Password Cracking Windows 7

M. Sulkhan Nurfatih
e-mail : 09121001061@students.ilkom.unsri.ac.id

Abstrak

Password cracking adalah teknik yang digunakan untuk memperoleh password pada sebuah sistem tertentu. Terdapat beberapa teknik dalam melakukan cracking diantaranya dictionary, hybrid, dan brute force. Dalam kasus berikut kita akan mengunakan metode brute force dengan menggunakan tools yang sudah ada yaitu cain and abel. Teknik brute force sendiri adalah sebuah teknik yang akan mencoba setiap kombinasi karakter yang memungkinkan mencapai set pada password yang tepat. Ini sangat memakan waktu karena ada huruf yang memungkinkan tak terhitung jumlahnya, nomor yang banyak dan kombinasi symbol dari seorang individu yang bisa digunakan untuk password. Hasil dari percobaan menunjukkan kekuatan password bergantung pada kerumitan password yang digunakan. Sebab semakin banyak kombinasi password semakin lama dalam proses cracking.

Kata kunci : *Password Cracking, Brute force, Cain and Abel*

I. Pendahuluan

Pada sebuah sistem operasi yang terdapat didalam sebuah komputer tentu sering kita temukan sebuah keamanan yang dibuat oleh sistem tersebut. Keamanan ini dibuat agar data yang ada di dalam tidak di salah gunakan atau dicuri oleh orang tidak bertanggung jawab. Keamanan standar yang ada berupa *password* (kata sandi) yang harus di masukkan saat mengoprasikan sebuah komputer. Pengertian *password* (kata sandi) sendiri adalah kumpulan karakter atau *string* yang digunakan oleh pengguna jaringan atau sebuah sistem ooperasi yang mendukung banyak pengguna (*multiuser*) untuk memverifikasi identitas kepada sistem keamanan yang dimiliki oleh jaringan atau sistem tersebut. Kata sandi juga dapat diartikan sebagai kata rahasia yang digunakan sebagai pengenal.

II. Password Cracking

Pengertian dasar dari *password cracking* adalah istilah umum yang menggambarkan sekelompok teknik yang digunakan untuk memperoleh *password* pada sebuah sistem tertentu. *Password cracking* khusus mengacu pada proses mendapatkan *password* dari data yang dilindungi dengan *password.* Namun, harus dicatat bahwa cara-cara menipu seseorang agar memberi *password,* seperti melalui *phishing,* tidak dianggap sebagai *paswor cracking.* Menebak password berdasarkan pengetahunan yang sudah ada sebelumnya dari pemilik sistem komputer dianggap *cracking,* karena *password* tidak dikenal sebelumnya. Berikut ini adalah beberapa teknik umum yang digunakan dalam *password cracking* :

1. Serangan Dictionary

   Sebuah serangan yang merupakan cara tercepat dan terbaik dalam melumpuhkan mesin. Sebuah file directionary (sebuah file teks yang berisi kamus password) diload pada aplikasi cracking seperti L0phtCrack atau Cain and Abel, yang dijalankan terhapad user account yang ditemukan oleh aplikasi tersebut. Karena sebagai besar password seringkali tergolong sederhana, menjalankan sebuah dictionary attack seringkali cukup membantu.

2. Serangan Hybrid

   Bentuk serangan lainnya yang terkenal adalah serangan "*Hyabrid*". Sebuah serangan hyabrid akan menambahkan angka atau symbol terhapad nama file untuk keberhasilan meng-crack password. Pola yang digunakan biasanya berbentuk *first month password is"cat"; second month password is "cat1"; third month password is "cat2";* dan seterusnya

3. Serangan Brute Force

   Bentuk serangan selanjutnya adalah brute force, biasanya memakan waktu yang sangat lama, tergantung kompleksitas password tersebut terkadang perlu waktu sampai seminggu guna menebak password. LophtCrack seringkali digunakan untuk melakukan serangan brute force. Serangan brute force merupakan metode password craking yang secara signifikan lebih kuat daripada serangan metode kamus. Sebuah program brute force attack akan mencoba setiap kombinasi karakter yang memungkinkan mencapai set pada password yang tepat. Ini sangat memakan waktu karena ada huruf yang memungkinkan tak terhitung jumlahnya, nomor yang banyak dan kombinasi symbol dari seorang individu yang bisa digunakan untuk password.

Metode cracking lain untuk password cracking bisa juga dengan menggunakan fungsi hash kriptografi sistem komputer. Sebuah fungsi hash kriptografi adalah suatu prosedur yang mengubah password ke bit string berukuran seragam. Jika hash dapat di crack, dimungkinkan untuk reverse-engineer password. Kebanyakan fungsi hash sangat kompleks dan tidak dapat di crack tanpa waktu dan usaha yang panjang.

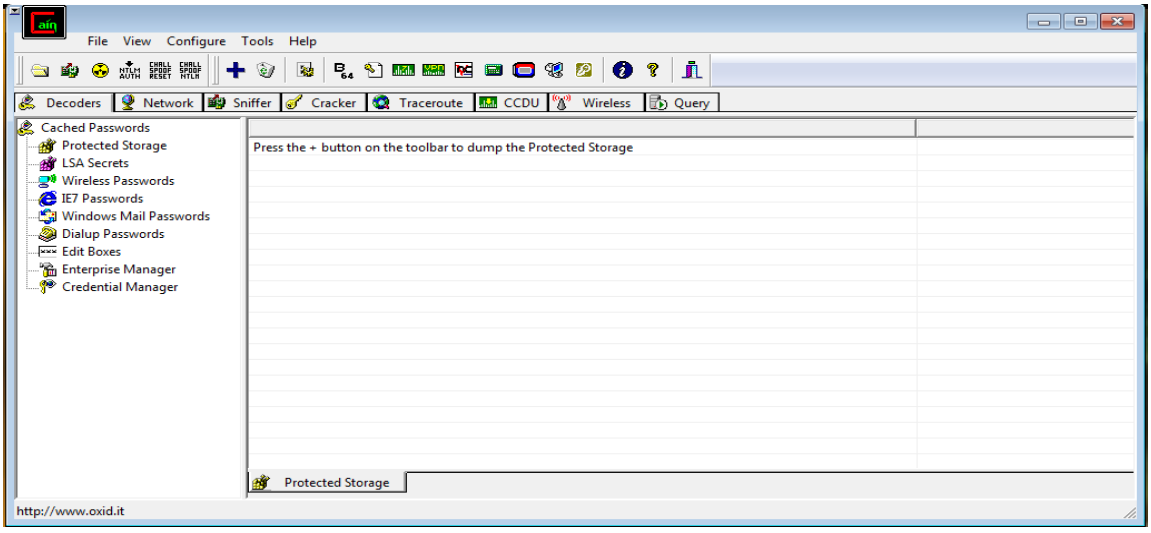
III. Tools Password Cracking

A. Tools Cain and Abel

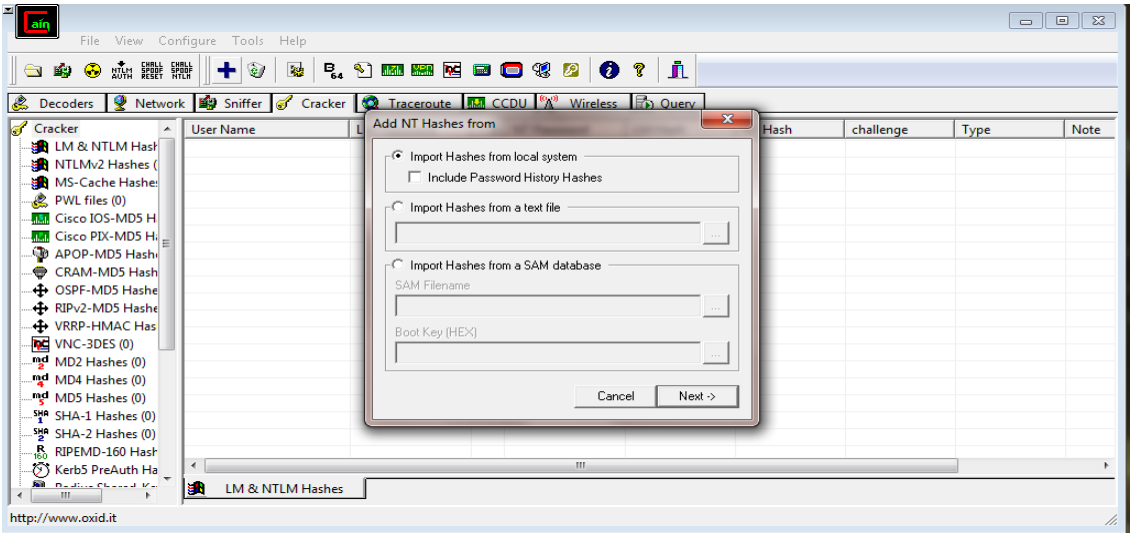
Pada kali ini kita akan menggunakan tools Cain and Abel. Tools ini merupakan salah satu alat cracking atas untuk password cracking dan pemulihan password untuk Windows OS. Cain and Abel dapat menggunakan serangan kamus (dictionary), brute force dan kriptoanalisis serangan crack password terenkripsi. Jadi hanya menggunakan kelemahan sistem crack password. Antara GUI dari perangakat lunak ini sangat sederhana dan mudah digunakan. Tetapi memiliki batasan ketersediaan, alat ini hanya tersedia untuk jendela berbasis sistem. Cain and Abel memiliki banyak fitur yang diantaranya ; digunakan untuk cracking WEP, memiliki kemampuan untuk merekam percakapan VoIP, sebagai jaringan password sniffer, menyelesaikan alamat IP untuk MAC, dan banyak lagi fitur yang terdapat didalamnya.

IV. Simulasi Password Cracking Pada Windows 7

Kita akan menjalan Cain and Abel yang sebelumnya sudah di Instal didalam sistem operasi Windows 7.

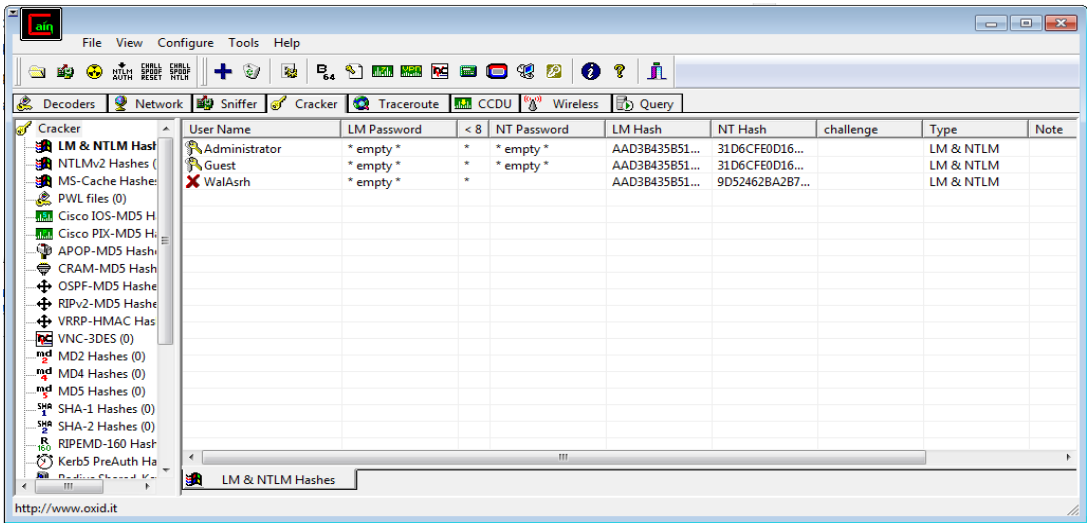


Gambar 1.1 Tampilan awal tools Cain and Abel



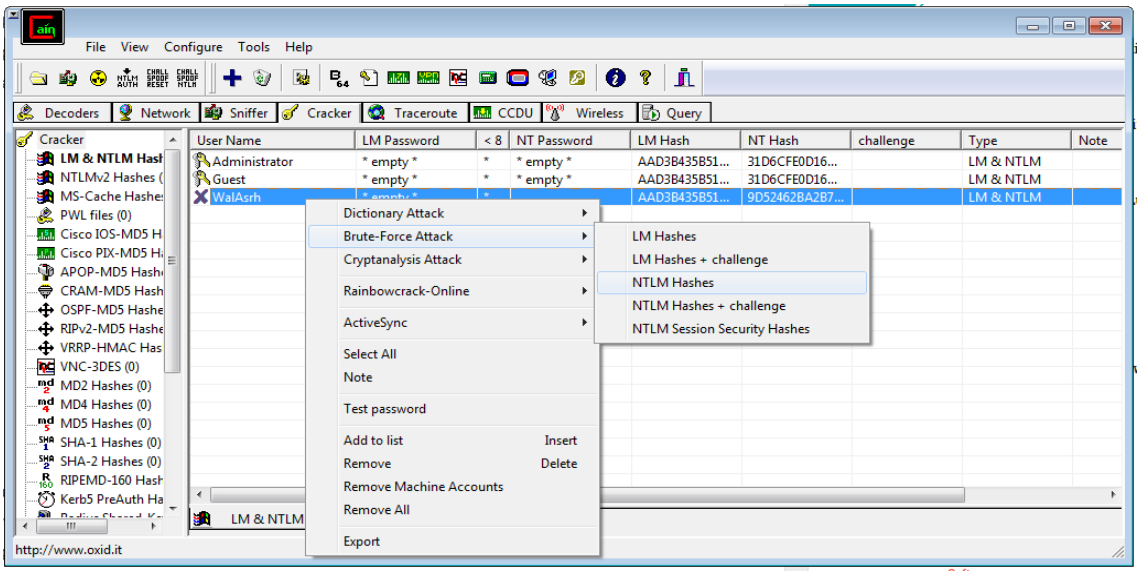
Gambar 1.2 Tampilan memulai proses cracking

Pada gambar 1.2 kita dapat melihat halaman Add NT Hashes Form yang di dapat dengan membuka tab cracker dan mengaktifkan tombol (+). Setelah itu pilih Next.

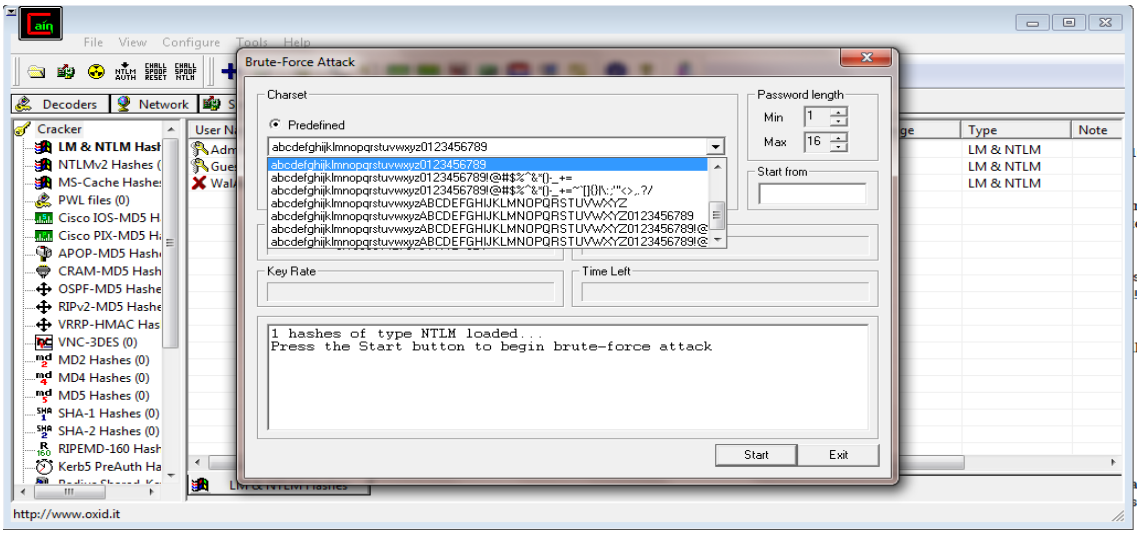


Gambar 1.3 Tampilan list user yang ada komputer

Pada gamabr 1.3 terdapat list dari user yang ada pada komputer, lengkap dengan nama user, jumlah karakter password, dan apakah user tersebut dilengkapi password atau tidak. Jika sebauh user dilengkapi dengan password, maka pada kolom NT Password, statusnya akan kosong. Jika passwordnya memiliki jumlah dibawah 8 karakter, maka pada kolom NTLM Hashes.

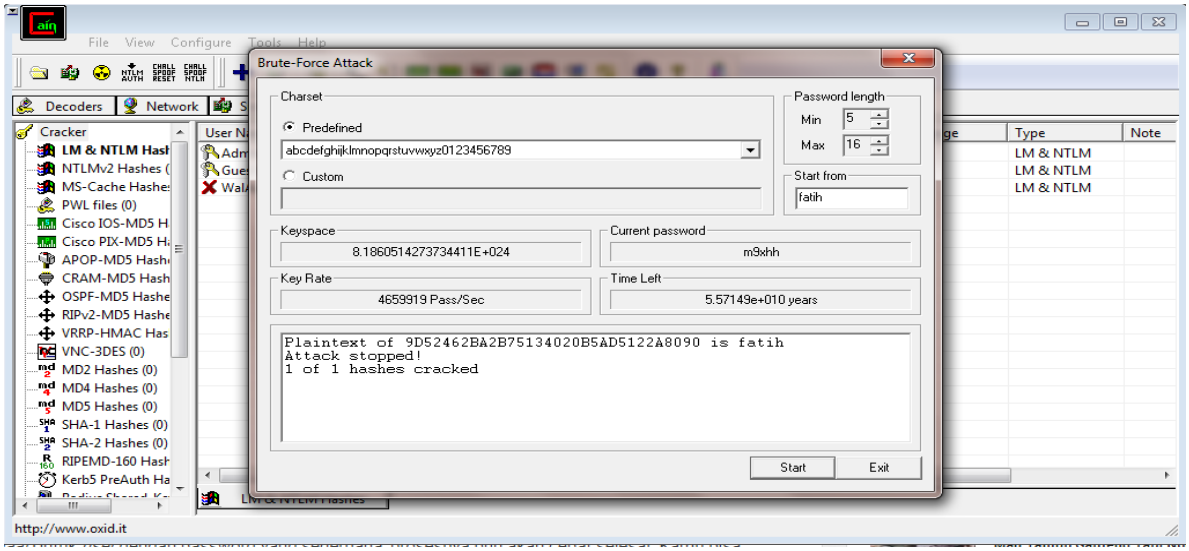


Gambar 1.4 Tampilan untuk membuka Brute Force Attack



Gambar 1.5 Tampilan halaman Brute Force Attack

Pada gambar 1.5 merupakan tampilan halaman brute force attack. Kolom Charset dapat kita ganti sesuai dengan karakter apa yang kemungkinan digunakan pada password yang ingin dihack. Semakin panjang list yang tersedia, maka proses hack brute force akan lebih lama. Dalam hal ini kita pilih yang pertama, kemudian Start.



Gambar 1.6 Tampilan hasil dari Brute Force Attack

Pada gambar 1.6 merupakan hasil setelah melakukan brute force attack dimana password yang didapat adalah “fatih”. Semakin rumit password yang digunakan, maka proses hack juga akan berjalan lebih lama.

V. Kesimpulan

Untuk melakukan sebuah password cracking saat ini bisa dibilang mudah. Sebab, banyak tools yang dapat digunakan untuk mewujudkan itu semua. Namun, yang menjadi parameter tetap kerumitan dari sebuah password yang akan menentukan seberapa lama password itu akan di hack. Pada kasus diatas password yang digunakan terbilang lemah sehingga tidak kurang dari satu menit password sudah dapat diketahui.

Daftar Pustaka

"*Cain and Abel*" http://id.wondershare.com/password/password-cracker-tools.html (diakses 22 April 2016)

"Password Cracking" http://dagangku.com/?page=tips-detail.html&news=101 (diakses 22 April 2016)

"Password" https://id.wikipedia.org/wiki/Kata_sandi (diakses 22 April 2016)