INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2024, VOL. 70, NO. 2, PP. 449-453
Manuscript received July 3, 2023; revised June, 2024. doi: 10.24425/ijet.2024.149565

Detection using Intrusion Detection System (IDS) and SMS Gateway Controller

Muhammad Arhami, Akhbar Arianda, Akmalul Fata, Yassir, Anita Desiani, and Muhammad Arifai

***Abstract*—Intrusion Detection System and SMS controller with Snort using SMS Gateway on public networks. The need for an attack detection system that can assist administrators in monitoring the network, so that administrators can cope with threats quickly and the network can operate optimally again, the purpose of this study is to facilitate network administrators in preventing and detecting attacks. this has been tested against ping of death attacks, sql injection, sysflooding attacks and port scanning. From the results of testing the system that has been tested, the system has been able to detect and prevent it quickly via SMS controller integrated with gammu as an sms gateway, as for information sent to the network administrator in the form of attack alerts in real time via SMS, the result of attack detection in the form of 4 (four) types of information, namely attack time, attack type, destination IP, and source IP. Blocking attacks is done by sending blocking commands via an sms controller that is integrated with php scripts, bash scripting and iptables, blocking attacks successfully executed after the gammu server receives an SMS reply from the network administrator in an average period of 40 seconds.**

***Keywords*—**Iptables; Sms gateway; Bash script; Snort

I. INTRODUCTION

THE internet has become a familiar medium for all people. Various facilities and activities related to services on average have used the internet as a medium that facilitates work such as sending letters, conversations and exchanging information through social media, watching entertainment, marketing, banking and shopping online, so the internet has become a primary matter for various daily activities, because the average communication and transaction has been carried out with various internet media.

The internet has provided extensive services to the public with various facilities of course by using the principles of the internet network. Service convenience is very necessary because when using internet networks the threat of attacks to the internet network system. The threat can come from anyone who intends to hack into the internet network and take advantage for his person. Attacks on internet network systems can disrupt service to customers and can reduce trust in the supply media.

Internet network security is very important to consider, so to prevent and or overcome these attacks it is necessary to build a system that can detect and prevent attacks that include ping of death, sysflooding attacks, port scanning and sql injection. This built system can analyze what is needed in handling prevention quickly and efficiently against a system that is attacked by irresponsible parties, the system built will be able to detect attacks optimally and realtime against alerts detected in network packets through the creation of Intrusion Detection System (IDS), so that network administrators can find out quickly if at any time an attack occurs, and administrators can take action by blocking the ongoing attack being attacked through an sms controler that is integrated with Gammu as a medium for sending short messages as a message alert system, To build a system that can detect attacks as an intrusion detection system, we need a tool that is snort that is connected to the database as an output alert system and accommodated in a table, and integrated with several programming languages such as i php, bash scripting iptables as firewall and html, so that all tools and systems built are connected to each other.

Detection of attacks carried out by IDS is based on specified rules while Remote Iptables takes precautions through terminating the attacks [1-3].

A. *Ping of death*

Ping of death is a type of DoS attack. The ICMP ECHO_REQUEST message is sent to the system host to check connectivity and expect ECHO_REPLY. In ping of death many systems are used to send several requests to the target system. Ping of death attacks an attempt to saturate the network by sending a continuous series of ICMP echo (ping) requests over a high bandwidth connection to the target host on a low bandwidth connection to cause it to send ICMP back echoreply to each request. ping of death attacks can slow down the network or even disable network connectivity [4].

B. *SYN flooding attack*

SYN *flooding attacks* are specially designed attacks, which employ a flood of SYN packets to consume all the new network connections available on the targeted host, resulting in delays responding to legitimate network connection requests and finally halting service providers. Theoretically, this attack applies to all TCP connections, such as WWW, Telnet, e-mail, and so on. In most UNIX systems, some memory structure needs to be allocated for each TCP connection establishment. Taking the BSD system as an example, the socket structure is used to

Muhammad Arhami, Akhbar Arianda, and Akmalul Fata1 are with Department of Information and Computer Technology, Politeknik Negeri Lhokseumawe, Indonesia (e-mail:

Yassir is with Department of Electrical Engineering, Politeknik Negeri Lhokseumawe, Indonesia (e-mail:

Anita Desiani is with Department 1 of Mathematics, Universitas Sriwijaya, Indonesia (e-mail:

Muhammad Arifai is with Department of Commerce Politeknik Negeri Lhokseumawe (e-mail:

store communication information, such as the protocol used, address information, queue connections, buffers and flags. The purpose of SYN flooding or (DOS) is not to gain unauthorized access to computers or data, but to prevent legitimate users of the service from using it. The attacker's goals are as follows:

1. Flood the network with traffic, thereby preventing legitimate network traffic.
2. Interrupting the connection between the two machines, thereby preventing access to services.
3. Prevent certain individuals from accessing services.
4. Interrupting services to certain systems [5].

C. *SQL injection*

SQL injection is a technique for exploiting a web application using data provided or inserted in an SQL query. How SQL injection works by entering SQL queries or commands as possible input through a web page or command prompt. The web page will take parameters from the user and then make an SQL query entered into the database. Thus, SQL injection can also be said as an activity that deceives queries from the database, so that someone who is not authenticated can find out and get information contained in the database. The SQL injection process can be done by inserting commands into a normal query [3].

D. *Port scanning*

Port scanning is the initial technique for hacking a system, by scanning the port so the attacker will know which ports are vulnerable and easy to attack.

Types of Scans:

- *Connect scan (-sT)*
  This type of scan is to connect to the target port and complete a three-way handshake (SYN, SYN / ACK, and ACK). This type of scan is easily detected by the target system [7].
- TCP SYN *scan (-sS)*
  The most popular and is the default scan for nmap. SYN scan is also difficult to detect, because it does not use a complete 3 way handshake, which is called the half open scanning technique. SYN scan is also effective because it can distinguish 3 state ports, which are open, filter d or close. This technique is known as half-opening scanning because a full TCP connection is not established. Instead, a SYN packet is sent to the target port. If the SYN / ACK is received from the target port, we can conclude that the port is in the LISTENING status. An RST / ACT will be sent by the scanning machine so that a full connection will not be established. This technique is stealth compared to full TCP connect, and will not be recorded in the target system log [8].
- TCP FIN *scan (-sF)*
  This technique sends a FIN packet to the target port. Based on RFC 793, the target system will send back an RST for each closed port. This technique can only be used on UNIX-based TCP / IP stacks [9].
- TCP *Xmas Tree scan (-sX)*
  This technique sends a FIN, URG, and PUSH packet to the target port. Based on RFC 793, the target system will return an RST for all closed ports [10].
- TCP *NULL scan (-sN)*
  This technique turns off all flags. Based on RFC 793, the target system will send back an RST for all closed ports.
- TCP ACK scan (-sA)
  This technique is used to map firewall rule sets, and can help determine whether a firewall is a simple packet filter that allows only certain connections (connections with bit set ACK) or a firewall that runs advance packet filtering [11].

II. RESEARCH METHODOLOGY

A. *System flow diagram*

Attacks made on the internet network can result in decreased network performance, so it needs detection and handling in the event of an attack, in this case the role of the IDS integrated with the SMS gateway is built where the SMS controller remotely ipsables with the SMS gateway.

The process flow chart can be seen in Figure 1 below.

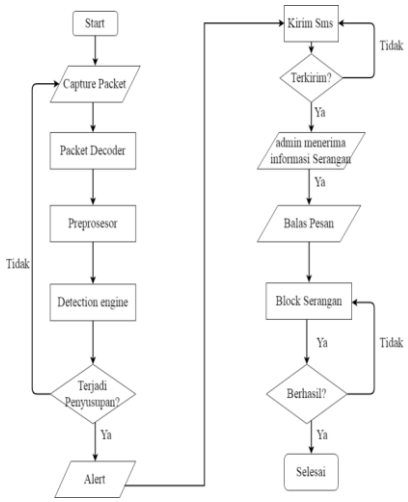

Fig. 1. Flowchart

B. *System planning*

The general system requirements design as shown in Figure 2.

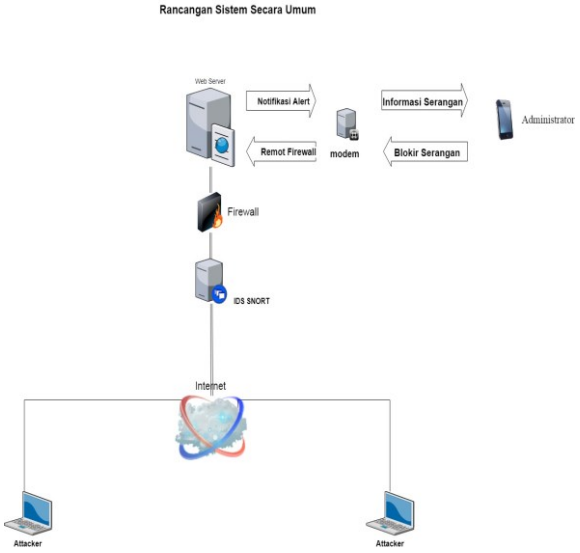

Fig. 2. General System Design Requirements

Figure 2 shows the system design that has been made where the test is done by giving 2 intruders / attackers using a public network connected to the internet. The server section can be seen as an ids firewall, to detect if an attack has occurred, then there is a tool in the form of gammu as a media for a message to be used as an alert message. Gammu lane also built a system controller that can remotely all activities on the server via sms gateway, which is connected with the programming language bash shell and PHP. The sms controller process aims to allow the network administrator to block the attacker if at any time an attack occurs, after an attack is detected, then enter the network administrator's cell phone, then the network administrator blocks the attack by replying to the message from the ids message alert with the specified format and using sms gateway, making it easier for administrators to respond to attacks.

C. *Execution of configuration*

The installation stages perform the stages of installation (installation) of the required software, namely Libpcap, Libpcre, Libdumbnet, Snort, Gammu, Mysql, apache2, PHP, Phpmy admin. The installation stage is done as root so that the generated file automatically has permissionroot.

D. *Execution of snort rules*

Making rules utilizes the rules format set by snort, with the IPSource PortSource -> IPDestination Port Destination (msg: message content) protocol alert format in accordance with the attack character. Making these rules is saved in the directory /etc/snort/rules/local.rules

E. *Execution of blocking syntax*

Creating a blocking syntax, Iptables is integrated with shellscripting to make it easier for administrators to block. The blocking syntax is in the directory / home / akhbar / with the file name blockpod.sh to block the ping of death attack and blockflood.sh to block the SYNfloodingattack attack.

F. *Execution of GAMMU configuration in order to detect and contact modems with database*

Configuring Gammu and Gammu-SMSD. Configuration function is to be able to detect the modem and gammu-smsd configuration to be integrated with the database.

G. *Execution of number of scripts to each other integrated in the system*

Making this script functions to integrate between tools so that the attack information (alerts) from the Intrusion Detection System can be sent via SMS to administrators with 4 (four) types of information, namely time of attack, type of attack, destination IP, and source IP. The information of the attack (alert) is contained in the snort database in 3 (three) different tables, namely the event table contains the time of attack information, the signature table contains the type of attack information and the iphdr table contains destination IP information and source IP. Below is a piece of script to send alerts in the form of attack information.

H. *Testing system*

System performance measurement is the stage where the entire system that has been built, tested where the results of this performance measurement determine whether the system is running optimally.

III. RESULT AND DISCUSSION

The results of the research that has been done is through a short message as a tool to connect between servers and network administrators to get alert information and block attacks. The final result shows that the system has been able to be implemented on a server with a linux u-dead operating system. Testing is done by giving 4 types of attacks alternately in public networks that are globally connected, the system is able to detect attacks quickly and accurately at the time of the attack, and the system the firewall succeeded in blocking attacks carried out by using an sms controller and can remotely integrate a firewall with gammu, then reply to the short message with a specific format that has been determined in the detection and blocking system, the result of the attack in the form of giving several types of attacks, namely:

A. *Ping of death*

Samples of this attack are carried out using the attack method via a reply request from the server with an icmp packet that is owned by the server, the attacker asks for the packet to continue by forcing a full system so that what happens to the server is if the attack is affected by the server going down or an internet connection has decreased rapidly, the results obtained after the intrusion detection system has been successfully implemented and integrated with several other systems that have been built as alert messages in the event of an attack like the one below, the system has successfully detected an attack which will then cause a system alert due to the packet being passed accordingly with the rules of ping of death set in the intrusion detection system. The results of the alerts obtained by the administrator are in the form of notification information that the system is under attack as shown in the following figure 3.

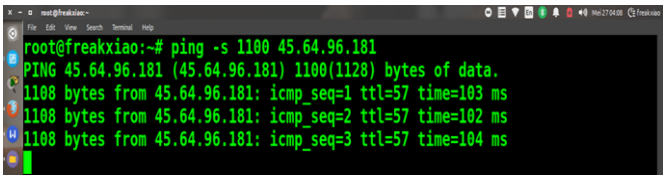

Fig. 3. Attack with ping of death

Remarks:

- ping -s 1100
  command is carried out to attack the server with the ping of death attack technique
- 45.64.96.181
  Public IP, also the IP address of the server attacked by the attacker.

Graph of ping of death attacks can be seen in Figure 4.

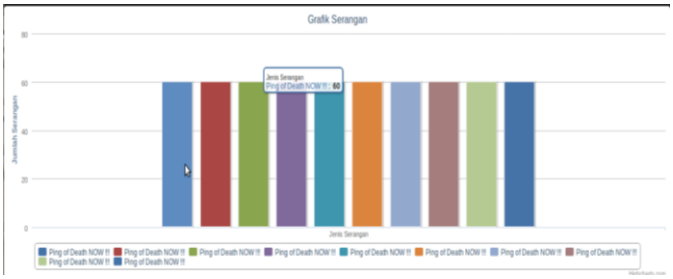

Fig. 4. Graph Number of attacks

Remark:
Displays a graph of attacks with the number of attacks based on the log results of attacks.

B. *Sysflooding attack*

The second attack method is carried out by providing a sysflooding attack on the intended server of the second attack. Two different operating system attacks are carried out, testing at this point is done using Android using the DDOS attack tool and for the second point testing is done using the Linux operating system. by giving the same attack that is sysflooding attack as for the attack can be seen as in Figure 5 below:

1) *Linux operating system*

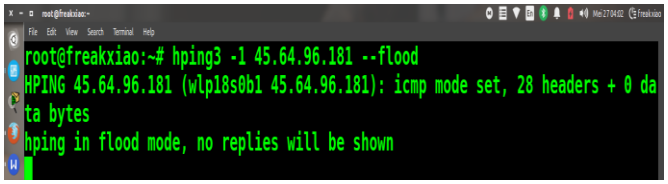

Fig. 5. Attack with Hping3

Remarks:
- Hping3 –l
  Hping3 is a tool for attack / pentester a network to test the strength of a server
  --flood
  This option command is carried out for sysflooding attack mode of attack to make the network run out of bandwidth, so that delays respond to requests for legitimate network connections and finally faltering service providers. Theoretically, this attack applies to all TCP connections, such as WWW, Telnet, e-mail, and so on.
- 45.64.96.181
  Public IP, as well as the IP address of the server attacked by the attacker by flooding network traffic.

2) *Android operating system*

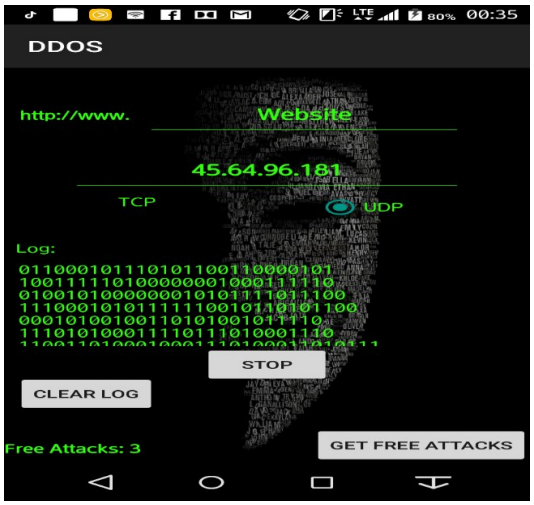

Fig. 6. Pengujian dengan Os android

Remarks:
- UDP
  The attack is carried out with UDP paths that are targeted to make the server down.
- 45.64.96.181
  Public IP, IP address of the server attacked by the attacker.

1. Alert information
   Alert information about an attack is obtained after providing an attack on the server and sent to the network administrator's cell phone as shown in Figure 7 below:

Fig. 7. Detection results of sysflooding attacks

2. Blocking attacks.
   Blocking attacks is done by replying to the contents of the alerts sent by the IDS system, the network administrator's reply message contains a bash shell script command, which is integrated with iptables and php, so that it can be used as an sms controller, the contents of the "BLOCKFLOOD" command, namely bash script calling, which is executed by the system, then processed through the gammu server which is in the inbox table.

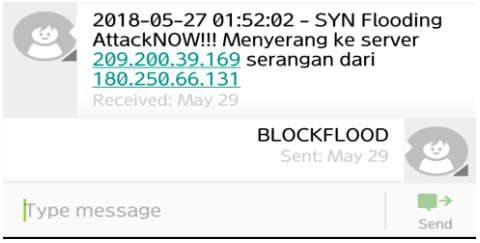

Fig. 8. Commands block attacks

3. Blocked attack.
   The attack is successfully blocked if the administrator has replied to the message correctly according to the format specified in the intrusion detection system.

C. *Port scanning*

Port scanning attacks by conducting a full scan to the destination server using the nmap tool, nmap scan results can be detected, and successfully sent to the administrator.

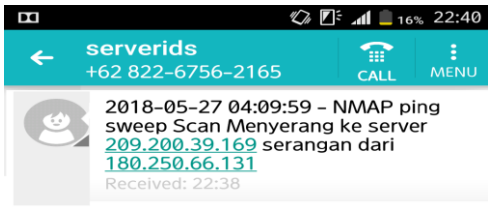

Fig 9. Detection of nmap portscanning attacks

D. *SQL injection*

Samples of this attack are carried out using the bypass authentication login method by entering a query that is in Surabaya into the login form which will then cause a system alert because the rules match the sqlinjection query set in the system intrusion detection system. notification that the system is under attack.

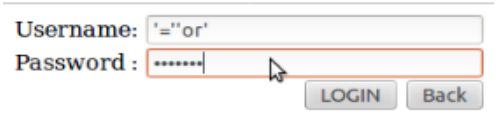

Fig. 10. SQL injection injection

Sql injection system intrusion detection system successfully sends alerts to network administrators.

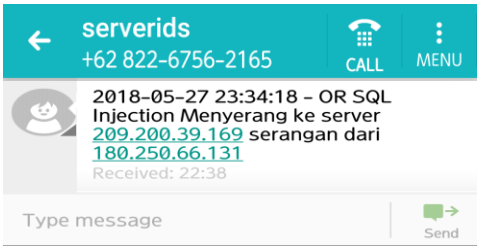

Fig. 11. SQL injection alert

E. Table of Result of Discussion

TABLE I
RESULTS OF TESTING SYSTEM PERFORMANCE MEASUREMENT WITH UBUNTU 16.04

Attacker	*Operating System*	Jenis Serangan	*Tools*	IDS	*Iptables*
	Ubuntu Desktop 16.04 *LTS*	*Ping of death*	Ping flood	V	X
		SYN flooding attack	*Hping3* Siege	V	X
		Sqlinjection	-	V	-
		Portscanning	*Nmap*	V	-

TABLE II
RESULTS OF TESTING SYSTEM PERFORMANCE MEASUREMENT WITH ANDROID LOLIPOP VERSION 5.0.3

ttacker	*Operating System*	Jenis Serangan	*Tools*	IDS	*Iptables*
2	Os Android lollipop versi 5.0.3	*SYN flooding Attack*	*Tool DDOS Attack*	V	X

TABLE III
RESULTS OF TESTING SYSTEM PERFORMANCE MEASUREMENT WITH WINDOWS 7 ULTIMATE

Attacker	*Operating System*	Jenis Serangan	*Tools*	IDS	*Iptables*
3	*Windows* 7 Ultimate	*Ping of death*	*Command prompt*	V	X

Remarks:
V: Deteced by *Intrusion Detection System*(*IDS*)
X: The attack was successfully blocked by Iptables

Based on Table I. System Performance Measurement results can be seen attackers (1) using the Operating System Ubuntu Desktop 16.04 LTS attacks the server (45.64.96,181) with 4 (four) types of attacks, namely Ping of death and SYN flooding attacks, Portscanning, sqlinjection. using several types of tools as shown in the table above. The result was the Intrusion Detection System (IDS) succeeded in detecting all four attacks and Iptables managed to block just 2 attacks. Attacker (2) uses the Windows 7 Ultimate Operating System to attack the server (45.64.96.181) with 1 (one) type of attack, namely Ping of death using Command Prompt tools.

(3) using the Android lollipop operating system version 5.0.3 to attack the server (45.64.96.181) with 1 (one) type of attack, namely SYN flooding attack using the DDOS attack tool. The result was the Intrusion Detection System (IDS) successfully detected both attacks and Iptables successfully blocked the attack.

IV. CONCLUSION

The conclusion of this research is to facilitate network administrators in monitoring and monitoring the server against attacks, the system built has been able to detect the presence of an attack and can be controlled remotely through short messages to block the attacker quickly, the system has also been able to control other commands that there is a server such as shutting down the server, restarting if necessary when the problem cannot be resolved anymore, all can be done only with a short message via the sms controller.

REFERENCES

[4] Taluja, Sachin, Pradeep Kumar Verma, Rajeshwar Lal Dua, 2012, "Network Security Using IP firewall" in International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2 Issue 8,August 2012, pp. 348-354.
[5] Ur Rehman, Rafeeq, "Intrusion Detection Systems with Snort," Prentice Hall PTR, pp. 23-73, 2003.
[6] Boob, Snehal, Priyanka Jadhav,2010, "Wireless Intrusion Detection System" in International Journal of Computer Applications, Volume 5– No.8, August 2010, pp.9-13
[7] Apriana,Windi, "Remote iptables dan intrusion detection system dengan snort bebantuan sms gateway pada jaringan fakultas teknik universitas ibn khaldun bogor," Seminar Nasional inovasi dan aplikasi teknologi di industri (ITN MALANG), malang,2017, ISSN 2085-4218
[8] Advanced Computational Engineering and Networking, Vol. 1, Issue 10, December 2013, pp. 26.
[9] Bhagavan, Surya Ambati, Deepti Vidyarthi, "A brief study and comparison of, Open Source Intrusion Detection System Tools" in International Journal of Ur Rehman, Rafeeq, 2003, Intrusion Detection Systems with Snort, Prentice Hall PTR, pp. 23-73, 2013.
[10] Boob, Snehal, Priyanka Jadhav, "Wireless Intrusion Detection System" in International Journal of Computer Applications, Volume 5– No.8, August 2010, pp. 9-13, 2010.
[11] Kumar, Ashish, Ajay K. Sharma, Arun Singh, Dr. B. R. Ambedkar, "Performance Evaluation of Centralized Multicasting Network over ICMP Ping Flood for DdoS" in International Journal of Computer Applications, Vol. 37, January 2012, pp. 3, 2012.
[12] Taluja, Sachin, Pradeep Kumar Verma, Rajeshwar Lal Dua, "Network Security Using IP firewalls" in International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2 Issue 8, August 2012, pp. 348-354, 2012.
[13] Ulfa, Farid Faaza, "Sms Gateway Untuk Verifikasi Kehadiran Dosen Dalam Information Display System Jadwal Perkuliahan Di Prodi Informatika FKI UMS", Surakarta, 2015.
[14] Ulum, Ucu Nurul, Perancangan dan Implementasi IDS (Intrusion Detection System) Pada Jaringan Nirkabel Menggunakan Snort di STMIK AMIKOM Yogyakarta, Yogyaka, 2014.