

Proposal Tugas Besar
Sistem Keamanan Lanjut (EC 7010)
Dosen: Dr. Ir. Budi Rahardjo



Nama : Puji Hartono
NIM : 232 05 027

Program Pasca Sarjana
Institut Teknologi Bandung
2006

Sistem Pencegahan Penyusupan (IPS) pada Jaringan Berbasis Snort IDS dan IPTables Firewall

Latar Belakang

Berkembangnya teknologi informasi khususnya jaringan komputer dan layanan-layanannya di satu sisi mempermudah pekerjaan-pekerjaan manusia sehari-hari, akan tetapi di sisi lain timbul masalah yang sangat serius, yakni faktor keamanannya. Di satu sisi manusia sudah sangat tergantung dengan sistem informasi, akan tetapi di sisi lain statistik insiden keamanan meningkat tajam. Hal ini secara umum terjadi karena kepedulian terhadap keamanan sistem informasi masih sangat kurang.

Untuk mencegah insiden keamanan perlu dilakukan langkah-langkah preventif baik teknis ataupun non teknis.

- Pencegahan dengan non teknis seperti membuat security policy yang baik dan terkendali.
- Pencegahan secara teknis dilakukan dengan langkah-langkah hardening di sistem operasi, aplikasi, infrastruktur jaringan, implementasi Sistem Pencegahan Penyusupan dan lain sebagainya.

Tujuan dan Batasan Masalah

Berdasarkan latar belakang di atas, tulisan ini akan membahas pencegahan penyusupan secara teknis yang secara khusus berupa hardening system dengan IPS berbasis Snort IDS dan IPTables Firewall, yakni sebuah system yang mampu melakukan deteksi dan kemudian pencegahan terhadap usaha penyusupan yakni dengan memblok (menutup) akses paket data yang berasal dari penyusup tersebut. Implementasi sistem pencegahan penyusupan ini dalam sebuah PCRouter dengan yang terkoneksi ke konsentrator berupa HUB dengan kabel UTP sebagai media koneksinya. Dalam tulisan ini tidak dibahas bagaimana implementasi teknis jika sistem pencegahan penyusupan ini diimplementasikan dengan konsentrator berupa switch ataupun jika diimplementasikan pada jaringan dengan *traffic* yang sangat padat.

Referensi

1. Budi Rahardjo. Security Tools untuk pengamanan, Firewall dan Intrusion
2. Detection System (IDS). IndoCisc
3. IDS FAQ, <http://www.sans.org/resources/idfaq/> Sans.
4. SnortTMUsers Manual The Snort Project, 2006.
5. Snort FAQ The Snort Project, 2006.
6. IPTables Manual