Password Cracking pada Sistem Operasi windows 7

Agung Fitrianda (09121001011),

Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya

Email : Agung.fitrianda@gmail.com

ABSTRAK:

Sebagian besar para pengguna computer tentu aware dengan sistem keamanan komputernya, oleh karena itu sering dijumpai computer yang memiliki password sehingga membatasi akses bagi orang asing yang ingin mengakses file dan menjalankan computer secara bebas, hal ini tentu menyulitkan bagi para pengguna asing yang ingin bebas mengeksplorasi dan dan melakukan berbagai macam operasi yang ada dalam komputer yang memiliki password. Oleh karena itu Proses cracking password ini bertujuan untuk mendapatkan password computer target sehingga kita bisa melakukan login administrator dalam computer tersebut dan melewati sistem keamanannya dengan mudah sehingga bisa menjalankan computer dengan bebas dan mengakses berbagai macam file yang diinginkan hanya dengan menjalankan beberapa aplikasi scanning untuk cracking password seperti Pwdump untuk mendapatkan hash dari password target dan cail and abel untuk mencocokkan hash tersebut dengan password yang digunakan computer sehingga hasilnya hash dari password target dan password administrator target bisa ditemukan.

Keyword : pwdump, cain and abel, hash, password

PENDAHULUAN

Dalam dunia keamanan computer, sebagian besar para pengguna computer sudah sangat aware dengan sistem keamanan pada komputernya sendiri, sehingga mereka meningkatkan sistem keamanan pada computer mereka sendiri dengan memberikan kode password login pada pengaturan user account control agar tidak semua orang bisa mengakses pengaturan komputer dan menjalankan aplikasi tertentu melainkan yang mengtahui kode password tersebut. Tentunya hal ini akan mempersulit orang lain untuk mengakses semua file dan program dalam computer secara bebas. Oleh karena itu, butuh suatu aplikasi yang memungkinkan penggunanya dapat mengetahui password pada computer untuk mendapatkan akses pada computer secara bebas. Pada kali ini, saya akan membahas tentang cracking password pada computer untuk mendapatkan informasi berupa password administrator pada computer target. beberapa scanning tools yang bisa digunakan diantaranya adalah pwdump7 dan cail and abel. Oleh karena itu, dengan menggunakan aplikasi password cracker seperti pwdump7 dan cail and abel, kita bisa memperoleh informasi berupa password kode untuk computer yang kita gunakan sehingga kita mendapatkan akses secara langsung dalam computer tersebut. Pada bagian selanjutnya akan dijelaskan langkah – langkah melakukan proses cracking password.

METODE PENELITIAN

Tahap pertama untuk melakukan proses cracking password pada windows 8 adalah mempersiapkan scanning tools untuk melakukan cracking password, pada percobaan kali ini, tools yang digunakan antara lain :

1. Pwdump7
2. Cain and Abel

PwDump

pwdump adalah nama dari berbagai program Windows yang output LM dan password NTLM hash dari account 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 yang berbahaya untuk mengakses password pengguna. Sebagian besar program-program ini open-source. Jenis – jenis pwdump yang diketahui antara lain:

Program asli oleh Jeremy Allison (domain publik, sumber tersedia) - pwdump

pwdump2 - oleh Todd Sabin dari BindView (GPL), menggunakan injeksi DLL

pwdump3 - oleh Phil STAUBs (GPL), bekerja melalui jaringan

pwdump 3e - oleh Phil STAUBs (GPL), mengirimkan dienkripsi melalui jaringan

pwdump4 - oleh bingle (GPL), peningkatan pwdump3 dan pwdump2

pwdump5 - oleh AntonYo! (Freeware)

pwdump6 - oleh fizzgig (GPL), peningkatan pwdump 3e

fgdump - oleh fizzgig, peningkatan pwdump6 w / addons

pwdump7 - oleh Andres Tarasco (freeware), menggunakan driver filesystem sendiri

Pada percobaan kali ini pwdump yang digunakan adalah pwdump7.

HASH

Hash adalah suatu teknik "klasik" dalam Ilmu Komputer yang banyak digunakan dalam praktek secara mendalam. Hash merupakan suatu metode yang secara langsung mengakses record-record dalam suatu tabel dengan melakukan transformasi aritmatik pada key yang menjadi alamat dalam

tabel tersebut. Key merupakan suatu input dari pemakai di mana pada umumnya berupa nilai atau string karakter.

Pelacakan dengan menggunakan Hash terdiri dari dua langkah utama, yaitu:

• Menghitung Fungsi Hash. Fungsi Hash adalah suatu fungsi yang mengubah key menjadi alamat dalam tabel. Fungsi Hash memetakan sebuah key ke suatu alamat dalam tabel. Idealnya, key-key yang berbeda seharusnya dipetakan ke alamat-alamat yang berbeda juga. Pada kenyataannya, tidak ada fungsi Hash yang sempurna. Kemungkinan besar yang terjadi adalah dua atau lebih key yang berbeda dipetakan ke alamat yang sama dalam tabel. Peristiwa ini disebut dengan collision (tabrakan). Karena itulah diperlukan langkah berikutnya, yaitu collision resolution (pemecahan tabrakan).

• Collision Resolution. Collision resolution merupakan proses untuk menangani kejadian dua atau lebih key di-hash ke alamat yang sama. Cara yang dilakukan jika terjadi collision adalah mencari lokasi yang kosong dalam tabel Hash secara terurut. Cara lainnya adalah dengan menggunakan fungsi Hash yang lain untuk mencari lokasi kosong tersebut.

Cain and Abel

Program bantu cain and abel merupakan program hasil buah karya *Massimiliano Montoro.* Program ini dikhususkan dalam penanganan *recovery password* pada system oprasi Micrososft Windows yang cenderung menangani masalah jaringan (baik aplikasi networking sampai dengan aplikasi yang menggunakan fitur database server). Target dari pengembangan Cain & Abel dalam penggunaannya menurut *Massimiliano Montoro* sendiri dapat digunakan oleh beberapa pelaku IT, diantaranya *network administrator, teacher, security consultant/professional, forensic staff, security software vendors, professional penetration testers.*Dengan melihat sasaran para pelaku pengguna program bantu ini, tentunya software ini dapat diandalkan juga oleh para pembaca lainnya yang tertarik dalam ilmu IT.

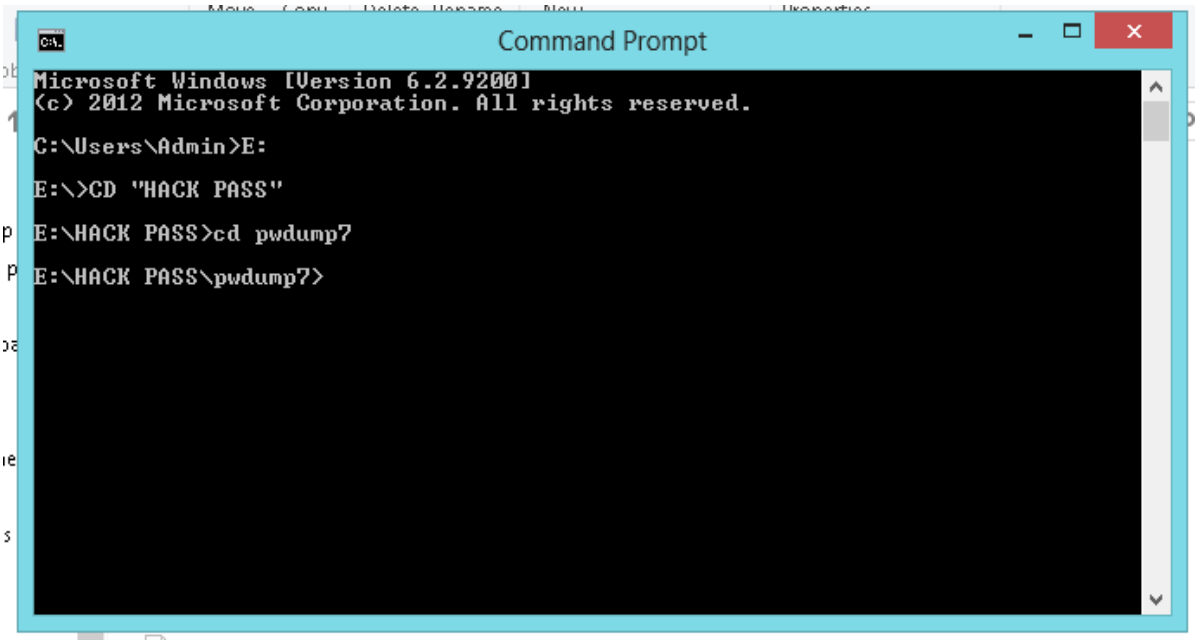
Berikut adalah fitur – yang dimiliki cain and abel :

Mendukung *recovery password* pada :

- Sniffing jaringan
- Cracking enkripsi password dengan model Dictionary, Brute-Force dan Crypanalysis attacks.
- Merekam percakapan melalui VoIP
- Memecahkan srambled password
- Recovery wireless network keys
- Revealing password
- Analisa routing protocol

LANGKAH PERCOBAAN

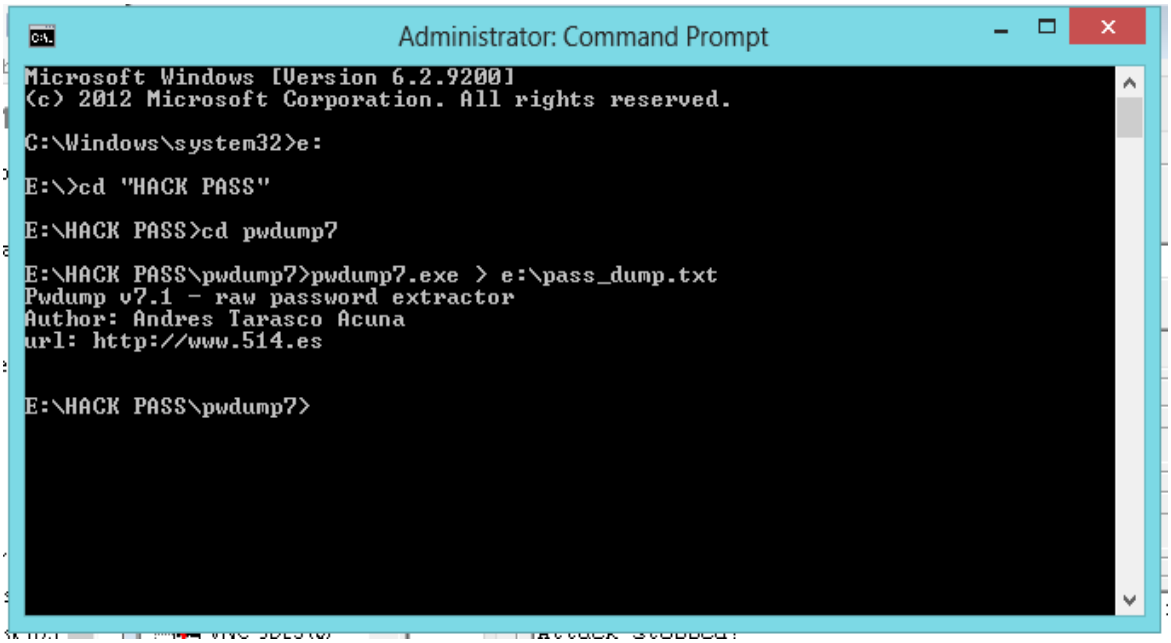
1. Setelah semua tools yang digunakan sudah lengkap dan terinstall pada computer target, maka langkah selanjutnya adalah memulai proses cracking password dengan menjalankan perintah untuk memanggil file register pada pwdump7 (pwdump7.exe) dengan menggunakan aplikasi CMD (Command Prompt). Seperti pada gambar 1 dibawah ini :



Gambar 1.

Pada gambar 1 diketahui bahwa file register pwdump7 berada pada partisi E dan di dalam folder “HACK PASS”, oleh karena itu kita bisa memanggil file pwdump7 dalam partisi E dan masuk ke folder “HACK PASS”.

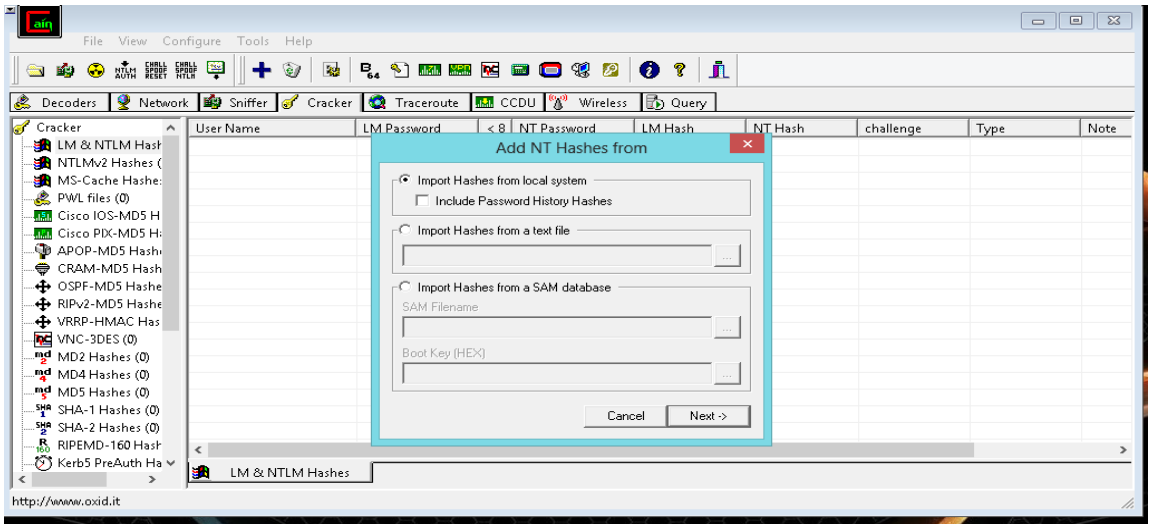
2. Kemudian Pada langkah selanjutnya adalah menjalankan file register yang ada pada pwdump7 dan membuat file baru yang berformat txt. Untuk menampung data hash dari password computer target seperti pada gambar 2 di bawah :



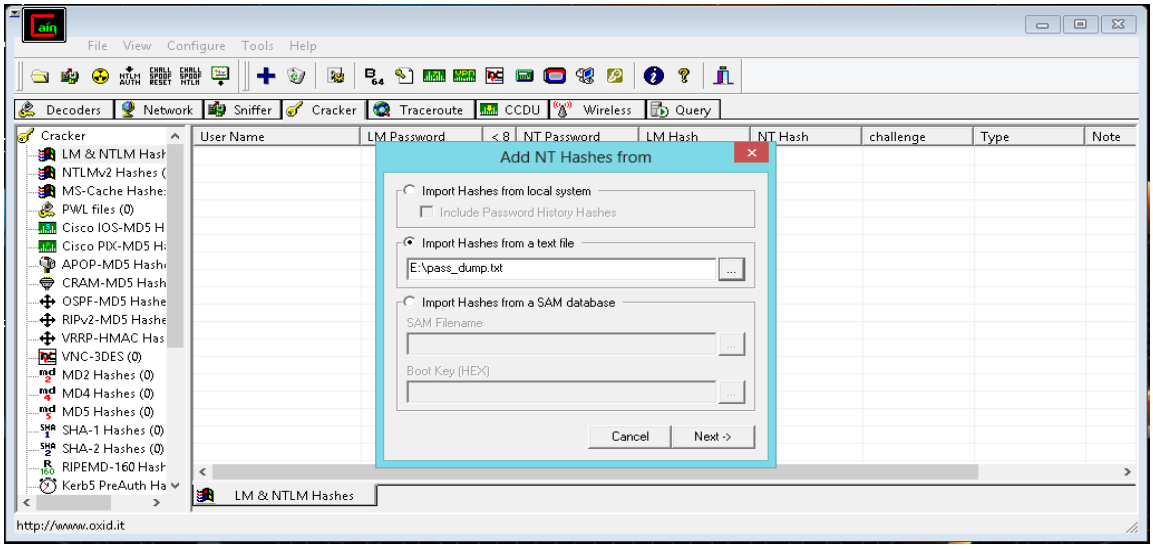
Gambar 2.

Pada gambar 2 diketahui bahwa file register yang digunakan untuk cracking password computer target adalah pwdump.exe setelah itu membuat file baru dengan nama pass_dump dan format .txt, dengan menuliskan perintah pada cmd e:\pass_dump.txt. setelah menekan enter, maka kemudian file dengan nama pass_dump.txt akan tersimpan di partisi E:.

3. Lalu, setelah file .txt yang memuat hash password computer target telah tersimpan, maka langkah selanjutnya adalah membuak aplikasi cain and abel untuk mengekstrak hash computer menjadi plain text yang berisi password computer target. Seperti pada gambar 3 dan 4 dibawah ini :



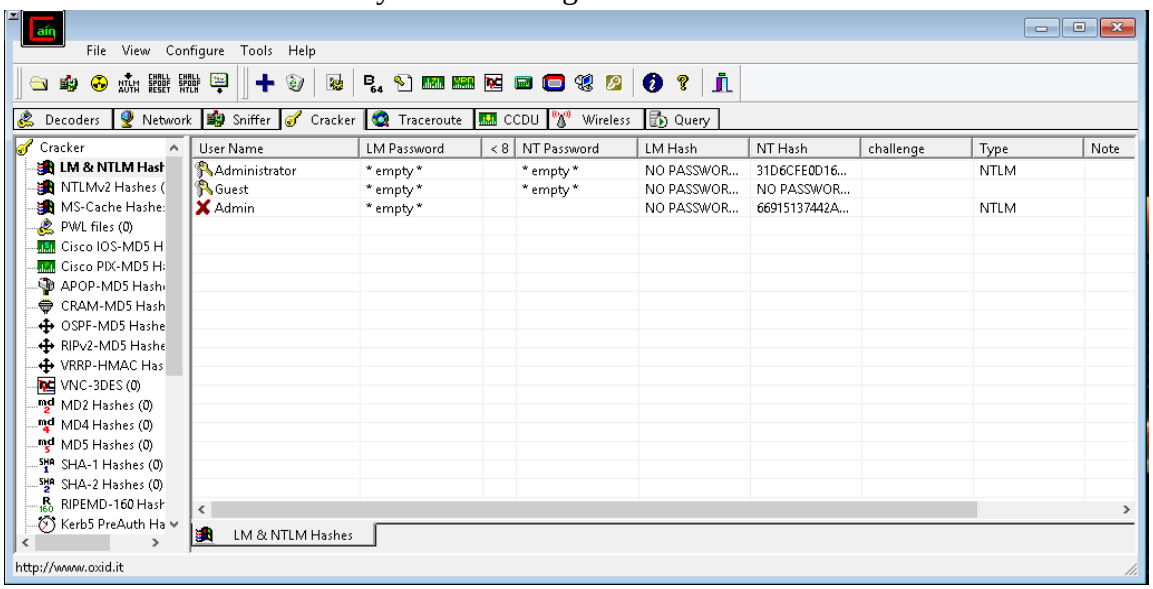
Gambar 3



Gambar 4.

Pada gambar 3, merupakan gambar interface dari aplikasi cain and abel yang siap digunakan, dengan memilih kolom cracker, kemudian pada opsi di menu kolom cracker di sebelah kiri yang digunakan adalah LM & NTLM Hash karena kita ingin menscan Hash dari password target. Sedangkan pada gamba 4 adalah gambar ketika file .txt sudah diimport. Kemudian import hash computer target yang ada di dalam file pass_dump.txt yang telah dibuat sebelumnya dan klik NEXT.

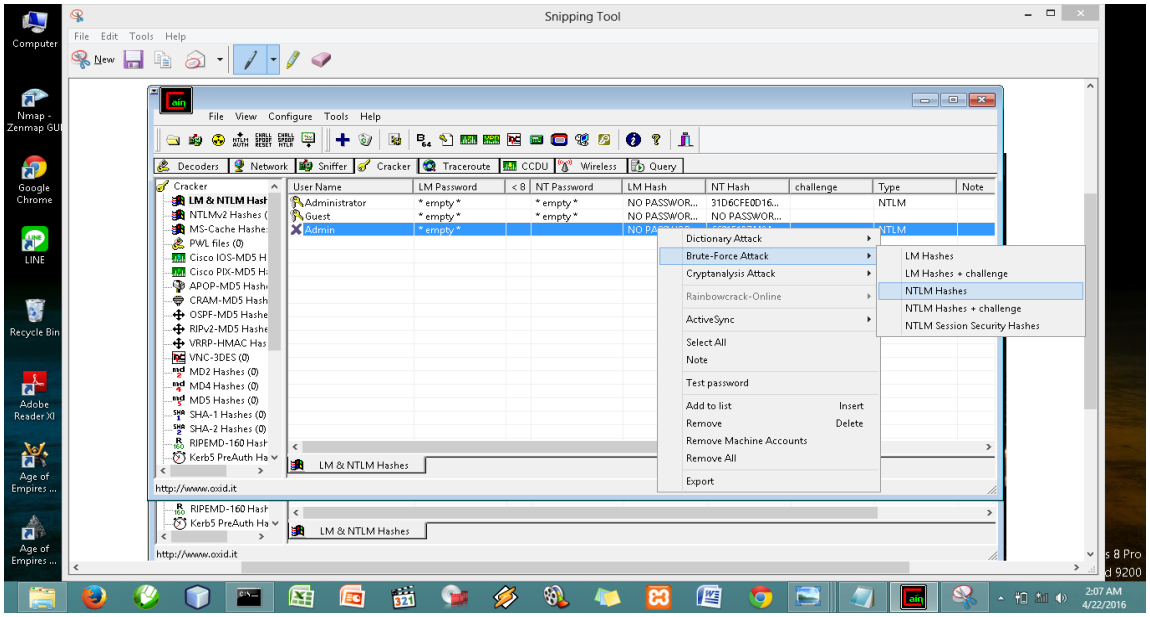
4. Selanjutnya aplikasi cain and abel akan menampilkan isi dari file pass_dump.txt yang berisi kode HASH dari password computer target. Kemudian HASH pada akun mana yang akan diserang, pada percobaan kali ini, hash yang ingin diserang adalah HASH pada akun administrator. Gambarnya adalah sebagai berikut :



Gambar 5.

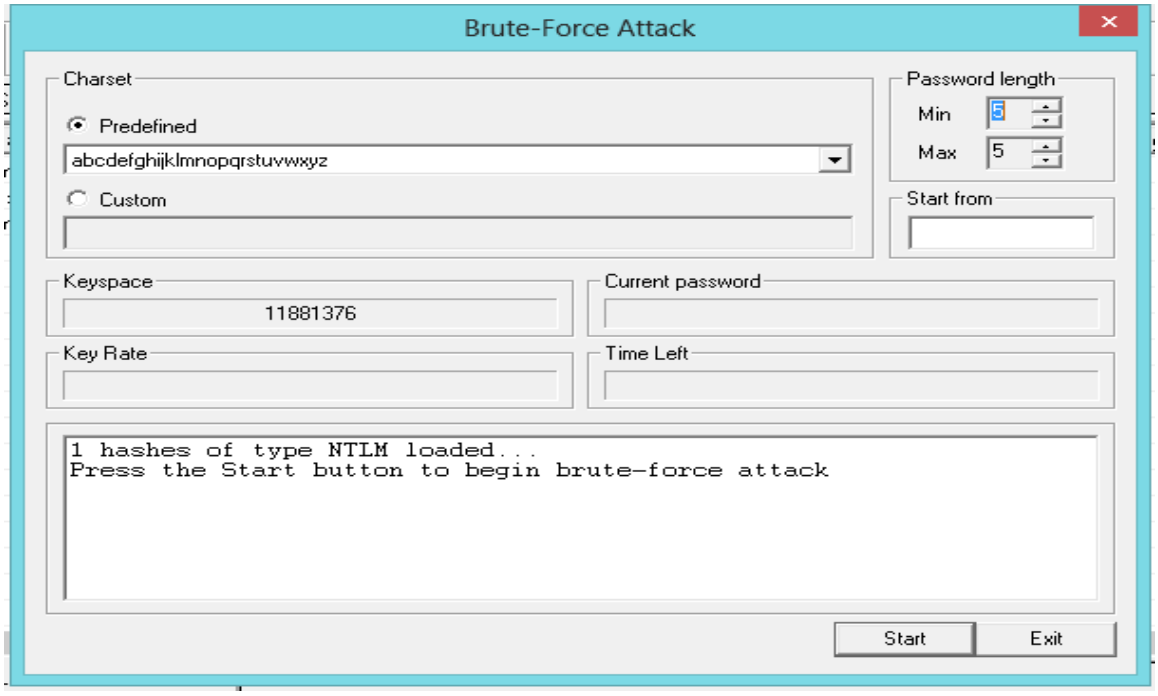
Pada gambar di atas diketahui bahwa HASH pada akun administrator yang berhasil didapat adalah 66915137442A04BB37263C0D02A9E8A dengan nama akun admin.

5. Tahap selanjutnya adalah melakukan serangan brute force terhada HASH yang telah didapatkan dengan opsi NTLM Hashes.



Gambar 6.

6. Setelah memilih opsi brute force terhadap HASH computer target, maka akan muncul interface brute force yang siap untuk melakukan scanning terhadap hash computer target, Seperti pada gambar 7 dibawah ini :

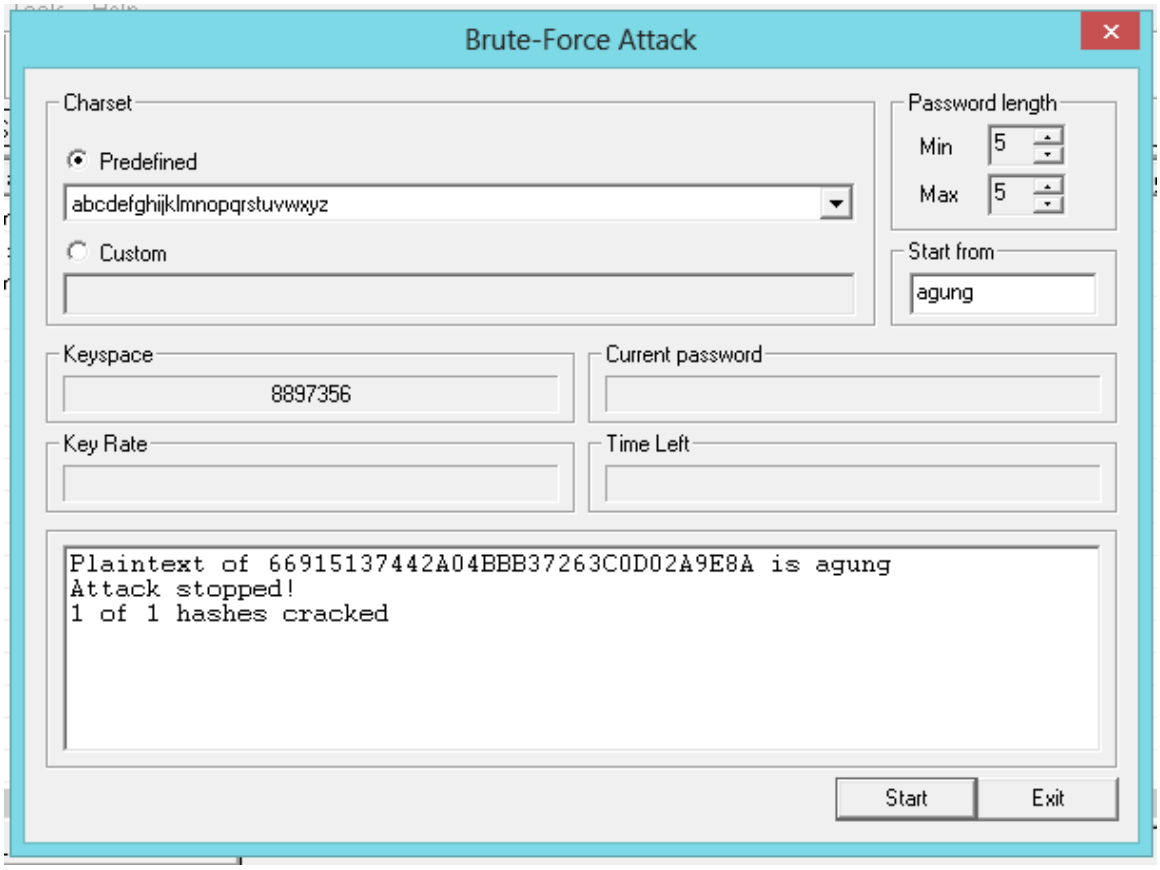


Gambar 6.

Setelah masuk di interface brute-force attack, dilakukan sedikit setting untuk menentukan tipe estimasi password pada kolom predefined. Pada percobaan ini, estimasi tipe password yang digunakan adalah semua dalam bentuk huruh tanpa huruf kecil dari a sampai z tanpa huruf capital ataupun angka, kemudian, melakukan estimasi panjamng password pada kolom password length (pada prcobaan ini, estimasi yang dipilih adalah panjang minimal 5baris dan panjang maksimal adalah 5 baris). Setelah menekan tombol start, maka proses scanning password akan dimulai dan tinggal menunggu hasil scan beberapa saat.

HASIL PERCOBAAN

Setelah proses scanning selesai, maka akan tampil hasil scanning tersebut berupa password administrator dari computer target. Kemudian hasil akhir proses cracking password akan muncul seperti pada gambar 7 dibawah ini :



Gambar 7.

Pada proses akhir ini, kita dapat mengetahui bahwa kode password administrator dari computer target adalah : agung. Sehingga dengan hasil ini, percobaan cracking password telah selesai dan berhasil dilakukan.

KESIMPULAN

1. Dengan menggunakan aplikasi pwdump dan cain and abel, kita bisa mendapatkan password dengan mudah dan login masuk kedalam sistem pada computer tersebut.
2. Aplikasi pwdump berguna untuk mendapatkan Hash dari password target dan aplikasi cain and abel mencocokkan data Hash dengan estimasi password yang dipakai dengan proses scanning untuk mendapatkan password computer yang sebenarnya. Semakin panjang karakter password dan semakin bervariasi karakter password yang digunakan, maka semakin lama juga proses scanning berjalan.

Sumber referensi :

1. http://cahpoetra.blogspot.co.id/2011/04/pengertian-fungsi-hash.html
2. https://ekachandra11.wordpress.com/2011/12/24/cain-abel-apa-itu/
3. https://en.wikipedia.org/wiki/Pwdump