Ramandika Pranamulia
13512078

Ringkasan Paper

Intrusion Detection System

by: Craig HI Rowland

Paper ini menjelaskan secara umum bagaimana Intrusion Detection System/IDS dapat diatasi pada sistem komputer. Pada umumnya IDS mendeteksi adanya intruder melalui pengamatan perilaku user pemakai dengan user profile sistem. Jika IDS mendapati adanya intruder maka IDS akan melakukan aksi untuk merespon event intrusion yang terjadi. Ada beberapa macam teknik dalam mengamati dan membandingkan antara perilaku *current user* dengan *user profile* diantaranya adalah sebagi berikut

1. Membandingkan current user behavior dengan rule set yang sudah dibuat berdasarkan user profile. Penyimpangan yang signifikan dari user behavior terhadap rule set akan membuat IDS menyimpulkan adanya intrusion.
2. Expert system, sama halnya dengan poin no satu, namun pada expert system perilaku tidak wajar juga dianalisis untuk meghasilkan rule.
3. Passive IDS, tidak dapat membuat rule based secara mandiri. Harus diberikan data secara langsung kepada sistem passive IDS seperti halnya antivirus.

Intrusion detection system yang ada sudah dapat menangani *intrusion* dengan *realtime* namun masih sangat rentan terhadap kasus *false positive* dan *false negative*. False positive adalah keadaan dimana IDS sistem menginterpretasi suatu event yang nyatanya bukan intrusion sebagai intrusion, sedangankan false negative adalah suatu keadaan dimana sistem IDS tidak dapat mendeteksi intrusion yang sedang atau sudah terjadi.

Komentar: Paper ini memberikan gambaran secara umum mengenai sistem IDS yang sudah dikembangakan sejauh ini dan kelemehan masing masing sistem IDS yang sudah dikembangkan. Paper ini juga memberikan gambaran secara umum bagaimana suatu IDS mendeteksi intrusion / apa saja yang dimonitor oleh sistem IDS untuk membuat rule.

An Architecture for Intrusion Detection using Autonomous Agents

by: Jai Sundar Balasubramaniyan et all

Paper ini menjelaskan secara umum kelemahan IDS yang sering digunakan sekarang yaitu hanya terdapat pada satu entitas sistem misalkan suatu router atau suatu pc, padahal pada suatu entity tidak semua data melewati entitas tersebut sehingga dapat diproses. Paper ini mengusulkan framework sistem IDS yang lebih baik dengan cara mendistribusikan komponen IDS pada jaringan, salah satu framework yang dijelaskan adalah AAFID. Suatu sistem IDS terdiri dari *agents, transceivers*, dan *monitors* yang akan disebar pada jaringan.

Komentar: Paper ini memberikan pemahaman mengenai komponen yang ada pada IDS dan fungsi masing masing komponen. Paper ini juga memberikan suatu metode untuk memmbuat sistem IDS yang scalable yaitu AAFID dengan metode dasar distributed system.

Ramandika Pranamulia
13512078

An Architecture for Intrusion Detection using Autonomous Agents

by: Yongguang Zhang, Wenke Lee

Paper ini menjelaskan mengenai IDS pada AD-Hoc wireless network yang sering digunakan pada mobile device. Paper ini memberikan suatu penjelasan mengenai framework yang tepat digunakan pada Ad-hoc network dengan IDS sistem disetiap node yang saling bekerja sama dengan IDS pada node lainnya untuk melindungi Ad-hoc network dari intrusion.Pada paper ini juga dibahas bagaimana cara mengatasi *anomaly intrusion* pada Ad-hoc network

Komentar: Framework IDS yang dijelaskan pada paper ini dirasa lebih reliable untuk Ad-hoc network dibandingkan dengan metode no 2 dikarenakan implementasi dan algoritma yang lebih sederhana mudah untuk mobile device. Namun untuk network yang lebih besar nampaknya framework ini akan berjalan lebih lambat dibanding framework yang diusulkan oleh Jai sundar yang sudah dijelaskan sebelumnya.

General Security Support for the Linux Kernel
by: Chris Wright and Crispin Cowan, Stephen Smalley

Paper ini mengenalkan Linux Security Modules frameworks sebagai jawaban dari permasalahan security pada linux. Linux Security Modules framework adalah suatu loadable kernel modul yang berisi implementasi akses control yang sudah ditingkatkan kualitasnya dengan bebarapa fungsi tambahan di luar fungsi access control seperti yang diterapkan pada native linux system.

Komentar: Paper ini menjelaskan bagaimana kita bisa mengimplementasi kernel module tambahan buatan kita pada sistem operasi linux dengan menggunakan Linux Security Modules frameworks.

A Data Mining Framework for Building Intrusion Detection Models
by: Wenke Lee, Salvatore J. Stolfo, Kui W. Mok

Paper ini menjelaskan cara menggunakan data mining untuk membangun model *intrusion*. Paper ini membahas mengenai metode yang sering digunakan pada IDS yaitu classification, link analysist, dan sequence analysis. Classification adalah suatu cara untuk menentukan suatu event normal atau tidak normal dengan melihat kelas yang sudah didefiniskan sebelumnya. Kelas tersebut dibangun berdasarkan data user profile terdahulu. Link analysist adalah korelasi fitur sistem dengan audit data, contohnya adalah command pada terminal dengan argument inputnya yang biasa digunakan normal user sebagai knowledge dasar untuk menentukan suatu event intrusion atau tidak. Sequence mining bertujuan untuk menentukan urutan event berdasarkan waktu yang sering muncul bersamaan atau berurutan.

Komentar: Paper ini memberikan gambaran jelas bagaimana cara melakukan data mining terhadap data network untuk menentukan adanya IDS atau tidak.