TUGAS AKHIR

APLIKASI IDS BERBASIS SNORT UNTUK DETEKSI PENYUSUPAN PADA JARINGAN KOMPUTER

Diajukan Guna Memenuhi Persyaratan
Menyelesaikan Pendidikan Program Diploma III
Politeknik Universitas Andalas

DEPARTEMEN PENDIDIKAN NASIONAL
UNIVERSITAS ANDALAS
UPT PERPUSTAKAAN

Oleh:

RIO KURNIA
BP. 06 093 021

PROGRAM STUDI TEKNIK KOMPUTER
JURUSAN TEKNOLOGI INFORMASI
POLITEKNIK UNIVERSITAS ANDALAS
PADANG
2009

MILIK
UPT PERPUSTAKAAN
UNIVERSITAS ANDALAS
TERDAFTAR
TANGGAL: 30-11-09
NO. INDUK: 2090710663

ABSTRAK

Intrusion Detection System (IDS) merupakan sebuah aplikasi yang berfungsi untuk memeriksa secara otomatis *audit logs* dan *event-event system* secara *realtime*. Metode IDS yang digunakan adalah IDS berbasis *Snort* yang dibantu oleh beberapa aplikasi tertentu. Aplikasi yang dibangun ini mempunyai tiga tugas utama yaitu membaca proses komunikasi data, *analisis* data, dan apabila terjadi penyusupan, aplikasi ini akan langsung menyimpan pada *database* yang digunakan, dan secara *otomatis* data yang tersimpan akan diperlihatkan melalui *web browser*.

Kata kunci : ***Intrusion Detection System (IDS), Snort, Database, Web Browser***

BAB I
PENDAHULUAN

1.1 Latar Belakang

Dalam program pendidikan Politeknik setiap mahasiswa yang akan menyelesaikan pendidikannya diwajibkan membuat Tugas Akhir yang merupakan syarat dalam mengikuti ujian Sidang Akhir, dimana Tugas Akhir ini merupakan implementasi atas kemampuan mahasiswa secara umum dalam memahami materi selama perkuliahan di Politeknik Universitas Andalas.

Jaringan komputer pada saat ini terus mengalami perkembangan, baik dari *skalabilitas*, jumlah *node*, dan teknologi yang digunakan. Hal ini berpengaruh pada pengelolaan jaringan yang lebih baik agar ketersediaan jaringan selalu tinggi. Tugas pengelolaan jaringan yang dilakukan administrator jaringan memiliki banyak permasalahan, diantaranya yang berkaitan dengan kegiatan penyusupan pada jaringan komputer yang mengakibatkan rusaknya sistem keamanan jaringan komputer tersebut.

Saat ini kegiatan penyusupan yang dilakukan oleh *intruder* terus mengalami perkembangan, kemajuan dari kegiatan penyusupan ini melebihi dari keamanan jaringan yang dibangun. Sepert halnya *firewall* yang berfungsi untuk menjaga keamanan saat terjadinya proses komunikasi data, namun hal tersebut tidak mampu untuk mencegah kegiatan penyusupan yang terjadi, karena para *intruder* telah mengetahui celah masuk untuk membobol *firewall* tersebut.

Para *intruder* mampu untuk memperoleh akses kedalam suatu sistem dan menemukan informasi tentang sistem tersebut.

Pada laporan Tugas Akhir ini mencoba membangun sebuah aplikasi yang berfungsi untuk memeriksa secara otomatis *audit logs* dan *event-event system* secara *realtime*, aplikasi yang dibangun ini mempunyai 3 (tiga) tugas utama yaitu membaca proses komunikasi data pada jaringan tersebut, menganalisa data yang melewati jaringan tersebut, dan apabila terjadi penyusupan, aplikasi ini akan langsung menyimpan pada *database* yang digunakan, dan secara otomatis data yang tersimpan akan diperlihatkan melalui *web browser*.

Aplikasi yang dimaksud adalah mencoba membangun sebuah *network intrusion detection system (NIDS)* yang bekerja pada sistem operasi *Windows XP Profesional* dengan metode NIDS berbasis *Snort* yang memiliki kelebihan yang tidak dapat diberikan oleh NIDS lainnya.

Network intrusion detection system yang nantinya akan disebut dengan NIDS merupakan usaha mengidentifikasi adanya penyusupan yang memasuki sistem tanpa *otorisasi* (misal *cracker*) atau sescorang *user* yang sah tapi menyalahgunakan *privelege* sumber daya sistem. NIDS atau sistem deteksi penyusupan adalah sistem komputer (bisa merupakan kombinasi dari *software* dan *hardware*) yang berusaha melakukan usaha deteksi penyusupan. NIDS akan melakukan pemberitahuan saat mendeteksi sesuatu yang dianggap mencurigakan atau sebagai tindakan *ilegal*. NIDS disini tidak melakukan pencegahan terjadinya penyusupan, melainkan hanya memberitahukan kepada *administrator* jaringan

BAB V

PENUTUP

5.1 KESIMPULAN

IDS merupakan sistem yang dapat memberikan peringatan dan inforamsi kepada admininistrator tentang perilaku yang dicurigai sebagai *intrusi* atau penyusupan. Tujuan utama dari IDS berbasis *Snort* ini adalah meminimalkan perkiraan kerugian yang terjadi akibat *intrusion*. Jadi untuk membangun sistem keamanan jaringan menggunakan IDS ini pastikan bahwa IDS yang digunakan memiliki spekulasi sebagai berikut :

1. Mampu mencegah serangan dan tidak hanya mendeteksi. Jangan gunakan IDS yang hanya dapat mendeteksi serangan saja, tapi gunakan IDS yang sudah mampu melakukan pencegahan terhadap serangan. IDS yang baik tidak memiliki batasan metoda pendeteksian dan dapat dipercaya dalam mencegah suatu serangan.
2. Memiliki cakupan yang luas dalam mengenal proses *attacking*.

   IDS harus memiliki pengetahuan yang luas, bisa mengenal apa yang tidak dikenalnya, mampu melakukan deteksi DOS mempergunalan analisis '*signature*' dan mampu menditeksi segala sesuatu yang mencurigakan. Untuk memenuhi kriteria ini IDS harus :

   a. Mampu melakukan proses deteksi *traffic* dan pembersihan terhadap *host* (*Layer* 3 - 7)
   b. Mampu malakukan '*scanning*' *TCP* dan *UDP*
   c. Mampu memeriksa keberadaan '*Backdoor*'

DAFTAR PUSTAKA

1. Bambang Sugiantoro, "Kajian Aplikasi Mobile Agent Untuk Deteksi Penyusupan Pada Jaringan Komputer", Yogyakarta, 2006.
2. Charlie Scott,Paul Wolfe, and Bert Hayes, "Snort For Dummies", Wiley Publishing, inc , 2004.
3. Helmi Zein Nuri, "Instalasi Moodle Pada Sistem Operasi Windows Xp", Yogyakarta, 2006.
4. Internet Security Systems, .Network VS Host-based Intrusion Detection: A Guide to Intrusion Detection Technology.,www.iss.net.net,2002
5. Mikael Keri, "OpenIDS Installation and configuration guide 1.0", www.prowling.nu, 2005.
6. Michael E. Steele, "Snort Installation Manual Windows NT4 Server, 2000, & XP (All Versions)", www.silicondefense.com, 2003.
7. Purbo, Onno W, "Snort Untuk Mendeteksi Penyusup", NeoTek, Agustus 2002
8. Purbo, Onno W., Wiharjito, Tony., Keamanan Jaringan Internet, Elex Media Komputindo, 2000
9. Purbo, Onno W., TCP/IP : Standar, Desain, dan Implementasi., Elex Media Komputindo, 1998
10. Puji Hartono, "Sistem Pencegahan Penyusupan pada Jaringan berbasis Snort IDS dan IPTables Firewall", Bandung, 2006.
11. Ryan Russel, "Snort Intrusion 2.0 Intrusion Detection", Syngress, 2003.