Tips Keamanan Host Server

Alwin Sanjaya
aak_drs@yahoo.com

Kali ini saya ingin memberikan tips untuk keamanan Host Server, tetapi disini saya tidak membahasnya dengan detail. Dengan kata lain saya akan menjelaskan secara umumnya saja.… yah …untuk lebih lanjut silahkan anda membaca buku-buku atau artikel online tentang keamanan lainnya.

Administrasi Account

Didalam masalah keamanan Host Server administrasi akun adalah masalah yang sangat penting, kenapa akun?seorang user bisa saja mengobrak-abrik pertahanan server anda walaupun seberapa hebatnya keamanan sever anda. Dalam hal keamanan saya sarankan agar tidak percaya dengan user manapun walaupun itu adalah teman sendiri, karena suatu saat si user ini akan bisa membobol keamanan anda, sebagai contoh anda berteman dengan A yang sebagai si user dan anda adalah si superuser atau yang memegang sebagai root, karena anda sangat percaya dengan si A maka anda memberikan password root kepada si A. Suatu ketika anda menyakiti perasaan A karena suatu hal, karena si A sakit hati maka si A ingin membalasnya dengan cara mengobrak-abrik Host Server yang sedang anda kelola, padahal keamanan Host Server anda terkenal sangat kuat dan sekarang hancur karena hal sekecil ini. Nah, ini adalah gambaran agar kita tidak percaya kepada orang yang sangat kita percaya sekalipun (hmmm udah kaya' di film Anti Trust yah….☺)…perlu diketahui juga tipe penyerangan seperti ini dikenal dengan istilah **Vandal** yang mana tipe penyerangan ini yang dilakukan oleh user yang sakit hati dan kemudian menyerang system dengan berniat untuk menghancurkannya untuk balas dendam.

Oleh karena itu sebaiknya superuser dan group administrator tidak diberikan kepada sembarang orang, masalah lainnya yang umum adalah masalah user non administrator. Untuk user-user yang sudah tidak digunakan lagi lebih baik dihapus, ini digunakan untuk memperkecil kemungkinan penyerang yang masuk kedalam system anda. Dan untuk memudahkan anda mengontrol user-user yang masih aktif.

Administrasi Password

Password…dengar kata password sudah pasti berhubungan dengan sesuatu yang sangat rahasia, yang bahayanya lagi kita lebih suka mengetahui rahasia orang lain…nah inilah salah satu tugas sang sysadmin untuk mengamankannya. Administrasi password sangat dibutuhkan untuk menghindari celah keamanan yang memungkinkan untuk dibobol oleh orang yang tidak bertanggung jawab. Masalah yang sering ditemukan adalah user yang tidak memiliki password, kebanyakan si user malas untuk menghafalkan password untuk accountnya. Ini sangatlah berbahaya, karena penyerang bisa saja memanfaatkan user yang tidak berpassword untuk sarana masuk kedalam system, oleh karena itu tugas sysadmin yang baik adalah mengecek tiap-tiap user, jika ditemukan ada user yang tidak memiliki password secepatnya diberitahu untuk membuat password jika teguran anda tidak dihiraukan sebaiknya anda menghapus accountnya.

Password sangatlah penting, maka dari itu pastikan password pada system anda tidak boleh diakses oleh user lain, lebih baik password superuser anda diganti dengan berkala sebagai contoh :
Minggu ini anda menggunakan password : p45c4l
Minggu depan anda sudah harus ganti dengan password lain, misal: w4k3upm4n
Hal ini sangat penting, untuk menghindari pengaksesan oleh user lain yang mengetahui password lama anda.
Jika anda menggunakan linux, sebaiknya password anda di shadow. Ini sangat ampuh untuk membingungkan si penyerang, karena selain dienkripsi password itu juga disembunyikan pada file lain.

Saran untuk pembuatan password:

1. Buatlah password sesulit mungkin tapi mudah untuk dihafal, kalau bisa gunakan kombinasi antara huruf dan character ini sangat ampuh untuk mempersulit si penyerang.
2. Menset batas berlakunya password.
3. Menggunakan password berkala.

Administrasi Akses

Administrasi Akses yang dimaksudkan adalah administrasi pada direktori maupun file penting yang perlu dijaga agar tidak dapat diakses oleh user lain. Usahakan selalu file atau direktori anda tidak bisa diakses oleh orang lain sekalipun itu orang yang sangat anda percaya.

Administrasi Layanan

Kebanyakan penyerang melakukan penyerangan melalui fasilitas yang satu ini, Host Server memiliki banyak port yang terbuka ketika layanan itu dibuka, sebagai contohnya anda memiliki Host Server sebagai Web Server dan Mail Server maka sebaiknya anda cukup membuka kedua layanan ini saja. Karena makin banyak port anda yang terbuka maka makin besar kemungkinan Server anda diserang. Karena pada umumnya penyerang akan melakukan scanning sebelum melakukan penyerangan, scanning ini

bertujuan untuk mengetahui port mana saja yang terbuka dan yang memungkinkan untuk di “masuki”.
Hal yang penting lainnya adalah memastikan bahwa program server yang anda jalankan benar-benar aman, dengan kata lain sebaiknya anda harus rajin-rajin meng-Up date program server anda, ini dikarenakan program server terkadang memiliki bug yang suatu saat bisa diekslpoitasi oleh penyerang untuk memperoleh akses.
Carilah program server yang memiliki fasilitas enkripsi untuk transfer datanya misalnya SSH (Secure Shell) untuk telnet, dan Apache + SSL untuk WWW. Hal ini untuk mencegah kebocoran data pada saat transfer data lewat daerah rawan.

Administrasi Log File

Disamping melakukan semua hal yang telah dibahas diatas, hal yang satu ini juga penting yaitu mencatat semua kegiatan yang terjadi pada system. Setiap kegiatan pada system pada umumnya sudah otomatis terekam pada log file. Nah tugas anda adalah rajin-rajinlah memeriksa log file untuk melihat setiap kegiatan-kegiatan yang terjadi, jika ditemukan kegiatan-kegiatan yang mencurigakan, misalnya upaya login berulang-ulang.
Beberapa program dapat memonitor system anda dan mendeteksi kalau ada hal-hal yang mencurigakan. Installah program semacam ini dan periksalah hasil monitoring secara berkala. Ini akan sangat berguna untuk mencegah adanya penyerangan terhadap system anda.
Disarankan untuk Host Server sebaiknya menggunakan Linux Operating System.

Cukup sekian saja tips dari saya, jika tips-tips ini dijalankan dengan disiplin… 99% keamanan Host Server anda terjaga dengan baik. (kok 99%?…hehehe…yang 1%nya kalau kita lagi teledor aja …☺) semoga bisa membantu (Amin).

Ini adalah beberapa alamat website yang berisi informasi keamanan secara umum:
http://www.securityfocus.com
http://www.lists.gnac.net/firewalls/
http://www.nfr.com.mailman/listinfo/firewall-wizards
http://www.sans.org/sansnews/
http://www.cert.org/
http://www.safemag.com/
http://www.ciac.org/
http://www.linuxsecurity.com/
http://www.insecure.org/
dan ini adalah alamat website yang mengulas tentang keamanan web:
http://www.w3.org/security/faq/
http://www.securityportal.com
http://www.2600.com
http://www.go2net.com/people/paulp/cgi-security/
http://www.consensus.com/security/ssl-talk-faq.html

Referensi :

1. Mengamankan Web Server dari Serangan Hacker / Cracker, Frans Newman.