HARDENING SEKURITI MENGGUNAKAN WINDOWS 2003
(Studi Kasus : Bank X)

Skripsi

Diajukan untuk Memenuhi Syarat Kelulusan Sebagai

Sarjana Teknik Informatika

Disusun Oleh :

FRANKY KAWILARANG

02230032

JURUSAN TEKNIK INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS DARMA PERSADA

JAKARTA

2007

HARDENING SEKURITI MENGGUNAKAN WINDOWS 2003
(Studi Kasus : Bank X)

Skripsi ini

Telah Diterima dan Disahkan Sebagai Salah Satu Syarat Untuk

Memperoleh Gelar Sarjana Strata Satu

Jurusan Teknik Informatika

Disusun Oleh:

FRANKY KAWILARANG

02230032

Mengetahui

Jakarta, Juli 2007

Ketua Jurusan Teknik Informatika	Dosen Pembimbing
(Suzuki Syofian, M. Kom)	(Herianto,Spd, MT)

Skripsi Sarjana yang berjudul :

HARDENING SEKURITI MENGGUNAKAN WINDOWS 2003
(Studi Kasus : Bank X)

Merupakan karya ilmiah yang saya susun dibawah bimbingan Herianto.Spd, MT tidak merupakan jiplakan Skripsi Sarjana atau karya orang lain, sebagian atau seluruhnya dan isinya sepenuhnya menjadi tanggung jawab saya sendiri.

Pernyataan ini saya buat dengan sesungguhnya di Jakarta, pada tanggal 20 Juli 2007.

Penulis

(FRANKY KAWILARANG)

NIM. 02230032

ABSTRAK

Perkembangan komputer di era globalisasi sekarang ini dirasakan sangat penting kegunaannya. Hal ini didukung oleh semakin mudahnya pengguna mengakses dan menggunakan komputer. Namun demikian, kemudahan yang diperoleh dapat menguntungkan pihak lain dalam mengakses data atau sistem dengan tujuan yang tidak baik atau kita lebih mengenalnya dengan julukan *hacker*. Kasus sederhana yang sering terjadi pada suatu perusahaan yang tidak melakukan pengembangan pada divisi Teknologi Informasinya adalah pada saat suatu divisi di suatu perusahaan tidak bisa melanjutkan pekerjaannya karena semua komputer di satu jaringan divisi itu terserang *virus*.

Hardening pada *Sistem Operasi* adalah jalan keluar untuk lebih memperkeras *sistem* yang kita miliki sehingga tidak mudah ditembus oleh sesuatu yang tidak punya hak untuk melihat – lihat atau bahkan merubah *sistem* yang dimiliki oleh *user*. Yang berhak atas full akses permission atas suatu system adalah administrator. *User* yang *login* kedalam *administrator* juga tidak mempunyai *full akses permission*. Inti dari *hardening* adalah mempersempit celah dan hak akses dalam suatu *sistem* dan juga akses kedalam *hardware* itu sendiri. Masing – masing *user* memiliki kebutuhan yang berbeda – beda sehingga *formula hardening* juga tidak sama, tergantung dari pada *sistem* dan kubutuhan para *user*.

Penulis telah mencoba melakukan contoh hardening terhadap : additional security, account policy, event log, system service, registry , file system dan additional registry.

Setelah diujicoba memang terbukti hardening akan meningkatkan security terhadap aktivitas hacker di Bank X.

KATA PENGANTAR

Dengan penuh rasa syukur kehadirat ALLAH SWT, atas Izin-Nya, maka skripsi ini bisa terwujud, penulisan skripsi ini disusun dalam rangka memenuhi salah satu syarat untuk memperoleh gelar kesarjanaan pada Fakultas Teknik, Jurusan Teknik Informatika.

Pada proses pembuatan tugas akhir, banyak sekali bantuan, dukungan, dorongan, dan bimbingan yang sangat berharga sekali bagi penulis, untuk itu pada kesempatan ini penulis ingin menghaturkan rasa terima kasih yang sebesar-besarnya kepada :

1. Ir. Eri Suherman, MT, selaku Dekan Fakultas Teknik Universitas Darma Persada.
2. Suzuki Syofian, M.Kom, selaku Ketua Jurusan Teknik Informatika Universitas Darma Persada yang selalu memberikan motivasi dan arahan dalam menyelesaikan skripsi ini.
3. Bapak Herianto.Spd, MT, selaku dosen pembimbing yang telah meluangkan waktu, tenaga dan pikirannya untuk memberikan bimbingan dan pengarahan serta sarannya bagi penulis dalam menyelesaikan laporan skripsi ini.
4. Seluruh dosen khususnya jurusan Teknik Informatika, Pak Suzuki, Pak Heryanto, Pak Eko, Bu Nur, Bu Eka yang selalu memberikan masukkan serta support yang telah memberikan informasi dan masukan kepada penulis dalam menyelesaikan laporan ini.
5. Khususnya Penulis ingin mempersembahkan Laporan Skripsi ini untuk kedua orang tua tercinta yang telah banyak memberikan doa, dukungan moril dan materil, serta kakak yang telah memberikan dorongan, motivasi dan doanya.

6. Rekan rekan TIF 02 yang telah senasib dan seperjuangan dalam menempuh jenjang SI, Sukses untuk kalian semuanya "amien".

7. Rekan-rekan di Universitas Darma Persada dan semua pihak yang tidak mungkin saya sebutkan satu persatu, yang telah memberikan bantuan dan dukungannya kepada penulis dalam menyelesaikan penulisan laporan skripsi ini.

Penulis menyadari bahwa dalam penyusunan skripsi ini masih banyak terdapat kekurangan dan jauh dari sempurna. Untuk itu penulis berharap saran dan kritik yang dapat membangun penulis agar menuju tingkat yang lebih sempurna dari berbagai pihak manapun.

Akhir kata penulis sampaikan terimakasih atas perhatiannya, semoga skripsi ini dapat bermanfaat bagi pihak manapun dan apa yang penulis hasilkan dapat bermanfaat bagi pihak manapun yang membutuhkan.

Jakarta, Juli 2007

Franky Kawilarang

DAFTAR ISI

		Halaman
LEMBAR JUDUL		i
LEMBAR PENGESAHAN		ii
LEMBAR PERNYATAAN		iii
ABSTRAKSI		iv
KATA PENGANTAR		v
DAFTAR ISI		vii
DAFTAR TABEL		x
DAFTAR GAMBAR		xi
BAB I.	PENDAHULUAN	
	1.1. Latar Belakang Masalah	1
	1.2. Identifikasi Masalah	2
	1.2.1. Rumusan Masalah	2
	1.2.2. Batasan Masalah	3
	1.3. Tujuan Penelitian	4
	1.4. Metode Penelitian	4
	1.5. Sistematika Penulisan	5
BAB II	LANDASAN TEORI	
	2.1. Security	7
	2.1.1. Definisi Security	8
	2.2. Definisi Hardening	8
	2.3. Sistem Operasi	9
	2.3.1. Sejarah Sistem Operasi	10
	2.3.2. Struktur Sistem Operasi	13
	2.4. Program BIOS	20
	2.4.1.Utility Setup BIOS	20
	2.5. TCP/IP	23
	2.6. Group Policy	27
	2.6.1. Local Group Policy	27

2.6.2. Domain Group Policy 27
2.7. Registry..... 28
2.8. File Sistem 31
BAB III ANALISA DAN PERANCANGAN SISTEM
3.1. Analisis Sistem Berjalan 32
3.2. Analisis Kebutuhan 38
3.3. Perencanaan 38
3.3.1. Phisical Security 39
3.3.2. System Policies..... 39
3.3.3. File System..... 40
3.3.4. Registry 41
BAB IV IMPLEMENTASI DAN UJI COBA
4.1. Implementasi 42
4.1.1. Perangkat Keras 42
4.1.2. Perangkat Lunak 43
4.1.3. Implementasi Hardening Windows 2003 43
4.1.3.1. Additional Security Setting 43
4.1.3.2. Account Policies 44
4.1.3.2.1. Paswword Policies 45
4.1.3.2.2. Account Lockout Policy 45
4.1.3.3. Local Policies 45
4.1.3.3.1. Audit Policy 46
4.1.3.4. User Rights Assigment 46
4.1.3.5. Security Option 48
4.1.3.6. Event Log 53
4.1.3.7. System Services 54
4.1.3.8. Registry 58
4.1.3.9. File System 59
4.1.3.10. Additional Registry Setting 61
4.1.3.10.1. Security considerations for network attacks 61
4.1.3.10.2. Configure netbios name release 63

DAFTAR TABEL

Tabel 4.1. Password Policies 45
Tabel 4.2. Account 45
Tabel 4.3. Audit Policy..... 46
Tabel 4.4. User Right assignment 48
Tabel 4.5. Security Options..... 53
Tabel 4.6. Event Log..... 54
Tabel 4.7. System Services..... 58
Tabel 4.8. Registry..... 59
Tabel 4.9. File System..... 61

BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Seorang Direksi suatu perusahaan pasti akan sangat senang apabila memiliki sumber daya manusia yang baik, aktif dan berprestasi. Merasa sangat puas dengan karyawan yang mempunyai kemampuan yang tinggi sehingga memberikan kebebasan kepada mereka dari segi keamanan di sisi teknologi informasinya. Bermain *game*, gosip sesama karyawan melalui *email*, mendengar musik, chating, menurutnya adalah hal normal yang dilakukan oleh karyawan. Selain dari pada itu, komputer yang mereka gunakan juga telah mendukung untuk melakukan semua hal itu. Jadi wajar apabila mereka mendapatkan fasilitas itu. Tetapi akan sangat dikecewakan apabila pada suatu saat kemudian, datang ke kantor dan menemukan ada banyak komputer yang menjadi lambat, sistem operasi *crash*, *virus*, koneksi jaringan putus, dan masih banyak kasus yang mungkin saja terjadi. Itu semua dikarenakan tidak ada *policy* atau aturan yang diberikan. Memang komputer yang semakin canggih memang sangat berguna, tetapi kegunaannya relatif, atau sesuai dengan kebutuhan masing –masing user atau *group* dalam suatu lingkup jaringan ataupun *stand alone*.

Kasus serupa yang ada pada Bank X adalah seringkali user menggunakan File Sharing untuk saling bertukar data, menginstall aplikasi yang bukan merupakan aplikasi standar dari Bank X, mengaktifkan soundcard pada masing-masing computer client, mengaktifkan port USB untuk membawa atau mengcopy

data dari luar yang kemungkinan data tersebut sudah terinfeksi virus dan merubah konfigurasi hardware yang ada pada BIOS(Basic Input Output System. Untuk masalah kali ini saya selaku penulis akan membahas tentang *hardening* pada sistem operasi. Selain itu analisa apakah aplikasi akan berjalan pada sistem yang telah diimplementasikan *hardening*.

Penulis pada Penyusunan Skripsi ini mengambil judul : "*HARDENING SECURITY* MENGGUNAKAN WINDOWS 2003 (Studi Kasus: BANK X)".

1.2. Identifikasi Masalah

1.2.1. Rumusan Masalah

Dari latar belakang yang sudah dipaparkan diatas diperoleh rumusan masalah, antara lain:

a. Seringkali *user*-user pada Bank X menambah/mengurangi hardware yang ada tanpa sepengetahuan perusahaan, sehingga banyak hardware yang tidak terdaftar dan banyak konfigurasi sistem yang dapat menghambat kinerja sistem yang ada. Bagaimana melakukan upaya hardening dalam bentuk *Additional Security Setting* dengan cara meng-*hardening* dari sisi BIOS, *service pack*, *hardware*, dan lain-lain
b. User administrator default server pada umumnya bernama administrator. Server pada Bank X pada umumnya menggunakan user default, yaitu administrator sebagai user admin, sehingga para hacker akan lebih mudah untuk masuk ke dalam Sistem Operasi karena hanya perlu mencari password saja. Untuk itu bagaimana melakukan upaya hardening dalam bentuk *User*

Right Assignment dengan cara *account policy* dan *policy user*. Hal ini diberikan untuk mengatur user yang ada pada Bank X. Contoh masalah yang ada pada Bank X adalah seperti penamaan user administrator pada server. Selain itu pada Server Bank X yang memiliki banyak user, masing-masing user ditentukan dapat akses kemana saja, sehinngga tidak semua user mendapat akses yang sama, dan juga disesuaikan dengan kebutuhan dari user itu sendiri.

c. Banyak service yang berjalan pada Sistem Operasi Bank X. Kenyataannya tidak semua service digunakan, dan mengakibatkan para user untuk menjalankan aplikasi yang sebenarnya tidak perlu dijalankan oleh user. Sehingga perlu menentukan bagaimana mengkonfigurasi sistem service sesuai standarisasi aplikasi yang ada pada Windows 2003 Server Bank X .

d. Banyak dari para administrator Server yang tidak mengetahui bahwa tidak semua sistem ataupun aplikasi default dapat diubah. Ada beberapa server di Bank X yang memiliki spesifikasi hardware yang kecil. Bagaimana menentukan "Edit" maupun penambahan "registry" dapat memperkecil fungsi aplikasi yang ada pada sistem operasi sehingga Server menjadi lebih optimal dan stabil.

1.2.2. Batasan Masalah

Dalam penulisan skripsi ini yang menjadi pokok pembahasan adalah mengenai *hardening* yang diterapkan pada *Operating* Sistem yang berbasiskan Windows. Penulis akan menggambarkan standar dari *security setting Windows*

untuk kebutuhan Bank X dalam aplikasi bank seperti *Branch teller, Signature, Ns Router,* dan lain-lain.

1.3. Tujuan Penelitian

Tujuan penelitian ini adalah menciptakan suatu formula *hardening* yang dimaksudkan untuk mempersempit dan memperkeras suatu sistem operasi sehingga diharapkan dapat memperkokoh *operating* sistem tersebut. Selain itu diharapkan dari penciptaan formula *hardening* ini akan diperoleh manfaat di sisi *security* seperti:

a. Mencegah penggunaan *hardware* yang tidak diperlukan oleh user
b. Mempercepat sitem operasi dan memperkokoh *security system*
c. Menciptakan suatu formula *hardening* sebagai standar dari *security setting windows 2003 server* untuk kebutuhan Bank X dalam aplikasi bank.

1.4. Metode Penelitian

Dalam menyusun skripsi ini penulis melakukan pengumpulan data yang berguna untuk proses *hardening* tersebut.

Dalam mengumpulkan data terdapat dua tahap yang dilakukan penulis, tahap-tahap tersebut antara lain :

- Metode Lapangan

  Dalam tahap ini, pengumpulan data dilakukan oleh penulis menggunakan beberapa metode yang umum digunakan yaitu:

  - Observasi, yaitu :

Metode pengumpulan data langsung dengan cara menganalisis secara satu persatu baik dari sisi *Hardware, BIOS, Policy User, Application Service*, dan lain-lain.

- Wawancara, yaitu:

  Metode ini digunakan dengan jalan mewawancarai orang-orang yang terlibat langsung dalam menngembangkan *hardening*.

- Studi Pustaka

  Dalam tahap ini, pengumpulan data dilakukan oleh penulis melalui literatur-literatur yang sesuai dengan pokok pembahasan. Literatur-literatur tersebut diperoleh dari:

- Buku-buku Referensi. *On-line Reading, Softcopy.*

1.5. Sistematika Penulisan

Penjelasan secara terinci dari Struktur Penulisan Skripsi penulis, dapat dilihat sebagai berikut:

BAB I PENDAHULUAN

Bab ini berisi latar belakang masalah, identifikasi masalah, tujuan penulisan, dan sistematika penulisan.

BAB II LANDASAN TEORI

Menguraikan teori-teori yang menunjang penulisan / penelitian, yang bisa diperkuat dengan menunjukkan hasil penelitian sebelumnya.

BAB III ANALISA DAN PERANCANGAN *HARDENING*

Menganalisa sistem yang berjalan pada saat ini, baik dari segi basic input output sistem, sistem operasi dan aplikas i yang ada di dalam sistem operasi tersebut. Melihat kebutuhan yang diperlukan untuk keamanan, vulnerability yang dapat menyebabkan serangan dari luar ataupun dari user sendiri. Peraneangan untuk implementasi hardening

BAB IV IMPLEMENTASI DAN EVALUASI

Implementasi hardening dan membahas tentang vulnerabilities dari keamanan pada suatu sistem pada sistem operasi. Membahas tentang keterkaitan antar faktor-faktor dari data yang diperoleh dari masalah yang diajukan kemudian menyelesaikan masalah tersebut dengan metode yang diajukan dan menganalisa proses sistem dan hasil penyelesaian masalah.

BAB V KESIMPULAN DAN SARAN

Bab ini menguraikan beberapa kesimpulan yang diperoleh dari implementasi hardening yang sudah dirancang serta saran-saran yang dapat diberikan dalam rangka perbaikan dan peningkatan dimasa yang akan datang Kesimpulan berdasarkan uraian singkat atas apa yang telah penulis hadirkan dalam laporan ini, sedangkan saran dan kritik adalah cara untuk pihak yang nantinya akan melakukan maintenance hardening yang telah ada untuk mengolah dengan baik dan *Up To Date*.