BAB I

LATAR BELAKANG

1.1 Latar Belakang Masalah

Dalam perkembangan teknologi yang semakin pesat, kebutuhan akan keamanan jaringan tentunya meningkat seiring dengan berkembangnya ilmu pengetahuan tentang masalah *hacking* dan *cracking* yang bersifat *free* dan ada pula yang dikomersilkan. Kemudian dari sisi *software* pendukung pun sudah banyak *tools* yang bersifat *free* yang kemampuannya sudah bisa dikatakan mumpuni untuk digunakan sebagai alat penyerangan oleh kalangan *attacker*.

Pada sisi lain timbul masalah serius yaitu faktor keamanannya, namun disatu sisi manusia sudah sangat tergantung dengan sistem informasi. Hal itu yang menyebabkan statistik insiden keamanan jaringan terus meningkat tajam dari tahun ke tahun. Ini disebabkan karena kepedulian masyarakat yang sangat kurang terhadap sistem keamanan jaringan

Keamanan jaringan lokal ini bergantung sepenuhnya terhadap bagaimana seorang *network administrator* merespon dengan cepat sebuah serangan yang terjadi. Tapi *network administrator* hanyalah seorang manusia yang terbatas akan waktu. Seorang *network administrator* tidak dapat mengawasi seluruh jaringan secara terusmenerus. Maka dari itu dibutuhkan sebuah sistem yang dapat membantu *network administrator* untuk digunakan sebagai mengetasi segala macam serangan. Pada permasalahan tersebut, pada penelitian ini akan dibuat sebuah aplikasi yang dapat membantu *network administrator* dalam *memonitoring server*, aplikasi ini bertujuan untuk mempermudah *network administrator* dalam mengamankan *server* dari berbagai macam jenis serangan *(ddos, scaning , brute force)*.

Selain itu aplikasi ini terhubung dengan fitur bot yang dimiliki oleh aplikasi *chat* telegram, yang berfungsi sebagai *command and control* pada server. Setiap serangan yang terdeteksi akan dikirim melalui telegram, sehingga *network administrator* dapat mengetahui serangan apa saja yang terjadi pada *server* ditambah dengan fitur bot dari telegram yang berfungsi sebagai *command and control* yang digunakan untuk memerintah *server* untuk melakukan pencegahan / *bloking*.

1.2 Rumusan Masalah

Dalam perkembangan teknologi sekarang yang sudah semakin pesat, kebutuhan akan keamanan jaringan tentunya meningkat seiring dengan berkembangnya ilmu pengetahuan tentang masalah *hacking* dan *cracking* yang bersifat free dan ada pula yang dikomersilkan. Kemudian dari sisi software pendukung pun sudah banyak tool-tool yang bersifat free yang kemampuannya sudah bisa dikatakan mumpuni untuk digunakan sebagai alat penyerangan oleh kalangan attacker. Serangan-serangan tersebut dapat melumpuhkan server. Sehingga dapat menimbulkan kerugian.

1.3 Batasan Masalah

Batasan masalah pada penelitian ini adalah:

1. Membutuhkan kapasitas memori yang cukup besar.
2. Berjalan sistem operasi linux .
3. Hanya bisa melakukan monitoring pada satu *interface network* saja..
4. Hanya mendeteksi serangan (DDoS, Scanning, Brute Force)

1.4 Hipotesis

Dengan menggunakan rule deteksi yang didapatkan dengan pengolahan datasheet akan ditemukan fitur serangan yang mempunyai ciri-ciri masing-masing dalam jenis serangan, hal ini akan mempermudah dalam melakukan deteksi serangan tersebut, dikarenakan semua jenis serangan akan dibedakan dari masing masing fitur serangan yang telah ditentukan. Dalam mendeteksi serangan diharapkan sekurang-kurangnya 70%

1.5 Tujuan Penelitian

Tujuan dari penelitian tugas akhir ini adalah membuat sebuah aplikasi yang digunakan untuk membantu *sysadmin* dalam memonitoring serangan-serangan yang terjadi pada *server*, baik dalam proses pencegahan dan pendektesian terhadap serangan yang mempu membahayakan *server*.

1.6 Metode Penyelesain Masalah

Metode penelitian yang digunakan:

1. STUDI LITERATUR.
   Melakukan pencarian refrensi mengenai telegram bot dan pengolahan data trafik jaringan berdasarkan serangan yang diperlukan.

2. PENGUMPULAN DATA.
   Pada tahap ini, dilakukan pengumpulan data training yang akan diolah menggunakan algoritma Decision Tree. Data training dikumpulkan menggunakan scapy. Data Training pada serangan DDoS, Brute Force dan Scanning masing-masing berjumlah 5 juta data.

3. PERANCANGAN KEBUTUHAN SISTEM.
   Melakukan perancangan sistem deteksi untuk mendeteksi serangan DDoS, Brute Force dan Scanning serta dapat di integrasikan terhadap library scapy

4. PENGUJIAN SISTEM.
   Pada tahap ini sistem yang telah dibangun akan diuji berdasarkan hasil analisa dari algoritma decision tree yang menghasilkan fitur dan rules serangan..Hasil dari pengujian tersebut, diantaranya adalah kemampuan sistem untuk menghasilkan tree berdasarkan jumlah data training yang ditentukan dan kemampuan sistem untuk mendeteksi serangan berdasarkan fitur dan rules serangan yang di inputkan kedalam sistem deteksi.

5. ANALISA HASIL PENGUJIAN.
   Pada tahap analisis hasil pengujian, dilakukan perbandingan trafik serangan terhadap jumlah keseluruhan trafik. Hasil dari analisis tersebut, diantaranya adalah akurasi untuk mendeteksi serangan.

6. PENYUSUNAN LAPORAN TUGAS AKHIR.
   Pada tahap ini semua data dan hasil dari penelitian akan dibuat menjadi sebuah laporan dengan sistematika penulisan yang sesuai dengan ketentuan institusi.

1.7 Sistematika Penulisan

BAB I : PENDAHULUAN

Pada bab ini dijelaskan latar belakang, rumusan masalah, batasan, tujuan, manfaat, keaslian penelitian, dan sistematika penulisan.

BAB II : TINJAUAN PUSTAKA DAN LANDASAN TEORI

Pada bab ini dijelaskan teori-teori dan penelitian terdahulu yang digunakan sebagai acuan dan dasar dalam penelitian.

BAB III : METODOLOGI PENELITIAN

Pada bab ini dijelaskan metode yang digunakan dalam penelitian meliputi langkah kerja, pertanyaan penilitian, alat dan bahan, serta tahapan dan alur penelitian.

BAB IV : HASIL DAN PEMBAHASAN

Pada bab ini dijelaskan hasil penelitian dan pembahasannya.

BAB V : KESIMPULAN DAN SARAN

Pada bab ini ditulis kesimpulan akhir dari penelitian dan saran untuk pengembangan penelitian selanjutnya.