Tugas Keamanan Jaringan

Password Cracking pada Sistem Operasi windows

Nama : Fitriyani

Nim : 09011181419040

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2018

Password Cracking pada Sistem Operasi windows

Sebagian besar para pengguna komputer sangatlah memperhatikan keamanan komputernya, oleh karena itu sering kita jumpai laptop teman kita yang memiliki password sehingga akan membatasi akses bagi orang yang lain yang ingin mengakses laptop tersebut. Hal seprti ini tentunya menyulitkan bagi para pengguna asing yang ingin bebas mengeksplorasi dan malakukan berbagai macam operasi yang ada dalam komputer yang memiliki password. Oleh karena itu proses melakukan cracking pasword ini bertujuan untuk mendapatkan password laptop yang kita targetkan. Sehingga kita bisa melakukan login administor dalam laptop yang kita hack. Sehingga kita bisa melewati sistem keamanan dengan mudah yang akan membuat kita bisa menjalankan computer dengan bebas dan mengakses berabagai macam file yang ada pada laptop tersebut. Dengan melakukan beberapa aplikasi scanning untuk cracking password seperti Pwdump untuk mendapatkan hash dari password target sehingga cail and abel untuk mencocokkan hash tersebut dengan password yang digunakan computer sehingga hasilnya hash dari password target dan password administrator target bisa ditemukan.

Sebenarnya sebagian besar para pengguna computer sangat peduli dengan sistem keamanan laptop mereka, sehingga mereka akan meningkatkan sistem keamanan pada laptop mereka sendiri dengan cara memberikan kode password login pada pengaturan user account control agar membuat seorang tidak bisa mengakses laptop dan menjalankan aplikasi tertentu sehingga hanya orang yang tauh password laptop tersebut yang bisa menggunakannya. Tentunya dengan cara seperti ini akan mempersulit orang lain untuk mengakses semua file dan program secara bebas. Oleh karena itu dibutuhkan 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.

Sebenarnya pwdump ini adalah nama dari berbagai program windows yang mana outputnya adalah LM dan password NTLM hash terdapat dari account pengguna lokal dari Account Manager Security (SAM). Untuk menjalankan proses tersebut maka harus dijalankan dibawah account administrator atau dapat mengakses account administrator pada laptop tersebut. Pwdump bisa dikatakan membahayakan keamanan karena bisa memungkinkan administrator yang berbahaya untuk mengakses password pengguna. Sebagian besar program-program ini open-source. Pwdump sebenarnya memiliki banyak jenis, adapun jenis-jenisnya adalah sebagai berikut. 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.

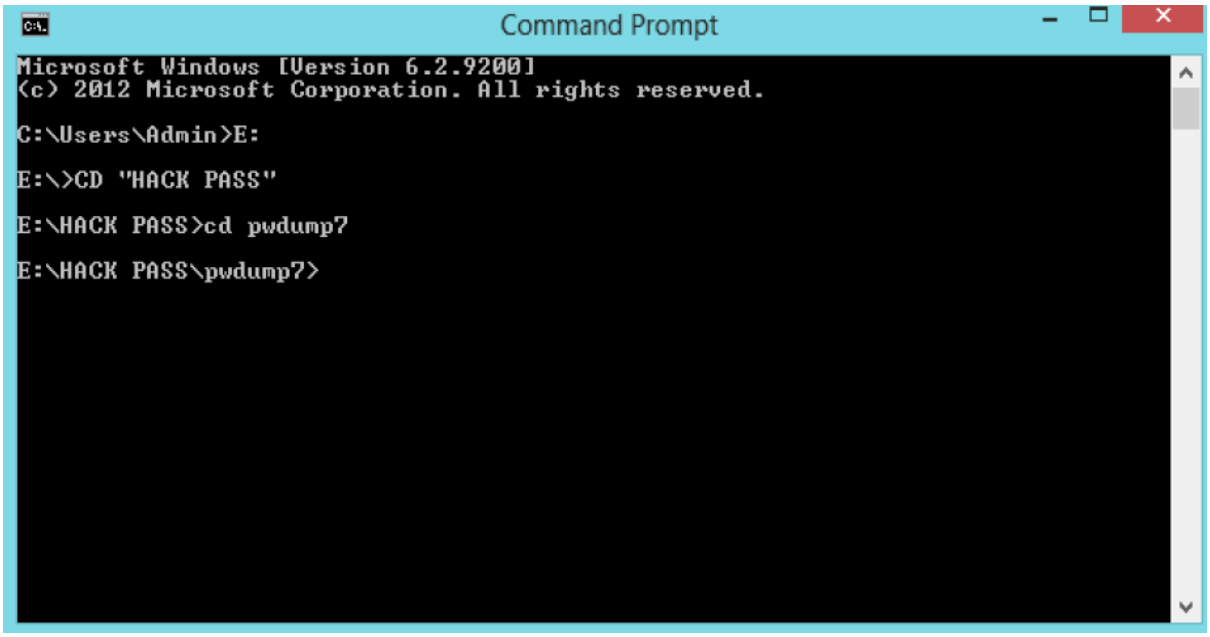
Hash merupakan metode yang dapat mengakses secara langsung dengan menggunakan record dalam suatu tabel dengan melakukan informasi aritmatik pada key yang menjadi alamat dalam berbentuk tabel. Key merupakan suatu input dari pemakai dimana pada umunya berupa nilai string karakter. Sebenarnya pelacakan menggunakan hash terdiri dari dua langakah yaitu yang pertama menghitung fungsi hash, yang mana hash ini berfungsi untuk mengubah key menjadi alamat dalam bentuk tabel. Fungsi hash ini akan memetakan sebuah key ke suatau alamat dalam tabel. Seharusnya, key yang berbeda akan dipetakan ke alamat yang berbeda juga. Tapi sebenarnya ada juga kemungkinan tidak ada fungsi hash yang sempurna. Sehingga kemungkina besar terjadi ada dua atau lebih keya yang berada dipetakan kealamat yang sama dalam tebel. 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.

Program bantu *cain and abel* merupakan program yang di khusukan dalam penanganan *recovery password* pada sistem oprasi microsoft windows yang cenderung menangani masalah jaringan baik aplikasi networking sampai dengan palikasi yang menggunakan fitur database server. Target dari pengembangan *cain and abel* dalam penggunaanya 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* adalah sebai berikut:

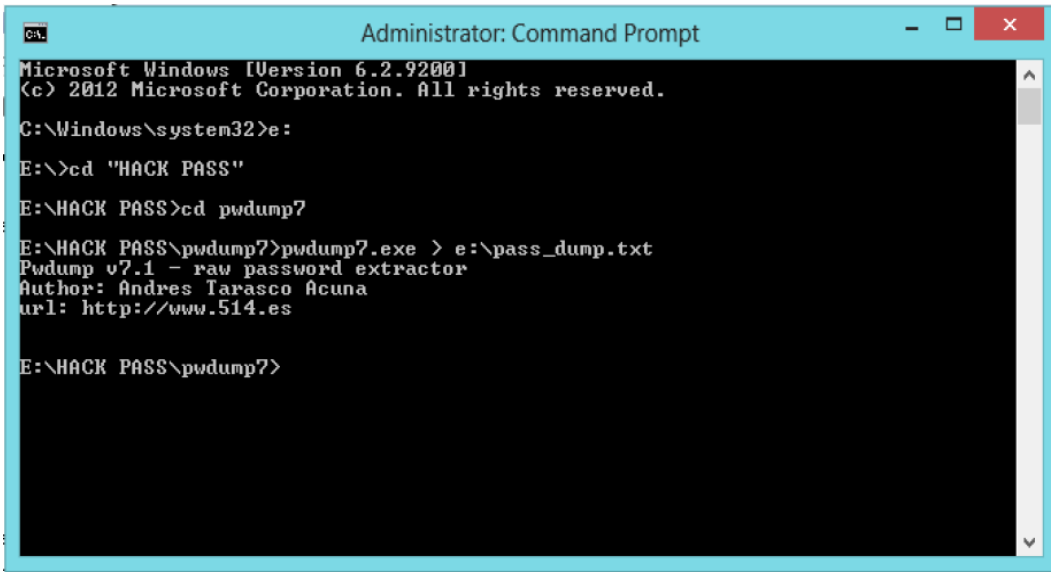
- Sniffing jaringan
- Cracking enkripsi password dengan model Dictionary, Brute-Force dan Crypanalysis attacks.
- Merekam percakapan melalui VoIP
- Memecahkan srambled password
- Recovery wireless network keys
- Revealing password
- Analisa routing protocol

Cara- cara melakukan Password Cracking pada Sistem Operasi windows 7 adalah sebagai berikut:

1. Hal yang pertama dalam melakukan hal ini adalah semua tools yang digunakan sudah lengakap dan terinstall pada laptop yang kita targetkan, setelah itu kita dapat memulai proses cracking password dengan menjalankan perintah untuk memanggil file register pada pwdump7 dengan menggunakan aplikasi CMD. Maka hasil yang didapat adalah sebagai berikut:

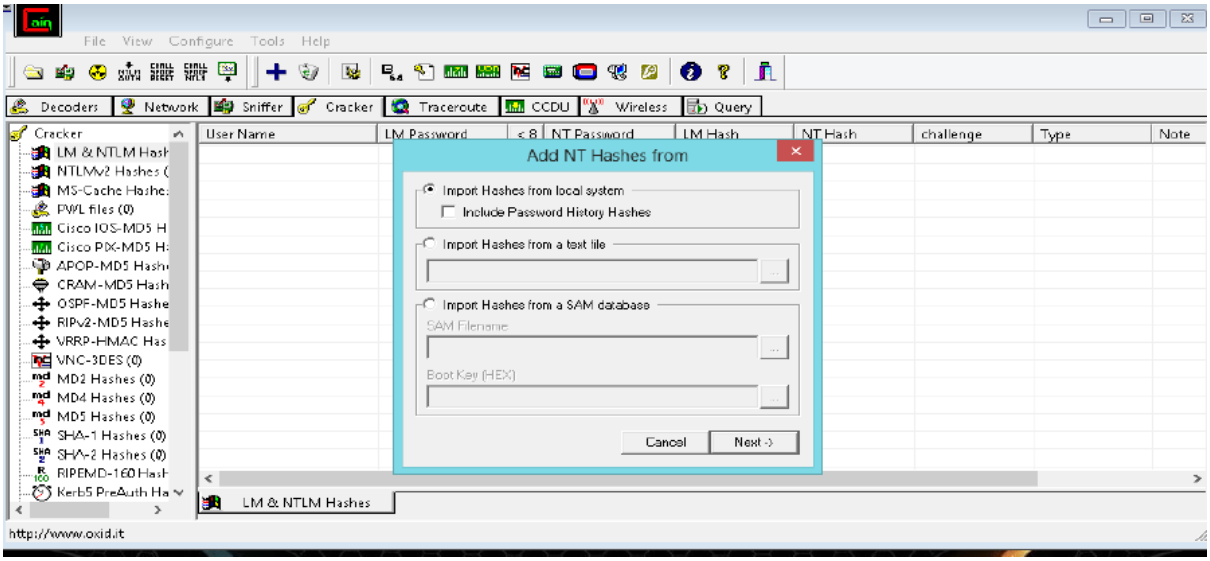


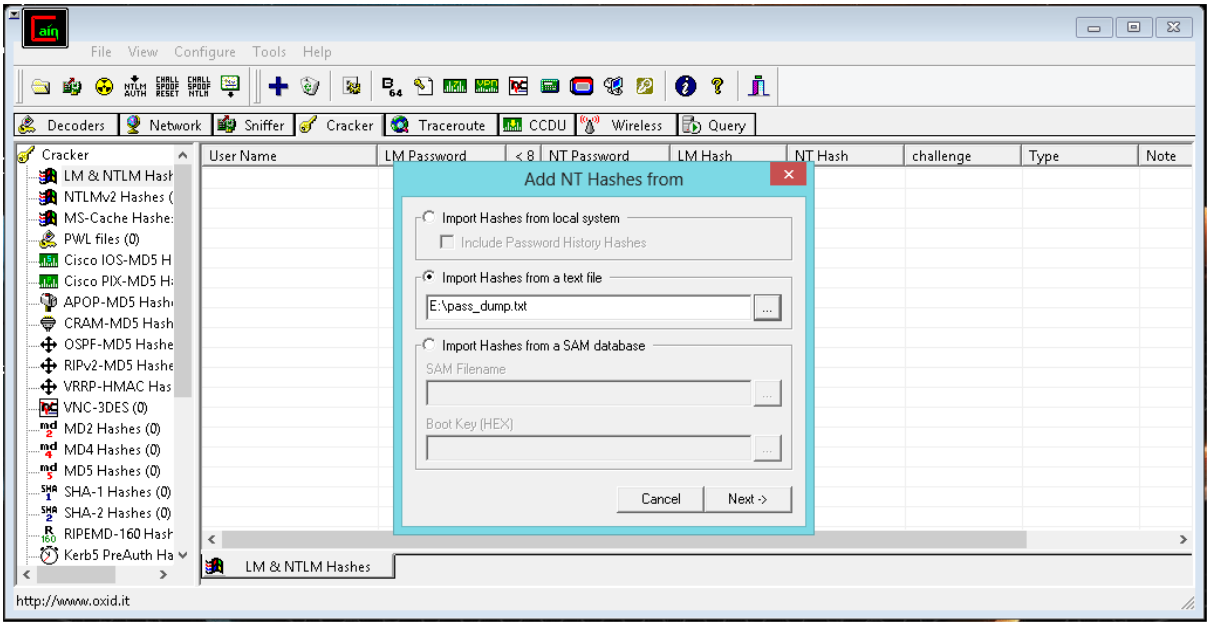
   Jika kita lihat dari hasil screen shoot di atas menujukan bahwa file register pwdump7 berada pada partisi E dan terdapat dalam folder “ Hack Pass” oleh karena itu kita bisa memanggil file dalam pwdump7 dalam partisi E dan berada dalam folder “ hack pass”.
2. Setelah itu kita akan menjalan file register yang ada pada pwdum7 dan membuat file baru yang berformat txt. Untuk menampung data hash dari password laptop seperti pada gambar dibawah ini:



Gambar diatas menunjukan bahwa file register yang digunakan untuk cracking password laptop. Target adalah pwdump.exe setelah itu membuat file baru dengan nama pass-dump dengan format .txt, dengan menuliskan perintah pada cmd e:/pass_dump.txt. setelah itu kita enterkan maka file dengan nama pass_dump.txt akan tersimpan dipartisi E.

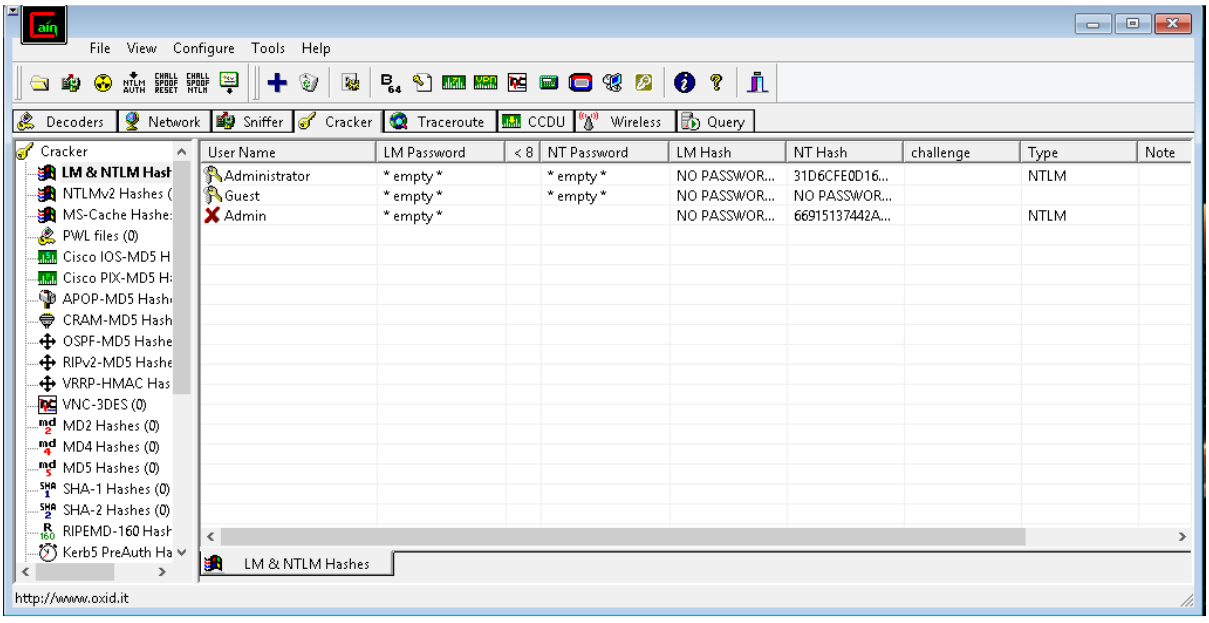
3. Langkah selanjutnya setelah file .txt yang memuat hash password laptop yang telah ditargetkan sudah disimpan, maka langkah selanjutnya adalah membuka aplikasi cain and abel untuk mengekstrak hash computer menjadi plain text yang berisi password laptop yang ditargetkan. Seperti gambar dibawah ini:





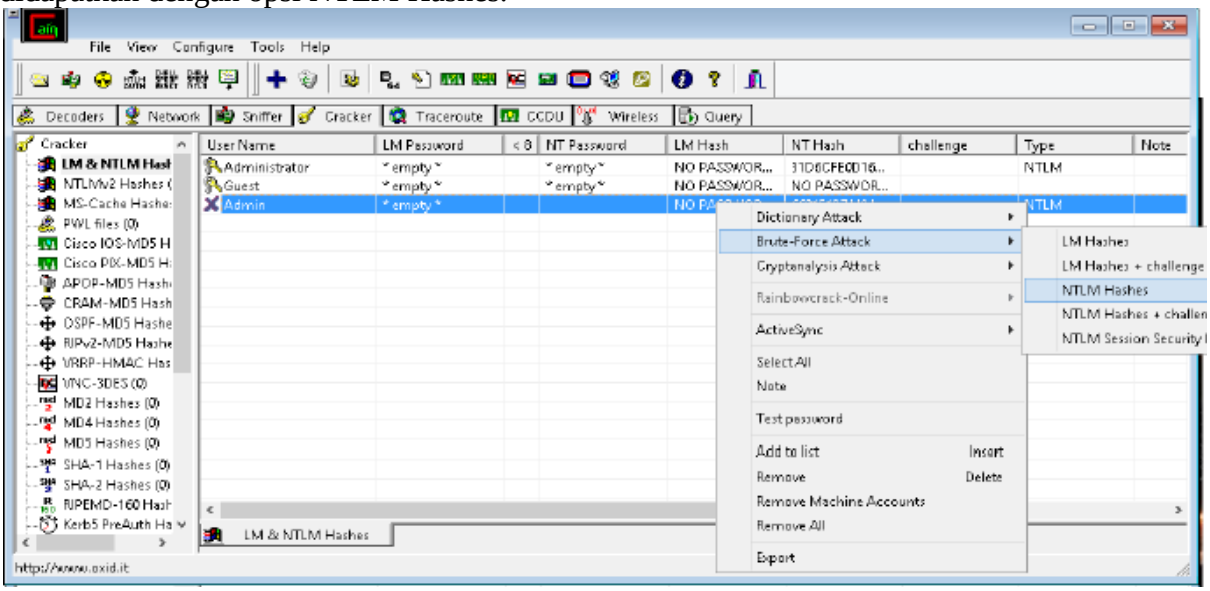
Gambar diatas merupakan interface dari aplikasi cain and abel yang sudah siap untuk digunakan, dengan memilih kolom cracker kemudian pada opsi di menu kolom cracker di sebelah kiri yang digunakan adalah LM & NTLM Hash karena kita ingin menscan Hash dari password target. Sedangkan pada gamba 4 adalah 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. Langkah selanjutnya dengan menggunakan aplikasi cain and abel yang akan menamplkan isi dari file pass_dump.txt yang berisi kode HASH dari password laptop yang kita targetkan. Setelah itu kita menentukan HASH pada akun mana yang diserang. Pada percobaan ini, HASH yang inggin diserang adalah HASH pada akun administrator seperti yang ditunjukan pada gambar dibawah ini:

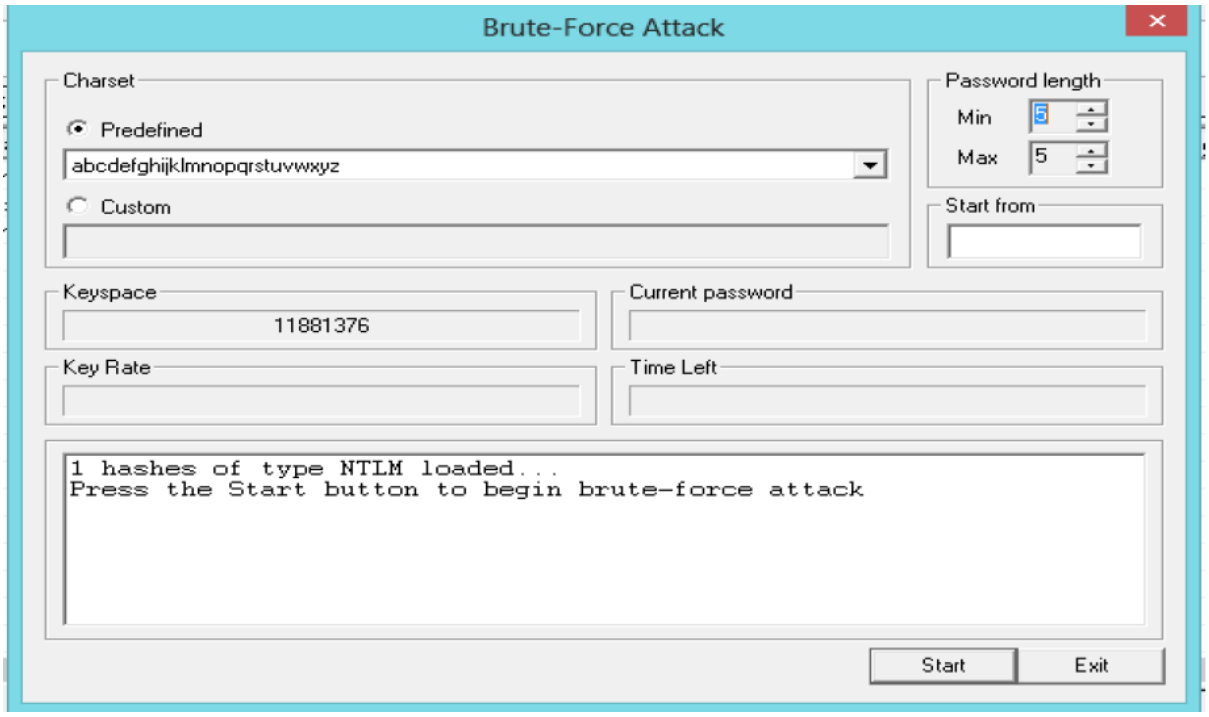


Pada gambar di atas menunjukan bahwa HASH pada akun administrator yang berhasil didapat adalah 66915137442A04BB37263C0D02A9E8A dengan nama akun admin.

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

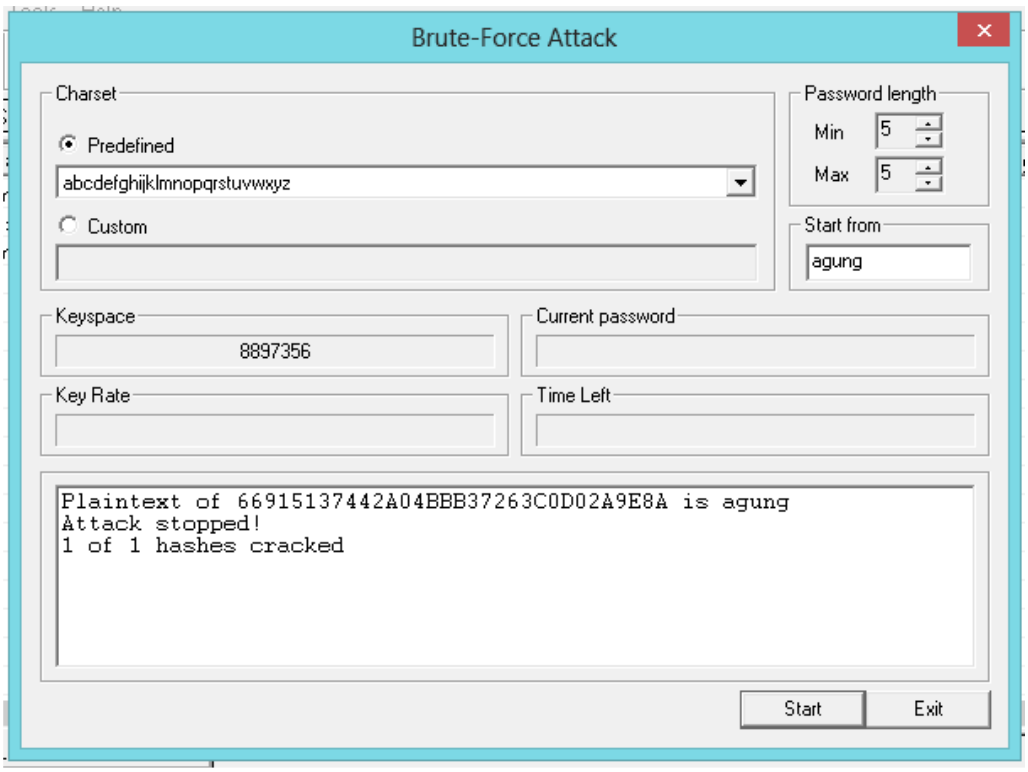


6. Setelah memilih opsi brute force terhadap HASH di laptop yang ditargetkan, maka akan muncul interface brute force yang siap untuk melakukan scanning terhadap hash computer seperti gamabar dibawah ini



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. 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 dibawah ini:



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. Dengan menggunakan aplikasi pwdump dan cain and abel, kita bisa mendapatkan password dengan mudah dan login masuk kedalam sistem pada computer tersebut. 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.