BAB I

PENDAHULUAN

1.1 Latar Belakang

Dalam perkembangan teknologi sekarang sudah sangat maju dalam bidang Pendidikan maupun usaha, seiring dengan majunya teknologi dan informasi sekarang banyak orang dalam perusahaan menggunakan seperangkat alat teknologi yang bertujuan agar bisa meningkatkan laju suatu organisasi agar menjadi lebih baik. Adanya kemajuan teknologi sekarang, banyak orang yang sudah sangat bergantung dengan teknologi khusnya pada jaringan komputer untuk pekerjaan sehari-hari. Dibalik penggunaannya yang bermanfaat, ada pula suatu kejahatan yang bisa dilakukan oleh orang atau organisai tertentu dengan memanfaatkan suatu kemajuan teknologi jaman sekarang untuk merusak suatu keamannya sehingga menjadi rawan tindak kriminal, alhasil banyak yang dirugikan. Kejadian ini tentunya terjadi karena kurang pedulinya terhadap keamanan informasi sangat kurang.

Seorang Admin jaringan pastinya memiliki tanggung jawab penuh atas tersedianya kerahasiaan informasi. Bukan hanya itu saja pastinya pemeliharaan kinerja jaringan juga sangat di perlukan. Administrator juga seorang manusia yang tidak selalu harus ada di depan layar untuk mengawasi suatu jaringan besar maupun kecil. Oleh karena itu dibutuhkanlah sebuah sistem yang bisa membantu kerja administrator.

Snort merupakan sebuah perangkat lunak yang fungsinya untuk mengamati aktivitas suatu jaringan komputer yang memberikan laporan secara detail dan tepat

sehingga suatu tindak kejahatan penyerangan bisa langsung diketahui. Snort juga disebut sebagai NIDS yang bersekala ringan. Akan tetapi pengoperasian snort cukup rumit.

Dirilis pada tahun 2004, Ubuntu adalah sebuah sistem operasi dan distribusi Linux berbasis Debian yang *free* dan *open soure*. Ubuntu dibangun dengan menggunakan infrastruktur Debian yang terdiri dari server, desktop dan sistem operasi linux. Sejak dirilisnya Ubuntu, banyak orang yang memfavoritkannya karena sistem operasi ini cukup mudah diinstall dan digunakan.

Aplikasi Telegram memungkinkan pengguna untuk mengirim dan menerima pesan untuk berbagai keperluan pada aplikasi. Telegram adalah Aplikasi pesan *chatting* yang memungkinkan pengguna untuk mengirimkan pesan *chatting* rahasia yang dienkripsi end-to-end sebagai keamanan tambahan.

Pada tugas skripsi ini peneliti mencoba melakukan suatu penelitian membuat suatu sistem keamanan jaringan menggunakan Snort dan Telegram alert pada Ubuntu. Hal yang melatar belakangi penulis untuk menganalisa dan menerapkan sistem deteksi ini adalah untuk mendeteksi adanya aktivitas jaringan yang mencurigakan dan merugikan dan melaporkannya dengan notifikasi berupa pesan Telegram yang digabungkan dengan Snort pada Linux.

Oleh karena itu, sesuai permasalahan yang dijelaskan, penulis mencoba membahas suatu maslaah dengan judul "**Sistem Monitoring Keamanan Jaringan Melalui Bot Telegram dengan Snort pada Ubuntu**"

1.2 Rumusan masalah

Berdasarkan latar belakang diatas maka dapat dibuat perumusan masalahnya yaitu, bagaimanakah merancang suatu mekanisme sistem pengamanan jaringan menggunakan Snort?

1.3 Batasan Masalah

Supaya penelitian tidak menyimpang dari pokok permasalahan dan tujuan yang akan dicapai, maka dibuatlah pembatas ruang lingkupnya oleh penulis, sebagai berikut :

1. Jaringan yang diuji adalah *Wireless Fidelity(WI-FI)*
2. Menggunakan sistem operasi Linux Ubuntu 16.4 LTS
3. Snort Versi *2.9.7.0 GRE (Build 149)*
4. Menggunakan *tool* penyerangan Hydra
5. Mengembangkan sistem pendeteksi serangan mengguunakan Bot Telegram Api

1.4 Tujuan Penelitian

Penelitian tugas akhir skripsi ini bertujuan membangun sistem Keamanan yang mumpuni dengan menggunakan Snort pada linux Ubuntu. Penulis memilih Snort selain karena bisa digunakan secara *free*, Snort juga berupa *open source*. Yang membuat beda yang dilakukan penulis dari yang sudah ada adalah ditambahkannya Telegram sebagai sistem yang memberitahu administratos jika ada penyerangan akan menerima informasinya melalui pesan Telegram dari server.

Pastinya ini akan sangat membantu sang administrator untuk melakukan Tindakan selanjutnya tanpa harus selalu berada di depan komputer.

1.5 Manfaat Penelitian

Manfaat penelitian yang dilakukan penulis adalah penulis dapat Mendapatkan informasi yang cepat ketika terjadinya penyerangan pada IP address yang dilindungi oleh *Snort* karena menggunakan aplikasi Telegram sebagai sarana notifikasi serangan.

1.6 Metode Penelitian

Dalam tugas akhir skripsi ini, penulis menggunakan beberapa Metode, antara lain :

1. Penelitian Pustaka (*Library Reseacrh)*

   Penelitian berikut dilakukan untuk mencari data, mengumpulkan data dan mempelajarinya dari buku-buku yang berhubungan dengan permasalahan yang dibuat dalam tugas akhir ini.

2. Penelitian Labor(Laboratory Reseacrh)

   Penelitian ini penulis melakukan pengolahan data menggunakan alat bantu. Berikut ditinjau dari penggunaan *Hardware* dan *Software* yang digunakan, sebagai berikut :

   a. *Hardware*

   1) 1 unit Laptop

   2) *Jaringan internet WI-FI*

   3) *1 Unit Smartphone*

   b. *Software*

1) *Snort Version 2.9.7.0 GRE (Build 149)*

2) *Aplikasi VMWare Workstation*

3) *Linux Ubuntu 16.4*

4) *Aplikasi Telegram*

5) *Api Telegram*

6) *Telegram Bot*

1.7 Sistematika Penulisan

Dalam penulisan ini, menggunakan sistematika penulisan sebagai berikut :

Bab I Pendahuluan

Bab ini menjelaskan latar belakang masalah, rumusan masalah, Batasan masalah, tujuan penelitian, metode penelitian dan sistematika penulisan

Bab II Landasan Teori

Bab ini berisi teori yang diambil dari berbagai sumber buku dan juga referensi lain yang berkaitan dengan penelitian penulis

Bab III Metode Penelitian

Bab ini membahas analisis dari yang diteliti dan apa saja alat-alat yang digunakan dalam penelitian ini.

Bab IV Implementasi dan Pembahasan

Bab ini membahas pengimplementasikan dan menjelaskan apa saja yang dibutuhkan untuk membuat rancangan penelitian yang dilakukan penulis.

Bab IV Hasil dan Pembahasan

Bab ini membahas hasil akhir dari rancangan sistem yang sudah dibuat penulis.

Bab V Penutup

Bab ini berisi pembahsan kesimpulan dan saran dari sistem yang dirancang penulis.