

Cracking Password Windows 8 Menggunakan Cain & Abel

Orlando Dacosta

Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya

09121001029@students.ilkom.unsri.ac.id

1. Pendahuluan

Password cracking adalah istilah umum yang menggambarkan sekelompok teknik yang digunakan untuk memperoleh password pada sebuah sistem data. Sebagian besar metode mendapatkan password, dilakukan dengan menetik berulang kali untuk menebak atau mengeksploitasi kelemahan keamanan dalam sistem komputer. Ada beberapa metode yang berbeda menebak password seseorang. Satu diantaranya misalnya menggunakan data seputar pribadi dari orang yang sistem komputernya akan dicrack untuk memprediksi kemungkinan. Mengetahui nama-nama orang yang dicintai atau binatang peliharaan, tanggal lahir, nomor telepon, tempat tinggal, biasanya digunakan untuk menebak password.

Cara lain untuk mendapatkan password berbasis cracking dikenal sebagai Brute Force Attack. 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.

Ada banyak tools yang digunakan untuk cracking password contohnya yang digunakan pada tugas ini adalah Cain & Abel. Cain & Abel sendiri adalah sebuah software yang dapat digunakan untuk melakukan hacking via LAN (snifing). Pada tugas ini saya mencoba cracking password pada windows 8.1 dengan bantuan software Cain & Abel dan PwDump7.

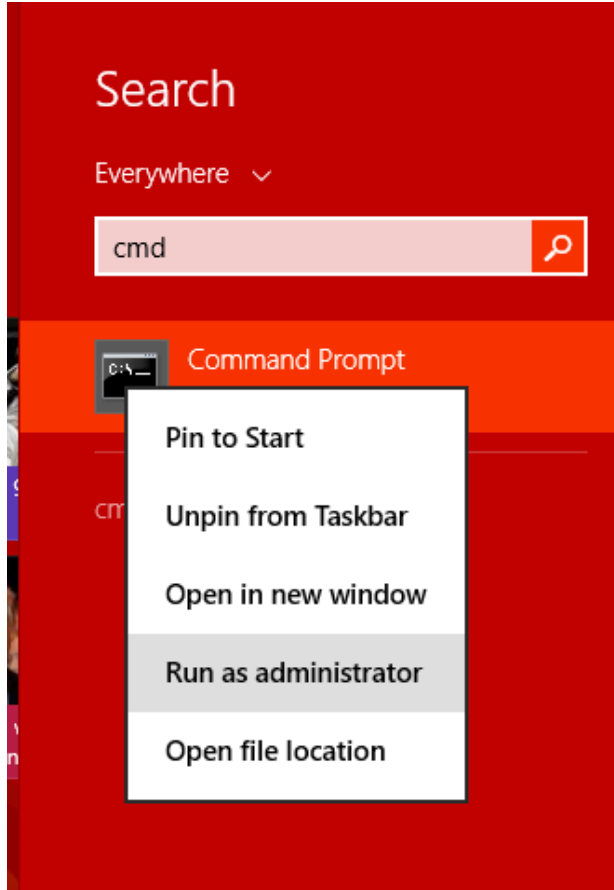
2. Tujuan dan Manfaat

- Mengetahui cara cracking password menggunakan Cain & Abel
- Mengetahui bagaimana teknik brute force attack

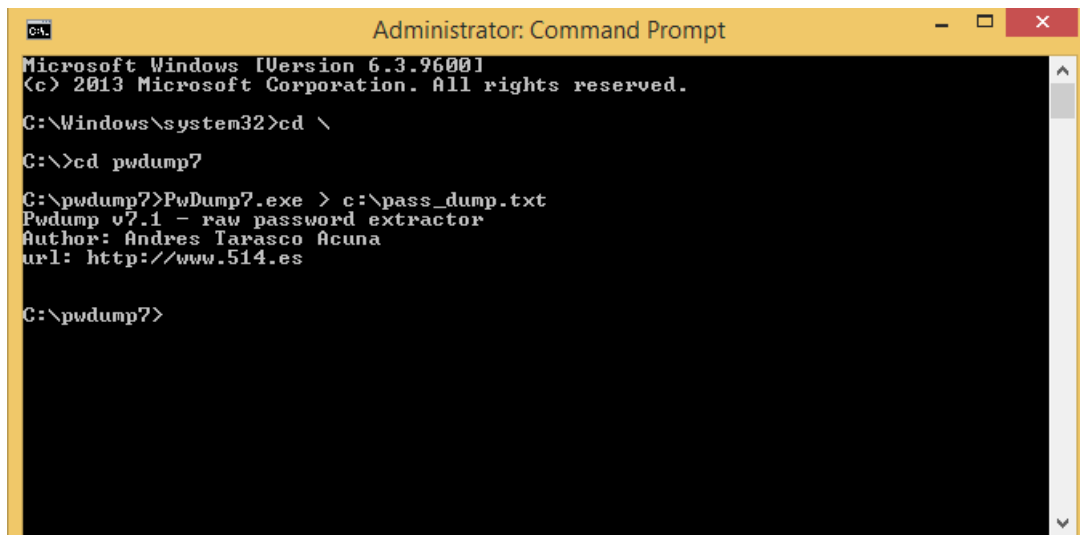
3. Perumusan Masalah

1. Bagaimana membuat password dump untuk bruteforce attack?
2. Bagaimana menggunakan software hacking Cain & Abel untuk cracking password?

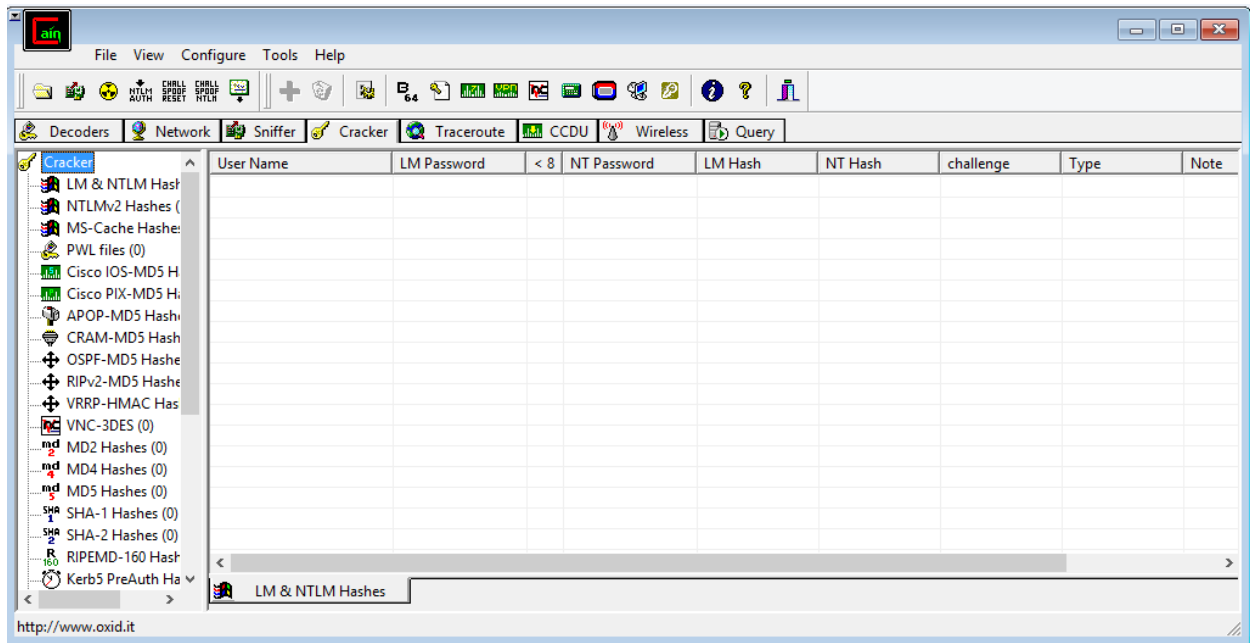
4. Hasil dan Pembahasan



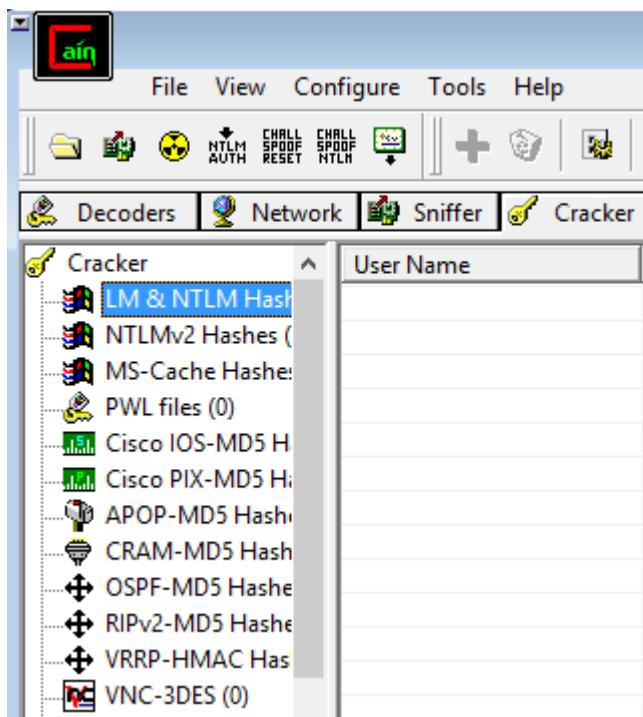
Gambar 1 adalah Buka CMD (Command Prompt) dengan Run as administrator



Gambar 2 adalah Masuk ke folder pwdump7 dan jalankan aplikasinya untuk mendapatkan pass_dump.txt.

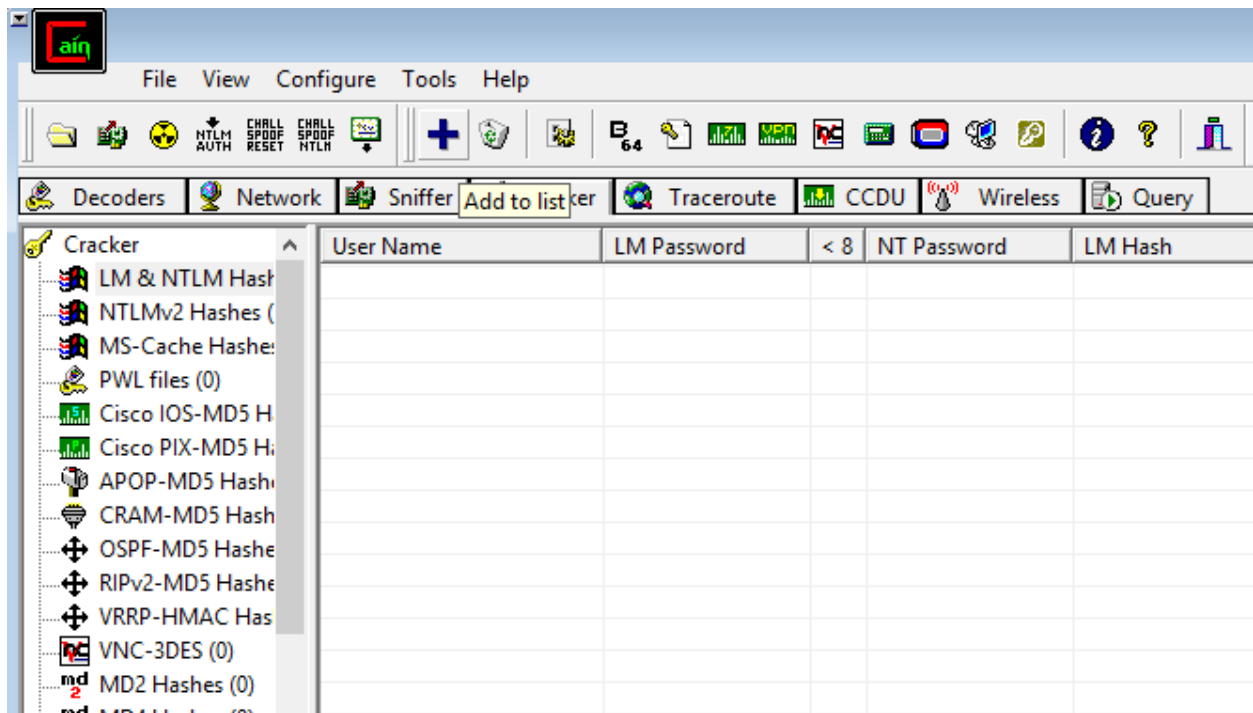


Gambar 3 adalah Buka tools Cain & Abel lalu pilih Cracker

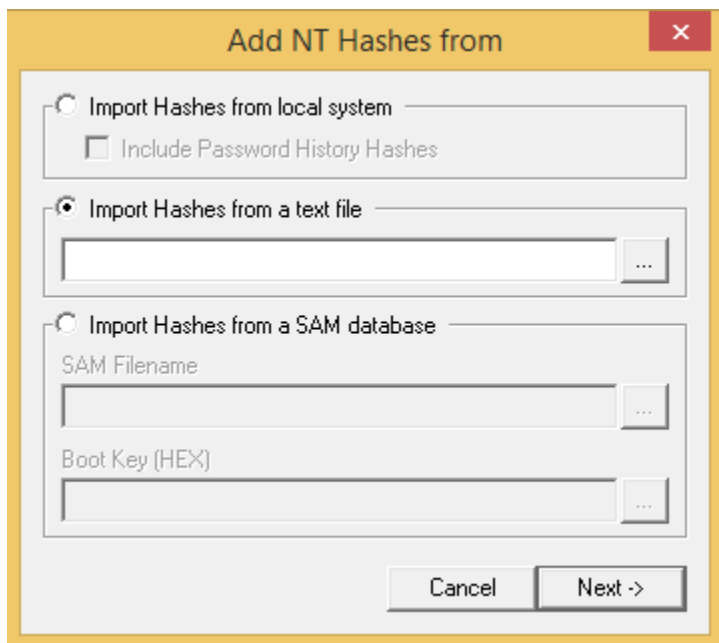


Gambar 4 adalah Pada bagian cracker pilih LM & NTLM Hashes

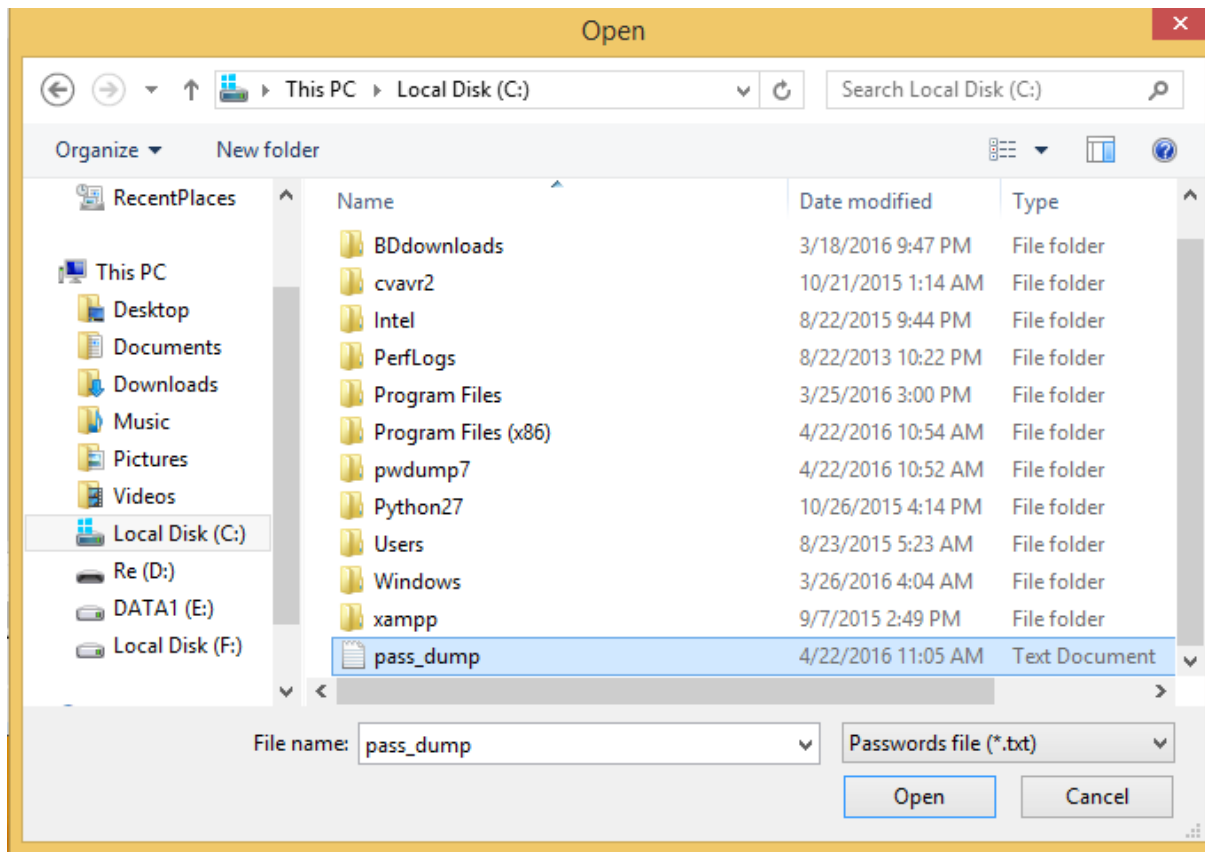
Untuk membaca hashes pada pass_dumb.txt digunakan LM & NTLM Hashes



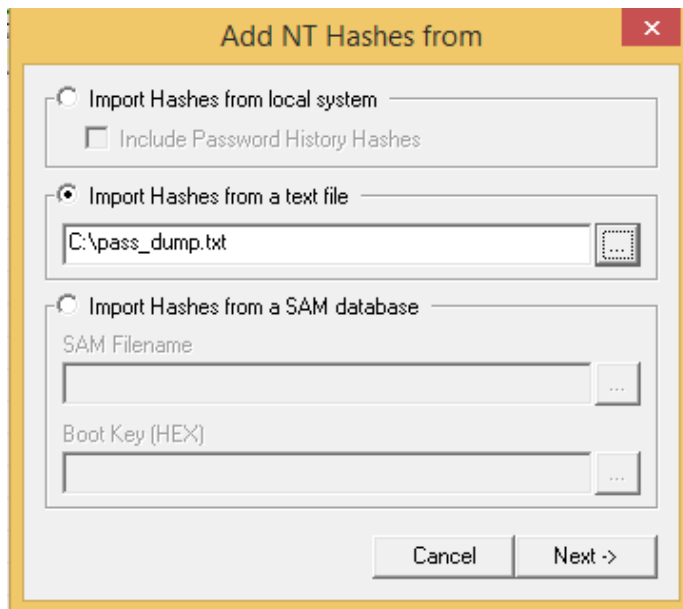
Gambar 5 adalah Pilih Add to list untuk memasukan file pass_dump.txt



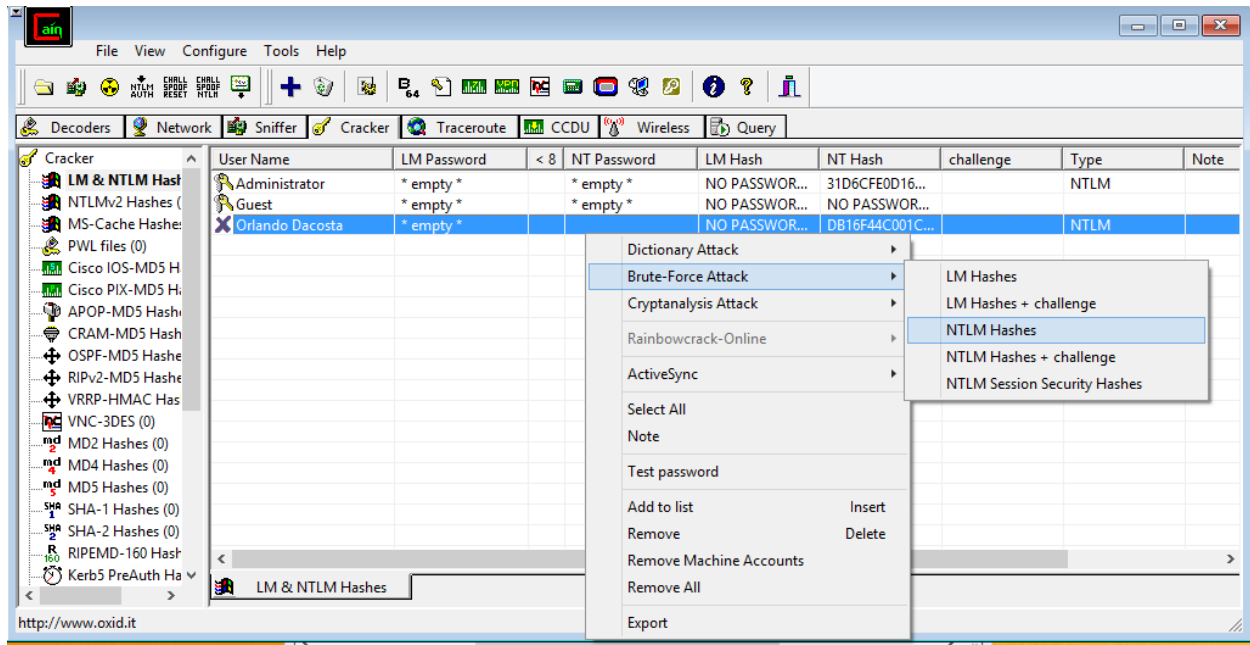
Gambar 6 adalah Setelah di pilih Add to list makan muncul box Add NT Hashes from, lalu pilih Import Hashes from a text file



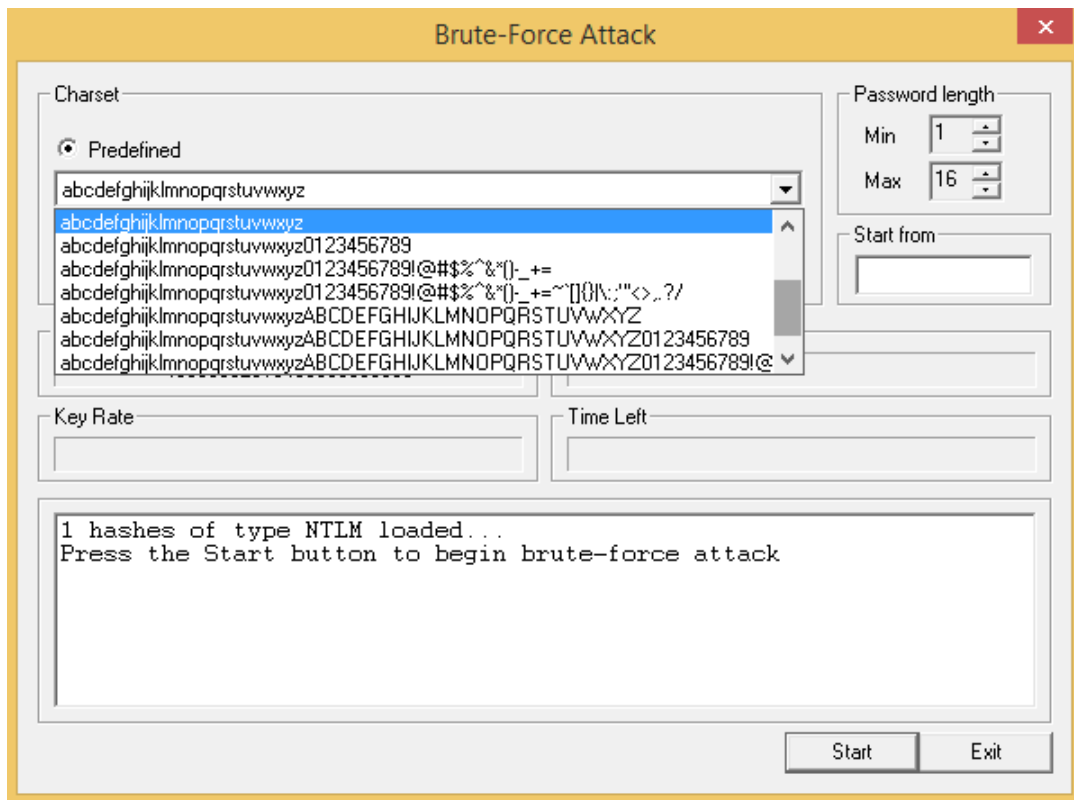
Gambar 7 adalah Untuk memasukkan hashes password pilih file pass_dump.txt yang telah dibuat menggunakan Pwdump7 yang ada pada gambar 2 sebelumnya.



Gambar 8 adalah Setelah pass_dumb.txt di import klik next untuk langkah selanjutnya

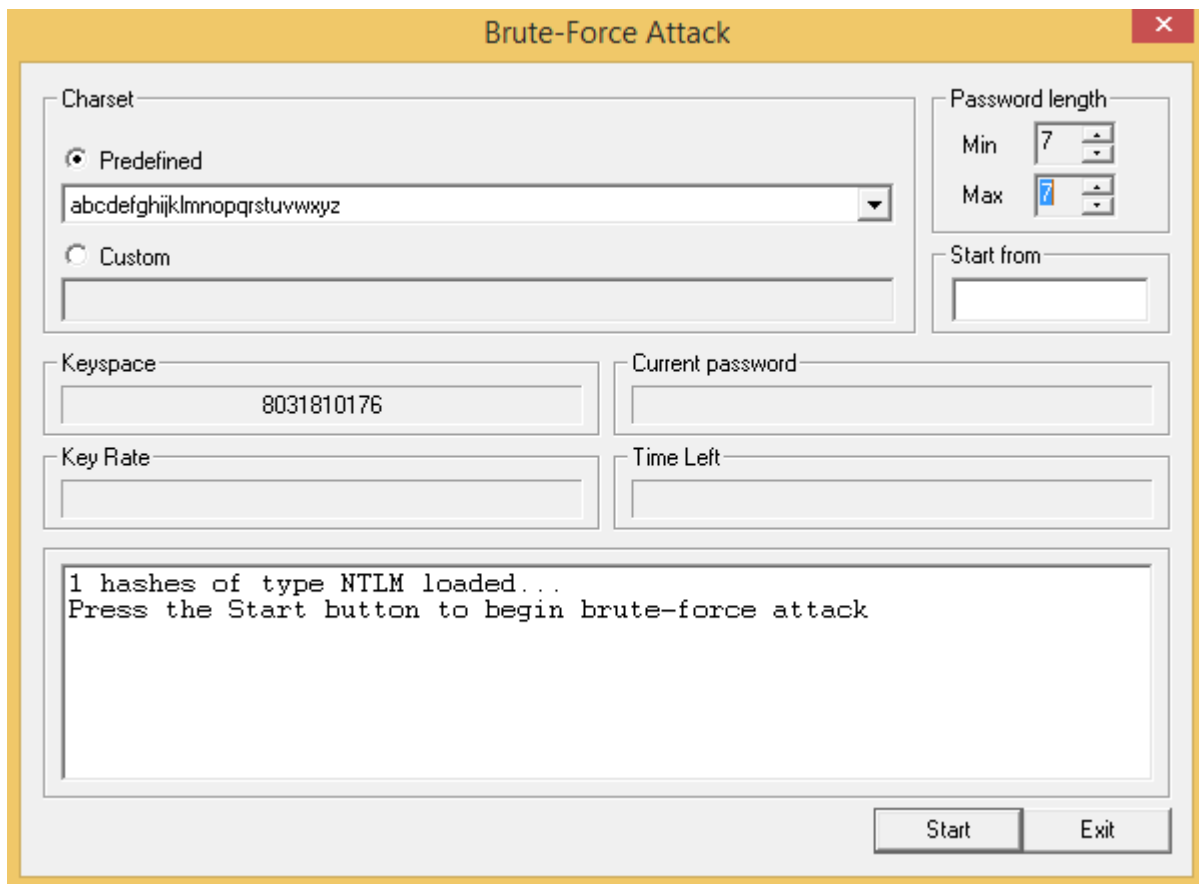


Gambar 9 adalah Pada gambar ini NT hash ditampilkan lalu klik kanan pada akun target. Pada kasus ini akun target adalah Orlando Dacosta kemudian pilih Brute-Force Attack > NTLM Hashes

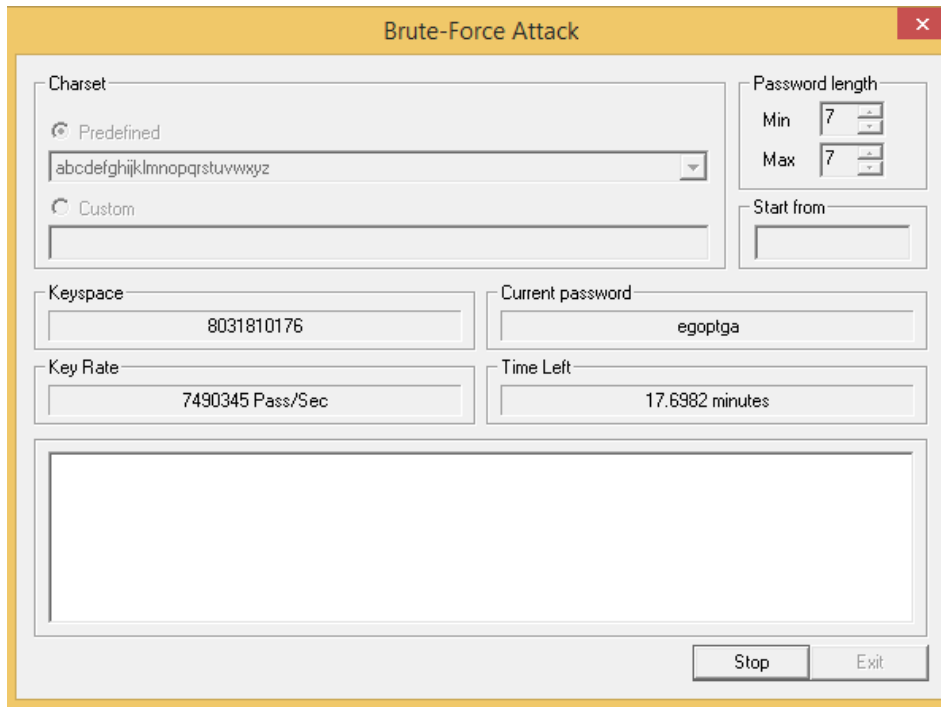


Gambar 10 adalah Box Brute-Force Attack.

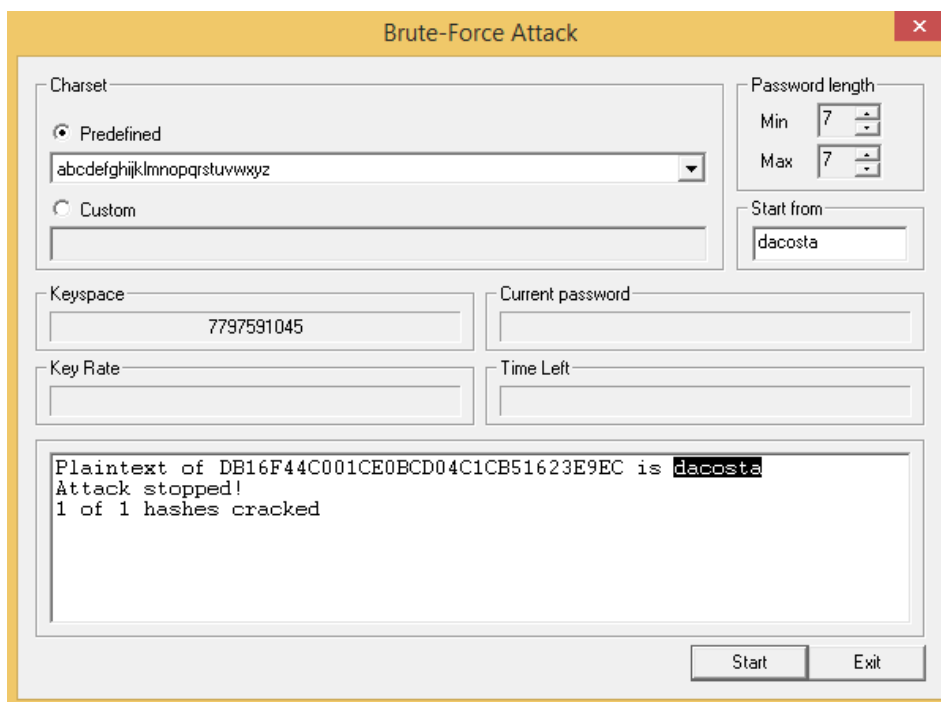
Setelah masuk pada box Brute Force Attack, tentukan kombinasi password target yang akan kita hack pada predefined. Disini saya hanya menggunakan alphabet A-Z tanpa menggunakan kombinasi angka/numeric.



Gambar 11 adalah Gambar ini menentukan perkiraan panjang dan minimal password target yang akan kita hack dimana di sini panjang password adalah 7 dan minimal ny adalah 7. Semakin panjang/banyak maka semakin lama waktu yang dibutuhkan untuk mendapatkan password target yang ingin kita hack. Untuk memulai brute-force attack klik start.



Gambar 12 adalah Ketika brute-force attack telah dijalankan maka akan ditampilkan keySPACE, keyrate, current password dan Time left. Time left yang di tampilkan pada gambar yaitu selama ±17menit, karena panjang password yang saya gunakan cuma 7 jadi waktu yang diperlukan tidak terlalu lama.



Gambar 13 Adalah Ketika serangan berhenti maka didapatkan 1 hashes cracked dan password telah berhasil ditemukan dari hasil plaintext DB16F44C001CE0BCD04C1CB1623E9EC adalah **dacosta**.

5. Kesimpulan:

Pada kasus ini saya membuat contoh password yang rentan/mudah terkena serangan jadi dalam membuat suatu password, hendaknya kita harus memilih kriteria password yang kuat dan tidak mudah di crack oleh seorang craker. Usahakan kita membuat password itu kita bisa menambahkan karakter baik angka, huruf besar atau kecil dan password tersebut mudah di ingat. “jangan menggunakan password yang ada dalam kamus atau password default contoh admin, administrator, password dll. Karena ini akan sangat mudah di bajak/crack.