SIMULASI *INTRUSION DETECTION SYSTEM* (IDS) DALAM KEAMANAN WEB SERVER PADA JARINGAN

Irma Malini Amir[1] , Yessi Mardiana, S.Kom., M.Kom[2]
Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Dehasen Bengkulu[1,2,3]
malinichaniago129@gmail.com[1], yessimrd@gmail.com[3]*

ABSTRACT

This study aims to design a computer network security system by implementing the Snort Intrusion Detection System (IDS). Built network security system. Integration between Snort Intrusion Detection System (IDS), Database System, and Monitoring System. In the test scheme, the system consists of two types, namely server and client. The server functions as an attack target and is also used to monitor the network. While the client functions as an intruder (intruder). The test method is to do Port Scanning so that you can get open ports 22, 80, 10000 and ping normally and ping by including data packets of 10000 and 65000. From the test results that have been done, Snort-IDS is able to detect packets that pass through network. From the results of the detection data, it will be sent to WhatsApp, then forwarded to the Snort GUI and stored in a log, making it easier to read the data. Linux Ubuntu Server When running the Snort Intrusion Detection System (IDS) it works well and requires a small source, namely a small CPU of 10% and a small memory of 50%.

Keywords: Snort, GUI Snort, Linux Ubuntu Information :

ABSTRAK

Penelitian ini bertujuan untuk merancang sebuah sistem keamanan jaringan komputer dengan menerapkan *Snort Intrusion Detection System* (IDS). Sistem keamanan jaringan yang dibangun. Integrasi *antara Snort Intrusion Detection System* (IDS), Database System, dan *Monitoring System*. Dalam skema pengujian, sistem terdiri dari dua jenis, yaitu server dan client. Server berfungsi sebagai target serangan dan sekaligus digunakan untuk melakukan pemantauan terhadap jaringan. Sedangkan client berfungsi sebagai intruder (penyusup). Metode pengujian adalah adalah melakukan Port Scanning sehingga di dapat port yang terbuka 22, 80, 10000 dan ping secara nornal serta ping dengan menyertakan paket data sebesar 10000 dan 65000. Dari hasil pengujian yang telah dilakukan, Snort-IDS mampu mendeteksi paket-paket yang melewati jaringan. Dari hasil data deteksi tersebut akan dikirim ke whastapp kemudian diteruskan ke GUI Snort dan di simpan pada log sehingga memudahkan untuk mebaca data tersebut. Linux Ubuntu Server Dalam menjalan *Snort Intrusion Detection System* (IDS) berjalan dengan baik dan membutuhkan source yang kecil yaitu CPU sebesar Kecil dari 10% and memory kecil dari 50%.

Kata Kunci: **Snort, GUI Snort, Linux Ubuntu**

1. Pendahuluan

Pertumbuhan internet dan jaringan komputer yang terjadi pada zaman sekarang ini memberikan keuntungan dan kemudahan kepada pengguna komputer untuk dapat berbagi sumber daya dan informasi antara beberapa komputer yang saling terhubung dalam suatu jaringan yang sifatnya lokal maupun internasional.

Sistem pengawasan dan pengamanan data harus mampu mencegah dan menghentikan potensi penyusupan dari orang yang tidak memiliki otoritas dalam jaringan tersebut. Ada banyak cara yang dapat dilakukan untuk mengatasi masalah keamanan jaringan dan gangguan sistem, Salah satunya yang digunakan adalah IDS *(intrusion detection system)*. Sistem pendeteksi intrusi atau IDS (*Intrusion Detection System*) merupakan salah satu metode untuk melindungi jaringan komputer dengan cara mendeteksi serangan-serangan yang ada dan memberitahukannya kepada administrator sistem jaringan komputer untuk segera mengantisipasi serangan tersebut. Fungsi utama IDS adalah untuk mendeteksi aktivitas yang

mencurigakan dalam sebuah sistem atau jaringan secara *realtime*/berkala terhadap kegiatan-kegiatan yang mencurigakan didalam sebuah sistem jaringan.

Keamanan web, sangat erat kaitannya dengan jaringan karena untuk mengakses sebuah *website* pasti dibutuhkan koneksi jaringan. Masalah keamanan merupakan salah satu aspek penting dari sebuah sistem informasi, namun masalah keamanan ini seringkali kurang diperhatikan oleh para pemilik dan pengelola sistem informasi sehingga memungkinkan terjadinya resiko yang cukup signifikan. Sebagai contoh, dalam suatu persaingan bisnis dalam dunia maya, dapat memungkinkan terjadinya suatu penyerangan terhadap *web server* yang kemudian akan menimbulkan kerugian bagi pemilik dimana *website* yang diserang menjadi *down* atau tidak dapat diakses oleh *client* sehingga dapat memberikan kontribusi bagi para pesaing bisnis lainnya.

Dibalik kemudahan pengaksesan informasi yang disediakan oleh internet terdapat bahaya besar yang mengintai, yaitu berbagai macam serangan yang berusaha mencari celah dari sistem keamanan jaringan komputer yang digunakan. Serangan – serangan itu dapat mengakibatkan kerusakan data dan bahkan kerusakan pada *hardware*. Karena itulah sistem keamanan terhadap jaringan komputer juga harus semakin ditingkatkan.

Masalah tersebut telah menuntut suatu instansi maupun perusahaan untuk melindungi integritas dan kerahasiaan informasi mereka, dikarenakan tidak semua informasi data bersifat terbuka untuk umum dan tidak semua orang dapat mengaksesnya. Suatu jaringan komputer memerlukan suatu sistem pengawasan dan pengamanan data untuk menjaga agar informasi penting yang ada dalam jaringan tersebut tetap aman.

2. Tinjauan Pustaka

A. Simulasi

Menurut Ahdan, dkk. (2018:29) Simulasi merupakan alat yang berguna untuk menganalisis sistem yang rumit dimana kita tidak dapat menggunakan metode standar dalam riset operasional, selain itu simulasi dapat diartikan sebagai meniru suatu sistem nyata yang kompleks dengan penuh sifat probabilistik, tanpa harus mengalami keadaan yang sesungguhnya.

Menurut Munifatussangadah dan Sutisna (2021:69) Simulasi adalah proses merancang model dari suatu sistem dan kemudian menjalankannya untuk mendeskripsikan, menjelaskan, dan memprediksi karakteristik dinamis sistem tersebut. Simulasi sebagai metode yang digunakan untuk menyelesaikan berbagai persoalan sebenarnya cukup lama diperkenalkan. Namun baru dirasakan kehadirannya seiring dengan perkembangan dunia komputer yang semakin berkembang saat ini. Tidak jarang banyak persoalan-persoalan rumit di industri dapat diselesaikan lebih cepat dan lebih mudah dengan menggunakan simulasi.

Dari beberapa pendapat di atas, dapat disimpulkan bahwa pengertian simulasi adalah suatu kegiatan merancang atau mendeskripsikan dengan menggunakan situasi tiruan untuk memahami tentang konsep, prinsip, atau keterampilan tertentu.

B. Intrusion *Detection System*(IDS)

Menurut Wijaya dan Pratama (2020:98) IDS merupakan suatu sistem yang memiliki kemampuan untuk menganalisis data secara realtime dalam mendeteksi, mencatat (log) dan menghentikan penyalahgunaan dan penyerangan. IDS merupakan security tools yang dapat digunakan untuk menghadapi aktivitas hacker. IDS ini mampu memberikan peringatan kepada administrator apabila terjadi suatu serangan atau penyalahgunaan di dalam jaringan, bahkan peringatan itu dapat pula menunjukkan alamat IP dari sebuah sistem penyerang.

Menurut Sutarti, dkk. (2018:2) *Intrusion Detection System* (IDS) adalah sebuah sistem yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan. Jika ditemukan kegiatan-kegiatan yang mencurigakan berhubungan dengan traffic jaringan, maka IDS akan memberikan peringatan kepada sistem atau administrator jaringan. Pada umumnya IDS terbentuk menjadi dua, yaitu:

1. NIDS (*Network - based Intrusion Detection System*)Menurut Purba dan Efendi (2020:145) NIDS (*Network - based Intrusion Detection System*) merupakan sebuah perangkat lunak yang bekerja secara otomatis untuk memantau suatu paket data yang masuk ke dalam sistem jaringan. Semua paket data yang berjalan pada sistem jaringan, akan dianalisis untuk melihat apakah ada percobaan serangan atau penyusupan ke dalam sistem jaringan. Jika ada kecocokan dengan *rules* yang telah dibuat, maka hasilnya akan dicatat dalam sebuah file.
2. HIDS (*Host Intrusion Detection System*)
   Menurut Purba dan Efendi (2020:146) HIDS (*Host Intrusion Detection System*) merupakan jenis IDS yang bekerja pada *host* yang individual atau perangkat tertentu pada sistem jaringan komputer secara *real-time*. HIDS akan memantau paket-paket data ketika sedang terjadi penyusupan saja.

Dalam melakukan tugasnya IDS (*intrusion detection system*) berada pada lapisan jaringan OSI (*Open System Interconnection*) model yang terdapat pada lapisan ketiga yaitu pada lapisan *network* dan sensor jaringan pasif yang secara khusus diposisikan pada *choke point* pada jaringan metode dari lapisan OSI.

Dari pengertian yang telah dikemukakan oleh beberapa para ahli diatas, maka penulis dapat menyimpulkan bahwa *Intrusion Detection System* (IDS) adalah sebuah metode yang dapat digunakan untuk mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan.

C. Web Server

Menurut Roihan (2018:91) Web Server adalah layanan server yang berfungsi menerima permintaan HTTP atau HTTPS dari klien dengan menggunakan web browser dan mengirimkan kembali hasilnya dalam bentuk halaman-halaman web yang umumnya berbentuk dokumen HTML dan format dokumen web lainnya.

Menurut Ramadhani (2017 : 309) Web server adalah perangkat lunak (*software*) dalam server yang memberikan layanan berbasis data dan berfungsi untuk menerima permintaan (*request*) berupa halaman web melalui protokol HTTP dan atau HTTPS dari klien yang lebih dikenal dengan nama *browser,* kemudian mengirimkan kembali (*respon*) hasil permintaan tersebut kedalam bentuk halaman web yang pada umumnya berbentuk dokumen HTML.

Berdasarkan pengertian diatas dapat disimpulkan bahwa Web Server adalah sebuah *Software* (perangkat lunak) yang memberikan layanan berupa data. Berfungsi untuk menerima permintaan HTTP atau HTTPS dari klien atau kita kenal dengan web browser (*Chrom, Firefox*).

Gambar 2.1 Web Server

Web Server berungsi menerima permintaan HTTP atau HTTPS dariklien atau kitakenal dengan web browser (*Chrom, Firefox*). Ia juga akan mengirimkan respon atas permintaan kepada *client* dalam bentuk halaman web yang umumnya HTML.
Jenis-jenis dari web server adalah sebagai berikut

1. Web Server Apache

Web server yang populer dan paling banyak digunakan kebanyakan orang, yaitu jenis Apache. Pada awalnya Apache didesain guna mendukung penuh sistem operasi UNIX. Selain cukup mudah dalam implementasinya, Apache juga memiliki beberapa program pendukung sehingga memberikan layanan yang lengkap, seperti PHP, SSI dan control akses. Berikut detailnya:

a. PHP (*Personal Home Page* atau PHP *Hypertext Processor*)
   Program semacam CGI, berfungsi memproses teks yang bekerja di server. Apache sangat mendukung PHP dengan menempatkannya sebagai salah satu modulnya (*mod php*). Hal tersebut membuat PHP bekerja lebih baik.
b. SSI (*Server Side Include*)
   Perintah yang bisa disertakan dalam bekas HTML. Kemudian ia dapat diproses oleh web server ketika pengguna mengaksesnya.
c. Access Control
   Kontrol Akses dapat dijalankan berdasarkan nama *host* atau nomor IP CGI (*Common Gateway Interface*). Lalu yang paling umum untuk digunakan adalah perl (*Practical Extraction and Report Language*), disupport oleh Apache dengan menempatkannya sebagai modul (*mod perl*).
   Apache sangat aman dan nyaman untuk digunakan karena memiliki beberapa keuntungan seperti proses instalasi yang mudah, freeware, dan sistem konfigurasi yang masih tergolong mudah. Selain itu ia juga mampu bekerja pada sistem operasi *open* atau *closed source*.

2. Web Server Nginx

satu pesaing unggul Apache yaitu Nginx. Nginx dikenal mampu melayani segala macam permintaan, seperti request pada dengan tingkat kepadatan lalu lintas atau *taffic* yang sangat padat. Nginx memang lebih unggul dari segi kualitas, kecepatan dan dalam hal performannya. Nginx memiliki banyak kelebihan dalam hal fitur, diantaranya *URL rewriting, virtual host, file serving, reverse proxying, access control*, dan masih banyak lagi.

a. Web Server IIS

Web Server IIS (*Internet Information Services*) adalah web server yang bekerja pada jenis protokol seperti DNS, TCP/IP, atau beragam *software* lainnya yang berguna untuk merangkai sebuah situs.

b. Web Server Lighttpd

Programmer asal Jerman telah menciptakan web server berbasis *open source*guna mendukung sistem *Linux* dan *Unix*. Bila dilihat dari segi keunggulan, web server yang satu ini memiliki beberapa keunggulan berdasarkan fitur tambahan yang tersedia. Seperti *FastCGI, Output-Compression, FastCGI, dan URL writing*. Jika kamu menggunakan web server Lighttpd, kamu akan merasakan performa yang lebih cepat dan efektif.

D. Jaringan Komputer

Menurut Rahmatulloh dan Firmansyah (2017:242) Jaringan Komputer adalah suatu sistem telekomunikasi yang didalamnya terdiri dari dua atau lebih perangkat komputer yang dirancang untuk dapat berkerja secara bersama-sama dengan tujuan dapat berkomunikasi, mengakses informasi, meminta serta memberikan layanan atau service antara komputer satu dengan yang lainnya.

Menurut Noviansyah dan Saiyar (2021:37) Jaringan komputer merupakan kumpulan dari beberapa komputer dan peralatan penunjang lainnya yang terhubung dalam satu kesatuan dan saling terkoneksi.

Berdasarkan pengertian diatas dapat disimpulkan bahwa jaringan komputer adalah suatu sistem telekomunikasi yang didalamnya terdiri dari dua atau lebih perangkat komputer yang terhubung dalam satu kesatuan dan saling terkoneksi.

Jaringan komputer pada umum nya di kelompokkan menjadi 5 kategori, yaitu berdasarkan jangkauan geografis, media tranmisi data, distribusi sumber informasi/data, peranan dan hubungan tiap komputer dapam memproses data, dan berdasarkan jenis topologi yang digunakan. Jenis jaringan komputer berdasarkan jangkauan geografis yaitu:

1. Local Area Network :
   Local area network atau disingkat LAN merupakan jaringan yang mencakup wilayah kecil. salah satu contoh adalah jaringan komputer yang berada dilingkup sekolah, kampus atau kantor. Biasanya jaringan LAN menggunakan teknologi IEEE 802.3 ethernet dengan kecepatan transfer data sekitar 10 MB/s, 100 MB/p dan 1 GB/s. selain menggunakan teknologi ethernet jaringan LAN bisa menggunakan teknologi nirkabel seperti wi-fi.
2. Area Network :
   Metropolitan area network atau disingkat WAN merupakan sebuah jaringan yang berada di dalam satu kota dengan kecepatan transfer data tinggi yang menghubungkan beberapa tempat tetapi masih dalam satu wilayah kota. jaringan MAN merupakan gabungan dari beberapa jaringan LAN
3. Area Network :
   Wide area network atau disingkat WAN merupakan jaringan yang jangkauannya mencakup daerah geografis yang luas, semisal antar wilayah, daerah, kota, negara bahkan benua.

E. Snort

Menurut Dewi (2017:74) Snort adalah perangkat lunak IDS dan NIDS berbasis opensource dan banyak digunakan untuk untuk mengamankan sebuah jaringan dari aktifitas yang berbahaya. Cara kerja Snort mirip dengan TcpDump, tetapi fokus sebagai security packet sniffing. Fitur utama Snort yang membedakan dengan TcpDump adalah payload inspection, dimana Snort melakukan analisis payload rule set yang disediakan.

Menurut Sutarti, dkk. (2018:2) Snort adalah suatu perangkat lunak untuk mendeteksi penyusup dan mampu menganalisi paket yang melintasi jaringan secara *real time traffic* dan *logging* ke dalam database serta mampu mengidentifikasi berbagai serangan yang berasal dari luar jaringan.

F. Ubuntu Server

Menurut Husen dan Surbakti (2020:21) Ubuntu adalah salah satu distribusi Linux yang berbasis Debian dan didistribusikan menjadi perangkat lunak sistem operasi yang bebas. Secara singkat dan jelasnya yaitu Ubuntu adalah sejenis sistem operasi yang berbasiskan Linux Debian. Adapun versi Ubuntu yang telah dirilis 5 tahun terakhir adalah sebagai berikut :

a. Versi 16.04 LTS (Xenial Xerus).
b. Versi 16.10 (Yakkety Yak).
c. Versi 17.04 (Zesty Zapus).
d. Versi 17.10 (Artful Aardvark).
e. Versi 18.04 LTS (Bionic Beaver).
f. Versi 18.10 (Cosmic Cuttlefish).
g. Versi 19.04 (Disco Dingo).
h. Versi 19.10 (Eoan Ermine)
i. Versi 20.04 LTS (Focal Fossa)
j. Versi 20.10 (Groovy Gorilla)

Menurut Sampurno (2019:2) Linux adalah sistem operasi yang bersifat *open source* dan bebas (*free*) di bawah lisensi GNU (GNU *is not Unix*) GPL (*General Public License*).
Adapun kelebihan Linux yaitu:

1. Bersifat *open source*, bebas dan terbuka. Sehingga tidak perlu biaya untuk mendapatkannya.
2. Linux sekarang sudah mudah untuk dioperasikan.
3. Hampir semua aplikasi yang digunakan di *windows* sudah ada aplikasi linuxnya yang dikembangkan oleh komunitas linux atau bisa juga menggunakan *software emulator*.
4. Memiliki keamanan yang lebih unggul karna didesain *multiuser* sehingga apabila *virus* menyerang *user* tertentu, akan sangat sulit untuk menyebar ke *user* yang lain.
5. Cocok untuk PC yang memiliki *spesifikasi* minimum karna linux membutuhkan *resource* yang lebih kecil dibandingkkan dengan windows.

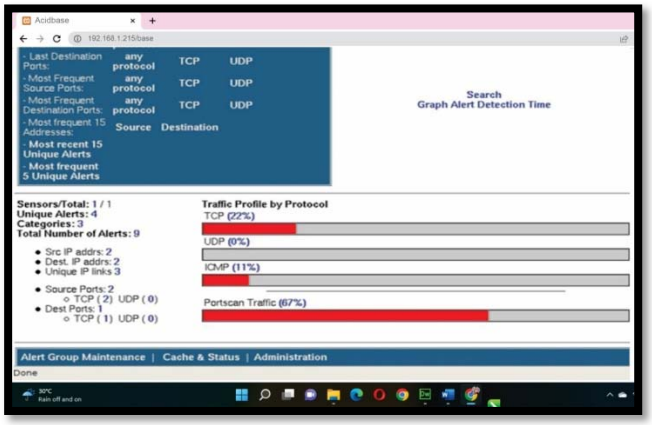
3. Metode Penelitian

Metode penelitian yang di gunakan adalah penelitian tindakan atau *action research*. Penelitian tindakan atau *action research* yaitu mendeskripsikan, menginterpretasi dan menjelaskan suatu situasi atau keadaan pada jaringan dan melakukan analisis terhadap implementasi *Intrusion Detection System*. Pada implementasi *Intrusion Detection System* yaitu dengan menggunakan beberapa komponen *Intrusion Detection System* yang terdiri dari *snort engine, php, apache, dan sql server* dengan menggunakan *software* atau modul tambahan seperti program BASE (*Basic Analysis and Security Engine*) serta sistem operasi linux ubuntu 20.04 server.

4. Hasil dan Pembahasan

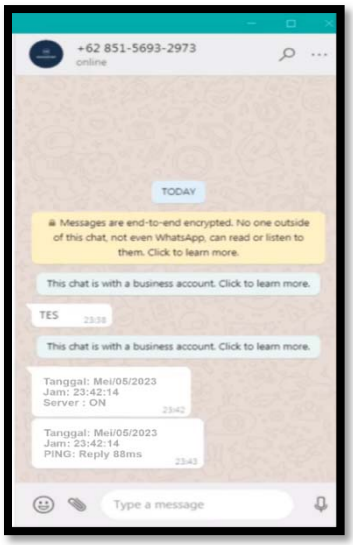
A. Tampilan Informasi Server A

Dari serangkaian pengujian yang dilakukan system keamanan jaringan menggunakan snort berjalan dengan baik, sesuai dengan konfigurasi-konfigurasi yang diterapkan. Adapun IP Server (Engine) Snor : 192.168.1.213, Server Web : 192.168.1.180 dan IP LAN : 192.168.1.0/24 yang berhasil di deteksi akan ditampilkan oleh ACIDBASE dengan engine snort dapat dilihat pada tampilan gambar dibawah ini :



Gambar 4.1 Tampilan Informasi Server A

Dari tampilan gambar diatas dapat dilihat untuk snort dengan webgui acidbase dapat melakukan deteksi dan pengamanan jaringan yaitu adanya deteksi terhadap aktitas yang menggunakan protocol (*traffic profile by protocol*) dengan hasil adanya aktifitas pada protocol TCP sebesar 20%, protocol UDP sebesar 0%, protocol ICMP sebesar 11% dan port scan sebesar 67%. Dimana semua aktivitas bersumber dari 2 buah IP *Address* yang ditampilkan pada *src ip address*. Dimana semua aktitas bersumber dari 2 buah IP *Address* yang ditampilkan pada *src ip address*. Hasil monitoring tersebut di kirim ke Whatsapp, seperti dapat dilihat pada tampilan gambar dibawah ini:



Gambar 4.2 Tampilan Notifikasi

B. Pengujian ICMP

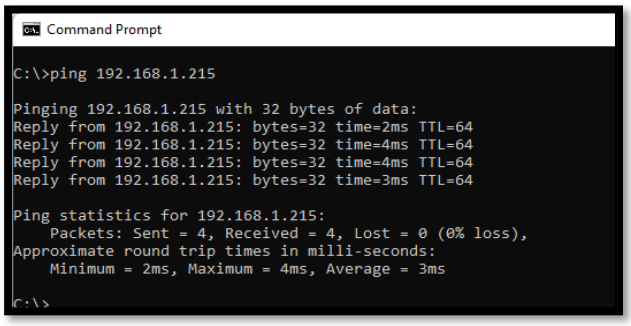
Pengujian dilakukan dengan melakukan perintah ping dari *command prompt*. Adapun *rules* yang di terapkan untuk melakukan deteksi paket ICMP adalah

Gambar 4.3 Tampilan *Rules* Snort

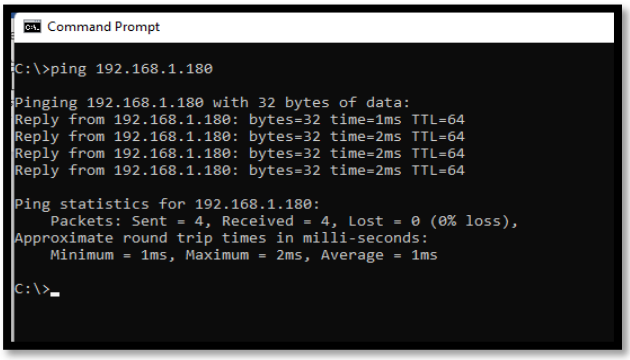
Setelah *rules* diatas diterapkan maka dilakukan pengujian dengan cara melakukan *ping* dari komputer *client* ke *server*, diantaranya:

a. Pengujian dengan PING dengan *buffer size standar*Pengujian dilakukan dengan melakukan perintah *ping* dari *command prompt*. Dengan perintah :
ping 192.168.1.215

Adapun hasil pengujian tersebut dapat dilihat pada tampilan gambar dibawah ini:



Gambar 4.4 Tampilan Ping Standar ke Server Snort



Gambar 4.5 Tampilan Ping Standar ke Server Web

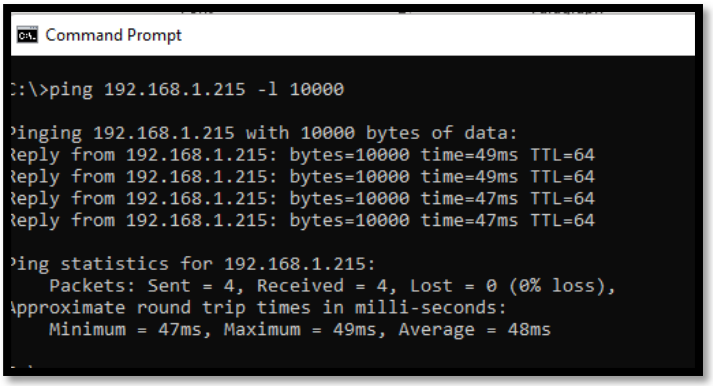
Dari tampilan gambar diatas dapat dijalan ping dengan paket data normal dari klien ke *server snort* berjalan, yang ditandai dengan *ping reply*, time = 2ms. Snort dapat dilihat adanya aktifitas *ping* yang dilakukan dari IP *Address* 192.168.1.4 (*client*) ke 192.168.1.215 (*server* snort) dengan hasil *fragmen* (*Frag*) paket data = 0.

b. Pengujian dengan PING dengan *buffer size* 10000

Pengujian dilakukan dengan melakukan perintah ping dari *command prompt*. Dengan perintah :

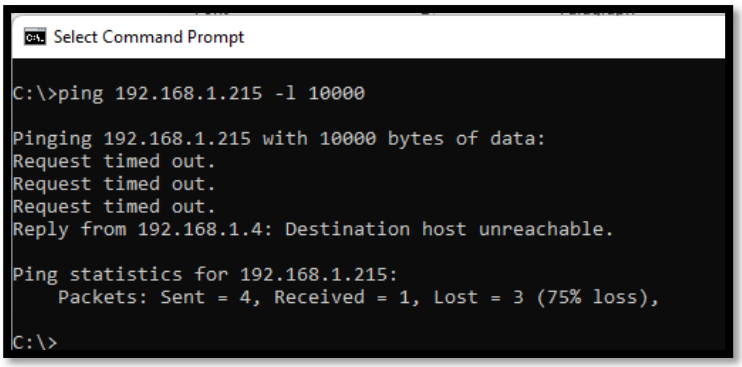
ping 192.168.1.215 -l 10000

Adapun hasil pengujian tersebut dapat dilihat pada tampilan gambar dibawah ini:



Gambar 4.5 Tampilan *Ping Buffer Size* 10000

Dari tampilan gambar diatas dapat dijalan *ping* dengan paket data normal dari *client* ke *server* snort berjalan, yang ditandai dengan *ping reply*, *time* = +/- 50ms. Dan setelah *engine* snort diaktifkankan maka *ping* dengan *buffer size* 10000 tidak berjalan (*time out*), seperti dapat dilihat pada tampilan gambar dibawah ini:



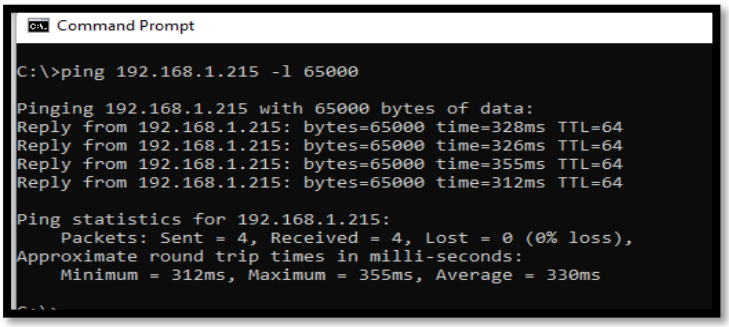
Gambar 4.6 Tampilan *Ping Buffer Size* 10000 ke *Server* Snort *Setelah Engine* Snort Aktif.

Dari tampilan gambar diatas dapat dilihat setelah snort diaktifkan *ping* dengan paket data 10000 tidak berjalan (*time out*). Dari Snort dapat melakukan deteksi terhadap *ping* dengan paket 10000, sehingga *ping* dari *client* tidak berjalan (*time out*). Deteksi snort dapat dilihat adanya aktifitas *ping* yang dilakukan dari IP Address 192.168.1.5 (client) ke 192.168.1.215 (*server* snort) dengan hasil *fragmen* (*Frag*) paket data = 225

c. Pengujian dengan *PING* dengan *buffer size* 65000

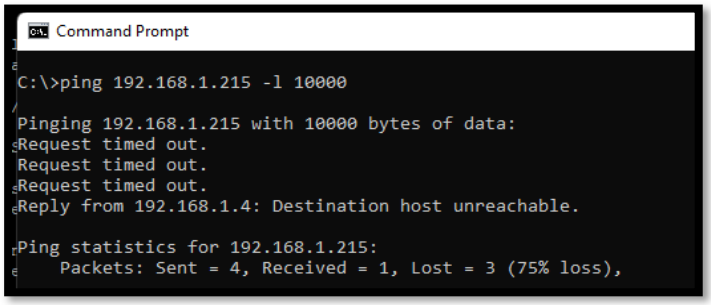
Pengujian dilakukan dengan melakukan perintah ping dari *command prompt*. Dengan perintah : *ping 192.168.1.215 -l 65000*

Adapun hasil pengujian tersebut dapat dilihat pada tampilan gambar dibawah ini:



Gambar 4.7 Tampilan *Ping Buffer Size* 65000 ke *Server* Snort

Dari tampilan gambar diatas dapat dijalan ping dengan paket data normal dari *client* ke *server* snort berjalan, yang ditandai dengan *ping reply*, *time* = +/- 300ms. Dan setelah *engine* snort diaktifkankan maka *ping* dengan *buffer size* 65000 tidak berjalan (*time out*), seperti dapat dilihat pada tampilan gambar dibawah ini:

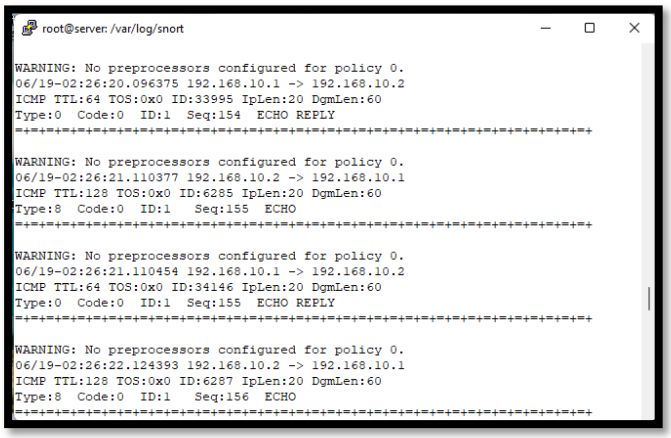


Gambar 4.8 Tampilan *Ping Buffer Size* 65000 ke *Server* Snort Setelah *Engine* Snort Aktif

Dari tampilan gambar diatas dapat dilihat setelah snort diaktifkan ping dengan paket data 65000 tidak berjalan (*time out*). Snort dapat melakukan deteksi terhadap *ping*

dengan paket 65000, sehingga *ping* dari *client* tidak berjalan (*time out*). Deteksi snort dapat dilihat adanya aktifitas *ping* yang dilakukan dari IP *Address* 192.168.1.5 (*client*) ke 192.168.1.215 (*server* snort) dengan hasil *fragmen* (*Frag*) paket data = 2608.

Hasil deteksi snort pada paket ICMP dapat dilihat pada tampilan gambar dibawah ini:

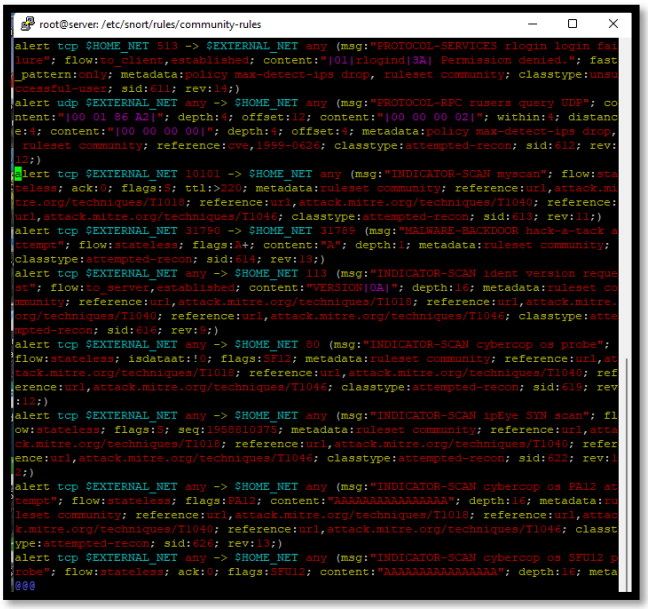


Gambar 4.9 Tampilan Hasil Deteksi Snort

Dari hasil deteksi snort diatas dapat dilihat kotak dengan nomor satu merupakan hasil detekse terhadap paket ICMP normal (dengan besaran data < 500) ditandai dengan ICMP TTL : 64 dan kotak dengan nomor dua merupakan hasil deteksi terhadap paket ICMP tidak normal (dengan besaran data > 500) ditandai dengan ICMP TTL : 128.

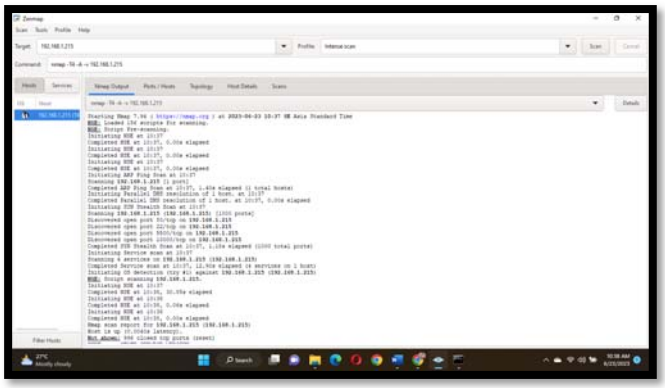
C. Pengujian dilakukan dengan aplikasi NMAP

Rules yang diterapkan pada snort untuk melakukan deteksi terhadap aktifitas port scan dapat dilihat pada tampilan gambar dibawah ini:



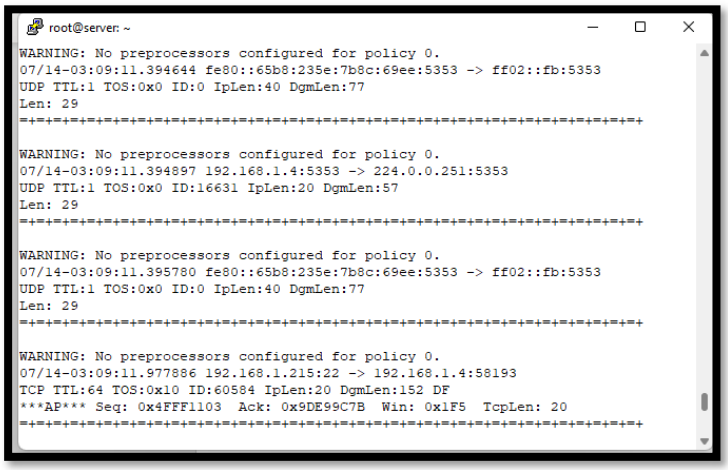
Gambar 4.10 Tampilan Rules Snort

Pengujian dilakuan menggunakan aplikasi NMAP yang bertujuan untuk melihat *port-port* yang terbuka setelah snort dijalankan. Adapun hasil *scan port* menggunakan NMAP dapat dilihat pada tampilan gambar dibawah ini:



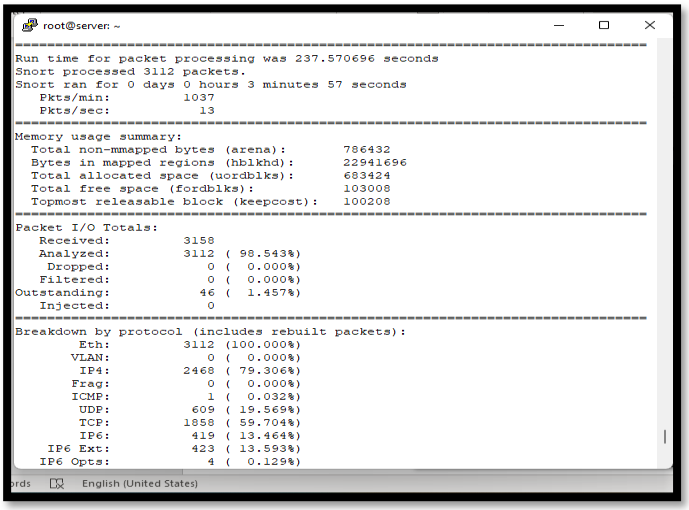
Gambar 4.11 Tampilan Hasil *Scan Port* Dengan NMAP

Dari hasil diatas dari dapat dilihat bahwa *port* yang terbuka ada 4 buah *port*, yaitu port 80, 22, 5500 dan 10000. Dimana *port* 80 berfungsi untuk HTTP, *port* 22 untuk SSH, *port* 5500 untuk GUI Snort dan *port* 10000 untuk webmin. Dan hasil deteksi *server* snort ketika melakukan *scan port* menggunakan NMAP dapat dilihat pada tampilan gambar dibawah ini:



Gambar 4.12 Hasil Deteksi (*Scan Port*)

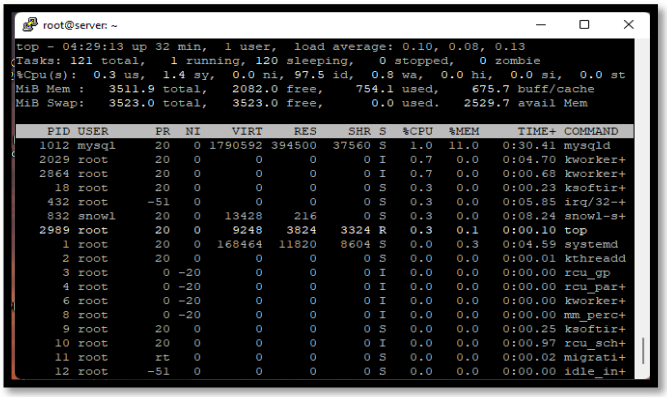
Dari gambar diatas snort dapat melakukan deteksi *scan* yang melalui protokol TCP dan UDP, dari gambar 4.11 diatas dapat dilihat adanya aktifitas scan melalui *protocol* UDP dan TCP dari 192.168.1.4 (laptop yang digunakan melakukan *scanner* dengan nmap) Dari semua pengujian yang dilakukan maka di dapat *log report* snort, seperti dapat dlihat pada tampilan gambar dibawah ini:



Gambar 4.13 Hasil Deteksi (*Scan Port*)

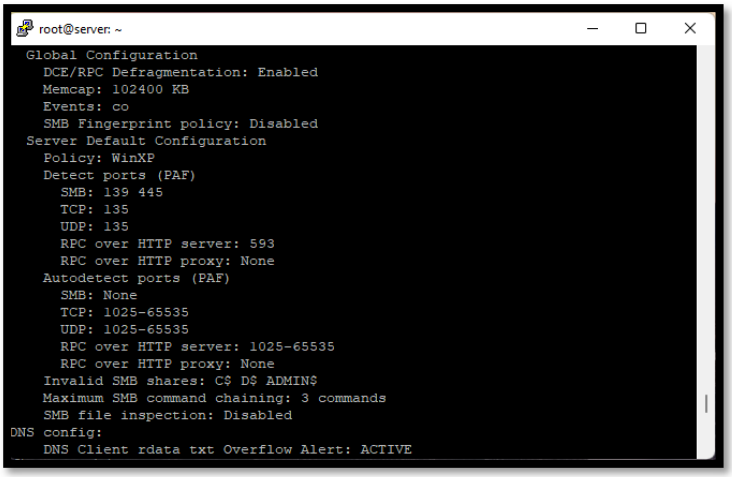
D. Pengujian dengan menggunakan perintah TOP

Pengujian menggunakan perintah TOP pada terminal linux bertujuan untuk melihat sumber daya pada *server*. Adapun hasil pengujian ini dapat dilihat pada tampilan gambar dibawah ini :



Gambar 4.14 Tampilan Pengujian Dengan Perintah TOP

Dari hasil diatas dari dapat dilihat bahwa dalam menjalankan snort tidak menggunakan *resource* yang besar, dari total *memory* sebesar 3511 tersisa 2082 (digunakan sebesar 3511 – 2082 = 1429). Hasil pada server snort dapat dilihat pada tampilan gambar dibawah ini:



Gambar 4.15 Tampilan Deteksi Snort

Dari tampilan gambar diatas dapat dilihat snort dapat melakukan deteksi terhadap aktifitas *port scanner*. Yang ditampilkan dalam bentuk informasi *protocol*, DNS dan *Autodetect Port*.

Dari serangkaian pengujian yang dilakukan pada sistem, maka didapat hasil seperti pada table 4.1 dibawah ini:

No	Jenis Pengujian	Kriteria Pengujian	Hasil Pengujian	Ket
1.	Pengujian ICMP Flooding	Pengujian dengan PING dengan buffer size standar	Terdeteksi sebagai paket ICMP	
		Pengujian dengan PING dengan buffer size 10000	Terdeteksi sebagai paket ICMP Flood	

No	Jenis Pengujian	Kriteria Pengujian	Hasil Pengujian	Ket
		Pengujian dengan PING dengan buffer size 65000	Terdeteksi sebagai paket ICMP Flood	
2.	Pengujian Port Scan	Pengujian dilakukan dengan aplikasi NMAP	Tidak dapat melakukan scan port terblokir oleh Snort	
3.	Pengujian Penggunaan Sumberdaya	Pengujian dilakukan dengan menggunakan perintah TOP pada terminal linux untuk melihat penggunaan sumber daya server IDS. Sumberdaya yang diuji seperti prosesor, memori.	Berjalan sesuai dengan fungsi linux. Penggunaan resource komputer (server) kecil. Penggunaan CPU < 10%, Memori < 25%	

5. Kesimpulan

Kesimpulan yang dapat diambil setelah mengimplementasikan sistem terdistribusi dangan replikasi master to master adalah sebagai berikut :

1. Dengan penerapan sistem pendeteksi dan keamanan jaringan menggunakan snort dapat memantau lalu lintas packet di dalam jaringan serta mampu mendeteksi serangan berdasarkan rules yang diset,
2. Dengan adanya alert pada Snort berdasarkan hasil deteksi yang dilakukan snort maka admin jaringan dapat melakukan pencegahan sedini mungkin terhadap aktifitas yang dapat menganggu jaringan.

REFERENSI

1. Ahdan, dkk., 2018. "*Aplikasi Mobile Simulasi Perhitungan Kredit Pembelian Sepeda Motor Pada Pt Tunas Motor Pratama*", jurnal TEKNOKOMPAK, Vol 12, No 1, Hal 29-33.
2. Kasih. 2017. "*Analisis Log Snort Menggunakan Network Forensic*", Jurnal Ilmiah Penelitian dan Pembelajaran Informatika, Vol 3, No 2, Hal 72-79.
3. Husen, Zakaria., dan Surbakti. 2020. *Membangun Server dan Jaringan Komputer dengan Linux Ubuntu*. Aceh: Syiah Kuala University Press. 155 hal
4. Munifatussangadah, dan Sutisna. 2021. "*Simulasi Traffic Light dengan Arduino Uno*", Jurnal SIBERNETIKA, Vol 6, No 2, Hal 68-75.
5. Noviansyah, Mohammad dan Saiyar, Hafdiasya. 2021. "*Pencegahan Packet Sniffing Menggunakan Metode VPN Tunnel untuk Keamanan Jaringan Komputer Berbasis Mikrotik*", Jurnal AKRAB JUARA, Vol 6, No 4, Hal 36-46.
6. Purba, W Wesley, dan Efendi, Rissal. 2020. "*Perancangan dan Analisis Sistem Keamanan Jaringan Komputer Menggunakan SNORT*", Jurnal Teknologi Informasi, Vol 17, No 2, Hal 143-158.
7. Rahmatulloh, dan Firmansyah, MSN. 2017. "Implementasi Load Balancing Web Server Menggunakan Haproxy dan Sinkronisasi File pada Sistem Informasi Akademik Universitas Siliwangi", Jurnal Nasional Teknologi dan Sistem Informasi, Vol 3, No 2, Hal 241-248.
8. Ramadhani, S. 2017. "Analisis Sistem Keamanan Web Server dan Database Server Menggunakan Suricata". Seminar Nasional Teknologi Informasi, Komunikasi Dan Industri (SNTIKI) 9 Fakultas Sains dan Teknologi, UIN Sultan Syarif Kasim Riau, 308-317 hal.
9. Roihan, A. 2018. *Instalasi & Konfigurasi Aplikasi Server (Sistem Operasi Debian)*. Palembang: AHATEK. 262 hal.

10. Sampurno, dkk., 2019. "*Implementasi Pembuatan Distro Linux Untuk Keperluan Laboratorium Informatika*". Jurnal INFRA, Vol 7, No 1, Hal 1-4.
11. Sutarti, dkk., 2018. "*Implementasi IDS (Intrusion Detection System) pada Sistem Keamanan Jaringan SMAN 1 Cikeusal*", Jurnal PROSISKO, Vol 5, No 1, Hal 2406-7733.
12. Wijaya, Benny dan Pratama, Arie. 2020. "*Deteksi Penyusupan pada Server Menggunakan Metode Intrusion Detection System (IDS) Berbasis Snort*", Jurnal SISFOKOM, Vol 09, No 01, Hal 97-101.