BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Jaringan komputer telah menjadi bagian integral dalam kehidupan manusia. Jaringan memungkinkan kita untuk berkomunikasi, berbagi informasi, dan mengakses berbagai layanan secara *online*. Namun, semakin besar ketergantungan kita pada jaringan, semakin besar pula risiko keamanan yang dihadapi di era digital ini. Berdasarkan data *survey* yang dilakukan oleh *We Are Social* pada Januari 2024, terdapat 5,35 miliar pengguna internet di seluruh dunia, yang merupakan 66,2% dari populasi global. Dari jumlah tersebut, 5,35 miliar, atau 66,2% dari populasi dunia, adalah pengguna media sosial [1]. Sedangkan menurut data yang diumumkan oleh APJII, jumlah pengguna *internet* Indonesia tahun 2024 mencapai 221.563.479 jiwa dari total populasi 278.696.200 jiwa penduduk Indonesia tahun 2023. Dari hasil survei penetrasi internet Indonesia 2024 yang dirilis APJII, maka tingkat penetrasi *internet* Indonesia menyentuh angka 79,5%. Dibandingkan dengan periode sebelumnya, maka ada peningkatan 1,4% [2].

Dengan bertambahnya jumlah pengguna *internet* di dunia, maka semakin meningkat pula tindakan serangan siber (*cybercrime*) atau peretasan yang di lakukan pada suatu jaringan internet. Menurut data yang diumumkan oleh Menteri Komunikasi dan Informasi, Indonesia berada di urutan kedua untuk *cybercrime* dengan persentase terbanyak yaitu peretasan dalam dunia maya dan sektor perbankan [3]. Serangan siber atau *cybercrime* sendiri merupakan upaya yang disengaja untuk mencuri, mengekspos, mengubah, melumpuhkan, atau menghancurkan data, aplikasi, atau aset lainnya melalui akses tidak sah ke jaringan, sistem komputer, atau perangkat digital.

Data statistik dari Badan Siber dan Sandi Negara (BSSN) mencatat bahwa telah terjadi 370,02 juta serangan siber terhadap Indonesia pada tahun 2022. Dibandingkan dengan tahun sebelumnya terjadi 266,74 juta serangan siber, jumlah ini meningkat sebesar 38,72% [4]. Serangan siber sendiri yang terjadi di Indonesia pada tahun 2022 sebanyak 700 Juta serangan. Data BSSN menunjukkan bahwa

714.170.967 anomali trafik atau serangan siber terjadi di sepanjang tahun 2022. Serangan tertinggi, yang mencapai 272.962.734 pada bulan Januari, mencapai lebih dari sepertiga dari total serangan selama semester pertama tahun itu. Serangan siber yang paling umum terjadi pada BSSN adalah serangan *ransomware* atau *malware* yang meminta tebusan untuk memiliki data, *phishing*, dan eksploitasi kerentanan. Data yang dirilis Interpol tentang serangan siber ASEAN 2021 menunjukkan bahwa Indonesia menempati urutan pertama di antara negara-negara ASEAN dalam hal serangan *malware*. Indonesia menempati urutan pertama dengan 1,3 juta kasus, diikuti oleh Vietnam dengan 886.874 kasus, dan Brunei dengan 257 kasus. Sebuah laporan terbaru dari *National Cyber Security Index* (NCSI) menunjukkan bahwa keamanan *cyber* Indonesia berada di peringkat ke-6 di antara 160 negara lain [5]. Pada kuartal pertama 2025, tercatat lebih dari 3,2 juta ancaman siber terdeteksi oleh *Kaspersky Security Network* (KSN) yang memengaruhi sekitar 15,5 % pengguna di Indonesia [6].

Melihat perkembangan teknologi informasi, ancaman kejahatan siber saat ini sangat penting. Bukan hanya secara teoretis, tetapi kejahatan siber memang terjadi dalam beberapa kasus. *Hacking*, *sabotage*, *spionase*, *garding*, serangan vandalisme, *spyware*, dan serangan jaringan listrik adalah beberapa jenis kejahatan siber yang telah berkembang dan beragam. Jenis teknologi yang digunakan, jenis kejahatan atau kerugian yang dilakukan, dan tujuan dari kejahatan siber berbeda.

Ancaman baru seperti *Cyber War* atau perang siber, saat ini telah menjadi ancaman nyata bagi suatu negara dimana ancaman modern ini tidak dapat dikategorisasi hanya sebatas militer dan non-militer saja. Perang saat ini tidak hanya dapat terjadi di dunia nyata saja melainkan dapat pula terjadi di dunia maya. Beberapa contoh perang atau serangan siber yang terjadi adalah *Email propagation* of malicious *code*, *Wide-scale Trojan distribution, Distributed attack tools, Distributed Denial of service (DDoS) attacks, Targeting of specific users, Antiforensic techniques, Wide-scale use of worms, dan Sophisticated command and control attacks*. Serangan siber yang terjadi ini bahkan akan terus berkembang sesuai dengan kemajuan teknologi informasi yang semakin canggih [7].

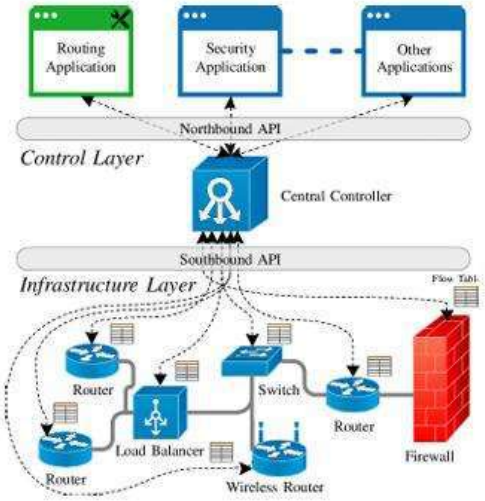
Salah satu ancaman yang paling merusak adalah *Distributed Denial-of-Service* (*DDoS*), yaitu serangan yang dilakukan dengan membanjiri sistem target menggunakan lalu lintas data palsu secara terus-menerus, hingga layanan menjadi tidak tersedia bagi pengguna sah. *Cloudflare* melaporkan bahwa pada kuartal pertama tahun 2025 saja, jumlah serangan *DDoS* meningkat hingga 358% dibandingkan tahun sebelumnya, dengan volume serangan tertinggi mencapai 7,3 Tbps dan 4,8 miliar paket per detik, yang menyasar sektor telekomunikasi, keuangan, dan layanan daring. [8].

Salah satu bentuk *DDoS* yang patut diwaspadai adalah *SYN flood*, yakni serangan berbasis protokol *TCP* yang mengeksploitasi kelemahan dalam proses *three-way handshake*. Dalam serangan ini, penyerang membanjiri *server* dengan paket *SYN* tanpa menyelesaikan koneksi, sehingga menyebabkan *server* kehabisan sumber daya karena menyimpan banyak koneksi setengah terbuka (*half-open connections*). Dampak dari serangan ini bisa sangat parah, terutama terhadap sistem yang memiliki kontrol terpusat seperti pada arsitektur *Software Defined Networking* (*SDN*).

Pada saat ini, jaringan tradisional mulai ditinggalkan karena dianggap terlalu lambat dan bergantung pada vendor dan pengembang dari luar, seperti komunitas *open source* yang tidak dapat mengembangkan perangkat jaringan komputer secara bebas. Pada jaringan konvensional, perangkat layer 2 (*switch*) dan layer 3 (*router*) menggabungkan *control plane* dan *data plane*, yang menyebabkan banyak kompleksitas pada jaringan komputer. Jika ada perangkat jaringan baru, router yang lama akan memberikan informasi ke *router* sebelah, sehingga *table routing* seluruh jaringan harus diupdate ulang. Jaringan tradisional menggunakan paradigma terdistribusi dalam bidang kontrol. Semua perangkat jaringan, protokol seperti *ARP*, *STP*, *OSPF*, *EIGRP*, dan *BGP* bekerja secara mandiri. Perangkat jaringan ini terhubung, tetapi tidak ada mesin terpusat yang mengelola seluruh jaringan atau meringkasnya. Perbedaan utama antara *SDN* dan jaringan tradisional adalah bahwa *SDN* biasanya berbasis perangkat lunak, sedangkan jaringan tradisional berbasis perangkat keras. diperlukan pembaruan teknologi jaringan komputer yang dapat

mengatasi kompleksitas jaringan konvensional yaitu dengan adanya arsitektur jaringan *SDN* (*Software Defined Network*).

Dalam beberapa tahun terakhir, para peneliti dan profesional telah menaruh minat yang lebih besar dalam mengeksplorasi keamanan siber yang dapat diprogram adalah konsep yang baru-baru ini mengalami kebangkitan yang signifikan dengan banyak perhatian yang dihasilkan oleh *SDN*, yang memungkinkan kontrol jaringan terpusat secara logis dengan memisahkan bidang kontrol dari bidang data. *Software Defined Networking* (SDN) adalah teknologi jaringan terbaru yang dirancang untuk mengatasi masalah yang ada pada teknologi informasi (TE). Karena cara kerjanya yang lebih fleksibel dan terpusat, *SDN* dapat secara signifikan mengurangi jumlah sumber daya jaringan yang dibutuhkan untuk komunikasi sehingga lebih banyak manfaat dari sumber daya jaringan. Arsitektur *SDN* mencakup pengontrol jaringan terpusat dengan pengontrol jaringan global dari jaringan dan *Application Programming Interface* (API) untuk mengembangkan aplikasi jaringan. Di antara keuntungan *SDN* adalah potensi untuk hampir seketika menghentikan lalu lintas berbahaya dari jaringan antarmuka setelah terdeteksi. *SDN* beroperasi sebagai "otak" dari sistem, yang mengontrol sakelar jaringan dan memelihara semua fungsi jaringan melalui pemantauan ekstensif dan administrasi. Perangkat seperti sakelar dan *router* adalah bertanggung jawab untuk mengirimkan semua data di jaringan [9]. Koneksi kabel atau nirkabel digunakan untuk menghubungkan ini gadget ini bersama-sama. Gambar 1.1 menggambarkan arsitektur SDN secara keseluruhan, dengan setiap lapisan diberi label yang jelas.



Gambar 1. 1 Arsitektur untuk Software Defined Networking (SDN) *[9]*.

Meskipun *SDN* menawarkan banyak manfaat, namun arsitekturnya yang terpusat juga menghadirkan beberapa tantangan keamanan baru. Serangan terhadap *controller SDN* dapat berakibat fatal bagi seluruh jaringan. *Controler SDN* merupakan "otak" dari jaringan, memegang kendali penuh atas konfigurasi dan aliran trafik. Serangan terhadap *controller* dapat berakibat fatal, memungkinkan penyerang untuk memanipulasi konfigurasi jaringan, mengalihkan trafik ke server jahat, memblokir akses ke sumber daya penting, atau bahkan meluncurkan serangan lebih lanjut ke perangkat lain di jaringan.

Untuk menghadapi tantangan tersebut, perlu diimplementasikan sistem keamanan yang andal, salah satunya adalah *Intrusion Detection and Prevention System* (*IDPS*). *IDPS* merupakan teknologi yang berfungsi untuk mendeteksi, memantau, dan mencegah aktivitas mencurigakan dalam jaringan. Sistem ini dapat mengidentifikasi pola serangan, termasuk trafik abnormal seperti *DDoS* berbasis *SYN flood*, dan memberikan respons secara *real-time* untuk mencegah eskalasi serangan. Penerapan *IDPS* sangat penting dalam konteks *SDN*, karena dapat memberikan lapisan perlindungan tambahan terhadap kontroler dan perangkat jaringan lainnya.

Dalam penelitian ini, digunakan salah satu *IDPS* berbasis *open source* yaitu *Snort* versi 2, yang telah terbukti luas digunakan dalam mendeteksi berbagai serangan

jaringan. *Snort* bekerja dengan menganalisis paket-paket data yang melewati jaringan dan mencocokkannya dengan *signature* serangan yang telah didefinisikan sebelumnya. Dengan dikombinasikan bersama arsitektur *SDN*, *Snort v2* dapat diimplementasikan pada *topologi* yang terpusat untuk memantau trafik secara menyeluruh serta melakukan *mitigasi* terhadap ancaman seperti *SYN flood*. Penelitian ini secara khusus akan menganalisis efektivitas deteksi dan perlindungan *Snort* ketika menghadapi serangan *SYN flood* dengan tingkat intensitas yang berbeda, guna menilai sejauh mana ketahanan sistem terhadap beban serangan yang meningkat.

Penelitian ini memiliki fokus utama pada pengukuran efektivitas jaringan *SDN* ketika menerima serangan *flooding attack* secara bersamaan dalam skala yang berbeda, serta mengevaluasi peran *IDPS* dalam menjaga kestabilan jaringan. Pengujian ini dilakukan untuk mengetahui seberapa besar dampak perbedaan intensitas serangan terhadap parameter kualitas layanan jaringan (*Quality of Service/QoS*) seperti *throughput*, *jitter*, *delay*, dan *packet* loss. Berdasarkan dasar latar belakang ini penulis bermaksud mengangkat topik analisis jaringan sebagai tugas akhir dengan judul **" Analisis Jaringan Taktis Pada *Software Defined Network* (*SDN*) Dengan Menggunakan *Intrusion Detection And Prevention System* (*IDPS*) Untuk Mengevaluasi Efektivitas Keamanan Pada Jaringan ".**

1.2. Rumusan Penelitian

Berdasarkan latar belakang di atas, maka dapat diiidentifikasikan menjadi rumusan masalah pada penelitian ini yaitu:

1) Bagaimana performa jaringan *SDN* ketika menerima serangan *flooding* berbasis *SYN flood* dengan tingkat intensitas yang berbeda?
2) Sejauh mana efektivitas *Snort* versi 2 sebagai sistem *Intrusion Detection and Prevention System (IDPS*) dalam mendeteksi dan memitigasi serangan *SYN flood*?
3) Bagaimana pengaruh implementasi *IDPS* terhadap parameter *Quality of Service* (*QoS*) jaringan seperti *throughput*, *delay*, dan *packet loss* saat terjadi serangan?.

1.3. Tujuan dan Manfaat

1) Menganalisis Integritas *SDN* dengan *IDPS* ketika disimulasikan menerima serangan *SYN Flood*.
2) Mengukur efektivitas *Snort v2* dalam mendeteksi serta memitigasi serangan *SYN flood* pada jaringan *SDN*.
3) Mengevaluasi dampak penggunaan *IDPS* terhadap *Quality of Service* (QoS) dalam menghadapi *SYN Flood*.

1.4. Batasan Masalah

1) Penelitian ini hanya akan fokus pada serangan *DDos Flooding Attack*.
2) Penelitian ini hanya akan menggunakan beberapa implementasi SDN dan IDPS yang spesifik.
3) Penelitian ini hanya akan dilakukan dalam skala laboratorium dan virtual.
4) Sistem Operasi yang digunakan dalam penelitian ini menggunakan *Linux Ubuntu* dan *Windows*.
5) Penilaian analisis dengan menggunakan *Quality of Service* yang meliputi *throughput, packet loss, delay,* dan *jitter*.

1.5. Rencana Kegiatan

1) Study Literatur

   Tahap awal dilakukan dengan mempelajari teori-teori yang relevan, mencakup konsep dasar *SDN*, *IDPS*, *QoS*, dan teknik keamanan jaringan dari buku-buku, jurnal dan penelitian tugas akhir sebelumnya yang dapat membantu untuk memecahkan masalah.
2) Merancang *Topologi*

   Setelah melakukan Studi Literatur dalam penelitian ini, akan dilanjutkan dengan merancang sistem secara keseluruhan. Langkah pertama yang dilakukan adalah membuat rancangan *topologi* jaringan yang akan digunakan.
3) Konfigurasi dan Instalasi

   Setelah merancang *topologi* akan di lakukan instalasi, sebagai berikut:

   a. *Ryu SDN Setup*

Proses *instalasi Ryu*, yakni pemasangan *Ryu* pada *virtual machine Controller*. Kemudian dilanjutkan dengan konfigurasi *OVS* agar terhubung dengan *Ryu Controller*, yaitu membuat *Open vSwitch bridge* dan menetapkan *controller IP*, sehingga *OVS* bisa mengirim paket aliran trafik ke *Ryu* secara otomatis.

b. *Snort Setup*

Instalasi *Snort*, termasuk dependensi dan konfigurasi dasar, kemudian proses dilanjutkan konfigurasi *snort* seperti penambahan *rules*, serta pembuatan *Script*.

c. Integrasi *SDN* dengan *Snort*

Menghubungkan *Snort* yang bertugas mendeteksi/memblokir dengan *Ryu Controller* yang mencatat laporan. Hasil integrasi ini memungkinkan sistem mendeteksi sekaligus memitigasi serangan secara *real time*.

d. Pembuatan *Script Drop* pada *Snort*

Pembuatan *Script Drop* dengan alur *snort* akan mendeteksi serangan dan segera memanggil fungsi *ipset* dan *iptables* secara otomatis untuk melakukan mitigasi. Setela berhasil di *drop*, *snort* akan segera mengirimkan laporan *flow* ke *Ryu* bahwa telah terjadi serangan dan *snort* telah berhasil memblokirnya.

e. Pembuatan *Script Monitoring Flow* Laporan pada *Ryu*

Script Monitoring yang bertugas untuk memantau laporan dari *Snort* bila terjadi serangan tanpa perlu mengirimkan *flow drop* pada snort. Isi laporan berupa alamat *IP* penyerang, waktu penyerangan, jenis serangan, waktu terdeteksi oleh *snort* dan waktu ketika telah berhasil di drop oleh *snort*.

f. Pengujian Sistem

Melakukan simulasi serangan terhadap jaringan atau sistem yang telah dikonfigurasi untuk mengumpulkan *dataset* tentang kinerja dan keamanan sistem sebelum di terapkannya *IDPS* sebagai perangkat keamanan.

4) Pengumpulan Data dan Analisis Data

Mengumpulkan data setelah melakukan penyerangan untuk menganalisis perbedaan kinerja dan efektivitas antara sebelum dan sesudah penerapan IDPS

dan juga perbandingan ketika jenis serangan yang sama tetapi dengan mode serangan yang berbeda, yaitu serangan *flooding* menggunakan -i u10000 dan serangan minimal. Data ini akan digunakan sebagai *dataset* untuk perbandingan dengan data awal sebelum di terapkannya *IDPS* sebagai sistem keamanan. Dan juga *dataset* ini digunakan sebagai perbandingan jika jenis serangan yang sama di lakukan dengan berbeda mode serangan. Langkah selanjutnya akan di lakukannya analisis data yang telah dikumpulkan untuk mengevaluasi keefektifan *IDPS* dengan menggunakan pendekatas *Quality of Service* (*QOS*) seperti *throughput, packet loss, delay,* dan *jitter*.