BAB II

TINJAUAN PUSTAKA

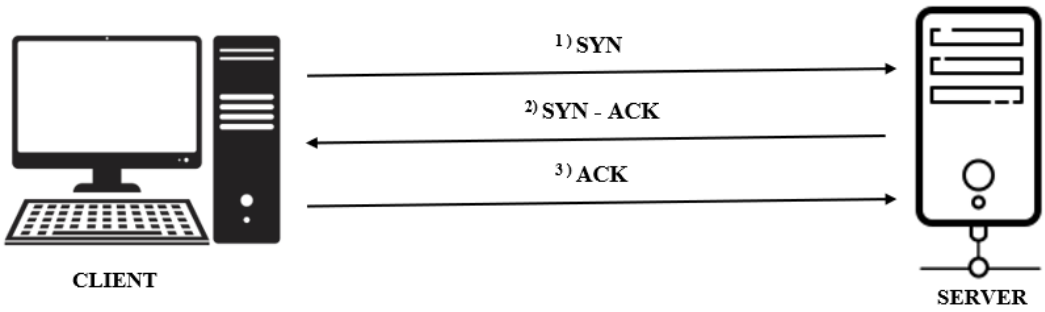
2.1. *Denial of Service (DOS)*

Denial of Service adalah serangan dalam lingkungan jaringan yang bertujuan untuk menguras sumber daya dan menghambat layanan server ke pengguna resmi (Afif et al., 2018). DOS dan DDOS pada dasarnya sama saja, akan tetapi serangan DDOS lebih terstruktur. DDOS memiliki dampak yang umumnya jauh lebih besar dari pada DOS (Hermawan, 2013). Terdapat beberapa jenis dari serangan *Denial of Service* diantaranya : *Syn Flooding*, *XMAS Flood,* dan *Slowloris*.

2.1.1. *Syn Flooding*

SYN Flood adalah sebuah serangan DOS yang menargetkan kelemahan pada protokol. Penyerang akan mengirim banyak paket *Syn* kepada target, sehingga mengakibatkan target harus terus menerus menjawab permintaan paket *Syn* tersebut (Bogdanoski et al., 2013).

Pada dasarnya ketika client terhubung pada server maka terjadi sebuah proses koneksi TCP ke server, kemudian client-server saling berbagi informasi umumnya seperti ditampilkan pada gambar 2.1.



Gambar 2.1 Koneksi TCP ke *Server*

Akan tetapi dalam kasus SYN Flood, ketika server merespon dengan mengirimkan kode SYN – ACK ke client, client tidak pernah mengembalikan kembali kode ACK, akan tetapi mengirimkan kembali paket SYN ke semua port dan mengakibatkan koneksi setengah terbuka antara client-server. Hal tersebut berdampak pada server yang berujung server menjadi down karena sibuk menerima request paket SYN yang tidak kunjung ada balasan dari client. Bakhan untuk pengguna/client sah pun tidak dapat terhubung kepada server.

2.1.2. *XMAS Flood*

TCP XMAS Flood atau *TCP All Flag Flood* adalah serangan *Denial of Service* yang bertujuan untuk mengganggu aktifitas jaringan dengan memenuhi *bandwith* dan sumber daya pada target. Dengan terus mengirimkan semua paket TCP *flags* (URG, ACK, PSH, RST, SYN, FIN) menuju target, pertahanan stateful bisa turun dan dimanfaatkan sebagai celah untuk menjalankan serangan lainnya (MazeBolt, n.d.).

2.1.3. *Slowloris*

Slowloris merupakan salah satu serangan *Denial of Service* yang sangat bertarget. Serangan s*lowloris* memungkinkan satu *web server* untuk menjatuhkan server yang lain tanpa mempengaruhi layanan atau *port* lain di jaringan target. Serangan ini menahan koneksi terhadap target sebanyak mungkin dan selama mungkin dengan hanya mengirimkan sebagian permintaan. *Slowloris* terus menerus mengirimkan permintaan dalam bentuk header HTTP tersebut tanpa pernah menyelesaikan permintaanya sehingga koneksi akan terus terbuka dan

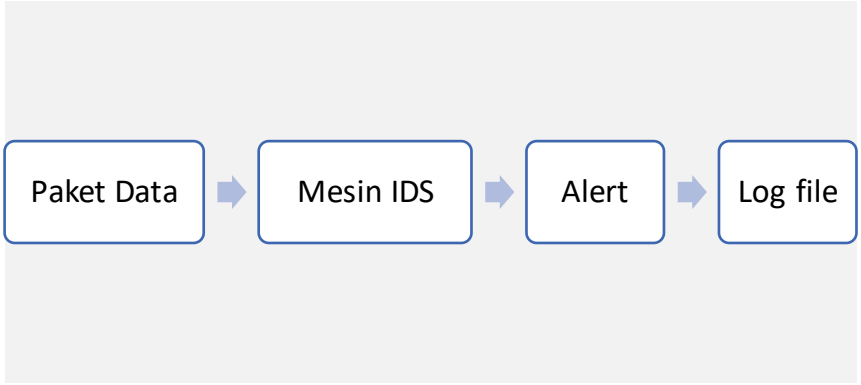
server akan mengalami atau melakukan penolakan layanan terhadap klien yang sah (Imperva, n.d.).

2.2. *Intrusion Detection System (IDS)*

Intrusion Detection System (IDS) adalah sebuah sistem untuk memeriksa *traffic* atau lalu lintas pada jaringan guna untuk mengidentifikasi pola jaringan yang mencurigakan atau yang dapat mengidikasikan serangan (Anwar et al., 2019).

Ada dua jenis yang terdapat pada sistem IDS yaitu *Rules Based System* dan *Adaptive System*. Perbedaannya adalah pada *signature* dan *rules*, jika RBS berdasarkan *database* sementara AS tidak hanya berdasarkan *database* yang ada, melainkan juga memiliki kemungkinan untuk mendeteksi serangan-serangan yang baru (Alamsyah et al., 2020).

Pada dasarnya proses pencatatan aplikasi *Imtrusion Detection System* melakukan pendeteksian terhadap paket anomali ketika paket tersebut diterima atau dideteksi oleh mesin IDS, seperti ditampilkan pada gambar 2.2.



Gambar 2.2 Alur deteksi IDS

Pada gambar 2 menjelaskan langkah dari pendeteksian dan pencatatan trafik anomali pada sebuah sistem IDS. Dimana ketika ada paket data yang masuk

kedalam sistem IDS, maka selanjutnya sistem IDS akan memberikan notifikasi berupa *alert* kepada admin, lalu alert tersebut tersimpan secara otomatis kedalam sebuah *log file* yang bisa di akses untuk mendapatkan informasi tentang paket data apa saja yang masuk pada jaringan tersebut.

2.3. *Intrusion Prevention System (IPS)*

Intrusion Prevention System (IPS) adalah suatu metode yang digunakan untuk mengkombinasikan firewall dan metode *Intrusion Detection System (IDS)*. Sistem IPS mencegah serangan yang masuk ke jaringan dengan mendeteksi dan mencatat paket data. disaat serangan telah teridentifikasi, sistem akan menolak akses (block) dan mencatat pada riwayat semua paket data yang teridentifikasi telah melakukan penyerangan (Khadafi et al., 2017).

2.4. Penelitian Terkait

Para peneliti saat ini mencoba menjawab tantangan tersebut dengan memperluas *state-of-the-art* bidang penelitian dengan unsur keterbaruan untuk dapat memenuhi kebutuhan analisa dari hasil analisis *Intrusion Detection System*. Tabel 1 menunjukan penelitian terkait yang akan digunakan sebagai referensi pada penelitian yang dilakukan.

Tabel 2.1 Penelitian terkait (*State of the art*)

No	Judul	Peneliti	Aplikasi	Serangan	Hasil Penelitian
1	*Intrusion Detection System using Fuzzy Rough Set Feature Selection*	Balakrishnan Senthilnayaki, Krishnan Venkatalakshmi, Arpputhar	Snort	KDD Dataset (Kelas Serangan : Probing, DOS, U2R, R2U)	Pengurangan redudansi pada deteksi snort dianalisis menggunakan algoritma klasifikasi KNN dan penggunaan fitur seleksi *fuzzy rough set.* Penelitian ini menghasilkan

No	Judul	Peneliti	Aplikasi	Serangan	Hasil Penelitian
	and Modified KNN *Classifier*.	aj Kannan (Senthilnayaki et al., 2019)			pengurangan waktu pada proses komputasi dan mendapatkan tingkat akurasi yang lebih besar.
2	Analisa Keamanan Jaringan Menggunakan Network Intrusion Detection and Prevention System	Hendri Alamsyah, Riska, Abdussalam Al Akbar (Alamsyah et al., 2020)	Suricata	*Port scanning*, FTP *attacks*, and *telnets*	Penelitian mendapatkan hasil yang menunjukan bahwa IDPS dapat melakukan pendeteksian sekaligus pencegahan ketika terdapat serangan pada sistem jaringan komputer melalui p*ort scanning*, FTP *attacks*, and *telnets.*
3	Klasifikasi Anomali *Intrusion Detection System* (IDS) Menggunakan Algoritma *Naïve Bayes Classifier dan Correlation-Based Feature Selection*	Saipul Anwar, Fajar Septian, Ristasari Dwi Septiana (Anwar et al., 2019)	Bro	Dataset UNSW-NB15 (*Fuzzer, Anlysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode, Worms)*	Penggunaan pemodelan dengan CFS menghasilkan waktu proses 6 kali lebih cepat dan akurasi yang lebih baik dari pada tanpa menggunakan CFS.
4	*Uses Of Artificial Intelligent Techniques To Build Accurate Models For Intrusion Detection System*	Anil Lamba, Satinderjeet Singh, Sachin Bhardwaj, Natasha Dutta, Sivakumar Sai Rela Muni	Snort	KDD Dataset (Kelas Serangan : *Probing*, DOS, U2R, R2U)	Penelitian ini menghasilkan kesimpulan bahwa penggunaan *random forest classification* mengungguli klasifikasi lain dalam pertimbangan parameter data set. Akurasi klasifikasi untuk pertimbangan parameter atau atribut penting klasifikasi anomali

No	Judul	Peneliti	Aplikasi	Serangan	Hasil Penelitian
		(Lamba et al., 2019)			dengan klasifikasi RFC menghasilkan akurasi sebesar 99%.
5	Keamanan Jaringan (*Firewall*) Dari Penyerangan Melalui Metode Dos (*Denial Of Service*) Dengan Menggunakan *Visual Basic* 6.0	Herbert A. Tambunan, Allwine (Tambunan et al., 2017)	-	Denial of Service	Penelitian ini membangun aplikasi untuk pencegahan berdasarkan kriteria penyerangan pada serangan *Denial of Service.*
6	Implementasi Metode *Deep Packet Inspection* untuk Meningkatkan Keamanan Jaringan pada *Software Defined Networks*	Danaswara Prawira Harja, Andrian Rakhmatsyah, Muhammad Arief Nugroho (Harja et al., 2019)	SDN	*Denial of Service*	Penelitian ini menghasilkan sebuah peningkatan keamanan dengan melakukan *blocking packet, controller (collect data, detection, mitigation).*
7	Optimasi Algoritma *Naïve Bayes Classifier* untuk Mendeteksi Anomaly dengan	Harianto, Andi Sunyoto, Sudarmawan (Harianto et al., 2020)	Bro	Dataset UNSW-NB15 (*Fuzzer, Anlysis, Backdoors, DoS, Exploits, Generic, Reconnai*	Penelitian ini menggunakan *Naive Bayes Classiofication* dengan penggunaan seleksi fitur *Univariate Selection* untuk menghitung tingkat akurasi dari aplikasi *Intrusion Detection System* dalam mendeteksi

No	Judul	Peneliti	Aplikasi	Serangan	Hasil Penelitian
	Univariate Fitur Selection			*ssance, Shellcode, Worms)*	serangan. Dengan penggunaan klasifikasi tersebut menghasilkan tingkat nilai akurasi yang lebih baik.
8	Analisis Perbandingan *Detection Traffic Anomaly* Dengan Metode *Naive Bayes* Dan *Support Vector Machine (Svm)*	Imam Riadi, Rusydi Umar, Fadhilah Dhinur Aini (Riadi et al., 2019)	Wireshark	*Denial of Service*	Penelitian ini menggunakan metode NBV dan SVM yang mendapatkan nilai probabilitas 0.1, dan probabilitas yang paling tinggi yaitu 0.8. Dimana penganalisisan dengan metode ini sangat optimal.
9	Analisis Statistik *Log* Jaringan Untuk Deteksi Serangan Ddos Berbasis *Neural Network*	Arif Wirawan Muhammad, Imam Riadi, Sunardi (Muhammad, 2016)	Wireshark	*Dataset* CAIDA 2007 *Distribute Denial of Service*	Penelitian ini menghasilkan prosentase rata-rata pengenalan terhadap tiga kondisi jaringan (normal, slow DDoS, Dan DDoS) sebesar 90,52%.
10	*Performance Comparison of Intrusion Detection Systems and Application of*	Syed Ali Raza Shah, Biju Issac (Shah & Issac, 2018)	Snort dan Suricata	SSH, FTP, HTTP, ICMP, ARP, dan Scan	Penelitian ini menghasilkan kesimpulan bahwa suricata memiliki penggunaan *resource* yang lebih banyak daripada aplikasi snort. Suricata memiliki kecepatan proses yang lebih baik ketika memproses paket dengan

No	Judul	Peneliti	Aplikasi	Serangan	Hasil Penelitian
	Machine Learning to Snort System				ukuran 10Gbps daripada snort.
11	Analisis Perbandingan Kinerja *Snort* Dan *Suricata* Sebagai *Intrusion Detection System* Dalam Mendeteksi Serangan *Syn Flood* Pada *Web Server Apache*	Lukman, Melati Suci (Lukman & Suci, 2020)	Snort dan Suricata	Syn Flooding	Hasil dari perbandingan pada penelitian ini adalah aplikasi snort lebih mengungguli dari performa deteksi dan penggunaan CPU yang rendah daripada suricata. Akan tetapi pada parameter penggunaan RAM menghasilkan penggunaan dari suricata lebih rendah daripada snort dengan 3,42% penggunaannya.
12	Analisis Perbandingan Quality of Service (QoS) Penerapan Snort IDS dan Bro IDS Dalam Arsitektur Software Define Network (SDN)	Hendrawan, Parman Sukarno, Muhammad Arief Nugroho (Sukarno & Nugroho, 2018)	Snort dan Bro	Serangan pada layer 3, layer 4, dan layer 7	Penelitian ini menghasilkan bahwa aplikasi bro lebih baik dari snort dari parameter *throughput* dengan perbandingan 4:1. Parameter *delay* menghasilkan bro lebih baik dari snort dengan perbandingan 3:1. Parameter *packet loss* menghasilkan bro lebih baik dari snort dengan perbandingan 5:1. Pada penggunaan *resource*, aplikasi bro lebih banyak

No	Judul	Peneliti	Aplikasi	Serangan	Hasil Penelitian
					penggunaannya daripada snort.

Berdasarkan penelitian terkait pada tabel 2.1 akan diambil tiga penelitian yang akan digunakan sebagai perbandingan dan pencarian keterbaruan terhadap penelitian yang dilakukan yaitu perbandingan kinerja deteksi aplikasi snort dan suricata berdasarkan pada jenis serangan *denial of service*.

Penelitian (Sukarno & Nugroho, 2018) mencoba melakukan pengujian kinerja aplikasi *snort* dan *bro.* Pengujian dilakukan dengan menggunakan penyerangan pada *layer 3, layer 4,* dan *layer 7* pada *layer* osi. Pengujian pada penelitian tersebut berdasarkan lima parameter yang di uji, yaitu : *throughput, Delay, Packet Loss,* CPU *Usage* dan *Memory Usage*. Hasil yang didapatkan dari penelitian menjelaskan perbandingan kinerja pada setiap parameter yang diujikan. Tetapi pada penelitian ini belum melakukan pengujian pada parameter *load average*. Parameter *load average* merupakan parameter yang bisa digunakan untuk melihat performa sistem yang menjalankan aplikasi IDS berdasarkan jangka waktu tertentu.

Penelitian (Shah & Issac, 2018) mencoba melakukan pengujian dan perbandingan aplikasi *snort* dan *suricata*. Pengujian pada penelitian ini menggunakan beberapa paket mencurigakan atau serangan yang dihasilkan oleh deteksi aplikasi IDS yaitu SSH, DoS, FTP, HTTP, ICMP, ARP, dan *Scan*. Parameter yang diuji adalah *CPU Utilisation, Memori Utilisation, Packet Processing,* dan *Packet Drop*. Pada skema dua penelitian ini melakukan uji akurasi deteksi dengan menggunakan *machine learning* pada aplikasi *snort.* Akan tetapi pada penelitian ini tidak fokus terhadap perbandingan kinerja deteksi pada masing-

masing serangan yang diuji. Penelitian ini berfokus kepada perhitungan akurasi dari aplikasi IDS snort.

Penelitian (Lukman & Suci, 2020) mencoba melakukan pengujian dan perbandingan aplikasi *snort* dan *suricata*. Serangan yang digunakan pada penelitian ini adalah serangan menggunakan protokol TCP yaitu TCP *Syn Flooding*. Pengujian yang dilakukan pada penelitian ini berdasarkan empat parameter : deteksi, penggunaan CPU, penggunaan RAM, dan *dropped packet*. Akan tetapi pada percobaan ini pengujian hanya menggunakan satu serangan saja, yaitu *syn flooding*. Sebaiknya pengujian dan perbandingan dilakukan pada dua atau lebih serangan yang berbeda.