BAB 1 PENDAHULUAN

1.1 Latar Belakang

Keamanan jaringan telah menjadi isu kritis dalam dunia teknologi, terutama dengan perkembangan pesat dalam komunikasi dan pertukaran data. Jaringan kampus sebagai bagian integral dari lingkungan Pendidikan juga tidak terlepas dari resiko ancaman keamanan digital. Salah satu ancaman yang semakin meresahkan adalah serangan data flooding. Serangan ini dapat memiliki dampak serius terhadap ketersediaan dan keandalan layanan jaringan, yang pada akhirnya memengaruhi produktivitas dan operasional Lembaga Pendidikan.

Seramgam data flooding, termasik dalam kategori Denial of Service (DoS) atau Distributed Denial of Service (DDoS), melibatkan pengiriman lalu lintas yang berlebihan ke infrastruktur jaringan target. Akibatnya, sumber daya jaringan menjadi terbebani dan layanan yang seharusnya dapat diakses oleh pengguna menjadi tidak tersedia. Dalam kasus jaringan kampus, serangan data flooding dapat mengganggu aktifitas mahasiswa, dosen, dan staff ke sumber daya online, sistem informasi akademik, dan layanan penting lainnya.

Kebutuhan akan akses internet semakin meningkat. Banyak juga Lembaga Pendidikan yang menggunakan internet sebagai sarana untuk membantu dalam kegiatan belajar mengajar. Internet memberikan kemudahan dalam kominikasi dan transmisi data. Selain memiliki banyak kelebihan, internet juga memiliki banyak kekurangan. Salah satu kelemahan internet adalah dalam hal keamanan siber. Serangan terhadap system keamanan siber merupakan hal yang umum akhir-akhir ini. Jenis serangan yang terjadi adalah DoS (Denial of Service) [1].

Flooding attack adalah serangan yang dilakukan dengan megirimkan permintaan (*request)* yang berlebihan ke server sehingga tidak dapat menerima permintaan bahkan dapat mengakibatkan hang dan crash. Akibar dari kejadian ini, jaringan komputer tidak lagi berfungsi seperti yang diharapkan, dampak serangan tersebut menghabiskan sumber daya, menghabiskan RAM, dan memenuhi hardisk

dengan data yang tidak perlu, sehingga mengganggu semua aktivitas, dan tidak dapat lagi memenuhi permintaan yang ambigu[2].

Flooding Data adalah sejenis serangan Denial of Service (DOS), dimana flooding data melakukan serangan terhadap sebuah komputer atau *server* di dalam jaringan lokal maupun internet dengan cara menghabiskan sumber (resource) yang dimiliki oleh komputer tersebut sampai komputer tersebut tidak dapat menjalankan fungsinya dengan benar [3].

Beberapa macam bentuk pendeteksi data flooding menggunakan beberapa metode seperti Blokir IP dan Port dan Wireshark sebagai alat untuk pemantauannya [4]. Penerapan filter firewall pada router mikrotik juga dapat mengurangi jumlah paket data UDP yang dikirim oleh attacker melalui port DNS sebanyak 60% dari jumlah paket yang masuk jika tanpa firewall [1]. Snort dan Firewall memiliki peran yang berbeda dalam keamanan jaringan. Snort lebih berfokus pada deteksi serangan dan analisis mendalam, sementara firewall memberikan perlindungan umum dengan penghalangan akses dan pemisahan jaringan. Namun, pada penilitian kali ini penulis akan membuat pendeteksi IDS dengan Tools Snort dan Bot Telegram sebagai penunjang penelitian ini.

Dalam konteks ini, penelitian akan memfokuskan pada pengembangan dan implementasi sistem pendeteksi data flooding menggunakan Snort dengan studi kasus pada jaringan kampus. Studi kasus ini akan memberikan pandangan yang lebih mendalam tentang cara kerja sistem pendeteksi dalam lingkungan nyata, serta menggambarkan tantangan dan keberhasilan dalam melindungi infrastruktur jaringan kampus dari data flooding.

Penelitian ini bertujuan untuk mendeteksi sebuah sistem traffik jaringan dan memonitoring adanya peringatan flooding data pada jaringan komputer secara terstruktur sehingga dapat memberikan kenyamanan bagi pengguna yang akan menggunakan sebuah jaringan. Penelitian ini menggunakan metode IDS dan tools Snort sebagai sarana untuk pendeteksian. Komputer IDS akan terhubung dengan jaringan dan memantau lalu lintas jaringan berdasarkan label data. IDS berjalan dengan adanya sebuah aturan. Snort adalah sebuah teknologi sensor pendeteksi terhadap penyalahgunaan pada jaringan. Snort juga memiliki Rules sebagai aturan

yang dapat membantu menentukan aktivitas jaringan. Ketika komputer server berhasil merekam kejadian, maka kejadian tersebut akan masuk kedalam log yang telah tersedia pada Snort. Lalu lintas tersebut dapat di monitoring oleh administrator jaringan ketika adanya flooding data dengan mengirim pesan melalui Bot Telegram. Bot telegram digunakan sebagai media untuk memonitoring adanya flooding. Penerapan system monitoring flooding data ini berjalan dengan ouput berupa notifikasi Telegram. Telegram adalah sebuah aplikasi perpesanan ponsel dan komputer, yang berbasis penyimpanan awan yang fokus pada keamanan dan kecepatan. Berdasarkan hal tersebut dalam tugas akhir ini dibuatlah sistem yang mampu mendeteksi serta memonitoring sebuah lalu lintas jaringan yang mengalami flooding data maupun tidak yang berupa output notifikasi Telegram.

1.2 Rumusan Masalah

Berdasarkan permasalahan yang telah dijelaskan pada latar belakang diatas, maka pada penelitian ini didapatkan suatu rumusan masalah yaitu :

1. Bagaimana membangun sebuah sistem untuk mengurangi atau mencegah terjadinya *flooding* data pada jaringan?
2. Metode seperti apa yang dapat mencegah atau mengurangi terjadinya DoS berupa *flooding* data pada Jaringan IT Telkom Surabaya?
3. Output seperti apa yang dihasilkan ketika sudah melakukan sebuah pendeteksian terjadinya *flooding* data?
4. Bagaimana tingkat efektivitas sistem dalam mengatasi atau melindungi jaringan IT Telkom Surabaya?

1.3 Tujuan dan Manfaat

Berdasarkan latar belakang dan rumusan masalah yang disebutkan, maka tujuan dilakukannya penelitian ini adalah

1. Membangun sistem pendeteksi flooding data pada jaringan IT Telkom Surabaya menggunakan software Snort yang berbasis *Host-based IDS.*

2. Mengembangkan metode untuk mencegah dan mengurangi terjadinya DoS berupa flooding data.
3. Memberikan Output berupa notifikasi pada telegram guna memudahkan *administrator* untuk memantau trafik jaringan
4. Mengukur tingkat efektivitas sistem dalam mengatasi atau melindungi jaringan IT Telkom Sruabaya dengan menggunakan Snort Efficiency

Berdasarkan tujuan diatas, penelitian ini diharapkan mampu memberikan manfaat seperti :

1. Dapat mendeteksi terjadinya *flooding data* pada jaringan IT Telkom Surabaya
2. Dapat memantau trafik lalu lintas jaringan dengan mudah menggunakan aplikasi Bot Telegram.
3. Dapat mengetahui keberhasilan dari tools snort dalam mendeteksi adanya sebuah percobaan serangan.

1.4 Batasan Masalah

Agar pembahasan dalam penelitian ini tidak meluas, maka diberikan batasan masalah sebagai berikut:

1. Jenis serangan *flooding* memiliki banyak macam, oleh karena itu dalam penelitian ini dibatasi pada pendeteksian serangan *SYN TCP Flood*, *UDP Flood,* dan *ICMP Flood.*
2. Metode yang diterapkan dalam pencegahan memiliki banyak macam, oleh karena itu dalam penelitian ini menggunakan metode IDS dengan tools Snort
3. Output yang dihasilkan adalah berupa notifikasi pada aplikasi telegram menggunakan API Bot Telegram

1.5 Metodologi Penelitian

a. Identifikasi masalah

Identifikasi masalah merupakan tahapan awal dalam sebuah penelitian yang berisikan penjelasan mengenai masalah dan membuat penjelasan yang dapat diukur.

Identifikasi masalah juga dapat dikatakan sebagai upaya untuk mendefinisikan suatu masalah penlitian Dengan mengidentifikasi sebuah ancaman serangan data flooding sebagai masalah keamanan pada jaringan kampus dan menyadari urgensi perlunya sistem pendeteksi yang efektif untuk mengatasi masalah tersebut

b. Studi literatur

Studi literatur adalah tahapan untuk mempelajari dan memahami dari beberapa sumber misalnya jurnal, artike, buku atau teori dari penelitian sebelumnya. Studi literatur dilakukan dengan tujuan agar penulis mendapatkan pemahaman yang lebih mengenai topik yang diangkat.

c. Perancangan.

Perancangan merupakan tahapan yang berisikan rancangan arsitektur jaringan yang akan digunakan. Pada tahapan ini bertujuan untuk memudahkan proses konfigurasi dan simulasi agar berjalan dengan baik.

d. Simulasi Penelitian

Simulasi merupakan tahapan menerapkan hasil dari perancangan yang telah dibuat. Tahapan simulasi ini dilakukan dengan menggunakan perangkat lunak Virtualisasi yaitu Virtual Box dengan Sistem Operasi Linux Ubuntu.

Konfigurasi pada metode yang akan digunakan. IDS (*Intrusion Detection System)* dan tools Snort yang akan dikonfigurasikan pada penelitian ini, Konfigurasi berisikan tahapan untuk mempersiapkan proses simulasi.

e. Pengujian

Pengujian adalah tahapan dimana dilakukan pengecekan terhadap sistem yang telah dibuat untuk mengetahui tingkat keberhasilan dari sistem tersebut. Pengujian akan dilakukan menggunakan aplikasi telegram dengan melihat hasil.

f. Analisa hasil

Analisa hasil adalah tahapan dimana dari hasil pengujian yang telah dilakukan akan dianalisa guna mengetahui seberapa baik metode yang diterapkan.