BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Dalam era digital yang semakin berkembang pesat, jaringan komputer menjadi infrastruktur yang sangat penting dalam mendukung berbagai aktivitas, termasuk bisnis, pendidikan, dan pemerintahan. Pertukaran data melalui jaringan membuat ketersediaan jaringan komputer dan keamanan informasi rentan terhadap serangan *cyber*. Dalam jaringan komputer, perangkat yang paling rentan adalah router, (Haeruddin, 2021).

Router merupakan perangkat infratruktur jaringan yang banyak digunakan dinegara berkembang, dimana dalam interkoneksi jaringan router difungsikan untuk memperluas jangkauan internet. Router dengan biaya rendah sering digunakan sebagai router rumah atau sebagai router inti pada infratruktur jaringan dengan kemampuan *routing* yang lebih canggih, (Ceron J. M., Scholten C., Pras A., & Santanna J., 2020).

Router yang dengan kata lain merupakan pusat kendali dari interkoneksi jaringan ini rentan terhadap serangan *cyber* seperti DoS (*Denial of Service*) dan *Brute-Force*. DoS merupakan suatu sistem serangan dimana peretas dapat melumpuhkan sistem target sehingga mengakibatkan sistem tidak berfungsi atau bahkan merusak perangkat keras, (Muhammad F., Wahidah I., & Irawan A. I., 2021). Serangan DoS ini memiliki tujuan untuk membuat jaringan router *down*

sehingga tidak mampu melayani permintaan pengguna yang memiliki hak akses yang sah. Hal ini mengakibatkan terganggunya aktivitas operasional organisasi dan menimbulkan kerugian material maupun nonmaterial.

Brute Force mengacu pada perolehan penyerangan akses admin ke kredensial server dengan akses jarak jauh sehingga peretas dapat mengeksploitasi alat administratif dan kerentanan untuk didistribusikan dan menginfeksi perangkat lain. (Reedy P., 2023). *Brute Force* dilakukan dengan cara *trial* dan *error* untuk memecahkan kata sandi, kredensial login maupun kunci enkripsi.

Berdasarkan uraian diatas maka dapat diketahui bahwa keamanan jaringan merupakan prioritas utama dalam dunia teknologi informasi. Serangan DoS dan *Brute-Force* adalah ancaman serius yang dapat mengganggu operasi bisnis dan layanan penting. Oleh karena itu, upaya untuk meningkatkan keamanan jaringan sangat relevan dan dibutuhkan.

Upaya yang dapat dilakukan untuk mengamankan suatu jaringan adalah dengan menggunakan *firewall*. *Firewall* pada router merupakan fitur yang digunakan untuk melakukan penyaringan paket data berdasarkan pengaturan yang telah ditetapkan. Metode lain yang dapat digunakan untuk mengamankan jaringan adalah dengan mengimplementasikan IDS (*Intrusion Detection System*) pada *firewall*.

IDS \adalah sebuah sistem yang digunakan untuk melakukan deteksi adanya usaha-usaha penyusupan terhadap sebuah sistem dengan melakukan pengamatan trafik data secara *real-time*. (Susanto D. J., 2019). Metode IDS digunakan untuk mendeteksi aktivitas mencurigakan dalam sebuah jaringan dimana metode IDS

akan memberikan peringatan kepada sistem atau administrator jaringan untuk membloking paket yang dicurigai seperti DoS atau *Brute-Force* menggunakan *Firewall RAW* pada MikroTik router.

WhatsApp adalah salah satu platform pesan instan yang paling banyak digunakan di dunia. Mengintegrasikan WhatsApp dalam sistem keamanan jaringan adalah langkah yang cerdas karena memanfaatkan teknologi yang sudah akrab bagi banyak orang. Notifikasi melalui WhatsApp memberikan respon yang cepat terhadap serangan. Ini adalah langkah penting dalam mengatasi serangan dan meminimalkan dampaknya. Menerima notifikasi segera memungkinkan administrator jaringan untuk mengambil tindakan yang diperlukan dengan cepat.

Melalui deteksi dini dan notifikasi segera, sistem keamanan diusulkan dapat membantu mengurangi dampak serangan DoS dan *Brute-Force* sehingga dapat menghemat waktu, sumber daya, dan uang yang mungkin dikeluarkan untuk mengatasi konsekuensi serangan.

1.2 Rumusan masalah

Berdasarkan latar belakang yang telah diuraikan diatas, maka didapatkan tiga rumusan masalah untuk melakukan penelitian ini. Pertama, bagaimana menerapkan metode IDS untuk mengamankan MikroTik router dari serangan DoS dan *Brute-Force*. Kedua, bagaimana cara menambahkan notifikasi melalui Bot WhatsApp untuk mendapatkan peringatan serangan DoS maupun *Brute-Force* pada router.

Ketiga, apakah metode IDS dapat mengoptimalkan beban CPU pada MikroTik router dari serangan DoS maupun *Brute-Force*.

1.3 Ruang lingkup

Berdasarkan rumusan masalah yang telah diuraikan diatas, maka dapat dijabarkan ruang lingkup penelitian sebagai berikut:

1. *Monitoring* MikroTik langsung dengan menggunakan Winbox pada Laptop *User* dengan sistem operasi Windows.
2. Laptop *Attacker* menggunakan sistem operasi Kali Linux.
3. *Software* Nmap digunakan *Attacker* untuk mencari celah dalam lalu lintas jaringan.
4. Jenis serangan DoS yang diakukan untuk pengujian adalah *Ping Flood* dan *Syn Flood* dengan menggunakan Hping3.
5. Penyerangan *Brute-Force* menggunakan Hydra.
6. Pengamanan MikroTik router menggunakan *Firewall RAW*.
7. Provider Bot WhatsApp menggunakan Twilio.

1.4 Tujuan penelitian

Tujuan penilitian ini adalah sebagai berikut :

1. Melakukan pengujian terhadap metode IDS sebagai metode keamanan jaringan terhadap MikroTik router.

2. Menganalisis kinerja MikroTik router terhadap serangan DoS dan *Brute-Force* sebelum ditambahkan pengamanan dengan metode IDS.
3. Menganalisis kinerja MikroTik router terhadap serangan DoS dan *Brute-Force* setelah ditambahkan pengamanan dengan metode IDS.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini antara lain:

1. Membantu meningkatkan keamanan jaringan komputer dengan menerapkan metode IDS dan penggunaan *Firewall RAW* pada MikroTik router.
2. Mengurangi dampak serangan dari DoS terhadap aktivitas operasional router.
3. Memungkinkan reaksi yang lebih cepat terhadap serangan dengan notifikasi melalui WhatsApp Bot.
4. Penelitian ini dapat digunakan sebagai sumber pembelajaran dan kesadaran keamanan jaringan.

1.6 Sistematika Penulisan

Penulisan skripsi ini dibagi atas lima bab dan masing-masing terdiri dari sub bab yaitu sebagai berikut :

BAB I : PENDAHULUAN

Bab ini berisikan uraian yang memuat tentang segala sesuatu yang melatar

belakangi penulis melakukan penelitian dan yang mendasari permasalahan yang terdiri atas latar belakang masalah, rumusan masalah, ruang lingkup, tujuan penelitian, maanfaat penelitian dan sistematika penulisan.

BAB II : TINJAUAN PUSTAKA DAN DASAR TEORI

Bab ini menjelaskan mengenai sumber data yang digunakan sebagai referensi dalam pengamanan jaringan pada router dari serangan *cyber* seperti DoS dan *Brute-Force* yang berisi teori-teori mengenai dampak yang ditimbulkan dari serangan DoS dan *Brute-Force* pada router serta pengamanan router dengan memanfaatkan fitur *firewall*.

BAB III : METODE PENELITIAN

Bab ini membahas tentang data-data dan peralatan yang diperlukan dalam penulisan dan perancangan sistem. Kebutuhan data yang meliputi kebutuhan data seperti data *input* dan data *output*. Sedangkan kebutuhan sistem meliputi sistem perangkat lunak (*software*) dan kebutuhan perangkat keras (*hardware*) serta membahas analisis perancangan sistem yang meliputi perancangan Diagram blok, topologi jaringan serta *flowchart*.

BAB IV : IMPLEMENTASI DAN PEMBAHASAN

Bab ini memuat langkah dan pembahasan yang sifatnya terpadu dan disajikan dalam bentuk gambar dan *script* dari proses pengamanan pada router yang dilakukan.

BAB V : PENUTUP

Bab ini dibagi menjadi dua sub bab yaitu, kesimpulan yang menjawab permasalahan yang dihadapi penulis dan saran yang berisi solusi alternatif untuk menyelesaikan permasalahan yang terjadi