BAB I PENDAHULUAN

I.1 Latar Belakang

Kemajuan dalam bidang teknologi informasi saat ini berkembang dengan sangat cepat. Hal ini juga berlaku untuk layanan internet, yang dikembangkan pada berbagai tingkat kompleksitas, desain, manajemen, dan pengoperasian. Masalah muncul ketika memiliki jenis perangkat keras dan protokol berbeda di jaringan. Dalam beberapa tahun terakhir, beberapa perusahaan besar telah memilih konsep SDN untuk memproduksi dan menggunakan perangkat keras mereka sendiri guna memfasilitasi manajemen dan pengembangan jaringan (Rahmawan et al., 2020).

SDN adalah konsep baru untuk mengkonfigurasi jaringan komputer dengan *data plane* dan *control plane* terpisah. Sebaliknya, dalam jaringan tradisional, kedua fungsi berada pada perangkat atau pengaturan yang sama. Perangkat yang memisahkan *data plane* dan *control plane* dalam SDN adalah *controller*. *Controller* memainkan peran penting dalam sistem SDN karena mereka memiliki beberapa protokol jaringan seperti *Openflow, Netconf, OF-config*, dan banyak *Controller* lainnya. Berbagai jenis *controller* yang digunakan dalam SDN mencakup RYU, POX, OpenDayLight, Maestro, dan ONOS. Setiap *controller* memiliki kekuatan dan kelemahan berbeda yang mempengaruhi kinerja jaringan (Shodiq & Prihanto, 2021).

DDoS merupakan ancaman signifikan terhadap ketersediaan jaringan, dan salah satu metode yang digunakan adalah dengan mengeksploitasi protokol *Simple Network Management Protocol* (SNMP). Dalam konteks ini, SNMP *Amplification* menjadi relevan sebagai jenis serangan yang secara langsung membanjiri target dengan lalu lintas UDP yang masif ke port SNMP (161). Berbeda dengan UDP flood pada umumnya, serangan ini ditandai dengan pengiriman sejumlah besar paket UDP yang ditujukan ke *port* SNMP dari perangkat target (Tung et al., 2020). Meskipun tidak selalu melibatkan amplifikasi respons dari server pihak ketiga, pengiriman pesan SNMP yang berulang, seperti *Get-Bulk-Request* yang meminta tabular variables dengan volume tinggi, dapat

menghasilkan respons yang signifikan dari perangkat target itu sendiri. Untuk mengatasi serangan SNMP pada SDN dilakukan penelitian dengan mengimplementasikan mitigasi dengan metode *Access Control List (ACL).*

Sebelum mitigasi dilakukan juga deteksi DDoS menggunakan berbasis *Support Vector Machine* (SVM). Menurut (Sahoo et al., 2020), SVM dikombinasikan dengan *Kernel Principal Component Analysis* (KPCA) untuk mengurangi dimensi fitur dan *Genetic Algorithm* (GA) untuk mengoptimalkan parameter, serta menggunakan fungsi kernel *Normalized Radial Basis Function* (N-RBF) untuk meningkatkan efisiensi pelatihan.

Mitigasi serangan DDoS dalam jaringan yang SDN dapat dilakukan dengan menggunakan ACL yang dinamis. Pendekatan ini melibatkan analisis paket yang masuk berdasarkan informasi headernya, seperti alamat sumber dan tujuan, serta port yang digunakan. Jika paket terdeteksi sebagai berbahaya atau berpotensi menyerang, sistem akan meningkatkan level risiko dan menolak paket tersebut, sehingga mencegah gangguan pada layanan. ACL ini berfungsi untuk membatasi akses dari *node* jahat dan mengatur lalu lintas yang diterima, dengan tujuan untuk melindungi integritas layanan. Dengan memanfaatkan pemodelan grafis dan teknik pembelajaran mesin, ACL dapat diperbarui secara otomatis untuk mengadaptasi terhadap serangan yang baru atau yang sedang berkembang, sehingga jaringan SDN dapat tetap beroperasi secara optimal meskipun dalam situasi serangan DDoS (Ramprasath & Seethalakshmi, 2021). Diharapkan dengan mitigasi ini dapat memberikan solusi serangan DDoS pada SDN.

I.2 Rumusan Masalah

Untuk perumasan masalah yang digunakan dengan topik yang dibahas pada penelitian akhir ini diantaranya:

1. Bagaimana implementasi serangan DDoS SNMP *Amplification* pada SDN?
2. Bagaimana implementasi mitigasi serangan DDoS SNMP *Amplification* dengan metode ACL pada SDN?

I.3 Tujuan Tugas Akhir

Berdasarkan rumusan masalah sebelumnya, dihasilkan tujuan penelitian sebagai berikut :

1. Mengetahui pengaruh serangan DDoS SNMP *Amplification* pada SDN.
2. Mengetahui efektifitas metode mitigasi ACL terhadap serangan DDoS SNMP *Amplification*.

I.4 Manfaat Tugas Akhir

Hasil dari penelitian yang dilakukan ini mampu memberikan manfaat baik secara teori maupun praktek, diantaranya sebagai berikut:

1. Bagi penulis, penelitian ini memberikan ilmu tambahan dalam pengembangan jaringan khususnya jaringan SDN
2. Bagi pembaca, dapat mengetahui analisis mitigasi serangan DDoS dari performa RYU *controller* pada SDN menggunakan metode ACL
3. Bagi Univeritas Telkom, dapat menambah referensi studi kepustakaan kampus.

I.5 Batasan dan Asumsi Tugas Akhir

Pada Batasan masalah penelitian ini meliputi beberapa hal pokok sebagai berikut:

1. Penelitian ini hanya sampai tahap simulasi menggunakan Mininet Emulator.
2. Pembangunan solusi tidak memperhatikan aspek biaya.
3. Penggunaan host pada topologi hanya 10 *hosts* dan 2 *switch.*
4. Pengujian performa jaringan dengan memanfaatkan *traffic* uji yang dihasilkan dari skrip sebagagai representasi kondisi nyata.

I.6 Sistematika Penulisan Tugas Akhir

Tugas akhir ini disusun dalam enam bab disertai bebrapa subbab untuk menjelaskan setiap tahapan dalam penelitian secara sistematis dan terstuktur. Tahapan ini dirancang untuk membantu pembaca memahami alur pelaksanaan dan proses penelitian secara menyeluruh. Adapun sistematika penulisan tugas akhir sebagai berikut:

1. BAB I Pendahuluan

   Bab ini menguraikan pengantar penelitian, memberikan gambaran awal mengenai konteks dan urgensi topik yang dibahas. Latar belakang menjelaskan perkembangan teknologi jaringan, khususnya SDN, serta tantangan keamanan seperti serangan SNMP *Amplification*. Perumusan masalah merangkum isu utama yang akan dijawab, yaitu implementasi serangan SNMP *Amplification* pada SDN dan mitigasinya menggunakan ACL. Tujuan penelitian dijelaskan untuk mengetahui pengaruh serangan SNMP *Amplification* dan efektivitas mitigasi ACL. Manfaat penelitian mencakup kontribusi teoritis dan praktis bagi penulis, pembaca, serta institusi. Batasan dan asumsi menetapkan ruang lingkup penelitian, seperti penggunaan simulasi Mininet dengan topologi terbatas. Sistematika penulisan memberikan peta laporan untuk memandu pembaca melalui struktur dokumen.
2. BAB II Landasan Teori

   Bab ini menyajikan dasar teoretis dan literatur yang mendukung penelitian. Bagian literatur membahas konsep-konsep kunci, dimulai

dengan SDN, yang mencakup pemisahan control plane, data plane, dan application plane, serta arsitekturnya. OpenFlow dijelaskan sebagai protokol komunikasi utama dalam SDN, diikuti dengan Ryu Controller sebagai alat pengelola jaringan. Serangan DDoS dan spesifikasinya, yaitu SNMP *Amplification*, diuraikan untuk memahami ancaman keamanan. SVM dibahas sebagai metode deteksi, sementara ACL dijelaskan sebagai mekanisme mitigasi. Mininet dan VMWare Workstation diuraikan sebagai alat simulasi. Pemilihan metode/kerangka kerja membandingkan ACL dengan metode lain seperti Rate Limiting, Firewall, dan Blacklist, dengan alasan pemilihan ACL karena kesesuaiannya dengan serangan SNMP yang prediktif. Penelitian terdahulu mengulas studi relevan untuk memperkuat posisi penelitian ini.

3. BAB III Metodologi Penyelesaian Masalah

   Bab ini memaparkan pendekatan sistematis untuk menyelesaikan masalah penelitian. Kerangka berpikir menjelaskan alur logis dari identifikasi masalah hingga solusi. Sistematika penyelesaian masalah merinci tahapan penelitian, yang mencakup metode pengumpulan data melalui observasi dan simulasi, metode pengolahan data menggunakan analisis statistik dan machine learning, serta metode evaluasi untuk mengukur keberhasilan solusi. Pendekatan ini dirancang untuk memastikan bahwa penelitian dilakukan secara terstruktur dan dapat diuji keabsahannya.

4. BAB IV Penyelesaian Permasalahan

   Bab ini menguraikan implementasi solusi secara rinci. Pengumpulan dan analisis data menjelaskan dataset yang digunakan dan pencatatan log untuk memantau lalu lintas jaringan. Perancangan sistem mencakup alur spesifikasi sistem, instalasi serta konfigurasi virtual machine, dan pengaturan Ryu Controller. Pengembangan sistem merinci arsitektur topologi jaringan, pemodelan SVM untuk deteksi serangan, implementasi mitigasi ACL, dan skenario pengujian untuk mengevaluasi performa sistem di bawah kondisi normal, serangan, dan mitigasi.

5. BAB V Validasi, Analisis Hasil, dan Implikasi

Bab ini membahas proses pengujian dan evaluasi hasil penelitian. Pengujian sistem mencakup hasil pengujian model SVM, skenario pengujian kondisi normal, skenario pengujian serangan SNMP *Amplification*, dan skenario pengujian implementasi mitigasi ACL. Evaluasi hasil pengujian menganalisis performa sistem berdasarkan metrik seperti akurasi deteksi dan efektivitas mitigasi. Dampak hasil tugas akhir menguraikan implikasi praktis dan teoretis dari penelitian, seperti kontribusi terhadap keamanan jaringan SDN dan potensi penerapannya di dunia nyata.

6. BAB VI Kesimpulan dan Saran

   Bab ini merangkum temuan utama penelitian, menjawab tujuan yang telah dirumuskan, dan menyimpulkan efektivitas solusi yang diusulkan. Saran disampaikan untuk pengembangan lebih lanjut, seperti peningkatan skala simulasi atau eksplorasi metode mitigasi lain, guna memperluas manfaat penelitian di masa depan.

7. Bagian Akhir

   Bagian ini mencantumkan semua referensi yang digunakan dalam penelitian, disusun sesuai standar penulisan akademik, untuk memastikan kredibilitas dan keabsahan sumber. Dan mencantumkan dokumen pendukung termasuk skrip kode untuk Ryu Controller, topologi jaringan, dashboard visualisasi, deteksi SVM, serta skrip untuk pencatatan lalu lintas normal dan serangan SNMP *Amplification*. Lampiran ini memberikan bukti teknis dari implementasi yang dilakukan dalam penelitian.