Konfigurasi Security Jaringan Cisco

Akhmad Syarifudin

175100012

Fakultas Komputer

Mahasiswa@institusi.ac.id

Abstract

Security adalah hal dasar yang harus disetting supaya tidak diganggu atau dirusak orang lain yang sengaja ataupun tidak sengaja masuk ke perangkat-perangkat jaringan yang kita miliki. Dengan menggunakan password, setidaknya orang lain sudah kebingungan bagaimana cara masuknya.

Dan cisco IOS IDS (Intrusion Detection System) adalah salah satu produk security berdaya guna yang ditawarkan Cisco System Inc, Cisco IOS Firewall Intrusion Detection System (IDS) atau dikenal dengan Net Ranger. Cisco IOS IDS memberikan level proteksi terhadap environment jaringan dari berbagai kesalahan dan usaha penyerangan yang datang dari user-user eksternal maupun internal. Teknologi ini memberi kelengkapan terhadap proteksi-prteksi yang ditawarkan system firewall. Cisco IOS IDS senantiasa mengambil aksi-aksi yang dipandang tepat terhadap paket-paket yang melanggar polic sekurity dan merepresentasikan aktifitas-aktifitas berbahaya dalam jaringan. Salah satu fitur utamanya adalah mengidentifikasi puluhan bentuk serangan umum dengan menggunakan “signature-signature”.

Cisco IDS beraksi sebagai sebuah sensor deteksi intrusi, memperhatikan setiap paket yang melintas, dan memindai mereka untuk memastikan mereka tidak ada yang masuk kriteria signature-signature IDS. Saat sebuah aktifitas berbahaya terdeteksi, Cisco IDS segera meresponnya sebelum keutuhan jaringan terganggu dan mencatat log event tersebut melalui fasilitas syslog Cisco IOS atau Post Office Protokol. Pengelola atau admistrator jaringan dapat merancang sistem IDS mereka untuk memilih tindakan-tindakan yang tepat terhadap bentuk pelanggaran yang spesifik.

Kata Kunci : Konfigurasi Security Jaringan Cisco.

A. PENDAHULUAN

Security atau keamanan dalam jaringan dalam jaringan komputer sangat penting dilakukan untuk memonitor akses jaringan dan mencegah penyalahgunaan sumber daya jaringan yang tidak sah. Tugas keamanan jaringan dikontrol oleh administrator jaringan.

Dan suatu jaringan sangatlah rentan terhadap serangan oleh orang-orang yang sengaja ingin merusak jaringan milik kita ataupun yang sekedar iseng-iseng saja. Maka dari itu security network atau keamanan jaringan menjadi kewajiban yang harus dikonfigurasi dalam switch atau perangkat lain.

Cisco IOS IDS (Intrusion Detection System) adalah salah satu produk security berdaya guna yang ditawarkan Cisco System Inc dan Cisco IOS Firewall Intrusion Detection System (IDS) atau dikenal dengan NetRanger. Cisco IOS IDS memberikan level proteksi terhadap environment jaringan dari berbagai kesalahan dan usaha penyerangan yang datang dari user-user eksternal maupun internal. Teknologi ini memberi kelengkapan terhadap proteksi-prteksi yang ditawarkan system firewall.

B. PEMBAHASAN / STUDI KASUS

Security atau keamanan dalam jaringan dalam komputer sangat penting dilakukan untuk

memonitor akses jaringan dan mencegah penyalahgunaan sumber daya jaringan yang tidak sah. Tugas keamanan jaringan dikontrol oleh administrator jaringan.

Segi-segi keamanan didefinisikan dari kelima point ini.

a. Confidentiality

Mensyaratkan bahwa informasi (data) hanya bisa diakses oleh pihak yang memiliki wewenang.

b. Integrity

Mensyaratkan bahwa informasi hanya dapat diubah oleh pihak yang memiliki wewenang.

c. Availability

Mensyaratkan bahwa informasi tersedia untuk pihak yang memiliki wewenang ketika dibutuhkan.

d. Authentication

Mensyaratkan bahwa pengirim suatu informasi dapat diidentifikasi dengan benar dan ada jaminan bahwa identitas yang didapat tidak palsu.

e. Nonrepudiation

Mensyaratkan bahwa baik pengirim maupun penerima informasi tidak dapat menyangkal pengiriman dan penerimaan pesan.

Serangan (gangguan) terhadap keamanan dapat dikategorikan dalam empat kategori utama :

1. Interruption

Suatu aset dari suatu sistem diserang sehingga

menjadi tidak tersedia atau tidak dapat dipakai oleh yang berwenang. Contohnya adalah perusakan/modifikasi terhadap piranti keras atau saluran jaringan.

2. Interception Suatu pihak yang tidak berwenang mendapatkan akses pada suatu aset. Pihak yang dimaksud bisa berupa orang, program, atau sistem yang lain. Contohnya adalah penyadapan terhadap data dalam suatu jaringan.
3. Modification Suatu pihak yang tidak berwenang dapat melakukan perubahan terhadap suatu aset. Contohnya adalah perubahan nilai pada file data, modifikasi program sehingga berjalan dengan tidak semestinya, dan modifikasi pesan yang sedang ditransmisikan dalam jaringan.
4. Fabrication Suatu pihak yang tidak berwenang menyisipkan objek palsu ke dalam sistem.

Firewall

Firewall merupakan sebuah perangkat keamanan jaringan computer yang melakukan fungsi control aliran data antara dua atau lebih network yang mempunyai perbedaan tingkat keamanan. Ada cara banyak untuk melindungi suatu private network atau sebuah situs internet. Perangkat firewall dapat ditempatkan pada posisi didepan maupun dibelakang kumpulan server web, maupun

tambahan koneksi dapat dibuat pada firewall tersebut dan server web dapat ditempatkan pada network internal.

Keputusan untuk bagaimana menggunakan firewall pada perancangan pada suatu system keamanan jaringan adalah berdasarkan pada aplikasi, manajemen serta ketersediaan kebutuhan perangkat yang ada. Saat ini terdapat cukup banyak firewall yang beredar dipasaran baik komersial maupun nonkomersial, berbasis hardware maupun software serta dengan berbagai macam fitur layanan fasilitas dan kemampuan fitur yang ditawarkan. sebagai contoh dapat disebutkan Cisco PIX, Checkpoint, Cyberguard dan lain-lain. Selain perangkat firewall yang ditujukan untuk keperluan manajemen network secara keseluruhan, saat ini cukup banyak tersedia juga perangkat firewall yang ditujukan untuk end user atau personal user terutama yang terhubung di internet. Setiap vendor mempunyai definisi yang spesifik terhadap masing-masing produk. Namun, secara umum akan diuraikan tipe-tipe firewall yang ada, antara lain;

- Packet filtering firewall
- Application-level gateways (contoh: proxy server)
- Circuit level gateways
- Stateful packet inspection firewalls.

Salah satu fitur utamanya adalah mengidentifikasi uluhan bentuk serangan umum dengan menggunakan “signature-signature”. Cisco IDS beraksi sebagai sebuah sensor deteksi intrusi, memperhatikan setiap paket yang melintas, dan memindai mereka untuk memastikan mereka tidak ada yang masuk criteria signature-signature IDS. Saat sebuah aktifitas berbahaya terdeteksi, Cisco IDS segera meresponnya sebelum keutuhan jaringan terganggu dan mencatat log event tersebut melalui fasilitas syslog Cisco IOS atau Post Office Protokol.

Pengelola atau administrator jaringan dapat merancang sistem IDS mereka untuk memilih tindakan-tindakan yang tepat terhadap bentuk pelanggaran yang spesifik. Saat beberapa paket dalam sesi koneksi terjatuh dalam signature, sistem IDS dapat kita atur untuk menganalisa-aksi berikut:

- Mengirim alarm ke server syslog atau Cisco Secure IDS Director
- Membuang paket
- Me-reset koneksi TCP yang berjalan.

Tugas-tugas Konfigurasi Cisco IOS Firewall IDS
Memperkenalkan Cisco IOS IDS Untuk menginisiasi atau memperkenalkan Cisco IOS firewall IDS pada sebuah router,

lakukan pada perintah berikut dari global konfigurasi mode:

Tahap 1: Mengeset jumlah penerima maksimum
Langkah ini mengeset pada spamming yang diijinkan atas pesan-pesan e-mail. Disini, flag recipients merepresentasikan jumlah maksimum penerima pada sebuah pesan e-mail. Nilai default-nya adalah 250

C. ID SECURITY

QWTD4452377-ASP-5244107

D. KESIMPULAN

Security adalah hal dasar yang harus disetting supaya tidak diganggu atau dirusak orang lain yang sengaja atau pun tidak sengaja masuk ke perangkat-perangkat jaringan yang kita miliki. Dengan menggunakan password, setidaknya orang lain sudah kebingungan bagaimana cara masuknya.

Dan cisco IOS IDS memberikan level proteksi terhadap environment jaringan dari berbagai kesalahan dan usaha penyerangan yang datang dari user-user eksternal maupun internal. Teknologi ini memberi kelengkapan terhadap proteksi-proteksi yang ditawarkan system firewall. Cisco IOS IDS senantiasa mengambil aksi-aksi yang dipandang tepat terhadap paket-paket yang melanggar policy security dan merepresentasikan aktifitas-aktifitas berbahaya dalam jaringan. Salah satu fitur

utamanya adalah mengidentifikasi puluhan bentuk serangan umum dengan menggunakan “signature-signature”.

E. DISKUSI

Saya bersama teman saya bernama Fiti Hidayatullah mendiskusikan tentang konfigurasi security jaringan cisco ini dengan sangat baik. Hasil diskusi dari materi ini adalah bahwasannya security adalah hal dasar yang harus disetting supaya tidak diganggu atau dirusak orang lain yang sengaja atau pun tidak sengaja masuk ke perangkat-perangkat jaringan yang kita miliki. Dengan menggunakan password, setidaknya orang lain sudah kebingungan bagaimana cara masuknya.

Dan cisco IOS IDS senantiasa mengambil aksi-aksi yang dipandang tepat terhadap paket-paket yang melanggar polic security dan merepresentasikan aktifitas-aktifitas berbahaya dalam jaringan.

F. REFERENCE

- [1] O. M. Febriani and A. S. Putra, “Sistem Informasi Monitoring Inventori Barang Pada Balai Riset Standardisasi Industri Bandar Lampung,” *J. Inform.*, vol. 13, no. 1, pp. 90–98, 2014.
- [2] A. S. Putra, “Paperplain: Execution Fundamental Create Application With Borland Delphi 7.0 University Of Mitra Indonesia,” 2018.
- [3] A. S. Putra, “2018 Artikel Struktur Data, Audit Dan Jaringan Komputer,” 2018.
- [4] A. S. Putra, “ALIAS MANAGER USED IN DATABASE DESKTOP STUDI CASE DB DEMOS.”
- [5] A. S. Putra, “COMPREHENSIVE SET OF PROFESSIONAL FOR DISTRIBUTE COMPUTING.”
- [6] A. S. Putra, “DATA ORIENTED RECOGNITION IN BORLAND DELPHI 7.0.”
- [7] A. S. Putra, “EMBARCADERO DELPHI XE 2 IN GPU-POWERED FIREMONKEY APPLICATION.”
- [8] A. S. Putra, “HAK ATAS KEKAYAAN INTELEKTUAL DALAM DUNIA TEKNOLOGY BERBASIS REVOLUSI INDUSTRI 4.0.”
- [9] A. S. Putra, “IMPLEMENTASI PERATURAN PERUNDANGAN UU. NO 31 TAHUN 2000 TENTANG DESAIN INDUSTRI BERBASIS INFORMATION TECHNOLOGY.”
- [10] A. S. Putra, “IMPLEMENTATION OF PARADOX DBASE.”
- [11] A. S. Putra, “IMPLEMENTATION OF TRADE SECRET CASE STUDY SAMSUNG MOBILE PHONE.”
- [12] A. S. Putra, “IMPLEMENTATION PATENT FOR APPLICATION WEB BASED CASE STUDI WWW. PUBLIKLAMPUNG.

- COM.”
- [13] A. S. Putra, “IMPLEMENTATION SYSTEM FIRST TO INVENT IN DIGITALLY INDUSTRY.”
- [14] A. S. Putra, “MANUAL REPORT & INTEGRATED DEVELOPMENT ENVIRONMENT BORLAND DELPHI 7.0.”
- [15] A. S. Putra, “PATENT AS RELEVAN SUPPORT RESEARCH.”
- [16] A. S. Putra, “PATENT FOR RESEARCH STUDY CASE OF APPLE. Inc.”
- [17] A. S. Putra, “PATENT PROTECTION FOR APPLICATION INVENT.”
- [18] A. S. Putra, “QUICK REPORT IN PROPERTY PROGRAMMING.”
- [19] A. S. Putra, “REVIEW CIRCUIT LAYOUT COMPONENT REQUIREMENT ON ASUS NOTEBOOK.”
- [20] A. S. Putra, “REVIEW TRADEMARK PATENT FOR INDUSTRIAL TECHNOLOGY BASED 4.0.”
- [21] A. S. Putra, “TOOLBAR COMPONENT PALLETTE IN OBJECT ORIENTED PROGRAMMING.”
- [22] A. S. Putra, “WORKING DIRECTORY SET FOR PARADOX 7.”
- [23] A. S. Putra, “ZQUERY CONNECTION IMPLEMENTED PROGRAMMING STUDI CASE PT. BANK BCA Tbk.”
- [24] A. S. Putra, D. R. Aryanti, and I. Hartati, “Metode SAW (Simple Additive Weighting) sebagai Sistem Pendukung Keputusan Guru Berprestasi (Studi Kasus: SMK Global Surya),” in *Prosiding Seminar Nasional Darmajaya*, 2018, vol. 1, no. 1, pp. 85–97.
- [25] A. S. Putra and O. M. Febriani, “Knowledge Management Online Application in PDAM Lampung Province,” in *Prosiding International conference on Information Technology and Business (ICITB)*, 2018, pp. 181–187.
- [26] A. S. Putra, O. M. Febriani, and B. Bachry, “Implementasi Genetic Fuzzy System Untuk Mengidentifikasi Hasil Curian Kendaraan Bermotor Di Polda Lampung,” *SIMADA (Jurnal Sist. Inf. dan Manaj. Basis Data)*, vol. 1, no. 1, pp. 21–30, 2018.
- [27] A. S. Putra, H. Sukri, and K. Zuhri, “Sistem Monitoring Realtime Jaringan Irigasi Desa (JIDES) Dengan Konsep Jaringan Sensor Nirkabel,” *IJEIS (Indonesian J. Electron. Instrum. Syst.)*, vol. 8, no. 2, pp. 221–232.
- [28] D. P. Sari, O. M. Febriani, and A. S. Putra, “Perancangan Sistem Informasi SDM Berprestasi pada SD Global Surya,” in *Prosiding Seminar Nasional Darmajaya*, 2018, vol. 1, no. 1, pp. 289–294.