# Penerapan OPNsense Sebagai Sistem Keamanan Web Server Menggunakan Metode Host Instrusion Prevention System

Adi Wijaya<sup>1\*</sup>, Toibah Umi Kalsum<sup>2</sup>, Riska<sup>3</sup>

<sup>123</sup>Program Studi Rekayasa Sistem Komputer Universitas Dehasen Bengkulu. Email : adiw0625@gmail.com

# ABSTRAK

Penelitian ini dilakukan untuk melakukan deteksi serta pencegahan terhadap gangguan ataupun intrusi yang terjadi pada web server, sebab secara default sistem keamanan pada web server dalam jaringan masih tergantung dengan administrator, sehingga keamanan terhadap suatu server sangat dari tergantung kesigapan dari seorang administrator dalam merespon gangguan yang terjadi pada web server. Penelitian ini menggunakan metode Eksperimen. Penelitian ini dilakukan penerapan OPNsense sebagai sistem keamanan web server menggunakan metode Host Intrusion Prevention System. Hasil eksprimen selanjutnya didokumentasikan untuk melakukan analisis sehingga dihasilkan rekomendasi yang tepat untuk perancangan sistem keamanan web server dengan metode HIPS. Hasil dari penelitian ini menunjukkan **OPNsense dapat digunakan sebagai** Host Intrussion Prevention System terhadap jaringan LAN untuk mengamankan web server. OPNsense dapat melakukan prevention terhadap Port Scanning yang dilakukan pada jaringan LAN. Proses SQL injection gagal dilakukan yang disebabkan tidak terdapat parameter id yang ditemukan. Selain itu juga terlihat informasi bahwa web server di lindungi oleh WAF/IPS. Aplikasi metasploit melalui eth0 tidak memiliki izin untuk melakukan DOS Attack terhadap perangkat jaringan dengan alamat 192.168.80.200 yaitu alamat dari web server.

Kata kunci: Web Server, OPNsense, HIPS, Port Scan, SQL Injection, DOS Attack

# ABSTRACT

This research was conducted to detect and prevent disturbances or intrusions that occur on web servers, because by default the security system on web servers in a network still depends on the administrator,

so the security of server really depends on the alertness of an administrator in responding to disturbances that occur on the web server. This research is using experimental method. This research was carried out by implementing OPNsense as a web server security system using Host Intrusion Prevention System method. The experimental results are then documented carry out analysis so that appropriate to recommendations are produced for designing a web server security system using HIPS method. The results of this research show that OPNsense can be used as a Host Intrusion Prevention System for LAN networks to secure web servers. OPNsense can prevent Port Scanning carried out on LAN networks. SQL injection process failed because no ID parameter was found. Apart from that, information is also visible that the web server is protected by WAF/IPS. Metasploit application via eth0 does not have permission to carry out a DOS attack on network devices with the address 192.168.80.200, which is the address of the web server.

*Keywords: Web Server, OPNsense, HIPS, Port Scan, SQL Injection, DOS Attack* 

# 1. PENDAHULUAN

Pemanfaatan jaringan komputer sebagai sarana untuk mencari informasi dan berkomunikasi telah mengalami perkembangan pesat pada saat ini. Jaringan komputer menjadi elemen krusial dalam evolusi teknologi informasi, karena segala aspek dalam ranah teknologi informasi memerlukan jaringan komputer sebagai medium komunikasi antar pengguna teknologi tersebut. Jaringan komputer juga berperan sebagai saluran akses ke berbagai situs web yang terhubung dalam suatu server web di dalam jaringan komputer. Namun, penggunaan jaringan ini tidak terlepas dari potensi ancaman yang mungkin timbul dari pengguna jaringan komputer lainnya. Oleh karena itu, diperlukan suatu sistem yang mampu mencegah serangan terhadap integritas jaringan komputer.

Secara default, sistem keamanan pada server web dalam jaringan masih sangat bergantung pada administrasi, sehingga keamanan suatu server sangat terkait dengan responsibilitas seorang administrator terhadap gangguan yang mungkin terjadi. Dalam situasi ini, sistem yang ada saat ini dapat menimbulkan kesulitan bagi administrator ketika terjadi gangguan serius terhadap server web, mengakibatkan downtime atau ketidakmampuan koneksi jaringan, yang pada gilirannya dapat memperlambat proses pemulihan server. Oleh karena itu, seorang administrator membutuhkan suatu sistem yang dapat membantu memonitor dan memberikan informasi segera ketika terdeteksi adanya gangguan atau ancaman terhadap server web. Sistem tersebut juga diharapkan mampu melakukan tindakan pencegahan terhadap gangguan atau ancaman yang berhasil diidentifikasi.

Salah satu metode yang dapat diimplementasikan untuk membangun sistem pencegahan tersebut adalah Host Intrusion Prevention System (HIPS). Dengan menggunakan metode ini, sistem dapat dibuat untuk melakukan pencegahan pada berbagai lapisan, termasuk filtering paket dan inspeksi sistem secara real-time. Ada banyak perangkat lunak yang dapat digunakan untuk menerapkan metode HIPS ini, salah satunya adalah OPNsense. OPNsense merupakan sistem operasi berbasis FreeBSD yang dapat digunakan untuk keperluan firewall dan routing dalam jaringan komputer. difungsikan OPNsense dapat sebagai sistem pendeteksian dan pencegahan intrusi dalam jaringan komputer. Dalam membangun Sistem Intrusion Prevention System (IPS) dengan OPNsense, pendekatan tersebut didasarkan pada Suricata dan memanfaatkan Netmap untuk meningkatkan kinerja serta mengurangi penggunaan CPU.

# 2. KERANGKA TEORITIS

Secara default sistem keamanan pada web *server* pada jaringan lokal hanya bergantung pada sorang administrator jaringan saja, dimana dengan keadaan seperti itu tidak menutup kemungkinan akan adanya gangguan dari dalam jaringan yang dapat menyebabkan kegagalan sistem pada *server*. Adapun skema diagram blok sistem defaul dari akses web *server* yang ada saat ini dapat dilihat pada Gambar 1.



Gambar 1. Blok Sistem Keamanan Default

Pada Gambar 1, dapat dilihat proses *default* akses website yang ada pada web *server*, dimana *client* dapat mengakses website dengan mengetikkan alamat dari website tersebut, baik berupa domain ataupun IP *address* dari web *server* tanpa adanya sebuah sistem keamanan. Untuk meningkatkan sistem keamanan terhadap web *server* dapat diterapkan sebuah sistem yang dapat mengamati dan melakukan pencegahan terhadap gangguan yang terjadi.

Dari sistem keamanan default tersebut memiliki kelemahan yaitu, kelemahan pertama, vaitu ketergantungan pada satu orang administrator, dapat menyebabkan web server rentan terhadap serangan jika administrator tersebut tidak kompeten atau tidak memiliki waktu untuk melakukan pemantauan keamanan. Administrator yang tidak kompeten mungkin tidak mengetahui cara konfigurasi dan pemantauan keamanan web server yang tepat. Administrator yang tidak memiliki waktu mungkin tidak dapat memantau aktivitas web server secara berkala. Kelemahan kedua, yaitu tidak dapat mendeteksi dan mencegah serangan secara otomatis, dapat menyebabkan web server tidak dapat segera dilindungi dari serangan. Administrator jaringan harus secara manual memantau aktivitas web server untuk mendeteksi adanya serangan. Jika serangan tidak terdeteksi secara cepat, maka serangan tersebut dapat menyebabkan kerusakan yang lebih parah.

Untuk mengatasi kelemahan-kelemahan tersebut, dapat diterapkan sistem keamanan yang lebih kompleks, yaitu sistem keamanan yang dapat mengamati dan melakukan pencegahan terhadap gangguan yang terjadi. Sistem keamanan tersebut dapat terdiri dari beberapa komponen, seperti firewall, IDS, dan IPS.

# 3. METODOLOGI PENELITIAN

# 1. DIAGRAM BLOK PERANCANGAN



Gambar 2. Diagram Blok Perancangan

Pada Gambar 2 dapat dilihat bahwa terdapat penambahan server dengan sistem operasi OPNsense yang akan digunakan sebagai Host Intrusion Prevention System (HIPS) server yang akan memantau ataupun melakukan deteksi serta pencegahan intrusi ataupun ancaman terhadap web server.

Prinsip kerja dari Host Intrusion Prevention System (HIPS) sebagai sistem keamanan pada web server dengan melakukan pemantauan ataupun deteksi lalu lintas data yang dianggap sebagai intrusi atau gangguang yang menuju ke web server sesuai dengan rules yang sudah diberikan, sehingga HIPS akan memicu peringan dan melakukan tindakan pencegahan dengan men-drop ataupun mem-blokir lalu lintas data yang mengarah ke web server.

# 4. HASIL DAN PEMBAHASAN

# A. Pembahasan

Dalam penelitian ini di masukkan aplikasi berbasis web DVWA, dimana DVWA ini adalah singkatan dari *Damn Vulnerable Web Application* yang merupakan sebuah aplikasi yang dirancang khusus dengan berbagai kerentanan untuk keperluan tes terhadap sistem keamanan. Adapun tampilan dari aplikasi web DVWA dapat dilihat seperti pada Gambar 3.



Gambar 3. Tampilan Aplikasi DVWA

Dalam mengamankan server web, OPNsense menggunakan tools suricata, dengan suricata ini web

server yang sudah diterapkan dalam jaringan dengan suricata sebagai HIPS tidak dapat diserang baik menggunakan Port Scanning, SQL Injection, dan juga DOS attack sesuai rencana pengujian yang dilakukan dalam penelitian ini. Adapun hasil dari deteksi oleh OPNsense dapat dilihat pada Gambar 4.

a a a a a a a a a a a a a a a a a a a		E Adventures ( pro-	andr: 8	8-10									
+ - a		0 A HILLINGTON	di Gaada	dera						0			1
ICPR	1	and the second second						-	= <u>a</u>			-	
i lineati	1	Services: Intrusio	n Dete	ction: #	idministra	tion						<b>r</b> (	
Capite Note:		Server Instant			vet 6415	-							
DHDHA DHDHA	1						(64)	0 1	interio	686	No.	12-	
(Destaught)	•	Desitang	10	Adam.	history.	Sevence .	fait	Destrution	Part 1	Albert		10	é,
Intrasee Detection	•	2022 11 17700 12 01 122	1812779	strend	**	0.004	- 10	Conceptual State	10	ST PERSONNEL	the horas		
Advertision.		\$120 (1-1) THE OWNER AND	1012112	durat	14	22.5.5		101.011.011.011		ET POLICYPer	In Asia		
Andrey Log-Dec		1115-11-11790-01-11.115	interes	aband	-	2224	-	101201201201		AT POLICY Pass	the marrie	. ,	
And Dell' (march	141	1012-10-10T00-08-02-242	10110	showed	lat.	-03.0.0		29,201,01,01	47	ET POLICIPAN	the Autors	- 1	
-		3110-10-11798-43-01.134	3412115	should	144	43.64		079-225-220-299	#7	IT POLICY	in and		
Network Tate	0	HID O HYPE COLUMN.	2422172	dent	in .	9.65.8	-	10.25.25.25.25	91.	(TPROTEM	the Aurist		
Converting	•	0005-01-00100-41.01-AM	1012103	daned	let .	0244		(0120120120)	80.	ET POLICY Page	10 6.01	. 1	
(moundplate	•	2023-85-07798-40.52.44L	101777	itered	144		40	75.25.25.351	42	\$7 14 5 63 Page	In Adv	- 1	
(and from )		1011-11-10700-11-01-008	1012173	about	lat.	584.5		101201-20120-0	4	IT POLICY From	Inner		
Preset .													

Gambar 4. Log File Deteksi OPNsense

Selain itu hasil dari deteksi tersebut, OPNsense juga melakukan *prevention* atau *host intrusion prevention system* yang dapat dilihat pada menu *alert adminstration intrusion detection* seperti yang terlihat pada Gambar 5.

18) - B- Hann Inc.		II topiet impression	ease a	1.000			
+ - 0		0 8	auno		projection 🙂	17 E	ŝ
I DPD-					exception Province and denian and		1
a viter		12 - 14 mm - 3	1.1	10.			-
A 1174		Services: Intrusio	on Detec	tion: Lo	og File	0.8	ŧ.
b tierrest							
Caption Probai	4						
040744					A ment Bernig + D He	18-	
0074							
0romes1NS	•	Dete	Sciently	Freques	- Line		
		00001031635438609039	-		(1000) (1000) (1000) (1000) (1000) (1000) (1000) (1000) (1000) (1000)		
		10010-01-010000-01	100.00	10000	http://www.energine.com/aparents/aparents/aparents/		
Pulses		2023 11 1710 01:34	toring.	interio.	(2000) minimal. Hash Assemptions is represent at the service is furness (see line 10.00		
August.		2122 11 12710-10120	Norme	1011000	(20104) recently . Reventors calculate calculated as "bo", the fragmente shipt		
mainter (and		100515-0108-0024	Ser.	-	BODOG (Harring) - Facal depended survigable (Eq. Sep); the Rights in effect		
ingent.		1000, 10, 20 Can-10, 20	tion of		Name of the second a fight decrementation is descended and an extended in the second and the second at the second at the		
mental law	0	and to strength of	-		New Sciences - In all how styles are der fan Ne's in Berkenne Bei	1	
Gawtines	•						
Orderand Division	•	10111111012134	The state	10100	There is a survey of the second	•	
last have		1011-12-17138-21-24	mering	10,2001	Starts) annuals - gain spondaroon, in photographic angle consistence in practice if no 2014 artists		
· manual ·	- 1	2010-12-17120-01-04	Stating.	lacking a	(300134) Philorenge - Faund dapended non-og alatt Sag Tat 58 at Sag Sauna affact		
· minu							
The state of		The second secon					

Gambar 5. Alert Deteksi OPNsense

Dari Gambar 5, dapat dilihat *alert* yang ditunjukkan dengan *action allowed* yang ditujukan ke ke *rules ET PPLICY Possible Kali Linux hostname in DHCP Request Packet* untuk dilakukan *drop* terhadap peringatan (*alert*) tersebut seperti yang terlihat pada Gambar 6.

Gambar 6. Alert Drop Deteksi OPNsense

#### B. Persiapan Alat dan Bahan

Adapun alat dan bahan yang harus disiapkan, antara lain sebagai berikut

- 1. 1 unit PC sebagai HIPS Server dan Web Server
- 2. 1 unit Switch 8 Port
- 3. 1 Unit Laptop sebagai Attacker (Penyerang)
- 4. Sistem Operasi OPNsense
- 5. Kali Linux sebagai Penyerang
- 6. Tools Masscan untuk port scanning
- 7. Tools Loic untuk DoS Atack
- 8. SQLMAP untuk SQL Injection
- 9. DVWA Web untuk aplikasi web

## C. Instalasi dan Konfigurasi Linux Ubuntu

Tahapan ini adalah tahapan awal sebelum melakukan pengujian terhadap keamanan jaringan menggunakan sistem deteksi intrusi *shorewall*. Jadi pada tahap ini dilakukan instalasi sistem operasi Linux Ubuntu yang berperan sebagai web server. Untuk konfigurasi IP *address* pada web *Server* dapat dilihat seperti Gambar 7.

₽ root@webserver./etc/netplan	_		×
GNU nano 4.8 00-installer-config.yaml			~
This is the network config written by "subiquity"			
network:			
ethernets:			
enp0s3:			10
dhcp4: false			
addresses: [192.168.80.200/24]			
gateway4: 192.168.80.1			
nameservers:			
addresses: [8.8.8.8]			
version: 2			
2 Hotel Country and Co			
(2 <u>9</u>			
[ Read 10 lines ]			
Get Help C Write Out W Where Is Cut Text D Justif	y ^0	Cur Pos	
Exit Read File Replace Paste Text To Spe	11 2	Go To Li	ne Y

Gambar 7. IP Address Web Server

#### D. Instalasi dan Konfigursi DVWA

DVWA adalah singkatan dari *Damn Vulnerable Web Application* yang merupakan aplikasi berbasis web yang digunakan khusus untuk mempelajari celah keamanan dalam sebiuah aplikasi website. DVWA dirancang mempunyai celah seperti *SQL injection, file upload*, XSS, dan masih banyak lagi. Adapun cara untuk melakukan instalasi aplikasi DVWA adalah sebagai berikut.

1. Install web *server* apache2

Web server apache2 akan digunakan sebagai wadah untuk menyimpan aplikasi DVWA, yang mana untuk melakukan instalasi terhadap web server apache2 dapat dilakukan dengan cara mengetikkan perintah "sudo apt install apache2 -y" dan tunggu proses instalasi selesai.
Install Mariadb

Mariadb akan digunakan untuk menyimpan database dari aplikasi DVWA. Untuk melakukan instalasi terhadap mariadb dapat dilakukan dengan mengetikkan perintah "sudo apt-get install mariadb-server mariadb-client - Jurnal Amplifier November 2023 Vol 13 No 2 P-ISSN 2089-2020 dan E-ISSN 2622-2000 10.33369/jamplifier.v13i2.31514 y" dan tunggu hingga proses instalasi selesai

dilakukan. 3. Install PHP

PHP merupakan bahasa pemrograman yang digunakan dalam infrasruktur aplikasi DVWA. Untuk melakukan instalasi terhadap mariadb dapat dilakukan dengan mengetikkan perintah "sudo apt-get install php7.4 php7.4-fpm php7.4-mysql libapache2-mod-php -y" dan tunggu hingga proses instalasi selesai dilakukan.

4. Setup DVWA

Adapun langkah-langkah untuk melakukan pengaturan DVMA yaitu:

- Masuk ke direktori web server dengan perintah: cd /var/www/html
- Download atau clone aplikasi DVWA dari GitHub dengan perintah: git clone https://github.com/digininja/DVWA
- Ubah hak akses terhadap folder aplikasi DVWA dengan perintah: sudo chmod -R 777 DVWA
- Pindah ke folder config aplikasi DVWA dengan perintah: cd DVWA/config
- Salin file config.inc.php.dist menjadi file config.inc.php dengan perintah: cp config.inc.php.dist config.inc.php
- Buka file config.inc.php dengan perintah:
- Buka me config.inc.php dengan perintan: nano config.inc.php
- Lakukan perubahan value terhadap db\_server, db\_database, db\_user, db\_password, dan db\_port sesuai dengan konfigurasi database yang digunakan. Sesuai dengan Gambar 8.



Gambar 8. File Config DVWA

- Simpan file config.inc.php dengan menekan Ctrl+O, lalu Enter.
- Tutup file config.inc.php dengan menekan Ctrl+X.
- Selanjutnya konfigurasi user dan database untuk DVWA, Buka MySQL server dengan perintah terminal: mysql -u root -p
- Masukkan password MySQL server.

- Buat user database dengan perintah create user 'dvwa'@'127.0.0.1' identified by 'p@ssw0rd'
- Berikan hak akses kepada user database dengan perintah grant all privileges on dvwa.\* to 'dvwa'@'127.0.0.1' identified by 'p@ssw0rd'
- Lalu Ketikan exit untuk keluar dari MySQL *Server*.
- 5. Menjalankan aplikasi DVWA

Setelah semua proses instalasi dan konfigurasi selesai dilakukan, untuk mengakses aplikasi DVWA dapat dilakukan dengan mengetikkan alamat http://192.168.80.200/DVWA menggunakan web *browser*. Maka akan terlihat pemeriksaan *setup* yang sudah dilakukan. Untuk menyelesaikan *setup*, gulir kebawah dan pilih tombol *create/reset database* seperti yang terlihat padaGambar 9.

Perfil wrenn: 7.4.3.4.bitemid;3 Perfil wrenn: 7.4.3.4.bitemid;3 Perfil wrenn: 7.4.5.4.bitemid;3 Perfil wrenn: 7.4.5.4.bitemid;3 Perfil wrenn: 8.4. ur (Feyn Exated Perfil wrenn: 8.4. ur (Feyn Exated Perfil wrenn: 9.4.bitemid;3) Perfil wrenn: 9.4.bitemid;3 Perfil wrenn: 9.4.bitemid;3
Barbani darbase Mp.GCR MoriaOB Databas posivorti ****** Databas posivorti ****** Databas (hori: £23.0.1 Databas hori: £23.0.1 Databas (hori: 526)
reCAPTCHA key Missing
Writable folder /var/www/ftmi/D/WA/hackable/upixado/. Yes Writable folder /var/www/ftmi/D/WA/config: Yes
Status in red, indicate there will be an issue when trying to complete some modules
If you see disabled on either allow_ur_figers or allow_urt_insilude, set the following in your php in the and restart Appoints
allow_orl_fopen = 0n allow_orl_include = 0n
These are only required for the Ne inclusion tabs as unless you want to play with those, you can ignore them.
Create / Reset Donatome

Gambar 9. Create atau Reset Database

Tunggu hingga proses pembuatan *database* selesai dilakukan hingga akan tampil halaman *login* dari aplikasi DVWA seperti Gambar 10.

Logie (Barro Saturate Merika) *			
+ + 0 0 B (connect)		W	0.0.5
	DVWA		
	Transie and the second se		
	300		
	Construction Call Average Street		

Gambar 10. Halaman Login Aplikasi DVWA

Untuk masuk ke aplikasi DVWA dapat menggunakan *username* "admin" dan *password* "password" sehingga tampilan dari aplikasi DVWA dapat dilihat pada Gambar 11.

+ - 0	O & TALIMAKER	mitta ka pi p	8.0	 Ď	-
	-	DVWA			
	i <mark>tenen</mark> Institus Timer Berlage / Reset 00	Welcome to Damn Vulnerable Web Application! See the wave of the Application (2010) is a MMM/KS, who policial a log is one starting the memory billion compared to provide a MMM/KS, who policial a log is a web starting the memory billion compared to provide a starting of the policy of the log is a starting of the descent policy of the log is a starting of the policy of the policy of the log is a starting with the descent policy of the log is a starting of the policy of the log is a starting of the descent policy of the log is a starting of the policy of the log is a starting of the descent policy of the log is a starting of the policy of the log is a starting of the descent policy of the log is a starting of the policy of the log is a starting of the descent policy of the log is a starting of the policy of the log is a starting of the descent policy of the log is a starting of the policy			
	Room Pattern Communication	The set of 2000s and package wains of the most contents with values stillates, with version books a difficulty, with a crope along theread studies			
	ESBY File Solation File Spheric Inscore CAPICIA	General Instructions La sate its can be derive approximation (2000). Einer by work ry through every context of a fixed best or seeing and works and names yor to sate this higher even the part before same part in the series or a new 1 and there is express or earlier, in same even which the the first two every series the approximation of the part of the series of	1.1		l
	Dill. Angeritess Dill. Indoctions (1970-11)	rystein as limit in twy protein model to entry fait particle schwichtly. Historie C., Now an both discummental and anticemented vehicedability with this patients. This is sometically the are encouraged in by and discummentation on proteins.			
	Alles Session Co. Alles South	These is a bady in time, as the transport each page, which elecars you includes time it lips for the consensing more periods addressed their terrarily socialization coding, which exists to this country ratios			
	XXS classes	WARNING			
	C'AF Bypans Jawa Script Authorsamon Dopens	Conv Vanceskis Vale Application is down observation for entraplied it is gave families provides public Most Faller on any Morreson Basics Access of Decival to exception of a provident strain reactions train as Viscontinuo er (Vincetta), which is and real maintening train. Inside a gave training and the distribution of an entral control to the second and and and accessing train.			
	Open HTTP Reditors	Disclaimer			

Gambar 11. Halaman Home Aplikasi DVWA

# E. Instalasi OPNsense

Untuk melakukan instalasi terhadap *firewall* OPNsense, terlebih dahulu harus menyiapkan media *booting* ataupun media yang akan digunakan untuk melakukan instalasi baik berupa *compact disk* ataupun *flashdisk* dengan memasukkan file sistem operasi OPNsense. Setelah semuanya siap, lakukan *booting* melalui media instalasi yang sudah disiapkan. Adapun proses instalasi OPNsense adalah sebagai berikut.

1. Login ke OPNsense

Setelah berhasil *booting* melalui media intalasi, selanjutnya *login* dengan menggunakan *username "installer*" dan *password* "opnsense" sehingga media instalasi akan masuk dan menampilkan halaman instalasi dari OPNsense.

2. Pengaturan instalasi

Pada tahapan ini akan dilakukan pemilihan mode instalasi yang akan digunakan, dimana mode yang akan digunakan dalam penelitian ini adalah mode extended instalation. Berikutnya akan ada tampilan pemilihan disk setup yang dalam penelitian ini menggunakan auto dengan menggunakan seluruh penyimpanan yang ada.

3. Proses Instalasi

Setelah melakukan pengaturan yang diperlukan, selanjutnya adalah proses intalasi. Tunggu proses intalasi selesai dilakukan dan sistem OPNsense siap untuk digunakan.

4. Penugasan Interface

Untuk menjalankan OPNsense dalam jaringan, terlebih dahulu harus menugaskan *interface* sesuai dengan fungsinya, seperti *interface* untuk WAN dan *interface* untuk LAN dengan cara *login* ke OPNsense dengan menggunakan *username* "root" dan *password* "opnsense", selanjutnya pilih *Assign Interface* dan tugaskan *interface* em0 untuk WAN dan *interface* em1 untuk LAN.

Setelah penugasan *interface*, langkah berikutnya adalah menambahkan IP *address* pada masing – masing *interface*, dimana untuk *interface* WAN akan menggunakan IP *address* 

Dinamis, sedangkan *interface* LAN akan menggunakan IP *address* statis dengan alamat 192.168.80.100. untuk menambahkan IP *address* pada *interface* LAN dapat dilakukan dengan memilih pilihan nomor 2 yaitu *set interface* IP address. Adapun hasil konfigurasinya dapat dilihat pada Gambar 12.

<ol> <li>2) Set interface IP address</li> <li>3) Reset the root password</li> <li>4) Reset to factory defaults</li> <li>5) Power off systen</li> <li>6) Reboot systen</li> </ol>	9) pfTop 10) Firewall log 11) Reload all services 12) Update from console 13) Restore a backup
Enter an option:	
*** OPNsense.localdonain: OPNsense 23.7	***
LRN (en1) -> v4: 192.168.80.100/ WRN (en0) -> v4/DHCP4: 10.0.2.15	24 //24
HTTPS: SHR256 94 6A 1C A9 8C ED AF 89 BC AE 8E A8 76 D8 E0 5B	50 F3 4C 3B 5E CA 7E A7 B3 F1 16 5B 7A 53 5F F1
8) Logout	7) Ping host
1) Assign interfaces	8) Shell
<ol><li>Set interface IP address</li></ol>	9) pfTop
<ol><li>Reset the root password</li></ol>	10) Firewall log
<ol> <li>Reset to factory defaults</li> </ol>	11) Reload all services
5) Power off system	12) Update from console
6) Reboot system	13) Kestore a backup
Enter an option:	

Gambar 12. Halaman OPNsense Localdomain

## F. Implementasi OPNsense pada Jaringan

Untuk mengimplementasikan OPNsense pada jaringan dapat dilakukan dengan beberapa konfigurasi. Dimana untuk melakukan konfigurasi terhadap OPNsense dapat dilakukan melalui aplikasi *web browser* dengan mengetikkan alamat IP LAN OPNsense yaitu 192.168.80.100 sehingga akan tampil halaman *login* OPNsense. *Login* dengan menggunakan *username* "root" dan *password* "opnsense". Setelah berhasil *login* maka akan ada halaman *dashboard* dari OPNsense seperti pada Gambar 13.

A Diteterer -	the other	- * F						
+ + 0		O A Insidesta	R.M. CHR. Computers			0	8	-
ECPD.				instant	na matteran 🗉 🔍			
Dething		Lobby: Dashb	oard			0.ettertyr.	2 stars	
Palament		types televadie	7.53	Sector				
topic A Postog		Venters	OPENEND STATEMENT OPENEND 25.5 million Penendi 25.5 million pri Penendi 15.5 million pri Penendi 15.5 millione 2021	carring!	Appendiate (self-genetice barrier Cree			
A medices & Grand		ayaana Dirolga	Her to down be optime. March Dawy With ADMINICPU & 200000 Discuss, 3	ege egel	shed, and Smapp Network Tree Summer			
ð smi		191-comp	treates	11	raciación Spánic Ladrag			7
D may		Load Average	130,137,138 Weiner	eurone over	teritoria de la callace			7 <b>#</b>
		Constraintine Let config marge	Maar Maar Kir alk Maar New 2023 Maar Maar II (1997) II (1997) II (1997)	entre entre	Renting og Dearrages Undear and 1990)		-	
		Chicage Intelativate	14	wite-	945-124			£
		The second second						

Gambar 13. Halaman Dashboard OPNsense

Selanjutnya untuk menerapkan OPNsense sebagai Host Intrusion Detection System (HIPS) dalam jaringan untuk mengamankan aplikasi berbasis web harus mengaktifkan dan melakukan download serta menerapkan rules yang dapat diakses pada menu service intrusion detection administration. Selanjutnya aktifkan mode intrusion detection dengan memberi cek list pada enable, IPS, Promiscuous mode, Enable syslog alerts, serta memilih patter matcher hyperscan dan interface yang akan diamankan yaitu LAN seperti yang terlihat padaGambar 14.

				ais © Q	
PRIMA	A Settings Developed Rule	a Userdelined Kiets 1	ichedule		
Firewalt	C atenad note				fuil tela 🗊
	O trabled				
Services	0 PS mode		4		
norma @	O Promiscuous mode				
DUCES .	O thable sysleg aterts				
Desman Dist	2 O trable eve syslog output				
Intrasion Dataction	O Pattern matcher	Pyperscen			
Administration	() interfaces	UN	2		
Policy	3	O these Ad			
Log File	O Rotate log	whenkity	2		
Monit Ø	O Save logs	12			
Countras .					
Linbourd DMS					
Web Proce 4	Apply				
Dimen					

Gambar 14. Halaman Administration Intrusion Detection

Setelah dilakukan pengaktipan IDS dan juga IPS, selanjutnya juga diperlukan *download* terhadap *rules* yang akan digunakan pada menu *download* agar OPNsense dapat merekam dan juga melakukan pencegahan dengan menggunakan *tools* suricata. Ada beberapa konfigurasi yang perlu dilakukan untuk menunjang suricata dalam menerapkan IDS dan juga IPS atara lain sebagai berikut.

## 1. Enable CRC, TSO, LRO, dan VLAN

Berikutnya untuk menjalankan mode IPS pada OPNsense juga harus melakukan *enable* terhadap *hardware checksum offload, hardware TCP segmentation offload, hardware large receive offload,* dan *VLAN hardware filtering* pada *Network interface* seperti yang terlihat pada Gambar 15.

6	- article and	II Senigr(Marker) (Phone	• A		58	
$\leftarrow \rightarrow 0$		0 6	economic analysis		0	19 D
ICPD				Fortag Officerum Socardonnam	- Q.	
⊆ luffly In Russiting	í	Interfaces: Settings				
18 typero		Between Interfaces				Arres D
A montest	1.4	Orantain CK	Other technic Section officer			
(MAR)		O Redware Tab	Other and the second se			
Angunetic	4	6 vartivart ukb	Ditable backson by provine official			
(and and		O VL/10 Hardware Printing	rables as reduce they			
Helphon: Security		Barrasha	C Anno 101 APP months			
Western Contract on Contract o	*	P45907				
Otherfight		C Travell Initian	0			
Magnetics		Bingland	Mandani	-		
a yesi		0 SHCP VHILLE BY REPORT				
· free		There is the Distance in				



# 2. Mengaktifkan Rules LAN

Rules LAN harus diaktifkan untuk menandai paket yang masuk dari jaringan LAN agar diteruskan kepada *rule* apapun yang sudah diaktifkan pada *intrusion detection* (*Default allow LAN to any rule*) seperti yang terlihat pada Gambar 16.

a anne		2 Littl ( here )		• 10									1
+ + 0		0.5	0000-100-1111	d, south and the s	ñ.,						\$		0 C =
ICPO											aline a ali		
in salay A depending	Î	Firewall: Rul	es: LAN							-	n ang ang	ţ,	-
A mailes		0	Personal	Annes	not	Instatta	Part	Arristo	Shine	4	Sourigton @		
a times!	_	100									hiteratulty present (who	•0	
1000		E == 1 0	invertigenter	LOU address	10	Distant	alumi)				Infailt along the same of	• •	0.8
Categories		0 =- 10	24"	1.All and				1			Selad about Application applies		10 *
Sitter .	-	r per	:	ting (dashed)		0 HAT			No.	4		· bernet	
No.		S B ADMINE	- Statute	the strend of the									
THEFT		The Max Idian to He	(date)										
iat Inspiration Inspiration		plantine killer vo	and on 2 fed. the could be a fed. the	er saut synda. Etni is sie synd	10,200	Beaddor ar fei neol 11 Hechnik	the week	need a pa	det i di bi a	uit	al, filoneare tratifiya oo bedi	nta, mani	forst pay.
2 Martin													
(Lettings	-												
Legities													
Dagworts	0												
Q (174		Contraction of Contra	all										

Gambar 16. Rules LAN

# G. Hasil Pengujian

#### 1. Pengujian port scanning

Pengujian ini dilakukan dengan menggunakan *tools* Masscan yang ada pada kali linux dengan tujuan untuk melihat *port* apa saja yang sedang dibuka pada web *server* yang sudah diterapkan dalam penelitian ini. Dimana untuk menjalankan *tools* masscan dapat dilakukan dengan membuka aplikasi masscan pada menu aplikasi di kali linux. Selanjutnya untuk melakukan *scan port* terhadap *web server* dapat menggunakan perintah "sudo masscan -p0-65500 192.168.80.200 –rate=10000" pada terminal aplikasi masscan seperti Gambar 17.



Gambar 17. Port Scanning dengan Masscan

Pada Gambar 17Gambar 17, dapat dilihat hasil dari *port scanning* tidak memperoleh informasi *port* yang ada pada web *server* yang disebabkan oleh pengaturan *rules drop* oleh IPS seperti yang terlihat pada Gambar 18.

1 Hammer	midel d	1.4 A									
+ - 0		0 & Harris Management	dere:						0	10 1	6 =
I OPD	į.	and a second second				erebje	Pound to donat	a .			٦
8 11mm	1	1010 LL LTT 2020 IT 364 2022/10	transfer	1	6224	6	123.123.225.225	17	ET POLICI Possibili PORU	- 1	
Q 1991		IT11 11 117-15 26 11 415 . 261275	thest	44	12.0.8	10.	125.253.255.255	(#	ET MACTIMUM PURA		
		mananimutan_ musit	shind	2	and the second		114.0m; 0m; 240	10	CONTRACTOR AND AND	1	
Capitol April	24	00010.0010.001.002	alloand.	-	3444	40.	34,316,216,116	40.	CONTRACTOR AND		
Dethe	41	2010-10-10700/01-0405	stand	14	10.02	- 44	101203-00203		ST POL CYPHIA Market		
D-served Dell		PROPERTY AND ADDRESS OF ADDRESS O	disard	-	23.0.0		111.211.211.211	17	AT PERSONNELLA PARTY	. 1	
Internation (Internation)		DID IN OTHER ADA	short	in .	4444	44	111.254.256.255	10	all reductive markly match		
		ATTA DA LITTRE DE LL'UNA 2002010	itenet	14	63.64	- 10	101203202035	67	ET POCCEPTION FAIL		
Adapt		2013 11 (1710) 27.07.495	should	10	22.5.5	68	105,201,201,201	17	ST POLICY PARTY AND		
rapite		1011 A. 17100 LUT 10. 1011	stivett	10	8865	- 18	101010-00120	17	ET POLICY Poor Dru Purcu	. 1	
Not DECOMPTING		mistr-to-magnate_ write/s	shield	1	mode		STATISTICS.	-	11 ISLEW MARKEN		
HUR.	*	10044-11100-001(100) 100/4/3	dent	-	0.0.00	-	104 (Percent Ann		11100-0110-04-04-0		
Network Line	0	INTO O TRANSPORT SAL. INFORM	-	-		- 62	Life life per per		STATI CARACTER STATE		
Garrint	•			1							
Sinteend Links	•	THE PERSON NEW YORK, DOTAGE	and a second		444.0		21120-21120		L' POLICI Possible Part	- 1	
Non-Prang		TTTP 13-13730-42-11-494 1812972	stored	24	0004		118-120-120-120	10	ET POLICIPANETS AND	- 1	
# free	- 12	TTULD, LA DIGAT, LA AND THE THE	distort	100	03.08		110,000,000,000	10	AT ICS CODE AND A DO		

Gambar 18. Hasil Alert Port Scanning

Dari gambar 4, dapat dilihat aksi *port scanning* yang sedang dilakukan langsung di deteksi oleh OPNsense dan dimasukkan ke *ruleset emerging threats* (ET) dengan *configured action drop* seperti Gambar 19.

Trenderty	3823-33-25106:52.57.528802-0100		
Mert.	BT POLICY Peterbin Hall Lines horry	mit in DHCP Report Packet	
ALANT SAID	3422011		
Protocial	510P		
Searce IP	0.0.0.9		
Destination IP	255.255.255.255		
NAUTH POST	18		
Destination part	67		
triorlaux	tan		
Ciefgard schet	Enabled		
	2-09		
			1.0

Gambar 19. Ruleset Emerging Threats (ET) Port Scanning

#### 2. Pengujian SQL Injection

Pengujian SQL *injection* dilakukan dengan menggunakan SQL map yang terdapat pada kali linux. Untuk melakukan SQL *injection* menggunakan SQLmas pada kali linux dapat dilkukan dengan membuka *tools* SQLmap kemudian gunakan perintah "sudo sqlmap -u http://192.168.80.200/DVWA/vulnerabilities/sqli/?id=5 1 –dbs" dan masukkan *password* dari kali linux yaitu "kali" kemudian enter. Adapun hasil dari SQL *injection* terhadap web *server* dapat dilihat seperti Gambar 20.



Gambar 20. Pengujian SQL Injection

Dari pengujian tersebut dapat dilihat informasi yang menunjukkan proses SQL *injection* gagal dilakukan yang disebabkan tidak terdapat *parameter* id yang ditemukan. Selain itu juga terlihat informasi bahwa web *server* di lindungi oleh WAF/IPS seperti yang terlihat pada gambar 4.18 diatas. Padahalan jika melakukan SQL *injection* langsung menggunakan aplikasi DVWA kode tersebut dapat diterima dan mendapatkan token yang dapat digunakan untuk proses lebih dalam lagi pada SQL *injection* seperti yang terlihat pada Gambar 21.



Gambar 21. Pengujian SQL Injection Berhasil dengan DVWA

# 3. Pengujian DoS Attack

Pengujian DoS dapat dilakukan Attack menggunakan aplikasi Metasploit yang terdapat pada kali linux dengan cara membuka tools metasploit. Selanjutnya ketikkan perintah "use auxiliary/dos/tcp/synflood" untuk mengaktifkan mode DOS attack pada metasploit. Setalah itu ketikkan lagi perintah "set RHOST 192.168.80.200" dan "set INTERFACE eth0" kemudian lihat informasi yang sudah dikumulkan dengan menggunakan perintah "show options" sehingga akan tampil informasi target DOS attack seperti Gambar 22.

		144 Landina	Shell No.1
File Actions	Edit View Help		
ten t <del>he s</del> und ten			
INTERFACE	eth0	no	The name of the interface
NUM		no	Number of SYNs to send (else unlim ited)
RHOSTS	192.168.80.200	yes	The target host(s), range CIDR ide ntifier, or hosts file with syntax 'file: <path>'</path>
RPORT	80	yes	The target port
SHOST		no	The spoofable source address (else randomizes)
SNAPLEN	65535	yes	The number of bytes to capture
SPORT		по	The source port (else randomizes)
TIMEOUT	500	yes	The number of seconds to wait for new data
<u>msf6</u> auxiliar	y(dos/tcp/synflo	<b>d</b> ) >	

Gambar 22. Target DOS Attack

Dari Gambar 22, dapat dilihat informasi *interface* yang akan digunakan untuk menyerang yaitu eth0 dan *Target host* yaitu 192.168.80.200 yang merupakan IP *address* dari web *server*. Selanjutnya untuk melakukan DOS *Attack* ketikkan perintah "exploit" seperti yang terlihat pada Gambar 23.



Gambar 23. Target DOS Attack

# Jurnal Amplifier November 2023 Vol 13 No 2 P-ISSN 2089-2020 dan E-ISSN 2622-2000 10.33369/jamplifier.v13i2.31514 Dari Gambar 23, dapat dilihat informasi *RuntimeError* dengan pesan *you don't have permission* to capture on that device yang artinya aplikasi metasploit melalui eth0 tidak memiliki izin untuk melakukan DOS Attack terhadap perangkat jaringan dengan alamat 192 168 80 200 yaitu alamat dari web

dengan alamat 192.168.80.200 yaitu alamat dari web server. Dari pengujian tersebut dapat dilihat pesan (alert) warning yang ditunjukkan oleh OPNsense dan diteruskan ke *ruleset Emerging Threats* (ET) untuk dilakukan drop seperti yang terlihat pada Gambar 24.

Transforma	2871 11 1172810 17 12880-010		
alart.	PT POLICY Provins Kall Lines net	and in 1992 Report Packet	
ADALLINE .	21(22972		
Protocol	LUD#		
Searce #	8.0.0.5		
Destination IP	255.255.355.255		
Source port	66		
transmutane pert	107		
unintace .	tat		
Cut Equind action	C Faultine		
	Dros		

Gambar 24. Ruleset Emerging Threats (ET) Drop DOS Attack

## H. Hasil Analisa

#### table 1

HASIL ANALISA DARI PENGUJIAN

Jenis Pengujian	Kriteria	Hasil	Keteranga n
Pengujian Port Scanning	Pengujian dilakukan menggunaka n <i>Tools</i> Masscan pada Kali Linux untuk melihat <i>port</i> yang terbuka pada web <i>server</i>	OPNsense dapat melakukan <i>prevention</i> terhadap <i>Port</i> <i>Scanning</i> yang dilakukan pada jaringan LAN	Berhasil Dilakukan
Pengujian SQL <i>Injection</i>	Pengujian dilakukan menggunaka n <i>Tools</i> SQLmap pada Kali Linux untuk melakukan injeksi database dari aplikasi	Proses SQL <i>injection</i> gagal dilakukan yang disebabkan tidak terdapat <i>parameter</i> id yang ditemukan	Berhasil Dilakukan

	web pada	Selain itu	
	web server	juga	
		terlihat	
		informasi	
		bahwa web	
		server di	
		lindungi	
		oleh	
		WAF/IPS	
Pengujian	Pengujian	Aplikasi	Berhasil
DoS	dilakukan	metasploit	Dilakukan
Attack	menggunaka	melalui	
	n <i>Tools</i>	eth0 tidak	
	LOIC pada	memiliki	
	Kali Linux	izin untuk	
	untuk	melakukan	
	membanjiri	DOS	
	lalu lintas	Attack	
	data pad	terhadap	
	web server	perangkat	
	dengan	jaringan	
	tujuan	dengan	
	membuat	alamat	
	server	192.168.80	
	DOWN.	.200 yaitu	
		alamat dari	
		web	
		server.	

# 5. **PENUTUP**

Dari hasil penelitian yang dilakukan, disimpulkan bahwa OPNsense efektif digunakan sebagai Host Intrusion Prevention System (HIPS) untuk mengamankan web server dalam jaringan LAN. OPNsense mampu melakukan pencegahan terhadap Port Scanning yang dapat membahayakan keamanan jaringan. Selain itu, proses SQL injection tidak berhasil dilakukan karena tidak ditemukan parameter id yang diperlukan, dengan tambahan informasi bahwa web server dilindungi oleh Web Application Firewall (WAF) atau Intrusion Prevention System (IPS).

Pentingnya OPNsense dalam melindungi jaringan juga terbukti dengan ketidakmampuan aplikasi Metasploit melalui eth0 untuk mendapatkan izin melakukan Denial-of-Service (DOS) Attack terhadap perangkat jaringan dengan alamat 192.168.80.200, yang merupakan alamat dari web server. Dengan demikian, penerapan OPNsense sebagai bagian dari sistem keamanan berhasil mengatasi berbagai ancaman potensial terhadap web server di lingkungan jaringan.

# Jurnal Amplifier November 2023 Vol 13 No 2 P-ISSN 2089-2020 dan E-ISSN 2622-2000 10.33369/jamplifier.v13i2.31514 **REFERENSI**

- [1]. Adha, R R, M F Rizal, and S J I Isma, "Membangun Sistem Keamanan Jaringan Berbasis Firewall Dan Ids Menggunakan Tools Opnsense.", eProceedings of Applied Science Volume 7 Nomor 6 : 2846–2856, 2021.
- [2]. Alamsyah, Hendri, Riska Riska, and Abdussalam Al Akbar, "Analisa Keamanan Jaringan Menggunakan Network Intrusion Detection and Prevention System." , JOINTECS (Journal of Information Technology and Computer Science) 5(1): 17, 2020.
- [3]. Arta, Yudhi, Abdul Syukur, and Roni Kharisma, "Simulasi Implementasi Intrusion Prevention System (IPS) Pada Router Mikrotik.", It Journal Research and Development 3(1): 104–14, 2018.
- [4]. Chaterine, Angelica Dwi Putri, "Analisis Kinerja Sistem Keamanan Jaringan Dengan Metode Intrusion Detection And Prevention System (IDPS) Menggunakan Snort Terhadap Serangan UDP Flooding & SYN Flooding.", 2022.
- Al Fauzan, Muhammad Afif, and Timur Dali [5]. Purwanto, "Perancangan Firewall Router Menggunakan Opnsense Untuk Meningkatkan Keamanan Jaringan Pt. Pertamina Asset 2 Prabumulih.", In Prosiding Seminar Hasil Penelitian Vokasi (Semhavok), , 137-46, 2021.
- [6]. Pradipta, Yoga Widya, "Implementasi Intrusion Prevention System (IPS) Menggunakan Snort Dan IP Tables Berbasis Linux.", Jurnal Manajemen Informatika 7(1), 2017.
- [7]. Pratama, I Putu Agus Eka, "Smart City Beserta Cloud Computing dan Teknologi - Teknologi Pendukung Lainnya.", Informatika, Bandung, 582 Halaman, 2014.
- [8]. Rahadjeng, Indra Riyana dan Ritapuspitasari, "Analisis jaringan local area network (LAN) pada PT. Mustika ratu tbk Jakarta Timur.", Jurnal PROSISKO, Vol. 5 No. 1, 53-60, 2018.
- [9]. Rahmatulloh, Alam, and Firmansyah MSN, "Implementasi Load Balancing Web Server Menggunakan Haproxy Dan Sinkronisasi File Pada Sistem Informasi Akademik Universitas Siliwangi.", Jurnal Nasional Teknologi dan Sistem Informasi 3(2): 241–48, 2017.
- [10]. Ramadhani, Aditya, "Keamanan Informasi.", Nusantara - Journal of Information and Library Studies 1(1): 39, 2018.
- [11]. Riza Muhammad, "Sistem Keamanan Jaringan Komputer", Artikel Microcyber2. https://webdev-

id.com/berita/sistem-keamanan-jaringan/. diakses tgl 20 Agustus 2022, 2016.

- [12]. Sofana, Iwan, "CISCO CCNA dan Jaringan Komputer Edisi Revisi.", Informatika. Bandung. 614 hal, 2012.
- [13]. Syafrizal, Melwin, "Pengantar Jaringan Komputer. Andi.", Yogyakarta. 274 hal, 2005.
- [14]. Stephani, Elsa, Fitri Nova, and Ervan Asri, "Implementasi Dan Analisa Keamanan Jaringan IDS (Intrusion Detection System) Menggunakan Suricata Pada Web Server.", JITSI : Jurnal Ilmiah Teknologi Sistem Informasi 1(2): 67–74, 2020.