Laporan Pendahuluan – Host Based IDS

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

**DEFINISI HOST-BASED IDS**

Host-based IDS(*Intrusion Detection System)* adalah IDS yang memantau kondisi sistem komputer untuk mendeteksi adanya anomali/penyalahgunaan dan bertanggung jawab terhadap log activity pada komputer. Jika ada sesuatu yang mencurigakan, HIDS akan memberikan notifikasi kepada system administrator agar system administrator dapat melakukan aksi pencegahan atau sejenisnya.

**CARA KERJA HOST-BASED IDS**

Cara kerja host-based IDS adalah dengan cara memantau file sistem atau file-file lainnya yang memang di*assign* kan oleh sistem administrator kepada HIDS. Biasanya, host-based IDS memantau file file penting dan vital yang ada di sistem komputer, yang keberadaannya sangat berpengaruh besar terhadap keamanan sistem komputer. Host-based IDS memantau sebuah file berdasarkan atribut :

* Ukuran file,
* Tanggal pembuatan, dan tanggal last-modified
* Ownership sebuah file,
* Tipe akses sebuah file,
* Permission sebuah file,
* Checksum
* Dll

**FILE YANG TERLINDUNGI OLEH HOST-BASED IDS**

Pada linux, direktori direktori yang vital dan secara umum akan diawasi oleh HIDS antara lain direktori penyimpan konfigurasi aplikasi yang terinstall, yaitu */etc* lalu direktori yang berisi aplikasi penting yang ada di linux, yaitu */usr/bin,* dan */usr/sbin*. Sebagian file yang ada di Linux, ada yang tidak perlu di monitor oleh host-based IDS karena file tersebut selalu berganti setiap detiknya, atau file file tersebut sering digunakan dalam waktu waktu biasa, antara lain file yang berada di direktori */home*, file log yang ada pada direktori */var*, lalu file temporary pada direktori */temp* lalu file file aplikasi yang bersifat dinamis pada direktori */dev*.

Pada saat instalasi, dan ketika melakukan monitoring sebuah file/object, HIDS harus melakukan inisialisasi checksum-databasenya terlebih dahulu dengan cara melakukan scanning object yang terkait. Sekali administrator telah memiliki object databased, HIDS dapat mulai melakukan monitoring object/file tersebut dan akan melaporkan adanya anomali/perubahan ke administrator lewat email ataupun media yang lain. Laporan yang dikirim bisa berupa logs, e-mail atau pemberitahuan yang lain.

**Contoh Host-Based IDS**

Salah satu contoh HIDS adalah Tripwire. Tripwire merupakan software opensource yang dapat memonitor dan memberitahukan adanya perubahan file atau beberapa jumlah file yang ada pada sistem komputer. Ketika pertama kali dinisialisasi, tripwire akan melakukan scan pada file system seperti yang sudah diarahkan oleh administrator dan menyimpan hasil scan nya di database yang disediakan.

Tripwire bekerja menggunakan *cryptographic hashes* untuk melakukan check perubahan sebuah file tanpa harus menyimpan seluruh atribut yang ada pada database. Selain itu, tripwire juga menyediakan fitur *integrity assurance*, *change management* dan *policy compliance.*

Beberapa masalah pada saat melakukan instalasi tripwire adalah, modul policy yang ada pada tripwire tidak secara default terinstall pada komputer pengguna. Sehingga pada saat awal instalasi tripwire modul policy harus direvisi terlebih dahulu dengan membuang policy yang dipasang pada modul yang tidak dimiliki pada komputer