BAB I
PENDAHULUAN

1.1 Latar Belakang

SYN Flood merupakan salah satu bentuk serangan Denial Of Service (DOS) yang mana si penyerang akan mengirimkan SYN request kepada mesin sasaran dengan tujuan memakan sumber daya dari server sehingga server susah dan tidak bisa lagi menyediakan lalu lintas yang memang benar-benar punya client, untuk kasus SYN Flood ini dia terus mengirimkan mengulangi SYN request ke semua port yang ada pada server. Client akan membuat semua SYN request tampak valid namun karena IP address adalah palsu maka tidak mungkin server untuk kemudian mengakhiri koneksi tersebut.

Perusahaan keamanan siber Kaspersky melaporkan data serangan Distributed Denial of Service (DDoS) untuk Q2 tahun 2022, Selama triwulan ke-dua tahun ini serangan DDoS mencapai level baru karena pangsa serangan cerdas dan durasi rata-rata mengalami peningkatan tajam. Dibandingkan tahun sebelumnya, rata-rata durasi serangan DDoS naik 100 kali lipat, mencapai 3.000 menit. Pangsa serangan cerdas hampir memecahkan rekor selama empat tahun, terhitung hampir 50% dari total.

Para ahli juga memperkirakan peningkatan aktivitas DDoS secara keseluruhan, terutama dengan runtuhnya cryptocurrency (mata uang kripto) baru-baru ini. Serangan Distributed Denial of Service (DDoS) dirancang untuk menghambat fungsi normal situs web atau merusaknya secara keseluruhan. Selama serangan yang biasanya menargetkan lembaga pemerintah, perusahaan ritel atau keuangan, media atau organisasi lain, korban akan kehilangan pelanggan karena situs web yang tidak tersedia dan turut berpengaruh pada reputasi mereka.

Durasi rata-rata serangan di Q2 2022 adalah 3.000 menit, atau dua hari. Ini 100 kali lebih lama daripada di Q2 2021, ketika serangan hanya berlangsung selama rata-rata 30 menit. Dibandingkan dengan Q1 2022, yang ditandai dengan durasi sesi DDoS yang belum pernah terjadi sebelumnya sebagai akibat dari

aktivitas hacktivist, angka Q2 juga menunjukkan peningkatan sebanyak tiga kali lipat. Beberapa serangan dalam kuartal terakhir berlangsung selama berhari-hari atau bahkan berminggu-minggu, sebuah rekor dibuat oleh serangan dengan durasi 41.441 menit dimana itu hampir mencapai 29 hari. [1].

Tujuan dari Penelitian ini adalah meningkatkan sistem keamanan jaringan dengan merancang dan mengimplementasikan IDPS dan Firewall Filter, dan memahami teknik-teknik cara kerja serangan SYN-Flooding pada server dan mekanisme IDPS dan Firewall Filter dalam usaha pendeteksi terhadap usaha tersebut. Manfaat dalam penelitian ini adalah membantu dalam meningkatkan sistem keamanan dan perlindungan dalam sebuah jaringan komputer.

1.2 Perumusan Masalah

Berdasarkan dari latar belakang yang telah dijelaskan pada bagian sebelumnya, maka rumusan masalah yang akan diselesaikan pada penelitian ini adalah sebagai berikut:

1. Bagaimana Mengimplementasikan Keamanan Jaringan Dengan Metode Idps Dan Firewall Filter Dari Serangan DDos (Syn-Flooding) Pada Router Mikrotik.

1.3 Maksud dan Tujuan Penelitian

1.3.1 Maksud Penelitian

Berdasarkan uraian latar belakang dan rumusan masalah diatas, maka maksud dari penelitian ini adalah membuktikan bahwa dengan menggunakan metode IDPS dan Firewall Filter bisa mencegah dari serangan SYN-Flooding.

1.3.2 Tujuan Penelitian

Tujuan penelitian yang hendak dicapai adalah meningkatkan sistem keamanan jaringan dengan merancang dan mengimplementasikan IDPS dan Firewall Filter.

1.4 Batasan Masalah

Sesuai dengan deskripsi permasalahan yang telah dijelaskan diatas,

adapun batasan permasalahan dari penyelesaian penelitian ini adalah sebagai berikut:

1. Hanya mengimplementasikan cara kerja dari serangan SYN-Flooding.
2. Menggunakan Snort Intrusion Prevention System (IDPS) dalam melakukan deteksi dan drop bila adanya serangan SYN Flooding.
3. Menggunakan jenis penyerangan SYN Flooding yang menunjukkan gambaran sederhana dalam keadaan normal dan terjadi serangan terhadap sebuah server.
4. Dengan menggunakan aplikasi telegram untuk memberikan notifikasi.
5. Untuk pengujian skripsi kali ini menggunakan software Virtualbox.

1.5 Manfaat Penelitian

Manfaat dalam penelitian ini adalah membantu dalam meningkatkan sistem keamanan dan perlindungan dalam sebuah jaringan komputer.

1.6 Metodologi Penelitian

Tahap-tahap yang dilakukan dalam penelitian ini adalah:

1.6.1 Metode Pengumpulan Data

Metode pengumpulan data diperlukan dalam mendapatkan informasi yang sesuai dengan topik penelitian yang diambil, adapun metode pengumpulan data yang akan digunakan adalah studi pustaka. Studi pustaka adalah suatu proses dalam pengumpulan bahan-bahan untuk penelitian antara lain buku, jurnal-jurnal, skripsi bahkan situs-situs di internet mengenai SYN-Flooding beserta komponen-komponennya, IDPS dan FIREWALL FILTER guna menunjang tujuan penelitian yang ingin dicapai.

1.6.2 Perancangan

Pada tahap ini akan dilakukan pengambilan data yang telah ditentukan pada analisis kebutuhan serta melakukan implementasi keamanan sesuai kebutuhan yang telah didefinisikan sebelumnya. Dengan membuat topologi jaringan dan Perancangan yang akan dibangun menggunakan metode snort untuk IDPS dan firewall filter untuk mengontrol, memfilter dan mengawasi lalu lintas data.

1.6.3 Tahap Pengujian

Pada tahapan ini penulis akan melakukan pengujian terhadap sistem keamanan jaringan yang telah dibangun. Penulis menggunakan pengujian dengan serangan yaitu SYN Flooding.

1.7 Sistematika Penulisan

Untuk lebih memahami pembahasan yang terdapat pada penelitian ini, maka penulisan materi yang akan disampaikan disusun dalam sistematika sebagai berikut.

PENDAHULUAN

Bab ini berisi mengenai latar belakang, rumusan masalah, batasan masalah, maksud dan tujuan, manfaat penelitian dan sistematika penulisan.

LANDASAN TEORI

Bab ini berisi tentang tinjauan pustaka yang menjadi rujukan serta memuat teori-teori yang dijadikan dasar penelitian ini.

ANALISIS DAN PERANCANGAN

Bab ini akan memaparkan tentang perancangan dan analisis sistem pada keamanan jaringan komputer untuk pencegahan serangan SYN-Flooding. Untuk menguji model yang diusulkan dengan menggunakan Snort pada IDPS dan firewall Filter.

IMPLEMENTASI DAN PEMBAHASAN

Bab ini berisi tentang kebutuhan sistem, data topologi dan implementasi rancangan keamanan jaringan yang telah dibuat.

PENUTUP

Bab ini berisi kesimpulan dan saran berkaitan dengan sistem keamanan, sehingga saat dapat digunakan untuk pengembangan penelitian yang serupa selanjutnya.

DAFTAR PUSTAKA

Dalam bab ini berisi tentang pustaka yang digunakan penulis sebagai acuan dan bahan dalam penelitian ini.