# IMPLEMENTASI METODE INTRUSION DETECTION SYSTEMS (IDS) DAN INTRUSION PREVENTION SYSTEM (IPS) BERBASIS SNORT SERVER UNTUK KEAMANAN JARINGAN LAN

**Ririn Agustin[1], Iskandar Fitri[2], Novi Dian Nathasia[3]**

[1, 2, 3] Informatika, Fakultas Teknologi Komunikasi dan Informatika, Universitas Nasional
Jl. Sawo Manila No 61, Pejaten Pasar Minggu, Jakarta Selatan 12520
Telp 021-7806700 – 7806462
e-mail: agustinririn22@gmail.com, iskandar.fitri@civitas.unas.ac.id, novidian@civitas.unas.ac.id

## *ABSTRACT*

*Currently in the world of network is being focused on computer network system, the dangerous and dangerous things from within the network itself. It requires techniques to secure the resources available in computer networks by using Intrusion Detection Systems (IDS) or intrusion detection systems, using an intruder detection system that enables preventive network and information systems (IPS) or backharming systems that will prevent intruder. In this research applied Intrusion Detection System (IDS) and Intrusion Prevention Systems (IPS) as detection and prevention system when intruders on computer network server, using Snort as rule based as alert to do security on computer network. Intrusion Detection Systems (IDS) implemented on Linux operating systems and Intrusion Prevention Systems (IPS) will be implemented with firewalls or iptables. From this research, Intrusion Detection System (IDS) system testing and response time analysis with 3 models of TCP flood attack, UDP Flood, and ICMP Flood. Results issued by the IDS system with 1 client and 2 clients simultaneously perform an attack that produces the same alert accuracy value with an average value of 99.98%. The average value of response time obtained from credit with 1 client is 0.53 seconds and when using 2 clients get an average value of 0.32 seconds. So in conclusion when an intruder detection system (IDS) is shared with 1 client or 2 client performs an attack, the system is able to detect well and produce the same performance in detecting attacks from 1 or more clients. And the results of the intruder deterrent testing system (IPS) is able to block Internet Protocol (IP) by filtering the attacker IP well.*

***Keywords*** **-** Computer Network Security, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Snort, IP Tables.

## ABSTRAK

Saat ini dalam dunia jaringan sedang fokus pada sistem keamanan jaringan komputer, hal ini disebabkan tingginya ancaman yang mencurigakan dan serangan dari dalam jaringan itu sendiri atau serangan dari jaringan internet. Maka dibutuhkan teknik untuk mengamankan sumber daya yang ada dalam jaringan komputer yaitu menggunakan metode *Intrusion Detection Systems (IDS)* atau sistem deteksi penyusup, dengan adanya sistem deteksi penyusup maka aktivitas jaringan yang mencurigakan dapat segera diketahui dan *Intrusion Prevention Systems (IPS)* atau sistem pencengah penyusup yang akan mencegah adanya

penyusup. Pada penelitian ini menerapkan *Intrusion Detection Systems (IDS)* dan *Intrusion Prevention Systems (IPS)* sebagai sistem deteksi dan pencegah adanya penyusup pada *server* jaringan komputer, dengan menggunakan *Snort* sebagai *rule based* sebagai *alert* untuk melakukan pengamanan pada jaringan komputer. *Intrusion Detection Systems (IDS)* diimplementasikan pada sistem operasi berbasis *Linux* dan *Intrusion Prevention Systems (IPS)* akan diimplementasikan dengan *firewall* atau *iptables*. Dari penelitian ini dilakukan pengujian sistem *Intrusion Detection System (IDS)* dan analisa *response time* dengan 3 model serangan *TCP flood, UDP Flood*, dan *ICMP Flood*. Hasil pengujian sistem *IDS* dengan 1 *client* dan 2 *client* secara bersamaan melakukan serangan menghasilkan nilai akurasi *alert* yang sama yaitu dengan nilai rata-rata 99.98%. Nilai rata-rata *response time* yang diperoleh dari pengujian dengan 1 *client* yaitu 0.53 *second* dan saat menggunakan 2 *client* mendapatkan nilai rata-rata 0.32 *second.* Jadi kesimpulannya saat sistem deteksi penyusup *(IDS)* diuji dengan 1 *client* atau 2 *client* melakukan serangan , sistem mampu mendeteksi serangan dengan baik dan menghasilkan akurasi kinerja yang sama dalam mendeteksi serangan dari 1 *client* atau lebih. Dan hasil pengujian sistem pencegah penyusup *(IPS)* mampu melakukan *blocking Internet Protocol (IP)* dengan mem-*filtered IP* penyerang dengan baik.

***Kata kunci—***Keamanan Jaringan Komputer, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Snort, IP Tables.

## I. PENDAHULUAN

Seiring berkembangnya teknologi dan kemudahan pengguna dalam mengakses internet untuk segala kepentingan. Dengan kemudahan ini tentu menimbulkan bahaya besar akan rentan ancaman dalam menggunakan jaringan internet. Banyak ancaman dan serangan yang terjadi berasal dari jaringan itu sendiri bahkan dari jaringan internet. Hal ini terjadi karena adanya sumber daya, layanan dan lainnya yang bersifat publik sehingga dibutuhkan sistem khusus untuk menjaga sumber daya serta layanan yang ada pada jaringan komputer. Salah satu metode untuk keamanan sumber daya serta layanan yang ada pada jaringan komputer ialah *Intrusion Detection* dan *Prevention Systems (IDPS). Intrusion Detection Systems (IDS)* ini ialah sistem deteksi penyusup, dengan *IDS* aktivitas jaringan yang mencurigakan dapat segera diketahui, sedangkan *Intrusion Prevention Systems (IPS)* ialah sistem pencegah penyusup, *IPS* bekerja sebagai pencegah penyusup yang akan melakukan serangan dengan *Snort* [5]. *Snort* merupakan tools yang digunakan pada *Intrusion Prevention Systems (IPS)* yang berfungsi sebagai *alert* untuk mengamankan jaringan komputer.

Pada sistem jaringan komputer sering terjadi masalah meningkatnya aktivitas dan trafik jaringan yang sangat cepat tanpa diketahui dan terdeteksi dengan jelas apa penyebabnya. Maka dibutuhkan sistem yang dapat melindungi dan memberi

keamanan pada setiap trafik data yang ada pada jaringan komputer. Ada beberapa *tools* yang dapat digunakan untuk sistem monitoring jaringan yang berdampak serangan pada komputer salah satunya ialah *Snort* berbasis *IDS*. Akan tetapi pengkonfigurasikan dan perancangan jurnal sebelumnya *Snort IDS* hanya digunakan untuk memantau dan mendeteksi serangan atau penyusup yang ada pada jaringan, dengan *network forensic* sebagai metode untuk memberikan *report* adanya serangan [1]. Pada penelitian ini menggunakan metode *IDS Snort dan IDS Suricata* untuk mengetahui hasil perbandingan dari pengukuran akurasi, kecepatan deteksi dan konsumsi sumber daya dengan hasil *Snort IDS* lebih unggul dalam kecepatan efektivitas dan akurasi deteksi sebesar 99% pada trafik normal [3]. Dilakukan impelementasi Snort IPS pada sekolah SMK Kristen 1 Salatiga kemudian dilakukan analisa kursioner atau responden dengan hasil 48% yang berarti cukup setuju bahwa layanan yang dibangun dapat membantu pengamatan trafik jaringan [4]. Penelitian kelima penerapan metode *IDPS* dilakukan dengan hasil mampu menahan serangan terhadap 4 port *(ICMP, FTP, SSH,* dan *TELNET)*[5]. Implementasi *Intrusion Detection Systems (IDS)* dan *Intrusion Prevention Systems (IPS)* dengan metode *rule based* untuk meningkatkan keamanan sumber daya jaringan komputer yang ada pada KPDE Provinsi Jambi dengan hasil kinerja sistem melakukan pencegahan mencapai 96% [6]. *Snort* menghasilkan *alert* yang dapat mendeteksi adanya serangan seperti *Ping Of Death* dan *Port Scan* dengan penggunaan *Pfsense* sebagai penindak lanjut dari *alert* yang akan melakukan *blocking* adanya penyalahgunaan jaringan[7]. Pada jaringan LAN dilakukan penerapan *IDS* sebagai pendekteksi sesuai dengan *rule*, kemudian *IPS* dengan *firewall* yang akan melakukan *blocking* terhadap serangan yang ada namun tidak dilakukan analisa kinerja mencapai berapa persenkah sistem dalam melakukan pencegahan serangan[8]. Penerapan *Snort IDS* dengan dilakukan pengujian penyerang melakukan *DoS* dengan mengirim paket *ICMP* saja dan hasil *blocking* belum terlihat hasil yang maksimal[9]. Dari penelitian sebelumnya perlu dikembangkan sistem *Intrusion Prevention Systems (IPS)* yang baik agar dapat memaksimalkan kinerja *blocking* terhadap serangan.

Penulis membatasi permasalahan yang akan dibahas dalam penelitian ini hanya pada konfigurasi metode *IDS* dengan *Snort* dan metode *IPS* dengan *IPTables* atau *Firewall, Snort server* diimplementasikan pada sistem operasi *Linux Ubuntu* dan *BASE snort* sebagai *web* monitoring

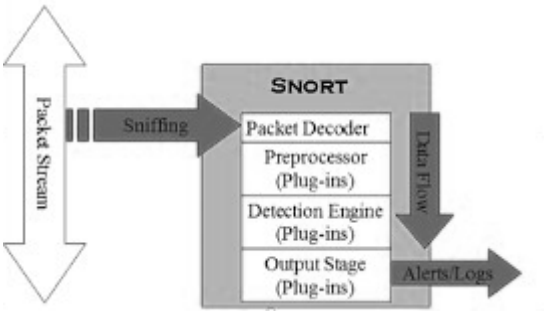
serangan. Pengujian dilakukan oleh komputer *Client 1* dan *2* dengan melakukan serangan bervariasi seperti *flooding* dengan protokol *TCP, ICMP, dan UDP* terhadap *server.* Kemudian analisa *response time* hasil pengujian deteksi serangan. pengujian *block Internet Protocol (IP)* atau pencegahan penyusup secara manual menggunakan *iptables.*

Tujuan yang ingin dicapai dari penelitian ini ialah terwujudnya jaringan komputer pada jaringan LAN yang baik dan memiliki sistem keamanan jaringan yang dapat mendeteksi dan melakukan pencegahan terhadap serangan atau penyusup yang ada. Kemudian mengetahui akurasi *snort server* dalam memberikan *alert* serangan yang terdeteksi oleh sistem *IDS* berbasis *Snort Rule* dan sistem *Intrusion Prevention System (IPS)* dengan *iptables* sebagai *firewall* dapat melakukan *blocking IP* penyerang sehingga *client* penyerang tidak dapat melakukan penyerangan.

## II. METODELOGI PENELITIAN

### *A. Sistem Deteksi Penyusup (IDS) Snort*

Flowchart ini menjelaskan prinsip kerja dari *Snort. Snort* sebagai *Network Intrusion Detection Systems (NIDS)* yaitu jaringan sistem deteksi penyusup yang berskala ringan.

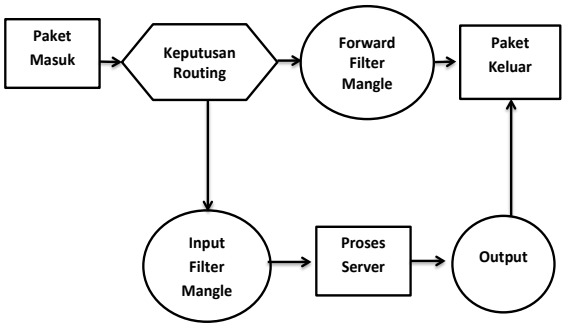



**Gambar 1. Fungsi komponen dalam *Snort***

*Snort* ialah perangkat lunak yang berfungsi mengamati aktivitas dalam suatu jaringan, yang bersifat *opensoure* dan gratis. Pada gambar 1 menjelaskan Snort merupakan paket *sniffing* dengan memanfaatkan *tcpdump* untuk mengambil gambar paket data, kemudian oleh *libcap* akan dipisahkan untuk diteruskan ke proses *Packet Decoder*, *Paket Decoder* akan memisahkan paket dari protokol IP, jenis paket yang digunakan. Kemudian *preprocessor* akan menganalisa atau seleksi paket apakah paket yang ada itu utuh atau tidak. Pada *Detection Engine* sebagai pusat deteksi paket akan disesuaikan dengan *rule signature* jika sesuai maka akan sampai pada *Output Stage* yang akan disimpan pada database *MySql* hasilnya berupa *report* atau *alert*.

### *B. Prinsip Kerja IP Tables*

*IP Tables* ialah sebuah *firewall* untuk *tools* keamanan yang ada pada *Linux*.

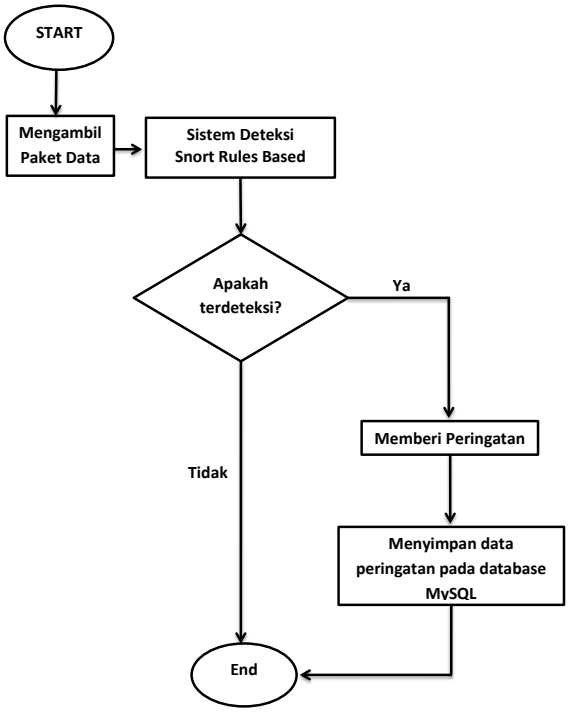



**Gambar 2. Sistem kerja *IP Tables***

Sistem kerja *IP Tables* ialah melakukan filter terhadap *traffic* lalulintas data dan tindakan dengan aturan yang diterapkan apakah paket akan di *drop*, *log*, *accept* atau *reject*. Pada *IP Tables* akan dibuat aturan (rule) untuk arus lalulintas data pada jaringan kedalam maupun keluar komputer. Pada gambar 2 menjelaskan konsep dari *IP Tables* dalam menerima paket dimulai dari paket masuk → diproses berdasarkan tujuan : jika merupakan tujuan *IP* untuk *firewall* maka akan masuk proses input, jika bukan tujuan *IP* untuk *firewall* akan diteruskan ke proses *forward*. Kemudian selanjutnya dicocokkan berdasarkan tabel *policy* yang dipunyai *firewall* apakah di terima atau ditolak.

*C. Flowchart Intrusion Detection System (IDS)*

*Intrusion Detection System (IDS)* ialah perangkat yang dapat mendeteksi aktivitas yang mencurigakan pada sebuah jaringan komputer secara *realtime*.



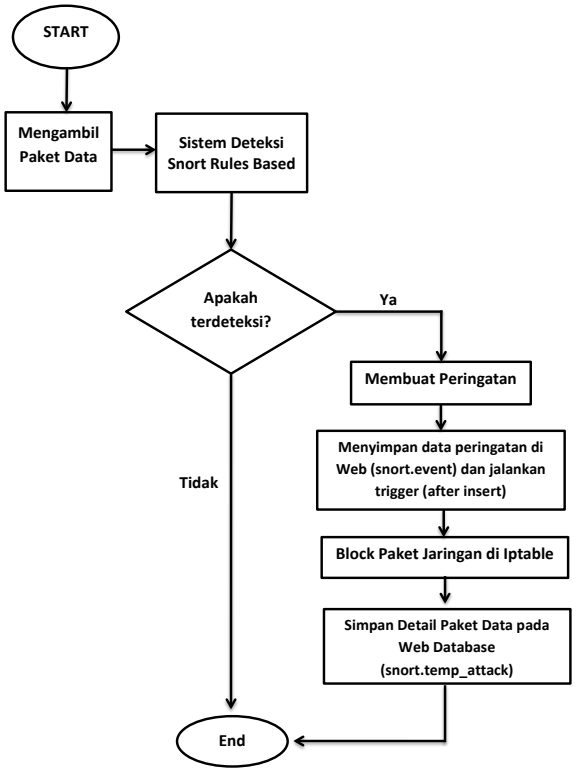

**Gambar 3. Prinsip kerja *Intrusion Detection Ssytem (IDS)***

Pada gambar 3 menjelaskan alur kerja dari *Instrusion Detection Systems (IDS)* dalam mendeteksi adanya aktivitas yang mencurigakan atau adanya penyusup. Dengan mengambil paket data yang ada pada jaringan komputer kemudian akan dilakukan deteksi dengan *Snort Rules Based*, jika terdeteksi maka akan memberi peringatan dan menyimpan data pada *database MySQL*. Jika tidak terdeteksi adanya aktivitas mencurigakan maka proses selesai.

*D. Prinsip kerja Intrusion Prevention Ssytem (IPS)*

*Intrusion Prevention System (IPS)* ialah perangkat pengamanan yang baik yang

dapat mendeteksi adanya aktivitas yang mencurigakan dan mencegah aktivitas tersebut.

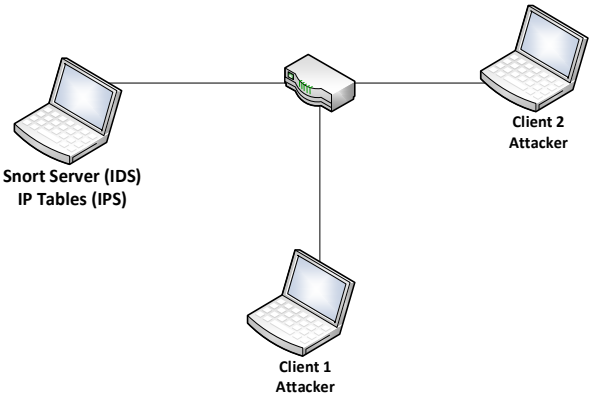



**Gambar 4. Alur metode *Intrusion Prevention System* (*IPS)***

Pada gambar 4 menjelaskan kerja dari *Instrusion Prevention Systems (IPS)* dalam mendeteksi aktivitas yang mencurigakan dan mencegah aktivitas tersebut. Dengan mengambil paket data yang ada pada jaringan komputer kemudian akan dilakukan deteksi dengan *Snort Rules Based*, jika terdeteksi maka akan membuat peringatan dan menyimpan data pada *web* aplikasi. *IPS* akan melakukan *blocking* paket yang lewat dengan cara memberikan *rule* pada *IP Tables* atau *firewall*.

*E. Topologi* perancangan sistem keamanan jaringan dengan *IDPS* berbasis *Snort Server*.

Topologi ini dibuat sebagai gambaran dari perancangan sistem keamanan *IDS* dengan *Snort* dan *IPS* dengan *IP Tables* yang dibangun pada *Virtual Machine VirtualBox.*




**Gambar 5. Topologi perancangan sistem keamanan dengan *Snort IPS* dan *IDS IPTables* pada *Server*.**

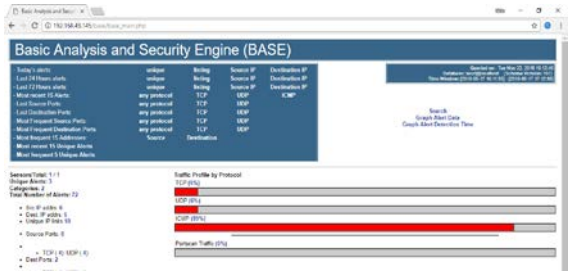
Topologi pada gambar 5 menjelaskan rancangan sistem keamanan jaringan yang akan dibangun dengan implementasi *Snort* dan *IPTables* dengan *IDPS* pada *PC server* pada jaringan *Local Area Network (LAN).* Kemudian *Client* 1 sebagai penyerang yang akan melakukan serangan bervariasi seperti *flooding* yaitu dengan membanjiri IP dengan berbagai protokol seperti *TCP, ICMP,* dan *UDP*. Dan untuk *Client* 2, bertindak sebagai *client* biasa.

*G. Hardware dan Software yang digunakan*

Pada implementasi ini penulis melakukan pengujian dengan perangkat keras dan perangkat lunak dengan spesifikasi *hardware :* Laptop ASUS X441U, Processor : Intel ® Core i3, CPU : 6006U @2.0GHz, RAM : 8.00 GB, VGA : Intel ® HD Graphics 520, *software* : Oracle VM VirtualBox 5.2.8, Linux Ubuntu Dekstop 16.04 LTS untuk OS Server Snort, Linux Ubuntu 14.04 32bit untuk OS Client1 dan Client 2, Windows 10 sistem operasi pada laptop, dan *Whireshark* v2.4.4 sebagai *network analyzer* untuk analisa kinerja jaringan yang dibangun.

## III. HASIL DAN PEMBAHASAN

Pengujian dilakukan dengan menguji fungsi dari sistem deteksi serangan *(IDS)* yang telah dibangun.




**Gambar 6. Tampilan *web BASE Snort***

Pada *web BASE Snort* ini akan digunakan untuk menganalisa adanya alert serangan dari client terhadap server. Pada gambar 6 terlihat adanya total awal 72 alert, *72 alert* yang terdapat dalam *web BASE Snort* disebabkan sudah dilakukan percobaan testing serangan atau penyusup oleh client penyerang untuk mengetahui bahwa secara fungsional sistem pendeteksi penyusup sudah mampu mendeteksi serangan dengan memberikan alert dengan total *72 alert*.

### *A. Pengujian Sistem Deteksi Serangan (IDS) pada Snort Server dengan 1 Client.*

Pengujian dilakukan oleh *client 1* saja yang bertindak sebagai penyerang. *Client* 1 melakukan serangan terhadap *server* dengan *variasi* serangan yaitu *flooding* atau membanjiri *IP atau Port* dengan menggunakan 3 Port/Protokol.yaitu 22/TCP flood, 68/UDP flood dan ICMP flood.

Tabel 1 menjelaskan rancangan pengujian sistem *IDS*. Pada pengujian ini dilakukan pada tanggal 22/05/2018 mulai pukul 08:47:27 WIB sampai dengan pukul 12:28:07 WIB.

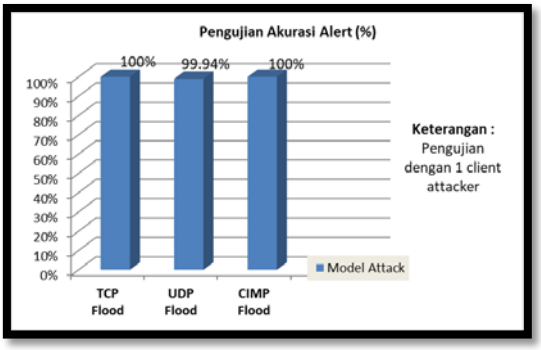
**Tabel 1. Tabel pengujian *Sistem Intrusion Detection System (IDS) Snort.***

| Model Serangan | Jmlh Client Penyerang | Paket dikirim | Jmlh Serangan/paket | Jumlah Alert | Hasil Akurasi |
|---|---|---|---|---|---|
| TCP flood | 1 | 1000 | 1 | 1000 | 100% |
| UDP flood | | 2500 | 2 | 4997 | 99,94 % |
| ICMP flood | | 5000 | 2 | 10000 | 100% |

Dengan melakukan serangan *flooding* atau membanjiri port TCP/22 dengan mengirimkan paket data sebesar 1000 paket dan 1 paket data berisi 1 serangan, hasil *alert* yang terdeteksi pada *web BASE snort* sebesar 1000, maka pengujian ini mencapai hasil 100%.

Pada model serangan port 68/UDP dilakukan *flooding port* dengan memberikan paket data sebesar 2500 paket dan 1 paket data dari *port UDP* terdapat 2 serangan, hasil alert yang terdeteksi pada *web BASE snort* untuk *port UDP* sebesar 4997 *alert*, maka pengujian pada model *UDP* mencapai hasil 99,94%**.**

Dan model serangan *Ping/ICMP* dilakukan flooding *IP* dengan memberikan paket data sebesar 5000 paket dan 1 paket ICMP terdapat 2 serangan, hasil alert yang terdeteksi pada *web BASE snort* sebesar 10000, maka pengujian pada model *UDP flood* mencapai hasil 100%.




**Grafik 1. Diagram hasil pengujian**

akurasi *alert*.

Pada Grafik 1 dapat diambil kesimpulan saat dilakukan model serangan UDP Flood sistem *IDS* tidak mampu mendeketsi paket serangan dengan maksimal, terjadi *error* sebesar 0.06% dan hanya mencapai hasil 99.94 %. Dan untuk model serangan *TCP Flood* dan *ICMP Flood* mampu mencapai hasil 100%.

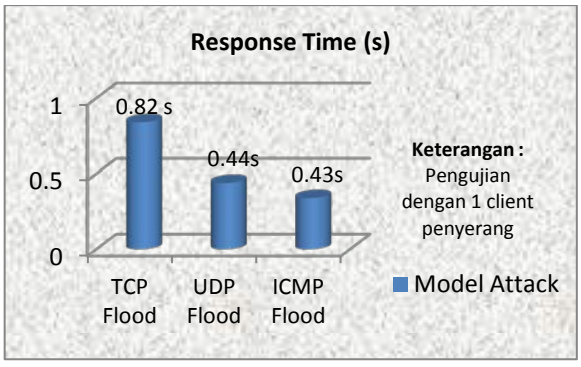
*B. Analisa Response Time Pengujian dengan 1 Client penyerang*

Analisa *response time* ini ialah analisa waktu respon *server* oleh *rules snort* terhadap adanya paket serangan yang dilakukan oleh 1 *client* penyerang secara bersamaan dengan 3 model serangan yaitu *TCP Flood*, *UDP Flood*, dan *ICP Flood* seperti pada tabel 2.

**Tabel 2. *Response Time Rules Snort***

| Model Attack | Time Span | Total Paket Diterma | Response Time |
|---|---|---|---|
| TCP flood | 1040.335 s | 1270 | 0.82 s/paket |
| UDP flood | 2561.886 s | 5778 | 0.44 s/paket |
| ICMP flood | 5395.634 s | 15869 | 0.34 s/paket |

Tabel diatas ialah hasil analisa *response time server* oleh *rules snort* dalam mendeteksi ketika ada paket serangan yang diberikan oleh 1 *client* penyerang. Untuk model serangan *TCP flood* menghasilkan *time span* 1040.335 s / total paket 1270 = 0.82 s/paket, *UDP flood* menghasilkan *time span* 2561.886 s / total paket 5778= 0.44 s/paket, dan *ICMP Flood* menghasilkan *time span* 5395.634 s / total paket 15869 = 0.34 s/paket.




**Gambar 7. Response Time Rules Snort**

Pada gambar 7 dapat dilihat response time dengan hasil terbesar pada model serangan *TCP flood* dengan hasil 0.82 s / paket. Hal ini disebabkan karena paket data yang dikirim lebih kecil.

Sehingga dapat disimpulkan *response time server* dalam mendeteksi adanya serangan memiliki rata-rata kurang dari 1 second / paket yaitu 0.53 s/paket.

*C. Pengujian Sistem Deteksi Serangan (IDS) dengan 2 Client.*

Pengujian dilakukan oleh 2 *client 1* yang bertindak sebagai penyerang. *Client* 1 dan Client 2 melakukan serangan secara bersamaan terhadap *server* dengan *variasi* serangan yaitu *flooding* atau membanjiri *IP atau Port* dengan menggunakan 3 Port/Protokol.yaitu 22/TCP flood, 68/UDP flood dan ICMP flood.

Tabel 3 menjelaskan racangan pengujian sistem *IDS*. Pada pengujian ini dilakukan Pada tanggal 23/05/2018 mulai pukul 04:20:32 WIB sampai dengan pukul 07:08:32 WIB dengan 2 client melakukan serangan *flooding* atau membanjiri port TCP/22 secara bersamaan.

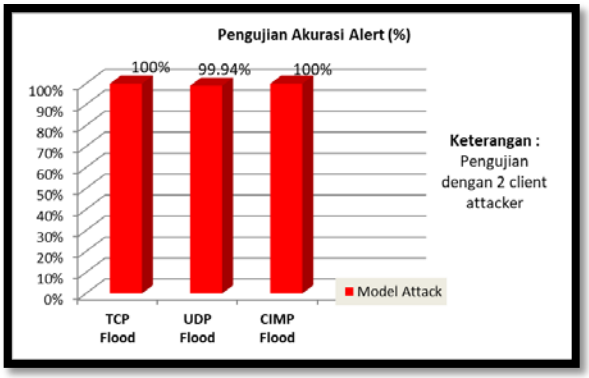
**Tabel 3. Tabel pengujian *Sistem Intrusion Detection System (IDS) Snort.***

| Model Serangan | Jumlah Client Penyerang | Paket dikirim | Jumlah serangan/paket | Jumlah Alert | Hasil Akurasi |
|---|---|---|---|---|---|
| TCP flood | 2 | 1000 | 1 | 2000 | 100% |
| UDP flood | | 2500 | 2 | 9997 | 99,94 % |
| ICMP flood | | 5000 | 2 | 20000 | 100% |

Dengan mengirimkan paket data sebesar 1000 paket dan 1 paket data berisi 1 serangan, hasil *alert* yang terdeteksi pada *web BASE snort* sebesar 2000 *alert*, maka pengujian ini mencapai hasil 100%.

Pada model serangan port 68/UDP dilakukan 2 client secara bersamaan melakukan serangan *flooding port* dengan memberikan paket data sebesar 2500 paket dan 1 paket data dari port UDP terdapat 2 serangan, hasil alert yang terdeteksi pada *web BASE snort* untuk port UDP sebesar 9997 *alert*, maka pengujian pada model UDP mencapai hasil 99,94%.

Dan model serangan Ping/ICMP dilakukan 2 client secara bersamaan melakukan flooding *IP* dengan memberikan paket data sebesar 5000 paket dan 1 paket ICMP terdapat 2 serangan, hasil alert yang terdeteksi pada *web BASE snort* sebesar 20000 *alert*, maka pengujian pada model UDP flood mencapai hasil 100%.




**Grafik 2. Diagram hasil pengujian akurasi *alert***

Pada Grafik 2 dapat diambil kesimpulan dari pengujian dilakukan oleh 2 client secara bersamaan memiliki hasil akurasi yang sama dengan pengujian menggunakan 1 client yaitu saat dilakukan model serangan UDP Flood sistem *IDS* mengalami *error* sebesar 0.06% dan hanya mencapai hasil 99.94 %. Dan untuk model serangan *TCP Flood* dan *ICMP Flood* mampu mencapai hasil 100%.

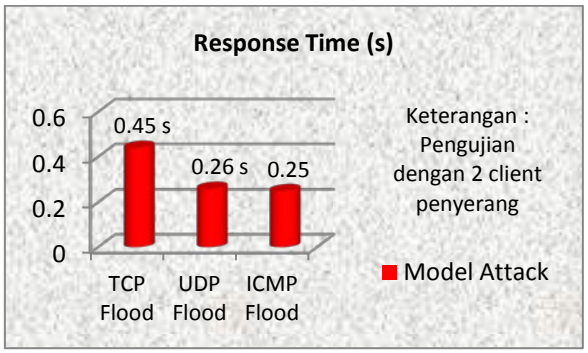
*D. Analisa Response Time pengujian oleh 2 client penyerang.*

Analisa *response time* ini ialah analisa waktu respon *server* oleh *rules snort* terhadap adanya paket serangan yang dilakukan oleh 2 *client* penyerang secara bersamaan dengan 3 model serangan yaitu *TCP Flood*, *UDP Flood,* dan *ICMP flood* seperti pada tabel 4.

**Tabel 4. *Response Time Rules Snort***

| Model Attack | Time Span | Total Paket Diterima | Response Time |
|---|---|---|---|
| TCP Flood | 1104.295 s | 2439 | 0.45 s/paket |
| UDP Flood | 2961.172 s | 11128 | 0.26 s/paket |
| ICMP Flood | 7291.117 s | 28522 | 0.25 s/paket |

Pada tabel 4 menggambarkan tabel hasil analisa *response time server* oleh rules snort dalam mendeteksi ketika ada paket serangan yang diberikan oleh 2 client penyerang secara bersamaan. Untuk model serangan *TCP flood* menghasilkan *time span* 1104.295 s / total paket 2439 = 0.45 s/paket, *UDP flood* menghasilkan *time span* 2961.172 s / total paket 11128 = 0.26 s/paket, dan ICMP Flood menghasilkan *time span* 7291.117 s / total paket 28522 = 0.25 s/paket.

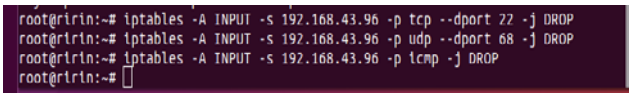



**Gambar 8. *Response Time Rules Snort* oleh 2 *Client* Penyerang**

Pada gambar 8 dapat dilihat *response time* dengan hasil terbesar pada model serangan *TCP flood* dengan hasil 0.45 s / paket. Dari diagram diatas rata-rata *response time* yang dihasilkan mencapai kurang dari 1 detik/paket yaitu 0.32 s/paket.

Sehingga dapat disimpulkan perbedaan *rules snort* dan model serangan yang berbeda akan mempengaruhi kecepatan pendeteksian serangan. Jadi ketika paket data yang dimasukkan itu semakin besar maka kecepatan pendeteksian akan semakin meningkat dan lebih cepat.

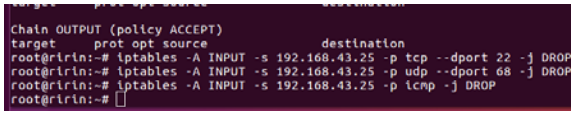
*E. Pengujian Sistem Pencegah Serangan (IPS) pada iptables.*




**Gambar 9. Tampilan *Firewall IP Tables* melakukan *block IP Client* 1 secara manual**

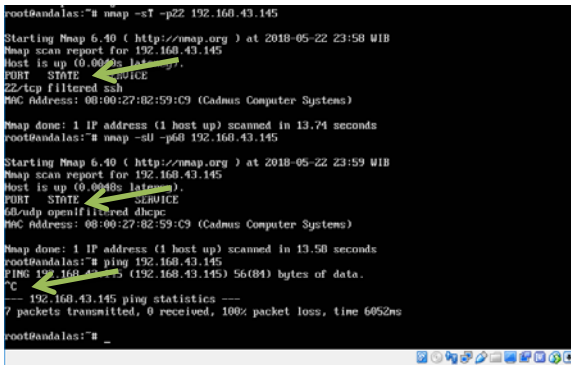
Pada gambar 9 dilakukan *setting blocking IP* penyerang yaitu protokol *TCP*, *UDP*,

dan *ICMP* dengan *IP Address* 192.168.43.96 seperti pada gambar 9.



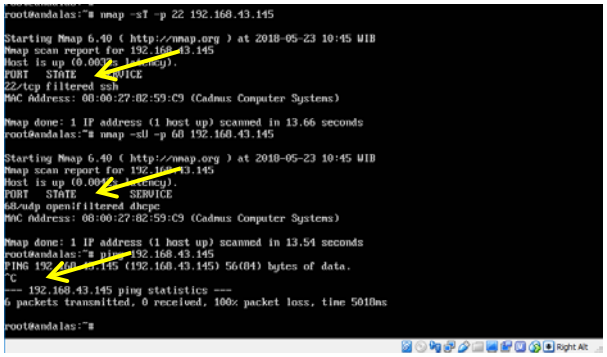

**Gambar 10. Tampilan *Firewall IPTables* melakukan *block IP Client 2* secara manual**

Pada gambar 10 dilakukan *setting blocking IP* penyerang yaitu protokol *TCP, UDP,* dan *ICMP* dengan *IP Address client* 2 yaitu 192.168.43.25.




**Gambar 11. Tampilan pada *Client* 1 saat di *Block***

Gambar 11 menunjukkan *client* 1 tidak dapat melakukan serangan karena sudah dilakukan *blocking / filtered* oleh sistem *IPS iptables*. Hasil *blocking IP* ialah keterangan *state "filtered"*. *State filtered* ini menunjukkan bahwa *Internet Protocol (IP)* penyerang telah berhasil di blok oleh sistem *Intrusion Prevention System (IPS)*




**Gambar 12. Tampilan pada *Client* 2 telah terblok**

Gambar 12 menunjukkan client 2 tidak dapat melakukan serangan karena sudah dilakukan *blocking / filtered* oleh sistem *IPS iptables*. Hasil *blocking IP* ialah keterangan *state "filtered"*. *State filtered* ini menunjukkan bahwa *Internet Protocol (IP)* penyerang telah berhasil di blok oleh sistem *Intrusion Prevention System (IPS).*

Sehingga dapat ditarik kesimpulan bahwa sistem *Intrusion Prevention System (IPS)* atau sistem pencegah penyusup secara fungsional dapat melakukan *blocking IP* dengan baik sehingga client penyerang tidak dapat lagi melakukan serangan terhadap *server.*

## IV. KESIMPULAN

Implementasi sistem keamanan jaringan pada LAN nantinya mampu terintegrasi dengan baik dan dapat dilakukan pengujian dengan baik.

1. Tercipta sistem keamanan *IDPS Snort* pada jaringan komputer *LAN* dan berfungsi dengan baik.

2. Sistem *IDS* dengan *Snort* yang diimplementasikan dapat melakukan deteksi serangan dengan hasil rata-rata nilai akurasi yang sama yaitu 99.98% pada pengujian dengan 1 client dan 2 client dan menghasilkan rata-rata nilai *response time server* oleh *rules snort* yang baik yaitu kurang dari 1 *second* membaca paket data yang ada, pada saat pengujian dengan 1 *client* yaitu 0.53 second dan dengan 2 *client* yaitu 0.32 second.
3. Sistem *IDS* mampu mendeteksi serangan dengan baik dan memiliki kemampuan kinerja yang sama dalam melakukan deteksi serangan dengan jumlah 1 client atau lebih banyak client.
4. Sistem *IPS* dengan *IP Tables* mampu melakukan *blocking IP s*erangan atau penyusup dengan baik.

## V. SARAN

Penulis menyadari bahwa pada implementasi sistem *Intrusion Detection System (IDS)* dan *Intrusion Prevention System (IPS)* ini masih memiliki hasil yang belum maksimal, sehingga perlu untuk dikembangkan sistem *Intrusion Detection System (IDS)* yang lebih baik lagi agar dapat mendeteksi model serangan yang lebih banyak dan sistem *Intrusion Prevention System (IPS)* yang dapat memblokir *IP* serangan secara otomatis.

## DAFTAR ACUAN


[1] Ervin Kusuma Dewi, Patmi Kasih, 2017, "Analisis Log Snort Menggunakan Network Forensic", *Jurnal Ilmiah Penelitian dan Pembelajaran Informatika (JIPI)*, Vol.02, No.02, pp : 72-79, Desember.

[2] Dwi Kuswanto, 2017, "Studi Analisis Host Based Intrusion Detection System Berbasis Snort", *Seminar Nasional Teknologi Informasi dan Komunikasi (SEMANTIKOM)*, Fakultas Teknik Universitas Trunojoyo, Bangakalan,.

[3] Emir Risyad, Mahendra Data, Eko Sakti Pramukantoro, 2017, "Perbandingan Performa Intrusion Detection System (IDS) Dan Suricata Dalam Mendeteksi Serangan TCP SYN Flood", *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, e-ISSN:2548-964X, Vol.2, No.9, hlm.2615-2624, September.

[4] Bryan Zico Octavian, Wiwin Sulistyo, 2017, "Rancang Bangun Snort Base IPS (Intrusion Prevention Systems) Pada Local Area Network", *Artikel Ilmiah*, Teknik Informatika, Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana, Salatiga, Mei.

[5] Fadlin Arsin, Muh. Yamin, La Surimi , 2017, "Implementasi Security System Menggunakan Metode IDPS (Intrusion Detection and Prevention System)

Dengan Layanan Realtime Notification", *semanTIK, ISSN : 2502-8928*, Vol. 3, No.2, pp.39-48, Juli – Desember.

[6] Abdul Rahim, 2016, "Rancang Model Sistem Keamanan Menggunakan Intrusion Prvention System Dengan Metode Rule Bases : Studi Kasus KPDE Provinsi Jambi", *Jurnal Ilmiah Media SISFO*, Vol.10, No.2, p-ISSN : 1978-8126, e-ISSN : 2527-7340, Oktober.

[7] Sutarti, Adi Putranto Pnacaro, Fembi Isnanto Saputra, 2018, "Implementasi IDS (Intrusion Detection System) pada Sistem Keamanan Jaringan SMAN 1 CIKEUSAL", *Jurnal PROSISKO*, Vol.5, No.1, e-ISSN : 2597-9922, Maret.

[8] Didit Suhartono, Andi Dwi Riyanto, Yogi Widy Astomo, 2015, "Intrusion Detection Prevention System (IDPS) pada Local Area Network (LAN) ", *Jurnal Telematika* , Vol.8, No.1 , e-ISSN : 2442-4528, Februari.

[9] Budi Sudradjat, 2017, "Sistem Pendeteksian Dan Pencegahan Penyusup Pada JARINGAN Komputer Menggunakan Snort dan Firewall", *Journal of Information System, Applied, Management, Accouting and Research (JISAMAR)*, ISSN : 2598-8700, Vol.01, No.01, November.

[10] C.Seelammal, K. Vimala Devi, 2016, "Computational Intelligence in Intrusion Detection System for Snort log using Hadoop", *Journal Conference on Control, Intrumentation, Communication and Computional Technologies*, IEEE, India,.

[11] L. J. G. Villalba, A. L. S. Orozco, J. M. Vidal, 2015, "Anomaly-Based Network Intrusion Detection System", *IEEE Latin American Transactions*, Vol.13, No.3, IEEE, March.

[12] Salamn Niksefat, Babak Sadeghiyan, Payman Mohassel, Saeed Sadeghian, 2016, "ZIDS: A Privacy-Preserving Intrusion Detection System Using Secure Two-Party Computation Protocols", *Journal Conference on Control, Intrumentation, Communication and Computional Technologies*, IEEE, India.

[13] Alessio Merlo, Elena Spadacini, Mauro Migliardi, 2016, "IPS-based reduction of network energy consumption", *IEEE Latin American Transactions*, Vol.24, No.6, IEEE, August.

[14] Eva Charismanty "Tutorial Snort untuk IDS", *Available* : http://andiwre.itmaranatha.org/tipsntrik/linux/SNORT%20untuk%20IDS%20-%20EvaCharismanty.pdf.

[15] Hengky Bintara "Mengenal Snort sebagai Network Intrusion Detection

System (NIDS)", *Available* : https://netsec.id/snort-nids/