Analisa Serangan *Password Cracking* Pada Windows 10 Menggunakan Tools *Pwdump v7.1* dan *Cain & Abel*

Muhammad Zikrillah[1]

[1]Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya

Jl. Raya Palembang – Prabumulih Km 32, Kabupaten Ogan Ilir, Sumatera Selatan

[1]Email : 09121001050@students.ilkom.unsri.ac.id

Abstrak

Istilah serangan password cracking atau juga disebut sebagai serangan brute-force merupakan masing-masing proses untuk menebak password. Dalam proses ini perangkat lunak atau tool menciptakan sejumlah besar kombinasi password. Pada dasarnya ini adalah teknik footprinting yang digunakan oleh perangkat lunak untuk memperoleh informasi sandi dari sistem. Pwdump v7.1 merupakan tool untuk mengambil file Security Account Manager (SAM) dari Windows yang kemudian akan dideskripsikan via command prompt. Sedangkan Cain & Abel merupakan tool untuk memecah beberapa kombinasi password yang didapat dari Pwdump. Kombinasi password tersebut selanjutnya akan dicocokan dengan password windows yang kita cracking dengan menggunaka serangan brute-force.

Keywords*: Password cracking, Pwdump, SAM, Cain & Abel, Serangan Brute-force*

BAB I. PENDAHULUAN

1. Latar Belakang

Password merupakan bagian sistem keamanan berbasis sistem operasi Linux, Windows, Ios, dan lain-lain. Password berfungsi untuk mengamankan data yang sangat penting dari suatu data sensitif pada sebuah komputer. Password terdiri dari suatu kalimat atau kata yang tersusun dari huruf, angka, simbol, ataupun kombinasi dari ketiganya. 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 kebayakan 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.

Tools 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.

Password cracking adalah istilah umum yang menggambarkan sekelompok teknik yang digunakan untuk memperoleh password pada sebuah sistem data. Password cracking khusus mengacu pada proses mendapatkan password dari data yang yang dilindungi dengan password. Password cracking menggunakan metode teknik footprinting yang kemudian akan dibuat beberapa kombinasi password dengan metode serangan brute-force.

Serangan Brute-force merupakan metode serangan yang paling rumit dan memakan waktu yang lama tergantung kompleksitas password tersebut terkadang perlu waktu sampai seminggu guna menebak password. Serangan brute-force merupakan metode password cracking yang secara signifikan lebih kuat daripada serangan metode kamus. Sebuah program brute force attack akan mencoba setiap kombinasi karakter yang mungkin mencapai set pada password yang tepat. Ini sangat memakan waktu karena ada huruf yang mungkin tak terhitung jumlahnya, nomor yang banyak dan kombinasi simbol dari seorang individu yang bisa digunakan untuk password.

Tools yang akan digunakan adalah pwdump versi 7.1 dan Cain & Abel. Tool pwdump berfungsi untuk memecah password yang ada di windows menjadi beberapa kombinasi password. Sedangkan Cain & Abel berfungsi mencocokan beberapa kombinasi password dari pwdump dengan password windows. Berdasarkan uraian diatas maka penulis mengambil judul "Analisa Serangan Password Cracking Pada Windows 10 menggunakan Tools Pwdump v7.1 dan Cain & Abel".

2. Tujuan

Adapun tujuan yang akan dicapai dari analisa ini adalah:

1. Mengimplementasikan tool Pwdump v7.1 pada sistem operasi windows 10.
2. Mengakses password sistem operasi windows 10 menggunakan tool Cain & Abel.

BAB II. LANDASAN TEORI

2.1 Password Cracking

Password cracking adalah istilah umum yang menggambarkan sekelompok teknik yang digunakan untuk memperoleh password pada sebuah sistem data. Password cracking khusus mengacu pada proses mendapatkan password dari data yang yang dilindungi dengan password; namun harus dicatat bahwa cara-cara menipu seseorang agar memberi password, seperti melalui phishing, tidak dianggap sebagai password cracking. Menebak password berdasarkan pengetahuan yang sudah ada sebelumnya dari pemilik sistem komputer dianggap cracking, karena password tidak dikenal sebelumnya.

Seorang hacker diartikan sebagai seseorang yang memiliki ketertarikan yang mendalam terhadap teknologi komputer; bukan didefinisikan sebagai seseorang yang ingin melakukan kerusakan. Sedangkan istilah "Penyerang" biasanya digunakan untuk menggambarkan seorang "hacker" perusak. Istilah lain dari Penyerang adalah "black hat". Para analis keamanan seringkali disebut sebagai "white hat" dan analisa white-hat merupakan hacking dengan tujuan pertahanan. Cara termudah password cracking adalah menemukan secarik kertas yang bertuliskan password yang diletakkan pada monitor atau disembunyikan dibawah keyboard. Teknik umum lainnya adalah "dumpster diving", yaitu seorang Penyerang yang mengais keranjang sampah untuk menemukan sampah dokumen yang mungkin berisikan password.

2.2 Serangan 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.

2.3 Security Account Manager (SAM)

SAM atau *Security Account Manager* adalah sebuah basis data dalam system operasi berbasis Windows NT yang menyimpan informasi mengenai semua akun pengguna *(user account)* dan kelompok pengguna *(user group).* Selain dimiliki oleh system windows NT secara individual , basis data ini juga dimiliki oleh *domain controller* dalam sebuah domain berbasis windows NT. basis data ini juga sering disebut sebagai Domain directory database atau Directory Database. SAM inilah yang sering di jadikan bahan oleh para hacker untuk dijadikan korban atau sasaran , tujuannya tentu saja mengambil informasi berupa password yang ada dalam sebuah sistem operasi terkhusus Windows.

2.4 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.

2.5 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.

BAB III. METODOLOGI PENELITIAN

Penelitian ini menggunakan sebuah PortAbel Computer (PC) yang terhubung ke internet . PC digunakan untuk subjek penelitian sedangkan internet digunakan untuk mencari informasi mengenai penjelasan dari masing-masing landasan teori. PC kali ini menggunakan sistem operasi windows 10 yang sudah diamankan menggunakan password user “emzikrillah”.

3.1 Pengumpulan Data

Pengumpulan data menggunakan teknik observasi yang artinya mengamati secara langsung penelitian, kemudian mencatat hasil dari penelitian tersebut, dan terakhir menganalisa hasil penelitian tersebut. Langkah pertama yang dilakukan yaitu mencari toos yang digunakan untuk mengakses password. Tools didapat dari mengunduh ataupun meminta dari orang yang mempunyai tools tersebut. Dalam hal ini penulis meminta dari teman yang memiliki tools tersebut.

Adapun tools yang digunakan adalah:

1. Pwdump v7.1
2. Cain & Abel

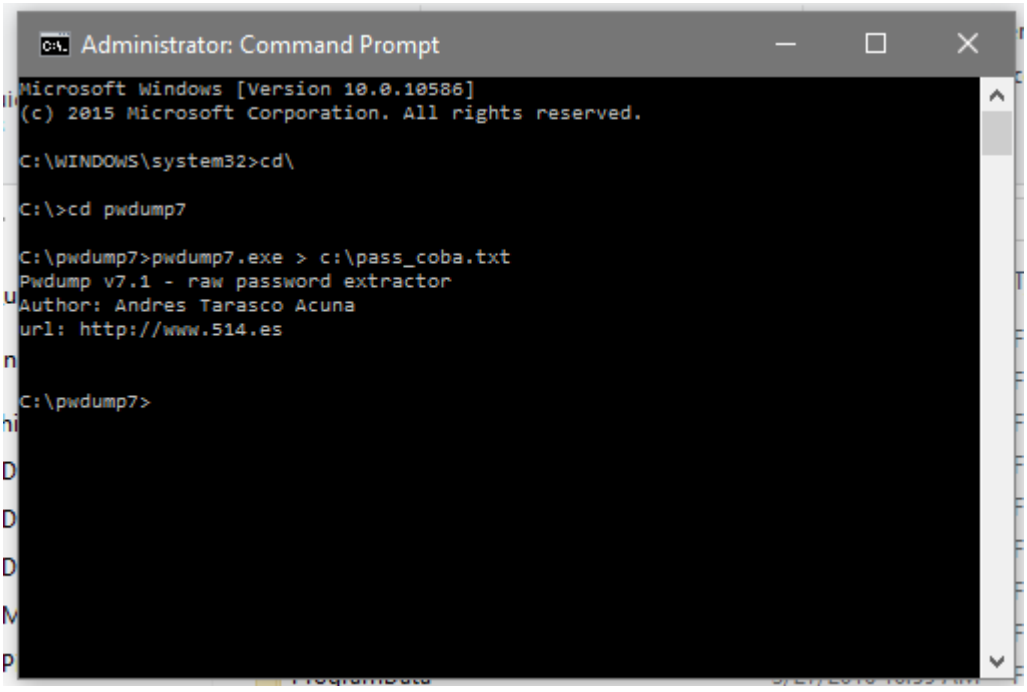
Selanjutnya instalasi Pwdump dan Cain & Abel. Pwdump yang digunakan penulis adalah Pwdump versi 7.1. Pwdump tidak perlu diinstal tetapi hanya dipindahkan ke LocalDisk C. Sedangkan untuk Cain & Abel harus diinstl terlebih dahulu. Kemudian jalankan command prompt via run as administrator. Didalam command prompt masukkan file pwdump7 di direktori c dan membuat file .txt password yang sudah di akses oleh pwdump.

Langkah terakhir jalankan Cain & Abel via run as administrator. Didalam menu Cain & Abel masukkan password .txt tersebut kemudian jalankan dan serang user password (emzikrillah) dengan serangan brute-force. Dari bruce-force attack tersebut dapat dilihat hasil dari password yang di cracking.

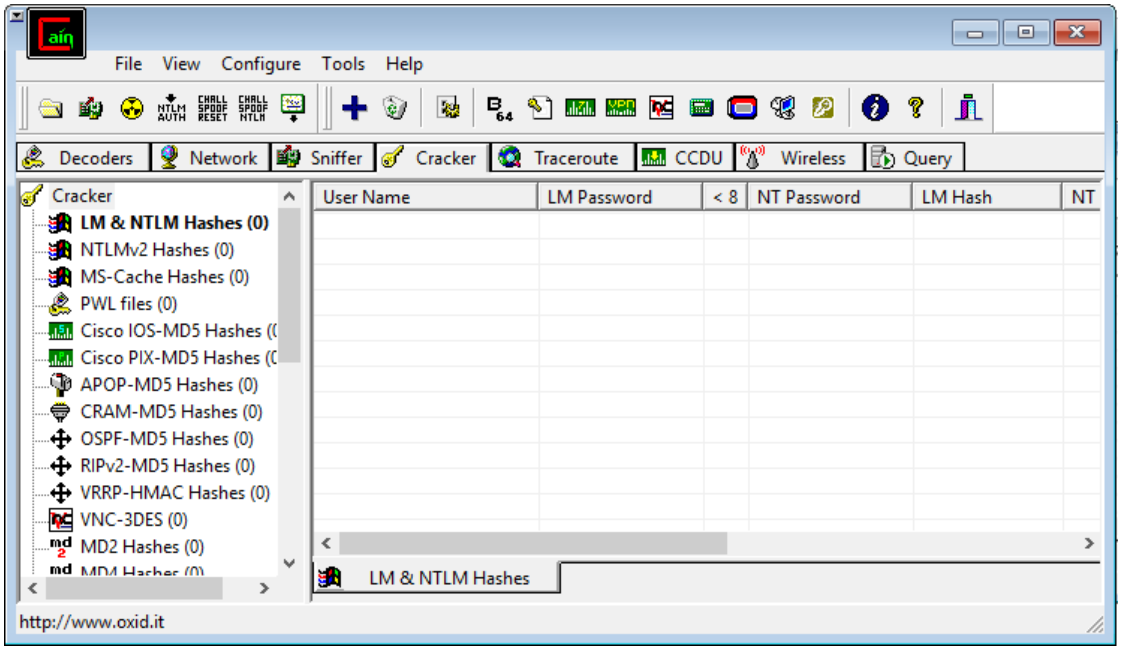
BAB IV. HASIL DAN ANALISA

Password cracking adalah istilah umum yang menggambarkan sekelompok teknik yang digunakan untuk memperoleh password pada sebuah sistem data. Password cracking khusus mengacu pada proses mendapatkan password dari data yang yang dilindungi dengan password; namun harus dicatat bahwa cara-cara menipu seseorang agar memberi password, seperti melalui phishing, tidak dianggap sebagai password cracking. Menebak password berdasarkan pengetahuan yang sudah ada sebelumnya dari pemilik sistem komputer dianggap cracking, karena password tidak dikenal sebelumnya.

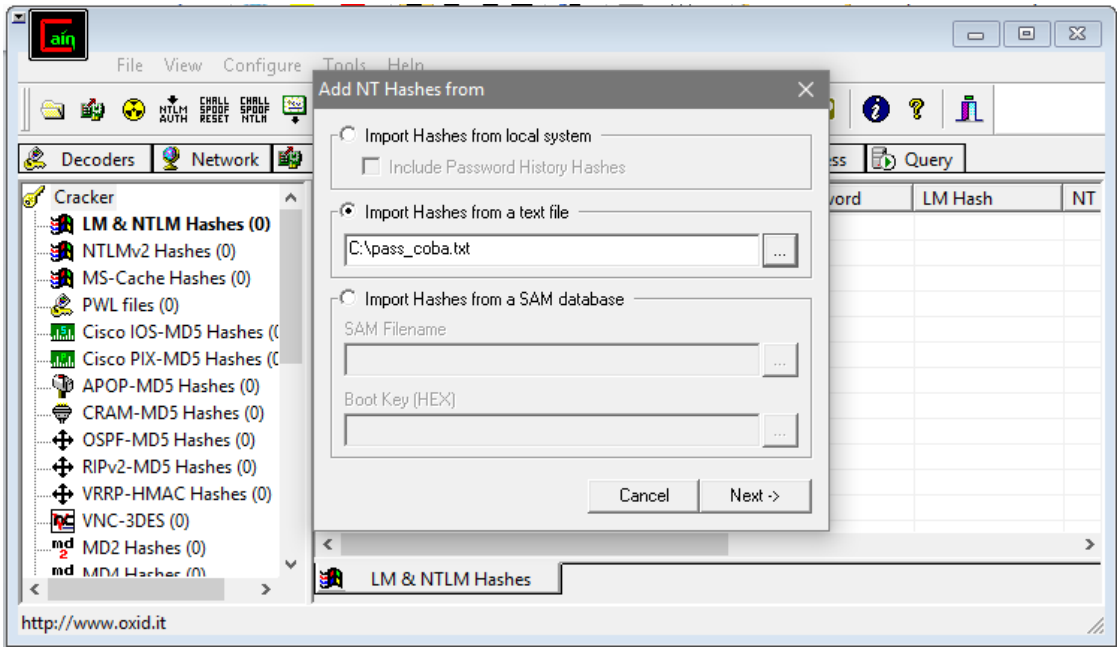
Langkah pertama dengan membuka command prompt via run as administrator, setelah itu memanggil pwdump yang kali ini menggunakan versi 7.1. Perintahkan pwdump menjalankan aplikasi .exe nya agar hash password pada komputer bisa didapatkan. Kemudian hash password tersebut ubah menjadi pass_coba.txt seperti gambar dibawah ini.



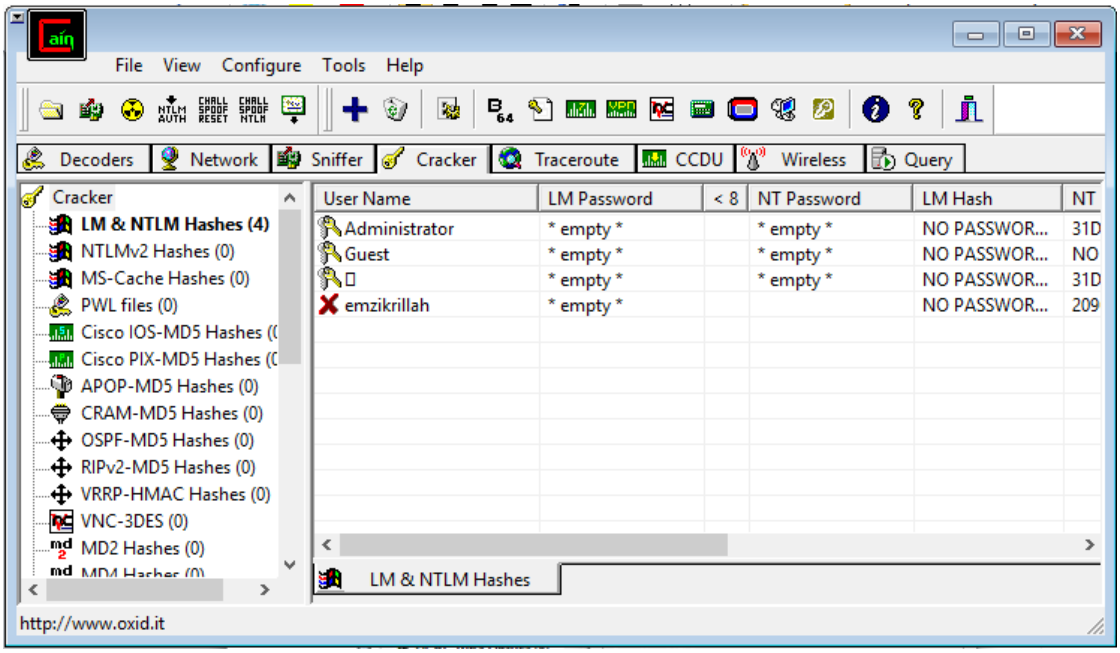
Langkah kedua jalankan Cain & Abel via run as administrator. Kemudian dibagian menu pilih “cracker” dan pada menu cracker pilih “LM & NTLM Hashes (0)” seperti gambar dibawah ini.



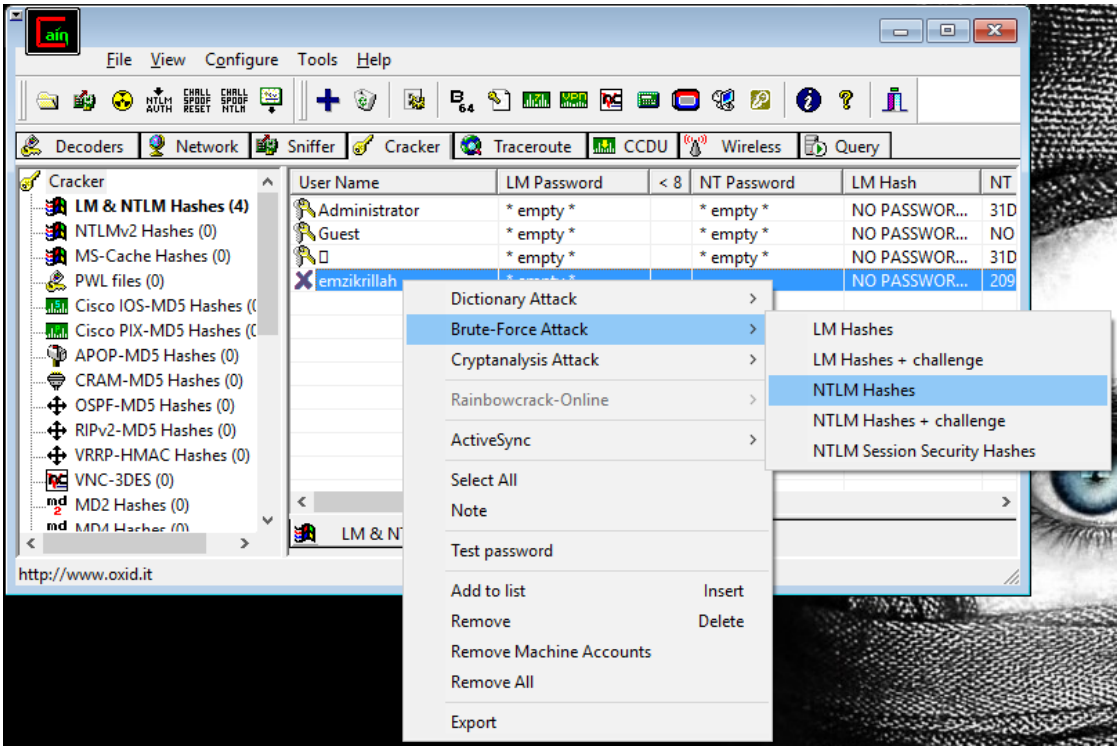
Langkah ketiga pilih “add to list” dan masukkan pass_coba.txt tadi ke bagian “import hashes from a text file”.



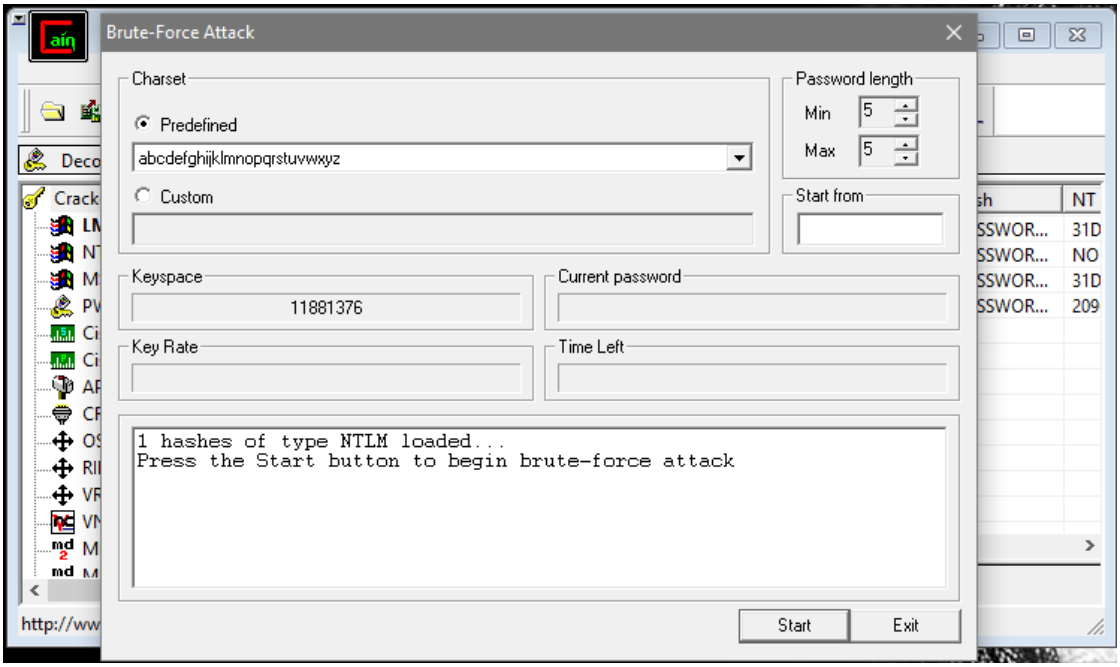
Setelah itu tekan “next” dan akan mendapatkan hasil seperti gambar dibawah ini.



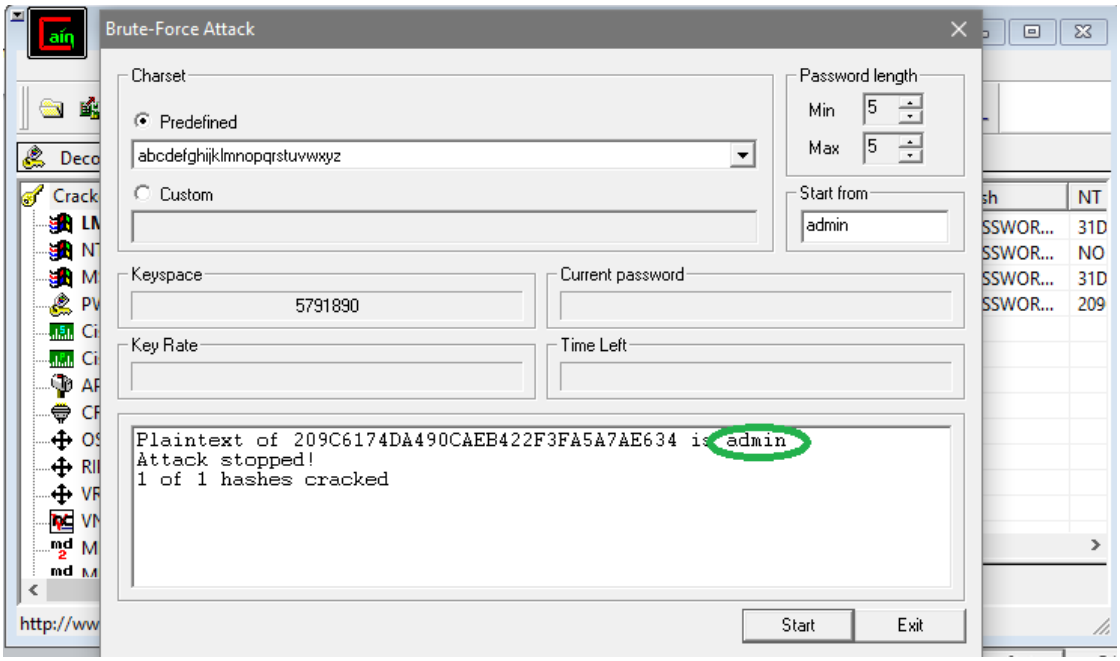
Langkah keempat pada user “emzikrillah” klik kanan mouse lalu pilih “Bruce-Force Attack dan pilih “NTLM Hashes”



Selanjutnya akan muncul menu seperti gambar dibawah ini.



Langkah kelima pada bagian “charset” pilih “predefined” dan masukkan pola karakter yang digunakan hash password. Penulis memilih karakter abjad kecil supaya memudahkan serangan brute-force, password length juga kita minimalkan menjadi seperti gambar diatas agar estimasi waktu yang terpakai tidak terlalu lama. Setelah itu klik start kemudian tunggu hingga password komputer didapatkan seperti gambar dibawah ini.



BAB 5. PENUTUP

5.1 Kesimpulan

Inti dari keamanan komputer adalah melindungi komputer dan jaringannya dengan tujuan mengamankan informasi penting yang berada di dalamnya. Password digunakan untuk memproteksi hal-hal yang sifatnya privasi. Beberapa orang sudah membuat *password* dengan menggabungkan beberapa jenis karakter sehingga sulit untuk ditebak. Ini membuktikan bahwa mereka tidak ingin informasi yang tersimpan didalamnya di-*hack* oleh pihak lain. Adapun cara membobol sistem seperti mencuri password bisa dilakukan dengan berbagai cara, salah satunya adalah dengan melakukan serangan brute-force terhadap password yang ada pada komputer tersebut. Serangan ini dilakukan untuk mengingatkan kepada pengguna yang memiliki data-data penting agar tidak lalai dalam meninggalkan pc nya dalam keadaan hidup. Namun, serangan brute-force ini tidak cocok digunakan untuk password yang memiliki karakter kombinasi karena akan memakan waktu yang lama.

5.2 Saran

1. Untuk pengguna sebaiknya membuat password dengan kombinasi angka, huruf, ataupun simbol agar tidak mudah dibobol oleh orang yang tidak berkepentingan.

2. Untuk peneliti yang ingin mencoba membobol password sebaiknya menggunakan tools yang benar-benar lengkap dalam hal footprinting, scanning, maupun cracking.

DAFTAR PUSTAKA

[1] 2016. Top 10 alat password cracking.

http://id.wondershare.com/password/password-cracker-tools.html

[2] 2016. Kata Sandi.

https://id.wikipedia.org/wiki/Kata_sandi

[3] Pramusinta87. 2011. Pengertian password cracking.

http://pramusinta87.blogspot.co.id/2011/04/pengertian-password-cracking.html

[4] 2016. Pengertian Brute-force Attack.

http://www.potter.web.id/pengertian-brute-force-attack/