BAB I

PENDAHULUAN

1.1 Latar Belakang

Dalam era teknologi informasi yang pesat saat ini, keamanan informasi sangatlah penting terlebih lagi pada suatu jaringan yang terkoneksi dengan internet. Perkembangan teknologi informasi sayangnya tidak diikuti dengan perkembangan keamanan yang memumpuni pada sistem itu sendiri dengan demikian cukup banyak sistem jaringan yang lemah dan harus ditingkatkan keamanannya, tidak luput dengan masuknya spam-spam sampai yang merusak suatu jaringan tertentu, hal ini akan sangat merugikan bagi si korban. Saat ini begitu banyak cara untuk melakukan serangan terhadap suatu sistem jaringan, cara-cara ini terus berkembang dari awal era perkembangan teknologi sampai sekarang ini.

Dahulu untuk melakukan suatu serangan membutuhkan pengetahuan dan pemahaman teknis IT yang tinggi, akan tetapi saat ini sangat mudah untuk melakukan serangan bukan hanya kepada orang yang mempunyai keahlian yang tinggi tapi juga bisa hanya dengan mereka yang ingin mencari tahu atau hanya sekedar mencoba, dikarenakan metode dan alat-alat yang digunakan semakin banyak dan mudah dioperasikan bahkan terhadap sistem keamanan jaringan. Serangan yang sering dilakukan seperti *DDoS Attack, Port Scanning, Sniffing, FTP brute force, SQL Injection, Malware, Phishing, Exploit, spaming, HackWeb, Hacking* dsb.

Dampak yang dihasilkan dari berbagai macam serangan yang di timbulkan beragam tentunya akan sangat merugikan bagi si korban, serangan bisa diartikan sebagai ancaman yang jelas, *server down*, pencurian berkas penting, pencurian uang, sampai dengan merusak suatu *system* sendiri itulah akibat umum yang dihasilkan serangan di jaringan *internet*. Sama halnya dengan virus, serangan akan semakin berkembang setiap waktunya, oleh karena itu diperlukan solusi untuk menangani serangan yang semakin berkembang ini.

Dengan Menggunakan *Intrusion Detection System* (IDS) snort merupakan salah satu solusi untuk menangani serangan-serangan tersebut. Snort merupakan aplikasi open source yang dapat berjalan dengan baik di banyak platform, salah satunya pada sistem operasi linux, snort sendiri sudah mendukung *software* web based, salah satunya adalah *base*. Dalam penelitian ini penulis akan membangun *system monitoring* jaringan yang akan mendeteksi serangan-serangan yang masuk pada jaringan yang terhunung pada *server linux*, sehingga seluruh paket yang masuk kedalam jaringan tersebut akan dibandingkan oleh *detection engine* apakah sesuai dengan *rules* atau tidak. Apabila sesuai dengan *rules* maka akan memberikan informasi berupa *telegram messages* kepada *administrator* jaringan bahwa telah terjadi sebuah serangan, jika tidak sesuai dengan rules maka paket dapat diteruskan masuk kedalam jaringan.

Berdasarkan masalah dan tinjauan di atas penulis mengambil sebuah judul "Rancang Bangun Sistem *Monitoring* Keamanan Jaringan menggunakan IDS snort melalui *Bot* Telegram di Linux Ubuntu 16.04 LTS 1"

1.2 Rumusan Masalah

Perumusan masalah yang menjadi acuan dalam penelitian tugas akhir ini adalah:

1. Bagaimana melakukan implementasi *Intrusion Detection System* (IDS) Snort menggunakan sistem operasi berbasis Linux?.
2. Bagaimana cara melakukan *Monitoring Security System* Pada server Linux Ubuntu 16.04 LTS 1?.
3. Bagaimana cara kerja *Intrusion Detection System* (IDS) snort bila terjadi serangan?
4. Bagaimana memantau keamanan terhadap serangan yang datang dengan *Bot Telegram*.

1.3 Batasan Penelitian

Batasan masalah dalam tugas akhir ini adalah:

1. *Server* menggunakan sistem operasi Ubuntu *server* 16.04 LTS 1.
2. Jaringan yang diuji hanya sebatas lingkup *Local Network*.
3. Menggunakan 2 perangkat *computer* dimana salah satu menjadi computer si penyerang menggunakan System Operasi Kali Linux dan satunya sebagai computer server menggunakan Ubuntu *server* 16.04 LTS 1 yang sekaligus menjadi tempat sistem IDS.
4. Menggunakan *tools* IDS Snort.
5. Server hanya melakukan pemantauan dan pencegahan penyerangan.

6. Serangan yang digunakan dalam pengujian adalah DDoS *Attack*, *port scanning*, *SSH brute force* dan FTP *bad login*.
7. Bot Telegram hanya mengirimkan notifikasi serangan.

1.4 Maksud dan Tujuan Penelitian

Berdasarkan perumusan masalah maka tujuan penelitian tugas akhir ini adalah:

1. Dapat melakukan implementasi *Intrusion Detection System* (IDS) Snort menggunakan sistem operasi berbasis Linux.
2. Dapat melakukan analisis *Monitoring Keamanan* pada Server Linux Ubuntu 16.04 LTS 1.
3. Dapat memahami cara kerja dari *Intrusion Detection System* (IDS) Snort.
4. Dapat melakukan pengecekan dan pemberitahuan serangan pada server melalui telegram di *smartphone*.
5. Sebagai syarat kelulusan pada prodi SI Informatika.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini adalah:

1. Bagi Peneliti
   a. Membuat karya tulis penelitian yang bermanfaat.
   b. Memberi pengalaman dan pemahaman dalam merancang dan membangun sistem monitoring jaringan pada sistem operasi Linux.
2. Bagi Pembaca
   a. Sebagai referensi untuk penelitian-penelitian selanjutnya.
   b. Dijadikan sebagai bahan pembelajaran.

1.6 Metode Penelitian

Metode penelitian yang akan penulis gunakan dalam penelitian ini adalah sebagai berikut :

1. **Studi Pustaka**

   Studi pustaka merupakan jenis metode yang dilakukan untuk mengumpulkan data dengan cara membaca dan mempelajari buku-buku dan jurnal penelitian sebelumnya yang berhubungan dengan topik permasalahan unutuk digunakan sebagai referensi.

2. **Perancangan dan Desain Jaringan**

   Perancangan dan desain jaringan dilakukan untuk meletakkan posisi Snort yang berada pada server Ubuntu 16.04 LTS 1 yang terhubung dengan jaringan Local yang telah di desain.

3. **Pembuatan Sistem**

   Pada tahap ini dilakukan *update* dan *upgrade Kernel*, instalasi paket pedukung *snort*, konfigurasi DAQ (*Data Acquisition Library*), konfigurasi *snort*, konfigurasi rules snort, konfigurasi database snort, konfigurasi *barnyard2*, konfigurasi *adodb*, konfigurasi *base*, konfigurasi *Mysql*, *Apache server*, konfigurasi statistik serangan dan yang terakhir adalah konfigurasi *trigger send message* API Telegram.

4. **Pengujian Sistem Keamanan**

   Pada tahap ini Pengujian dilakukan dengan dua tahap berbeda, yang pertama adalah skenario penyerangan menggunakan sistem operasi *linux kali* dimana diharapkan setiap serangan akan terdeteksi oleh sistem IDS *snort* dan

dikirimkan ke *telegram* sehingga seorang *administrator* dapat mengetahuinya, pengujian yang kedua adalah dengan mengimplementasikan sistem IDS *snort* kedalam topologi jaringan yang sebenarnya dan akan ada serangan dari 10 *IP Add* yang berbeda, diharapkan sistem IDS snort mampu menangkap serangan yang masuk dari luar yang akan diteruskan ke notifikasi telegram. Serangan hanya dibatasi empat tipe serangan antara lain, *Port Scanning, FTP Bad Login, SSH brute force dan DDoS* .

1.7 Sistematika Penulisan

Untuk memperoleh gambaran yang lebih mudah dimengerti mengenai isi dalam skripsi ini, sistematika penulisan skripsi ini ditulis dengan menguraikan bab secara *global* yang dapat dilihat sebagai berikut :

1.7.1 BAB I PENDAHULUAN

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

1.7.2 BAB II LANDASAN TEORI

Bab ini berisi penjelasan mengenai landasan teori yang digunakan diantaranya tinjauan pustaka, konsep dan teori serta perangkat lunak yang akan digunakan dalam perancangan dan pembangunan *system monitoring* menggunakan *snort* pada penelitian ini.

1.7.3 BAB III METODE PENELITIAN

Bab ini berisi Metode Penelitian berupa rancangan dan design sistem yang nantinya akan dibangun oleh penulis dalam penelitiannya.

1.7.4 BAB IV IMPLEMENTASI DAN PEMBAHASAN

Bab ini berisi penjelasan mengenai tahapan pembangunan sistem, implementasi metode, hasil *testing system*, dan pembahasannya.

1.7.5 BAB V PENUTUP

Bab ini berisi penjelasan mengenai kesimpulan dan saran yang diperoleh dari pembahasan pada bab sebelumnya.

1.7.6 DAFTAR PUSTAKA

Alamat referensi.

1.7.7 LAMPIRAN

Lembar Tambahan berupa data *quisioner*.