BAB I

PENDAHULUAN

1.1 Latar Belakang

Pemindaian jaringan dan Port terdiri dari pemindaian port jaringan serta pemindaian kerentanan, Pemindaian port adalah metode pemindaian paket data melalui jaringan ke nomor port layanan yang ditentukan seperti port 23 untuk telnet, port 80 untuk HTTP dan sebagainya, Untuk mengidentifikasi layanan jaringan yang tersedia pada sistem tertentu. Pemindaian port adalah pendekatan favorit para cracker komputer, memunculkan ide di mana untuk menyelidiki kelemahan. Nmap (atau Network Mapper) adalah alat sumber terbuka. Ini adalah utilitas pemindaian jaringan yang dapat digunakan untuk menemukan, mengaudit, dan memecahkan masalah sistem jaringan. Setiap administrator jaringan harus tahu tentang Nmap dan fitur-fiturnya. Nmap dapat memindai port yang terbuka menggunakan opsi paket TCP dengan sejumlah besar opsi baris perintah. Ini adalah alat berfitur lengkap yang mencakup beberapa subproyek hebat lainnya, seperti Ncrack, Ncat, Nping, Zenmap dan Nmap Scripting Engine. Ini adalah utilitas gratis untuk penemuan jaringan dan audit keamanan. Nmap menggunakan paket IP mentah dengan cara baru untuk menentukan host apa yang tersedia di jaringan seperti nama dan versi aplikasi, Sistem Operasi dan versi, dan jenis filter/firewall apa yang digunakan. Data yang dikumpulkan terdiri dari pemindaian port, pemindaian ICMP, pemindaian kerentanan, serangan yang berhasil, dan lalu lintas manajemen. Ini dirancang untuk memindai jaringan besar dengan cepat. Alat lain dalam subproyek Nmap di jaringan adalah kebutuhan spesifik pengguna.

1. Nping mengkhususkan diri dalam pembuatan paket jaringan.
2. Ncrack difokuskan pada cracking otentikasi jaringan.

3. Ncat atau Netcat memungkinkan pengalihan baca, tulis, dan modifikasi data jaringan ke pengguna.
4. Zennmap adalah platform GUI, berfokus pada kegunaan.

Nmap adalah utilitas yang kuat. Kira-kira lima belas metode pemindaian berbeda dan dua puluh opsi berbeda untuk digunakan saat pemindaian dan keluaran dapat menghadirkan setidaknya empat cara berbeda, dalam Nmap. Sangat mudah untuk memahami cara menggunakan Nmap tetapi agak sulit untuk memahami opsi mana yang digunakan dalam situasi apa. Ini paling sering digunakan oleh administrator jaringan dan profesional keamanan TI untuk memindai jaringan.[10]

Keamanan jaringan pada server merupakan faktor penting dalam jaringan. Keamanan yang baik dapat memberikan rasa percaya pada suatu server yang digunakan dan mengurangi kerugian dari serangan yang terjadi pada jaringan suatu server.

Aspek keamanan suatu jaringan menerukan stabilitas, integritas dan validasi data. Snort merupakan salah satu program Network-Base Intrusion Detection System, yaitu program yang dapat mendeteksi suatu usaha penyusupan pada sistem jaringan komputer.

Implementasi pendeteksi intrusi/ Intrusion Detection System berbasis Snort dapat menghemat biaya pengadaan software karena bersifat open source dan cukup handal dalam mendeteksi suatu serangan terhadap keamanan jaringan suatu server. Snort sebagai IDS bisa diimplementasikan pada berbagai sistem operasi termasuk Linux Ubuntu.[2]

Dalam jaringan komputer, khususnya yang berkaitan dengan keamanan jaringan merupakan hal yang sangat penting untuk diperhatikan, karena akan banyak terjadi hal-hal yang dapat mengganggu keamanan atau kestabilan koneksi jaringan komputer tersebut, baik yang berkaitan dengan hardware (pengaman fisik, sumber daya listrik) maupun yang berkaitan dengan software (sistem, konfigurasi, sistem akses).

Beberapa contoh masalah yang sudah umum dalam keamanan

jaringan adalah adanya gangguan pada sistem yang dapat terjadi karena faktor ketidak sengajaan yang dilakukan oleh pengelola (human error), akan tetapi tidak sedikit pula yang disebabkan oleh pihak ketiga yang mencoba mengganggu pengguna jaringan tersebut yang berupaya melakukan perusakan, penyusupan atau penyalahgunaan data maupun sistem. Maka untuk membantu mempermudah administrator jaringan dalam mengelola jaringan tersebut dibutuhkan satu sistem yang dapat membaca dan mengenali setiap paket data yang masuk atau yang keluar secara cepat dan tepat.

Salah satu solusi yang dapat digunakan adalah dengan membangun Intrusion Detection System (IDS). IDS sendiri dapat membaca paket-paket data yang masuk maupun yang keluar secara otomatis yang nantinya akan memberikan sebuah laporan atau log kepada administrator jaringan.

Dengan memanfaatkan sistem IDS pada suatu jaringan maka kemungkinan adanya gangguan yang disebabkan oleh pihak ketiga terhadap suatu jaringan dapat di meminimalisir, karena nantinya setiap gangguan yang disebabkan akan terdeteksi oleh IDS, dan nantinya IDS akan memberikan peringatan atau alert kepada admin jaringan

1.2 Rumusan Masalah

Setelah diidentifikasi berdasarakan latar belakang tersebut, maka penulis dapat merumuskan masalah yaitu bagaimana merancang suatu server linux dengan keamanan IDS dan snort berfungsi dengan baik dalam memberikan peringatan pada admin jaringan bahwa ada arus lalu lintas internet yang tidak normal, atau ada penyerangan pada server yang admin buat.

1.3 Tujuan dan Manfaat Penulisan

Berikut adalah tujuan dan manfaat dari laporan ini berdasarkan latar belakang serta rumusan masalah.

1.3.1 Tujuan

Tujuan penulisan skripsi ini dapat dilampiran dalam beberapa poin, diantaranya adalah :

1. Untuk Mengetahui Seberapa amankah Perangkat milik kita dan koneksi yang terhubung ke perangkat kita.

2. Untuk mempermudah pihak pengelola jaringan dan server memfilter data yang lewat.

3. Menguji Keamanan Pada koputer client dan computer target.

1.3.2 Manfaat

Beberapa manfaat yang ingin dicapai dalam melakukan penelitian skripsi ini sebagai berikut:

1. Pihak pengelola mudah mengetahui adanya arus transfer data yang tidak normal
2. Memperkuat keamanan server dan data client yang terhubung ke jaringan
3. Mempermudah server dalam memutuskan transfer data.

1.4 Batasan Masalah

Adapun penulis membuat batasan masalah untuk menghindari pembuatan Laporan Penelitian yang tidak terarah dan cakupan tidak begitu luas. Berikut beberapa masalah yang dibahas pada laporan ini adalah sebagai berikut:

1. Server Snort IDS dibangun pada sistem operasi Linux Ubuntu Desktop 22.04 Jellyfish.
2. Menggunakan perangkat lunak Snort IDS sebagai pendeteksi gangguan.
3. Menggunakan Basic Analysis and Security Engine (BASE) sebagai interface untuk pembacaan log gangguan.
4. Pengujian gangguan hanya dilakukan dengan dua cara, yaitu : dengan teknik Denial of Service (DoS) dan Port Scanner menggunakan aplikasi Nmap.

5. Implementasi sistem hanya dilakukan pada jaringan lokal.

1.5 Sistematika Penulisan

Untuk mengetahui kerangka keseluruhan penulisan, penulis menjabarkan sistematika penulisan sebagai berikut **:**

BAB I PENDAHULUAN

Berisi tentang latar belakang, perumusan masalah, tujuan dan manfaat .

BAB II LANDASAN TEORI

Bab ini berisikan teori yang berupa definisi model Pengamanan server, definisi IDS SNORT, definisi rules snort, teori pendukung, dan penelitian terdahulu.

BAB III METODOLOGI PENELITIAN

Bab ini berisikan metodologi penelitian yang akan dipakai sebagai *Rules* untuk menjabarkan hasil dan pembahasan, meliputi model pengembangan sistem, metode pengembangan.

BAB IV HASIL DAN PEMBAHASAN

Bab ini berisi pembahasan, konfigurasi snort,dan pengujian.

BAB V PENUTUP

Bab ini berisi kesimpulan dan saran yang berkaitan dengan analisa dan optimalisasi sistem berdasarkan yang telah diuraikan pada bab sebelumnya.

DAFTAR PUSTAKA LAMPIRAN


I S B
ATMA LUHUR
PANGKALPINANG