

FIRST 2016

Forum In Research, Science, and Technology

ISSN: 2461-0739



Renewable Energy for Sustainable Development

PROCEEDING INTERNATIONAL CONFERENCE

OCTOBER 18-19, 2016



Held by:



SUPPORTED BY:



International Conference
Forum in Research, Science, and Technology (FIRST) 2016

October 18 – 19, 2016
Palembang, Indonesia

Held by:



State Polytechnic of Sriwijaya – Indonesia

CONTENTS

Contents	ii
Remark from Director of State Polytechnic of Sriwijaya,	iii
Message from Chairman of th Committee	v
Keynote Speaker	vii
Invited Speaker.....	viii
Scientific Committee.....	ix
Organizing Committee	x
Keynote Speaker’s Abstract.....	xi
Invited Speaker’s Abstract	xiv
List of Paper based on Sub Theme.....	xvi
Sub Theme A – Environment (A1-A9).....	1
Sub Theme B – Biomass to Energy (B1-B11).....	10
Sub Theme C – Renewable Energy (C1-C7).....	21
Sub Theme D – Audit Energy (D1-D4).....	28
Sub Theme E – Technology for Energy (E1-E7).....	32
Sub Theme F – Design/Modelling (F1-F17).....	39
Sub Theme G – Economic Sustainability (G1-G4)	56
Sub Theme H – Management (H1-H10).....	60

REMARKS FROM DIRECTOR



AssalamualaikumWaRahmatullahiWaBrakaturuh,
In the Name of Allah, the Most Beneficent, the Most Merciful
May the peace, the mercy, and the blessing of Allah be upon you.

Distinguished Participants, Ladies and Gentlemen,
On the behalf of State Polytechnic of Sriwijaya, I would like to welcome you all to the
International Conference FIRST 2016 on Renewable Energy for Sustainable
Development

Forum in Research, Science, and Technology(FIRST)is a meeting organised to accomodate researchers, academics, businessman, and government to follow up research results, to identify industry needs and to keep updated with the government policies. This forum has moved from national scale into an international conference which is conducted annually by State Polytechnic of Sriwijaya. This year, FIRST brings a theme “Renewable Energy for Sustainable Development”. It is realised that efforts to solve environmental problems that we are facing today need long term potential actions for sustainable development; And renewable energy resources is one of the most appropriate solutions. Therefore discussing about renewable energy automatically deals with sustainable development.

All papers presented in the conference are documented in proceedings. The proceeding features 71 papers divided into several fields including Environment, Biomass to Energy, Renewable Energy, Audit Energy, Technology for Energy, Design/Modelling, Economic Sustainability and Management. In brief, the relations between renewable energy and sustainable development are described with practical cases and several issues relating to renewable energy, environment and sustainable development from both current and future perspectives.

Our thanks are conveyed to the Governor of South Sumaterafor providing us direction and views related to the importance of renewable energy resources. Also appreciation and gratitude to the keynote speakers, H. Alex Nurdin, Governor of South Sumatera Province, Prof. TjandraSetiadi, Ph.D., ITB, Indonesia, and Prof. Dr. Werner Rammensee, Cologne University, Germany. Also to invited speakers,Prof. Dr. ErryYulianTriblasAdesta, International Islamic University, Malaysia, Christian Overfeld, Lucas Nuelle, Germany, Dr. Sonny Zuhuda, International Islamic University, Malaysia,Ir. Tri Mumpuni, Kementerian ESDM dan IBEKA, Indonesia, Ir. Fahrurrozi, M.Si., Business Head Chemicals Group, PT. BASF Indonesia and Head of Business Development, FederasiIndustri Kimia Indonesia ontheirpresentation related to renewable energy for sustainable development.

Further we extend deepest gratitude and high appreciation to all presenters and contributors to make this conference possible and these proceedings published. It is realised that publication of these proceedings are still far from being perfect; however, hopefully it will be useful for energy scientist, engineers, policy makers and any other readers as references for enriching their knowledge .

May God bless us all with the health to make this event a successful and enjoyable one!

Thank you.

Dr. Ing. Ahmad Taqwa, M.T.
Director of State Polytechnic of Sriwijaya

MESSAGE FROM THE CHAIRMAN

BISMILLAHIROHMANIRROHIM,
ASSALAMUALAIKUM WW.,
Good Morning Everyone
May the peace, the mercy, and the blessing of Allah be upon you.

The honorable governor of South Sumatra Province, Bapak H. Alex Noerdin
The honorable Director of State Polytechnic of Sriwijaya, Bapak Dr. Ahmad
Taqwa
Distinguishedspeakers, Presenter, Guests, and Participants,

It is my great pleasure to welcome and thank you very much for your contributions to this renewable energy conference. This conference which will take place on 18 up to 19 of October 2016, is conducted firstly this year through the initiation of Chemical Engineering Department, State Polytechnic of Sriwijaya, aims to exchange the ideas from governments, non-governmental organizations, research and academic institutions, international organizations, and industries, to learn from each other and build on successes that advance renewable energy for sustainable development.

I am very happy to inform that the committee is very lucky to have 3 keynote speakers, i.e Bapak H. Alex Noerdin, the governor of SS province, Prof. Chandra Setiady from ITB Bandung and Prof Werner Ramensee from Cologne University of Germany, who supported us from the very beginning with their capabilities to present, sharing knowledge and experiences with us here as well as the invited speaker i.e Prof. Dr. Erry Yulian Triblas Adesta, International Islamic University, Malaysia, Christian Overfeld, Lucas Nuelle, Germany, Dr. Sonny Zuhuda, International Islamic University, Malaysia, Ir. Tri Mumpuni, Kementerian ESDM dan IBEKA, Indonesia, Ir. Fahrurrozi, M.Si., Business Head Chemicals Group, PT. BASF Indonesia and Head of Business Development, Federasi Industri Kimia Indonesia.

Distinguished Guests, Presenter, and Participants,

On this special occasion, I would like to report that the conference manage to succesfully attract more than 71 academician to present their abstract, i.e from Kuwait, Germany, Algeria, Malaysia, Cambodia and of course Indonesia. Amongst others there 69 abstract to be presented in this seminar under professional selective review. And for that reason, I personally would congratulate you all as distinguished speaker to this event.

This conference has collaborated with two international journal i.e Journal of Engineering and Technological Science, ITB and Gadjah Mada International Journal of Business. All selected papers are then peer-reviewed to meet the publication standard. The peer reviewer of each manuscript is rigorous and concentrates on objective and technical concern to determine whether the research has been sufficiently well conceived, executed and described.

Excellencies, Distinguished Guests, Ladies And Gentlemen

I would also like to give special welcome to Lucas Nuelle, PT. Merck Chemicals and Life Sciences, CV. BestariSetiaAbadi, PT. BangunEnergi, PT. Ditek Jaya, PT. Bank MandiriTbk., PT. Indofood SuksesMakmur and individual who support this conference through sponsorship. I believe that we could never thank you enough for that.

Finally, I expect all participants have memorable moment through this conference and enjoy your stay in Palembang, South Sumatra Province, Indonesia. Thank you.

Sincerely
Chairman of Organizing Committee
H. Firdaus

KEYNOTE SPEAKER



H. Alex Noerdin
Governor of South Sumatera



Prof. Tjandra Setiady, Ph.D
ITB, Indonesia



Prof. Dr. Werner Rammense
Cologne University, Germany

INVITED SPEAKER



Prof. Dr. Erry Yulian Triblas Adesta
International Islamic University,
Malaysia



Christian Overfeld
Lucas Nuelle, Germany



Dr. Sonny Zuhuda
International Islamic University,
Malaysia



Ir. Tri Mumpuni
Kementerian ESDM dan IBEKA,
Indonesia



Ir. Fahrurrozi, M.Si.
Business Head Chemicals Group, PT.
BASF Indonesia and Head of Business
Development, Federasi Industri Kimia
Indonesia

SCIENTIFIC COMMITTEE

1. Prof. Dr. Erry Yulian Triblas Adesta, IPM., Ceng., MIMechE
IIUM, Malaysia
2. Prof. Dr. Werner Rammensee
Cologne University, Germany
3. Dr. Sonny Zuhuda
IIUM, Malaysia
4. Prof. Ir. Subriyer Nasir, M. Sc., Ph.D
Universitas Sriwijaya, Indonesia
5. Prof. Dr. Hj. Badia Perizade, MBA
Universitas Sriwijaya, Indonesia
6. Dr. Ali Ridho Baragbah
Politeknik Elektronika Negeri Surabaya, Indonesia
7. Dr. Ismet Ilyas
Politeknik Manufaktur Negeri Bandung, Indonesia
8. Dr. Ing. Ahmad Taqwa, M.T.
Politeknik Negeri Sriwijaya Palembang, Indonesia
9. Dr. Eng. Tresna Dewi, S.T., M. Eng.
Politeknik Negeri Sriwijaya Palembang, Indonesia
10. Dr. Ir. Rusdianasari, M. Si.
Politeknik Negeri Sriwijaya Palembang, Indonesia
11. Dr. Ir. Abu Hasan, M. Si.
Politeknik Negeri Sriwijaya Palembang, Indonesia
12. M. Yusuf, S.E., M. Si., Ph.D
Politeknik Negeri Sriwijaya Palembang, Indonesia
13. Dr. Ir. Leila Kalsum, M.T.
Politeknik Negeri Sriwijaya Palembang, Indonesia

ORGANIZING COMMITTEE

- Advisory Board** : 1. Dr. Ing. Ahmad Taqwa, M.T.
2. Carlos RS. S.T., M.T.
3. Ir. IrawanRusnadi, M.T
4. Drs. Zakaria, M.Pd
5. Dr. Ir. Leila Kalsum, M.T
- Chairman** : H. Firdaus, S.T., M.T.
- Vice Chairman** : 1. Ir. Jaksen, M.Si
2. AhyarSupani, S.T., M.T.
- Administrator** : 1. Firdaus, S.E., MM.
2. HariMulyono, S.E., MM.
- Secretary** : Dr. Ir. Rusdianasari, M.Si
- Vice Secretary** : Eviliana, S.Pd
- Treasurer** : Yuniar, S.T., M.Si.
- Vice Treasurer** : LetyTrisnaliani, S.T., M.T.

Committee Members

1. Ir. Zulkarnaini., M.T
2. Dr. Martha Aznuri, M.Si
3. Dr. Eng. TresnaDewi, M.Eng
4. M. Yusuf, S.E., M.Si., Ph.D
5. M. Miftakul Amin, S.Kom., M.Eng
6. Drs. MochamadAbsor, M.T
7. Dr. Ir. Abu Hasan, M.Si
8. Ir. SelastiaYuliati, M.Si
9. Zurohaina, S.T., M.T
10. Ir. AisyahSuciNingsih, M.T
11. Indah Purnamasari, S.T., M.Eng.
12. Suyanto
13. Baheramsyah
14. Prandoko
15. Hermanto

ANALYSIS INTRUSION PREVENTION SYSTEM (IPS) ON COMPUTER NETWORKING

Tamsir Ariyadi¹, Aan Restu Mukti²

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 Exchange-traded 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

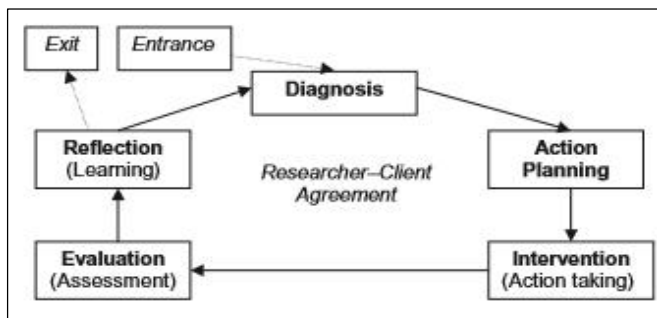


Figure 2.1 Action Research Method

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:

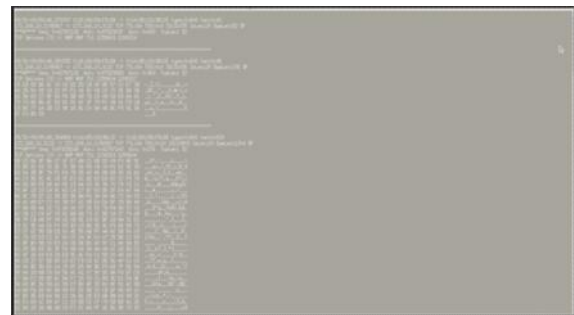


Figure 3.1 Output network intrusion detection Next displays the types of RAID port 22 on the server computer that occur in the application of the base as shown in Figure 3.2:

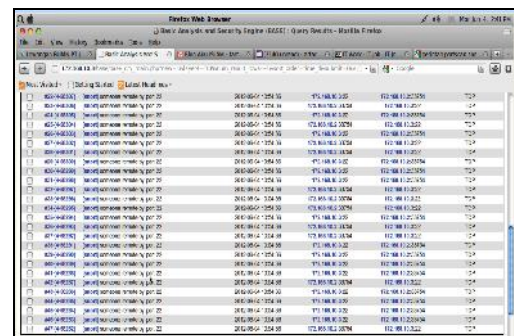


Figure 3.2 Information attacks through port 22

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.

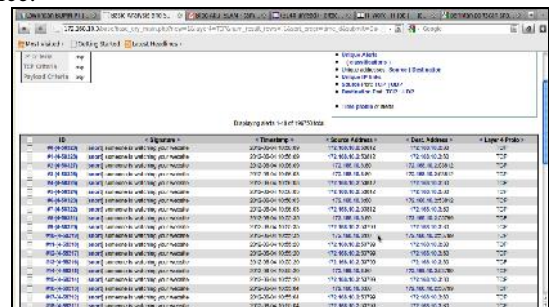


Figure 3.3 the information attacks through port 80

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 -l - 10000 t.

b. UDP flood

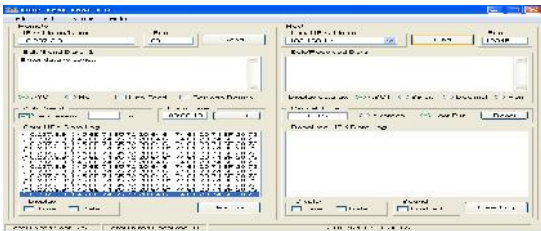


Figure 3.4 the delivery of UDP packet flood

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

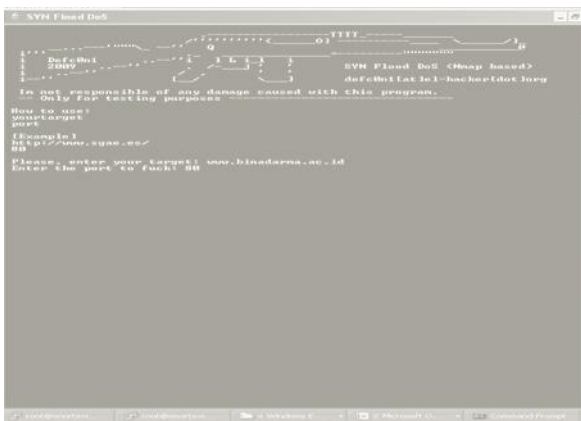


Figure 3.7 SYN Flood DoS 1

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:

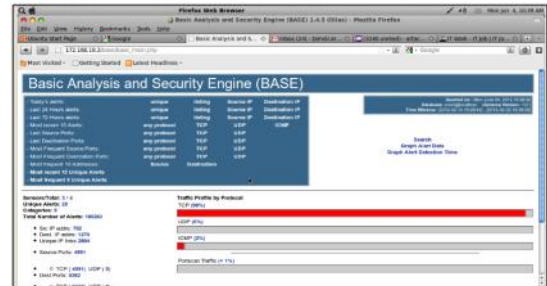


Figure 3.8 Display Application Base

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:

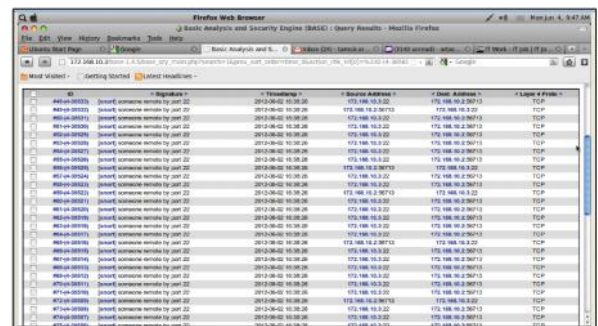


Figure 3.9 the attack through the TCP protocol

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.

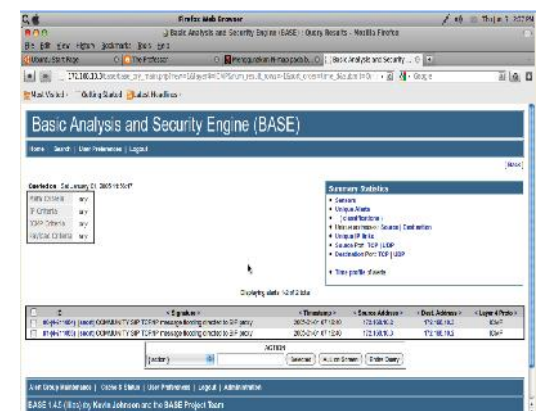


Figure 3.10 the attack through the ICMP protocol

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 -l 10000 -t. Following testing done against the Server client:

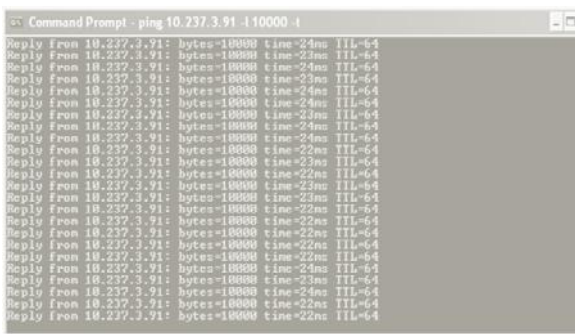


Figure 3.12 Output ICMP Flood

b. Limiting UDP Flood

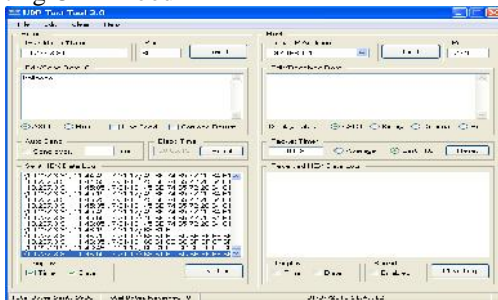


Figure 3.13 Outputs UDP Test Tool

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

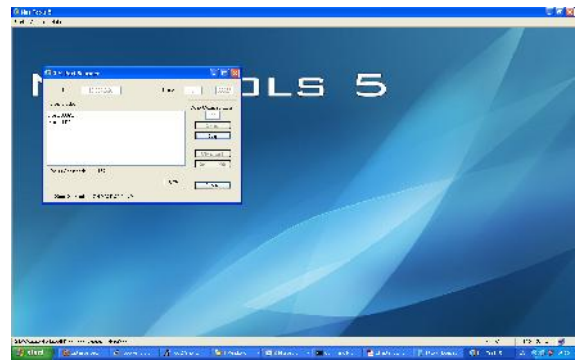


Figure 3.14 the Output port scanning

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
<code>#iptables -A INPUT -p tcp --tcp-flags SYN,ACK SYN,ACK -m state --state NEW -j DROP</code>	Because the function performs port scanning detection ports are open, 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.
<code>#iptables -A INPUT -p tcp --tcp-flags ALL NONE -j DROP</code>	
<code>#iptables -A INPUT -p tcp --tcp-flags SYN,FIN SYN,FIN -j DROP</code>	
<code>#iptables -A INPUT -p tcp --tcp-flags SYN,RST SYN,RST -j DROP</code>	
<code>#iptables -A INPUT -p tcp --tcp-flags ALL SYN,RST,ACK,FIN,URG -j DROP</code>	
<code>#iptables -A INPUT -p tcp --tcp-flags FIN,RST FIN,RST -j DROP</code>	
<code>#iptables -A INPUT -p tcp --tcp-flags ACK,FIN FIN -j DROP</code>	
<code>#iptables -A INPUT -p tcp --tcp-flags ACK,PSH PSH -j DROP</code>	
<code>#iptables -A INPUT -p tcp --tcp-flags ACK,URG URG -j DROP</code>	

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.

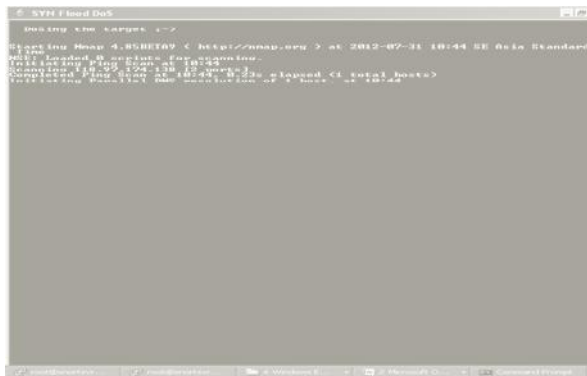


Figure 3.15 Output SYN Flood DoS

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-block-common-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.



9 772461 073015

STATE POLYTECHNIC OF SRIWIJAYA
PALEMBANG
INDONESIA
2016