

Cracking Akun dan Password Windows XP Menggunakan Software *Cain Able*

Anggoro Prasetyo (09121001064)
Jurusan Sistem Komputer
Universitas Sriwijaya
Jl. Raya Palembang–Prabumulih Km.32 Indralaya Ogan Ilir 30662
Email : angga.destiny94@gmail.com

ABSTARK

Jika orang lain mengetahui data yang bersifat rahasia maka hal tersebut dapat saja merugikan pemilik data. Sangat dikhawatirkan jika data tersebut digunakan untuk akses control suatu sistem. Untuk mengamankan data suatu sistem biasanya data akan di lindungi dengan teknik kriptografi. Hal ini bertujuan untuk melindungi data asli dari pencurian. Pencuri data akan mendapatkan data yang telah di enkripsi sehingga membuat hacker butuh waktu untuk memecahkan password. Pada windows XP, password login administrator dapat diketahui dengan mencoba teknik brute force password dimana sebelumnya kita harus mengetahui kode hash dari password tersebut. Salah satu tools yang dapat digunakan ialah *Cain and Able*, software ini berfungsi untuk mencari hash dari password akun yang ada di windows XP. Setelah mendapatkan kode hash selanjutnya kode hash tersebut akan di brute force dengan options yang flexible hingga menemukan password aslinya.

Kata Kunci : Brute Force, Hash, *Cain and Able*

I. PENDAHULUAN

1. LATAR BELAKANG

Kerahasiaan data saat ini menjadi hal yang sangat dilindungi. Jika orang lain mengetahui data yang bersifat rahasia maka hal tersebut dapat saja merugikan pemilik data. Sangat dikhawatirkan jika data tersebut digunakan untuk akses control suatu sistem. Untuk mengamankan data suatu sistem biasanya data akan di lindungi dengan teknik kriptografi. Hal ini bertujuan untuk melindungi data asli dari pencurian. Pencuri data akan mendapatkan data yang telah di enkripsi sehingga membuat hacker butuh waktu untuk memecahkan password. Pada windows XP, password login administrator dapat diketahui dengan mencoba teknik brute force password dimana sebelumnya kita harus mengetahui kode hash dari password tersebut. Salah satu tools yang dapat digunakan ialah *Cain and Able*, software ini berfungsi untuk mencari hash dari password akun yang ada di windows XP, dari akun admin, akun guest dan akun lainnya. Setelah mendapatkan kode hash selanjutnya kode hash tersebut akan di brute force dengan options yang flexible hingga menemukan password aslinya.

2. TUJUAN

Tujuan dari percobaan ini ialah untuk mengetahui password akun administrator maupun akun lainnya yang berada pada windows XP dengan menggunakan teknik brute force berdasarkan kode hash dari password yang ada..

II. TINJAUAN PUSTAKA

1. CRACKING

Cracking adalah kegiatan membobol suatu sistem komputer dengan tujuan menggambil. Sedangkan orang yang melakukan cracking disebut cracker. Cracker biasanya mencoba masuk ke dalam suatu sistem komputer tanpa ijin (authorisasi), individu ini biasanya berniat jahat/buruk, sebagai kebalikan dari 'hacker', dan biasanya mencari keuntungan dalam memasuki suatu sistem.

Dengan berhubungan dengan koleganya, seorang cracker dapat belajar mengenai teknik-teknik baru, memahami ideologi cracker, barter informasi, mengajak cracker lain untuk melakukan cracking hingga berbagi pengalaman. Sosialisasi cracker dengan cracker lainnya sebagai kerap terjadi di suatu tempat yang sama dan dapat dianggap sebagai sebuah komunitas.

Dalam komunitas tersebut, cracker melakukan hubungan melalui alat komunikasi elektronis sehingga komunitas tersebut bisa dinyatakan sebagai komunitas elektronis atau maya. Komunitas maya tersebut kerap menggunakan aplikasi chat atau Internet Relay Chat (IRC).

2. BRUTE FORCE

Brute force attack atau dalam bahasa Indonesia disebut juga dengan Serangan brute force ini adalah sebuah teknik serangan terhadap sebuah sistem keamanan komputer yang menggunakan percobaan terhadap semua kunci password yang memungkinkan atau istilah gampangnya mungkin menggunakan Random password/password acak. Pendekatan ini pada awalnya merujuk pada sebuah program komputer yang mengandalkan kekuatan pemrosesan komputer dibandingkan kecerdasan manusia. Istilah brute force sendiri dipopulerkan oleh Kenneth Thompson.. Teknik yang paling banyak digunakan untuk memecahkan password, kunci, kode atau kombinasi. Cara kerja metode ini sangat sederhana yaitu mencoba semua kombinasi yang memungkinkan memecahkan tembok keamanan.

Sebuah password dapat dibongkar dengan menggunakan program yang disebut sebagai password cracker. Program password cracker adalah program yang mencoba membuka sebuah password yang telah terenkripsi dengan menggunakan sebuah algoritma tertentu dengan cara mencoba semua kemungkinan. Teknik ini sangatlah sederhana, tapi efektivitasnya luar biasa, dan tidak ada satu pun sistem yang aman dari serangan ini, meski teknik ini memakan waktu yang sangat lama, khususnya untuk password yang rumit.

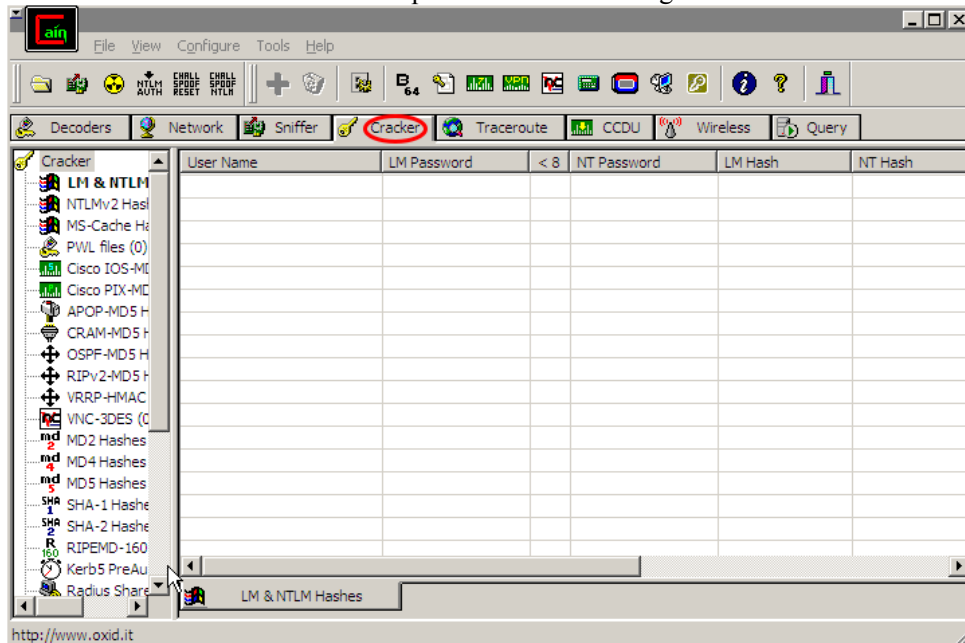
Namun ini tidak berarti bahwa password cracker membutuhkan decrypt. Pada prakteknya, mereka kebanyakan tidak melakukan itu. Umumnya, kita tidak dapat melakukan decrypt password-password yang sudah terenkripsi dengan algoritma yang kuat. Proses-proses enkripsi modern kebanyakan hanya memberikan satu jalan, di mana tidak ada proses pengembalian enkripsi. Namun, anda menggunakan tool-tool simulasi yang mempekerjakan algoritma yang sama yang digunakan untuk mengenkripsi password orisinal. Tool-tool tersebut membentuk analisa komparatif. Program password cracker tidak lain adalah mesin-mesin ulet pintar. Ia akan mencoba kata demi kata dalam kecepatan tinggi. Mereka menganut "Azaz Keberuntungan", dengan harapan bahwa pada kesempatan tertentu mereka akan menemukan kata atau kalimat yang cocok. Teori ini mungkin tepat mengena pada anda yang terbiasa membuat password asal-asalan. Dan memang pada kenyataannya, password-password yang baik itu lebih sulit untuk ditembus oleh program password seperti halnya password Cracker.

III. METODELOGI

Sebenarnya konsep cracking password windows XP sangat sederhana dimana setelah mendapatkan kode hash dari akun yang berada di sistem operasi windows, selanjutnya kode tersebut akan dicocokkan namun dengan menggunakan cara brute force. Brute force sendiri berarti dengan mencoba satu persatu huruf-huruf yang telah kita tentukan dan akan di acak secara acak hingga menemukan kecocokan dari kode hash yang didapat sebelumnya.

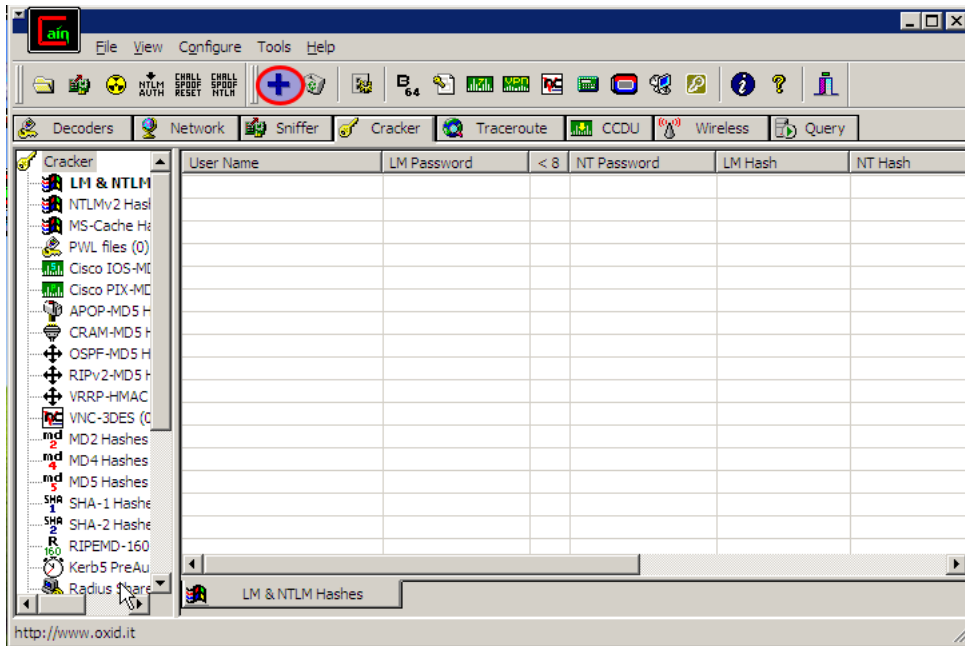
1. MENDAPATKAN HASH PASSWORD DARI SETIAP AKUN YANG ADA DI WINDOWS XP

Hal pertama yang akan dilakukan adalah membuka software Cain and Able. Setelah membuka software tersebut pilih tab craker. Lihat gambar 1



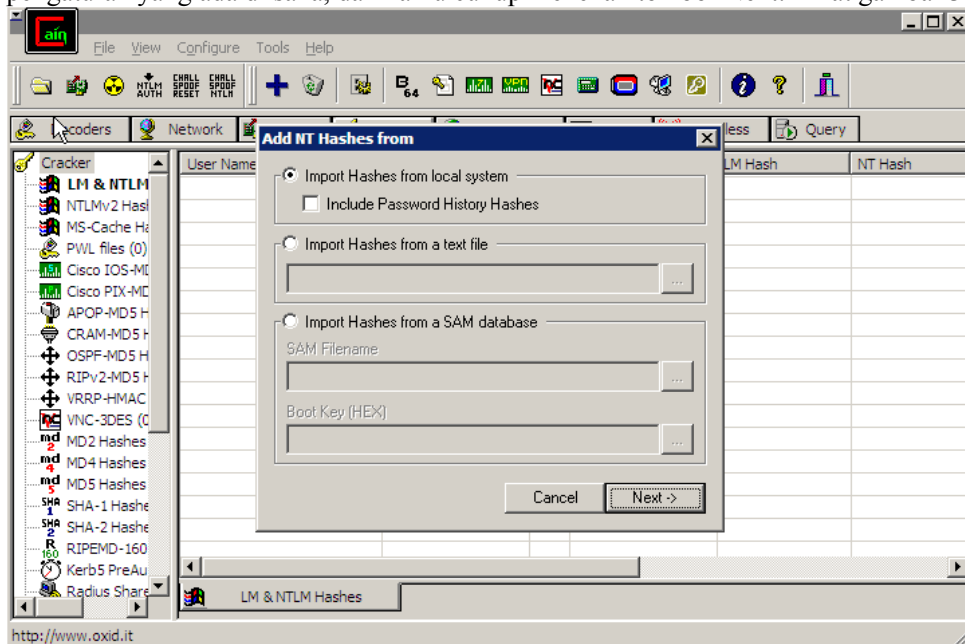
Gambar 1

Selanjutnya klik list kolom yang masih kosong, lalu klik tanda plus (+). Lihat gambar 2.



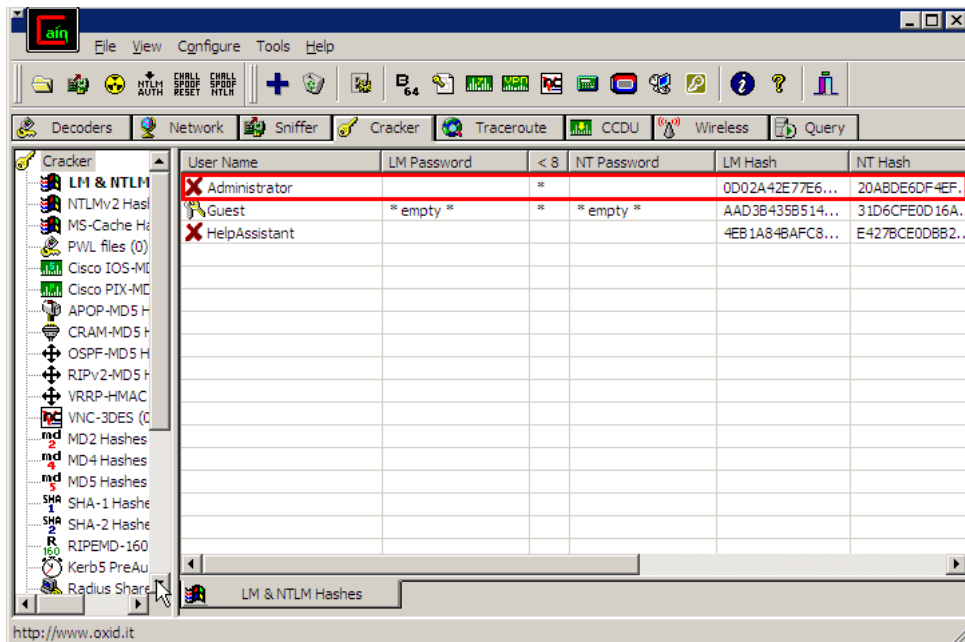
Gambar 2

Ketika halaman Add NT Hashes from sudah tampil di Cain & Abel, abaikan pengaturan yang ada di sana, dan kamu cukup menekan tombol Next. Lihat gambar 3.



Gambar 3

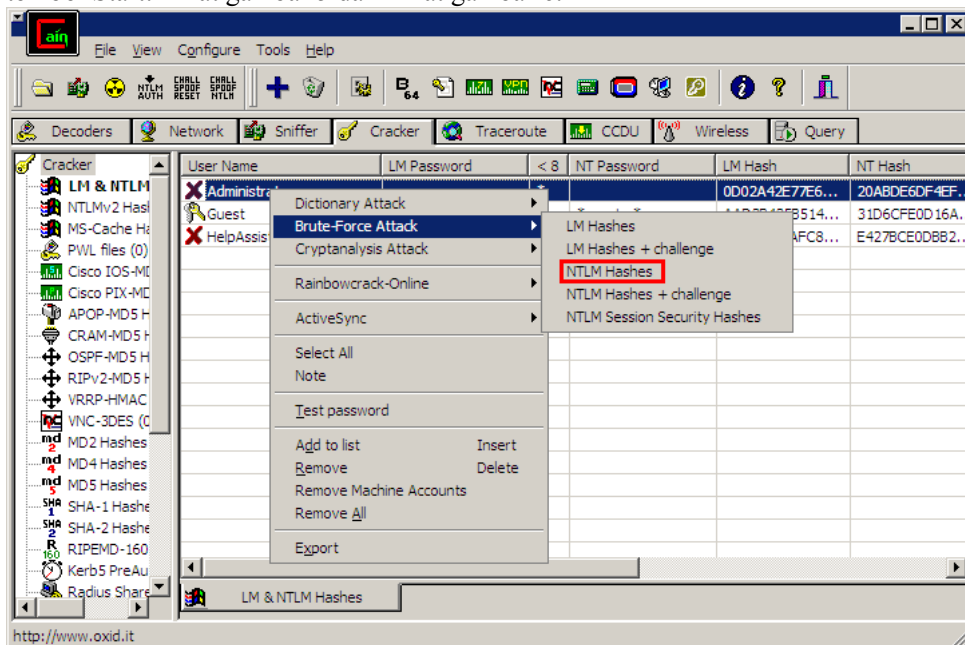
List dari user yang ada pada komputer akan muncul, lengkap dengan nama user, jumlah karakter password, dan apakah user tersebut dilengkapi password atau tidak. Jika sebuah user dilengkapi dengan password, maka pada kolom NT Password, statusnya akan kosong. Jika passwordnya memiliki jumlah di bawah 8 karakter, maka pada kolom NTLM Hashes. Karena tagret yang kita pilih adalah Administrator maka kita akan fokus pada akun Adminstrator. Lihat gambar 4



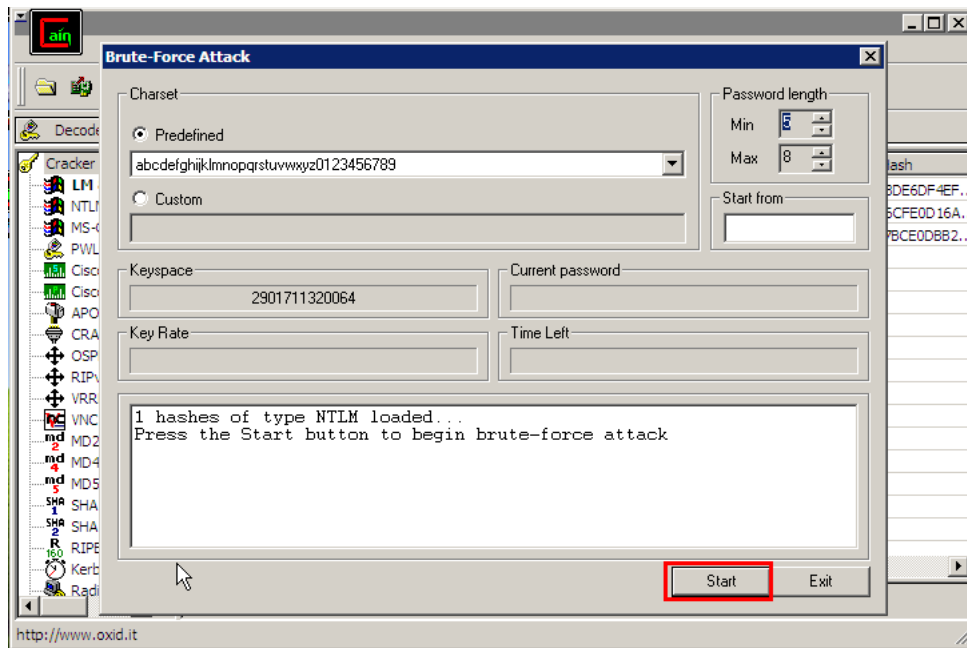
Gambar 4

2. CRACK PASSWORD DENGAN TEKNIK BRUTE FORCE

Klik kanan pada list akun yang akan di cracking. Halaman Brute-Force Attack akan muncul. Di dalamnya, atur Password Length menjadi sesuai dengan yang kamu kehendaki. Karena pada step sebelumnya, kita mengetahui bahwa password yang ada tidak lebih dari 8 karakter, maka pada bagian Max, isilah dengan angka 8. Kolom Charset juga bisa kamu ganti sesuai dengan karakter apa yang kemungkinan digunakan pada password yang ingin kamu hack. Semakin panjang list yang tersedia, maka proses hack brute force akan lebih lama. Jika sudah siap, kamu tinggal menekan tombol Start. Lihat gambar 5 dan Lihat gambar 6.

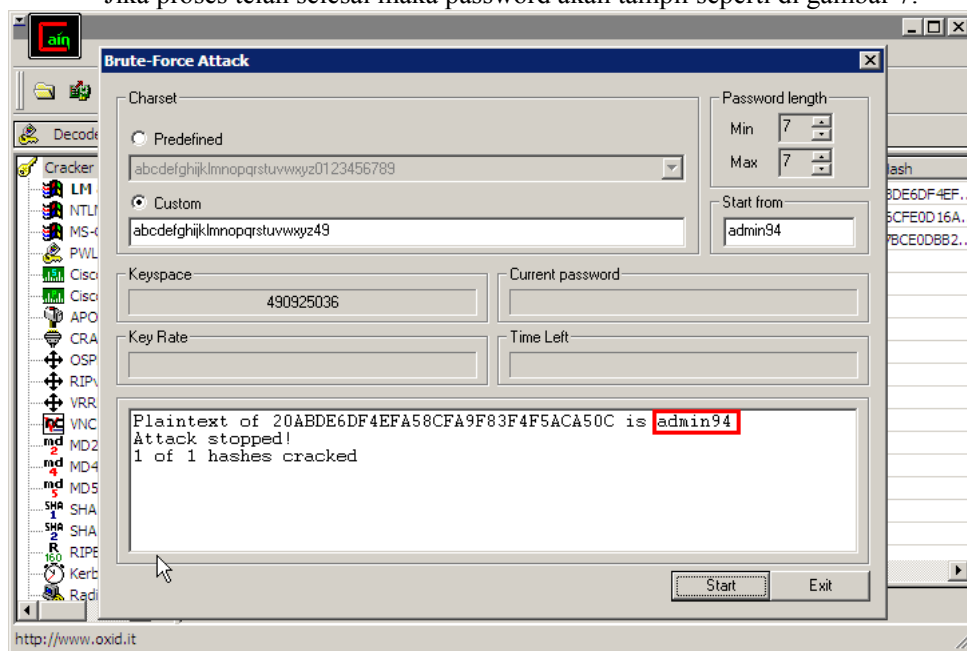


Gambar 5



Gambar 6

Jika proses telah selesai maka password akan tampil seperti di gambar 7.



Gambar 7

IV. ANALISIS

Pada percobaan ini kelemahannya ialah kita harus bisa terlebih dahulu login ke OS windows XP. Setelah masuk baru kita dapat mendapatkan kode hash dari password Administrator dengan bantuan software *cain and able*, jika hast password telah di dapat, maka kita dapat melakukan teknik brute force. Keberhasilannya tergantung dari tipe karakter password itu sendiri. Jika password tersebut sederhana maka akan didapat dengan waktu yang tidak lama. Namun jika karakter password tersebut unik dan jumlah karakter panjang maka waktu yang di butuhkan cukup lama.

Sebenarnya tidak sepenuhnya teknik kriptografi ini akan berhasil. Karena waktu yang dibutuhkan cukup lama bahkan hingga bertahun-tahun.

V. KESIMPULAN

- Semua password dapat di crack jika diketahui kode hash dari password tersebut.
- Brute force password membutuhkan waktu yang lama dalam memecahkan password.
- Semakin unik password yang digunakan maka semakin lama proses brute force.

VI. SARAN

- Sebaiknya password yang digunakan menggunakan kata yang unik, menggunakan angka dan karakter spesial.
- Sebaiknya jumlah karakter password melebihi 8 karakter, hal tersebut bertujuan untuk menyulitkan dalam proses brute force karena akan membutuhkan waktu yang cukup lama.

Referensi

- [1] <http://cybercrime4c.blogspot.co.id/2013/06/apa-yang-dimaksud-cracking.html>
- [2] <http://www.potter.web.id/pengertian-brute-force-attack/>
- [3] <https://jalantikus.com/tips/cara-hack-password-login-windows/>