Miskonfigurasi Pada SQL Server, Awal Dari Bencana Besar !!

Sony Arianto Kurniawan
sonyarianto@yahoo.com
The Sony AK Knowledge Center

Bagi Anda orang IT pasti sudah tidak asing lagi mendengar nama Microsoft SQL Server. Produk RDBMS terkenal buatan Microsoft ini memang sangat banyak dipakai di seluruh dunia oleh perusahaan-perusahaan untuk menyimpan informasi dan aset digital mereka. Banyak yang menggantungkan nasib perusahaan pada sang SQL Server.

Namun kesalahan konfigurasi atau miskonfigurasi dari SQL Server bisa menyebabkan suatu keadaan yang fatal bagi sistem database dan bahkan mengakibatkan efek yang berbahaya bagi sistem komputer tempat SQL Server diinstall. Bisa hapus file dan shutdown sistem lho hueheheh ;)

Sebelumnya penulis perlu menjelaskan bahwa artikel ini tidak mempunyai maksud tertentu selain untuk ilmu pengetahuan dan kebebasan dalam berbagi ilmu pengetahuan. Penulis tidak bertanggung jawab apapun terhadap segala sesuatu yang terjadi akibat artikel ini. Artikel ini bersifat terbuka yang berarti Anda bisa memberikan kritik dan saran terhadap artikel ini melalui article@sony-ak.com. Anda dilarang keras mengutip sebagian atau seluruh artikel ini tanpa sepengetahuan penulis.

SQL Server yang akan kita bahas disini menggunakan SQL Server 7 atau bisa juga versi 2000 nya. SQL Server 7 memberikan dua jenis autentikasi untuk mengakses server database yaitu:

1. Windows NT Authentication Mode
2. Mixed Mode

Jika Anda menginstall SQL Server dengan menggunakan Windows NT Authentication Mode maka secara otomatis login ke SQL Server akan mengikuti login Windows NT dan user dari Windows NT sajalah yang berhak untuk mengakses SQL Server.

Jika SQL Server diinstall pada Mixed Mode maka setiap user yang login ke SQL Server bisa diautentikasi oleh Windows NT atau oleh SQL Server itu sendiri. User login yang diautentikasi oleh SQL Server harus memberikan username dan password yang dimaintenance sendiri oleh SQL Server dan ini merupakan salah satu awal bencana.

Ketika Anda menginstall SQL Server pada Mixed Mode maka secara otomatis SQL Server memiliki default account SA (system administrator) dengan password kosong (blank password). Jika Anda login dengan account "sa" ini maka Anda sudah memiliki hak akses sangat luar biasa terhadap SQL Server yang meliputi semua database, tabel, stored procedure, security dan bahkan secara sadar atau tidak Anda juga otomatis memiliki akses besar ke sistem komputer tempat SQL Server diinstall.

Menurut pengamatan penulis dilapangan menunjukkan bahwa masih sangat banyak sekali SQL Server baik yang bersifat production server atau experiment server yang ternyata belum dikonfigurasi dengan benar. Salah satu contoh miskonfigurasi di SQL Server ya seperti yang sudah disebutkan diatas, yaitu DBA nya lupa memberi password untuk account "sa" dan SQL Server diinstall pada Mixed Mode. SQL Server memiliki extended stored procedure xp_cmdshell yang sangat mematikan. xp_cmdshell ini bisa menjalankan perintah shell pada SQL Server seperti jika Anda mengetikkan perintah-perintah shell pada layar console Windows NT. xp_cmdshell ini berada pada database master dan ini juga harus diatur hak pemakaiannya atau jika memang tidak perlu bisa dihapus. Tulisan mengenai SQL Server security check list akan disampaikan pada kesempatan yang lain.

Oh ya, SQL Server bisa diakses oleh berbagai protokol seperti Named Pipe Net-Library atau melalui TCP/IP. SQL Server melalui TCP/IP akan membuka port 1433.

Para pembaca mungkin masih ada yang bingung mengenai bencana apa saja akibat miskonfigurasi diatas. OK, penulis akan memberi contoh beberapa bencana yang mungkin terjadi jika Anda sudah bisa login ke SQL Server sebagai user "sa":

1. Bisa membuat user pada Windows NT dengan level sekelas Administrator.
Ini bisa dicapai dengan cara mengeksekusi command seperti berikut pada SQL Server

```
use master
xp_cmdshell 'net user adminbaru admin /add'
go
xp_cmdshell 'net localgroup Administrators adminbaru /add'
go
```

Dengan perintah diatas maka Anda membuat user adminbaru dengan password admin pada Windows NT dan sekaligus menjadikannya sekelas Administrator.

2. Bisa men-start atau men-stop service pada Windows NT
Ini bisa dilakukan dengan perintah net start atau net stop, contoh berikut adalah untuk men-stop service HTTP pada Windows NT yang berakibat matinya web server :)

```
use master
xp_cmdshell 'net stop w3svc'
go
```

3. Bisa membuat FTP script untuk melakukan suatu download file dari server lain.

4. Bisa digunakan untuk men-deface website ;) Nah kalo yang ini mungkin banyak yang suka ;) Karena men-deface lewat SQL Server jauh lebih mudah daripada lewat bug unicode. Kalo pada bug unicode kita masuk ke sistem sesuai denganhak akses dari user IUSR_MACHINENAME, maka jika kita masuk ke sistem dengan SQL Server maka kita akan masuk dengan hak akses LocalSystem sehingga kita bisa melakukan apa saja di server, termasuk bisa men-shutdown sistem kalo mau :)

5. Bisa untuk mass-defacing, ah masak? Lho iya, penulis sendiri pernah masuk ke host SQL Server

yang kebetulan adalah milik suatu perusahaan web hosting di Israel dan kebetulan didalamnya terdapat puluhan wwwroot untuk beberapa domain yang berbeda. Tinggal copy aja file kita ke masing-masing folder tadi, jadilah sudah mass defacing yang ternyata cuman masuk ke satu host saja huehehe ;)

6. Bisa mengakses registry windows yang berakibat dengan mengambil password Windows NT atau juga membuat key dan value pada registry.

Demikian beberapa bencana yang dapat menimpa sistem Windows NT yang terdapat SQL Server yang belum dikonfigurasi dengan benar. Sebenarnya masih banyak lagi bencana-bencana lain yang dapat muncul dan itu memang tergantung dari imajinasi Anda para hacker ;) Semakin Anda mengerti dan menguasai suatu sistem maka semakin banyak pula trik dan kemampuan Anda untuk mengeksploitasi sistem.

Jika Anda berminat untuk mencoba maka sekarang mulai saja men-scan host yang port 1433 nya terbuka dan jika sudah menemukan host yang port 1433 nya terbuka cobalah akses kesana dengan menggunakan program Query Analyzer atau Anda juga bisa menggunakan SQL Server query dalam mode dos yaitu isql.exe.

Jika Anda ingin mencobanya dengan ISQL maka coba ajah ketikkan perintah berikut untuk login ke SQL Server dari command prompt:

```
C:>isql -S targethost -U sa
```

Kemudian tekan enter, dan akan muncul inputan password, terus tekan enter saja. Jika host tersebut masih menggunakan password blank maka akan muncul SQL prompt seperti dibawah

```
1>
```

Pada prompt tersebut Anda bisa mengetikan perintah SQL anda, misalnya seperti dibawah

```
1>select * from sysusers
2>go
```

OK, akhirnya penulis berpesan bahwa jaga baik-baik SQL Server Anda, jangan lupa untuk mengisi password pada account "sa" (account "sa" tidak bisa di-rename atau dihapus). Sebenarnya masih banyak lagi yang harus diperhatikan pada SQL Server daripada sekedar mengganti password account "sa", tetapi dengan begitu saja sudah meminimalkan intrusion pada sistem Anda.