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

Adi Wijaya[1*], Toibah Umi Kalsum[2], Riska[3]
[123]*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 tergantung dari 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 to carry out analysis so that appropriate 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

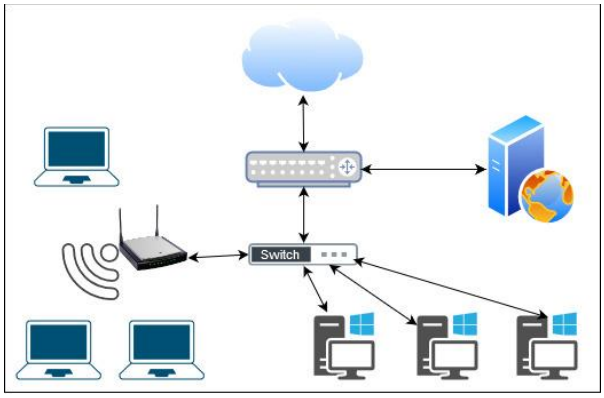
Pemanfaatan jaringan komputer sebagai sarana untuk mencari informasi dan berkomunikasi telah mengalami perkembangan pesat pada saat ini. Jaringan komputer menjadi elemen krusial dalam evolusi teknologi informasi, karena segala aspek dalam ranah teknologi informasi memerlukan jaringan komputer sebagai 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. OPNsense dapat difungsikan 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*

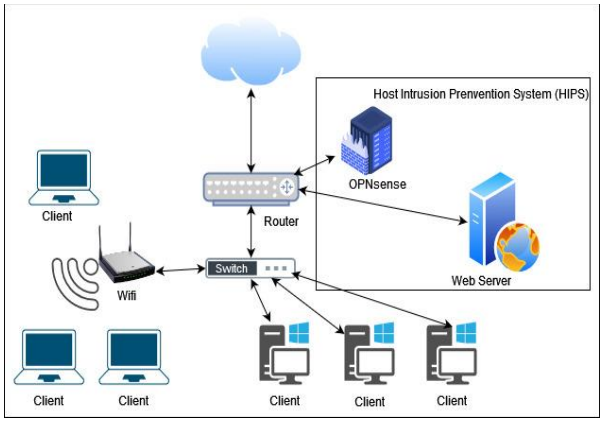
Pada Gambar 1, dapat dilihat proses *default* akses website yang ada pada web *server*, dimana *client* dapat mengakses website dengan mengetikkan alamat dari website tersebut, baik berupa domain ataupun IP *address* dari web *server* tanpa adanya sebuah sistem keamanan. Untuk meningkatkan sistem keamanan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

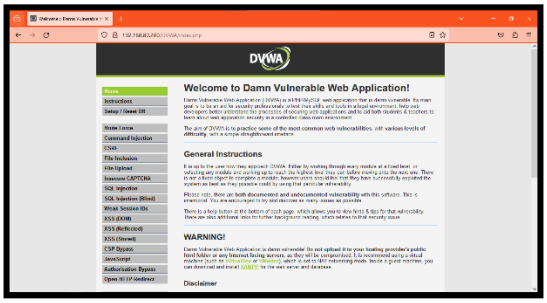
Pada Gambar 2 dapat dilihat bahwa terdapat penambahan server dengan sistem operasi OPNsense yang akan digunakan sebagai Host Intrusion Prevention System (HIPS) server yang akan memantau ataupun melakukan deteksi serta pencegahan intrusi ataupun ancaman terhadap web server.

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

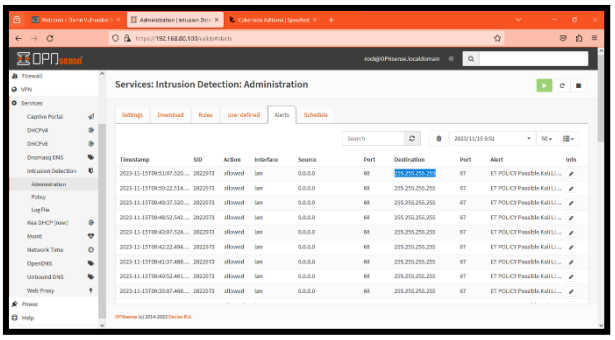
### A. Pembahasan

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.



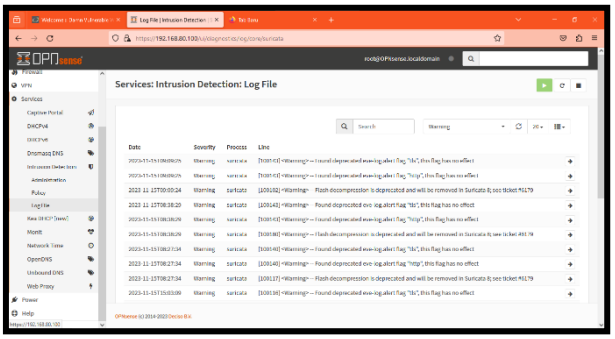

*Gambar 3. Tampilan Aplikasi DVWA*

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.



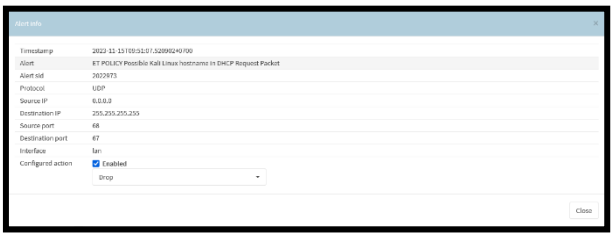

*Gambar 4. Log File Deteksi OPNsense*

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.




*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*

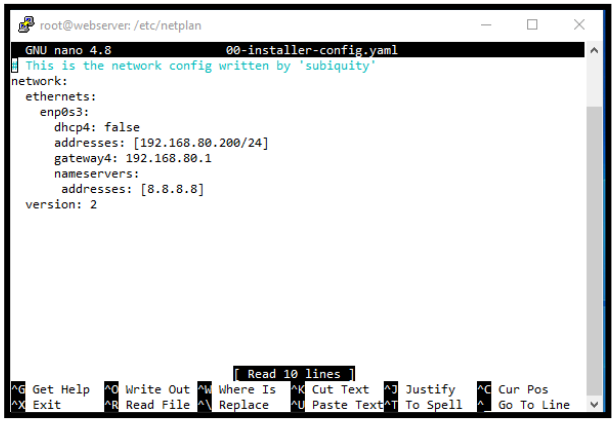
### B. Persiapan Alat dan Bahan

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.

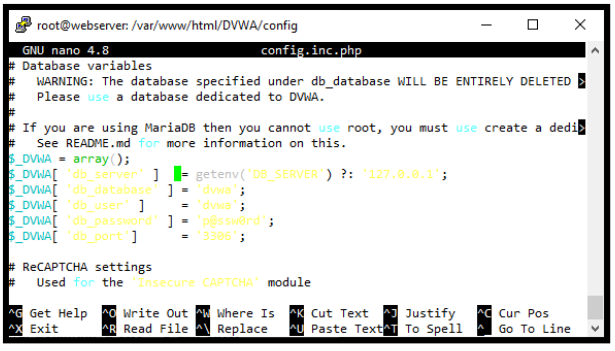



*Gambar 7. IP Address Web Server*

## 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.
2. 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 -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: 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.

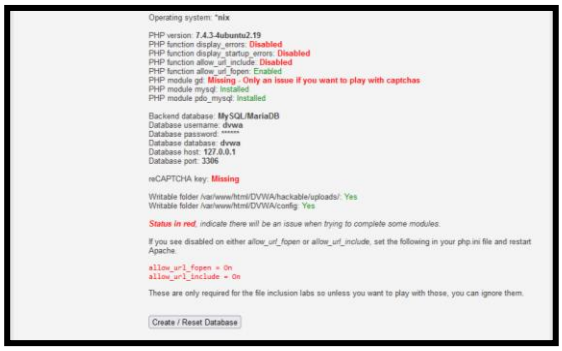



*Gambar 8. File Config DVWA*

- 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 pada Gambar 9.

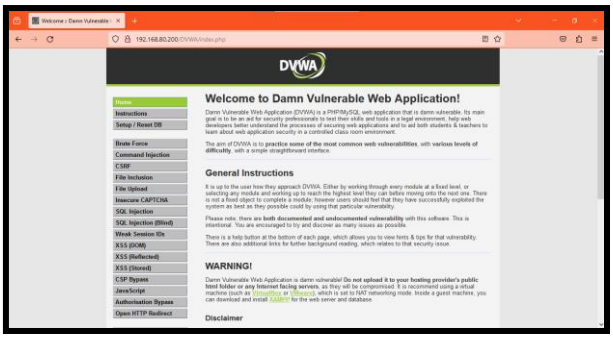



*Gambar 9. Create atau Reset Database*

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


*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.



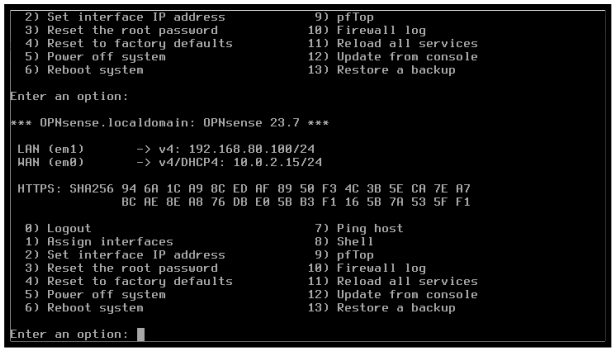

*Gambar 11. Halaman Home Aplikasi DVWA*

## 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 *interfaec* WAN akan menggunakan IP *address*

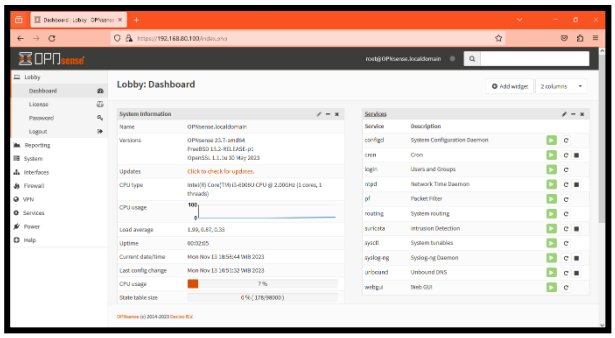
Dinamis, sedangkan *interface* LAN akan menggunakan IP *address* statis dengan alamat 192.168.80.100. untuk menambahkan IP *address* pada *interface* LAN dapat dilakukan dengan memilih pilihan nomor 2 yaitu *set interface IP address*. Adapun hasil konfigurasinya dapat dilihat pada Gambar 12.




*Gambar 12. Halaman OPNsense Localdomain*

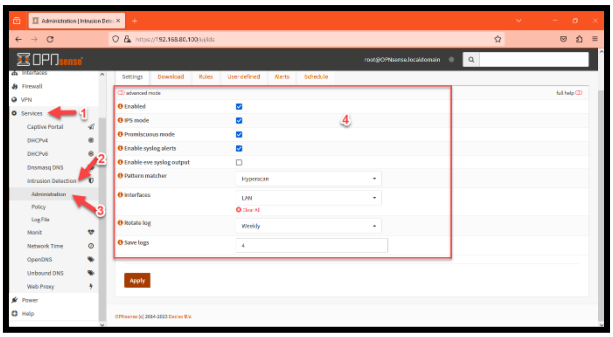
## F. Implementasi OPNsense pada Jaringan

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.




*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.

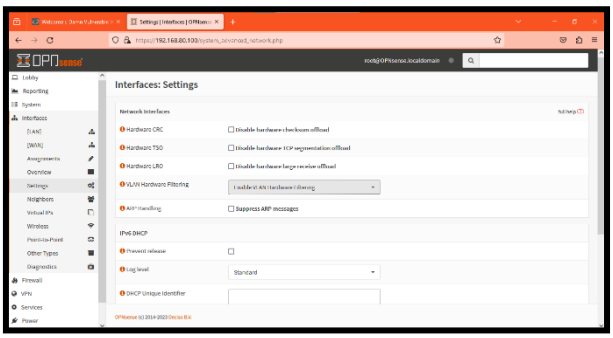


*Gambar 14. Halaman Administration Intrusion Detection*

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

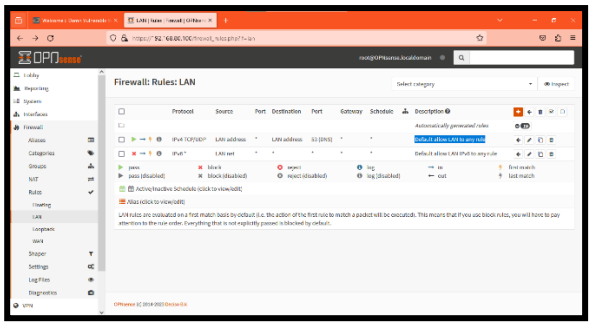
   Berikutnya untuk menjalankan mode IPS pada OPNsense juga harus melakukan *enable* terhadap *hardware checksum offload*, *hardware TCP segmentation offload*, *hardware large receive offload*, dan *VLAN hardware filtering* pada *Network interface* seperti yang terlihat pada Gambar 15.




*Gambar 15. Enable CRC, TSO, LRO, dan VLAN*

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.

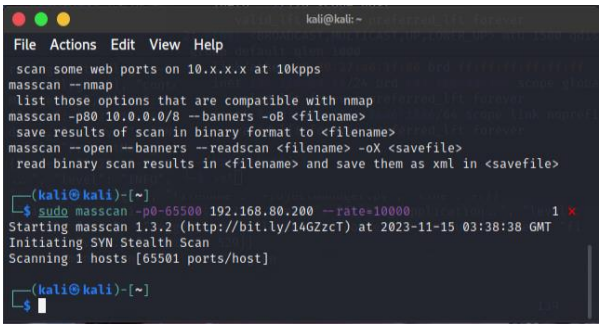



*Gambar 16. Rules LAN*

## G. Hasil Pengujian

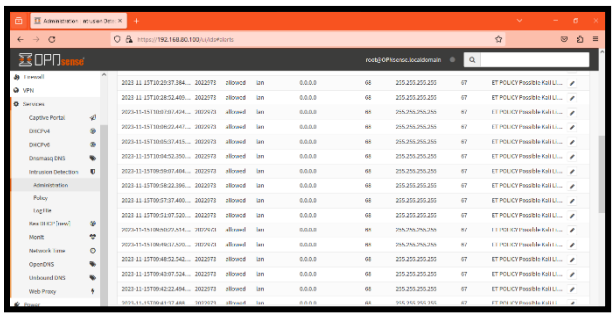
1. Pengujian port scanning

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.



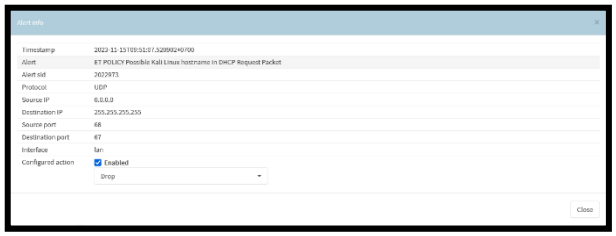

*Gambar 17. Port Scanning dengan Masscan*

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.



*Gambar 18. Hasil Alert Port Scanning*

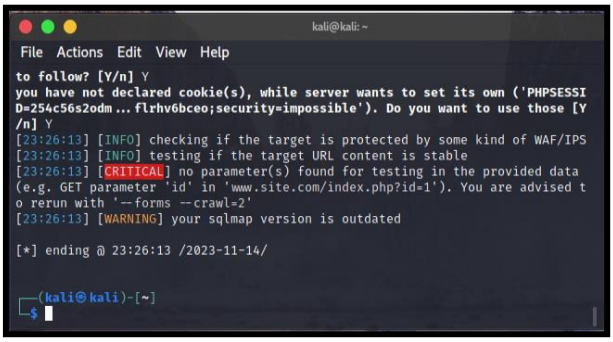
Dari gambar 4, dapat dilihat aksi *port scanning* yang sedang dilakukan langsung di deteksi oleh OPNsense dan dimasukkan ke *ruleset emerging threats* (ET) dengan *configured action drop* seperti Gambar 19.




*Gambar 19. Ruleset Emerging Threats (ET) Port Scanning*

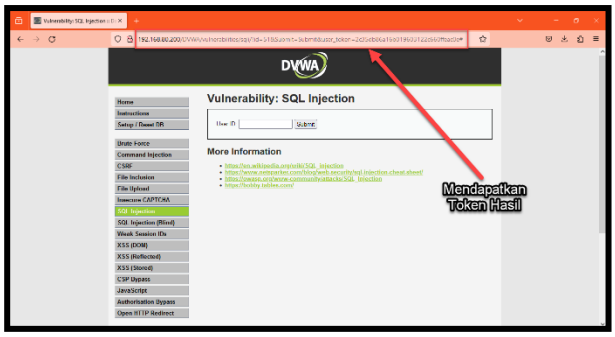
2. Pengujian SQL *Injection*

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*

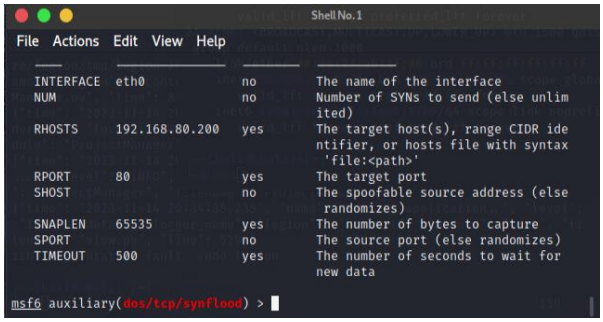
Dari pengujian tersebut dapat dilihat informasi yang menunjukkan proses SQL *injection* gagal dilakukan yang disebabkan tidak terdapat *parameter* id yang ditemukan. Selain itu juga terlihat informasi bahwa web *server* di lindungi oleh WAF/IPS seperti yang terlihat pada gambar 4.18 diatas. Padahalan 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*

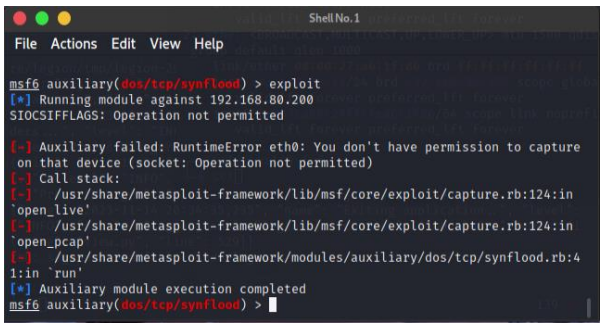
3. Pengujian DoS *Attack*

Pengujian DoS *Attack* dapat dilakukan 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.



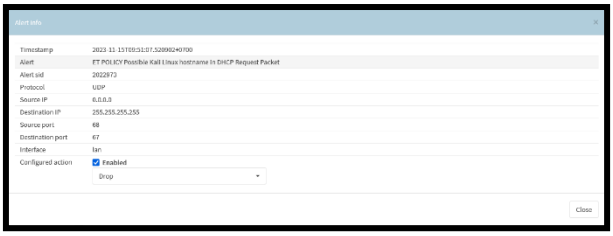

*Gambar 22. Target DOS Attack*

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*

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 *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.




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

## H. Hasil Analisa

TABLE 1

HASIL ANALISA DARI PENGUJIAN

| Jenis Pengujian | Kriteria | Hasil | Keterangan |
|---|---|---|---|
| Pengujian *Port Scanning* | Pengujian dilakukan menggunakan *Tools* Masscan pada Kali Linux untuk melihat *port* yang terbuka pada web *server* | OPNsense dapat melakukan *prevention* terhadap *Port Scanning* yang dilakukan pada jaringan LAN | Berhasil Dilakukan |
| Pengujian SQL *Injection* | Pengujian dilakukan menggunakan *Tools* SQLmap pada Kali Linux untuk melakukan injeksi database dari aplikasi | Proses SQL *injection* gagal dilakukan yang disebabkan tidak terdapat *parameter* id yang ditemukan. | Berhasil Dilakukan |

| | | | |
|---|---|---|---|
| | web pada web *server* | Selain itu juga terlihat informasi bahwa web server di lindungi oleh WAF/IPS | |
| Pengujian DoS Attack | Pengujian dilakukan menggunakan *Tools* LOIC pada Kali Linux untuk membanjiri lalu lintas data pad web *server* dengan tujuan membuat server *DOWN*. | 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*. | Berhasil Dilakukan |

## 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.

## 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.

[5]. Al Fauzan, Muhammad Afif, and Timur Dali 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.