



Analisis 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, ²aawaskita@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 Indonesia (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 kamanan 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

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 seperti 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 Demilitarized Zone (DMZ). Hasil yang di harapkan adalah ids dan nips dapat mendeteksi dan melakukan block pada aktifitas yang mencurigakan.

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.xx/24 179.xxx.xx.2/24
2	Server Web Service	179.xxx.xx.3/24

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 :

Tabel 2.2 Kebutuhan Hardware

No	Jenis Perangkat	Spesifikasi	Jumlah
1	Server Rackmount	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• CPU AR9344 600MHz• RAM 128MB• Storage 128MB• OS RouterOS• 10 Port	1
4	PC Tower	<ul style="list-style-type: none">• Intel Pentium Dual-Core E5800 @3.20GHz• RAM DD3 4GB• WD HDD 3.5" 300GB• OS Kali Linux 2024.2	1

5	Server Rackmount	<ul style="list-style-type: none"> • Intel Xeon E5 2620 @2.10GHZ • RAM DDR4 70GB • HDD 6TB • OS Ubuntu Server 22.04 	1
---	---------------------	---	---

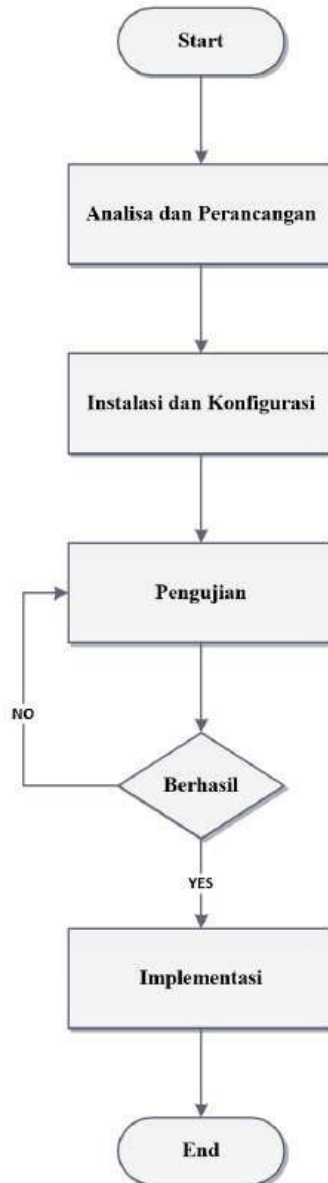
3. Kebutuhan Software

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

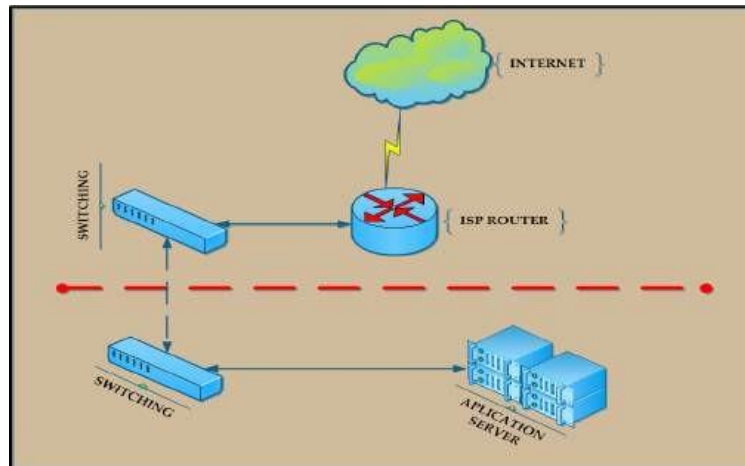


Gambar 1. Flowchart kerangka kerja

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



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
...
# 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.

# 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
```


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
```

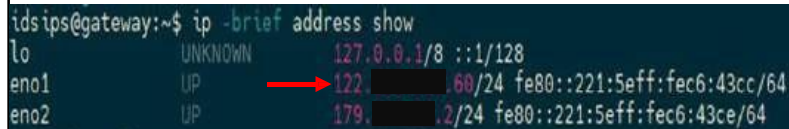
Step 2 – Install jq atau output dengan type json

```
$ sudo apt -y jq
```

Step 3 – Temukan IP Publik server

```
$ ip -brief address show
```

Output



```
idsips@gateway:~$ ip -brief address show
lo          UNKNOWN    127.0.0.1/8  ::1/128
eno1       IP          122.160/24  fe80::221:5eff:fec6:43cc/64
eno2       IP          179.12/24   fe80::221:5eff:fec6:43ce/64
```

Step 4 – Masukkan file aturan baru ke dalam konfigurasi suricata

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

```
...
rule-files:
- suricata.rules
- local.rules
...
```

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
```

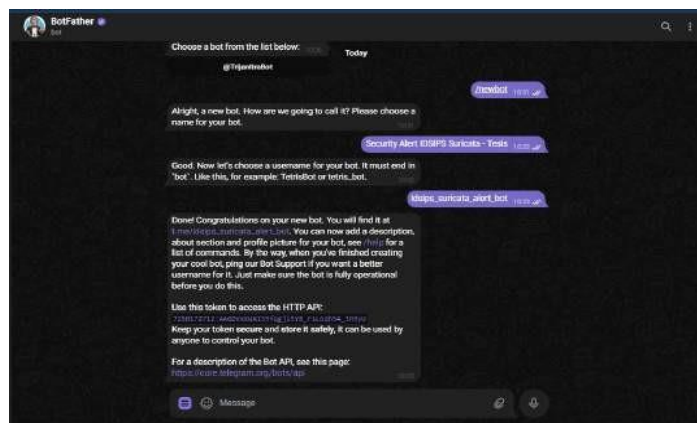
```
# Listen mode: pcap, nfqueue, custom_nfqueue or af-packet
# depending on this value, only one of the two following options
# will be used (af-packet uses neither).
# Please note that IPS mode is only available when using nfqueue
#LISTENMODE=af-packet
LISTENMODE=nfqueue
# Interface to listen on (for pcap mode)
IFACE=eno1
```

Gambar 4. Aktivasi IPS Mode

2.5.3. Konfigurasi Notifikasi Bot Telegram

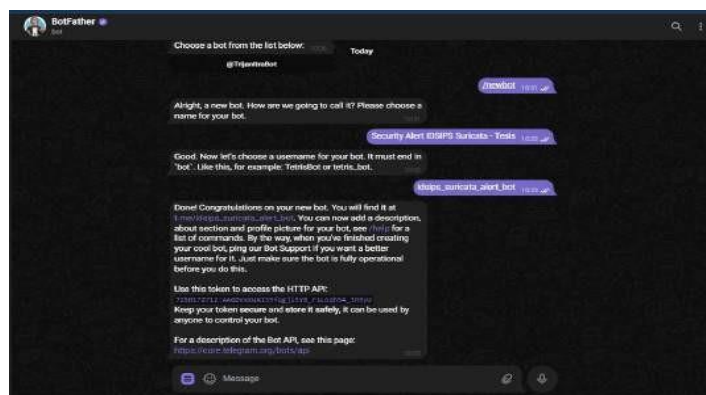
Telegram tidak hanya menyediakan fitur untuk chatting online tetapi juga menambahkan bot secara fungsional dengan fungsi tertentu yang beroperasi secara otomatis sebagai respons terhadap perintah atau permintaan pengguna.[9] **Step 1 – Membuat bot untuk notifikasi suricata menggunakan Feature di Telegram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

- Ketik /newbot



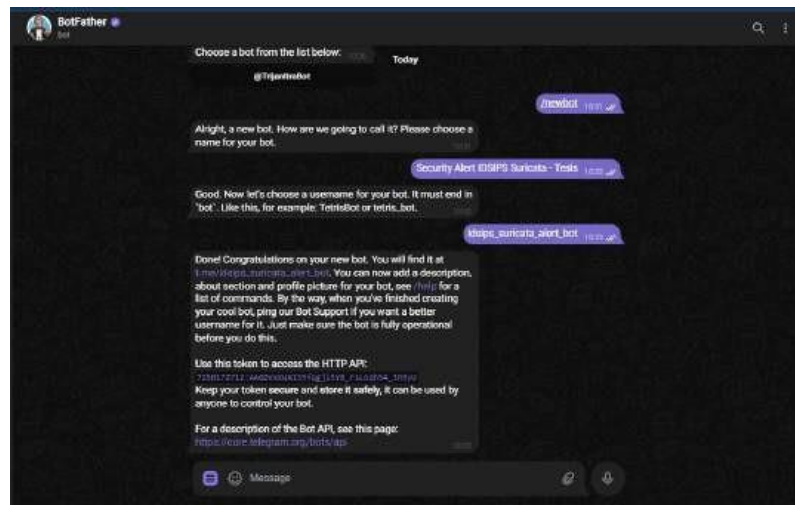
Gambar 5. Membuat bot baru

Step 2 – Masukan Nama Bot



Gambar 6. Masukan nama bot

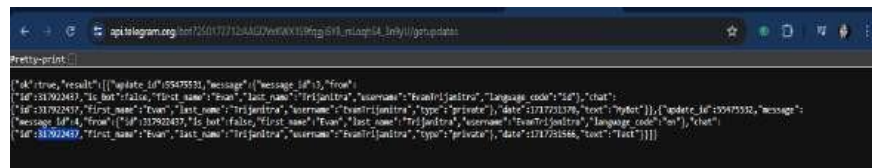
Step 3 – Masukan Username Bot



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

```
$ sudo nano suricata_IDSIPS_alert.sh
```

Step 6 – Masukan Skrip berikut

```
#!/bin/bash

# Ganti dengan API token bot Anda
BOT_TOKEN="7250172712:AAGDVxKWX1S9fqgji5YB_rsLoqhS4_3n9yU"

# Ganti dengan chat ID Anda
CHAT_ID="317922437"

# Path ke file log Suricata
LOG_FILE="/var/log/suricata/fast.log"

# Fungsi untuk mengirim pesan ke Telegram
send_telegram_message() {
    curl -s -X POST
```

```
"https://api.telegram.org/bot$BOT_TOKEN/sendMessage" -d
"chat_id=$CHAT_ID" -d "text=$1" > /dev>
}
# Fungsi untuk memantau log Suricata dan mengirim notifikasi ke Telegram
monitor_suricata_log() {
    tail -F -n0 "$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 – Masukkan skrip berikut

```
[Unit]
Description=Suricata          Telegram          Notifier
After=network.target

[Service]
Type=simple
ExecStart=/home/idsips/suricata_IDSIPS_alert.sh
Restart=always
RestartSec=10
User=nobody
Group=nogroup

[Install]
WantedBy=multi-user.target
```

Memulai ulang konfigurasi system

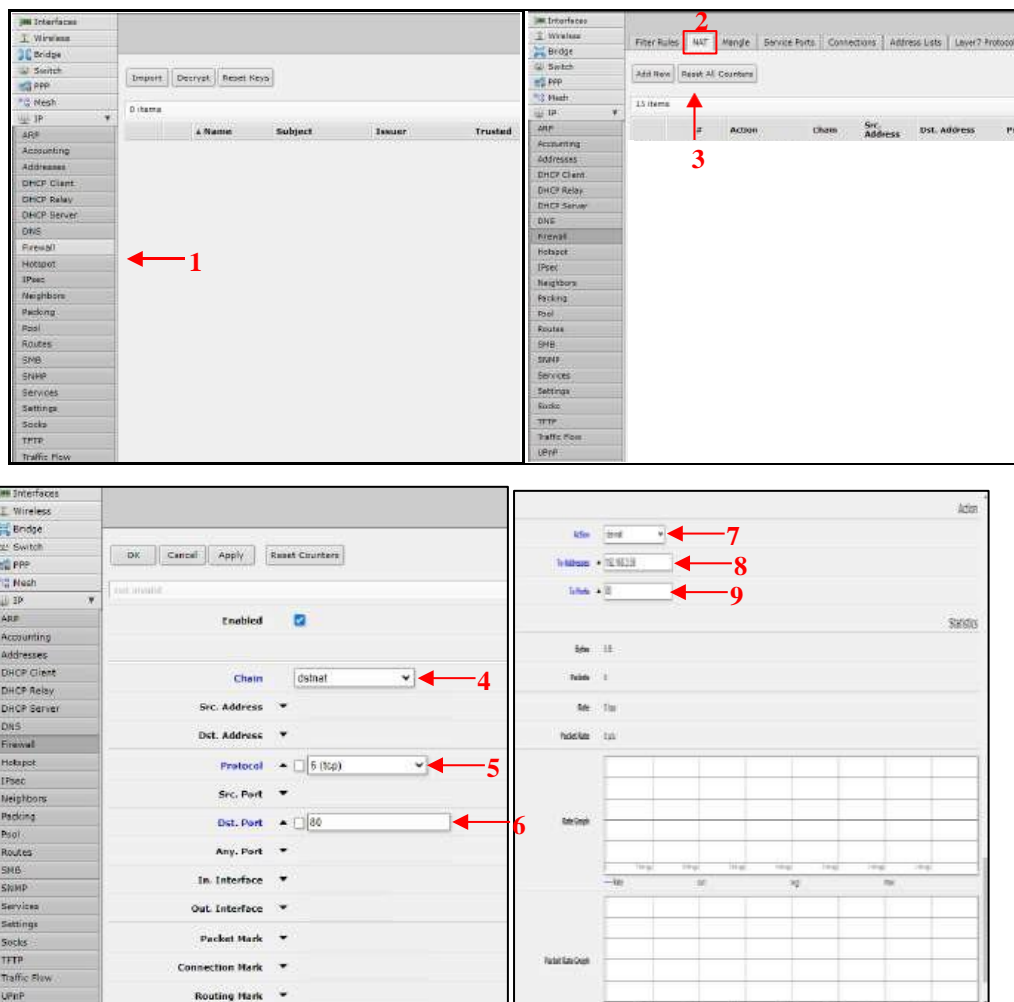
```
$ sudo systemctl daemon-reload
```

Step 10 – Menjalankan notifikasi telegram

```
sudo systemctl start suricata-telegram.service
```

2.5.2. Konfigurasi Demilitarized Zone (DMZ)

DMZ atau zona demilitarisasi, 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 mengetahui kinerja dari Suricata. Pengujian dilakukan dalam satu pekan dan waktu yang sudah ditentukan 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 Demilitarized 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 Demilitarized Zone dilakukan skenario pengujian berupa akses port 80 atau http, akses port 443 atau https dan ping ke server aplikasi. Maka didapatkan hasil seperti table berikut ini :

Tabel 1. Hasil Pengujian

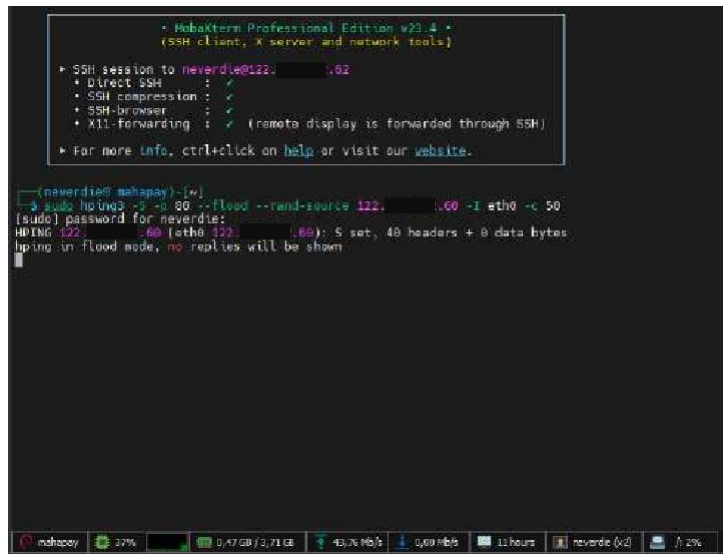
NO	PORT	JENIS SERANGAN	PERCOBAAN PENGUJIAN	ATTACKER	HASIL DETEKSI	DURASI ALERT
1.	80	Syn Flood Attack	Intrusion Detection System	Berhasil di Drop	Berhasil di Drop	10 Detik
2.	443			Berhasil di Drop	Berhasil di Drop	10 Detik
3.	80	Port Scanning		Berhasil di Drop	Berhasil di Drop	10 Detik
4.	443			Berhasil di Drop	Berhasil di Drop	10 Detik
5.	80	Ping Of Death		Berhasil di Drop	Berhasil di Drop	10 Detik
6.	443			Berhasil di Drop	Berhasil di Drop	10 Detik
7.	80	Syn Flood Attack	Intrusion Prevention System	Berhasil di Drop	Berhasil di Drop	10 Detik
8.	443			Berhasil di Drop	Berhasil di Drop	10 Detik
9.	80	Port Scanning		Berhasil di Drop	Berhasil di Drop	10 Detik
10.	443			Berhasil di Drop	Berhasil di Drop	10 Detik
11.	80	Ping Of Death		Berhasil di Drop	Berhasil di Drop	10 Detik
12.	443			Berhasil di Drop	Berhasil di Drop	10 Detik
13.	80	Akses Port	Demilitarized Zone	Client Laptop	Berhasil di Block	Real Time 1 Detik
14.	443	Akses Port			Berhasil di Akses	
15.	-	Ping IP Server Aplikasi			Berhasil di Block	

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.

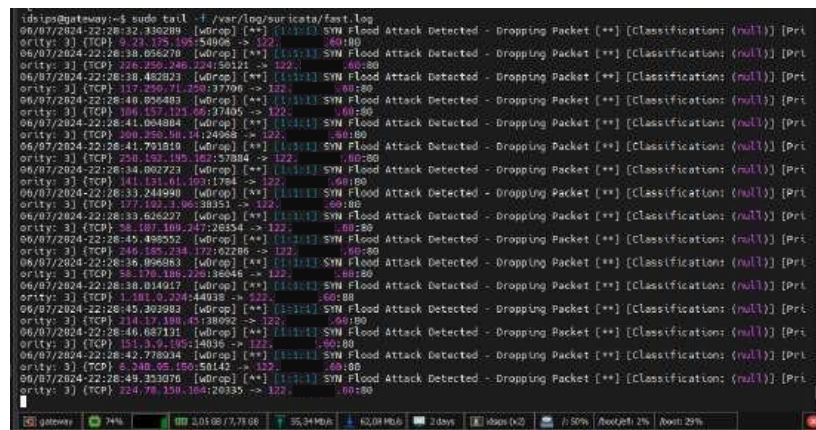
1) Syn Flood Attack

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.



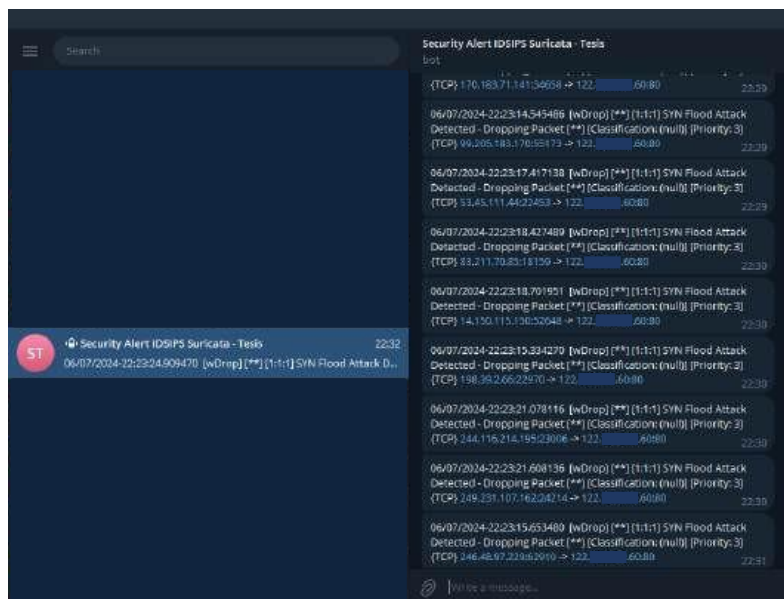
Gambar 8. Percobaan serangan Syn Flood Attack

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.



Gambar 9. Hasil Deteksi Serangan Syn Flood Attack

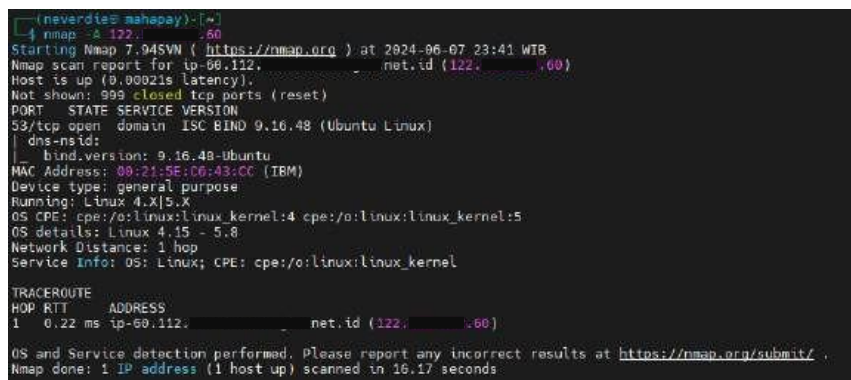
Sedangkan untuk Notifikasi sesuai dengan skrip yang diberikan bahwa di kirimkan ke Telegam di jeda 10 detik, Berikut adalah notifikasi yang diterima oleh Telegram.



Gambar 10. Notifikasi Telegram

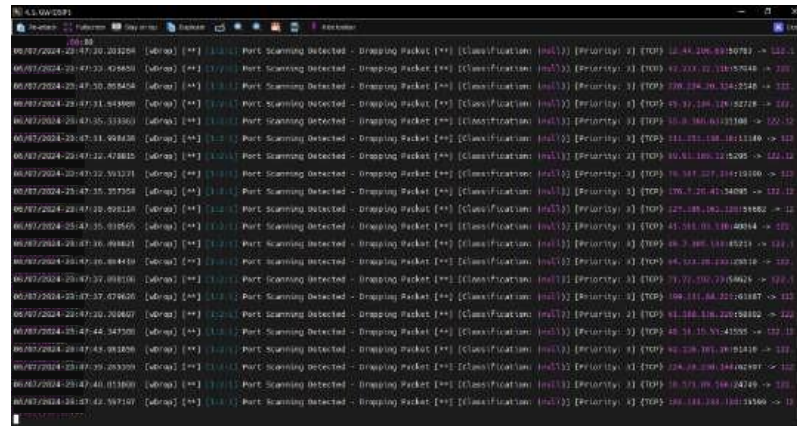
2) Port Scanning

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.



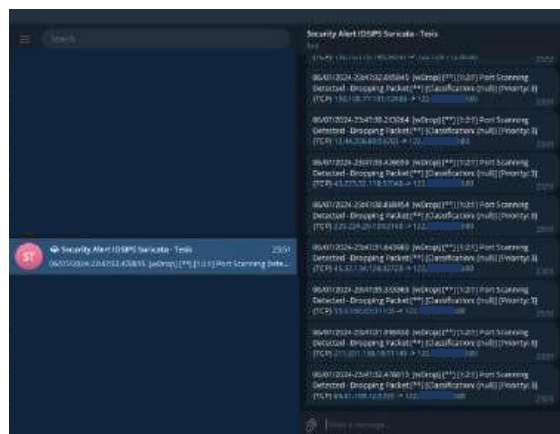
Gambar 11. Percobaan Port Scanning

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



Gambar 12. Notifikasi Port Scanning pada log suricata

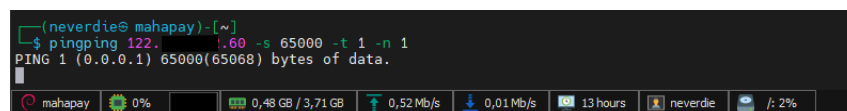
Sedangkan untuk Notifikasi sesuai dengan skrip yang diberikan bahwa di kirimkan ke Telegram di jeda 10 detik, Berikut adalah notifikasi yang diterima oleh Telegram.



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

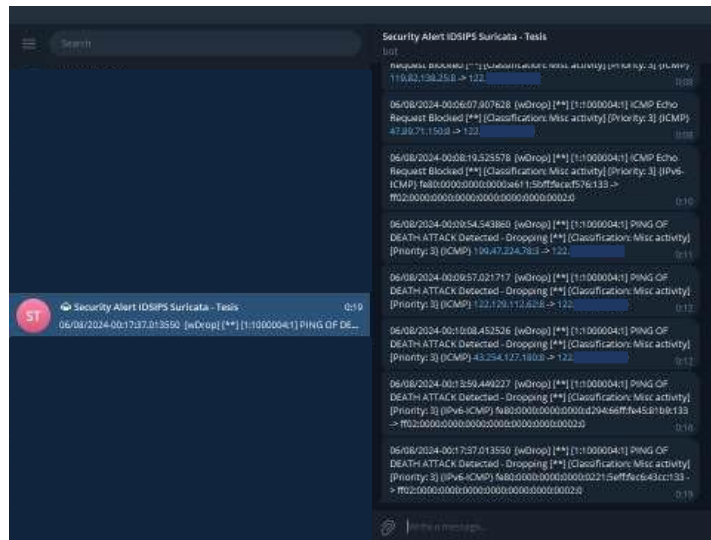
Komputer melakukan penyerangan kepada target IP yang sudah ditentukan dan dalam

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

```
06/08/2024-00:00:54.000000 [wdrop] [**] [1:1000004:1] PING OF DEATH ATTACK Detected - Dropping [**] [Classification: Misc activity] [Priority: 3] [ICMP] 198.47.224.18  
59 -> 222.154.50.11  
06/08/2024-00:00:57.021717 [wdrop] [**] [1:1000004:1] PING OF DEATH ATTACK Detected - Dropping [**] [Classification: Misc activity] [Priority: 3] [ICMP] 122.129.111.18  
18 -> 222.154.50.11  
06/08/2024-00:01:01.482926 [wdrop] [**] [1:1000004:1] PING OF DEATH ATTACK Detected - Dropping [**] [Classification: Misc activity] [Priority: 3] [ICMP] 43.254.127.10  
10 -> 222.154.50.11  
06/08/2024-00:15:32.319525 [wdrop] [**] [1:1000004:1] PING OF DEATH ATTACK Detected - Dropping [**] [Classification: Misc activity] [Priority: 3] [ICMP] 43.254.127.10  
10 -> 222.154.50.11  
06/08/2024-00:15:55.449227 [wdrop] [**] [1:1000004:1] PING OF DEATH ATTACK Detected - Dropping [**] [Classification: Misc activity] [Priority: 3] [ICMP] 43.254.127.10  
10 -> 222.154.50.11  
06/08/2024-00:17:27.013550 [wdrop] [**] [1:1000004:1] PING OF DEATH ATTACK Detected - Dropping [**] [Classification: Misc activity] [Priority: 3] [ICMP] 43.254.127.10  
10 -> 222.154.50.11
```

Gambar 15. Notifikasi Ping Of Death pada Log Suricata

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



Gambar 16. Notifikasi Ping Of Death pada Telegram

3.1.2. Pengujian Demilitarized Zone (DMZ)

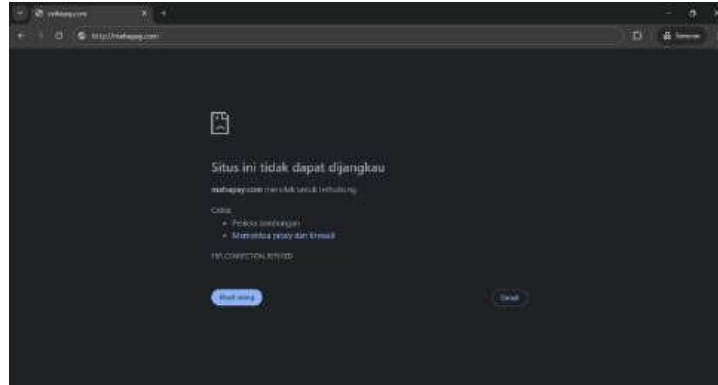
Pada konfigurasi sebelumnya bahwa untuk mengakses server private atau production hanya bias menggunakan port 443. DMZ akan dikatakan layak jika rule yang diterapkan telah berjalan dengan semestinya. Dimana Rule tersebut adalah: “Jika

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.



Gambar 17. Pengujian akses port 80 atau http

2) Pengujian Akses Web Port 443

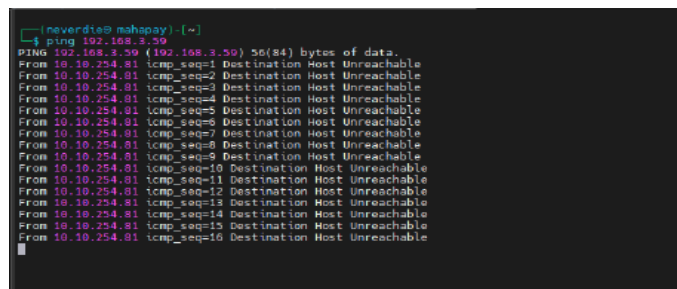
Pada pengujian ini Client mencoba mengakses web mahapay.com dengan port 443 atau https request.



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.



Gambar 19. Pengujian Ping ke IP aplikasi

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

- [1] 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>
- [2] 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/josce.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>
- [5] F. T. Anugrah *et al.*, “Implementasi Intrusion Prevention System (IPS) Menggunakan Suricata Untuk Serangan SQL Injection,” *Techné J. Ilm. Elektrotek.*, vol. 21, p. 12, 2022.
- [6] E. Suteja, E. N. Kumalasari, and S. Raharjo, “PERANCANGAN SISTEM 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.
- [8] Y. Arta, A. Syukur, and R. Kharisma, “Simulasi Implementasi Intrusion 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.
- [10] T. Rahman and R. M. Adha, “Keamanan Jaringan dengan Metode Access List Demilitarized Zone pada Cisco RV042,” *Keamanan Jar. dengan Metod. Access List Demilitarized Zo. pada Cisco RV042 Taufik*, vol. 6, no. 2, p. 11, 2021.