Database Security

Database Security

Apa itu database?

kumpulan data yang disimpan dan diatur/ diorganisasikan sehingga data tersebut dapat diambil atau dicari dengan mudah/ efisien

Contoh database engine:

- Sql Server
- MS Access
- Oracle Database
- MySQL
- Firebird
- PostgreSQL
- DB2

Database Security

- Merupakan komponen penting dalam infrastruktur informasi
- Aplikasi-aplikasi sistem informasi hampir semuanya menggunakan database
- Situs-situs e-commerce atau situs-situs lainnya menggunakan database untuk menyimpan informasi dari visitor
- Apakah perlu diamankan ?? PERLU!
- Pada prakteknya tidak demikian → jarang diperhatikan dan sering diabaikan
- Kenapa ??

  Karena mereka lebih memperhatikan web server atau application server ketimbang database server

Database Security

- Perhatian lebih banyak diberikan untuk perlindungan terhadap serang DoS dan deface
- Apa yang terjadi bila database server diserang??

  akan mengalami kerugian yang besar, bahkan lebih besar dibandingkan kerugian akibat downtime
- Apa yang dilakukan oleh hacker terhadap database server?

  bukan menghapus

  bukan merubah

  bukan merusak

  tetapi MENCURI !!

Database Security

Apa dampak dari pencurian database?

- Paling ringan: Perusahaan HANYA akan kehilangan waktu dan uang untuk biaya penyelidikan
- Menghentikan layanan kepada customer sampai sistemnya dinyatakan dapat dipercaya, misalnya website ditutup sementara waktu
- Diperas oleh pelaku

Database Security

Contoh kasus:

- Desember 2000, situs egghead.com, sebuah toko penjual komputer retail, mengalami pencurian database, diperkirakan 3.7 juta data kartu kredit pembeli telah dicuri
- Tahun 1999, seorang Rusia bernama Maxus, berhasil mencuri data kartu kredit dari cdUniversal dan memeras perusahaan tersebut.
- November 2001, situs playboy.com mengalami hal yang sama
- Musim semi 2001, diperkirakan sebanyak 98000 informasi kartu kredit telah berhasil dicuri
- Maret 2001, FBI melaporkan lebih dari 40 situs perbankan mengalami pencurian oleh hacker dari Rusia dan Ukraina

Database Security

Langkah-langkah yang melindungan database

- Database server harus dikonfigurasi dengan benar, baik database enginenya maupun infrastrukturnya
- Pemberian otoritas user harus sesuai dengan kebutuhan aplikasi
- Sebaiknya password database tidak diberikan kepada user
- Hanya diperbolehkan untuk mengakses data yang diperlukan saja
- Jangan menggunakan user root, system atau selevelnya pada aplikasi untuk mengakses database server
- Jangan pernah user root atau selevelnya tanpa password

Database Security

Bagaimana dengan infrastruktur jaringan?

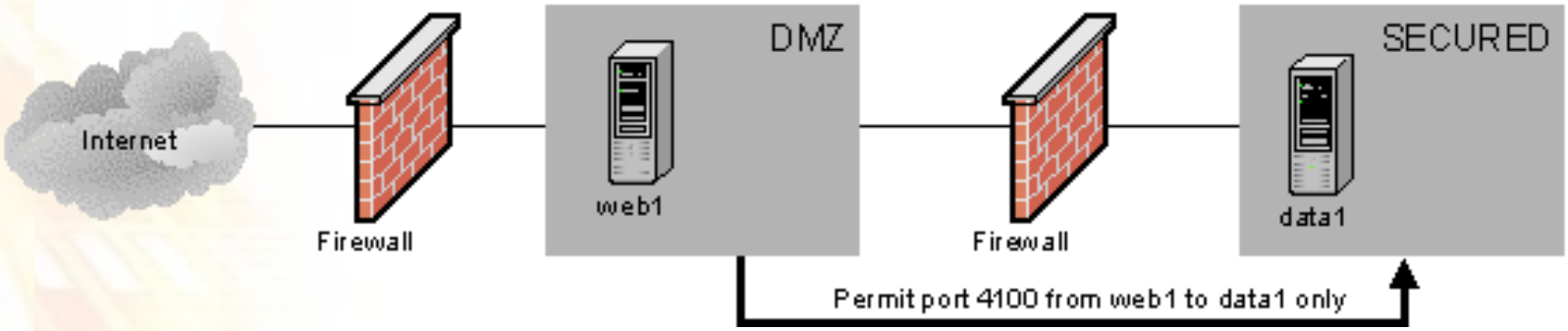
1. Pisahkan database server dari application server
   - Model 3-tier, bukan 2-tier
   - 2-tier, jika hacker berhasil menjebol web server, maka mereka akan memperoleh akses ke database kita.
   - Muncul masalah
     - ada cost untuk server lagi, tetapi lebih murah dibanding kerugian bila database dicuri orang
     - 3-tier→ kinerja menurun karena butuh waktu untuk transfer data antara web dan database server, tetapi pada kenyataannya justru yang butuh waktu lama adalah transfer dari client ke application server
     - Database ←→ Application server cepat, karena intranet

Database Security

2. Jangan menaruh database server di area DMZ
   - Kalau di DMZ, dapat diakses dari publik
   - Ada pemikiran bila ditaruh pada area DMZ dan dipasang firewall maka database server aman
   - Yakin aman?? TIDAK !!
   - Memang benar firewall akan men-drop paket yang datang dari luar menuju ke database server, tetapi tidak men-drop paket yang datang dari area DMZ, misalnya mail server yang telah ‘tercemar’

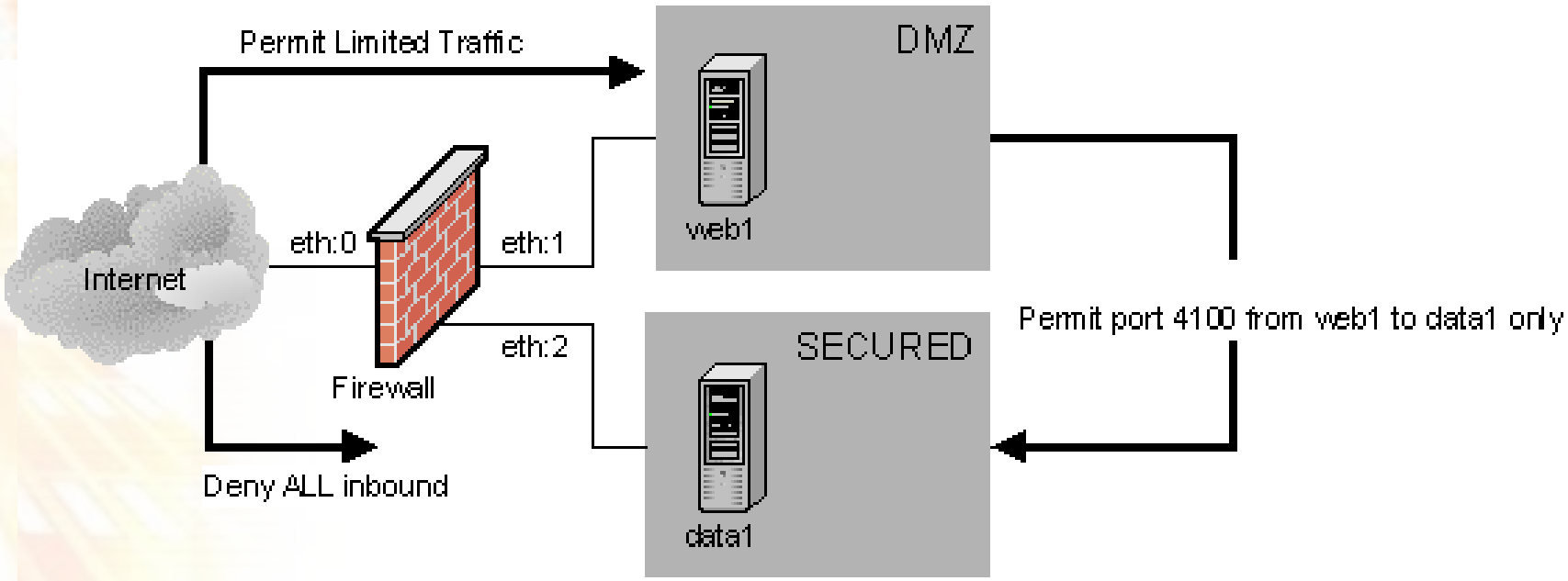
Database Security

Ada 2 cara penerapan database server bila di luar DMZ



- Firewall sebelah kanan, dikonfigurasi agar yang menuju ke ‘data1’ harus berasal dari ‘web1’ dan melalui port 4100
- Jika ada server lain yang ‘tercemar’ di area DMZ, maka server itu tidak dapat menyerang ‘data1’

Database Security



- Firewall dikonfigurasi agar yang menuju ke ‘data1’ harus berasal dari ‘web1’ dan melalui port 4100
- Jika ada server lain yang ‘tercemar’ di area DMZ, maka server itu tidak dapat menyerang ‘data1’
- ‘data1’ tidak menerima paket yang datang dari luar

Database Security

3. Ganti Peralatan Hub dengan Switch

- Untuk menghindari bila intruder memasang program di salah satu server untuk menangkap data yang lewat pada jaringan
- Kebanyakan switch dapat dikontrol melalui telnet konsol
- Apakah dengan memakai switch sudah aman ??
- Bagaimana bila intruder sudah menguasai salah satu server dan berusaha untuk mendapatkan akses ke switch
- Jika switch sudah dikuasai, maka intruder dapat meneruskan trafik di area DMZ ke port dari server yang sudah dikuasai

Database Security

4. Enkripsi Data Antara Web dan Database Server

- Ada yang mengatakan, “Saya sudah menggunakan SSL, sehingga datanya aman”
- Perlu diingat, SSL itu hanya dari client ke web server
- Bagaimana dari web ke database server ?? TIDAK DIENKRIP
- Jadi ?? Trafik data antara web dan database server harus dienkrip
- Caranya ?? Beberapa database engine sudah dilengkapi dengan enkripsi melalui SSL
- Bagaimana kalau belum dilengkapi dengan SSL ?? Bisa menggunakan SSH Port Forwarding dan STunnel

Database Security

Kesimpulan

- Memang benar tidak ada jaringan yang kebal terhadap serangan hacker, namun dengan langkah-langkah pencegahan ini, kita dapat membuat sulit bagi intruder untuk mencuri data baik dari database atau dari lalu lintas data
- Membiarkan database server tanpa pengamanan dengan firewall dan enkripsi akan menimbulkan masalah yang besar
- Pastikan bahwa web server dan database server sudah dipatch dengan versi yang terakhir
- Perlu pendidikan mengenai keamanan administrator jaringan, database administrator dan web programmer
- Pastikan bahwa web programmer/ web developmer dan DBA telah melaksanakan tugasnya dengan baik

TERIMA KASIH