CRACKING PASSWORD SISTEM OPERASI WINDOWS MENGGUNAKAN *TOOLS* PWDUMP dan CAIN & ABEL

Avid Jonra

Fakultas Ilmu Komputer, Universitas Sriwijaya, Sumatra Selatan – Indonesia

ABSTRAK

Keamanan perangkat yang kita gunakan sehari-hari merupakan hal yang sangat di perhatikan di zaman modern sekarang ini, seperti handphone dan pc. Pc atau *personal computer* sudah menjadi barang wajib di era ini. Tetapi tetap saja tidak ada kata aman untuk perangkat ini, karena setiap sistem keamanan yang dibuat selalu saja ada orang yang ingin merusaknya. Banyak cara yang telah berhasil dilakukan orang untuk membobol password sistem operasi pada pc, seperti menggunakan aplikasi pwdump dan cain & abel, dengan mencari hash menggunakan command prompt maka serangan brute force dapat dilakukan dengan waktu yang singkat selama password tersebut lemah. Jika password tersebut memiliki kombinasi yang kuat maka akan memakan waktu yang sangat lama.

PENDAHULUAN

Salah satu metode pengaman informasi yang umum digunakan oleh pengguna adalah password. Password mempunyai peran penting dalam mengamankan informasi-informasi yang bersifat penting atau pribadi.

Penulis ingin memberikan cara membobol password operasi sistem Windows 8 menggunakan hash yang ada dalam basis data komputer menggunakan software pwdump dan cain & abel. Pencurian password dilakukan dengan mengambil hash password tersebut dan melakukan serangan terhadap hash tersebut, serangan-serangan terhadap hash bisa dilakukan dengan bnyak cara salah satunya adalah brute force attack. Pada metodologi, penulis akan menjelaskan lebih lanjut tentang cara mencuri password sistem operasi windows 8 menggunakan pwdump dan cain & abel.

METODOLOGI

Menurut Drs.Agus M. Hardjana metodologi adalah mengemukakan metode ialah cara yang telah dipikirkan secara matang yang dilakukan dengan mengikuti langkah-langkah tertentu demi tercapainya sebuah tujuan. Di tulisan ini penulis menggunakan metode serangan brute force dengan menggunakan *tools* pwdump dan *tools* cain & abel.

1. PWDUMP

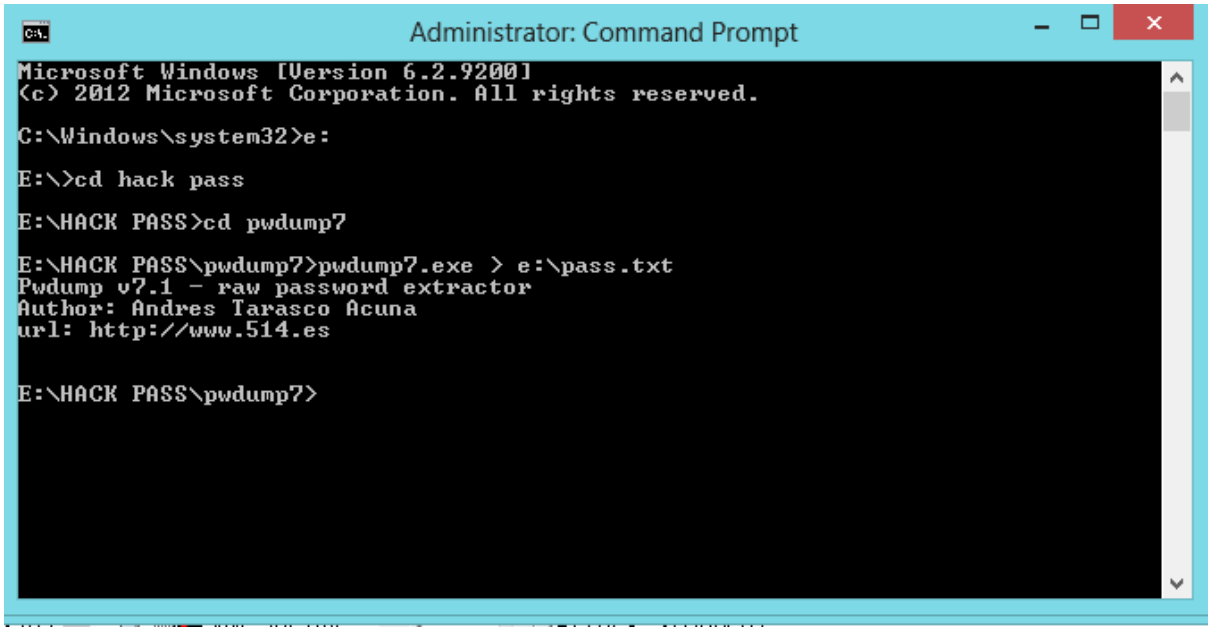
   PWDUMP adalah nama dari berbagai program Windows yang output LM dan password NTLM hash dari akun pengguna lokal dari Account Manager Security (SAM). Dalam rangka untuk bekerja, itu harus dijalankan di bawah account Administrator, atau dapat mengakses account Administrator pada komputer di mana hash harus dibuang. Pwdump bisa dikatakan membahayakan keamanan karena bisa memungkinkan administrator berbahaya untuk mengakses password pengguna. Sebagian besar program-program ini open-source.

2. CAIN & ABEL

Cain & Abel adalah pemulihan password alat untuk Microsoft Sistem Operasi. Hal ini memungkinkan pemulihan mudah berbagai jenis password dengan mengendus jaringan, cracking password terenkripsi menggunakan Dictionary, Brute-Force dan serangan pembacaan sandi, rekaman percakapan VoIP, decoding password orak-arik, memulihkan kunci jaringan nirkabel, mengungkapkan kotak password, mengungkap password cache dan menganalisis routing yang protokol. Program ini tidak mengeksploitasi kerentanan software atau bug yang tidak dapat diperbaiki dengan sedikit usaha. Ini mencakup beberapa aspek keamanan / kelemahan hadir dalam standar protokol, metode otentikasi dan mekanisme caching; tujuan utamanya adalah pemulihan disederhanakan password dan kredensial dari berbagai sumber, namun juga kapal beberapa "non standard" utilitas untuk pengguna Microsoft Windows.

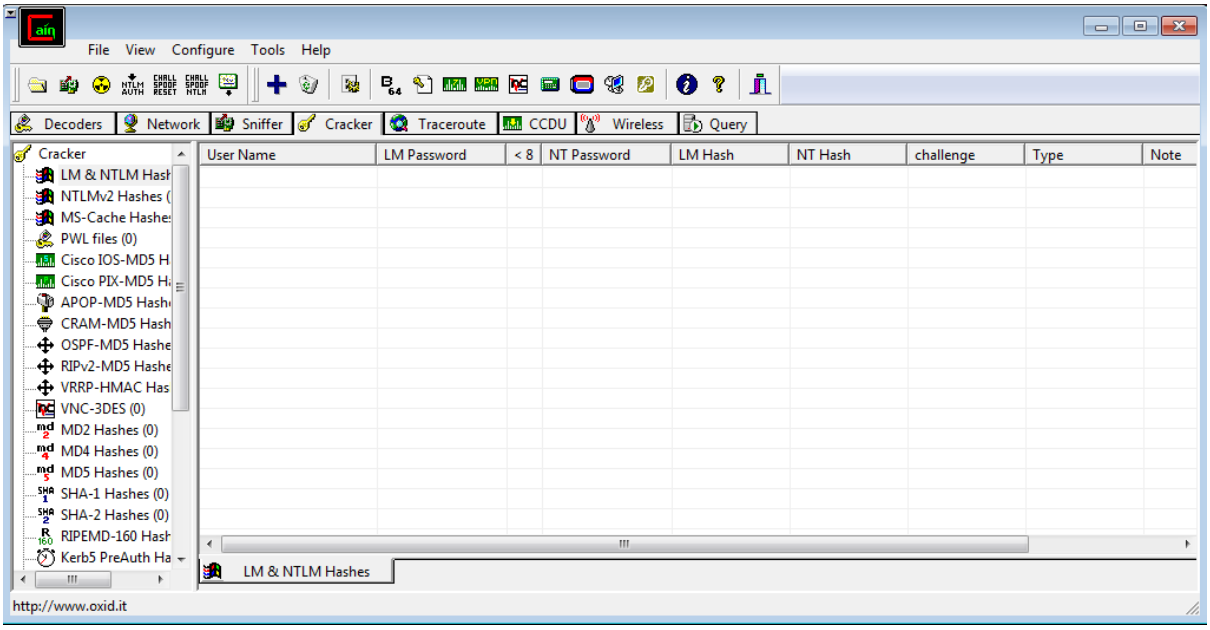
PERCOBAAN DAN HASIL PENELITIAN

Yang pertama dilakukan adalah dengan mencari hash password dan mengubah nya menjadi file .txt, buka command prompt lalu panggil folder tempat dimana pwdump disimpan Lalu perintahkan pwdump menjalankan aplikasi .exe nya agar hash password pada komputer bisa didapatkan. Kemudian hash password tersebut ubah menjadi file .txt seperti gambar dibawah ini.



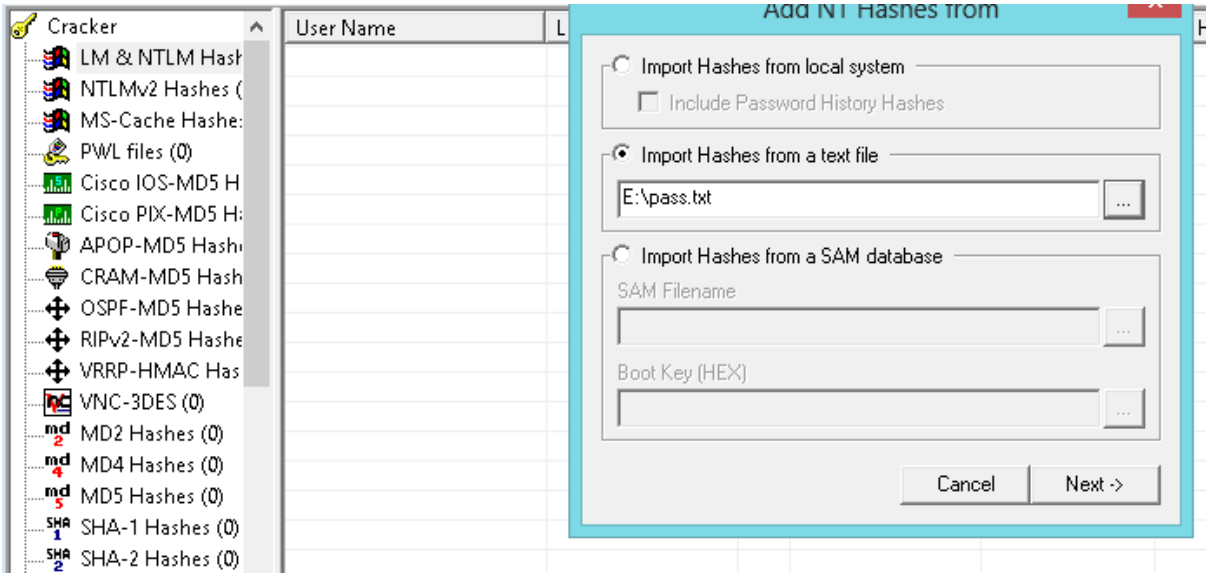
Gambar 1, mendapatkan hash dengan pwdump dan mengubah hash password menjadi file .txt menggunakan command prompt.

Pada gambar 1, file .txt diberi nama pass.txt, setelah itu buka aplikasi cain & abel dengan cara run as administrator. Setelah program terbuka masuk ke direktori cracker seperti gambar dibawah ini.



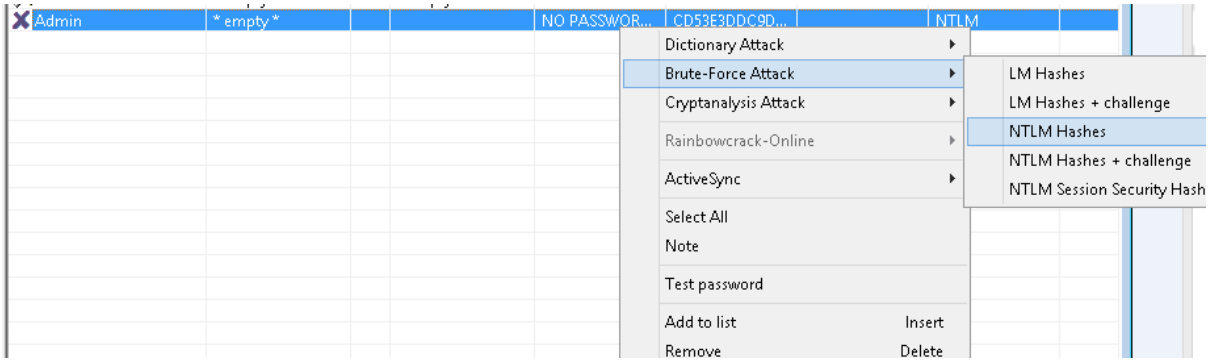
Gambar 2, aplikasi cain & abel yng telah masuk ke direktori cracker.

Setelah itu pilih menu cracker LM & NTLM Hashes dan dipilih tools tanda “plus”. Pilih import hashes from text file lalu tambahkan file pass.txt yang telah kita simpan tadi seperti dibawah ini.



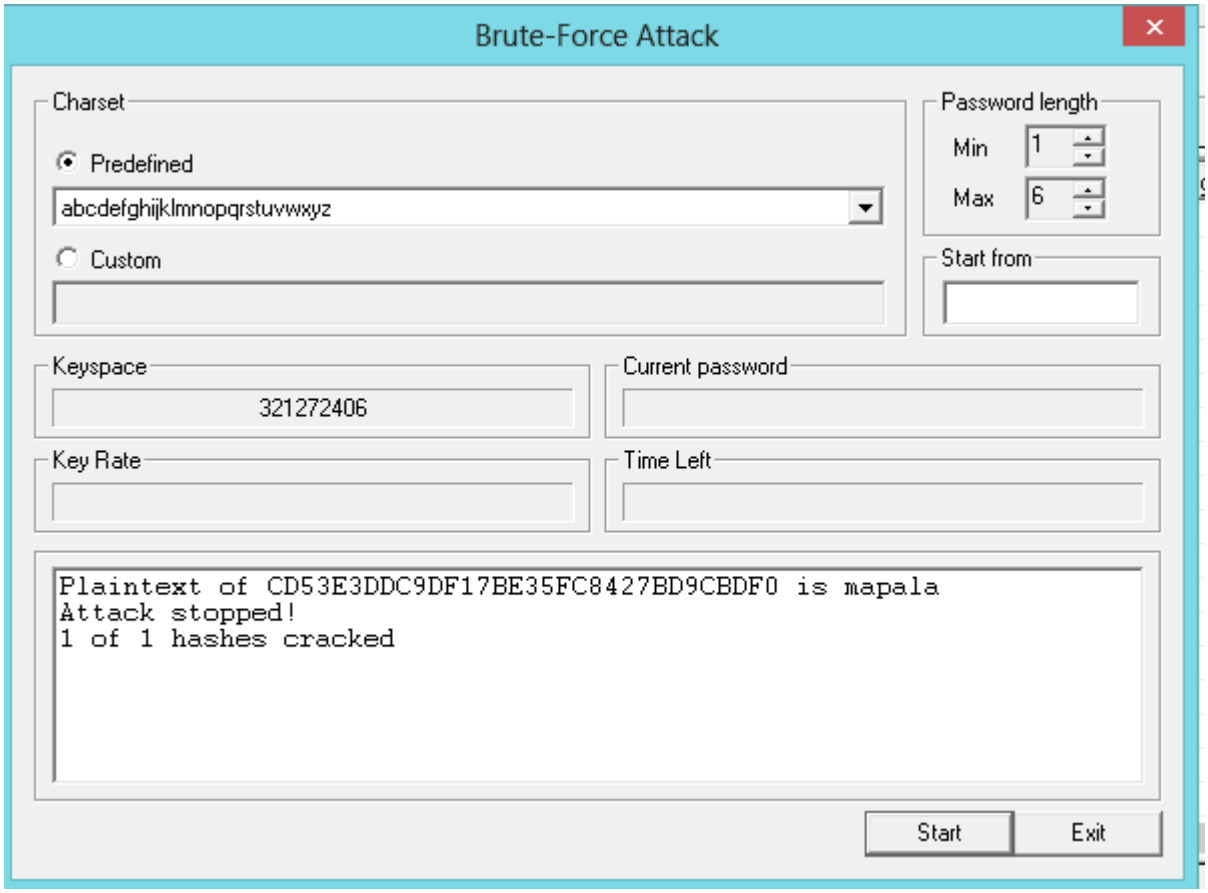
Gambar 3, penambahan note hash dari text file.

Kemudian pilih next dan oke. Setelah mendapatkan hash di cain & abel kemudian pilih user yang digunakan, disini penulis menggunakan user admin sebagai administrator. Lalu klik kanan kursor pada admin lalu pilih Brute-Force Attack dan pilih NTLM Hashes seperti pada gambar dibawah ini.



Gambar 4, pemilihan serangan pada hash yang telah dipilih menggunakan cain & abel.

Setelah NTLM Hashes di klik akan muncul tampilan brute-force attack,. Penulis memilih karakter abjad kecil pada predefined supaya memudahkan serangan bruteforce, panjang karakter password juga kita minimalkan agar waktu yang terpakai tidak terlalu lama. Setelah mengatur panjang password serangan brute force, klik start kemudian tunggu hingga didapatkan hasili password komputer seperti gambar dibawah ini.



Gambar 5, password yang telah didapatkan dengan serangan brute force.

Seperti yang bisa dilihat pada gambar, password yang didapatkan adalah “mapala”. Maka percobaan diatas berhasil dilakukan.

KESIMPULAN

Dapat kita simpulkan bahwa belum ada kata aman untuk perangakat pc karena setiap pembaharuan keamanan selalu saja ada orang yang ingin mencoba merusaknya, sangat penting untuk menjaga data informasi kita agar tetap rahasia. Adapun salah satu cara membobol kemamanan sistem operasi windows bisa dengan melakukan serangan brute force dengan bantuan tools pwdumpdan cain & abel. Namun, serangan brute force ini akan memakan waktu yang lama dalam proses mendapatkan password apabila pengguna menggunakan password dengan kombinasi karater yang kuat.