Password Cracking Windows XP

D
I
S
U
S
U
N

OLEH :
Ahmad Fitri Rashad
09121001023

SISTEM KOMPUTER

FAKULTAS KOMPUTER

UNIVERSITAS SRIWIJAYA

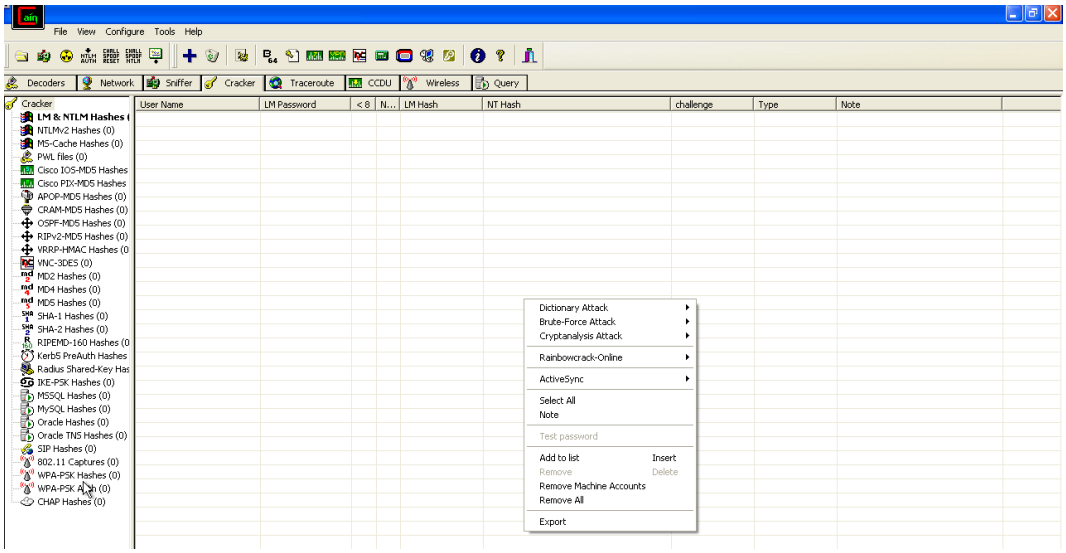
INDRALAYA

TAHUN AJARAN 2015 / 2016

Pada tugas *password cracking* ini, saya menggunakan:

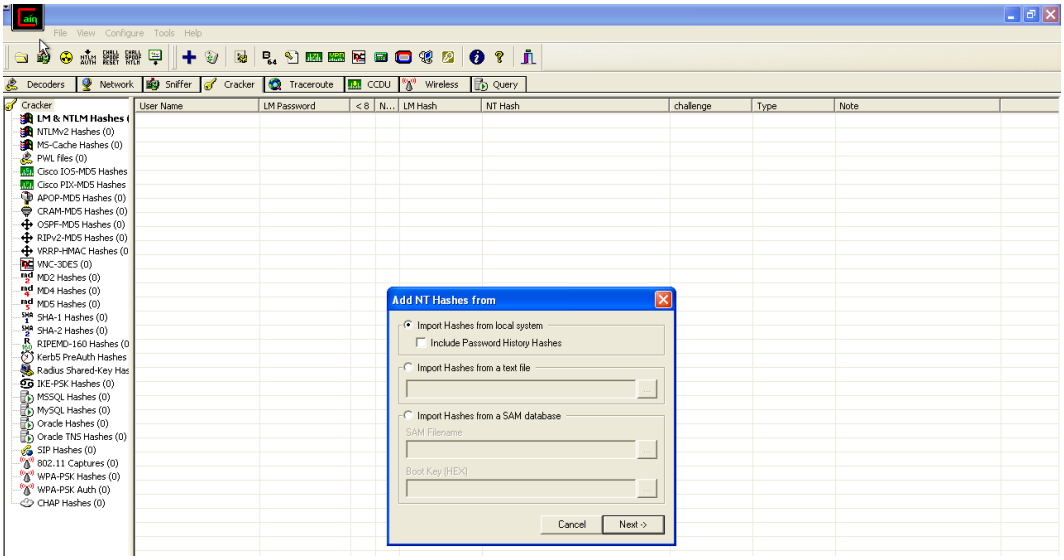
- Windows XP Service Pack 3 (yang di-*install* di Oracle Virtual Machine)
- Kali Linux 2.0
- Cain & Abel
- Hashcat

Pertama – tama, kita *install* software Cain and Abel di Windows XP (yang bisa dapat diunduh di http://www.oxid.it/cain.html). Kemudian kita jalankan aplikasi Cain and Abel tersebut. Setelah dibuka, pada *tab* bagian *Cracker*, klik kanan pada tabel yang kosong, kemudian pilih Add To List.



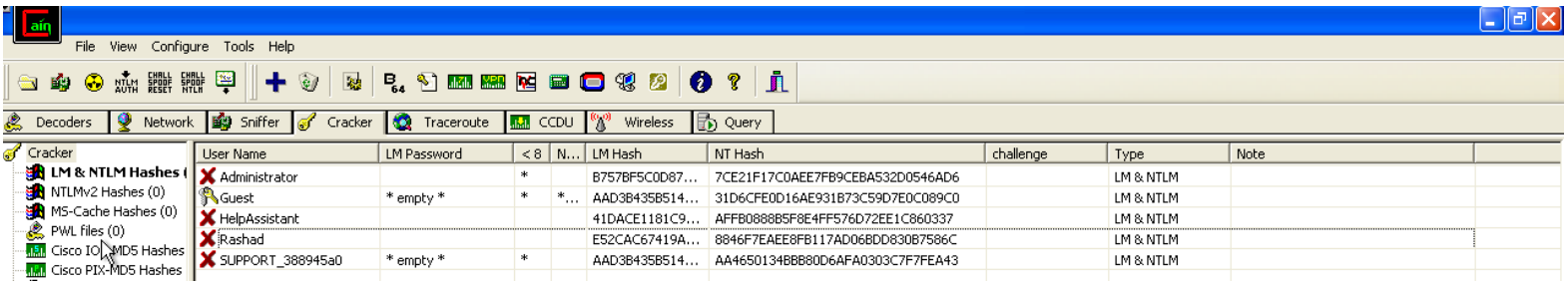
Gambar 1.

Kemudian, kita pilih Next dengan pilihan pada gambar di bawah ini.



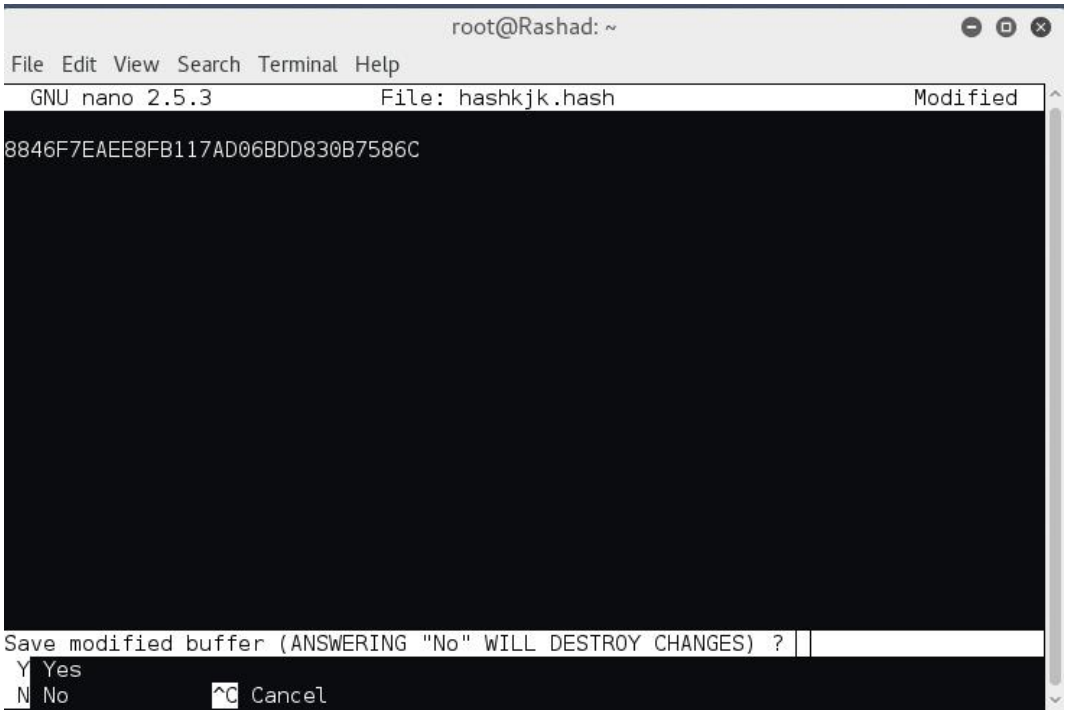
Gambar 2.

Lalu, hasil hash akan muncul. Kita akan gunakan hash tipe NT Hash. Karena NT Hash merupakan tipe hash yang sangat lemah dan mudah untuk di *exploit*, jika dibandingkan dengan hash *password* Linux. Untuk kali ini, saya akan mau mengeksploit username Rashad. (Karena OS Windows kali ini saya instalasikan di dalam Virtual Machine, maka hash tersebut kita catat manual dalam Leafpad atau GNU Nano pada Kali Linux).

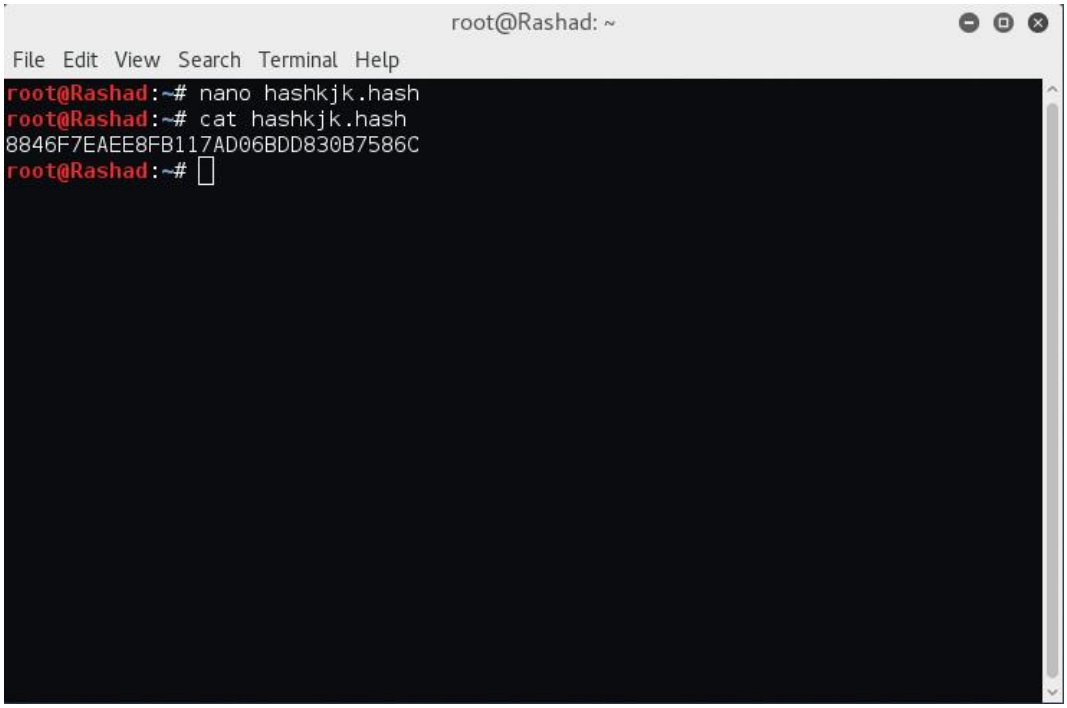


Gambar 3.

Pada OS Kali Linux 2.0, buka Terminal dan ketik “nano hashkjk.hash” (tanpa tanda kutip). Lalu kita ketik hasil hash kita tadi, kemudian untuk menyimpan hash tersebut, tekan CTRL + X, Y, dan enter. Setelah disimpan, kita bisa melihat isi hash kita dengan mengetik “cat hashkjk.hash” (tanpa tanda kutip) pada Terminal.



Gambar 4.



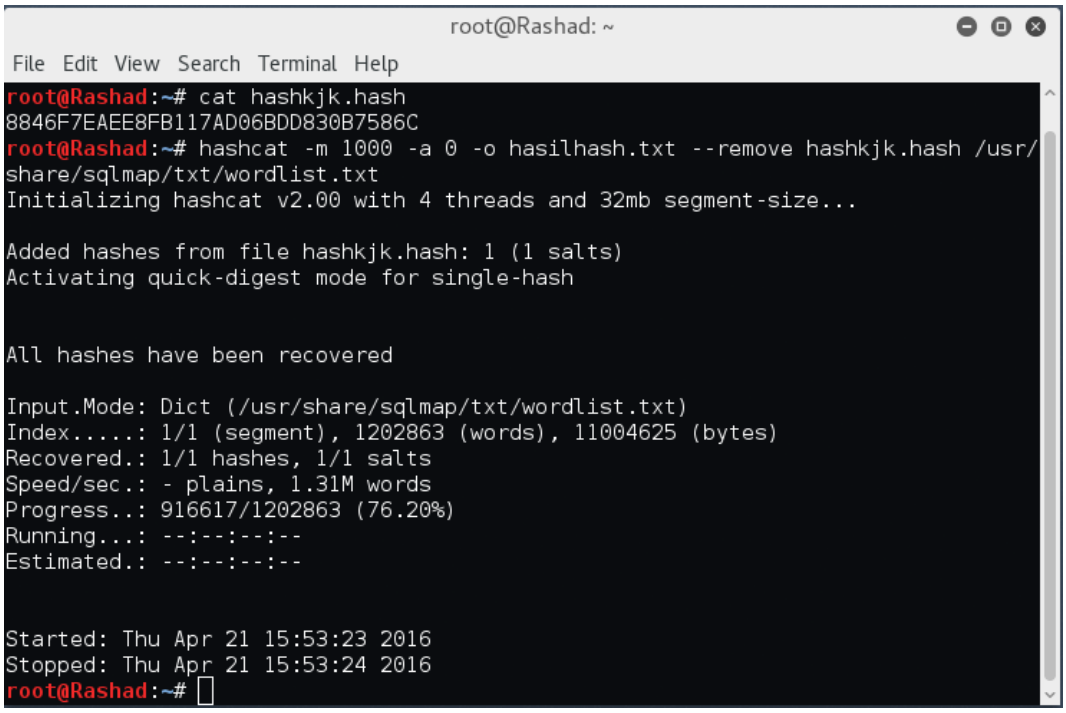
Gambar 5.

Selanjutnya, kita akan mencoba *brute force* menggunakan *dictionary* default dari Kali Linux 2.0 tersebut. Lokasi *dictionary* tersebut berada di /usr/share/sqlmap/txt/wordlist.txt. Cara *brute force* password Windows XP tersebut adalah dengan cara mengetik di terminal: "hashcat -m 1000 -a 0 -o hasilhash.txt –remove hashkjk.hash /usr/share/sqlmap/txt/wordlist.txt" (tanpa tanda kutip).

Catatan:

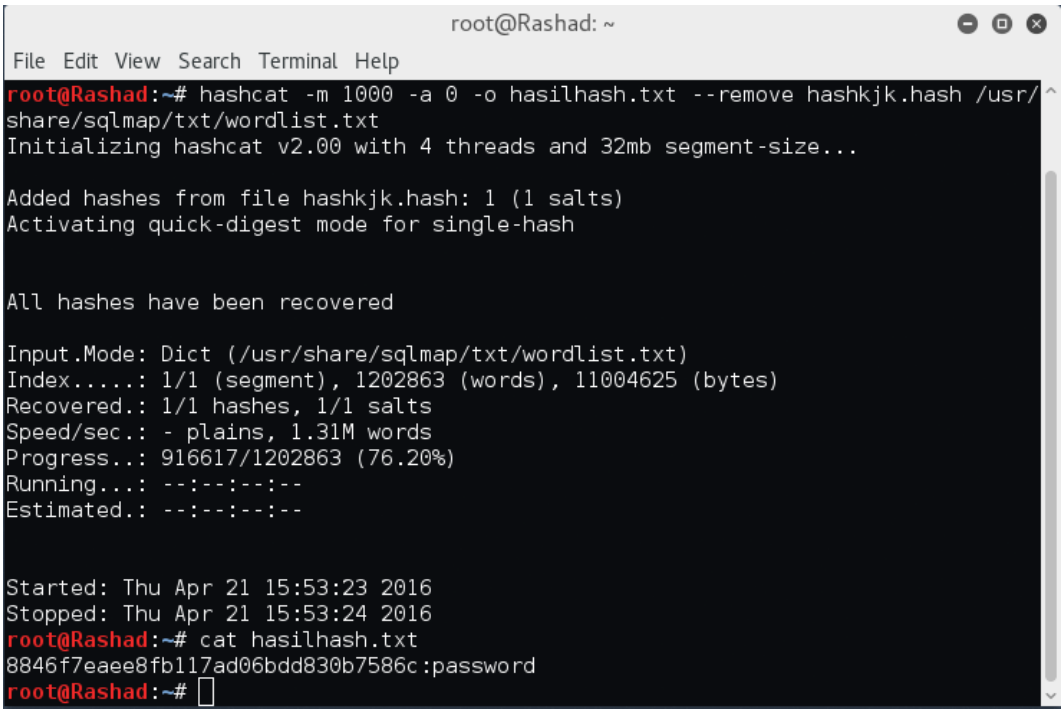
- Perintah -m 1000 merupakan tipe Windows NT hash, karena tipe hash yang kita dapatkan dari software Cain and Abel sebelumnya adalah NT hash
- Perintah -a 0 merupakan *dictionary attack*
- hasilhash.txt merupakan hasil output
- Perintah --remove merupakan hash tersebut akan dihapus jika hashnya ditemukan
- hashkjk.hash merupakan hail input
- Menggunakan *dictionary* default dari Kali Linux 2.0 yang berlokasi di /usr/share/sqlmap/txt/wordlist.txt

Lalu, hasil hash tersebut akan diproses oleh tool hashcat tersebut. Setelah mendapatkan hasil hash, maka akan tampil sesuai dengan gambar di bawah ini.



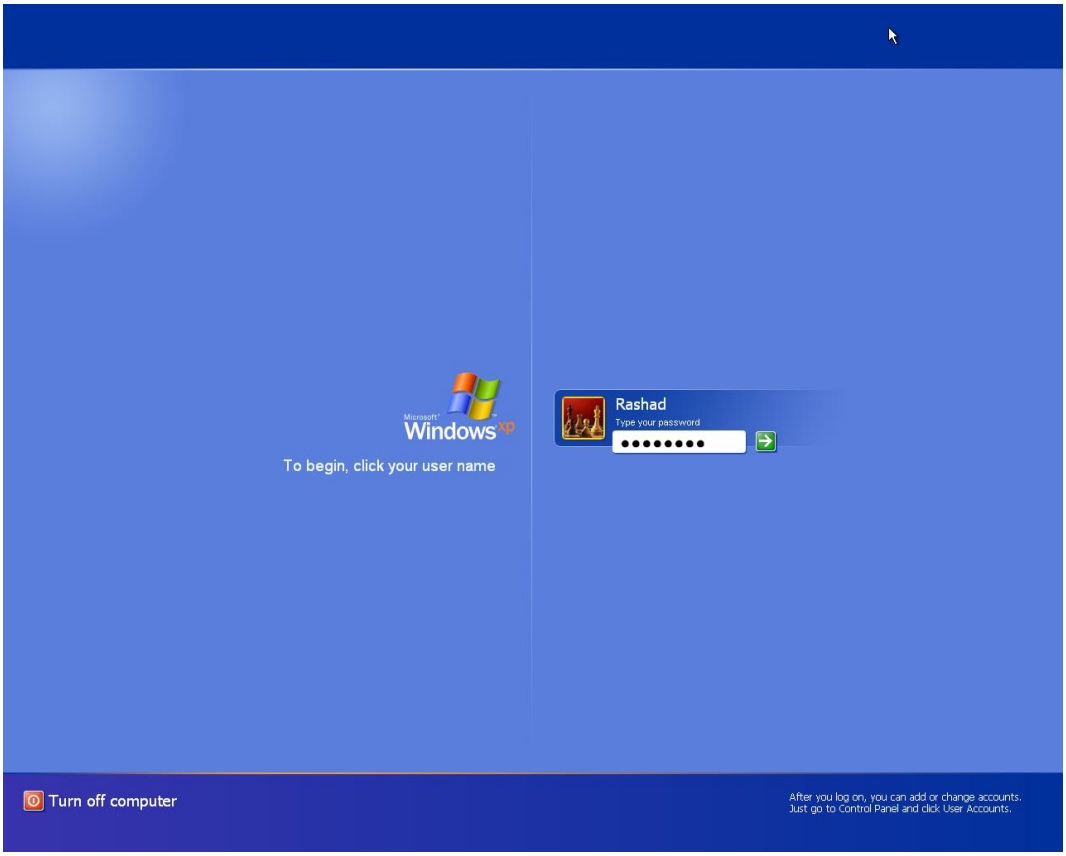
Gambar 6.

Untuk mengetahui hasil output hash tersebut, ketik cat hasilhash.txt di Terminal.

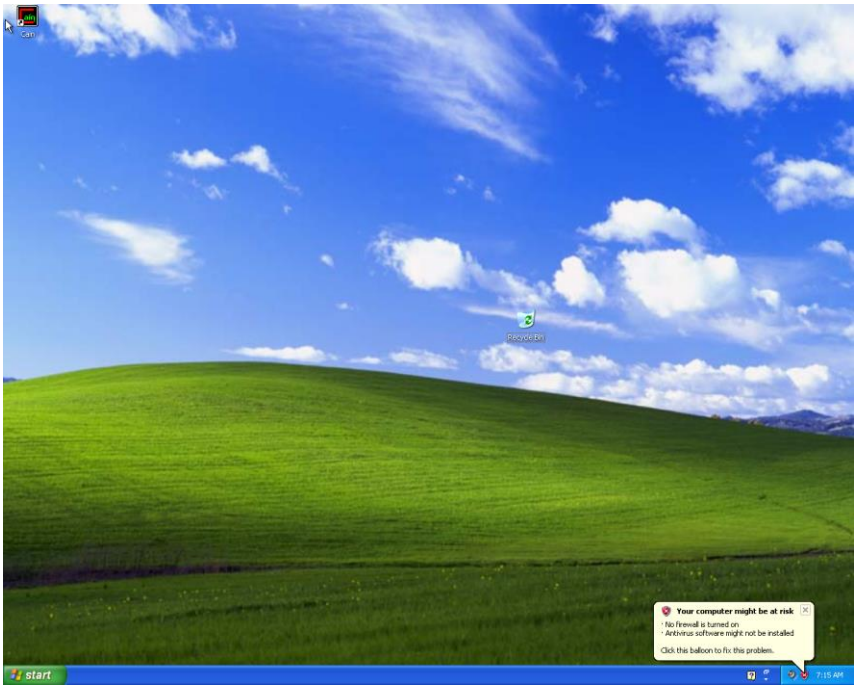


Gambar 7.

Dapat dilihat pada gambar di atas, username dengan nama Rashad passwordnya adalah: password. Untuk mengetahui apakah benar atau tidaknya metode password cracking di atas, dapat kita masukkan password “password” (tanpa kutip) untuk username Rashad di OS Windows XP sebelumnya (ditunjukkan pada gambar 8 dan 9).



Gambar 8.



Gambar 9.