

Melindungi *Password* dari Serangan *Hacker*

H. Mochamad Wahyudi, MM, M.Kom, CEH, CHFI
Program Pascasarjana Magister Ilmu Komputer STMIK Nusa Mandiri
Jl. Salemba Raya No. 5 Jakarta 10440
wahyudi@nusamandiri.ac.id

Mengelola *password* merupakan elemen penting untuk menjaga keamanan sistem. Seorang *administrator* sistem harus menjamin bahwa setiap *account* atau *user name* memiliki sebuah *password* yang hanya diketahui oleh *user* yang bersangkutan dan tidak mudah ditebak oleh *user* yang lain atau dijadikan sasaran serangan "*brute force*". Untuk memastikan keamanan sistem sangat bergantung pada kerahasiaan penyimpanan *password*.

Password merupakan sarana umum yang masih memegang peran dalam melindungi aset-aset penting dalam sebuah sistem. Sistem *password* sederhana belum cukup untuk mengidentifikasi siapakah sebenarnya seorang *user* atau mengatur apa saja yang dapat diakses olehnya, terlebih lagi kadang *user* harus mengingat banyak *password* sehingga pemilihan *password* cenderung *password-password* yang mudah dipecahkan atau mudah ditebak dengan cara mencoba-coba kemungkinan-kemungkinan yang ada. Sementara banyak *hacker* diantara para *user*, sehingga pencurian *password* masih seringkali terjadi. Akhirnya pelanggaran dan kehilangan *resource* masih tetap berlangsung.

Ada beberapa cara atau motif yang sering sekali dilakukan oleh seorang *hacker* untuk mencuri *user name* dan *password*, misalnya :

1. Mencoba-coba karakter demi karakter yang ada pada setiap *password* (serangan *brute force*).
2. Mencoba-coba *password* berdasarkan kamus *password* yang ada dan tentunya kamus yang diperguakan dalam bahasa inggris (serangan *dictionary password*).
3. Mencoba mendapatkan *password* berdasarkan informasi dari *user name* itu sendiri (nama *user name* dan *password*-nya sama).
4. Memasang *sniffer* pada suatu jaringan komputer untuk menganalisa jaringan serta mendapatkan data-data dari *user* yang berupa *clear text* (seperti *user name* dan *password*).
5. Memasang program penyusup seperti *trojan* dan *backdoor*.
6. dll

Perkembangan teknologi informasi dan semakin rentannya sebuah jaringan terhadap serangan atau ancaman kerusakan telah mendorong *vendor-vendor* ternama dalam memasarkan produk sistem keamanan yang terintegrasi. IBM hadir dengan merk *software* Tivoli, yaitu perangkat lunak pengelolaan keamanan dan identitas yang mencakup produk-produk seperti *IBM Tivoli Access Manager*, *IBM Tivoli Identity Manager* dan *IBM Tivoli Risk Manager*. *Computer Associates* memasuki pasaran dengan produk *eTrust Identity* dan *Access Management Suite*, dan masih banyak lagi.

Software-software pengelolaan *password* ini membantu dalam mengkonsolidasikan data identitas dan mengotomatiskan penggunaan hak akses karyawan, kontraktor, mitra bisnis dan para pelanggan ke berbagai aplikasi dan sumber daya berdasarkan kebijakan bisnis yang ada. Hal ini akan membantu perusahaan dalam mengurangi biaya investasi Teknologi Informasi dan meningkatkan keamanan.

Pengelolaan *password* pada dasarnya mengkombinasikan proses dan teknologi untuk mengelola dan mengamankan akses menuju informasi (*resource*) sekaligus melindungi profil identitas *user*. Setiap *user* (peralatan) diidentifikasi lalu akses masing-masing *user* dikontrol sesuai dengan hak dan batasan yang diberikan. *Password management* memiliki kemampuan untuk mengelola hal tersebut tersebut secara efektif baik untuk *user* di dalam maupun di luar perusahaan/organisasi (karyawan, pelanggan, partner bisnis, atau bahkan sebuah aplikasi, pada dasarnya semua orang atau alat yang hendak berhubungan dengan perusahaan/organisasi).

Pengelolaan *password* secara umum dapat dipandang sebagai suatu cara untuk :

1. Mendefinisikan identitas dari sebuah entitas/obyek (orang, tempat, alat).
2. Menyimpan informasi-informasi yang berkaitan dengan entitas tersebut, seperti nama/pengenal, dalam sebuah tempat penyimpanan (biasanya direktori aktif) yang aman, fleksibel, dan dapat disesuaikan.
3. Menjadikan informasi-informasi tersebut dapat diakses melalui beberapa ketentuan.
4. Menyediakan infrastruktur yang baik, terdistribusi dan memiliki performansi yang tinggi.
5. Mengatur hubungan antara *resource* dan entitas/obyek sesuai dengan konteks dan dalam waktu tertentu.

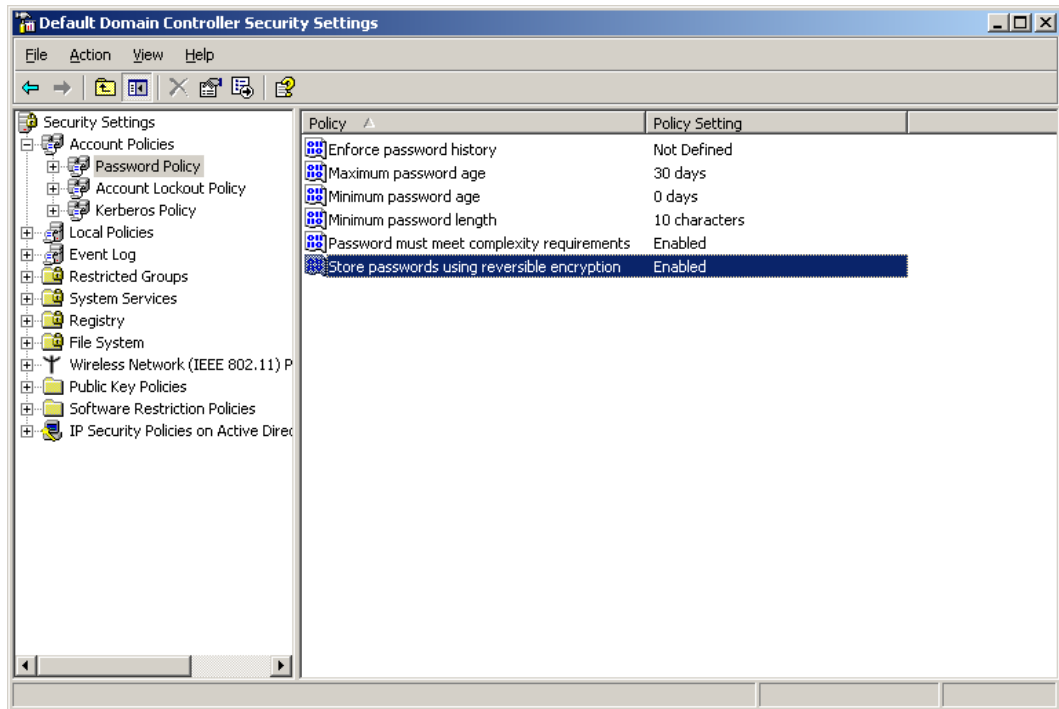
Komponen penting dalam sebuah sistem keamanan terintegrasi yang komprehensif, yaitu : privasi, proteksi, serta kontrol/pengawasan.

1. Privasi membutuhkan koneksi yang aman dan teknologi-teknologi seperti *IP Security (IP Sec)*, *Secure Socket Layer (SSL)* maupun *Virtual Private Network (VPN)*, yang membantu untuk meyakinkan bahwa komunikasi dalam sebuah WAN atau LAN merupakan komunikasi yang aman.
2. □□□Proteksi membutuhkan pertahanan yang kuat dalam menghadapi ancaman internal maupun eksternal. Proteksi ini dapat berupa *firewall* dan sistem pencegah penyusupan.
3. □□□Kontrol membutuhkan sistem identitas yang cermat dan teliti termasuk kontrol terhadap suatu akses.

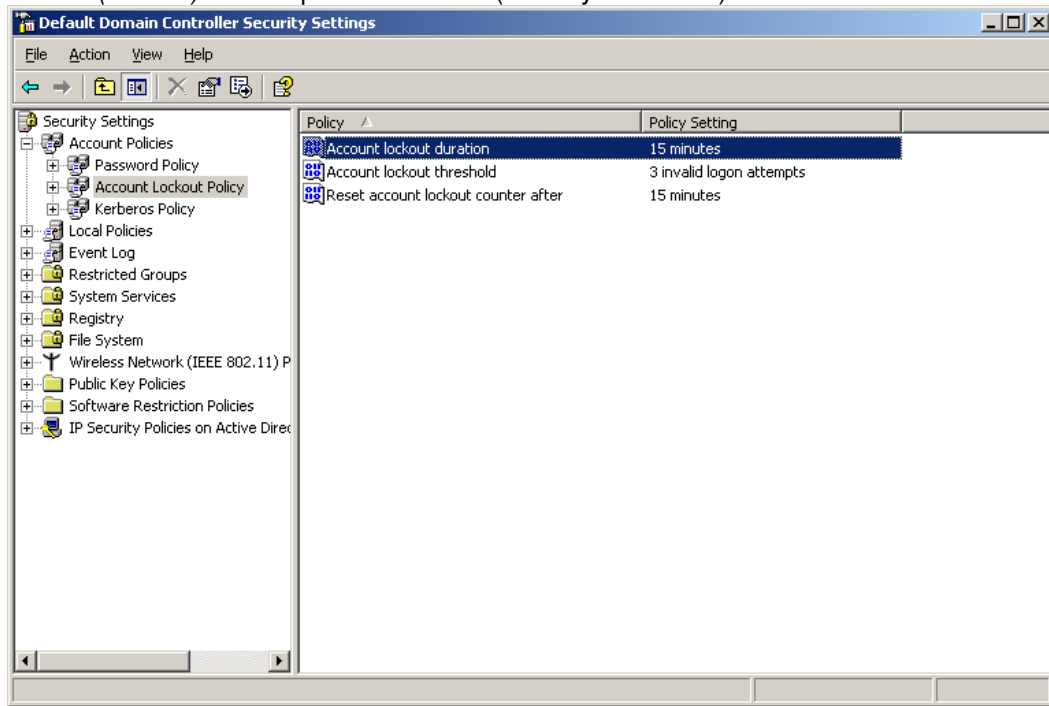
Dalam sistem operasi Microsoft Windows, sistem *password* disimpan pada sebuah file dengan nama SAM yang terdapat pada folder C:\Windows\System32 (Windows XP) serta C:\Windows\System32\Config (Windows Server 2003). Sedangkan pada sistem berbasis Linux, *password* disimpan pada direktori /etc/passwd.

Untuk menghambat serangan Brutu Force maupun serangan *dictionary password* terhadap suatu *password*, pembuatan *password* konvensional seperti yang selama ini dilakukan oleh *user* harus diperbaiki. Metode pembuatan *password* yang baik adalah sebagai berikut :

1. Buatlah *password* antara 10 s/d 12 karakter.
2. *Password* yang dibuat harus mempunyai kompleksitas yang tinggi, yaitu dengan membuat *password* tersebut terdiri dari gabungan : huruf kapital (huruf besar), huruf kecil, angka dan tanda baca (*special character*)
3. Jangan menggunakan *password* yang sama dengan *user name* atau *account*.
4. Untuk memudahkan *user* mengingat *password*-nya, buatlah *password* berupa suatu kalimat (*passphrase*). Misalnya : I Love Water. Lakukanlah training terhadap *user* untuk membuat *password* dengan menggunakan pola-pola tertentu dan *user* dapat dengan mudah mengingatnya *password*-nya. Misalnya : l7ov3w@+3r (yang artinya adalah I Love Water, tanpa tanda spasi).
5. *Password* yang dibuatnya harus memiliki masa berlaku maksimal 1 (satu) bulan. *User* harus merubah *password* tersebut, setelah masa berlakunya habis (*password expired*) untuk memasuki sitem kembali.



6. Untuk menghindari ada *user* yang tidak berhak untuk mengakses sutau *user account* dengan cara menebak nama *user name* dan *password*-nya, *account* sebaiknya dikunci (*Account Lockout Treshold*). Apabila ada *user* yang memasukan *username* dan *password* yang dimasukan yang salah dalam kurun waktu tertentu (misalnya *user* salah memasukan *password* selama tiga kali berturut-turut), maka *account* tersebut akan dikunci (*lockout*) selama periode tertentu (misalnya satu hari).



Penggunaan *password* yang mudah ditebak akan dapat dengan mudah diambil atau dicuri oleh seorang *hacker* yang terdapat di jaringan komputer. Perhatikanlah gambar berikut ini yang menunjukkan account-account yang terdapat pada suatu mesin sedang diam, bil atau dicuri *user name* dan *password*-nya.

Domain	User Name	LM Password	<8	NTLM Password	Audit Time	Method
NOTEBOOKAKU	aji	LOVE	x	love	0d 0h 0m 1s	Dictionary
NOTEBOOKAKU	angga	ADMIN	x	admin	0d 0h 1m 8s	Brute Force
NOTEBOOKAKU	Guest	* empty *	x	* empty *		
NOTEBOOKAKU	H. Moch. Wahyudi					
NOTEBOOKAKU	HelpAssistant					
NOTEBOOKAKU	IUSR_WAHYUDI					
NOTEBOOKAKU	IWAM_WAHYUDI					
NOTEBOOKAKU	miwan	MIWAN	x	miwan	0d 0h 0m 0s	User Info
NOTEBOOKAKU	SUPPORT_388945a0	* empty *	x			
NOTEBOOKAKU	wahyudi					

DICTIONARY STATUS

words total: 29156
 words done: 29156
 % done: 100.000%

BRUTE FORCE

time elapsed: 0d 1h 2m 31s
 time left: 0d 6h 3m 45s
 % done: 14.5706%
 current test: I08YPIN
 keyrate: 2871418 k/s

SUMMARY

total users: 10
 audited users: 3
 % done: 30.000%

User Info Check
 Dictionary
 Hybrid
 Brute Force

Pada gambar di atas terlihat dengan jelas ada beberapa *user name* dan *password* yang berhasil diambil atau dicuri dari seorang *user* oleh *hacker*. Sebagai contoh, anda bisa melihat sebuah *user name* dengan nama aji berhasil diketahui *password*-nya dalam waktu 1 detik dengan menggunakan metode penyerangan *Dictionary Password Attack* (*Password* yang didapatkan adalah : love). *User name* dengan nama angga berhasil diketahui *password*-nya dalam waktu 1 menit 8 detik dengan menggunakan metode penyerangan *Brutu Force Attack* (*Password* yang didapatkan adalah : admin) sedangkan *user name* dengan nama miwan berhasil diketahui *password*-nya dalam waktu kurang dari 1 detik dengan menggunakan metode penyerangan berdasarkan informasi *user* itu sendiri (*Password*-nya di dapatkan adalah : miwan). *User name* dengan nama wahyudi sampai dengan 1 jam 30 menit, *hacker* berusaha untuk mencuri *password* yang ada belum ada satu karakter *password*-pun yang berhasil untuk didapatkan atau ditemukan. Hal ini disebabkan karena *password* yang ada pada *user name* atau *account* wahyudi terdiri lebih dari 8 (delapan) karakter (Minimal 10-12 karakter) dan memiliki kompleksitas *password* yang tinggi (gabungan huruf besar, huruf kecil, tanda baca dan *special character*). Dengan metode *Brutu Force Attack*, *password* untuk *user name* atau *account* wahyudi baru dapat dipecahkan dalam waktu tidak kurang dari 7 X 24 jam atau bahkan tidak pernah terpecahkan.