

JURNAL ILMU KOMPUTER

Volume 2 Nomor 2, Desember, 2024 ISSN: 3031-125X (DNLINE) Penerbit: Program Studi Teknik Informatika S-2 Universitas Pamulang

Analis Perancangan Dan Penerapan Keamanan Jaringan Menggunakan Metode Intrusion Detection System (IDS), Intrusion Prevention System (IPS) Dan Demilitarized Zone (DMZ) Pada PT. Maha Digital Indonesia (Mahapay)

Evan Trijanitra¹, * Arya Adhyaksa Waskita², * Taswanda Taryo³ ^{1,2,3)} Teknik Informatika, Universitas Pamulang Kota Tangerang Selatan, Banten Email: ¹evan.trijanitra@gmail.com, ² aawaskita@unpam.ac.id, ³dosen02234@unpam.ac.id

ABSTRACT

Network security systems, in recent years have become the main focus in the world of securing other important data, this is due to the high number of suspicious threats (Suspicious Threats) and attacks from the Internet. Network security involves efforts to protect data and computer systems from detrimental threats, such as cyberattacks, malware, and data theft. The existence of increasingly complex and evolving threats has increased awareness of the need for strong network security. PT. Maha Digital Indonesia (Mahapay) is a company operating in the field of EDC Field Service where it is very important that client data is kept confidential. This requires good network security to maintain the confidentiality of the data. So the aim of this research is to implement network security using the Intrusion Detection System (IDS), Intrusion Prevention System (IPS) and Demilitarized Zone (DMZ) methods as network security at PT. Maha Digital Indonesia (Mahapay). The results of this research are the formation of connections between networks in the topology along with the successful functioning of the Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) detecting and preventing suspicious activities carried out by attackers and the operation of rules for the DMZ area. Success in the application is tested again by carrying out several attack methods that will be analyzed such as Syn Flood Attack, Ping Of Death and Port Scanning which will be handled by the configuration that has been applied to the network and server.

Keywords: Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Demilitarized Zone (DMZ), firewall, Network Security, Server

ABSTRAK

Sistem keamanan jaringan, dalam beberapa tahun ini telah menjadi fokus utama dalam dunia mengamankan data hal penting lainnya, hal ini disebabkan tingginya ancaman yang mencurigakan (Suspicious Threat) dan serangan dari Internet. Keamanan jaringan melibatkan upaya untuk melindungi data dan sistem komputer dari ancaman yang berpotensi merugikan, seperti serangan siber, malware, dan pencurian data. Keberadaan ancaman yang semakin kompleks dan terus berkembang telah meningkatkan kesadaran akan perlunya keamanan jaringan yang kuat. PT. Maha Digital Iindonesia (Mahapay) sebagai perusahaan yang bergerak dibidang Field Service EDC dimana data – data pada client sangat penting dijaga kerahasiannya. Hal tersebut membutuhkan suatu keamanan jaringan yang baik untuk menjaga kerahasiaan data tersebut, Maka Tujuan dari Penelitian ini adalah menerapkan menerapkan kemanan jaringan menggunakan metode Intrusion Detection System (IDS), Intrusion Prevetion System (IPS) dan Demilitarized Zone (DMZ) sebagai keamanan jaringan pada PT. Maha Digital Indonesia (Mahapay). Hasil dari penelitian ini adalah terbentuknya koneksi antar jaringan dalam topologi beserta suksesnya fungsi dari Intrusion Detection System (IDS) dan Intrusion Prevention System (IPS) mendeteksi dan mencegah aktifitas mecurigakan yang dilakukan attacker dan

bekerjanya rule untuk area DMZ. Keberhasilan dalam pengaplikasian diuji kembali dengan melakukan beberapa metode serangan yang akan di analisa seperti Syn Flood Attack, Ping Of Death dan Port Scanning yang akan ditanggulangi oleh konfigurasi yang telah diterapkan pada jaringan dan server.

Kata kunci: Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Demilitarized Zone (DMZ), firewall, Keamanan Jaringan, Server

1. PENDAHULUAN

Kebutuhan akan teknologi informasi di era modern ini sangat besar serta dapat diaplikasikan dalam berbagai bidang, sebab itu juga banyak pihak-pihak yang saat ini jadi bergantung pada sistem komputer sehingga sistem komputer dituntut untuk berjalan sepanjang waktu pada jaringan internet.[1] PT. Maha Digital Indonesia (*Mahapay*) merupakan perusahaan teknologi yang bergerak dibidang jasa pembuatan software dan field service, di mana keamanan jaringan harus menjadi prioritas utama pada PT. Maha Digital Indonesia (*Mahapay*). Kelemahan - kelemahan yang terdapat pada jaringan komputer jika tidak dilindungi dan dijaga dengan baik akan menyebabkan kerugian berupa kehilangan data, kerusakan sistem server, tidak maksimal dalam melayani user atau bahkan kehilangan aset-aset berharga. terlebih lagi ketika jaringan local sudah terhubung ke internet maka ancaman keamanan jaringan akan semakin meningkat. misalnya DDoS attack dan sebagainya, juga serangan hacker, virus, trojan yang semuanya merupakan ancaman yang tidak bisa diabaikan.[2].

Untuk menangkal ancaman jaringan, ada beberapa teknik yang bisa diterapkan, Pertama Intursion Detection System (IDS), Intrusion Prevention System (IPS) dan teknik demilitarized zone (DMZ). Dengan menggunakan 3 Teknik keamanan berikut maka akan terbentuk pengamanan berlapis pada server sehingga akses dari luar tidak bisa langsung memasuki komputer server, sehingga hal ini membuat server menjadi lebih aman.[3].

Intrusion Detection System atau IDS adalah sebuah sistem yang memonitor trafik jaringan untuk mendeteksi aktivitas-aktivitas mencurigakan. Jika aktivitas mencurigakan tersebut ditemukan, IDS akan melaporkannya dalam bentuk peringatan. Dengan kata lain, IDS bisa dibilang sebagai perangkat lunak pemindai sistem atau jaringan guna terhindar dari kegiatan yang melanggar kebijakan.[4]

Intrusion Prevention System (IPS), adalah pendekatan yang sering digunakan

Lisensi: Creative Commons Attribution-ShareAlike 4.0 International License (CC BY-SA 4.0)

untuk membangun system keamanan komputer, IPS mengkombinasikan teknik firewall dan metode Intrusion Detection System (IDS) dengan sangat baik. Teknologi ini dapat digunakan untuk mencegah serangan yang akan masuk ke jaringan lokal dengan memeriksa dan mencatat semua paket data serta mengenali paket dengan sensor, disaat

attack telah teridentifikasi, IPS akan menolak akses (block) dan mencatat (log) semua paket data yang teridentifikasi tersebut. Jadi IPS bertindak sepeti layaknya Firewall yang akan melakukan allow dan block yang dikombinasikan seperti IDS yang dapat mendeteksi paket secara detail.[5]

2. METODE

2.1 Metode Penelitian

Metode penelitian yang digunakan yaitu metode eksperimen dimana dilakukan percobaan menggunakan sistem operasi Ubuntu server 20.04 dengan menerapkan system keamanan jaringan berupa intrusion detection system (*IDS*), Intrusion prevention system (*IPS*) dan Demiliterized Zone (*DMZ*). Hasil yang di harapkan adalah ids da nips dapat mendeteksi dan melakukan block pada aktifitas yang mencurigaan.

2.2 Analisa Kebutuhan

1. Pengalokasian IP Address

Dalam membuat daftar kebutuhan IP Address penulis menggunakan bantuan Ms.Visio dari topologi yang sebelumnya dibuat. IP Address sangat penting karena agar komputer klien dapat terhubung ke internet dan juga server.

Tabel 2.1	Pengalokasian	IP	Address
-----------	---------------	----	---------

No	Pengguna	IP Address	
1	Server IDPS	122.xxx.xxx/24	
2	Server Web Service	179.xxx.xx.2/24 179.xxx.xx.3/24	

Lisensi: Creative Commons Attribution-ShareAlike 4.0 International License (CC BY-SA 4.0)

3	Mikrotik	179.xxx.xx.4/24
4	Server Aplication	192.xxx.x.59/24
5	PC Tower	122.xxx.xxx.62/24

2. Kebutuhan Hardware

Kebutuhan hardware ini digunakan dalam membangun topologi jaringan sesuai dengan yang dirancang oleh penulis berikut merupakan tabel 3.1.2 kebutuhan hardware :

No	Jenis Perangkat	Spesifikasi	Jumlah
1	Server Rackmount	 Inter Xeon CPU E5504 @2.00GHz (4 Core) RAM DDR3 8GB HDD SAS 2.5" HP 270GB OS Ubuntu Server 20.04 Lts 	1
2	Server Rackmount	 Inter Xeon CPU X3360 @2.83GHz (4 Core) RAM DDR2 4GB HDD SAS 3.5" HP 300GB OS Ubuntu Server 20.04 Lts 	1
3	Mikrotik Routerboard RB2011UiAS- RM	 CPU AR9344 600MHz RAM 128MB Storage 128MB OS RouterOS 10 Port 	1
4	PC Tower	 Intel Pentium Dual-Core E5800 @3.20GHz RAM DD3 4GB WD HDD 3.5" 300GB OS Kali Linux 2024.2 	1

Tabel 2.2 Kebutuhan Hardware

			•	Intel Xeon E5 2620 @2.10GHZ		
	5	Server Rackmount	•	RAM DDR4 70GB	1	
			•	HDD 6TB	1	
			•	OS Ubuntu Server 22.04		

3. Kebutuhan Software

Software adalah merupakan suatu program komputer yang berfungsi untuk melakukan tugasnya masing masing. Dalam penelitian ini berikut merupakan software yang digunakan adalah :

Tabel 2.3 Kebutuhan Software

No	Nama	Spesifikasi	Keterangan
1	Sistem Operasi Server IDS&IPS	Ubuntu Server 20.04Lts	Sistem Operasi
2	Web Service	Nginx 1.18.0	Web Service redirect port web
3	PC Tower	Kali Linux	PC Untuk simulasi serangan
4	NMAP	Nmap v8.23	Tester Tools
5	HPING	Hping3	Tester Tools
6	SSH Client	MobaXterm	Remote SSH/SFTP
7	Browser	Chrome v125.0.6	Software untuk browsing

2.3 Perancangan Penelitian



Gambar 1. Flowchart kerangka kerja

2.4 Perancangan Topologi Jaringan

Layout jaringan atau topologi jaringan dimaksudkan untuk merancang topologi yang kiranya sesuai dengan sistem yang dikembangkan, sehingga gambaran topologi berikut dapat memberikan gambaran secara jelas tentang sistem yang hendak dibangun.

1. Topologi jaringan sebelum diterapkan keamanan jaringan

Lisensi: Creative Commons Attribution-ShareAlike 4.0 International License (CC BY-SA 4.0)



Gambar 2. Topologi Jaringan sebelum diterapkannya keamanan jaringan

2.5 Konfigurasi keamanan jaringan

Pada tahap Implementasi sistem ini dibuat sebuah sistem keamanan menggunakan topologi yang dirancang sebelumnya. Berikut merupakan implementasi yang dilakukan :

2.5.1 Konfigurasi Intrusion Detection System (IDS)

Teknik keamanan yang akan penulis terapkan adalah teknik Intrusion Detection System (IDS).[7] IDS adalah sebuah sistem yang memonitor trafik jaringan untuk mendeteksi aktivitas-aktivitas mencurigakan.

Step 1 - Installasi dan Update Package Ubuntu 20.04

\$ sudo apt update -y

Step 2 - Add Repository Install Suricata IDS Ubuntu

\$ add-apt-repository ppa:oisf/suricata-stable

\$ sudo apt update -y

Step 3 – Install Suricata IDS Ubuntu (Install Suricata Ubuntu)

\$ sudo apt install suricata -y

Step 4 – Enable service suricata

\$ sudo systemctl enable suricata.service

Step 5 – Stop service suricata

\$ sudo systemctl stop suricata.service

Step 6 – Enabling Community ID

\$ sudo nano /etc/suricata/suricata.yaml

Cari kalimat community-id, default nya adalah false maka dirubah ke

true seperti berikut :

/etc/suricata/suricata.yaml
<pre># Community Flow ID # Adds a 'community_id' field to EVE records. These are meant to give # records a predictable flow ID that can be used to match records to # output of other tools such as Zeek (Bro). # # Takes a 'seed' that needs to be same across sensors and tools # to make the id less predictable.</pre>
enable/disable the community id feature. community-id: true

Gambar 3. Enable Community ID

Step 7 – Menentukan Interface Jaringan untuk digunakan

\$ ip -p -j route show default

Step 8 – Edit Interface yang akan di gunakan untuk suricata mendeteksi ancaman.

\$ sudo nano /etc/suricata/suricata.yaml

Step 9 – Validasi konfigurasi suricata

\$ sudo suricata -T -c /etc/suricata/suricata.yaml -v

Lisensi: Creative Commons Attribution-ShareAlike 4.0 International License (CC BY-SA 4.0)

192

2.5.2. Konfigurasi Intrusion Prevention System (IPS)

Intrusion Prevention System adalah sistem yang dapat secara otomatis mendeteksi aktivitas mencurigakan yang berpotensi berbahaya dalam jaringan.[8].

Step 1 – Update Repository Ubuntu

\$ sudo apt -y update

Step 2 – Install jq atau output dengan type json

\$ sudo apt –y jq

Step 3 – Temukan IP Publik server



Step 4 – Masukan file aturan baru ke dalam konfigurasi suricata



Step 6 – Validasi Konfigurasi setelah menambahkan rules

\$ sudo suricata -T -c /etc/suricata/suricata.yaml -v

Step 7 – Aktifkan IPS Mode

\$ sudo nano /etc/default/suricata



Gambar 4. Aktivasi IPS Mode

2.5.3. Konfigurasi Notifikasi Bot Telegram

Telegram tidak hanya menyediakan fitur untuk chatting online tetapi juga menambahkan bot secara fungsional dengan fungsi tertentu yang beroperasi secara otomatis sebagai respons terhadap perintah atau permintaan pengguna.[9] **Step 1 – Membuat bot untuk notifikasi suricata menggunakan Feature di Telegram dengan nama** *BotFather*

- Ketik /newbot



Gambar 5. Membuat bot baru

Step 2 – Masukan Nama Bot

Change a bot from the list below		
Today		
g Transfindbot		
Inewird	Lannia -	
Alright, a new bot. How are we going to call it? Please choose a name for your bot.		
Security Alert IDSIPS Suricuta - Tests	1 1000 at 1	
Good. Now lefts choose a username for your bot. It must end in "bot". Like this, for example. TetrifoBot or tetris_bot.		
Muju, anicuta, aint, bo	10000 at	
Denied Comparisations on system are both. You will find it all transformation and the start of the start of the start of the start about association and profile pictures for your both one's first a field of commonly. By the away when provide fielded in rounding the start of the start of the start of the start of the start automation of the start makes the both is fully operational before system and the start.		
Lise this token to access the HTTP AP: 7290726712 Accession(Config)[2018 - Substreet Integer		
Keep your token secure and stare it safely, it can be used by anyone to control your bot.		
For a description of the Bot API, see this page: https://care.idegram.arg/bots/aps		

Gambar 6. Masukan nama bot

Lisensi: Creative Commons Attribution-ShareAlike 4.0 International License (CC BY-SA 4.0)

Step 3 – Masukan Username Bot



Gambar 7. Membuat username BOT

Step 4 – Copy Token API, Paste ke url :

https://api.telegram.org/bot{TOKENBOT}/getupdates



Step 5 – Buat skrip di server



Step 6 – Masukan Skrip berikut

#!/bir	1/bash							
#	Ganti	deı	ngan	API	token	bot	Anda	
BOT	_TOKEN=	''7250172'	712:AAG	DVxKW.	X1S9fqgji5YB	_rsLoqhS4_3	n9yU''	
#	Ganti	dengan	chat	t ID	Anda			
СНА	T_ID=''317	922437''						
#	Path	ke	file	log	Suricata			
LOG	_FILE=''/v	ar/log/sur	ricata/fast	.log''				
# F1	# Fungsi untuk mengirim pesan ke Telegram							
send telegram message() {								
cu	rl -s -X PO	ST						

```
''https://api.telegram.org/bot$BOT_TOKEN/sendMessage'' -d
''chat_id=$CHAT_ID'' -d ''text=$1'' > /de>
}
# Fungsi untuk memantau log Suricata dan mengirim notifikasi ke Telegram
monitor_suricata_log() {
   tail -F -n0 ''$LOG_FILE'' | while read -r line; do
      send_telegram_message ''$line''
      sleep 10 # Menambahkan penundaan 10 detik
   done
}
# Jalankan fungsi pemantauan log Suricata
monitor_suricata_log
```

Step 7 – Konfigurasi layanan system

\$ sudo nano
/etc/system/system/suricata_IDSIPS_alert.service

Step 8 – Masukan skrip berikut

[Unit]		
Description=Suricata	Telegram	Notifier
After=network.target		
[Service]		
Type=simple		
ExecStart=/home/idsips/suri	cata_IDSIPS_alert.s	sh
Restart=always		
RestartSec=10		
User=nobody		
Group=nogroup		
[Install]		
WantedBy=multi-user.target	t	

Memulai ulang konfigurasi system

\$ sudo systemctl daemon-reload

Step 10 – Menjalankan notifikasi telegram

sudo systemctl start suricata-telegram.service

2.5.2. Konfigurasi Demiliterized Zone (DMZ)

DMZ atau zona demiliterisasi, adalah sebuah keamanan firewall yang memisahkan jaringan area lokal (LAN) dari jaringan tidak terpercaya biasanya, internet publik.[6]



2.5.3. Skenario pengujian

Pengujian Sistem Keamanan Jaringan adalah proses untuk mengevaluasi

efektivitas Sistem Keamanan Jaringan dalam mencegah, mendeteksi, dan merespons serangan. Tujuan pengujian ini adalah untuk menentukan apakah sistem keamanan jaringan dapat mencegah serangan yang dicobakan. Penelitian ini melakukan pengujian untuk mengambil data dengan beberapa skenario serangan yang sudah dilakukan untuk menegtahui kinerja dari Suricata. Pengujian dilakukan dalam satu pekan dan waktu yang sudah di tentukan oleh pihak perusahaan dengan menggunakan komputer penyerang dengan berbeda lokasi dan IP dengan melakukan serangan dengan Serangan Syn Flood Attack, Port Scanning dan Ping of Death. Pengambilan Data dilakukan oleh peneliti dengan melakukan pengamatan secara langsung log Suricata pada saat terjadi Serangan.

3. HASIL DAN PEMBAHASAN

3.1 Hasil Pengujian

Hasil penelitian yang dilakukan berupa Intrusion Detection System (IDS), Intrusion Prevention System (IPS) dan Demiliterized Zone di PT. Maha Digital Indonesia. Skenario pengujian Intrusion Detection System (IDS) dan Intrusion Detection System ada 3 yaitu Syn Flood Attack, Port Scanning, dan Ping Of Death menggunakan sistem operasi Kali Linux. Dan Pada metode Demiliterized Zone dilakukan skenarion pengujian berupa akses port 80 atau http, akses port 443 atau https dan ping ke server aplikasi. Maka didapatkan hasil seperti table berikut ini :

NO	PORT	JENIS SERANGAN	PERCOBAAN PENGUIIAN	ATTACKER	HASIL DETEKSI	DURASI ALERT
1.	80	C T1 1 411 1		Berhasil di Drop	Berhasil di Drop	10 Detik
2.	443	Syn Flood Attack		Berhasil di Drop	Berhasil di Drop	10 Detik
3.	80	Dort Coopping	Intrusion	Berhasil di Drop	Berhasil di Drop	10 Detik
4.	443	Port Scanning	Detection System	Berhasil di Drop	Berhasil di Drop	10 Detik
5.	80	Dine Of Death		Berhasil di Drop	Berhasil di Drop	10 Detik
6.	443	Ping Of Death		Berhasil di Drop	Berhasil di Drop	10 Detik
7.	80	Sam Flood Attack		Berhasil di Drop	Berhasil di Drop	10 Detik
8.	443	Syn Flood Atlack		Berhasil di Drop	Berhasil di Drop	10 Detik
9.	80	Dent Geometre	Intrusion	Berhasil di Drop	Berhasil di Drop	10 Detik
10.	443	Port Scatting	Prevention System	Berhasil di Drop	Berhasil di Drop	10 Detik
11.	80	Dine Of Death		Berhasil di Drop	Berhasil di Drop	10 Detik
12.	443	Ping Of Death		Berhasil di Drop	Berhasil di Drop	10 Detik
13.	80	Akses Port			Berhasil di Block	
14.	443	Akses Port	Demiliterized	Client Lenten	Berhasil di Akses	Real Time 1
15.	70	Ping IP Server Aplikasi	Zone	Спена Сартор	Berhasil di Block	Detik

3.1.1 Pengujian Intrusion Detection System (*IDS*) dan Intrusion Prevention System (*IPS*)

Dalam Skenario Pertama ini serangan yang dilakukan berupa komputer penyerang akan melakukan serangan secara bergantian dengan jenis serangan yang berbeda dan dalam waktu yang berbeda dengan tiga jenis serangan yaitu Syn Flooding, Port Scanning dan Ping of Death dengan target alamat IP yang sama dan sudah ditentukan oleh PT Maha Digital Indonesia.

1) Syn Flood Attack

Serangan ini dilakukan oleh komputer penyerang dengan IP 122.xxx.xxx.62 dengan operation system kali linux dan melakukan serangan ke IP Target yaitu

122.xxx.xxx.60 dapat dilihat pada Gambar 9.



Gambar 8. Percobaan serangan Syn Flood Attack

Sedangkan Suricata memberikan alert serta melakukan drop paket yang dilakukan penyerang, perlu diperhatikan waktu penyerangan pada pukul 22.31 tanggal 07 Juni 2024 untuk memastikan Suricata bekerja secara real time dan sesuai dengan yang di terima Telegram. Hasil alert dan drop oleh Suricata seperti pada Gambar 9.

de institute and the test of over discrete instant fact	
00/07/2014-22/28:22.330209 [wDrop] [**] [10:0] SM# Flood Attack Detected - Dropping Packet [**] [Classification:	(mill) [Pri
ority: 3] (TCP) 9 23 175 195 54006 -> 122	
06/07/2024-22:20:38.056270 [w0rop][**][[111:1]]SYN Flood Attack Detected - Dropping Packet [**][Classification:	(null)] [Pri
britty: 3] (TCP) 226:256:246:224:56121 -> 122	ANTINE POR
BN/07/2024-22/2018.462623 (MUROP) [**] [1115] SHI FOOD ATTACK DEVICES - UPOPPING PACKET [**] [LIABSTICATION: ority: 31 (TCP) 117 286, 71 (260 17706 -> 177) (2018)	CHOICEAT THEFE
06/07/2024-22/28:40.030483 [WDrop] [4+] [11] SYN Flood Attack Detected - Dropping Packet [++] [Classification:	(mull) [Pri
erity: 3] {TCP} 106.157.121.66:37405 -> 122. 100:80	
06/97/2824-22128:41.064884 [wfrop] [**] [10111] SYN Flood Attack Detected - Dropping Packet [**] [Classification:	(mull)] [Prt
printy 3] (LCP) 200.200.00.14124988 - 222. Constant 6:00:0004 12:0041 Table Longen Test Long Constant Attack Datasted - Department Dashet Feel [Classification]	AND TALL PROFE
ority 31 (TCP) 230 133 145 142 157884 -> 122 10:88	America These
96/97/2024-22:28:34.002723 [w0rop] [**] [11:01] SYN Flood Attack Detected - Dropping Packet [**] [Classification:	(mull)] [Pri
srity: 3] {TCP} 141.131.61.193:1764 -> 122	
06/07/2024-22:28:33.244990 [w0rop] [**] [[] [] [] [] [] [] [] []	(nutty) (Pri
Decempion 2010 A	Condition (Peri
ority: 3] {TCP} 38 10/ 100.747:20354 -> 127	
56/07/2024-22:28:45.498552 [wDrop] [**] [11111] SYN Flood Attack Detected - Dropping Packet [**] [Classification:	(mill)] [Pri.
arity: 3] {TCP} 246 185,214 172:02286 -> 122. (80:80	A REAL PROPERTY AND INCOME.
DB/D//2024-22/20146.0950653 (WUrop) [**] 11111 SHN Ficod Attack Detected - Dropping Packet [**] [Lissification:	COUNTY ISSUE
06/07/2024-22:28:38.034917 [w0rop] [**] [Indian SYN Flood Attack Detected - Dropping Packet [**] [Classification:	CONTRACTOR PRESS
ority: 3] {TCP} 1.181.0.204:44038 -+ 122. 60:88	
96/87/2024-22:28:45.303983 [w0rop] [**] [1=1=1] SNN Flood Attack Detected - Dropping Packet [**] [Classification:	(null)] [Pri
prity 3] (TCP) 114(17,199,45338092 -> 122)	AND TANK THE COLOR
W0/0/2024-22/22/20-30.00/131 (W0/OP) (**) SIN PLOOD ATTACK Detected - Dropping Packet (**) [Liassification: write: 31 (TCD) 151 3.0 (105 1409) (**) SIN PLOOD ATTACK Detected - Dropping Packet (**) [Liassification:	VINCENT FRIE
06/07/2824-22:28:42.778934 [WDrop] [**] [511] SYN Flood Attack Detected - Dropping Packet [**] [Classification:	(MALTER IPPE
srity: 3] (TCP) 6.240.05.150:50142 -+ 12260:00	
96/87/2824-22:28:49.353076 [wDrop] [**] [SYN Flood Attack Detected - Dropping Packet [**] [Classification:	(mail)] [Pri
Sector 31 (reb) 224 /0 200/105/20335 -> 121	
💽 gatewar 🛛 🔯 74% 🔄 🖬 2,05.08 / 7,78.68 🕴 55,34 Mb/r 📥 62,08 Hb/r 🗰 2,days 🕼 Kaps (x2) 📓 7:50% Abord,eth 2% Abord, 29%	

Gambar 9. Hasil Deteksi Serangan Syn Flood Attack

Sedangkan untuk Notifikasi sesuai dengan skrip yang diberikan bahwa di kirimkan ke Telegam di jeda 10 detik, Berikut adalah notifikasi yang diterima oleh Telegram.



Gambar 10. Notifikasi Telegram

2) Port Scanning

Komputer penyerang akan melakukan serangan dengan jenis serangan yang sama dengan target Alamat IP yang sudah ditentukan. Tampak pada Gambar 11. Komputer Penyerang melakukan serangan Port Scanning.

(neverdie⊖ mahapay)-[*] 					
Starting Nmap 7,945VN (https://	nmap.org) at 2024-06	5-07 23:41 WIB			
Nmap scan report for ip-60.112.	net.id	(122	60)		
Host is up (0.00021s latency).					
Not shown: 999 closed top ports	(reset)				
PORT STATE SERVICE VERSION					
53/tcp open domain ISC BIND 9.	16.48 (Ubuntu Linux)				
dns-nsid:					
bind.version: 9.16.48-Ubuntu					
MAC Address: 00:21:5E:C0:43:CC [LBM)				
Device type: general purpose					
Running: Linux 4.xjs.x	I af anna ta il incord inc	or based of			
OC detailer Linux 4 15 5 9	cr4 cper/or colux: colu	ax_kernet:a			
Network Distance: 1 hon					
Service Info: 05: Linux: CPE: cn	e:/o:linux:linux kern	uel			
eriter entry eriter entry eret ek					
TRACEROUTE					
HOP RTT ADDRESS					
1 0.22 ms ip-60.112.	net.id (122;	60)			
en e					
OS and Service detection perform	ad. Please report any	/ incorrect re	sults at https:	//nmap.org/submit/	
Nmap done: 1 IP address (1 host	up) scanned in 16.17	seconds			

Gambar 11. Percobaan Port Scanning

Komputer melakukan penyerangan kepada target IP yang sudah ditentukan dan dalam waktu yang bersamaan, untuk hasil deteksi dari Suricata dapat dilihat pada Gambar 12.

\$ 4.5.9W(2071									. —	a ×
🙆 Javetari: 🔡 Futureer 💷 Sini	arrige 👌 Dagadam	•		I sectors						🔣 Core
.06:89 98/47/2024-23:47:30.203264	(+erres) [***]	<u>iu</u> in pr	ort scanning	Detected	Dromping Packet (**)	(classification				i ilian
05/07/2804-23+07-33-03450			ort Scenning		. Unspiring Facker, (**)					40 (4,333)
66/67/2624-23:47:30.855454	[abrast] [**]		wit Sciencing							48 -+ 311.
00/07/2024-22147131-54588		in the second	int sciming							28 -> 2020
60,00772024-21-07135-333360	Evening E++3		nit Stanning	Detected -	Brasping Hacket [**]					a 222112
00/02/2024-23:47:11.990436	[etrop] [44]	10 P	art Scienting	Detected -	Drapping Fachet [**]					149 -> 113
05/07/2024-25147112.478815	(ubras) [++]		ort Scanning	Detected	Dropping Facket (++)				Automotic receipter	is min
MEANTY2024-20147122-393271			ort Scarning		Oropping Packat [++]					100
00/17/2024-23:47:35.357364	[ubras] [**]	(LILL) P	ort Scanning		- Drapping Packet [**]				w.1.21041-34643	- million
00/07/2024-22(47)30.020110	(worea) (++)		ort scanning		Drate ing workst [**]					1852
6674972824125147.15.016565	(whrow) [++]		art Scanling		Dropping Packet [**]				Calif. (1), 110 (403	64 - e 110.
062022004-28:07:06.000021	Debrand Deel		ert Scamieg		Branning Packet [++]					and the second
MUNICIPALITY - 20147-10-104430	[worse] [**]		int training							18-19-122.
0578772924-20147137.008500	DePropT Tert1		ert Scanning	Ostected -	Brossona Packet [**]	Classification			0771-1071-00 (\$402	See Block
0020722024-23107-37.079626	[wbrops] [**]		ort Scanning	Detected	- Dropping Packet (++)		intiti periority:	1) (TCP) 1		111 -> 781
05/07/2024-22:47:30.700607	[vpras] [++]	in in	ert Scanning	Detected	Drapping Tacket [++]	(Canadianation)	millel printing		100 110. 200 100	102
MI/87/2024-25 47:44.347300	(adrops) (++)		ort Scenning	Detected -	Dropping Facket [++]			1) (TOP): 4		t#1.13
86/07/2024 29147 49-081850	(-Drop) [11]		ort spanning	DETECTOR	- troubing muchot [**]					40 -> 117-
en/#7/20104-221(#7-39-283309	Tethnasi 1=+1		wit scanning		- propping micket [++]					sur 🛹 taz
06743729324-22147-40.013000	Lubreal (++1		ort Spanning	Ontected	- Drampting Packet [**]					49.10 100.
MANTANIA 28127-42.597197					- Aropping Facket [**]			8] (109) I		¥\$69 → 13

Gambar 12. Notifikasi Port Scanning pada log suricata

Sedangkan untuk Notifikasi sesuai dengan skrip yang diberikan bahwa di kirimkan ke Telegam di jeda 10 detik, Berikut adalah notifikasi yang diterima oleh Telegram.

	Security Alert (DSIPS Survey) Texa
	BARDISTAN CONTRACTORISTIC INCOMENTATION OF THE CONTRACTOR OF THE C
	AGAVY/S224-25-8138 200544 [w0hop] [***] [1-21] And Steaming Denotes - Desping Factor(**1) Classification (null) (Pointip I) [YCF1124-25-8188 [v0h-4-127]
	BANTISTAL SANTAN ADMIN WOMAN (** 1152) (** 1527) (** 1527) Detected - Docygong Recket (** 1 (Damefracture (** 16)) (** 167) (** 1944) (** 16)
	MANU/ADA SERVICE 46864 Wareput (P11) Add (Peer Scenning Detactive Detactive Detaction gradies (Provide and Provide 2022) 2012 Part (P12) Add (Part Part Part Part Part Part Part Part
Security Alexandro Savientes Teste 2001 Securito de Calendaria por por primi primi forma de porte portes.	BANDARY CONTRACTORS AND AN ADDRESS OF THE SECTION O
	Weinforder zweiten asseen weroopi (**) hat i pressioning Detected - Descring Packet (**) Standformer (n. R.) (Preside 19 (**) 13 al februari (**) - * 10
	assertation and an annual second difference in discovery in the second s
	96/47/2024-254/352 4/We15 (editing) (¹⁴) (1/23) Perr Sources Detected: Despiring Fischer(¹⁴) (Carolinations (nulli (Possible II) (15.47) (A.4.17) (editing) = 1.02

Gambar 13. Notifikasi Port Scanning pada Telegram

3) Serangan Ping Of Death

Komputer penyerang akan melakukan serangan dengan jenis serangan yang sama dengan target Alamat IP yang sudah ditentukan. Tampak pada Gambar 15. Komputer Penyerang melakukan serangan Ping Of Death.



Gambar 14. Percobaan Serangan Ping Of Death

Komputer melakukan penyerangan kepada target IP yang sudah ditentukan dan dalam

waktu yang bersamaan, untuk hasil deteksi dari Suricata dapat dilihat pada Gambar 4.8



Gambar 15. Notifikasi Ping Of Death pada Log Suricata

Sedangkan untuk Notifikasi sesuai dengan skrip yang diberikan bahwa di kirimkan ke Telegam di jeda 10 detik, Berikut adalah notifikasi yang diterima oleh Telegram.



Gambar 16. Notifikasi Ping Of Death pada Telegram

3.1.2. Pengujian Demiliterized Zone (DMZ)

Pada konfigurasi sebelumnya bahwa untuk mengakses server private atau production hanya bias menggunakan port 443. DMZ akan dikatakan layak jika rule yang diterapkan telah berjalan dengan semestinya. Dimana Rule tersebut adalah: "Jika

trafik yang berasal dari komputer Client menuju WEB server dengan protocol tcp

dengan Dst. Port 80, maka request layanan WEB server akan di block".[10]

1) Pengujian Akses Web Port 80

Pada pengujian ini Client mencoba mengakses web mahapay.com dengan port 80 atau http request.

			*
+ - 0 6 012//100400	- Andrew Control of Co		
	E		
	Situs ini tidak dapat dijangkau		
	management of the state of the second second second		
	Color: • Policies contrangen • Manunitas provy dan tirmail		
	(111)		

Gambar 17. Pengujian akses port 80 atau http

2) Pengujian Akses Web Port 443

Pada pengujian ini Client mencoba mengakses web mahapay.com dengan port 443 atau https request.



Gambar 18. Pengujian akses port 443 atau https

3) Pengujian Ping ke IP Server Aplikasi

Pada pengujian ini client atau attacker mencoba Ping ke IP server aplikasi.

s ping 192,168.3.59
PING 192,168,3.59 (192,168,3.59) 56(84) bytes of data.
From 10.10.234.81 icmp seg=1 Destination Host Unreachable
From 10.10.254.81 icmp seg=2 Destination Host Unreachable
From 10.10.254.81 icmp seg=3 Destination Host Unreachable
From 10.10.254.81 icmp seg=4 Destination Host Unreachable
From 10.10.254.01 icmp seg=5 Destination Host Unreachable
From 10.10.254.81 icmp seg=6 Destination Host Unreachable
From 10.10.254.81 icmp seg=7 Destination Host Unreachable
From 10.10.254.81 icmp seq=8 Destination Host Unreachable
From 10.10.254.81 icmp_seq=9 Destination Host Unreachable
From 10.10.254.81 icmp_seq=10 Destination Host Unreachable
From 10.10.254.81 icmp_seq=11 Destination Host Unreachable
From 10.10.254.81 icmp_seq=12 Destination Host Unreachable
From 10.10.254.81 icmp_seq=13 Destination Host Unreachable
From 10.10.254.81 icmp_seq=14 Destination Host Unreachable
From 10.10.234.81 icmp_seq=15 Destination Host Unreachable
From 10.10.254.81 icmp_seq=16 Destination Host Unreachable



Lisensi: Creative Commons Attribution-ShareAlike 4.0 International License (CC BY-SA 4.0)

204

4. KESIMPULAN

Berdasarkan dari hasil penelitian yang ditulis penulis telah dilakukan, maka penulis menarik kesimpulan bahwa System Intrusion Detection System (IDS) dan Intrusion Prevention System (IPS) Pada installation suricata berhasil mendeteksi serangan yang dilakukan oleh attacker atau penyerang yang hendak melakukan serangan Syn Flood Attack, Port Scanning dan Ping Of Death. Dalam penelitian ini, Suricata berhasil mendeteksi serangan Syn Flood Attack, Port Scanning, dan Ping of Death dengan berbagai skenario yang telah dilakukan. Pentingnya penggunaan rules yang tepat juga terbukti dapat meningkatkan kemampuan deteksi serangan pada jaringan. Selain itu, keberhasilan Suricata dalam mendeteksi serangan juga bergantung pada pembaruan dan konfigurasi yang tepat. Adanya pembaruan rules terbaru dan penyesuaian dengan kebutuhan jaringan yang spesifik sangat penting dalam memastikan efektivitas Suricata. Berdasarkan hasil pembahasan dapat diberikan informasi yaitu penggunaan fungsi DMZ dan firewall filtering untuk Port Knocking pada router firewall Mikrotik dapat memberikan keamanan kepada server utama (DMZ) dan keamanan pada server router (Port Knocking).

Dengan demikian, Topologi yang di rancang terbukti efektif dan dapat diterapkan sebagai kemanan jaringan pada PT. Maha Digital Indonesia (*Mahapay*), penggunaan Suricata juga dapat membantu administrator jaringan dalam mengidentifikasi serangan dan mengambil tindakan pencegahan yang tepat. Dengan keandalannya dalam mendeteksi serangan dan fleksibilitasnya dalam integrasi dengan sistem keamanan lainnya, Suricata menjadi pilihan yang baik sebagai sistem IDS/IPS untuk meningkatkan keamanan jaringan.

5. DAFTAR PUSTAKA

- A. Elanda and D. R. R. Simamora, "Audit dan Investigasi Intrusion Detection System (IDS) pada Infrastruktur Jaringan Kampus dengan menggunakan Metode Indeks KAMI (Studi Kasus: STMIK Rosma)," 2021. [Online]. Available: https://e-journal.rosma.ac.id/index.php/inotek/article/view/128
- W. W. Widiyanto, "SIMRS Network Security Simulation Using Snort IDS and IPS Methods," *Indones. Heal. Inf. Manag. J.*, vol. 10, no. 1, pp. 10–17, Jun. 2022, doi: 10.47007/inohim.v10i1.396.
- [3] P. B. Pramudya, "Implementation of signature-based intrusion detection

system using SNORT to prevent threats in network servers," J. Soft Comput. Explor., vol. 3, no. 2, pp. 93–98, 2022, doi: 10.52465/joscex.v3i2.80.

- [4] N. Nuroji, "Penerapan Intrusion Detection and Prevention System (IDPS) pada Jaringan komputer sebagai pencegahan serangan Port-Scanning," J. Data Sci. Inf. Syst., vol. 1, no. 2, pp. 41–49, 2023, [Online]. Available: https://doi.org/10.58602/dimis.v1i2.44
- F. T. Anugrah et al., "Implementasi Intrusion Prevention System (IPS) [5] Menggunakan Suricata Untuk Serangan SQL Injection," Techné J. Ilm. Elektrotek., vol. 21, p. 12, 2022.
- E. Suteja, E. N. Kumalasari, and S. Raharjo, "PERANCANGAN SISTEM [6] KEAMANAN JARINGAN UNTUK MENGURANGI KEJAHATAN CYBER MENGGUNAKAN TEKNIK DEMILITARIZED ZONE (DMZ) DAN FIREWALL RULES (Studi Kasus: Laboratorium Basis Data IST AKPRIND)," 2021.
- [7] D. Hidayat, "Mengoptimalkan Pencegahan Serangan Brute Force pada Linux melalui Penerapan Metode Aplikasi IDS Snort," JITEKH, vol. 11, no. 2, 2023, doi: 10.35447/jitekh.v11i2.764.
- Y. Arta, A. Syukur, and R. Kharisma, "Simulasi Implementasi Intrusion [8] Prevention System (IPS) Pada Router Mikrotik," IT J. Res. Dev., vol. 3, no. 1, pp. 104–114, Aug. 2018, doi: 10.25299/itjrd.2018.vol3(1).1346.
- [9] J. A. Dharma and Rino, "Network Attack Detection Using Intrusion Detection System Utilizing Snort Based on Telegram," bit-Tech, vol. 6, no. 2, pp. 118-126, 2023, doi: 10.32877/bt.v6i2.943.
- T. Rahman and R. M. Adha, "Keamanan Jaringan dengan Metode Access List [10] Demilitarized Zone pada Cisco RV042," Keamanan Jar. dengan Metod. Access List Demilitarized Zo. pada Cisco RV042 Taufik, vol. 6, no. 2, p. 11, 2021.