DESAIN DAN IMPLEMENTASI SISTEM DETEKSI PENYUSUPAN JARINGAN SECARA OTOMATIS DAN INTERAKTIF

Bayu Ariefianto[1], Rendy Munady . Mt ; Gandhi Santoso[2], [3]

[1]Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom

---

Abstrak

Kata Kunci :

Abstract

Keywords :

Telkom University

BAB I

PENDAHULUAN

1.1 Latar Belakang

Dalam era teknologi informasi saat ini, hampir seluruh informasi yang penting bagi suatu institusi dapat diakses oleh para penggunanya. Keterbukaan akses tersebut memunculkan berbagai masalah baru, antara lain :

- Pemeliharaan validitas dan integritas data/informasi tersebut
- Jaminan ketersediaan informasi bagi pengguna yang berhak
- Pencegahan akses informasi dari yang tidak berhak
- Pencegahan akses sistem dari yang tidak berhak

Sistem pertahanan sistem terhadap aktivitas gangguan yang ada saat ini umumnya dilakukan secara manual oleh administrator. Hal ini mengakibatkan integritas sistem bergantung pada ketersediaan dan kecepatan administrator dalam merespon gangguan yang terjadi. Apabila gangguan tersebut telah berhasil membuat jaringan mengalami malfungsi, administrator tidak dapat lagi mengakses sistem secara remote. Sehingga administrator tidak dapat melakukan pemulihan sistem dengan cepat.

Karena itu dibutuhkan suatu sistem yang dapat menanggulangi ancaman-ancaman yang mungkin terjadi secara optimal dalam waktu yang cepat secara otomatis dan memungkinkan administrator mengakses sistem walaupun terjadi malfungsi jaringan. Hal ini akan mempercepat proses penanggulangan gangguan serta pemulihan sistem atau layanan.

1.2 Tujuan Penelitian

1. Mendesain dan mengimplementasikan sistem deteksi penyusupan jaringanyang otomatis dan interaktif.
2. Menganalisa performansi sistem deteksi penyusupan jaringan dalam menangani gangguan terhadap sistem.

1.3 Perumusan Masalah

1. Insiden-insiden yang mungkin terjadi terhadap keamanan jaringan adalah
   a. Probing
   b. Scanning
   c. Denial of Services (DoS)
   d. Account Compromize
   e. Root Compromize
   f. Packet Sniffing
   g. Exploits
   h. Malicious code
   i. Infrastructure Attacks
2. Administrasi sistem keamanan jaringan secara manual mengandung resiko keterlambatan respon terhadap intrusi jaringan.
3. Sistem deteksi intrusi jaringan harus memiliki fitur-fitur sebagai berikut :
   a. Deteksi serangan yang akurat
   b. Respon sistem dengan memblok semua paket yang berasal dari alamat penyerang yang terdeteksi secepat mungkin
   c. Database pola-pola serangan yang lengkap
   d. Memiliki interaktivitas dengan administrator sistem
4. Aksesibilitas administrator harus tetap terjaga dan terjamin otentikasinya walau terjadi malfungsi jaringan.

1.4 Batasan Masalah

1. Implementasi dilakukan pada jaringan dengan arsitektur *routed network*.
2. Interaktivitas sistem dengan administrator menggunakan SMS (Short Message Service) dua arah.
3. Parameter performansi sistem yang diukur adalah akurasi deteksi dan blocking paket, beban CPU dan memory, serta performansi troughput, jitter dan packet loss pada jaringan.

1.5 Metode Penelitian

1. Studi Pustaka
2. Desain Sistem
3. Implementasi pada jaringan.
4. Pengujian performansi sistem.
5. Analisa performansi sistem

Telkom University

BAB V
PENUTUP

5.1 Kesimpulan

- Sistem deteksi penyusupan jaringan secara otomatis dan interaktif telah berhasil dirancang dan diimplementasikan
- Sistem ini mampu melindungi jaringan beserta sumber daya yang ada di dalamnya tanpa mempengaruhi unjuk kerja jaringan tersebut
- Sistem ini mampu meningkatkan efisiensi administrasi sistem jaringan
- Sistem ini mampu menyediakan interaktivitas dengan administrator sistem apabila diperlukan
- Sistem ini memiliki kekurangan sebagai berikut :
    - Tidak mampu melakukan bloking per paket seperti aplikasi proxy
    - Masih memerlukan update rule secara teratur
    - Tidak memiliki kemampuan untuk mengenali pola serangan baru yang tidak terdapat dalam rule

5.2 Saran

- Perlu dikembangkan interface yang lebih mudah digunakan untuk mengontrol sebagian sub sistem yang masih harus dikonfigurasi secara manual
- Untuk keamanan sebaiknya semua interface yang berbasis web di-host dalam web server menggunakan SSL agar data yang dikirimkan dienkripsi
- Untuk pengembangan lebih lanjut perlu dibuat program serupa yang mampu mendeteksi serangan dengan lebih cepat
- Perlu dikembangkan sistem yang mampu mengatasi kekurangan-kekurangan sistem yang masih ada

DAFTAR PUSTAKA

Chapman , D. Brent. *Network (In)Security Through IP Packet Filtering*, 1992

Firewall HOWTO

Gerhard, Mourani. *Securing and Optimizing Linux : Red Hat Edition*, 2000

Gnokii C API Reference

Grennan, Mark. *Firewalling and Proxy Server HOWTO*

IDS HOWTO

IPTables HOWTO

Jon Postel, *Internet Protocol* , RFC 791, 1981

Jon Postel, *Transmission control Protocol*, RFC 793, 1981.

Mann, Scott and L . Mitchell, Ellen. *Linux System Security*

MySQL Database Programming Reference

Purbo, Onno W., Keamanan Jaringan Internet, Elex Media Komputindo, 2000

Purbo, Onno W., TCP/IP:Standar, Desain, dan Implementasi., Elex Media Komputindo, 1998

RFC 1244 Site Security Handbook

S. Kent., R.Atkinson., *Security Architecture for the Internet Protocol*,RFC 2401, 1998.

S. Kent., R. Atkinson., *IP Authentication Header*, RFC 2402, 1998.

SNORT Manual

Stalling,W.*Data&Computer ommunications*, Prentice Hall Internasional

Wack, John. *Packet Filtering Firewall.*

Ziegler, Robert L, *Linux Firewalls*, 1999