SELF DEFENDING LINUX NETWORK

TUGAS AKHIR

Disusun Untuk Melengkapi Persyaratan Guna

Memperoleh Gelar Sarjana Jurusan Komputer Fakultas Teknik

Universitas Muhammadiyah Surakarta

Disusun Oleh :

AVICENNA HAMDAN
D400020027

FAKULTAS TEKNIK JURUSAN ELEKTRO

UNIVERSITAS MUHAMMADIYAH SURAKARTA

2008

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Keamanan jaringan komputer sebagai bagian dari sebuah sistem informasi adalah sangat penting untuk menjaga *validitas* dan integritas data serta menjamin ketersediaan layanan bagi penggunanya. Sistem harus dilindungi dari segala macam serangan dan usaha-usaha penyusupan oleh pihak yang tidak berhak.

Banyak cara dikembangkan untuk mengamankan infrastruktur jaringan dan komunikasi di internet, mereka memakai *firewall*, enkripsi, dan *Virtual Private Network*. *Intrusion Detection* adalah metode yang relative baru. Dengan metode *Intrusion Detection*, dapat dikumpulkan dan digunakan informasi tipe penyerangan yang telah diketahui dan ditemukan jika seseorang mencoba menyerang jaringan atau *host* tertentu.

Intrusion Detection adalah merupakan cara bertahan diri dari serangan. *Software Intrusion Detection* yang digunakan adalah menggunakan Snort. Snort adalah *software open source* yang gratis. Snort akan diintregasikan dengan dengan beberapa *software* dan bahasa pemrograman. Bahasa pemrograman yang digunakan adalah PHP dan database MySql. *Software* lain yang digunakan adalah *Apache Web Server* dan BASE. *Hardware* yang

digunakan satu unit komputer *server*, satu unit komputer *attacker* dan *client*, serta kabel jaringan secara *cross*.

1.2 Rumusan Masalah

Berdasarkan rumusan masalah yang dikaji maka penelitian ini bertujuan untuk :

1. Merancang dan membuat sitem pertahanan diri jaringan dari serangan.
2. Menerapkan *software open source* Snort dan BASE pada *server*.
3. Menerapkan aplikasi IDS yang terintegrasi dalam jaringan komputer.

1.3 Batasan Masalah

Agar dalam perancangan ini dapat mencapai sasaran dan tujuan yang diharapakan, maka permasalahan yang ada dibatasi sebagai berikut :

1. Aplikasi *software open source* diinstal dan dikonfigurasi di komputer *server* dengan sistem operasi Fedora Core5.
2. Menggunakan *software* Snort untuk mendeteksi *intrusion*, dan *software* BASE untuk melihat dan menganalisa data snort menggunakan *web browser*, dan Apache untuk web *server*nya.
3. Antarmuka *software* dengan pengguna berupa halaman web dengan akses melalui *web browser*.
4. Jaringan komputer yang dibangun menggunakan satu komputer *server* dan satu komputer *client* dengan model jaringan *client-server*.
5. *Client* akan difungsikan sebagai *attacker* atau *intruder*.

6. Komputer Client Server diimplementasikan dengan menggunakan *IP version 4* (*ipv4*).
7. Simulasi computer secara *offline*.
8. Menggunakan *software Nessus Vulnerability Scanner* serta Nmap untuk pengujian komputer *server*.

1.4 Tujuan

Berdasarkan rumusan masalah yang dikaji maka penelitian ini bertujuan untuk :

1. Merancang dan membuat sitem pertahanan diri jaringan komputer dari serangan.
2. Menerapkan *software open source* snort pada jaringan.
3. Menerapkan aplikasi *Intrusion Detection* yang terintegrasi dalam jaringan komputer.

1.5 Manfaat

Perancangan dan pembuatan sistem pertahanan diri jaringan berbasis Linux ini diharapkan dapat memberikan kontribusi dalam bidang pengembangan sistem keamanan jaringan komputer tanpa biaya seperti *software* keamanan komersial serta bisa mengetahui adanya berbagai macam gangguan keamanan komputer..

1.6 Tinjauan Pustaka

Dalam penyusunan tugas akhir ini, penulis mengambil referensi dari sebuah buku yang dibuat oleh Dony Ariyus, M. Kom dengan judul *Intrusion Detection System*, diterbitkan oleh Andi Publisher Yogyakarta tahun 2007. Buku ini berisi tentang Sistem Pendeteksi Penyusup Pada Jaringan. *Software* yang digunakan untuk pendeteksi adanya penyusup menggunakan Snort. Snort akan diintegrasikan dengan MySql untuk *database* nya, serta menggunakan BASE untuk analisa menggunakan *web browser*.

1.7 Metode Penelitian

Langkah-langkah yang akan ditempuh selama menyusun tugas akhir ini adalah sebagai berikut :

1. Melakukan serangkaian percobaan untuk mendapatkan hasil yang diinginkan.
2. Konsultasi dengan dosen pembimbing serta mencari sumber informasi yang berhubungan dan mendukung perancangan sitem ini.
3. Studi kepustakaan dengan mempelajari buku yang mnjadi referensi.

1.8 Sistematika Penulisan

BAB I PENDAHULUAN

Berisi mengenai latar belakang pemilihan judul, permasalahan, pembatasan masalah, tujuan yang hendak dicapai, manfaat, dan sistematika penulisan.

BAB II LANDASAN TEORI

Membahas konsep dasar jaringan, *Intrusion Detection System, Firewall dan Virus Trojan Backdoor*..

BAB III PERANCANGAN SISTEM

Membahas perancangan *Self Defending Linux Network*, disertai dengan aplikasi *software* Snort dan BASE beserta langkah instalasinya.

BAB IV PENGUJIAN DAN ANALISA

Menunjukkan hasil pengujian dari pertahanan diri jaringan linux menggunakan *software Nessus Vulnerability Scanner* dan *Nmap*, disertai dengan analisa sehingga didapatkan bukti kuat dari hipotesis yang dilakukan.

BAB V PENUTUP

Menguraikan kesimpulan Tugas Akhir dan saran-saran sebagai bahan pertimbangan untuk pengembangan penelitian selanjutnya.