BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan globalisasi saat ini telah membawa kemajuan teknologi yang pesat , dimana dunia informasi telah berpengaruh terhadap majunya bidang informatika terutama pada berkembangnya internet. Hingga saat ini perkembangan internet tidak luput dari berbagai macam kejahatan *cyber* , salah satunya adalah serangan *Brute Forces*. *Brute Forces* adalah serangan yang dilakukan untuk membobol password dengan cara mencoba setiap password secara acak dari kombinasi huruf, angka dan simbol, sampai akhirnya menemukan password yang tepat. Serangan *Brute Forces* juga bisa dilakukan melalui *file transfer* (*FTP*) , *SSH* , dan juga paket *ICMP flood (DDoS)* .

Dengan maraknya serangan pada perangkat jaringan komputer , diperlukan suatu sistem yang dapat mendeteksi dan melakukan monitoring serangan pada perangkat jaringan yang pada penelitian ini peneliti menggunakan contoh objek *router* MikroTik. Sistem monitoring serangan pada jaringan komputer umumnya hanya bisa mendeteksi berbagai jenis serangan tetapi tidak bisa mengambil tindakan yang lebih lanjut atau harus ditangani secara manual. Maka dari itu butuh pengamanan secara *realtime* dan efektif . Kombinasi antara sistem pencegahan serangan (*IPS*) dan deteksi serangan (*IDS*) sangat tepat untuk membantu pengamanan sebuah jaringan komputer. Sistem pencegahan serangan (*IPS*) bekerja secara otomatis setelah sistem deteksi (*IDS*) melacak adanya serangan pada jaringan komputer .

Bedasarkan permasalahan dari paragraf sebelumnya penulis membuat penelitian yang berjudul "*Perancangan Sitem Monitoring dan Pencegahan Serangan Brute Forces Pada Mikrotik Berbasis Bot Telegram*" dengan menggunakan beberapa parameter seperti rule firewall, scheduler, dan script sebagai acuan keberhasilan sistem yang penulis bangun. Rancangan sistem ini akan melakukan pengiriman notifikasi saat terjadi serangan jaringan ini tergantung pada interval sistem *scheduler* setelah *IDS/IPS (Intrusion Detection and Prevention System)* yang sudah terkonfigurasi dalam *Firewall Rule* perangkat MikroTik akan melakukan aksi melacak dan memblokir ip address penyerang .

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas , Rumusan masalah yang dapat di definisikan dalam penelitian ini adalah sebagai berikut :

1. Bagaimana cara kerja sistem pencegahan dan pendeteksi *IDS/IPS* serangan *Brute Force* pada perangkat MikroTik berbasis bot Telegram ?
2. Berapa waktu yang dibutuhkan *IDS/IPS* pada *Firewall Rule* di perangkat MikroTik untuk mendeteksi dan melakukan aksi pencegahan saat terjadi serangan *Brute Force* pada router MikroTik ?
3. Apakah sistem monitoring dan pencegahan serangan yang dibangun dapat berjalan memenuhi proses yang diinginkan dalam menjalankan sistem secara fungsional?

1.3 Batasan Masalah

Pada penelitian ini batasan masalah dibuat dengan tujuan membatasi pembahasan masalah agar tidak meluas dan tetap berfokus pada bidang yang dibahas , maka batasan masalahnya sebagai berikut :

1. Proses uji sistem notifikasi *bot telegram* dilakukan melalui perangkat berbasis komputer *desktop* dengan sistem operasi *Windows 10* dan *virtual machine (Virtual Box)* yang memiliki sistem operasi *Kali Linux*.
2. Notifikasi serangan akan diterima jika komputer administrator yang digunakan terhubung oleh internet melalui jaringan kabel lokal (*LAN*) .
3. Uji coba serangan dilakukan dalam satu lingkup jaringan nirkabel lokal (*WLAN*).
4. Sistem deteksi dan pencegahan (*IDS/IPS*) diimplementasikan dalam *Firewall Rule* pada perangkat MikroTik.

1.4 Tujuan Penelitian

Penelitian ini memiliki tujuan sebagai berikut :

1. Sebagai syarat untuk menyelesaikan pendidikan program strata 1 Teknik Informatika di Universitas Amikom Yogyakarta .
2. Mengoptimalkan penggunaan aplikasi media sosial sebagai sarana monitoring perangkat jaringan MikroTik.
3. Mengetahui seberapa efektif aplikasi *Telegram* dapat memperoleh data berupa output notifikasi serangan *bruteforce* pada suatu jaringan *LAN* .

1.5 Manfaat Penelitian

Penelitian ini memiliki beberapa manfaat yang dapat diperoleh , yaitu sebgai berikut :

1. Mempermudah admin jaringan dalam mendapatkan notifikasi apabila terjadi serangan pada sebuah perangkat MikroTik melalui sebuah *Bot Telegram* .
2. Memberikan informasi kepada pembaca tentang perancangan sistem monitoring dan pencegahan serangan pada MikroTik berbasis *Bot* aplikasi *Telegram* .
3. Sebagai referensi pembaca jika ingin melakukan penelitian lebih lanjut dengan tema yang sama .

1.6 Alur Penelitian

1.6.1 Pengumpulan Data

Pengumpulan data menggunakan studi literatur dari beberapa sumber jurnal penelitian terdahulu dengan tema yang sama yaitu tentang keamanan jaringan sebagai rujukan dan acuan dalam penulisan laporan skripsi ini. Selain dari jurnal peneliti juga mendapatkan data melalui artikel-artikel yang ada dari berbagai *website* .

1.6.2 Analisis dan Perencanaan

Setelah mendapatkan data dari berbagai sumber yang valid , peneliti melakukan analisis data guna melakukan perencanaan dalam membuat penelitian ini. Perencanaan meliputi menentukan kebutuhan fungsional dan non fungsional untuk menunjang proses penelitian. Selanjutnya peneliti melakukan desain topologi jaringan dan merancang skenario pengujian agar mendapat hasil yang sesuai dengan batasan dan tujuan penelitian.

1.6.3 Implementasi dan Pengujian

Implementasi dilakukan bedasarkan perencanaan dan skenario pengujian yang sudah ditentukan. Pada tahap ini peneliti melakukan instalasi seluruh perangkat keras dan lunak beserta konfigurasinya sesuai dengan desain topologi. Setelah semua proses instalasi selesai akan dilakukan skenario pengujian serangan *brute forces* agar mendapatkan hasil data *output* untuk menyimpulkan hasil dari penelitian ini.

1.6.4 Penulisan Laporan

Penulisan laporan dilakukan sebagai bukti telah dilaksanakannya penelitian ini dan membuahkan hasil. Laporan penelitian ini diharapkan dapat dijadikan acuan dalam melakukan pengembangan bagi para peneliti selanjutnya yang akan mengambil tema yang sama.

1.7 Sistematika Penulisan

Untuk mempermudah dalam penyusunan laporan penelitian ini maka peneliti menggunakan sistematika penulisan secara sederhana yang terdiri dari :

BAB I PENDAHULUAN

Bab ini membahas tentang latar belakang mengapa dipilihnya topik permasalahan penelitian ini , rumusan masalah , batasan masalah , tujuan dan manfaat penelitian serta sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini berisi tentang berbagai teori sebagai dasar penulisan yang yang meliputi perancangan penelitian seputar dasar jaringan komputer hingga pembahasan teori mengenai keamanan jaringan.

BAB III PERANCANGAN PENELITIAN

Dalam bab ini menguraikan tentang tinjauan umum seputar penelitian ini , analisis kebutuhan , serta rencana kerja dari penelitian ini.

BAB IV IMPLEMENTASI DAN PEMBAHASAN

Bab ini menjelaskan tentang hasil implementasi dan pembahasan dari hasil implementasi *IDS/IPS* pada *router* MikroTik serta pengujian notifikasi serangan melalui *bot* Telegram.

BAB V PENUTUP

Bab ini beriai tentang kesimpulan dan saran dari bab-bab sebelumnya yang berdasar pada rumusan dan batasan masalah dalam penelitian ini . Saran diberikan dengan harapan menjadi pengembangan untuk penelitian selanjutnya serta sebagai penyempurnaan dari hasil penulisan peneliti.

DAFTAR PUSTAKA

Berisi tentang referensi yang digunakan peneliti sebagai acuan dan studi pustaka dalam bembuatan laporan skripsi ini .

LAMPIRAN