INTERNATIONAL JOURNAL of DYNAMICS in ENGINEERING and SCIENCES (IJDES)
LLDIKTI WILAYAH X
Vol. 8, No. 1, Mei 2023
e-ISSN: 2502-0692

Network Security with Snort Using IDS and IPS

Hasri Awal*[1], Aulia Fitrul Hadi[1], Ruri Hartika Zain[3]
[1,2,3] Universitas Putra Indonesia YPTK Padang
Jl. Raya Aru, Padang, Indonesia

doi. 10.22216/jod.v8i1.2379
*Correspondence should be addressed to hasriawal@upiyptk.ac.id

Article Information

Submitted
15 Mar 2023

Accepted :
20 May 2023

Published
30 May 2023

Abstract

Mayor's office paddock is place mayor along ranks carry out duties and powers in accordance the job they do live it , of course the data stored is also there inside. Moment This not enough maximum security office network mayor paddock make party office not enough be wary attack from outside . So from That mayor need method increase system server security. The method used is IDS (Intrusion Detection System) and IPS (Intrusion Prevention System). The goal can know results attack as well as secure something server network using snort with based on IDS and IPS. Benefits obtained _ that is with he made system security network with snort app uses IDS and IPS methods then can increase system security network office . Based on results and discussion obtained in conclusion , that the snort has designed and configured with Good capable detect manipulated attack with port scanning and also Ping Of Death performed by the attacker against the server and then prevented with enable firewall features through configuration IPTables.

Keywords: office mayor field , security network , snort, intrusion detection system, intrusion prevention system

1. Introduction

The Padang City Hall is the place for the mayor and his staff to carry out their work in accordance with their duties. The Mayor of Padang who is currently serving is Mr. Hendri Septa, B.Bus.(Acc), MIB who was born in Padang City, West Sumatra, September 6 1976. The location of the Padang City Hall is located Jl. Bagindo Azis Chan No. 1, Aie Pacah, Balai Gadang, Kec. Tangah City, Padang City. The lack of maximum network security at the Padang Mayor's office made the office less aware of attacks from outside . computer network is A system consisting from a number of computer components and interrelated devices relate through transmission cable or wireless [1] . Moment This security network is very necessary , a lot exploitative crime _ gap security without case especially before [2] . Snort is an open source software that has many functions that really help administrators in dealing with threats that have occurred. [3] . Snorts are open source with the GNU General Purpose License license so that this software can be used to secure server systems without having to pay license fees [4]. , the Snort system can be placed in several places in the network, either through the client or above between the switch and the router and several other placements according to network specifications [5] . In practice, snort is very reliable in logging packets and analyzing traffic in real time in a TCP/IP-based network.

IDS (Intrusion Detection System) is a method that automatically monitors suspicious network traffic [6]. This IDS is able to provide a warning to the administrator if an attack or misuse occurs in the network, the warning can even show the IP address of an attacker's system [7] . The ability of IDS to detect all port scanning activities is because IDS is placed on a computer that acts as a gateway and also functions as a firewall [8]. . Placement of IDS on this gateway server will protect data on the gateway server from hacker attacks [9] . IPS monitors packet traffic in real time with

malicious activity or according to a certain profile and will trigger alerts, perform drops, block traffic through the network in real time [10]. Intrusion Prevention System (IPS) is able to provide protection 24 hours non-stop, IPS itself is used as an initial preventive measure against everything that happens between clients and servers [11]. Using this device greatly facilitates network security administrators to maximize network security. By therefore using an Intrusion Prevention System (IPS) is highly recommended. Especially if the scale of the computer network is very large.

Research Methods

This study aims to understand the object under study as a whole, both in the form of problems faced by the research object or other problems that occur in the research object. This research can conclude whether or not a research object is suitable for the research theme raised by the researcher himself. At stage This discuss about collection of data and information . In do study For get data and information , then method in the process of data collection is carried out with stages.

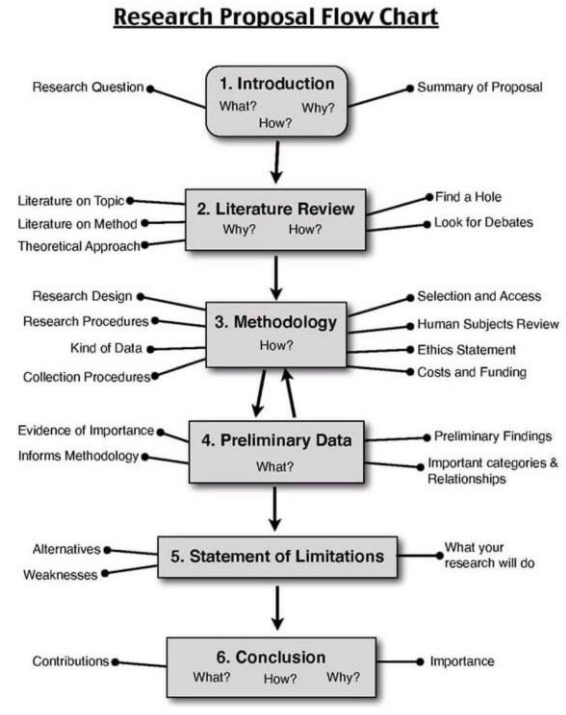

Figure 1. Reseacrh Flow Diagram

This study aims to understand the object under study as a whole, both in the form of problems faced by the research object or other problems that occur in the research object. This research can conclude whether or not a research object is suitable for the research theme raised by the researcher himself.

Results and Discussion

At stage This discuss about later required parameters used in planning system snort safety . Following some of the parameters used :

A. Virtual machine creation : perform virtual machine installation for add service .
B. Ubuntu installation : system Ubuntu operation is used as the Snort configuration server .
C. Installation IpTables : IpTables used For do blocking to attack to servers.

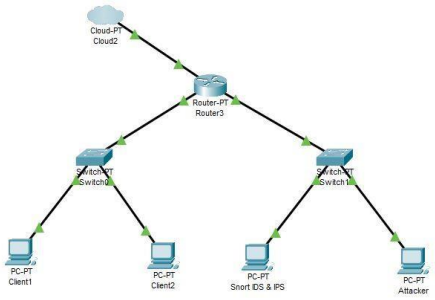

Figure 2. Design Of Snort topology

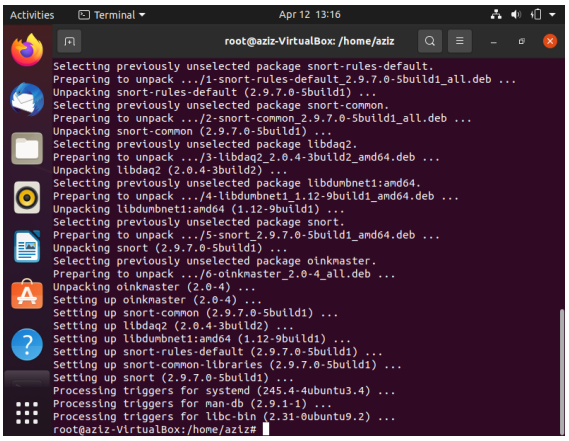

Figure 3. Snort Installation

Steps snort installation and configuration as following :

#sudo apt-get install snort
To install snort on Ubuntu

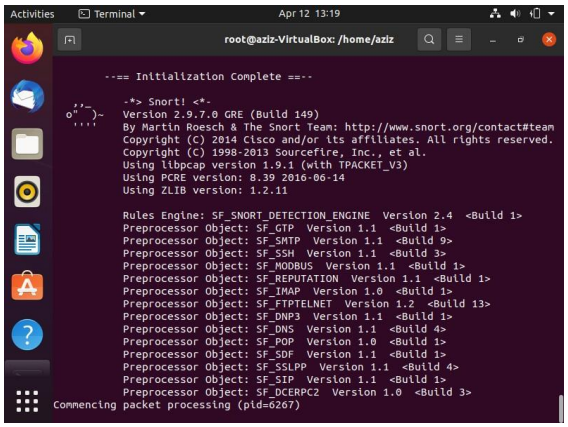

Figure 4. Activate Monitor Current Network

In this design the author uses the HIPS method. Host-based Intrusion Prevention System (HIPS) is a prevention system consisting of several layers of security that uses packet filtering, status inspection and methods, real-time countermeasures to keep the host or server in a state of proper performance. The working process is to prevent malicious code or ports that enter the host from being executed without the need to check the threat signature.

The design of the attack aims to test the system when receiving an attack. In this study the attack used is port scanning. Port scanning is an attack to obtain target information. The goal is to request icmp and tcp ports to get information through those ports. Attacks through port scanning can be done using the nmap application. Here's the configuration:

1. To scan the target computer network, run the following command: #nmap 192.168.181.242 –sP. From the picture above it can be seen that there are several hosts that have been scanned. The -sP command is executed so as not to display open ports on the computer being scanned.
2. After scanning using nmap, the server captures incoming packets in the form of logging packets.

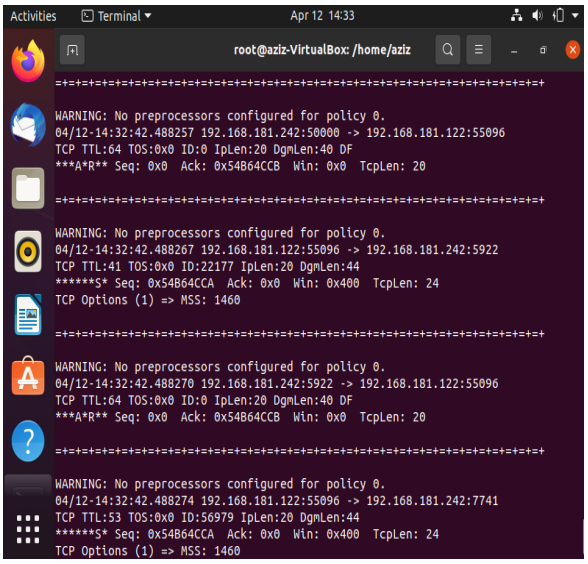

Figure 5. Snort Catch Logging Package

It can be seen in Figure above above that the server catches packets sent that are too large, causing "Bad Traffic" or the flow of network traffic to be chaotic.

QoS (Quality of Service)

QoS calculations can be done through several parameters that will be measured depending on the type of service. Here are some parameters on QoS:

Throughput category	throughput	Index
Very good	100%	4
Good	75%	3
Currently	50%	2
Bad	< 25%	1

Table 1. Throughput Category

To calculate throughput, the formula is used:

$$\text{Throughtput} = \frac{\text{Amount of data sent}}{\text{Data sending time}}$$

Delay is the time required for data to travel the distance from origin to destination. Delay can be affected by distance, physical media, congestion or long processing times.

To calculate the average delay, the formula is used:

Average delay = Total Delay
Total Packages received

Jitter is a measure of the time variation between arrivals of data packets sent over a network. To calculate jitter, you can calculate the average absolute deviation of the time difference between packet arrivals.

Degradation Category	Peak jitters	Index
Very good	0 ms	4
Good	0 to 75 ms	3
Currently	75 to 125 ms	2
Bad	125 to 225 ms	1

Table 2. Jitter Category

To calculate the jitter, the formula is used:
Jitter = Total Variation of Delay
Total Packages received – 1
The total delay variation is obtained from the sum of:
(delay 2 – delay 1) + (delay 3 – delay 2) + … + (delay n – delay (n-1))

Attack Testing With Port Scanning
Port Scanning is a command to view detailed open ports on the target host. To run Port Scanning, you need tools, namely Nmap. Nmap (Network Mapper) is an open source tool useful for auditing and exploring network security. The following is testing the attack using Port Scanning:

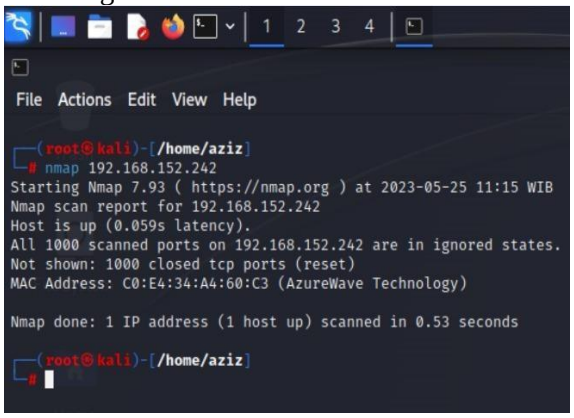

Figure 6. Nmap is running

Iit can be seen that nmap has been run and port scanned the server's ip address, namely 192.168.152.242, where nmap uses ip in a sophisticated way to determine which hosts are available on the network, what services are provided, what operating system is used, what type firewall used, and a number of other characteristics.

Figure 6. Ping of Death run

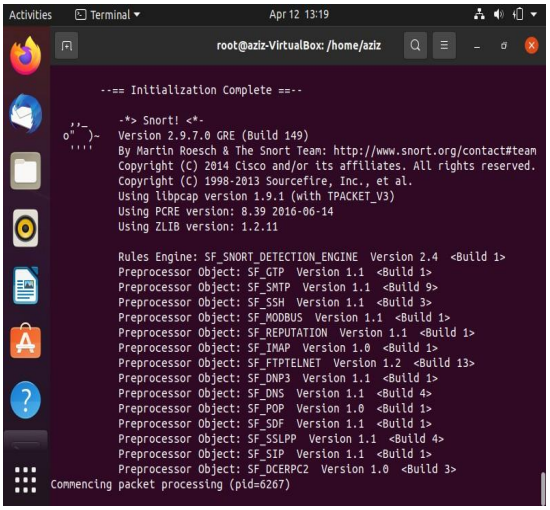

Figure 7. Snort Enabled

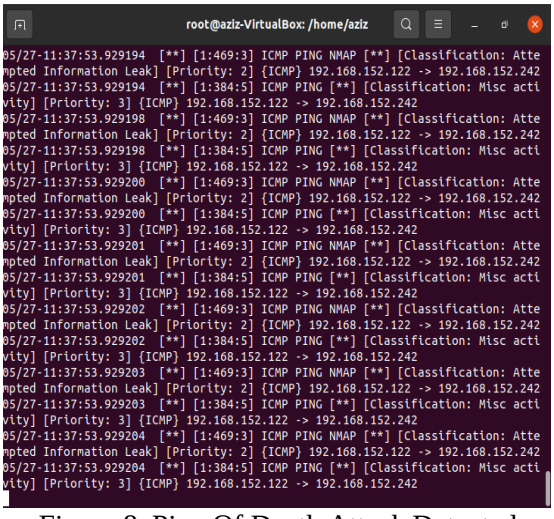

Figure 8. Ping Of Death Attack Detected

CONCLUSION

The network security system can be implemented virtually by using VM VirtualBox as the console prompt and configured using the Ubuntu operating system as the snort configuration. For attackers, the authors use the virtual-based Kali Linux operating system with D-Dos and Ping Of Death tools as a simulation of an attack on the server.

2. Snort IDS is a software that functions to detect intruders and is able to analyze real-time traffic, it can detect various types of attacks. Features in the snort software can help network system administrators because they are able to warn us of intruders who are potentially dangerous to the server.

3. Snort which has been well designed and configured is able to detect attacks simulated by port scanning and also Ping Of Death carried out by attackers against servers and then prevented by activating firewall features via iptables configuration.

BIBLIOGRAPHY

[1] J. Education et al. , “EduTIK: Journal of Information and Communication Technology Education Volume 1 Number 5, October 2021,” vol. 1, no. 19, pp. 528–541, 2021, [Online]. Available: https://ejurnal.unima.ac.id/index.php/edutik/article/view/2922

[2] J. Lirama et al. , “IMPLEMENTATION OF INTRUSION DETECTION SYSTEM (IDS) TO DETECT METASPLOIT EXPLOIT ATTACKS,” no. April, pp. 41–50, 2023.

[3] VARBarao, RCCoata, JAShibli, M.Bertolini, and JGSSouza, “No主観的健康感を中心とした在宅高齢者における 健康関連指標に関する共分散構造分析Title,” Braz Dent J. , vol. 33, no. 1, pp. 1–12, 2022.

[4] I. Gede, W. Bangga, and SM Ladjamuddin, "Snort Simulation as an Intrusion Detection Tool on Web Damn Vulnerable Web Applications," J. Engineering Inf. , vol. 11, no. 2, 2022.

[5] Y. Abdulloh, J. Triyono, and U. Lestari, "The Influence of Snort Placement on Network Security (Case Study of Campus Vi Campus Network 3 Ist Akprind Yogyakarta)," J. JARKOM , vol. 8, no. 1, pp. 10–19, 2020.

[6] ZA Tyas, A. Firdonsyah, and W. Ramdhani, "Network Security Analysis of DoS Attacks on the Inventory System of the Natya Lakshita Dance Studio using IDS," INFORMAL Informatics J. , vol. 7, no. 3, p. 258, 2022, doi: 10.19184/isj.v7i3.34943.

[7] I. Ramadhan, "Network Security Monitoring with Snort Ids Using Network Forensic Methods (Case Study: Cv.Trie m Gunung Mas Sejahtera)," J. Ilm. MIKA AMIK Al Muslim , vol. 3, no. 1, pp. 13–18, 2019.

[8] M. Anis, A. Hilmi, and E. Khujaemah, "Network Security Monitoring With Intrusion Detection System," J. Tek. inform. , vol. 3, no. 2, pp. 249–253, 2022, [Online]. Available: https://doi.org/10.20884/1.jutif.2022.3.2.117

[9] M. Anif, S. Hws, and MD Huri, "Application of Intrusion Detection System (IDS) with the Port Scanning Detection method on Computer Networks at Semarang State Polytechnic," J. TELE, Vol. 13 Number 1 , vol. 13, no. 1, pp. 25–30, 2015.

[10] H. Alamsyah, R. -, and A. Al Akbar, "Network Security Analysis Using Network Intrusion Detection and Prevention System," JOINTECS (Journal Inf. Technol. Comput. Sci. , vol. 5, no. 1, p. 17, 2020, doi: 10.31328/jointecs.v5i1.1240.

[11] MA Prabowo, U. Darusalam, and S. Ningsih, "Linux Server Security Design With Hardening Methods at Layer 1 and Layer 7," J. Media Inform. Budidarma , vol. 4, no. 3, p. 591, 2020, doi: 10.30865/mib.v4i3.2157.