

**PROPOSAL PROYEK AKHIR
KEAMANAN SISTEM INFORMASI (EC-5010)
SECURITY PADA LEVEL KERNEL
Hankky Arief (13200035)**

Abstraksi

Dengan semakin banyaknya lubang keamanan terhadap sistem komputer, tidak akan mungkin ada sistem yang betul-betul aman/trusted. Namun, mengamankan sistem komputer melalui kernel space (Kernel Security) nampaknya bisa melindungi bagian-bagian terpenting dari sistem komputer. Kernel security dilakukan dengan memperbaiki (mem-patch) kernel sehingga ia dapat memproteksi dirinya maupun program/data yang penting/kritis. Kernel security patch yang tersedia saat ini, antara lain: Openwall kernel patch, LIDS (Linux Intrusion Detection System), Medusa DS9, LoMac, RSBAC (Rule Set Based Access Control) dan lainnya. Pada proyek akhir ini saya ingin mencoba patch Medusa DS9 dan melihat kemampuan sekuriti yang diberikannya.

Overview Medusa

Medusa adalah package yang memperbaiki tingkat keamanan sistem operasi linux dengan memperluas arsitektur keamanan standar linux. Medusa terdiri dari dua bagian: sebuah patch kecil untuk kernel linux dan daemon pada user space (dengan nama "Constable") sebagai implementasi authorization server. Cara kerjanya: pada saat operasi tertentu akan dieksekusi, kernel akan bertanya ke authorization server untuk konfirmasi, yang kemudian mengizinkan atau melarang operasi tersebut. Authorization server ini juga dapat mempengaruhi jalannya operasi yang dieksekusi. Penyetingan Constable dilakukan melalui file konfigurasinya yang terdapat di /usr/local/etc/constable.conf.

Beberapa contoh penggunaannya, antara lain:

1. Melindungi sebuah file sehingga tidak dapat dihapus bahkan oleh root sekalipun
2. Mengubah jalannya eksekusi suatu operasi, misal: user dari luar memiliki file passwd dan shadow yang palsu
3. Medusa DS9 menggunakan konsep virtual space. Hal ini memungkinkan kita meng-assign suatu proses atau file ke virtual space. Proses yang berada di virtual space tidak akan dapat melihat, mengubah, atau mempengaruhi proses atau file yang ada di virtual space yang lain. Misalnya: kita assign FTP daemon pada virtual space nomor 1, lalu file-file pada /etc kita beri virtual space nomor dua.
4. Memonitor system calls
5. Menjalankan code/fungsi tertentu didalam suatu proses, layaknya code tersebut terkompilasi sebagai satu kesatuan dengan proses itu, misalnya: kita dapat memaksakan eksekusi fungsi `exit` ketika ada user/program yang ingin menghapus file tertentu.

Pada makalah akan diberikan analisis arsitektur medusa (cara kerja), kemampuan-kemampuannya, dan hasil dari percobaan penggunaannya. Sampai saat ini, saya baru mem-patch kernel saya (2.4.22) dengan patch dari medusa tersebut, namun belum mencoba untuk mengkonfigurasikannya.

Referensi:

- <http://medusa.fornax.sk/>
- Berbagai dokumen mengenai linux kernel security