Implementasi dan Analisa Snort dan Suricata Sebagai IDS dan IPS Untuk Mencegah Serangan DOS dan DDOS

Darryl Santoso, Agustinus Noertjahyana, Justinus Andjarwirawan
Program Studi Informatika Fakultas Teknologi Industri Universitas Kristen Petra
Jl. Siwalankerto 121 – 131 Surabaya 60236
Telp. (031) – 2983455, Fax. (031) - 8417658
Email: darrylsantosa9@gmail.com, agust@petra.ac.id, justin@petra.ac.id

ABSTRAK

DOS dan DDOS merupakan salah satu serangan yang paling banyak digunakan oleh *hacker*. DDOS adalah serangan dengan beberapa penyerang untuk menghabiskan resource dari target hingga target tidak bisa menghandle request. Untuk mencegah serangan diatas bisa menggunakan firewall, fungsi dari firewall adalah pertahanan pertama dari komputer yang memfilter paket yang masuk atau keluar dengan *rules* di jaringan tersebut. Firewall memfilter data berdasarkan IP Address, protokol, dan port, sehingga jika menggunakan firewall maka tidak bisa menganalisis serangan lebih lanjut. Di penelitian ini, untuk mencegah serangan ini menggunakan sebuah sistem yaitu *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS). Fungsi IDS yaitu tindakan mendeteksi lalu lintas yang tidak diinginkan pada jaringan atau perangkat, sedangkan IPS bisa mendeteksi dan langsung memperbaiki masalah tersebut.Dengan menggunakan IDS dan IPS serangan lebih bisa dianalisis, IDS dan IPS merupakan *tools* yang lebih handal dibanding *firewall*. Pengujian dilakukan dalam beberapa skenario DOS dan DDOS menggunakan tool Hping3 dan Slowloris, hasil pengujian menunjukan dari 10 skenario serangan dan bukan serangan, snort dan suricata seimbang dalam mengeluarkan alert True Positive dengan masing-masing menang 3 skenario, untuk penggunaan CPU Suricata unggul di 7 skenario , dan dalam serangan HTTP Flood suricata menghilangkan serangan lebih cepat.

Kata Kunci: IDS, IPS,DDOS,DOS

ABSTRACT

DOS and DDOS is one of the most widely used attacks by hackers. DDOS is an attack with multiple attackers to deplete the resources of the target until the target cannot handle the request. To prevent the above attacks can use a firewall, the function of the firewall is the first defense of the computer that filters incoming or outgoing packets with rules on the network. Firewalls filter data based on IP addresses, protocols, and ports, so if you use a firewall, you can't analyze further attacks. In this study, to prevent this attack using a system namely Intrusion Detection System (IDS) and Intrusion Prevention System (IPS). The function of IDS is to detect unwanted traffic on a network or device, while IPS can detect and immediately fix the problem. By using IDS and IPS attacks can be analyzed more, IDS and IPS are more reliable tools than firewalls. The test was carried out in several DOS and DDOS scenarios using the Hping3 and Slowloris tools, the test results showed that from 10 attack scenarios and not attacks, snort and suricata were balanced in issuing True Positive alerts with 3 win scenarios each, for CPU usage Suricata excelled in 7 scenarios , and in HTTP Flood attacks suricata eliminate attacks faster.

Keywords: *DOS, DDOS, IDS, IPS*

1. PENDAHULUAN

Keamanan di dunia internet sangat penting, karena ada banyak celah untuk terjadinya serangan. Di antara banyak serangan yang ada, Distributed Denial of Service (DDOS) adalah serangan yang relatif sederhana tetapi sangat kuat untuk menyerang sumber daya dari target hingga pengguna yang sah tidak bisa mengakses layanan dari target [7]. *Distributed Denial of Service* atau lebih dikenal dengan nama DDoS adalah sebuah percobaan penyerangan dari beberapa sistem komputer yang menargetkan sebuah server agar jumlah *traffic* menjadi terlalu tinggi sampai server tidak bisa *menghandle requestnya*. Perbedaan DOS dan DDOS terdapat pada sumber serangan, DOS menggunakan satu komputer, sedangkan DDOS menggunakan beberapa sistem komputer. Pada penelitian ini, serangan akan dijalankan melalui *Virtual Machine*. *Virtual Machine* (VM) adalah perangkat lunak untuk implementasi komputer dan menjalankan program seperti host pada komputer. VM menggunakan sumber daya fisik dari komputer host [2].

Alasan memakai *Virtual Machine* agar memudahkan implementasi serangan DDOS yang membutuhkan beberapa *host*. Jika ingin memakai mesin asli, maka akan membutuhkan banyak alat dan biaya. Untuk mencegah serangan diatas bisa menggunakan firewall, fungsi dari firewall adalah pertahanan pertama dari komputer yang memfilter paket yang masuk atau keluar dengan *rules* di jaringan tersebut. Firewall memfilter data berdasarkan IP Address, protokol, dan port. Namun ada kekurangan dari firewall misalnya untuk mencegah suatu paket masuk ke dalam jaringan dibuat suatu rule, selamanya paket tersebut tidak akan bisa masuk sampai rule tersebut dihapus. Di penelitian ini, untuk mencegah serangan ini menggunakan sebuah sistem yaitu *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS). Fungsi IDS yaitu tindakan mendeteksi lalu lintas yang tidak diinginkan pada jaringan atau perangkat, sedangkan IPS bisa mendeteksi dan langsung memperbaiki masalah tersebut. Dengan menggunakan IPS, administrator bisa membuat *rule* dengan parameter tambahan sehingga tidak perlu menghapus *rule* agar mengizinkan suatu paket data masuk ke jaringan. IDS dan IPS merupakan *tools* yang lebih handal dibanding *firewall*. Ada banyak contoh tools untuk IDS yaitu Solar Winds Security Event Manager, Manager Engine EventLog Analyzer, Snort dan lain-lain. Untuk contoh tools IPS yaitu Datadog Real-Time Threat Monitoring, OSSEC, Suricata, dan lain-lain.

Snort berjalan secara single thread, sementara suricata dapat dijalankan dalam multi thread sehingga bisa memakai lebih dari satu cpu core. Snort dan Suricata bisa dipakai untuk IDS maupun

IPS, mendukung beberapa OS , dan dapat dijalankan secara Network Intrusion & Prevention System.

Pada penelitian ini, implementasi sistem IDS dan IPS akan menggunakan *tools* Snort dan Suricata untuk mendeteksi dan mencegah serangan DOS dan DDOS di dalam *virtual machine.*

2. DASAR TEORI

2.1 Intrusion Detection System

Intrusion Detection System adalah perangkat lunak atau perangkat keras yang dirancang untuk mendeteksi aktivitas berbahaya atau serangan terhadap sistem atau jaringan [5]. IDS dapat melakukan inspeksi terhadap lalu lintas jaringan inbound dan outbound dalam suatu sistem atau jaringan, dan ketika menemukan serangan, maka akan memberikan peringatan apakah aktifitas tersebut termasuk berbahaya atau tidak berdasarkan beberapa level, yaitu *low*, *medium*, *high*, dan *serious*. Peringatan ini nanti akan dikirim ke *administrator* untuk dilakukan analisis dan mencari bukti dari percobaan intrusi (penyusupan). Intrusion Detection System dibagi menjadi 2 yaitu Network-based Intrusion Detection System (NIDS) dan Host-based Intrusion Detection System (HIDS) [1]:

- *Network-based Intrusion Detection System* (NIDS)
  Berfungsi untuk memantau dan memonitor semua lalu lintas jaringan pada keseluruhan jaringan, NIDS akan menangkap semua lalu lintas jaringan dan mengirimkan *copy* dari lalu lintas yang ditangkap dan mengirimkan ke IDS. NIDS biasanya diletakkan di dalam segmen jaringan di mana server berada atau di pintu masuk jaringan. Contoh IDS yaitu Snort.
- *Host-based Intrusion Detection System* (HIDS)
  Berfungsi memantau dan menganalisis lalu lintas jaringan yang masuk dan keluar dari host. Perbedaan utama HIDS dengan NIDS adalah NIDS memonitor seluruh segmen jaringan, sedangkan HIDS hanya memonitor pada host tertentu, biasanya diletakkan di server-server kritis di jaringan seperti firewall dan web server. HIDS juga menangkap lalu lintas jaringan seperti *snapshot* dan dibandingkan dengan *snapshot* sebelummnya, jika terdapat perbedaan maka akan mengirimkan alert kepada *administrator*.

2.2 Intrusion Prevention System

Intrusion Prevention System adalah sistem yang dapat secara otomatis mendeteksi aktivitas mencurigakan yang berpotensi berbahaya dalam jaringan [6]. Cara kerja dari IPS dimulai dengan memindai paket yang datang dari luar jaringan, IPS mempunyai file konfigurasi yang berisi rule-rule untuk mengidentifikasi paket yang aman dan tidak. Ketika suatu paket yang masuk terdeteksi tidak aman, maka paket tersebut akan dihapus dari jaringan. Selanjutnya IPS akan memberikan peringatan kepada administrator tentang aktifitas yang dilakukan oleh IPS. Di penelitian ini, Intrusion Prevention System yang digunakan yaitu Suricata.

2.3 Snort

Snort merupakan sebuah perangkat lunak yang berfungsi untuk mengamati aktifitas dalam suatu jaringan komputer. Komponen pada Snort terdiri dari beberapa bagian yaitu [2]:

1. *Packet Decoder*
   Berfungsi untuk mengekstrak paket dari jaringan dalam bentuk file berformat tcpdump dan mengirimkan paket ke preprocessor.
2. *Preprocessor*
   Berfungsi untuk memodifikasi paket yang rusak menggunakan beberapa operasi dan kemudian mengirimkan ulang ke *Detection Engine*.
3. *Detection Engine*
   Berfungsi untuk mendeteksi ancaman aktivitas yang ada dalam paket dengan menggunakan snort *rules*.
4. *Logging and Alerting System*
   Berfungsi untuk menghasilkan alarm atau log aktivitas intrusi yang terdeteksi oleh *Detection Engine*.
5. *Output Modules*
   Berfungsi untuk menyimpan output yang dihasilkan oleh
6. *Logging and Alerting System.*

Untuk mengoperasikan Snort ada beberapa cara yaitu:

- Sniffer mode: Pada mode ini, Snort akan menangkap semua paket pada jaringan tertentu.
- Packet Logger Mode: Pada mode ini, Snort akan menangkap semua paket yang melintas, dan menyimpan di storage.
- Network Intrusion Detection Mode: Pada mode ini, Snort akan menjalan file konfigurasi yang sudah diatur pada file snort.conf.

2.4 Suricata

Suricata adalah perangkat lunak yang bersifat *open source* dan digunakan untuk mendeteksi ancaman pada suatu jaringan. Suricata bisa diatur untuk menjadi *Intrusion Detection System* dan I*ntrusion Prevention System*. Suricata mempunyai file konfigurasi seperti yang ada di Snort, yaitu Suricata.yaml.

2.5 DOS dan DDOS

Denial Of Service (DOS) merupakan serangan untuk membanjiri lalu lintas jaringan internet pada server, sistem, atau jaringan. Serangan ini biasanya dilakukan dengan menggunakan 1 komputer. Perbedaan dengan Distributed Denial Of Service (DDOS) yaitu jumlah komputer yang dipakai untuk penyerangan jumlahnya lebih dari 1. Jika serangan DDOS dikategorikan berdasarkan layer OSI, ada 3 macam yaitu [8]:

1. Serangan berbasis volume
   Serangan ini adalah bentuk serangan DDOS yang paling umum. Serangan ini menggunakan *botnet* untuk membanjiri jaringan atau server dengan lalu lintas yang tampak sah, tetapi melampaui kemampuan jaringan atau server dalam memproses lalu lintas. Contoh serangan ini adalah UDP *flooding*, ICMP *flooding*.
2. Serangan protokol
   Serangan ini mengeksploitasi cara server memproses data untuk membebani dan membanjiri target yang dituju. Jenis serangan ini menyerang pada layer 3 dan 4. Serangan ini meniru proses 3 *Way Handshake* ketika 2 host ingin melakukan komunikasi melalui protokol TCP. Cara kerja serangan penyerang mengirimkan paket *Syn* dalam jumlah yang banyak , dan tidak memberikan *ACK*. Akibatnya target akan terus menunggu paket *ACK* tersebut dan tidak bisa melayani pengguna yang sah. Contoh serangan ini adalah SYN *flood*
3. Serangan lapisan aplikasi
   Serangan ini menyerang web server, dengan cara mengirimkan banyak respon ke HTTP *request* hingga *web server* menjadi error dan tidak bisa melayani *target*, serangan ini meniru permintaan server normal. Jenis

serangan ini menyerang pada layer 7. Contoh serangan ini HTTP *flooding*.

2.6 Virtual Box

Aplikasi yang sering dipakai untuk virtualisasi. Virtualisasi bertujuan untuk membuat mesin PC virtual yang bisa berjalan secara independen di atas sistem operasi utama [3]. Dengan memakai Virtual Box, seperti mempunyai beberapa macam PC dengan sistem operasi yang bisa diatur sesuai keinginan contohnya Windows, Linux, macOS x, dan lain-lain.

2.7 Firewall

Firewall adalah sebuah sistem keamanan jaringan komputer yang bekerja seperti tembok untuk melindungi komputer dari ancaman yang membahayakan yang berasal dari jaringan internet [4]. Firewall bertugas memonitor dan mengatur lalu lintas jaringan inbound maupun outbound berdasarkan rules yang tersedia. IPS akan diletakkan secara inline setelah firewall. Firewall dibagi menjadi beberapa jenis yaitu:

1. *Packet-filtering firewalls*
   Firewall jenis ini diletakkan di beberapa tempat seperti router atau switch. Mempunyai beberapa aturan yang dikonfigurasi berdasarkan alamat IP sumber, no port, dan lain-lain. Jika sebuah paket tidak cocok dengan aturan yang dibuat, paket tersebut akan dibuang.
2. *Circuit-level Gateways*
   Ini adalah firewall sederhana yang tidak memakan banyak sumber daya. Firewall ini menerima atau menolak paket berdasarkan lalu lintas pada saat *TCP* handshake*Stateful Inspection Firewalls*
   Jenis firewall ini menggabungkan 2 firewall sebelumnya agar mempunyai keamanan yang lebih kuat.
3. *Application-level gateways (Proxy firewalls)*
   FIrewall ini beroperasi di tingkat aplikasi. Menyaring lalu lintas antar jaringan dan sumber. Firewall Proxy membuat koneksi dengan sumber dan kemudian memeriksa isi paket.
4. *Next-generation Firewalls*
   Firewall ini menggabungkan metode seperti *Deep packet inspection, Intrusion Prevention System, Bandwidth management , URL filtering Antivirus* dan *Malware detection*. Kelebihan firewall ini dapat dapat mencegah ancaman terhadap jaringan dan memberikan tingkat keamanan yang lebih tinggi.
5. *Cloud Firewalls*
   Firewall ini dapat diimplementasikan dengan bantuan *cloud.* Firewall *Cloud* dianggap sama dengan firewall proxy.

2.8 Iptables

Iptables adalah firewall open source yang tersedia pada linux versi 2.4 atau yang lebih baru [1]. *Iptables* didasarkan pada Modul *Netfilter* yang dapat memeriksa isi dari paket untuk string tertentu dengan menggunakan dukungan pencocokan *string* pada kernel linux. *Iptables* dapat mendeteksi serangan lapisan aplikasi. *Iptables* mempunyai 3 *primary tables*, yaitu:

1. *Filter table* : menyaring paket lalu menentukan apakah paket tersebut di *ACCEPT* atau di *DROP*.
2. *Nat table* : berisi *Network Address Translations* dan *demilitarized zone*.
3. *Mangle table* : memeriksa paket dengan parameter TOS, TTL , dan lain-lain.

Terdapat 3 jenis chains default, yaitu :

1. *INPUT* : rantai ini menangani semua paket yang masuk ke dalam *server*
2. *OUTPUT* : rantai ini berisi aturan untuk lalu lintas yang dibuat oleh *server*
3. *FORWARD* : rantai ini untuk menangani lalu lintas yang dikirimkan ke server lain dan yang tidak dibuat di server utama.

Ketika *pattern* dari paket sama dengan *rules* yang tersedia maka akan dilakukan *action* yaitu:

1. *ACCEPT* : mengizinkan paket untuk masuk ke dalam *server*.
2. *DROP*: membuang paket tersebut.
3. *RETURN* : menghentikan paket agar tidak melintasi rantai (*chains*) dan mengirimkan paket kembali ke rantai sebelumnya.

3. DESAIN SISTEM

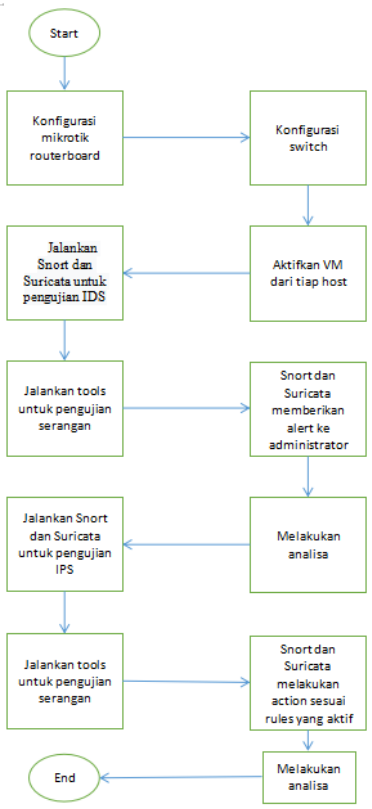
3.1 Arsitekstur Sistem

Desain topologi yang dibuat menggunakan:

1. 3 Personal Computer
2. 1 Switch
3. 1 Mikrotik Routerboard

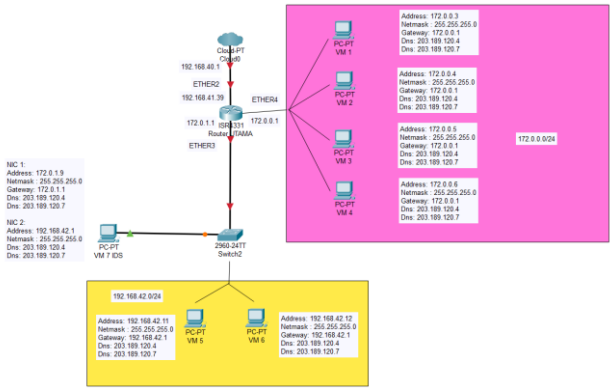
3.2 Flowchart

Flowchart untuk penelitian ini bisa dilihat pada Gambar 1.



Gambar 1. Flowchart Sistem

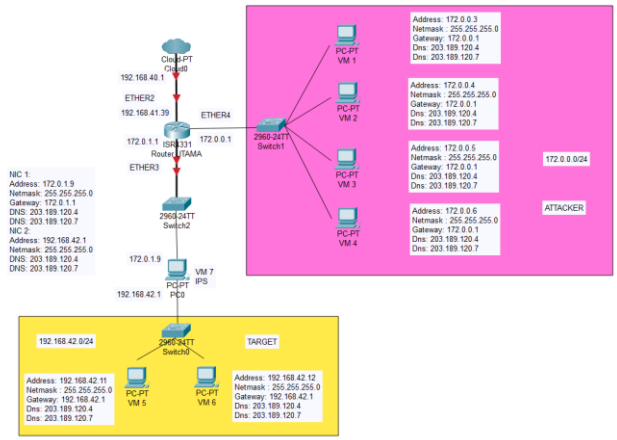
3.3 Desain Topologi Jaringan Metode IDS



Gambar 2. Desain IDS

Pada Gambar 2, Area yang berwarna magenta akan berperan sebagai Attacker, dan area berwarna kuning menjadi target serangan. Untuk penerapan IDS, Snort dan Suricata akan diletakkan di VM 7 secara SPAN dengan menggunakan switch, sehingga setiap paket yang menuju ke *target*, Switch akan mengirimkan salinan dari paket itu menuju VM 7 untuk dilakukan evaluasi.

3.4 Desain Topologi Jaringan Metode IPS



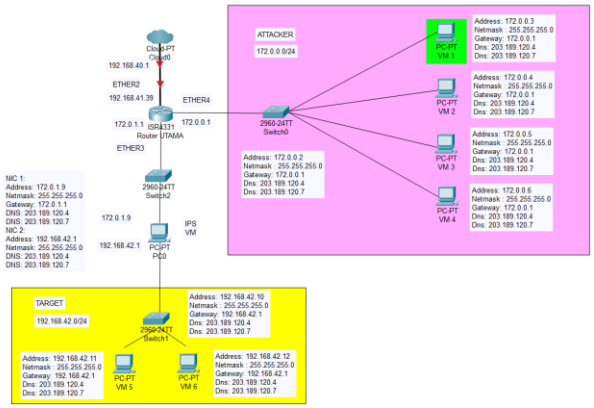
Gambar 3. Desain IPS

Pada Gambar 3, untuk penerapan IPS, VM 7 akan dijadikan *Gateway*, sehingga setiap paket yang dikirimkan ke *target* harus melewati VM tersebut dan jika ada paket yang jahat bisa dicegah agar tidak masuk ke *server*. Untuk menjadikan VM sebagai *gateway* membutuhkan 2 NIC.

3.5 Skenario Pengujian

3.5.1 Skenario DOS

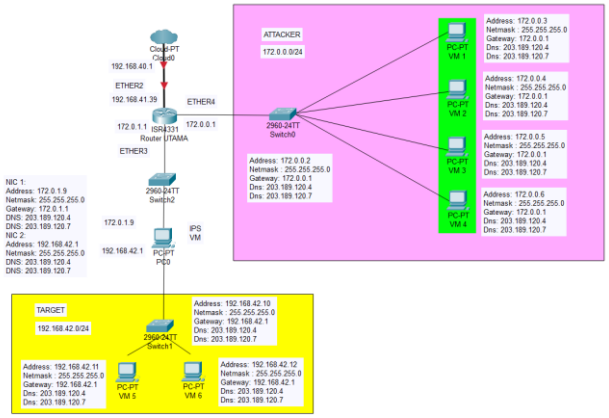
Pada skenario ini, akan menggunakan serangan berbasis DOS dengan menggunakan 1 VM sebagai attacker dan 2 VM sebagai target. Pada Gambar 4, PC berwarna hijau akan menjadi penyerang,



Gambar 4. Skenario Serangan DOS

3.5.2 Skenario DDOS

Pada skenario 2, akan mengimplementasikan serangan berbasis DDOS dengan menggunakan 4 VM sebagai attacker dan 2 VM sebagai target. Pada Gambar 5, PC berwarna hijau akan menjadi penyerang.



Gambar 5. Skenario serangan DDOS

3.6 Parameter Pengujian

Setelah melakukan pengujian serangan, akan dilakukan pengukuran kemampuan IDS dan IPS dalam mendeteksi dan menghilangkan serangan berdasarkan parameter-parameter berikut ini:

1. Performa IDS dan IPS dalam mendeteksi serangan.
2. Waktu yang dibutuhkan untuk IDS dan IPS dalam menangani serangan.

4. PENGUJIAN SISTEM

Pengujian serangan akan dilakukan dalam beberapa skenario dengan menggunakan 2 tools yaitu Hping3 dan Slowloris. Tools Hping3 akan mengirimkan serangan ICMP flood dan SYN flood,

sedangkan Slowloris akan mengirimkan serangan HTTP flood. Serangan akan dideteksi dan dicegah oleh Snort dan Suricata menggunakan rules yang sudah dibuat. Command untuk menjalankan tools yaitu:

1. sudo hping3 --icmp --flood target_ip
2. sudo hping3 -S -p 22 --flood target_ip --rand-source
3. sudo python3 slowloris.py target_ip -s 500

- --icmp : menentukan jenis paket yang ingin dikirim.
- --flood : kecepatan pengiriman.
- -s : jumlah socket sebagai penyerang
- --rand-source: menyembunyikan *source address*

Setiap serangan akan dilakukan dalam 2 bagian yaitu pengujian serangan dan pengujian bukan serangan, untuk membedakan tindakan serangan dan tindakan normal dari user.

4.1 Skenario IDS

4.1.1 Skenario DOS

4.1.1.1 Pengujian Ping Flood

Pada pengujian IDS pada Snort dan Suricata dengan paket Ping menunjukan bahwa IDS Snort lebih banyak mendeteksi serangan / *True positive alert* yang lebih banyak dan dengan waktu yang lebih cepat dibandingkan Suricata. Sementara pada pengujian bukan serangan , kedua IDS tidak mengeluarkan *alert*. Dalam pemakaian CPU, Suricata menggunakan CPU yang lebih banyak dibandingkan dengan Snort.

4.1.1.2 Pengujian Syn Flood

Pada pengujian IDS pada Snort dan Suricata dengan paket Syn menunjukan bahwa Suricata lebih banyak mendeteksi serangan / *True positive alert* yang lebih banyak dan dengan waktu yang lebih cepat dibandingkan Snort. Sementara pada pengujian bukan serangan , kedua IDS tidak mengeluarkan *alert*. Dalam pemakaian CPU, Suricata menggunakan CPU yang lebih banyak dibandingkan dengan Snort.

4.1.1.3 Pengujian HTTP Flood

Pada pengujian IDS pada Snort dan Suricata dengan paket Get request menunjukan bahwa Snort dan Suricata mendeteksi *true positive alert* dengan jumlah sama. Sementara pada pengujian bukan serangan , kedua IDS tidak mengeluarkan *alert*. Dalam pemakaian CPU, Suricata menggunakan CPU yang lebih banyak dibandingkan dengan Snort.

4.1.2 Skenario DDOS

4.1.2.1 Pengujian Ping Flood dan Syn Flood

Dari hasil tabel menunjukan bahwa pengujian IDS Snort dan IDS Suricata dengan serangan Ping Flood dan Syn Flood, hasilnya Suricata mendeteksi serangan / True positive alert yang lebih banyak dan dengan waktu yang lebih cepat dibandingkan Snort. Untuk pemakaian CPU, suricata menggunakan CPU lebih banyak dibandingkan dengan Snort.

4.1.2.2 Pengujian Ping Flood dan HTTP Flood

Dari hasil tabel menunjukan bahwa pengujian IDS Snort dan IDS Suricata hasilnya Suricata mendeteksi serangan / True positive alert yang lebih banyak dan dengan waktu deteksi yang lebih cepat dibandingkan Snort. Dalam pemakaian CPU, Snort sedikit lebih unggul dari Suricata dari pemakaian CPU.

4.2 Skenario IPS

4.2.1 Skenario DOS

4.2.1.1 Skenario Ping Flood

Dari hasil tabel menunjukan bahwa pengujian IPS Snort dan IPS Suricata dengan serangan Ping Flood hasilnya Snort mencegah serangan / True positive alert yang lebih banyak. Suricata unggul dalam waktu yang lebih cepat dalam mendeteksi serangan dibandingkan snort . Pada pengujian bukan serangan, kedua IPS tidak mengeluarkan alert. Untuk penggunaan CPU, snort lebih unggul dibandingkan Suricata.

4.2.1.2 Skenario Syn Flood

Dari hasil tabel menunjukan bahwa pengujian IPS Snort dan IPS Suricata dengan serangan Syn Flood hasilnya Suricata mencegah serangan / True positive alert yang lebih banyak . Dalam penggunaan cpu dan waktu deteksi serangan suricata juga unggul dibandingkan Snort. Suricata tidak bisa membedakan Syn flood dengan Syn normal sehingga semua paket Syn normal yang dikirim ke target akan di drop oleh suricata.

4.2.1.3 Skenario HTTP Flood

Dari hasil tabel menunjukan bahwa pengujian IPS Snort dan IPS Suricata dengan serangan HTTP Flood hasilnya Snort mencegah serangan / True positive alert yang lebih banyak dan untuk waktu menghilangkan serangan dan pemakaian CPU suricata lebih unggul.

4.2.2 Skenario DDOS

4.2.2.1 Skenario Ping Flood dan Syn Flood

Dari hasil tabel menunjukan bahwa pengujian IPS Snort dan IPS Suricata dengan serangan Ping Flood dan Syn Flood hasilnya Suricata mencegah serangan / True positive alert yang lebih banyak. Dalam penggunaan cpu dan waktu deteksi serangan suricata lebih unggul dibandingkan Snort. Suricata tidak bisa membedakan Syn flood dengan Syn normal sehingga semua paket Syn normal yang dikirim ke target akan di drop oleh suricata.

4.2.2.2 Skenario Ping Flood dan HTTP Flood

Dari hasil tabel menunjukan bahwa pengujian IPS Snort dan IPS Suricata dengan serangan Ping Flood dan HTTP Flood hasilnya Snort mendeteksi serangan / True positive alert yang lebih banyak. Dalam penggunaan CPU Snort lebih unggul , namun dalam mendeteksi serangan dan mencegah serangan Suricata lebih unggul.

4.3 Perhitungan CPU

Setiap pengujian di atas akan dicek juga untuk penggunaan CPU dari Snort dan Suricata. Untuk menghitung pemakaian CPU rata-rata pada snort dan suricata menggunakan bantuan tool Top. Top akan dijalankan dalam 5 kali dengan jeda waktu 3 detik dan akan disimpan ke dalam file txt untuk dianalisis. Command untuk menjalankannya :

sudo top -b -n 5 -p *target_process* > hasilcpu.txt

1. -b : menjalankan top dalam batch mode agar bisa mengirimkan output ke dalam program atau file lain.
2. -n : menentukan jumlah maksimum iterasi.
3. -p : untuk memonitor proses tertentu dengan id nya.

5. KESIMPULAN

Dari hasil implementasi dan pengujian terhadap sistem, dapat disimpulkan bahwa:

- Untuk pengujian IDS dan IPS pada Snort dan Suricata dengan serangan Ping Flood, Syn Flood, dan HTTP Flood menggunakan skenario DOS dan DDOS dengan 10 skenario hasilnya menunjukan Suricata unggul sedikit dalam mengeluarkan alert serangan dibandingkan Snort dengan jumlah Suricata unggul di 5 skenario, snort di 4 skenario dan 1 seimbang. Untuk penggunaan CPU Suricata lebih banyak dalam pemakaian CPU dibandingkan Snort dengan unggul 7 skenario sementara snort unggul di 2 skenario dan 1 seimbang, dan untuk waktu deteksi serangan Suricata mengeluarkan alert yang lebih cepat dibandingkan Snort dengan unggul 6 skenario , snort di 2 skenario dan 2 skenario seimbang.
- Untuk penerapan IPS pada Snort dan Suricata menggunakan mode NFQUEUE. Ketika Suricata dijalankan dalam mode NFQUEUE, Suricata tidak bisa membedakan antara syn normal dan syn flood, semua paket syn normal yang dikirimkan akan di drop oleh Suricata sehingga tidak masuk ke target. Namun ketika Suricata dijalankan dalam mode PCAP/IDS, suricata bisa membedakan antara syn normal dan syn flood.
- Untuk pengujian IPS pada Snort dan Suricata terhadap serangan HTTP Flood, Suricata lebih unggul dalam menghilangkan serangan yang menuju ke target. Pada serangan DOS di http flood snort membutuhkan waktu sekitar 45 detik untung menghilangkan serangan sementara suricata 11 detik , dan pada serangan DDOS di http flood snort membutuhkan waktu 37 detik dan Suricata di 32 detik.

6. DAFTAR PUSTAKA

[1] Gandotra, N. and Sharma, L. S. 2020. Exploring the use of iptables as an application layer firewall. Journal of The Institution of Engineers (india): Series B, (October. 2019), 707–715. DOI=https://doi.org/10.1007/s40031-020-00497-y.

[2] Garg, A. and Maheswari, P. 2016. Performance analysis of snort-based intrusion detection system. In International Conference on Advanced Computing and Communications *S*ystems (Coimbatore, India, January 22-23, 2016), 1-5. DOI=https:doi.org/10.1109/ICACCS.2016.7586351.

[3] Matthews, J, A., George, G, P., and Dhanalakshmi, M, P. 2020. Analysis of virtual machine in digital forensics. International Research Journal of Engineering and Technology(IRJET).7,3 (Maret. 2020), 3663-3668. URI=https://www.academia.edu/44168423/IRJET_Analysis_of_Virtual_Machine_in_Digital_Forensics?from=cover_page.

[4] Mukkamala, P, P. and Rajendran, S. 2020. A survey of the different firewall technologies. International Journal of Engineering Applied Sciences and Technology.5,1 (May. 2020), 363-365. URI=https://ijeast.com/papers/363-365,Tesma501,IJEAST.pdf.

[5] Othman, S, M., Alsohybe, N, T., Alwi, F, M, B., & Zahary, A, T. 2018. Survey on intrusion detection system types. International Journal of Cyber-Security and Digital Forensics. 7,4 (December. 2018), 444-462. URI=https://www.researchgate.net/profile/Ammar-Zahary/publication/329360916_Survey_on_Intrusion_Detection_System_Types.

[6] Pratama, R, F., Suwastika, N, A., and Nugroho, M, A. 2018. Design and implementation adaptive intrusion prevention system (ips) for attack prevention in software-defined network (sdn) architecture. In International Conference on Information and Communication Technology (Bandung, Indonesia, May 3-5, 2018), 299-304. DOI=https://doi.org/10.1109/ICoICT.2018.8528735.

[7] Sharafaldin, I., Lashkari, A, H., Hakak, S., and Ghorbani, A, A. 2019. Developing realistic distributed denial of service (DDOS) attack dataset and taxonomy. In International Carnahan Conference on Security Technology (Chennai, India, October 1-3 2019), 1-8. DOI=https://doi.org/10.1109/CCST.2019.8888419.

[8] Weisman, S. 2020. What is a distributed denial of service attack (ddos) and what can you do about them?. Norton. URI=https://us.norton.com/internetsecurity-emerging-threats-what-is-a-ddos-attack-30sectech-by-norton.html.