Laporan Pendahuluan – Praktikum Keamanan Data

Dimas Rizky H.P. – 2110141011 – 3 D4 IT A

IDS & Host-IDS

Intrusion Detection System (IDS) ditujukan untuk mendeteksi, memantau keadaan komputer dan melaporkan kejadian berdasarkan anomali jaringan yang disebabkan oleh adanya intruder pada jaringan. Setelah tahap pendeteksian, umumnya IDS disetting agar memberi informasi ke network administrator agar NetAdmin dapat melakukan sesuatu.

Tipe IDS terbagi menjadi dua, yaitu host-based dan network-based IDS. Contoh program IDS yang bertipe hostbase IDS adalah Tripwire. Tripwire berfungsi untuk menjaga integrity dari file sistem dan direktori. Metodenya adalah dengan mencatat setiap perubahan yang terjadi pada file dan direktori. Penggunaannya digunakan untuk mempermudah system administrator untuk mengamankan system yang berjalan.

Host-based IDS (HIDS) adalah IDS yang bertugas mengamati dan menganalisa kondisi internal dari sistem komputer. HIDS merupakan tipe IDS yang dibuat dengan pada awalnya target dari IDS ini adalah melindungi komputer mainframe.

Berbeda dengan HIDS, network-based IDS bertugas untuk memantau traffic jaringan yang keluar masuk ke komputer. Cara kerjanya adalah dengan menempatkan NIC dalam mode promiscuous untuk menangkap semua traffic jaringan yang melewati segmen jaringan tersebut. Network-based IDS bekerja dengan melihat packet yang keluar masuk melalui jaringan komputernya. Contoh program network-based IDS adalah AXENT, Cisco, CyberSafe, ISS, dll.

Secara garis besar, tujuan kedua tipe sama, yaitu memberi tahu administrator jika terjadi anomali. Sehingga, segera setelah network/system administrator mengetahui adanya intrusion/anomali, mereka dapat melakukan tindakan protektif terhadap anomali tersebut

Detailnya, cara kerja Tripwire adalah dengan melakukan perbandingan file dan direktori yang ada dengan database system yang dibuat pada saat Tripwire diinstall. Perbandingannya meliputi perubahan tanggal file, ukuran, tanggal penghapusan file di folder dan lain lain. Setelah tripwire dijalankan, aplikasi ini secara otomatis akan melakukan pembuatan database sistem. Kemudian secara periodek database akan di update dengan laporan setiap perubahan file dan direktori.

Cara Instalasi Tripwire :

1. Login sebagai root
2. Update system menggunakan perintah $apt-get update
3. Lalu install tripwire menggunakan perintah $apt-get install tripwire
4. Pada saat ditanyakan site key passphrase dan local key passphrase, masukan keynya
5. Setelah selesai instalasi, ubah mode file dari file tripwire : *tw.cfg & tw.pol* dengan perintah $chmod 0600 tw.cfg tw.pol
6. Lakukan konfigurasi file policy pada direktori /etc/tripwire
7. Lakukan inisialisasi database
8. Lalu jalankan tripwire

Tripwire sendiri dapat mendeteksi dua jenis aturan yang didefinisikan dalam policy file, dua aturan tersebut adalah Normal rule dan Stop Points. Normal rule digunakan untuk mendefinisikan properti dari file tertentu atau direktori yang dipantau oleh tripwire. Sedangkan stop points digunakan untuk mengecualikan file tertentu atau direktori tertentu dari pemantauan tripwire.