Analisis Perbandingan Kinerja Snort Dan Suricata Sebagai Intrusion Detection System Dalam Mendeteksi Serangan Syn Flood Pada Web Server Apache

Lukman[1], Melati Suci[2]
Informatika Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta
Jl. Ring Road Utara Condong Catur, Depok, Sleman, Yogyakarta 55283
[1]masman@amikom.ac.id, [2]melati.suci@students.amikom.ac.id

INTISARI

Keamanan jaringan pada web server merupakan bagian yang paling penting untuk menjamin integritas dan layanan bagi pengguna. Web server sering kali menjadi target serangan yang mengakibatkan kerusakan data. Salah satunya serangan SYN Flood merupakan jenis serangan Denial of Service (DOS) yang memberikan permintaan SYN secara besar-besaran kepada web server.

Untuk memperkuat keamanan jaringan web server penerapan Intrusion Detection System (IDS) digunakan untuk mendeteksi serangan, memantau dan menganalisa serangan pada web server. Software IDS yang sering digunakan yaitu IDS Snort dan IDS Suricata yang memiliki kelebihan dan kekurangannya masing-masing.

Tujuan penelitian kali ini untuk membandingkan kedua IDS menggunakan sistem operasi linux dengan pengujian serangan menggunakan SYN Flood yang akan menyerang web server kemudian IDS Snort dan Suricata yang telah terpasang pada web server akan memberikan peringatan jika terjadi serangan. Dalam menentukan hasil perbandingan, digunakan parameter-parameter yang akan menjadi acuan yaitu jumlah serangan yang terdeteksi dan efektivitas deteksi serangan dari kedua IDS tersebut.

Kata kunci: *Keamanan jaringan, Web Server, IDS, SYN Flood, Snort, Suricata.*

ABSTRACT

Network security on the web server is the most important part to guarantee the integrity and service for users. Web servers are often the target of attacks that result in data damage. One of them is the SYN Flood attack which is a type of Denial of Service (DOS) attack that gives a massive SYN request to the web server.

To strengthen web server network security, the application of Intrusion Detection System (IDS) is used to detect attacks, monitor and analyze attacks on web servers. IDS software that is often used is IDS Snort and IDS Suricata which have their respective advantages and disadvantages.

The purpose of this study is to compare the two IDS using the Linux operating system with testing the attack using SYN Flood which will attack the web server then IDS Snort and Suricata that have been installed on the web server will give a warning if an attack occurs. In determining the results of the comparison, the parameters used will be the reference, namely the number of attacks detected and the effectiveness of attack detection from the two IDS.

Keywords: *Network Security, Web Server, IDS, SYN Flood, Snort, Suricata.*

I. PENDAHULUAN

A. Latar Belakang Masalah

Saat ini website merupakan salah satu layanan informasi yang banyak diakses oleh pengguna internet di dunia. Sebagai salah satu layanan informasi maka perlu dibangun Website yang mampu menangani permintaan (request) dari banyak pengguna dengan baik (reliable). Web server berisi web pages, yang di dalamnya mengandung informasi, dokumen yang ingin disebarluaskan atau diperlukan oleh para Pengguna. Netcraft web server survey mejelaskan bahwa pada bulan agustus 2019 ini salah satu web server yang sering banyak digunakan yaitu web server Apache. Web Server seringkali menjadi target dari berbagai jenis serangan baik yang sifatnya minor maupun major sehingga berakibat fatal. Hal ini dapat terjadi karena aspek keamanan web server kurang diperhatikan atau tidak diterapkan secara optimal, sehingga memungkinkan terjadinya resiko yang cukup signifikan. [1]

Mualfah, Desti (2017) serangan yang paling banyak didapati pada web server adalah serangan Denial of Service. DOS adalah jenis

serangan terhadap sebuah komputer atau server di dalam jaringan internet dengan cara menghabiskan resource yang dimiliki oleh server tersebut, sampai server tersebut tidak dapat menjalankan fungsinya dengan benar sehingga secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan dari komputer atau server yang diserang tersebut. Salah satu jenis serangan DOS yaitu serangan SYN flood. Penyerang akan membanjiri server dengan paket syn sehingga server akan secara terus menerus mengirimkan kembali paket syn-ack. Efek dari metode ini adalah server tidak dapat melayani request yang lain dan resource dari server tersebut akan terus menerus meningkat.[2]

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. [3] 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. Akan tetapi sebuah aplikasi IDS tersebut pastilah memiliki kelebihan dan kekurangannya, dengan adanya kelebihan dan kekurangan dari masing-masing IDS tersebut, penulis tertarik melakukan penelitian untuk menganalisa dan membandingkan kinerja dari beberapa IDS tersebut yaitu *Snort* dan *Suricata* yang merupakan *software* berlisensi *Open Sources* yang banyak digunakan sehingga menjadi pilihan peneliti untuk membandingkan dengan beberapa parameter yaitu jumlah serangan yang terdeteksi dan efektivitas dari kedua IDS tersebut dalam menangani serangan *SYN Flood* terhadap *web server* Apache.

Kriteria yang digunakan untuk membandingkan kedua IDS ini yaitu jumlah serangan yang mampu terdeteksi, efektivitas serangan, dan peggunaan *resources* yang digunakan untuk mengelola serangan. Yang menjadi acuan dalam menganalisa *software* IDS mana yang lebih baik yaitu dari jumlah serangan terdeteksi yang paling banyak, efektivitas serangan, serta penggunaan resources terkecil. Maka penulis perlu menganalisis perbandingan kinerja *snort* dan *suricata* sebagai *IDS* dalam mendeteksi serangan *SYN flood* pada *web server* apache dengan tujuan untuk mengetahui IDS mana yang lebih unggul yang nantinya diharapkan mampu menjadi bahan pertimbangan untuk penerapan keamanan pada jaringan yang lebih komplek.

B. Maksud dan Tujuan Penelitian

Maksud dan tujuan dari analisis perbandingan kinerja *snort* dan *suricata* sebagai *IDS* dalam mendeteksi serangan *SYN flood* pada *web server* apache yang ingin dicapai dalam penelitian ini antara lain:

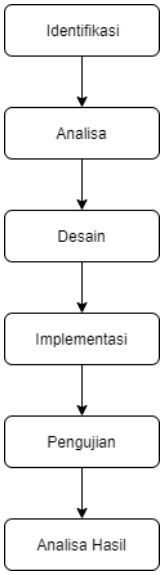
1. Menganalisa perbandingan kinerja IDS Snort dan *Suricata* untuk mendeteksi serangan *SYN Flood* pada *web server* Apache.
2. Mengetahui kinerja dari kedua IDS yaitu Snort dan *Suricata* dalam mendeteksi serangan *SYN Flood* pada *web server* Apache sehingga dapat diambil kesimpulan mana IDS yang terbaik.

II. METODOLOGI PENELITIAN

Keamanan jaringan pada web server memiliki macam-macam level pengamanan sesuai dengan ancaman yang dikirim oleh attacker dalam menggunakan serangan terhadap sistem jaringan. Setiap serangan tehadap jaringan memerlukan penanganan sistem keamanan yang berbeda, alat dan metode pengamanan serta penanggulangan yang berbeda, juga hasil yang berbeda.

Penelitian ini difokuskan pada proses analisa sistem keamanan jaringan yang terjadi pada web server menggunakan serangan SYN Flood dengan membandingkan kinerja dari Snort dan Suricata sebagai Intusion Detection System. Dalam penelitian ini metode yang digunakan yaitu metode SPDLC (*Security Policy Development Life Cycle*) karena metode ini tepat digunakan dalam menyajikan tahapan development system yang berhubungan dengan keamanan jaringan sesuai dengan penelitian yang diangkat.

SPDLC merupakan metode yang menetapkan strategi untuk melakukan pembaruan suatu organisasi dari sistem jaringan, siklus pengembangan sistem jaringan didefinisikan pada sejumlah fase. Menurut Luay A. Wahsheh and Jim Alves Foss (2008:1120), pengembangan sistem SPDLC yang diambil melakukan penelitian dengan 6 tahap diantaranya, identifikasi, analisis, desain, implementasi, pengujian/audit, analisa hasil/evaluasi.



Gambar 1. Metode SPDLC

Menurut Goldman dan Rawles 2004, SPDLC digambarkan sebagai suatu tahapan yang dimulai dari tahap evalulasi yang menvalidasi efektivitas dari tahap analisa awal. Umpan balik dari evaluasi ini bisa berdampak pada perubahan dalam arsitektur dan teknologi yang digunakan saat ini.

Adapun penjelasan tahap-tahap pada gambar 1 sebagai berikut :

1. Identifikasi : Pada tahap ini dilakukan proses identifikasi masalah yang dijadikan dasar dari jurnal-jurnal, dan buku untuk menunjang penelitian.
2. Analisis : Pada tahap ini penulis melakukan analisis berdasarkan masalah yang telah diuraikan pada identifikasi masalah, seperti menentukan perangkat lunak yang akan digunakan, menentukan topologi yang berkaitan dengan masalah.
3. Desain/Perancangan : Pada tahap ini penulis membuat rancangan seperti alur pendeteksian serangan, merancang topologi yang akan digunakan.
4. Implementasi : Penulis melakukan implementasi berdasarkan scenario yang telah dibuat, dengan menginstall dan mengkonfigurasi semua perangkat lunak yang digunakan dan siap untuk di uji coba.
5. Pengujian : Pada tahap ini dilakukan pengujian terhadap kedua IDS yaitu Snort dan Suricata sesuai dengan parameter yang telah dientukan dan dilakukan perbandingan dari kedua IDS tersebut.
6. Analisa Hasil : Tahap terakhir yaitu memaparkan hasil yang diperoleh dari pengujian kedua IDS tersebut dengan analisa sesuai dengan parameter yang dibuat sehingga didapati kesimpulan dari pengujian kedua IDS tersebut.

Kebutuhan fungsional adalah kebutuhan yang berisi proses – proses yang nantinya dilakukan oleh sistem. Kebutuhan fungsional juga berisi informasi-informasi apa saja yang harus ada dan dihasilkan oleh sistem. Adapun beberapa kebutuhan fungsional sistem IDS pada web serveryang akan dibangun adalah sebagai berikut :

1. Sistem *web server* dan sistem *attacker* berjalan pada sebuah network dengan fasilitas *Virtual Enviroment.*
2. Sistem *web server* menjalankan fungsi minimal berupa database service, dan page authentication login.
3. Sistem *web server* dapat menjalankan fungsi *Intrusion Detection System* dengan baik.
4. *Attacker* dapat melakukan fungsi *attacking* dengan metode serangan *SYN Flood* ke *web server*.
5. Sistem IDS pada *web server* dapat mencatat aktifitas *input traffic* dari berbagai paket data yang masuk ke *web server* secara minimal berupa IP Address, Port Address, data *filtering analisis, time lapse logging*, dan beberapa fungsi logging lainnya.

Analisis Kebutuhan Non-fungsional dilakukan untuk mendeskripsikan perangkat keras dan perangkat lunak yang diperlukan untuk mewujudkan semua fitur yang diperlukan untuk kebutuhan fungsional, sesuai dengan penabaran Analisa identifikasi masalah sebelummnya.

Perangkat keras yang dibutuhkan dalam penelitian ini dalam menjalankan fungsi IDS pada web serverdapat dilihat pada table I.

TABEL I.
KEBUTUHAN PERANGKAT KERAS

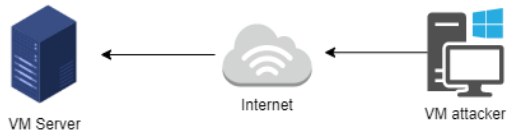
No	Perangkat Keras	Spesifikasi
1	*Processor*	Intel(R) Core(TM) i7 7700HQ
2	Memory	16 GB RAM
3	Penyimpanan	SSD 250GB
4	VGA/Screen	NVIDIA GeForce GTX 1050 – 4GB / 15inch

Perangkat lunak yang dibutuhkan dalam sistem ini meliputi sistem operasi, server, serta perangkat lunak yang digunakan untuk konfigurasi server dan proses aplikasi. Perangkat lunak yang digunakan dalam perancanga ini bisa dilihat dalam table II berikut.

TABEL II.
KEBUTUHAN PERANGKAT LUNAK

NO	Perangkat Lunak	Keterangan
1	Ubuntu versi 18.0	Sistem operasi *web server*
2	Snort versi 2.9.7.0	Software IDS
3	Suricata versi 5.0.0	Software IDS
4	Hping3	Software *attacker SYN Flood*
5	Putty	Perangakat lunak untuk melakukan remoute telnet / SSH *server*
6	VirtualBox versi 6.0	Software virtualisasi
7	Apache v2, mysql, php, wordpress	*Web server*

Tahap perancangan membahas mengenai mekanisme dari alur perancangan dan juga rancangan dari sistem agar dapat beroperasi sesuai kebutuhan yang telah dijelaskan pada tahap perencanaan. Pada penelitian perancangan sisem IDS web server ini dilakukan dengan merancang topologi infrastruktur keamanan jaringan yang akan digunakan sebagai simulasi dan pengujian sistem keamanannya serta merancang skema penerapan pengujian itu sendiri. Perncangan topologi infrastruktur jraingan dilakukan pada virtual mesin yang tetap mampu mempresentasikan web server yang sesungguhnya di Internet.

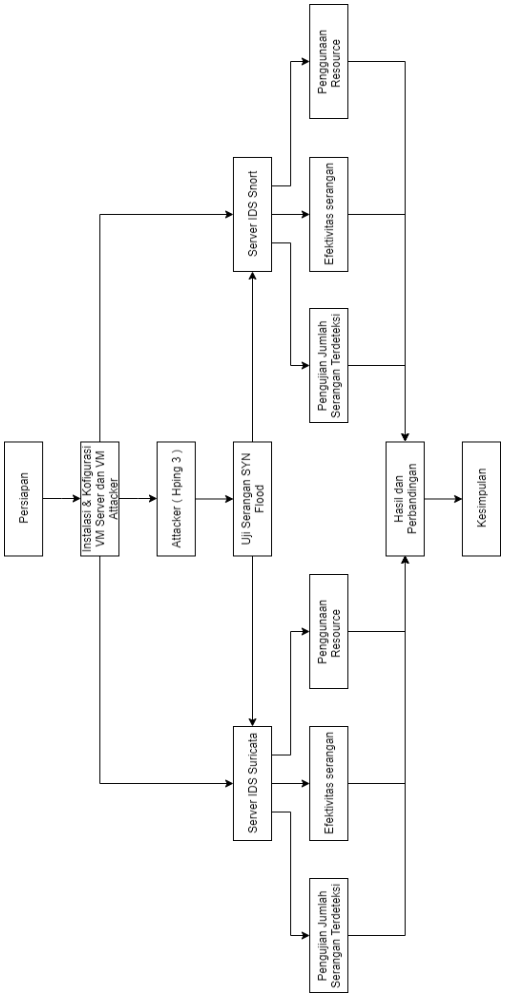


Gambar 2. Topologi Jaringan

Pada gambar 2 menggambarkan topologi yang akan digunakan pada saat proses implementasi. Pada topologi diatas terdapat PC attacker dan PC server yang terhubung dalam jaringan internet local. PC server akan berjalan pada software VirtualBox dan menggunakan sistem operasi Linux Ubuntu. Lalu akan dilakukan instalasi software web server Apache2, Snort dan Suricata pada PC server, PC attacker sendiri akan dilakukan instalasi HPing3 sebagai tool dalam melakukan penyerangan. Serangan dilakukan dengan cara membanjiri web server dengan paket syn.

Dalam melakukan analisis dan pengujian, tentunya harus sesuai dengan parameter-parameter yang akan menjadi acuan dalam melakukan sebuah perbandingan nantinya. Parameter yang digunakan yaitu :

1. Jumlah serangan yang terdeteksi, pada pengujian pertama menguji jumlah serangan yang terdeteksi. Pada pengujian ini dilakukan serangan SYN Flood yang menyerang web server, baik web server yang berisi IDS suricata maupun web server yang berisi IDS Snort dengan serangan yang dilakukan dalam waktu 30 detik dalam setiap percobaan serangan. Peneliti melakukan 30 kali percobaan yang sama untuk menghasilkan analisa data yag lebih akurat.
2. Efektivitas deteksi serangan, pada pengujian selanjutnya yaitu dengan membandingkan efektivitas deteksi masing-masing IDS dilihat dari nilai uncaptured paket yang terdiri dari dropped packet,dropped packet adalah paket yang secara sengaja diabaikan oleh IDS.
3. Penggunaan resource, data yang akan dijadikan sampel untuk melakukan perbandingan selanjutnya dalam deteksi masing-masing IDS adalah penggunaan RAM, CPU.



Gambar 3. Skema Pengujian

Langkah – langkah yang akan dilakukan pengujian sistem keamanan pada web server, yaitu sebagai berikut :

1. Melakukan instalasi dan konfigurasi Virtual Machine untuk *Web server* dan untuk *atacker* dalam sebuah jaringan virtual. Pada tahap ini akan dibuat sebuah VM *attacker* dan dua buah VM Server (satu buah VM *web server*untuk IDS *Snort*, dan satu buah VM *web server*untuk IDS *suricata*).
2. Melakukan instalasi dan konfigurasi sistem operasi serta sistem IDS Snort dan Suricata agar aktif dan terhubung dalam jaringan virtual.
3. Melakukan instalasi dan konfigurasi sistem operasi VM *attacker* agar aktif dan terhubung ke jaringan virtual.
4. Melakukan instalasi dan konfigurasi HPing3 pada VM *attacker* sebagai simulator serangan *SYN Flood* ke *web server*.
5. Melakukan uji konektivitas dari VM *attacker* ke *web server* dengan mode normal hingga menghasilkan tampilan web standar sebelum serangan dilakukan.
6. Melakukan uji serangan *SYN Flood* dari VM *attacker* menggunakan HPing3 ke *web server* yang berisikan IDS *snort* sistem menggunakan port 80.
7. Melakukan uji serangan *SYN Flood* dari VM *attacker* menggunakan HPing3 ke *web server* yang berisikan IDS *suricata* menggunakan port 80.
8. Mengambil data system log pada kedua VM *web server* dan memasukkan data hasil pengujian ke aplikasi data *processor* untuk dianalisa hasil penelitiannya sesuai parameter pengujian yang telah ditetapkan.

III. HASIL DAN PEMBAHASAN

A. Implementasi

Tahap implementasi menurut metode pengembangan sistem berbasis SPDLC, merupakan tahapan lanjutan dari proses analisis dan desain sistem yang telah dirumuskan dan dijabarkan pada bab sebelumnya. Pada tahap implentasi, dilakukan serangkaian aktivitas instalasi, konfigurasi, simulasi percobaan/pengujian, pencatatan hasil percobaan serta proses perhitungan hasil pengujian berdasarkan variable yang diuji. Tahapan tersebut dilakukan secara bertahap dan berurutan agar pengujian sistem mendapatkan hasil penelitian yang benar dan akurat.

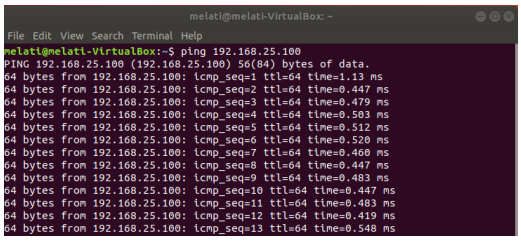
Langkah pertama dalam tahap inplementasi adalah proses instalasi dan konfigurasi perangkat lunak, sistem operasi maupun sistem aplikasi yang digunakan pada pembuatan dan pengujian sistem baik pada web server maupun pada mesin attacker. Urutan tahap instalasi sebagai berikut :

1. Instalasi aplikasi VirtualBox pada OS Windows.
2. Konfigurasi jaringan pada virtualbox.
3. Instalasi OS Ubuntu pada VM *web server* dan *attacker.*
4. Instalasi putty.
5. Installasi dan konfigurasi VM *web server* pada OS ubuntu.
6. Installasi dan konfigurasi *web server* (Apache, dan komponen pendukungnya).
7. Installasi dan konfigurasi IDS Snort.
8. Installasi dan konfigurasi IDS Suricata.
9. Installasi dan konfigurasi Hping3 pada VM attacker.

B. Pengujian

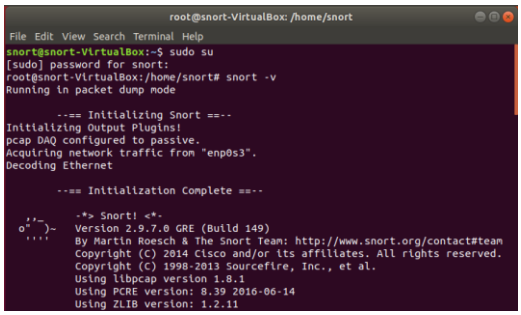
Analisis dan pengujian dilakukan berdasarkan dengan parameter-parmeter yang telah dijabarkan diatas sebagai acuan dalam melakukan sebuah perbandingan.

Pada pengujian IDS Snort, terlebih dahulu dilakukan pengaktifan pada VM attacker dan VM web server IDS Snort. Pada tahapan ini dilakukan pengujian konektivitas antara VM attacker dan VM web server IDS Snort, untuk memastisakan kedua VM tersebut sudah terkoneksi dalam sebuah jaringan. Menguji konektifitas dengan cara membuka command line interfaces dengan menggunakan perintah PING dari VM attacker ke VM web server IDS Snort, seperti pada gambar 4.



Gambar 4. Ping Attacker ke Web Server

Selanjutnya jika kedua VM tersebut sudah saling terkoneksi dengan baik, maka dilakukan pengaktifan service IDS Snort untuk memastikan IDS Snort berjalan dengan baik. Untuk mengaktifkan service IDS Snort yaitu dengan perintah : #snort -v



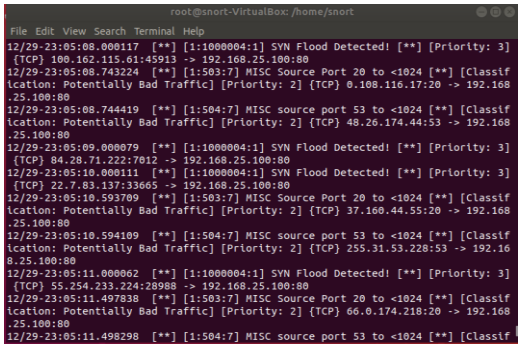
Gambar 5. Pengaktifan service Snort

Pada tahap ini dilakukan konfigurasi pada VM attacker yang berisi tool Hping3 sebagai alat serangan SYN flood. Untuk melakukan serangan SYN Flood dilakukan perintah berikut:

```
#hping3 -S -p 80 -flood -rand-source 192.168.25.100
```

Tahapan ini merupakan tahapan yang utama dalam penelitian. Dimana tahapan ini dilakukan untuk menguji sistem IDS snort yang diserang oleh serangan SYN flood, melalui tool Hping3 yang mengirimkan paket ack sehingga IDS Snort mendeteksi paket yang terfilter maupun tidak terfilter.

Selanjutnya dilakukan penyerangan pada web server yang berisi IDS snort. Di sisi lain VM web server Snort akan diaktifkan dengan perintah : snort -A console Pada saat Snort dijalankan dan VM attacker melakukan serangan SYN flood, Snort berhasil mendeteksi serangan tersebut.



Gambar 6. Deteksi Serangan oleh Snort

Sama seperti pada pengujian IDS Snort, IDS Suricata juga terlebih dahulu dilakukan pengaktifan pada VM attacker dan VM web server IDS suricata.

Sama seperti pada pengujain IDS sebelumnya yaitu dilakukan pengujian konektivitas antara VM attacker dan VM web server IDS suricata, untuk memastisakan kedua VM tersebut sudah terkoneksi dalam sebuah jaringan. Menguji konektifitas dengan cara membuka command line interfaces dengan menggunakan perintah PING dari VM attacker ke VM web server IDS Suricata.

Tahap selanjutnya yaitu memastikan service IDS Suricata telah berjalan dengan baik dan siap untuk menerima paket data yang akan dianalisis. Untuk memastikan IDS Suricata berjalan normal masukkan perintah

```
#suricata -c /etc/Suricata/Suricata.yaml -l enp0s3
```

Pada tahap ini dilakukan konfigurasi pada VM attacker yang berisi tool Hping3 sebagai alat serangan SYN flood. Untuk melakukan serangan SYN Flood dilakukan perintah seperti berikut :

```
#hping3 -S -p 80 -flood -rand-source 192.168.25.100
```

Tahapan ini dilakukan untuk menguji sistem IDS suricata yang diserang oleh serangan SYN flood, melalui tool Hping3 yang mengirimkan

paket ack sehingga IDS suricata mendeteksi paket yang terfilter maupun tidak terfilter.

Selanjutnya dilakukan penyerangan pada web server yang berisi IDS suricata. Di sisi lain VM web server suricata akan diaktifkan dengan perintah : "#tail -f /var/log/suricata/fast.log"

Pada saat IDS suricata dijalankan dan VM attacker melakukan serangan SYN flood, suricata berhasil mendeteksi serangan tersebut, seperti gambar dibawah ini.

Gambar 7. Deteksi Serangan oleh Suricata

C. Analisa Hasil

Hasil pengujian yang didapatkan dari data serangan yang dilakukan dalam waktu 30 detik dalam setiap percobaan serangan dengan melakukan sampling sebnayak 30 kali percobaan yang sama untuk menghasilkan analisis yang lebih akurat. Peneliti mengambil beberapa variable data primer serangan yang digunakan sebagai basis analisis kedua IDS, yaitu :

1. Jumlah serangan yang terdeteksi server IDS selama 30 detik setiap kali serangan, dengan melakukan 30 kali percobaan serangan yang sama.
2. Data CPU sebelum proses pengujian berlangsung oleh masing-masing IDS.
3. Data yang diperoleh dalam penggunaan CPU selama proses pengujian berlangsung oleh masing-masing IDS.
4. Data RAM sebelum proses pengujian berlangsung oleh masing-masing IDS.
5. Data yang diperoleh dalam penggunaan RAM selama proses pengujian berlangsung oleh masing-masing IDS.

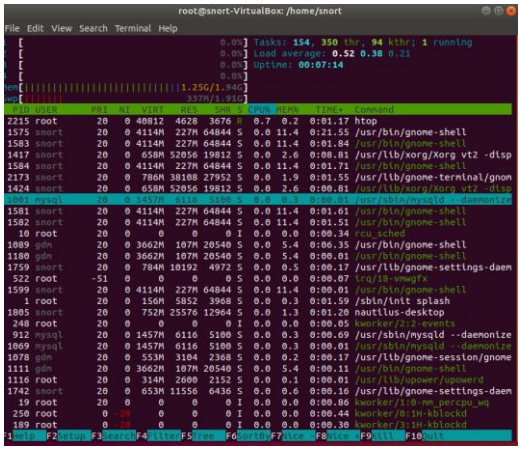
Data dari jumlah serangan dan banyak serangan yang terdeteksi dapat dilihat pada tabel III.

Data aktifitas pengguaan resource RAM dan CPU IDS Snort sebelum dilakukan penyerangan menunjukan nilai yang normal, aktifitas RAM dan CPU sebelum dilakukan penyerangan terlihat pada Gambar 8.

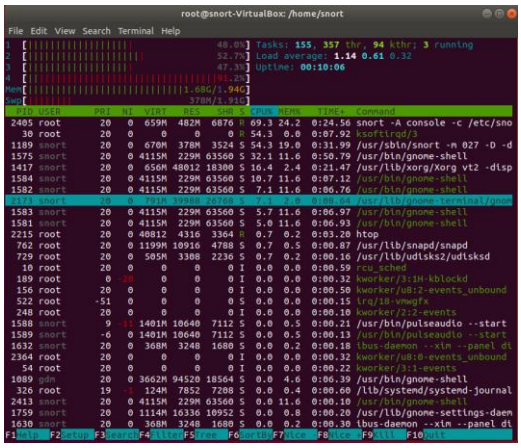
Berikut merupakan data yang diperoleh dalam penggunaan resource CPU dan RAM setelah dilakukan penyerangan, menunjukan peningkatan aktivitas baik RAM maupun CPU dapat dilihat pada Gambar 9.

TABEL III.
JUMLAH SERANGAN TERDETEKSI

Uji	Jumlah Serangan (30 Detik)		Jumlah Serangan terdeteksi	
	Snort	Suricata	Snort	Suricata
1	760631	698740	272720	625607
2	480501	748284	305731	622087
3	351771	660886	296200	653077
4	591710	1633871	301993	1060140
5	420819	939444	314783	732168
6	383972	672834	324857	624288
7	759820	682763	712408	632355
8	441725	689651	417465	643147
9	772901	892637	691329	729645
10	750191	696813	684793	637303
11	692269	863196	675973	793019
12	337813	779120	300039	692107
13	313088	1423340	277439	839569
14	344750	941259	315620	705666
15	535813	797648	497947	655309
16	363212	808682	332717	675526
17	703546	2005225	646879	1224257
18	351979	1215624	317419	786554
19	366176	849728	313886	658095
20	438094	1162047	342899	707987
21	362071	1084527	296954	693389
22	339069	1609608	294218	694089
23	534813	1137530	487372	687133
24	667860	775662	586135	675142
25	611337	1504325	558291	701185
26	813525	1039844	711810	677917
27	619695	978901	570595	678845
28	560730	874603	479034	677586
29	749494	1036708	710214	636270
30	729513	1410077	656515	755941

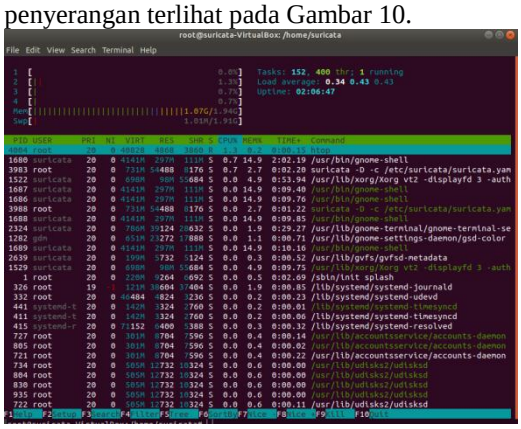


Gambar 8. CPU RAM Snort Sebelum Serangan



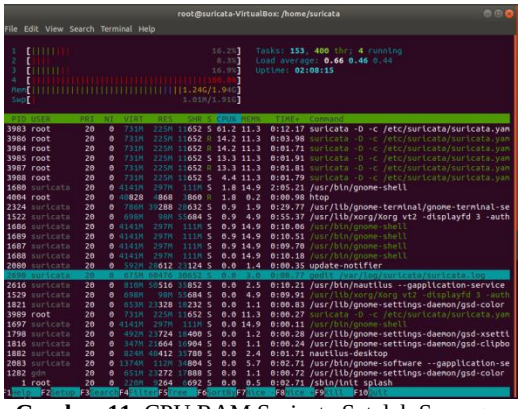
Gambar 9. CPU RAM Snort Setelah Serangan

Data aktifitas pengguaan resource RAM dan CPU IDS Surcicata sebelum dilakukan penyerangan menunjukan nilai yang normal, aktifitas RAM dan CPU sebelum dilakukan penyerangan terlihat pada Gambar 10.



Gambar 10. CPU RAM Suricata Sebelum Serangan

Berikut merupakan data yang diperoleh dalam penggunaan resource CPU dan RAM setelah dilakukan penyerangan, menunjukan peningkatan aktivitas baik RAM maupun CPU dapat dilihat pada Gambar 11.



Gambar 11. CPU RAM Suricata Setelah Serangan

Dari hasil olah data penelitian yang dilakukan, maka diperoleh hasil sebagai berikut.

TABEL IV.
REKAPITULASI PERFORMA IDS

Uji	Jumlah Serangan (30 Detik)		Jumlah Serangan terdeteksi	
	Snort	Suricata	Snort	Suricata
min	313088	698740	272720	625607
max	813525	748284	305731	622087
average	538296,26	660886	296200	653077
total	16148888	1633871	301993	1060140

TABEL V.
REKAPITULASI HASIL PENGUJIAN CPU

Uji	CPU Usage					
	Start Test		Finish Test		Penggunaan	
	Snort	Suricata	Snort	Suricata	Snort	Suricata
min	1,3	0,6	50,9	51,4	48,9	47,5
max	2,6	3,9	91,6	99,8	89,8	98,5
average	1,67	1,34	79,98	81,43	78,31	80,08
total	50,1	40,4	2399,5	2442,9	2349,4	2402,5

TABEL VI.
REKAPITULASI HASIL PENGUJIAN RAM

Uji	RAM Usage					
	Start Test		Finish Test		Penggunaan	
	Snort	Suricata	Snort	Suricata	Snort	Suricata
min	0,2	0,1	19,6	7,3	19,4	7,2
max	1,9	1,9	29,1	14,3	28,9	13,8
average	0,25	1,22	24,14	12,59	23,89	11,36
total	7,7	36,8	724,4	377,8	716,7	341

TABEL VII.
REKAPITULASI EFEKTIFITAS SERANGAN

Uji	Jumlah Serangan Terdeteksi		Dropped Paket	
	Snort	Suricata	Snort	Suricata
min	272720	622087	142509	10471
max	712408	1224257	608502	102661
average	456474,5	719180,1	327632,77	25648,2
total	13694235	21575403	9828983	769446

Dari data pengujian pada tiap-tiap tabel tersebut, akan diambil standar deviasi, untuk menentukan performa dari masing-masing IDS.

Serangan yang paling banyak didapati pada web server adalah serangan Denial of Service, salah satu jenis DOS adalah SYN Flood .

Sebelum serangan Penggunaan resource CPU dan RAM berjalan dengan normal sesuai kebutuhan. Setelah serangan Penggunaan resource CPU dan RAM meningkat, memakan resource cukup besar menyebabkan server agak lambat.

Berikut hasil perhitungan rasio performa sistem IDS Snort dan Suricata terhadap serangan yang dilakukan, sebagai berikut.

1. IDS Snort memiliki rata-rata performa yang lebih besar (84,97%) dibandingkan IDS Suricata (74,62%) dalam mendeteksi serangan
2. Standar deviasi jumlah serangan ke IDS Snort 168.944,926.
3. Standar deviasi jumlah serangan ke IDS Suricata 342.033,537.
4. Standar deviasi jumlah serangan terdeteksi oleh IDS Snort 167.248,4366.
5. Standar deviasi jumlah serangan terdeteksi oleh IDS Suricata 128.160,397.

Selanjutnya untuk hasil perhitungan rasio penggunaan resource IDS Snort dan Suricata sebagai berikut.

1. Hasil pengujian IDS Snort memiliki rasio penggunaan CPU sebanyak 78,31% sedangkan IDS Suricata sebanyak 80,08%.
2. Hasil pengujian IDS Snort memiliki rasio penggunaan RAM sebanyak 23,89% sedangkan IDS Suricata sebanyak 11,36%.
3. Hasil rasio performa *uncaptured* paket untuk IDS Snort sebesar 68,2% sedangkan untuk IDS Suricata sebesar 3.42%.

IV. KESIMPULAN

Dari hasil analisis perbandingan kinerja Snort dan Suricata sebagai intrusion detection system dalam mendeteksi serangan SYN flood pada web server Apache, penulis menyimpulkan bahwa :

1. Berdasarkan pengujian menggunakan parameter jumlah serangan terdeteksi, IDS Snort lebih banyak melakukan pendeteksian serangan dibandingkan dengan IDS Suricata setelah melakukan 30 kali pengujian. Hal ini dapat dibuktikan dari data yang telah didapat yaitu IDS Snort dapat mendeteksi serangan dengan rata-rata performa sebanyak 84,97% dan memiliki standar deviasi 167248,43 dibandingkan IDS Suricata sebanyak 74,62% dan memiliki standar deviasi 128160,39 dari 30 kali pengujian.
2. Berdasarkan pengujian menggunakan parameter penggunaan resource CPU Snort lebih baik dibandingkan IDS Suricata setelah melakukan pengujian sebanyak 30 kali, data yang diperoleh dari rata-rata rasio penggunaan CPU sebanyak 78,31% dibandingkan IDS Suricata yang memperoleh rata-rata penggunaan CPU sebanyak 80,08%. Namun dalam penggunan RAM, IDS Suricata lebih unggul dengan rata-rata rasio penggunaan RAM sebanyak 11,36% dibandingkan Snort dengan rata-rata rasio penggunaan RAM sebanyak 23,89%
3. Berdasarkan pengujian dengan menggunakan parameter efektifitas serangan yang diperoleh dari uncaptured paket, IDS Suricata lebih baik dibandingkan IDS Snort setelah melakukan pengujian sebanyak 30kali, data yang diperoleh dari rasio efektifitas IDS Snort memiliki rasio uncaptured paket sebanyak 68,2% sedangkan Suricata sebanyak 3,42%.
4. Dari segi fitur Snort lebih unggul karena dapat menampilkan infromasi data serangan dan data outstanding paket secara langsung, sedangkan Suricata harus membuka file log terlebih dahulu untuk melihat informasi data serangan dan Suricata tidak memiliki informasi data outstanding paket.
5. Maka hasil pengujian dapat disimpulkan bahwa IDS Snort lebih unggul dalam pendeteksian serangan, penggunaan resource CPU, dan fitur informasi data serangan, sedangkan Suricata lebih unggul dalam efektivitas serangan dari data uncaptured paket dan penggunaan RAM.

REFERENSI

[1] A. Chendramata, J. M. Sunarto and I. Rahayu, "Panduan Keamanan Web Server", Jakarta: Direktorat Keamanan Informasi, 2011.

[2] Riyo and d. , "Implementasi dan Analisis Keamanan Jaringan Virtual HIPS Snort pada Layanan Web Server dengan Penyerangan DOS dan DDOS," Telkom University, vol. 5, 2018.

[3] H. P. Sukarno and M. A. Nugroho, "Analisis Perbandingan Quality of Service (QoS) Penerapan Snort IDS dan Bro IDS Dalam Arsitektur Software Define Network (SDN)," Telkom University, vol. 5, p. 7522, 2018.

[4] J. Prakoso, "Perbandingan Performansi Snort dan Suricata Sebagai Sistem Deteksi Intrusi," Universitas Gajah Mada, vol. 10, p. 297653, 2018.

[5] L. N. Hakim, "Analisis Perbandingan Snort dan Suricata," Universitas Muhamadiyah Suricata, 2015.

[6] H. S. P. and N. , "Analisis Perbandingan Quality of Service (QoS) Penerapan Snort IDS dan Bro IDS Dalam Arsitektur Software Define Network (SDN)," Telkom University, vol. 5, p. 7522, 2018.

[7] F. R. Joutulis, "Analisis Perbandingan Intrusion Detection System pada Web Server Menggunakan Suricata dan Ossec," Universitas AMIKOM Yogyakarta, 2018.

[8] Cisco, "*Modern Network Security Threats*," in CCNA Security, 2018.

[9] R. Fahrudin, "Membangun Firewall dengan IPTables di Linux", Jakarta: PT Elex Media Komputindi, 2005.

[10] M. R. Arief, "Penggunaan Sistem IDS (Intrution detection System) Untuk Pengaman Jaringan dan Komputer," Universitas AMIKOM Yogyakarta, 2007.

[11] D. Wahyudi, "Deteksi Serangan Denial of Service Menggunakan Rule Based Signature Analysis pada Jaringan Internet of Things," Universitas Sriwijaya, p. 9947, 2019.

[12] A. Nuryanto, "Analisis dan Implementasi Suricata, Snorby, Banyard pada VPS Ubuntu," Universitas Muhmmadiyah Surakarta, 2015.

[13] Ryanda, "Simulasi dan Analisis Keamanan Jaringan Virtual Data Center dengan Memanfaatkan S Flow dan Open Flow untuk Mendeteksi dan Memitigasi SYN Flood," SIFO Microskill, vol. 117, 2016.

[14] S. Arjuni, "Perancangan dan Implementasi Proxy Server dan Manajemen Bandwidth Menggunakan Linux Ubuntu Server," Telkom University, vol. 8, 2012.

[15] Y. A. Prabowo, "Penggunaan NMAP dan Hping3 dalam menganalisa keamanan jaringan pada Penggunaan NMAP Dan HPING 3 Dalam Menganalisa Keamanan Jaringan Pada B2P2TO2T (Karanganyar, Tawangmangu)," Universitas Muhammadiyah Surakarta, vol. 31267, 2014.

[16] G. R. Kaciak, "Mengenal Aplikasi Virtualisasi Oracle VM VirtualBox," Dosen Gufron, 2013.