BAB I
PENDAHULUAN

1.1 Latar Belakang

Intrusion Detection System (IDS) dan Intrusion Prevention System (IPS) adalah teknologi keamanan yang memantau lalu lintas jaringan atau aktivitas host untuk mencari tanda-tanda akses tidak sah atau aktivitas jahat. IDS biasanya terbentuk melalui beberapa komponen yang saling bekerja sama untuk memantau, menganalisis, dan merespons potensi ancaman keamanan atau pelanggaran dalam jaringan atau sistem[1]. Pentingnya IDS dan IPS dalam keamanan jaringan tidak dapat dipandang sebelah mata. Dengan semakin canggihnya ancaman dari dunia maya, penting bagi suatu Lembaga atau organisasi untuk menerapkan langkah-langkah keamanan yang efektif untuk melindungi jaringan dan data mereka. Peretas dan penjahat siber terus-menerus mengembangkan teknik dan alat baru untuk menembus sistem keamanan yang sifatnya tradisional/terdahulu, sehingga penting bagi suatu Lembaga atau organisasi untuk memiliki teknologi keamanan canggih seperti IDS dan IPS [2].

Akhir-akhir ini penggunaan internet, jumlah data penting, data sensitif, rahasia baik individu maupun perusahaan yang melewati internet semakin bertambah. Dengan adanya celah dalam sistem keamanan, penyerang berusaha menyusup ke jaringan, sehingga mendapatkan akses ke informasi penting dan rahasia, yang dapat membahayakan pengoperasian sistem, dan juga mempengaruhi kerahasiaan data [3]. Untuk mengatasi kemungkinan serangan ini, sistem deteksi intrusi (IDS), yang merupakan cabang penting dari keamanan siber, dan dipakai untuk memantau serta menganalisis lalu lintas jaringan sehingga dapat mendeteksi dan melaporkan aktivitas berbahaya [4].

Menempatkan seorang administrator jaringan adalah tindakan pencegahan yang umum dilakukan. Karena membutuhkan waktu, administrator tidak dapat melakukan pengawasan tanpa henti. Masalah tersebut dapat diatasi dengan sistem deteksi ancaman atau gangguan jaringan (NIDS). Sistem ini merupakan suatu

teknik yang dapat digunakan sebagai pemantau lalu lintas masuk dan keluar serta lalu lintas bagian jaringan lokal atau biasa disebut lalu lintas antar host [5]. Sistem deteksi intrusi jaringan (NIDS) dapat terdiri dari perangkat keras atau sensor dan perangkat lunak atau konsol untuk mengontrol dan memantau paket lalu lintas jaringan di beberapa lokasi untuk potensi intrusi atau anomali.

Berdasarkan penelitian yang dilakukan Shah dkk., (2021) trafik protokol ICMP lebih mudah dikenali sehingga rule filtering yang diterapkan pada firewall secara otomatis mendrop paket flood tersebut. Hanya saja dalam penelitian ini belum dikembangkan Sistem Filtering yang memfilter protokol-protokol yang dapat menyebabkan serangan *flood* selain TCP, UDP, dan ICMP sehingga untuk meningkatkan Kinerja *Firewall* berbasis Filtering ini dibutuhkan sistem monitoring serangan *flood* yang lain seperti IDS dan IPS [6]. Selain itu, pada penelitian Abuswhereb dkk., (2020) yang mempelajari mengenai berbagai serangan DOS penting didapatkan hasil bahwasannya sensitifitas serangan terbesar dipegang oleh TCP-SYN dengan serangan jenis SYN yang paling bertanggung jawab atas 79,70% dari semua serangan DoS pada jaringan sehingga apabila dilakukan penelitian yang dapat mendeteksi serangan TCP-SYN nantinya akan sangat berguna di masa mendatang oleh karena itu dibutuhkan sistem monitoring seperti IDS dan IPS untuk mendeteksi serangan tersebut [7]. Hal ini didukung oleh penelitian Roslan (2023) yang mengemukakan bahwa alat terbaik untuk melakukan pemindaian port menggunakan teknik scan TCP SYN dan scan TCP *Connect* adalah Nmap. Teknik pemindaian port yang terbaik adalah pemindaian TCP SYN karena memiliki waktu respons paling rendah dan dengan demikian paling tidak berdampak pada host target. Pemindaian TCP SYN juga dikenal sebagai teknik pemindaian port yang paling tersembunyi [8].

Pada penelitian ini akan dibahas prosedur yang diperlukan untuk menginstal IDS dan IPS pada jaringan komputer beserta saran mengenai pemilihan perangkat lunak dan perangkat keras yang dapat digunakan. Kemudian dibahas cara memasukkan notifikasi menggunakan Telegram ke dalam sistem IDS. Penelitian ini bertujuan untuk mengetahui bagaimana cara teknologi IDS dan IPS bekerja

sama dalam melindungi jaringan dan penggunaan notifikasi pada Telegram dapat meningkatkan respon terhadap kemungkinan ancaman dengan memeriksa keamanan jaringan komputer. Selain itu, pada penelitian ini diharapkan dapat menjadi panduan untuk membantu administrator sistem dan pakar keamanan jaringan dalam menjaga keamanan jaringan komputer.

1.2 Rumusan Masalah

Bagaimana efektifitas IDS dan IPS untuk mendeteksi dan mencegah serangan *TCP Port Scanning* dan serangan *ICMP Flooding* serta memberikan notifikasi secara *real-time* dengan menggunakan Telegram.

1.3 Batasan Masalah

Untuk membuat ruang lingkup masalah yang diambil, maka perlu diberikan beberapa batasan-batasan masalah yang jelas agar nantinya tidak keluar dari pembahasan pada penelitian ini. Adapun Batasan masalah sebagai berikut:

1. Ruang lingkup penelitian ini hanya dilakukan berdasarkan aplikasi.
2. Perancangan IDS dan IPS menggunakan Ubuntu
3. Pengujian serangan yang digunakan TCP Port Scanning dan ICMP Flooding

1.4 Tujuan Penelitian

Tujuan yang akan dicapai oleh peneliti dalam penelitian ini adalah untuk mengetahui dan menguji efektifitas IDS dan IPS untuk mendeteksi dan mencegah serangan *TCP Port Scanning* dan serangan *ICMP Flooding* serta memberikan notifikasi secara *real-time* dengan menggunakan Telegram.

1.5 Manfaat Penelitian

1) Bagi Organisasi

   Penelitian ini dapat memberikan panduan yang berguna bagi para profesional keamanan jaringan dan administrator sistem dalam menjaga keamanan dan integritas jaringan komputer khususnya mengenai penggunaan IDS dan IPS.

2) Bagi Penulis

Manfaat bagi penulis yaitu dapat mengimplementasikan dan mengembangkan ilmu pengetahuan yang didapat selama proses perkuliahan di AMIKOM Yogyakarta, mendapat wawasan baik secara teori maupun praktek, menganalisis dan mengambil kesimpulan dari suatu permasalahan khususnya pada penggunaan IDS dan IPS.

1.6 Sistematika Penulisan

Dalam penelitian ini, penulis membagi sistematika penulis menjadi beberapa bagian sesuai dengan permasalahan masing-masing sebagai berikut:

BAB I PENDAHULUAN, Pada bab ini penulis menguraikan tentang latar belakang masalah, perumusan masalah, batasan masalah, tujuan, manfaat. sistem dan definisi istilah.

BAB II TINJAUAN PUSTAKA, pada bab ini berisi tentang uraian teori-teori yang menjadi landasan pembuatan penelitian ini. Bab ini juga menjelaskan tinjauan pustaka, kajian teori dan perangkat lunak yang digunakan.

BAB III METODE PENELITIAN, pada bab ini penulis akan menjelaskan tentang konfigurasi, serta perangkat lunak digunakan. Selain itu desain sistem yang digunakan juga dibahas bab ini.

BAB IV HASIL DAN PEMBAHASAN, pada bab ini penulis akan menguraikan hasil analisis dan perancangan yang telah selesai dibuat, apakah hasil penelitian memecahkan masalah atau tidak.

BAB V PENUTUP, Pada bab ini penulis akan memberikan kesimpulan terhadap hasil penelitian yang dilakukan dan saran bagi siapa saja yang berminat membuat atau mengembangkan jaringan atau tema yang serupa.