Implementasi IDS *Snort* menggunakan Pfsense

Erick Andika, Mohamed Irvink Elmarreza
Program Studi Teknik Komputer, Politeknik Sukabumi
Jl. Babakan Sirna No.25, Benteng, Kec. Warudoyong, Kota Sukabumi, Jawa Barat 43132
erickandika@polteksmi.ac.id[1],mirvink01@gmail.com[2]

Abstrak

Keamanan jaringan merupakan hal yang paling utama dalam membangun sebuah infrastruktur jaringan. Saat ini marak terjadi pencurian data oleh pihak yang tidak bertanggung jawab, maka dari itu diperlukan tindakan untuk mengamankan sebuah jaringan. Sistem pertahanan terhadap server masih banyak yang tergantung secara manual kepada admininistrator, sehingga membuat integritas sistem menjadi tergantung pada ketersediaan dan kecepatan administrator dalam merespon gangguan yang terjadi. Salah satu alternatif untuk menanggulangi masalah tersebut menggunakan teknologi IDS (*Intrusion Detection System*). Penelitian ini menerapkan mekanisme IDS dengan menggunakan RouterOS Pfsense. Fokus dari penelitian ini adalah eksplorasi fitur IDS Snort pada RouterOS Pfsense. Pengujian konfigurasi IDS dilakukan menggunakan serangan DoS (*Denial Of Service*), *Bruteforce* dan *Portscaninng*. Metode yang digunakan adalah dengan cara Simulasi dan Studi Pustaka. Hasil pengujian dari Tugas Akhir ini adalah IDS Snort dapat mendeteksi serangan yang dilakukan oleh *Attacker* dan IDS Snort akan memberikan *Allert* serangan kemudian IP dari *Attacker* tersebut akan di blok oleh IDS Snort.

Kata kunci: Keamanan Jaringan, Pfsense, Suricata, Snort, Web Server

I. PENDAHULUAN

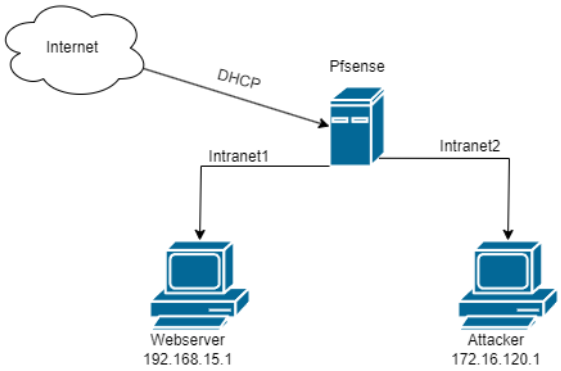
Pendeteksian serangan terhadap sebuah jaringan sebagian besar masih didasarkan pada cara-cara tradisional dengan membaca data secara numerikal, hal ini mengakibatkan proses monitoring yang dilakukan rumit dan tidak langsung dapat terbaca secara visual sementara proses infeksi terus berjalan. Selain itu para administrator keamanan jaringan cenderung menggunakan keamanan jaringan sistem *Firewall* yang ada tanpa harus memonitor lalu lintas jaringan secara real-time, sehingga seringkali sebuah perangkat/*user* baru diketahui setelah terjadi masalah tanpa sempat melakukan tindakan preventif. Sistem pertahanan terhadap server masih banyak yang tergantung secara manual kepada admininistrator, sehingga membuat integritas sistem menjadi tergantung pada ketersediaan dan kecepatan administrator dalam merespon gangguan yang terjadi. Apabila gangguan tersebut telah berhasil membuat server down atau jaringan menjadi malfungsi, administrator tidak dapat lagi mengakses sistem secara remote [1]. Untuk mencegah pengguna layanan yang tidak sah. *Intrusion Detection System* atau IDS adalah sebuah *software* yang ditujukan menjadi pemantau aktivitas jaringan atau sistem dan dapat mendeteksi jika terjadi aktivitas yang berbahaya. Terdapat beberapa software IDS yang sering digunakan didunia jaringan antara lain Snort, Suricata, OSSEC, Sagan, Bro, Solar Winds Logs & Event Manager, Open WIPS dan lain sebagainya [2].

Penelitian sebelumnya yang pernah membahas tentang Perancangan dan Analisis Kinerja Sistem Pencegahan Penyusupan Jaringan Menggunakan Snort IDS dan Honeyd oleh [3]. Analisis Sistem Monitoring Keamanan Server Dengan SMS Alert Berbasis Snort oleh [4]. Analisis Celah Keamanan Jaringan dan Server Menggunakan Snort Intrusion Detection System oleh [5].

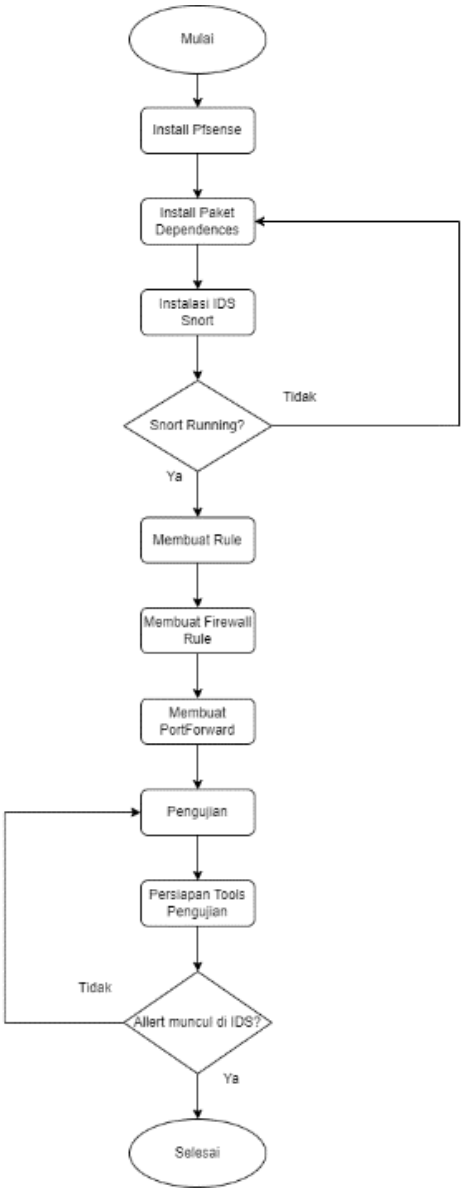
Perbedaan dengan penelitian sebelumnya pada tugas akhir ini menggunakan RouterOS Pfsense, dibandingkan dengan Linux Ubunt RouterOS Pfsense lebih unggul karena pada dasarnya Pfsense adalah router virtual. Dengan adanya tugas akhir ini diharapkan administrator server dapat dengan mudah memonitoring server.

II. METODE PENELITIAN

A. Perancangan Topologi



Gambar 1. Topologi jaringan



Gambar 2. Diagram Alir Kerja

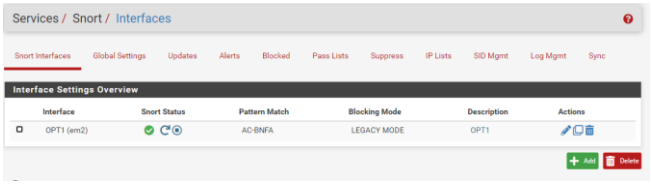
Tabel 1. IP *Address*

Device	IP *Address*	*Subnet Mask*	*Default Gateway*
IDS Snort	192.168.18.66	255.255.255.0	192.168.18.1
Web Server	192.168.15.5	255.255.255.0	192.168.15.1
Attacker	172.16.120.5	255.255.255.0	172.16.120.1

III. HASIL DAN PEMBAHASAN

1. *Interface Snort*

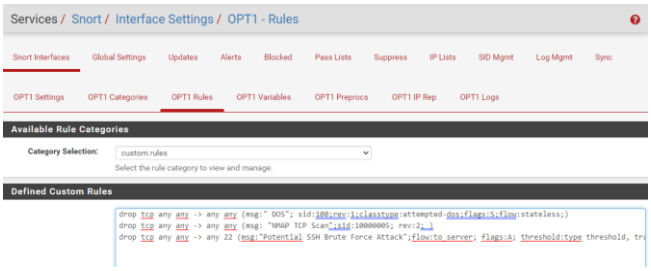
Pada Gambar 3 Interface Snort sudah aktif artinya Snort sudah bisa mengamankan web server.



Gambar 3. *Interface Snort* Aktif

2. *Rule*

Rule berfungsi agar IDS Snort dapat merespon terhadap serangan sesuai dengan rule yang ditambahkan.



Gambar 4. Menambahkan rule

Penjelasan *rule* diatas :

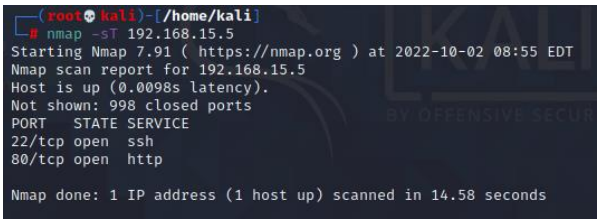
a) *drop* merupakan tindakan atau aksi sebuah *rule* yang diaktifkan, apabila diaktifkan *drop* maka aksi yang dilakukan yaitu memblokir paket yang masuk dan apabila diaktifkan alert maka hanya melaporkan atau memberi peringatan.
b) tcp adalah jenis protokol dari paket yang akan masuk.
c) any any -> any any adalah alur datangnya sumber paket menuju target, dimana pada *rule* ini sumber paket ditentukan dari mana saja dan sembarang identitas port kemudian target darimana saja sesuai dengan IP yang akan

menjadi targer oleh *Attacker*, di sembarang identitas port.

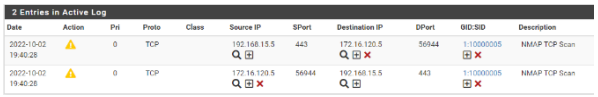
d) msg adalah pesan yang ditampilkan ketika adanya sebuah notifikasi.
e) flags adalah penentuan jenis paket yang akan masuk dimana didefinisikan S yaitu paket Syn, PA sebagai Push Ack dan R sebagi RST.
f) Classtype merupakan pengelompokan tipe *rule* yang diterapkan.
g) sid adalah signature id dari *rule* yang diaktifkan.

3. Pengujian *Portscaninng*

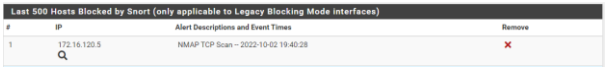
Port Scaninng merupakan ancaman yang cukup serius bagi suatu sistem jaringan komputer, *Attacker* mendapatkan informasi-informasi berharga yang dibutuhkan dalam melakukan serangan. Dengan kata lain, melakukan *Port Scaninng* ialah untuk mengidentifikasi port-port yang terbuka.



Gambar 5. Penyerangan *Portscaninng*



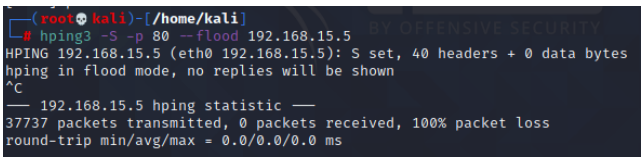
Gambar 6. *Allert Portscaninng*



Gambar 7 *Block* IP *Attacker*

4. Pengujian Dos(*Denial of Service*)

Hping adalah sebuah TCP/IP assembler dan juga merupakan command-line yang berorientasi pada pemrosesan paket TCP/IP. Hping dapat diguakan untuk membuat paket IP yang berisi TCP, UDP, atau ICMP payloads.



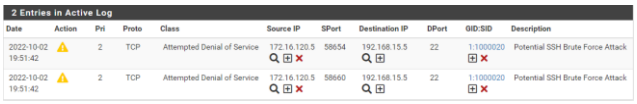
Gambar 8. Penyerangan DoS

Gambar 9. *Allert* DoS

Gambar 10. *Block* IP *Attacker*

5. Pengujian *Bruteforce*

Brute Force Attack adalah serangan paling konvensional yang bekerja di aplikasi web. Untuk memperoleh akses akun pengguna dengan mencoba menebak kata sandi dari satu pengguna atau kelompok pengguna adalah tujuan inti dari serangan *bruteforce*.



Gambar 11. *Allert Bruteforce*

Gambar 12. *Block* IP *Attacker*

IV. KESIMPULAN

IDS Snort yang di install pada RouterOS Pfsense dapat mendeteksi serangan Portscaninng, Bruteforce, Dos (*Denial of Service*) dan memberikan info IP, serangan yang dilakukan, Waktu saat penyerangan dilakukan dan dapat blok IP Attacker maka hasil dari tugas akhir dapat memudahkan administrator server karena info yang diberikan berguna terlebih lagi IDS Snort sendiri sudah memblok IP yang masuk sebagai Attacker sebelum admin melakukan tindakan.

REFERENSI

[1] E. Stephani, Fitri Nova, and Ervan Asri, "Implementasi dan Analisa Keamanan Jaringan IDS (Intrusion Detection System) Menggunakan Suricata Pada Web Server," *JITSI J. Ilm. Teknol. Sist. Inf.*, vol. 1, no. 2, pp. 67–74, 2020, doi: 10.30630/jitsi.1.2.10.

[2] L. Lukman and M. Suci, "Analisis perbandingan kinerja snort dan Suricata sebagai intrusion detection system dalam mendeteksi serangan syn flood pada web server Apache," *Respati*, vol. 15, no. 2, pp. 6–15, 2020, [Online]. Available:

http://jti.respati.ac.id/index.php/jurnaljti/article/view/343

[3] A. Syaimi, P. Utami, L. Lidyawati, and Z. Ramadhan, "Perancangan dan Analisis Kinerja Sistem Pencegahan Penyusupan Jaringan Menggunakan Snort IDS dan Honeyd," *J. Reka Elkomika ©TeknikElektro | Itenas J. Online Inst. Teknol. Nas. J. Reka Elkomika*, vol. 1, no. 4, pp. 2337–439, 2013.

[4] I. K. K. A. Marta, I. N. B. Hartawan, and I. K. S. Satwika, "Analisis Sistem Monitoring Keamanan Server Dengan Sms Alert Berbasis Snort," *Inser. Inf. Syst. Emerg. Technol. J.*, vol. 1, no. 1, p. 25, 2020, doi: 10.23887/insert.v1i1.25874.

[5] A. Hafiz, T. Kurniawan, N. A. Sivi, F. K. Ikhsan, and P. A. Pratomo, "Volume.8 Nomor.2 2020 Tahun," *Anal. Celah Keamanan Jar. Dan Serv. Menggunakan Snort Intrusion Detect. Syst.*, 2020.

[6] Utomo, Dias Sholeh, Muchammad Avorizano, Arry," Membangun Sistem Mobile Monitoring Keamanan Web Aplikasi Menggunakan Suricata dan Bot Telegram Channel "2017

[7] Suyuti Ma'sum, Muhammad Azhar Irwansyah, Muhammad Priyanto, Heri, " Analisis Perbandingan Sistem Keamanan Jaringan Menggunakan Snort dan Netfilter " 2017

[8] Wijaya, Benny Pratama, Arie " Deteksi Penyusupan Pada Server Menggunakan Metode Intrusion Detection System (Ids) Berbasis Snort " 2020

[9] We Muftihaturrahmah Tenri Sau Sepha Siswantyo, " Analisis Penggunaan Hasil Deteksi IDS Snort pada Tools RITA dalam Mendeteksi Aktivitas Beacon ", 2021

[10] Purba, Winrou Wesley Efendi, Rissal " Perancangan dan analisis sistem keamanan jaringan komputer menggunakan SNORT " 2021