

# Meminimalisasi server dari serangan hacker

Kontribusi Dari Administrator

Kamis, 29 Oktober 2009

Pemutakhiran Terakhir Senin, 02 November 2009

Ada beberapa metoda yang digunakan untuk meminimalisasi server dari serangan hacker ke server yang di fungsikan bersama-sama untuk saling melengkapi.

## 1. Intrusion Prevention System

Intrusion Prevention System (IPS) adalah suatu perangkat active yang bekerja berdasarkan signature base dan anomali traffic base yang diletakkan diantara koneksi internet menuju ke perangkat server.

Segala jenis traffic yang sesuai dengan signature atau traffic yang anomali akan di block oleh IPS sebelum menuju server.

## 2. Firewall

Firewall berfungsi untuk membuka/menutup port dari dan menuju server.

Sehingga port yang dapat di akses dari user hanya di batasi port tertentu saja.

Firewall juga membatasi akses untuk server2 tertentu, yang dapat di akses dari ip tertentu.

Pada firewall ini juga dilakukan Network Address Translation (NAT) sehingga user tidak mengetahui IP sebenarnya dari server.

## 3. Hardening Operating System

Di level operating system perlu dilakukan hardening dengan mematikan semua service yang tidak di gunakan, serta melakukan update patch (bila ada) untuk menutup kelemahan di sisi operating system.

## 4. Application Security

Sisi lain yang diperhatikan adalah pembuatan script pada suatu aplikasi atau aplikasi itu sendiri, harus dipastikan bahwa aplikasi tersebut tidak dapat di exploit melalui layer aplikasi.

## 5. Konfigurasi Bertingkat

Yang di maksud dengan konfigurasi bertingkat adalah pemisahan perangkat menjadi Front End server, Middle End server dan Back End Server.

Front End Server, adalah server yang di khususkan diletakkan langsung berhadapan dengan pengakses. Biasanya pada server ini tidak terdapat data. Data yang di akses dihasilkan dari server di belakangnya (Middle dan back End Server).

Middle End server, adalah suatu server yang memiliki data dan aplikasi yang di butuhkan pengakses. Biasanya server middle ini tidak bisa langsung di akses oleh pengakses, tetapi melalui front end server.

Back End Server, adalah suatu server seperti database yang memiliki data yang di butuhkan tetapi tidak bisa di akses langsung oleh pengakses. Backend server ini hanya dapat di akses oleh Middle End server.

Dengan strukture bertingkat ini diharapkan bila terjadi serangan maka yang terkena dampaknya hanyalah server yang terletak di Bagian depan (Front End Server), sedangkan data tetap terjaga.

## 6. Backup

Tingkat terakhir dari pengamanan yang diterapkan adalah melakukan Backup data baik menggunakan tape library, disk backup maupun menggunakan standby server.