BAB 1

PENDAHULUAN

1.1 Latar Belakang

Berkembangnya teknologi informasi khususnya jaringan komputer dan layanan layanannya di satu sisi mempermudah pekerjaan-pekerjaan manusia sehari-hari, akan tetapi di sisi lain timbul masalah yang sangat serius, yakni faktor keamanannya. Di satu sisi manusia sudah sangat tergantung dengan sistem informasi, akan tetapi di sisi lain statistik insiden keamanan meningkat tajam. Hal ini secara umum terjadi karena kepedulian terhadap keamanan sistem informasi masih sangat kurang. Keamanan jaringan adalah suatu cara atau suatu system yang digunakan untuk memberikan proteksi atau perlindungan pada suatu jaringan agar terhindar dari berbagai ancaman luar yang mampu merusak jaringan. Tujuan membuat keamanan jaringan adalah untuk mengantisipasi resiko jaringan berupa bentuk ancaman fisik maupun logic baik langsung ataupun tidak langsung yang dapat mengganggu aktivitas yang sedang berlangsung dalam jaringan.Satu hal yang perlu diingat bahwa tidak ada jaringan yang anti sadap atau tidak ada jaringan yang benar-benar aman. karna sifat jaringan adalah melakukan komuikasi, dan setiap komunikasi dapat jatuh ke tangan orang lain dan di salah gunakan. Oleh sebab itu keamanaan jaringan sangatlah dibutuhkan.

Pencegahaan yang paling sering dilakukan untuk masalah ini adalah dengan menempatkan seorang administrator, yang bertugas untuk mengawasi dan melakukan tindakan preventif ketika terjadi aksi penyusupan dan serangan. Masalah akan timbul ketika administrator sedang tidak berada pada kondisi yang memungkinkan untuk memantau lalu lintas jaringan. Berdasar permasalahan tersebut, administrator

membutuhkan suatu sistem yang dapat membantu mengawasi jaringan, menginformasikan serangan, dan mengambil tindakan tepat untuk pencegahan yang akan membantu mengautomatisasi fungsi kerja dasar administrator. Penelitian ini bertujuan untuk mengimplementasikan sebuah aplikasi IDS yang dapat mendeteksi adanya serangan pada server dengan menganalisa alert dan log yang dihasilkan dan memanfaatkan jejaring sosial sebagai media notifikasi (Catur,2014)

Salah satu software yang dapat digunakan untuk memonitoring jaringan adalah Snort. Snort adalah sebuah software opensource ringkas yang sangat berguna untuk mengamati aktivitas dalam suatu jaringan komputer. Snort dapat digunakan sebagai suatu NIDS (*Network Intrusion Detection System*) yang ber-skala ringan (*lightweight*), dan software ini menggunakan sistem peraturan-peraturan (*rules system*) yang dapat dibuat sesuai kebutuhah untuk melakukan deteksi dan pencatatan (*logging*) terhadap berbagai macam serangan pada jaringan komputer. Selain itu Snort juga memiliki beberapa mode yang dapat digunakan untuk mengamankan suatu jaringan seperti sniffer mode, packet logger mode, NIDS mode dan Inline mode. Sistem keamanan firewall tidaklah cukup untuk meminimalkan terjadinya serangan terhadap suatu jaringan komputer. Banyak serangan yang terjadi pada jaringan komputer dapat diketahui setelah adanya kejadian-kejadian yang aneh pada jaringan. Para administrator jaringan tidak bisa mengetahui dengan pasti apa yang sedang terjadi, sehingga dibutuhkan waktu yang cukup lama untuk diatasi(Asep,2016).

Sebuah Intrusion Detection System adalah aplikasi yang digunakan untuk memantau jaringan dan melindunginya dari penyusup (Vijayarani dan Sylviaa, 2015). Dengan kemajuan teknologi berbasis internet yang pesat, area aplikasi baru untuk

jaringan komputer telah muncul. Dalam berbagai kasus, bidang-bidang seperti sektor usaha, keuangan, industri, keamanan dan kesehatan, aplikasi LAN dan WAN telah berkembang. Semua area aplikasi ini membuat jaringan menjadi target yang menarik untuk penyalahgunaan dan kerentanan besar bagi masyarakat. pengguna jahat atau hacker menggunakan sistem internal organisasi untuk mengumpulkan informasi dan penyebab kerentanan seperti bug Software, Selang dalam administrasi, meninggalkan sistem ke konfigurasi default. Perkembangan internet dalam masyarakat, barang baru seperti virus dan worm diimpor ke dalam sistem. Begitu ganas, pengguna menggunakan teknik yang berbeda seperti retak password, mendeteksi teks terenkripsi digunakan untuk menyebabkan kerentanan pada sistem. Oleh karena itu, keamanan diperlukan bagi pengguna untuk mengamankan sistem mereka dari penyusup. Teknik Firewall adalah salah satu Teknik perlindungan yang populer dan digunakan untuk melindungi jaringan pribadi dari jaringan publik. IDS digunakan dalam kegiatan jaringan yang terkait, aplikasi medis, penipuan kartu kredit, agen asuransi.

Telegram adalah layanan pesan populer yang berbasis pada platform open-source yang dibangun oleh Rusia Pavel Durov pada tahun 2013.Telegram merupakan aplikasi cloud based dan sistem enkripsi yang menyediakan enkripsi end-to-end, self destruction messages, dan infrastruktur multi- data center. Kemuadahan akses yang diberikan telegram yang dapat berjalan di hampir semua platform memberikan kemudahan bagi administrator untuk membangun system notifikasi dengan memanfaatkan fasilitas open Aplication Programing Interface (API) yang disediakan oleh telegram melalui bot yang dapat digunakan untuk mengirimkan pesan secara otomatis. Cloud base pada telegram memungkinkan proses pengiriman jauh lebih cepat serta media penyimpanan yang besar.

1.2 Rumusan Masalah

Berdasarkan uraian yang ada di latar belakang,maka rumusan masalah yang dapat di tarik adalah:

a. Bagaimana cara implementasi snort untuk monitor keamanan jaringan?
b. Bagaimana cara mendeteksi serangan terhadap ubuntu server menggunakan Snort agar bisa dimonitor oleh administrator?
c. Bagaimana cara membuat Telegram Bot sebagai media notifikasi untuk memonitor jaringan?

1.3 Batasan masalah

Untuk menghindari penyimpangan dari judul dan tujuan yang sebenarnya, maka dibuatkan ruang lingkup batasan masalah sebagai berikut

a. Merancang jaringan dan mengkonfigurasi snort dan aplikasi pendukung lainnya
b. Mengkonfigurasi Telegram sebagai media notifikasi
c. Melakukan pengujian terhadap komputer server apa sistem yang terkonfigurasi sudah berjalan dengan benar
d. Melakukan pengujian terhadap server apa serangan IDS yang sudah dilakukan sudah terkonfigurasi
e. Melakukan Analisa apakah Telegram bisa menjadi media notifikasi
f. Serangan yang dilakukan adalah Port Scanning

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah dijelaskan diatas, tujuan dari penelitian ini adalah sebagai berikut :

a. Untuk mengimplementasikan Snort sebagai solusi untuk mengamankan aktivitas jaringan computer
b. Untuk menganalisa telegram apakah bisa menjadi media notifikasi dalam monitoring dan keamanan jaringan
c. Untuk menganalisa aktifitas penyerang berupa log serangan yang akan ditampilkan di dalam aplikasi telegram

1.5 Manfaat

Adapun manfaat dari penelitian ini adalah sebagai berikut :

a. Manfaat yang didapat dan diharapkan dari penelitian kali ini adalah untuk memahami tentang cara mengamankan jaringan yang baik,khususnya menggunakan Snort sebagai media untuk memonior suatu serangan
b. Manfaat bagi penulis yang dapat diharapkan dari penelitian ini adalah untuk dapat menambah wawasan dan menerapkan pengetahuan mengenai keamanan jaringan computer khususnya dalam hal menganalisa keamananan jaringan menggunakan *SNORT* sebagai pendeteksi dan Telegram sebagai media notifikasi yang diperoleh selama menempuh ilmu dibangku perkuliahan. Selain itu bagi penulis khususnya penelitian ini merupakan syarat kelulusan program studi Teknik Informatika Universtias Pembangunan Nasionan “Veteran” Jawa Timur

c. Manfaat pihak lain yang diharapkan dari penelitian ini adalah untuk dapat digunakan sebagai bahan referensi serta menambah informasi mengenai implementasi *intrusion detection system* IDS menggunakan Telegram Bot sebagai media notifikasi.

1.6 Sistematika penulisan

Dalam tugas akhir ini laporan akan dibagi menjadi 5 bab dengan sistematika penulisan sebagai berikut :

BAB I PENDAHULUAN

Berisi Latar Belakang, Perumusan Masalah, Batasan Masalah, Tujuan, Manfaat, Metodelogi dan Sistematika Penulisan

BAB II TINJAUAN PUSTAKA

Berisi tentang penelitian terdahulu yang sebelumnya telah dilakukan serta berisi teori – teori dan penjelasan dari metode yang akan digunakan dalam membuat perancangan *honeypot* untuk mendeteksi pola serangan pada jaringan.

BAB III METODE PENELITIAN

Berisi tentang perencanaan serta analisis terhadap pembuatan sistem keamanan *Snort* yang digunakan sebagai perlindungan dari aktivitas serangan hacking

BAB IV HASIL DAN PEMBAHASAN

Berisi tentang pembuatan sistem serta pengujian dan pengecekkan terhadap sistem yang telah dibuat.

BAB V KESIMPULAN DAN SARAN

Berisi kesimpulan yang dapat diambil dari tugas akhir serta saran yang berguna untuk pengembangan selanjutnya