CRACKING (MERETAS) PASSWORD SISTEM OPERASI WINDOWS MENGGUNAKAN PWDUMP dan CAIN & ABEL BERBASIS HASH

Dwiky Reziandino

Fakultas Ilmu Komputer, Universitas Sriwijaya, Indralaya – Indonesia

Email: Dwikyreziandino@gmail.com

ABSTRAK

Keamanan merupakan hal penting dalam menjaga keamanan informasi, namun selama perangkat keamanan dibuat tangan manusia maka tidak akan sempurna, yang kita perlukan adalah mengurangi resiko bobolnya informasi yang kita miliki. Penggunaan password bisa diretas menggunakan berbagai aplikasi , beberapa diantaranya adalah aplikasi pwdump dan cain & abel, dengan mencari hash menggunakan command prompt maka serangan brute force dapat dilakukan dengan estimasi waktu yang singkat selama password tersebut lemah. Jika password tersebut kuat dan memiliki karakter kombinasi maka serangan brute foce ini tidak cocok digunakan karena memakan estimasi waktu yang sangat lama.

***Keyword**: keamanan, password, hash, pwdump, cain & abel.*

PENDAHULUAN

Dalam perkembangan ilmu teknologi dan komunikasi dan komunikasi data didunia senantiasa membawa perkembangan perangkat lunak dan perangkat keras maju pesat, keamanan merupakan hal penting baik itu keamanan fisik maupun keamanan aplikasi. Keamanan sangat penting untuk menjaga berbagai informasi penting yang kita miliki, dapat kita ketahui bersama bahwasanya selama perangkat keamanan itu tidak akan pernah sempurna selama itu masih dibuat oleh tangan manusia. Namun, yang kita perlukan adalah mengurangi resiko bobolnya informasi yang kita miliki.

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. Beberapa perangkat maupun aplikasi seperti komputer, telepon pintar, kartu ATM dan lain sebagainya mengusung penggunaan password baik itu berupa sandi, pin, sidik jari maupun kunci pola. Semuanya memiliki kelemahan-kelemahan yang berujung bocornya informasi-informasi penting.

Pada tulisan kali ini, penulis ingin memberikan cara membobol password operasi sistem Windows 7 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 dictionary attack, bruteforce attack dan cryptanalysis attack. Pada metodologi, penulis akan menjelaskan lebih lanjut tentang cara mencuri password sistem operasi windows 7 menggunakan pwdump dan cain & abel.

METODOLOGI

Mengamankan data informasi pada perangkat komputer sangat perlu dilakukan agar data tersebut tetap bersifat pribadi dan hanya orang-orang tertentu yang mengetahui informasi tersebut. Namun, banyak pengguna yang tidak memperhatikan lemah atau tidaknya password yang mereka gunakan. Jika password tersebut lemah, maka akan mudah sekali meretas keamanan komputer tersebut yang mengakibatkan informasi-informasi pribadi atau penting

dapat diambil dan disebar ke berbagai media. Salah satu cara mencuri password adalah dengan mencari hash password tersebut dan melakukan serangan brute force. Berikut adalah penjelasan tentang hash, software pwdump dan software cain & abel.

1. HASH

   Fungsi Hash banyak sekali digunakan untuk mempercepat pencarian dalam tabel data atau pembandingan data seperti di dalam basis data, mencari duplikasi atau kesamaan (rekaman) disebuah arsip komputer yang besar, menemukan goresan-goresan yang sama di sebuah DNA, dan sebagainya.

   Fungsi hash haruslah stabil (referential transparent), artinya, jika ia dipanggil dua kali oleh masukan yang benar-benar sama (sebagai misal,string yang mengandung sekuen karakter yang sama), maka ia haruslah memberi hasil yang sama pula.Ini adalah sebuah kontrak dalam banyak bahasa pemrograman yang membolehkan pengguna melakukan *override* pada kesamaan morfologi dan fungsi hash bagi sebuah objek, jika dua objek adalah sama, maka kode hash-nya pun sama.menjadi hal yang sangat penting untuk menemukan sebuah elemen di dalam tabel hash dengan cepat,juga karena dua elemen yang sama akan sama-sama meng-hash ke slot yang sama.

   Beberapa fungsi hash dapat memetakan dua atau lebih kunci ke nilai hash yang sama,menyebabkan kolisi. Fungsi-fungsi hash ini mencoba memetakan kunci-kunci ke nilai hash seketat mungkin karena tabrakan-tabrakan (kolisi) akan semakin sering terjadi saat tabel hash semakin terisi penuh.Sehingga, nilai hash digit-tunggal (jumlah dari *probing* setiap nilai hash dibagi dengan jumlah tabel hash) terbatas hanya di 80% ukuran tabel yang ada. Bergantung kepada algoritma yang digunakan, aturan-aturan yang lain mungkin diperlukan, seperti Double Hashing dan Linear Probing(1).

2. 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).

3. 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

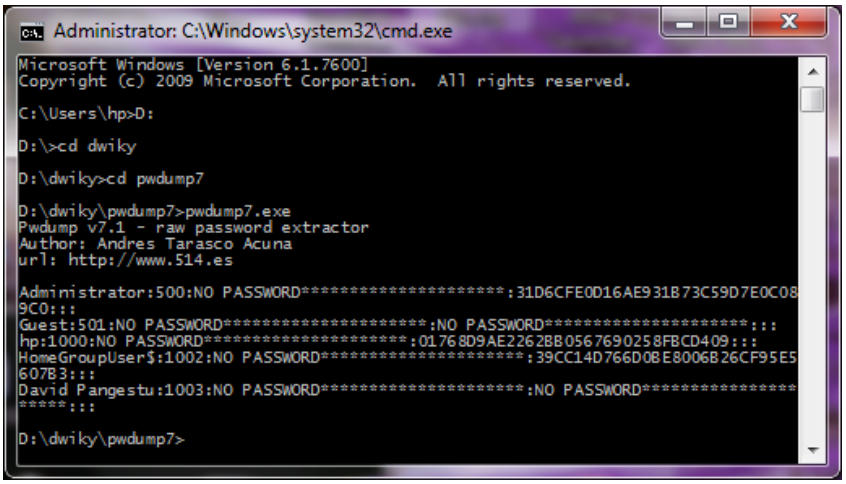
pemulihan disederhanakan password dan kredensial dari berbagai sumber, namun juga kapal beberapa "non standard" utilitas untuk pengguna Microsoft Windows.
Cain & Abel telah dikembangkan dengan harapan bahwa itu akan berguna bagi administrator jaringan, guru, konsultan keamanan / profesional, staf forensik, vendor perangkat lunak keamanan, profesional penetrasi tester dan orang lain yang berencana untuk menggunakannya untuk alasan etis. Penulis tidak akan membantu atau mendukung aktivitas ilegal dilakukan dengan program ini. Diperingatkan bahwa ada kemungkinan bahwa Anda akan menyebabkan kerusakan dan / atau kehilangan data menggunakan software ini dan bahwa tidak ada peristiwa akan penulis bertanggung jawab atas kerusakan atau kehilangan data tersebut. Bacalah Perjanjian Lisensi termasuk dalam program sebelum menggunakannya.
Versi terbaru lebih cepat dan berisi banyak fitur baru seperti April (Arp Poison Routing) yang memungkinkan sniffing pada LAN diaktifkan dan serangan Man-in-the-Tengah. Sniffer dalam versi ini juga dapat menganalisis protokol terenkripsi seperti SSH-1 dan HTTPS, dan berisi filter untuk menangkap mandat dari berbagai mekanisme otentikasi. Versi baru juga kapal protokol routing monitor otentikasi dan rute extractors, kamus dan brute-force kerupuk untuk semua algoritma hashing umum dan untuk beberapa otentikasi spesifik, kalkulator sandi / hash, serangan kriptanalisis, Decoder kata sandi dan beberapa utilitas tidak begitu umum terkait dengan jaringan dan sistem keamanan(3).

Dengan software pwdump dan cain & abel sangat memungkinkan meretas sebuah password yang lemah dengan estimasi waktu yang singkat, dengan serangan brute force yang memetakan karakter-karakter lemah sehingga didapatkan password yang kita inginkan. Penggunaan pwdump dan cain & abel ini dilakukan pada kondisi komputer telah hidup dan telah login ke akun pengguna. Jika belum melakukan login ke akun pengguna maka pencurian password tidak akan berjalan dengan kedua software tersebut. Cara melakukan pencurian password adalah dengan mencari hash password tersebut, kemudian pwdump melakukan pemetaan karakter yang kemudian disimpan dalam bentuk format .txt lalu cain & abel mengambil hash yang berupa format .txt tersebut kemudian dilakukan serangan brute force, proses serangan brute force memakan waktu yang berbeda tergantung karakter dan kombinasinya, jika password tersebut lemah makan akan membutuhkan waktu yang singkat sedangkan jika password tersebut merupakan password kombinasi yang kekuatan dari password tersebut adalah kuat atau sangat kuat maka serangan brute force ini akan memakan waktu yang sangat lama tergantung kondisinya. Bahkan, jika password tersebut sangat kuat, serangan brute force akan memakan waktu hingga bertahun-tahun lamanya.

Pada tulisan ini, penulis melakukan serangan terhadap password yang lemah sehingga tidak memakan waktu yang lama, pada hasil percobaan dapat dilihat langkah-langkah yang penulis lakukan.

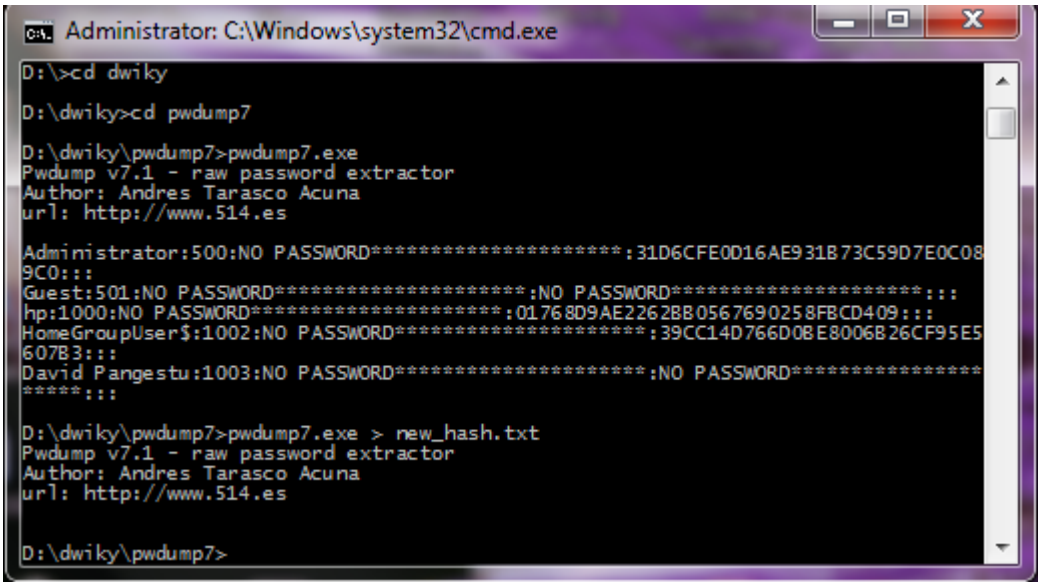
PERCOBAAN DAN HASIL PENELITIAN

Yang pertama dilakukan adalah dengan mencari hash password, buka command prompt lalu panggil folder tempat dimana pwdump disimpan seperti pada gambar dibawah ini



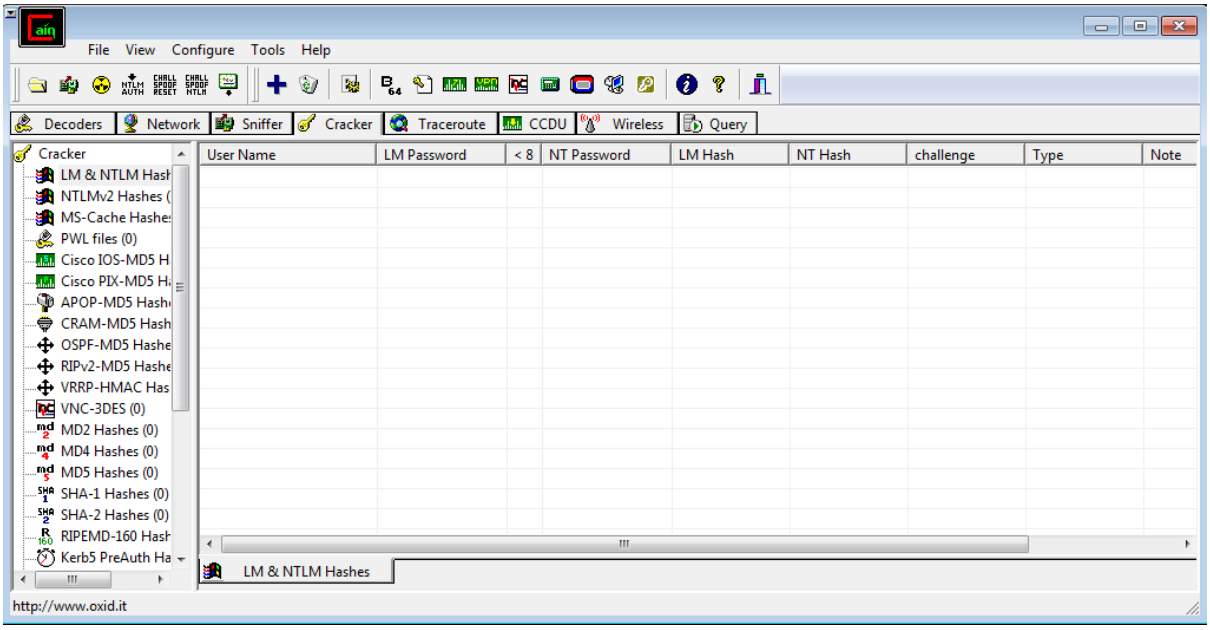
Gambar 1, mendapatkan hash dengan pwdump menggunakan command prompt.

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.



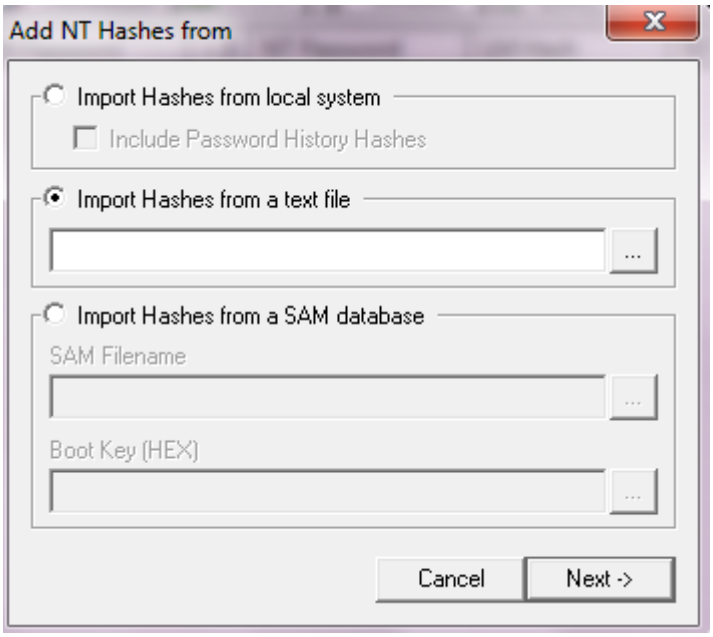
Gambar 2, mengubah hash password menjadi file .txt.

Pada gambar 2, file .txt diberi nama new_hash.txt, setelah itu buka aplikasi cain & abel dengan cara run as administrator. Setelah program terbuka masuk ke direktori cracker seperti gambar dibawah ini.



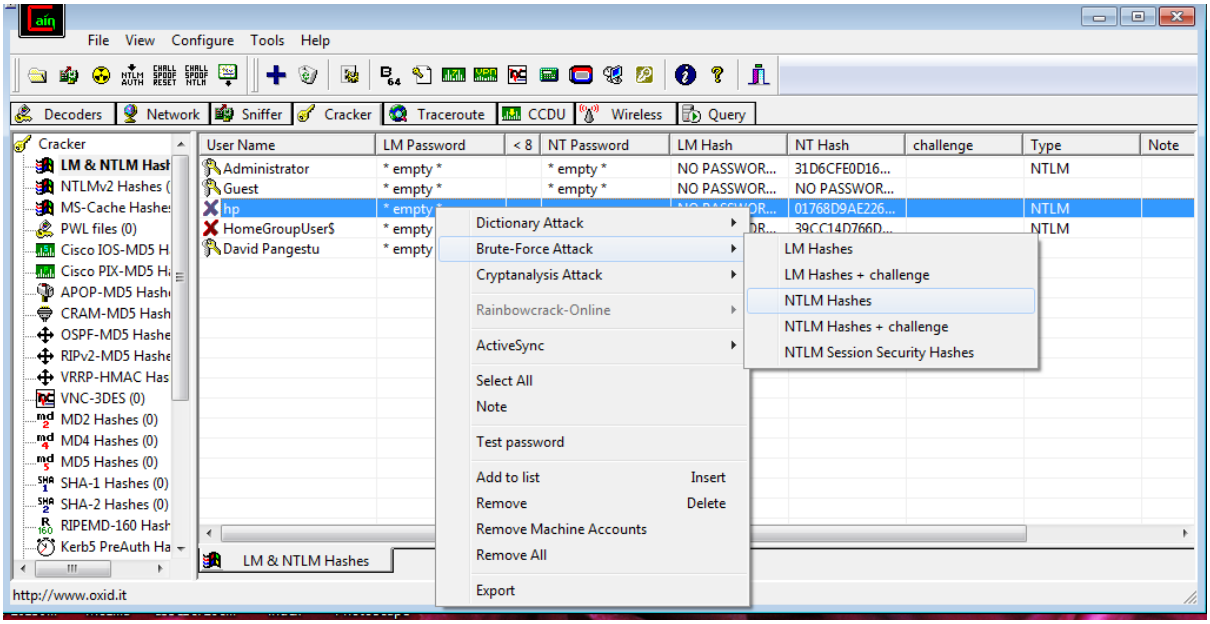
Gambar 3, aplikasi cain & abel yng telah masuk ke direktori cracker.

Setelah itu pilih menu cracker LM & NTLM Hashes dan dipilih tools tanda "plus". Kemudian akan terbuka seperti dibawah ini.



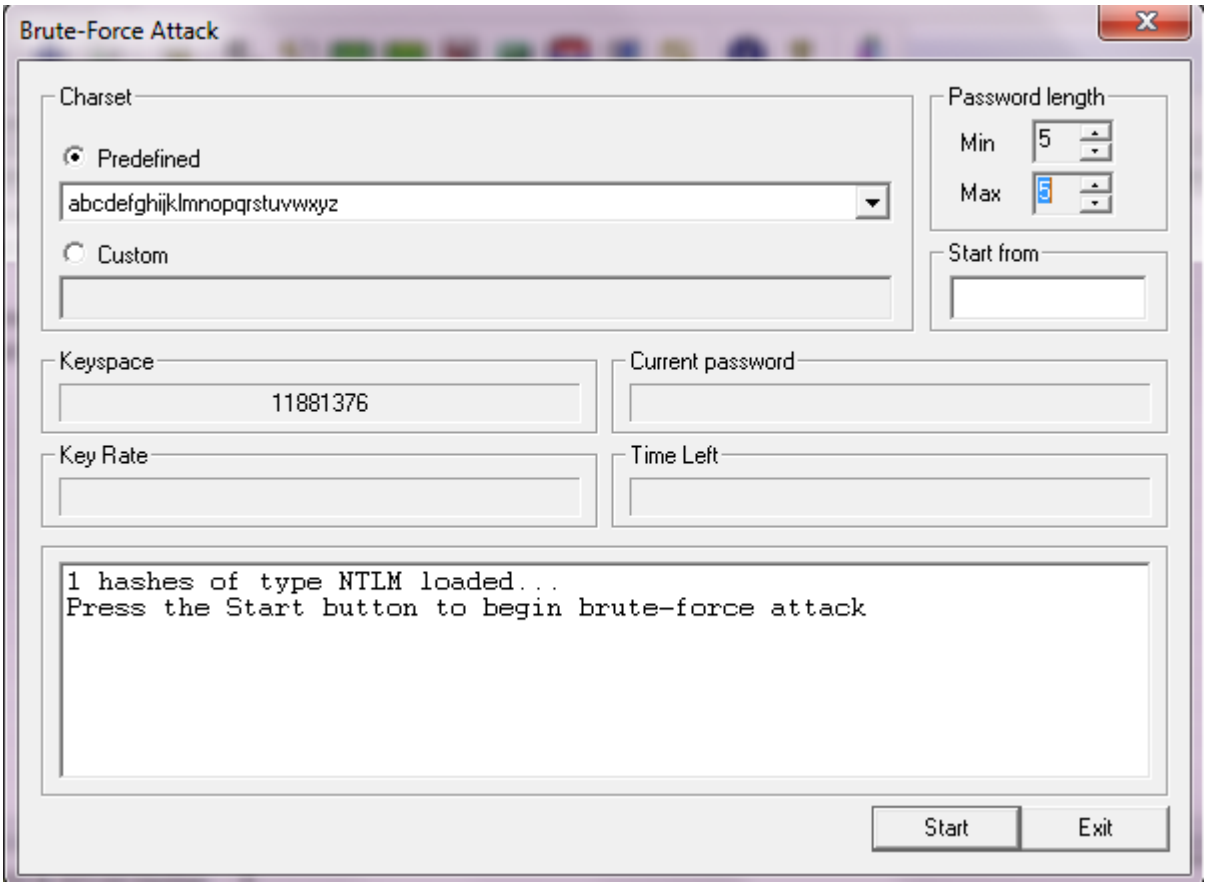
Gambar 4, penambahan note hash dari text file.

Pilih import hashes from text file lalu tambahkan file new_hash.txt yang telah kita simpan tadi. Kemudian pilih next dan oke. Setelah mendapatkan hash di cain & abel kemudian pilih user yang digunakan, disini penulis menggunakan user HP sebagai administrator. Lalu klik kanan kursor pada HP lalu pilih Brute-Force Attack dan pilih NTLM Hashes seperti pada gambar dibawah ini.



Gambar 5, pemilihan serangan pada hash yang telah dipilih menggunakan cain & abel.

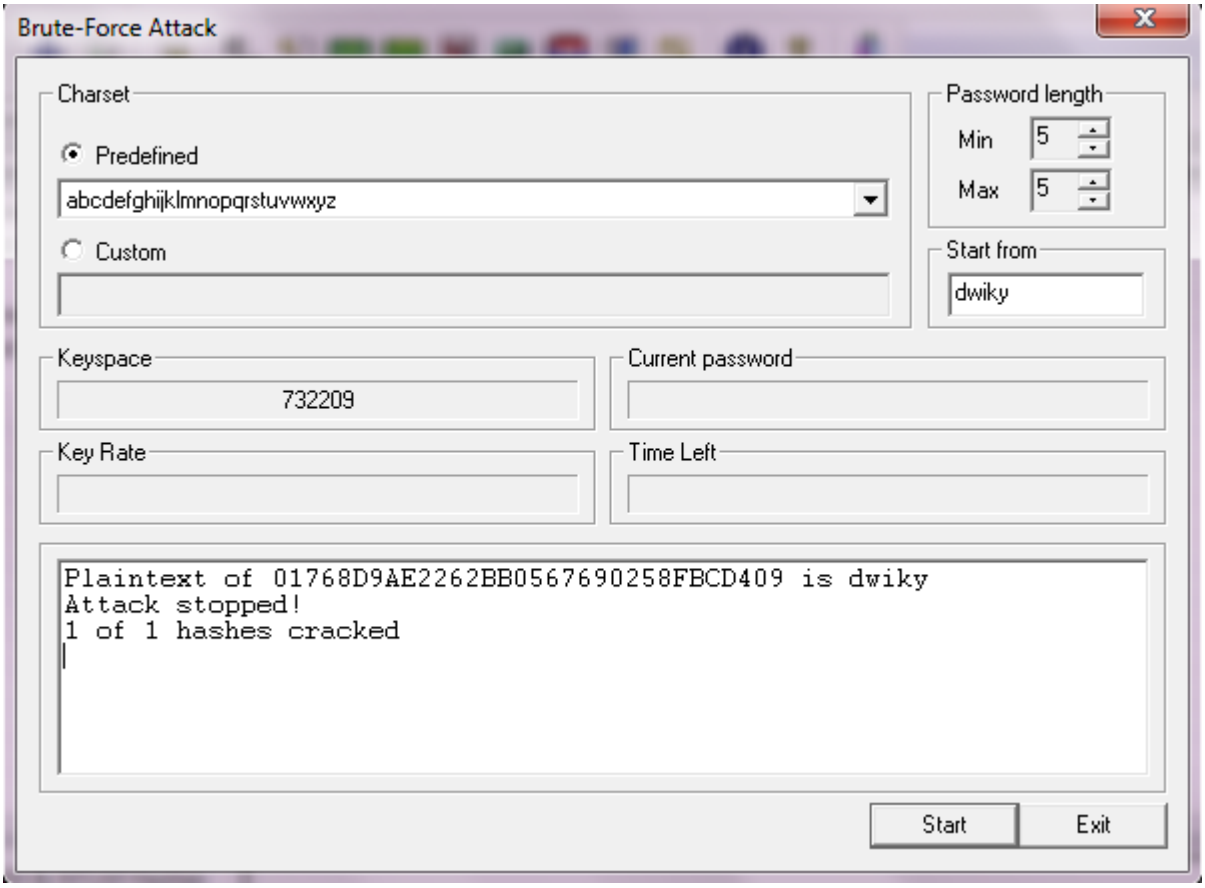
Setelah NTLM Hashes di klik akan muncul tampilan seperti gambar dibawah ini.



Gambar 6, pemilihan cara serangan brute force pada cain & abel.

Pada gambar diatas, penulis mendapati predefined untuk memilih pola karakter yang digunakan hash password. Penulis memilih karakter abjad kecil supaya memudahkan serangan bruteforce, panjang karakter password juga kita minimalkan seperti gambar diatas

agar estimasi waktu yang terpakai tidak terlalu lama. Setelah mengatur panjang password serangan brute force, klik start kemudian tunggu hingga password komputer didapatkan seperti gambar dibawah ini.



Gambar 7, password yang telah didapatkan dengan serangan brute force.

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

KESIMPULAN

Dapat kita simpulkan bahwa keamanan komputer sangat penting untuk menjaga data informasi kita agar tetap rahasia, namun selama teknik keamanan itu dibuat oleh tangan manusia maka keamanan tersebut tidaklah sempurna dan masih bisa dibobol. Adapun cara membobol sistem seperti mencuri password bisa dilakukan dengan berbagai cara, salah satunya adalah dengan melakukan serangan brute force terhadap hash yang didapat dalam sistem basis data komputer tersebut. Serangan ini dilakukan bertujuan untuk memberikan informasi kepada pengguna dan mengingatkan pengguna terhadap serangan yang bisa dilakukan ketika pengguna lupa menutup perangkat komputernya dan diambil password operasi sistemnya. Namun, serangan brute force ini tidak cocok digunakan untuk password yang memiliki karakter kombinasi karena memakan waktu yang sangat lama, selain itu sofware pwdump dan cain & abel tidak bisa digunakan pada kondisi komputer yang belum masuk ke sistem operasi (jika sistem operasi tersebut memakai password).

REFERENSI

1. https://id.wikipedia.org/wiki/Hash
2. https://en.wikipedia.org/wiki/Pwdump
3. http://www.oxid.it/cain.html