the infiltration could mean attacks or threats to the security and integrity of the data, as well as actions or attempted to pass through security systems carried out by someone from the internet as well as from within the system. Intrusion Prevention System (IPS) is an application that works to monitor network traffic, detect suspicious activity and conducting early intrusion prevention or event that can make the network be running unlike as expected with the firewall. It could be due to an attack from the outside and etc. Technology that will help to improve the security of the network. The use of ids and IPS technology will greatly enhance the network security when properly configured and managed in order to protect computer networks. Intrusions prevention system used for active data packet drop or disconnect that contains data that is not valid. Intrusion prevention technology is also often an extension of the technology of intrusion detection (IDS).

Keywords: IDS, IPS, Firewall, Network Security.

#### I. INTRODUCTION

The current situation of the internet where network technology is a dynamic computer needs are very important to streamline all activities in all fields. This development has managed to improve the way social interaction, commercial, political, religious and personal follow the evolution of computer networks globally. In General, the computer network is called a few interconnected computers and communicate with one another using network hardware (Ethernet card, token ring, bridge, modems, and other). Computers that are in a network can perform Exchangetraded information/data with other computers in the network. The user of a computer can see and access the data on other computers in the network when done file sharing.

At the time when the internet is already used by people in different parts of the Earth. In addition to bringing positive impact, the internet also has a negative impact, which caused very threatening new problems, namely the problem of network security. These myriad security threats found by the user such as viruses, Malicious, Trojan, worms, hackers, DoS, Spoofing, Sniffing, Spamming, and other Crackers, which makes uncomfortable and threatening the system and the data at the time of this occurrence are attacking the network. The more a network it will be increasingly complex administration of a network that, therefore. According to Iwan, Sofana (2009) explains that the security of the computer network as part of an information system is very important to maintain the validity and data integrity and ensures the availability of services for its users. The system must be protected from all kinds of attacks and infiltration attempts by Parties not entitled. Computer security systems, in recent years has become a major focus in the world of computer networks, this is due to high threat of suspicious

(Suspicious Threat) and attacks from the internet. Computer security (Security) is one of the keys that can affect the level of Reliability (reliability) including performance (performance) and Availability (available) an internetwork.

Bina Darma University is one of the establishments that its activities are supported by a network of internet services, from processing the data, including the system of KRS online, mail servers and web portals in each work unit. Computer network administrator University of Bina Darma building systems network security by implementing a system of firewalls and proxy servers on each server including server. Security system that uses a firewall and a proxy server is not everything can be controlled, sometimes there is still blamed for hackers, viruses, and so on can be on the firewall. The sophisticated technology that can use a variety of tools to get past firewalls built.

In this study the author would implement the Intrusion Prevention System (IPS) on computer network Bina Darma University as solutions for network security. Where the author is going to implement Intrusion Prevention System (IPS) by using the snort Intrusion Detection System (IDS) and IP Tables Firewall.

### II. RESEARCH METHODOLOGY

2.1 Data Collection Methods

In performing the data collection, the author uses a number of ways including:

1. The study from library, Data obtained through the study of library, namely seeking material from the internet, journals and library as well as books that correspond to the objects that will be examined. 2. Observation, Data collected with a view directly from the object examined on VLAN server Campus University of Bina Darma.

3. Interviews, Data were collected by means of conducting discussions with parties related to IT systems that exist in Bina Darma University to obtain information directly from the sources.

## 2.2 Research Methods

Research methods used in this study using a research method of action or action research. According to a quarter Guritno, Sudaryono, and Raharja (2011:46) Action Research is a form of research stages (applied research) aimed at finding effective ways that result in intentional change in an environment that is partially controlled (controlled).

Action research according to Davison, Martinsons and Knock (2004) i.e. research actions describe, interpret and describe a social situation or at the same time by making a change or intervention with the purpose of improvement or participation. As for the stages of research that is part of this action research, namely:

- 1. Diagnose (Diagnosing)
- 2. Make a plan of action (Action Planning)
- 3. Performance actions (Action Taking)
- 4. Conducting evaluations (Evaluating)
- 5. Learning



Figure 2.1Action Research Method

#### **III. RESULTS**

After gradually researchers do in implementation of Intrusion Prevention System (IPS) on a computer network with snort IDS and IP tables firewall detection as a deterrent of infiltration.

For enable the network intruder detection system mode (Network Intrusion Detection System). Where snort. config file is the name of the place rule-rule Intrusion Detection System is stored. Rule-the rule that has been stored it can decide what action to take against any package found appropriate rule-the rule that has been set. The following is the output with the snort network intrusion detection in Figure 3.1:



Figure 3.1 Output network intrusion detection Next displays the types of RAID port 22 on the server computer that occur in the application of the base as shown in Figure 3.2:



The type of attack that is accessing a web server that is marked on the snort signature that is someone is watching your website by port 22 through port 22 flood the network service.

Notes - Longham Saras Salas 1999 - Al 1993 - Al 1993 - Al	1 start and 2 start and 3 start and 3 start and 4 start and 4 start and 5 start and 5 start and 5 start 5 start and 5 start 5 s			
	AND ADDRESS OF			
E (April of	1744-01	Decis Manual	Contract Automatical	d get i Ber
manne ar Louis Library party of		10-10-10-10-10-1	11000000	22.62
APRES Sades an unklasses and	22359-1585	T & D.D.C.	15.8.024	114
tergenetise, service and any phenomene	2010/08/01 19:51	10100-010-010	CONTRACTOR OF	32
ADDED SHITTER ADDITION	1753A 7575	A. 918-24	14 M 3 CYL	17.8
PETRON ON COMPANY STATEMENT	1012 AV 1842	ISA WAR	1.1.240.000	342
ingens, pair on a takepoorde	PT. 84	111100000	79.0.110	100
device the second process and	2140-0 2010-	E HEID	15.6.52.008	125
ROATE ALL MODELING CONTRACT	Contraction of the local division of the loc	- MET.	And and Address of	100
Abits information and supervise	1124 1289	24072	11.4.516	125
PERSONAL AND DESCRIPTION OF THE OWNER.	100.000.000	IN SUBARY	Turner Laboration	The Party
A MARY & COMMANNEL MARKAN	STARS COM		178 10 114	***
THE PARTY OF AN ANY ANY ANY ANY ANY	water water	THE REAL PROPERTY.	1111111111	12.0
And a second stand of the second state of the	And Ann American	TRANSPORT OF L	1010104	844
PARTY I AND	AP\$ 94.75 (A	P 418 1 1	-1994 (Sec. 1)	81a.
The state of the second second second	2129 - 1822	104 642	124/214	115
THE REAL PROPERTY AND A DESCRIPTION OF	CONTRACTORS.		THE OWNER.	3.7
and a faulter waited function	174644 1715	11 9 11 19	13. 11 CHC	121
THE PARTY OF THE P	100 At 100	CONTRACTOR OF STREET,	THE REPORT OF A	1.1

Figure 3.3 the information attacks through port 80

3.1 Testing Intrusion Prevention System (IPS)

The system that has been created, perform a test against the server that was created, some experimental attacks, among others, as follows:

a. ICMP flood

3.4 delivery images. ICMP flood

Experiment attacks against servers that have been built with ICMP packets sent launched in large sizes so categorized as DOS attack (Denial of Service), as for the process of the invasion begins by opening the command prompt through the client computer and then type the command ping 172.168.10.3 - 1 - 10000 t.

# b. UDP flood



Figure 3.4 the delivery of UDP packet flood

UDP flood hooking two system unawares. By way of spoofing, UDP flood attack will stick to the UDP services, for the purposes of "experiment" will send a group of characters to another machine, programmed to echo each character submissions received through servicing chargen. In Figure 4.14 above an attacker sends a UDP packet flood using UDP Test Tool 3.0 to the server by sending every second.

# c. Port Scanning



Figure 3.5 Scanning port scan

Scanning against the server to get the lay of the shortcomings of the system and find out about the network ports that are open on the server. The experiment is carried out using Net Tools 5.

## d. SYN Flood DoS



#### Figure 3.7 SYN Flood DoS 1

The attacker will send SYN packets into the ports that are listening in a State that is in the target host. Experiment in the image above the target www.binadarma.ac.id and port 80. 3.2 After testing the Server in Server VLAN

After doing a test against the server Intrusion Prevention System (IPS) by doing some of the attacks. Testing done in the VLAN server with server cursor Intrusion Prevention System (IPS). The first step to do is to put a PC network connected sensor Switch in the VLAN server, then through the PC Client monitoring against attack by opening the http://172.168.10.3/base base address as shown below:



#### Figure 3.8 Display Application Base

Next up is the observed forms of attack are already recorded on the database application base such attacks through the protocol TCP, UDP, ICMP and Raw IP, a form of attack that happened can be seen in the pictures below are 3.9:

			Wardso and Disease			Job - Barren ba	
		44					
the int	Contract Contra	or provinging them inter-					
-	and the second second	(Manual)	the name and the pass		and the local division of the local division	Contraction of the	
111						and the second se	
812	E 11110	(a)	the second s			- 18	
-	-	tion in the Party of Street, or other					
-							
1.1.1.		Constant of the second	P Remains P 1	The second second second	1000 00000	10000000	
10	-	provide a set of all of		PERMIT	100000000000000000000000000000000000000	1704	
0.0		particular international and particular international particular intern	01110000 110000	CPU - HE LA LOWING	710,000,000,000	114	
	04 81 85 EV	( percent) (second second to part ))	and and in 1993	10.00.000	- HER SHE SHE SHE WATER	110	
	the second second	proved presented and the part of		File and character.	100 CB 810 BUD 00711	110	
	CONTRACTOR OF	Annual Annual of the local di-		10.0610.00	254 EM (MARCH)		
	-	print immunities, by post of	0011.00.00 11.00.00	100.000.00.000	The two exceptions	194	
	COMMON/	second demonstratives to just of	0.0000000000000000000000000000000000000	10.000	100.000 000 0000	100	
	104-0-005	stated in concern whether and the		THE REAL PROPERTY.	Transaction and Amplication	16.8	
	1004-0004	And summaries in 14	2010-00 NO.	THE REAL PROPERTY.	10.46.4.02	10	
	the bridgets	the second secon		110-100 No.110	- 213 hall do 40"	164	
	100000	particul property which is not 1	24146.H343	170,000,000	20030-014870	100	
	and an owned	period presses where it got it	ALARY DIST.	10% M Page 101	110.000.000	164	
	THE SCHOOL ST	International Action in the later	00 Call (0 MAR 10	10.00.0.00	VALUE AND ADDRESS	1.164	
	the second	state when we do not the		110-108-10-210	100 000 010 000	100	
	CONTRACTOR	Second Annual and the last of	ansasa	PERMIT	2010/06/07 07:00		
		production and the set of the set	artisten 11 mild.	10.000.000.000	100 000 013 0070	110	
1000	-marriers.	and the second second second in	40.0640 (20.06	10.08.0.00	100 045 44 2 104 10	100	
111	data data	second pressed on the part of	4014 (8-4) 10 (8 14	The second second	70.00.000	1(#	
100	- net scattering -	descent) preserve which to used it	antenaria ini ini ini ini ini ini ini ini ini i	12.06.0.00	110 140 414 100111	118-	
	-	the second secon	000 00 00 00 00 00 00 00	Fig. 26 (d. or d)	100 per manager 1	164	
100	COLUMN 1	And the party of the local day of the	C	101204-0.040	CONTRACTOR OF THE OWNER	110	
	000.000	print annual states to post 1	100 ALC: 100	101004-0.000	THE OWN AND INCOME.	10.0	
100	(#10.001)	And the second second to be a set of		10.04.0.00	201000-00200710	CNR)	
	a prime	and senses and to get 1	271.46.0 10.000	10.08.0.00	201208-0120010	108	
100	00e-008.	and a summer state or own 1	-2018-6 H (M)	100.00.01.000.00		CHECK	
18	- P1+- D004	provide press of the part of the	011010-01010	10.00.00.00	11 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	104	
		Including the second se	91100 H 44	10.00.000	199 4 M 4 4 4 4 4 1 4 1 1 4 1 4 1 4 1 4 1 1 4 1	118	
			and the local distance of the local distance				

Figure 3.9 the attack through the TCP protocol The attack through the TCP protocol will look like the picture above look at the Layer 4 Protocol that can slow down and affect network performance.



Figure 3.10 the attack through the ICMP protocol

This type of attack is through ICMP protocol that would overwhelm a network and slow down the network by sending messages namely Community SIP TCP/IP Message DOS flooding self-directed SIP Proxy.

To search for events on a network by using either a BASE according to hours, days, 15 of the latest alert, source and destination port, the frequency of 15 last address and so forth have been made available by the BASE console with snapshot view on the main page of the BASE. As in Figure 3.11 below:



Figure 3.11 Traffic Sensors

## 3.3 Discussion

#### a. Limiting ICMP flood

To test the firewall way launched an attack on the system package are covered by the IPS. On testing this ICMP packet sent in large sizes so categorized as DOS attack (denial of service). By entering the command ping 10.237.3.91 - 110000 - t. Following testing done against the Server client:

Distant Contract of Contract o	The betas - DOWN there - Disc The of the second states - DOWN the second states - Disc The secon	
	.vi: botes=UNDER tide=Ther TTL-	
Carl and the second sec	.VI herri-links the line line	
the four ideally-	The borner-18566 4 ton-Cline III. rid	
als of an inclusion	71 hotax -10400 time-24nn 11,464	
all some second	.73 Vetri-19888 time-Che .71-64	
112 Cran 40.130.1	.71 Vytra-1998 time Chu 77.464	
21s from 10.237-3	1917 Metry 10000 time 2ftrs 111-64	
-1. com 13-512-1	<ul> <li>21 Setts 1000 Core 20cc 11.54</li> <li>21 Setts 1000 Core 20cc 11.54</li> <li>21 Notes 1000 Core 20cc 11.54</li> <li>21 Notes 1000 Core 11.55</li> </ul>	
I SHOW THE PAY.	70 Matter 10000 File-Tille TT. 44	
ale ann Malaye	ATT NYLES-LUMINE & HIR-SHIP TILLING	
1	The second se	
	(1) Note-damping ture-flux T1.464 (2) Notes-damping ture-flux T1.464	
21. 2000 BA. 227-2	A REAL PROPERTY AND ADDRESS OF THE PARTY ADDRES	
al ( 18		
	The weight think have the life the	
71. fran 10.13V.1	[1] Spine Land, Land Cine Till, 54 (21) Series 19980 Class Tile Till 54 (21) Series 19980 Class Tile Till 54 (21) Series 19980 Class Tile Till 54	
21 250 10 217 2	111 Marco 10000 Core Dies III. 61	
The Frank American	13: Betes-19989 time-2hus TIL-64	
	Vi: betro-team con-from These	
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1		

Figure 3.12 Output ICMP Flood b. Limiting UDP Flood



## Figure 3.13 Outputs UDP Test Tool

UDP flood limitation is carried out by entering the target IP, then perform a UDP application delivery Test Tool 3.0 received every 10 seconds. As for the iptables command: # iptables-A INPUT - p - m limit - limit 10/s - j ACCEPT. If the UDP flood attacks then the firewall will respond to and limit it as shown in the picture above, the time span of 4.31 slowed down. c. Port Scan



Figure 3.14 the Output port scanning

After committing attacks against the server, port scanner will change the time range and not properly before it is applied to orders in IP tables. On the application of the Net Tools 5 visible scanning is slowing down not as usually, it's because the firewall is already responding or restrict access to the server. As for rule port scan in IP tables firewall as follows:

Rules	Description	
#iptables -A INPUT -p tcptcp-	Because the function	
flags SYN,ACK SYN,ACK -m	performs port scanning	
statestate NEW -j DROP	detection ports are	
#iptables -A INPUT -p tcptcp-	open, then on the	
flags ALL NONE -j DROP	above firewall IP	
#iptables -A INPUT -p tcptcp-	tables rule that the	
flags SYN,FIN SYN,FIN -j DROP	protocol TCP SYN,	
#iptables -A INPUT -p tcptcp-	ACK SYN, ACK, Fin	
flags SYN,RST SYN,RST -j DROP	SYN, Fin, RST SYN,	
#iptables -A INPUT -p tcptcp-	RST, URG and PSH is	
flags ALL	rejected. IP tables	
SYN,RST,ACK,FIN,URG -j	firewall will do the	
DROP	response to scanning,	
#iptables -A INPUT -p tcptcp-	scan that was done	
flags FIN,RST FIN,RST -j DROP	against port so should	
<i>#iptables -A INPUT -p tcptcp-</i>	be denied access	
flags ACK,FIN FIN -j DROP	because it could	
<i>#iptables -A INPUT -p tcptcp-</i>	interfere with the	
flags ACK,PSH PSH -j DROP	security of the network	
#iptables -A INPUT -p tcptcp-	system.	
flags ACK, URG URG -j DROP		

Table 3.1 The command IP tables firewall port scanning Because the function performs port scanning for detecting open ports, then on the above firewall IP tables rule that the protocol TCP SYN, ACK SYN, ACK, Fin SYN, Fin, RST SYN, RST, URG and PSH is rejected. IP tables firewall will do the response to scanning, scan that was done against port so should be denied access because it could interfere with the security of the network system.

#### d. SYN Flood DoS

After performing an experiment that is allocated by the system receiver can experience the "fullness" and target respond to connections that come up to the earlier SYN packet will enter to the server. Commands in the IP tables firewall: #IPTABLES-A INPUT-p tcp-syn-m limit-limit 3/s-j ACCEPT, look at pictures of 4.33 that nmap done will be responded by the firewall, thus limiting every 3 seconds by the server if there is a SYN flood.



Figure 3.15 Output SYN Flood DoS

After performing an experiment that is allocated by the system receiver can experience the "fullness" and target respond to connections that come up to the earlier SYN packet will enter to the server. Commands in the iptables firewall: #IPTABLES-A INPUT-p tcp--syn-m limit--limit 3/s-j ACCEPT, look at pictures of 4.33 that nmap done will be responded by the firewall, thus limiting every 3 seconds by the server if there is a SYN flood.

#### **IV. CONCLUSIONS**

Based on the results of research and discussion that have been outlined in a study entitled implementation of Intrusion Prevention System (IPS) On campus computer network University of Bina Darma then can be summed up as follows:

- 1. Attacks or infiltration can be prevented by implementation of Intrusion Prevention System (IPS).
- 2. Attacks can be detected or not depends on the pattern of such attacks are in rule IDS or not. Therefore, IDS Manager must regularly update the latest rule.
- 3. The management of the rule needs to be user interface (front end) such as webmin added plugin snort rule.
- 4. The analysis of notes IDS (security event) needs to be added to additional modules such as ACID.
- 5. Update the rule on the firewall should be in the form of a daemon process to process works in realtime.
- 6. Managing the rule should be made individually, can be done.

#### REFERENCES

- [1] (JTB\_Journal of Technology and Business. October 2007).
- [2] Abraham N.S. Jr., Gus h. Alexander. 2009, the journal. Design and Implementation Intrusion Detection System on wireless networks Binus University. Jakarta: BINUS University.
- [3] Andi. 2005. An Administrator on Computer Networks. Yogyakarta: Andi.
- [4] Davison, R M, Martinsons, m. g., Kock, n. (2004), Journal: Journal Information Systems: Principles of Canonical Action Research 14, 65 – 86
- [5] Eslam Mohsin Hassib et. Al. International Journal of Engineering Science and Technology.
- [6] HARTONO, Praise, (2006), Intrusion Prevention Systems: Journal on network based Snort IDS and IP Tables Firewall.
- [7] http://tomicki.net/syn.flooding.php
- [8] http://www.cyberciti.biz/tips/linux-iptables-10-how-to-blockcommon-attack.html
- [9] http://www.linuxtopia.org/online\_books/linux\_system\_administratio n/securing\_and\_optimizing\_linux/Secure-optimize.html

- [10] https://help.ubuntu.com/10.04/serverguide/firewall.html Quarter guritno, S, Sudaryono, and Raharja, u. 2011. Theory and Application of IT Research. Yogyakarta: Andi.
- [11] Rafiudin, grace, 2010. "Hackers with Mengganyang Snort". Yogyakarta: Andi Offset.
- [12] SMARTek journal, vol. 9, no. 3. August 2011:223 229.
- [13] Sofana, Iwan. 2010. & CISCO CCNA COMPUTER NETWORK. Bandung: Informatics.
- [14] Stiawan, Deris., (2010), journal: Intrusion Prevention System (IPS) and challenges in pengembanganya. (Lecturer Department of computer systems WHITE FOB).
- [15] Tom, Thomas. 2005. "Networking Security First-Step". Yogyakarta: Andi OFFSET.