

Password Cracking Windows XP



D
I
S
U
S
U
N

OLEH :
Ahmad Fitri Rashad
09121001023

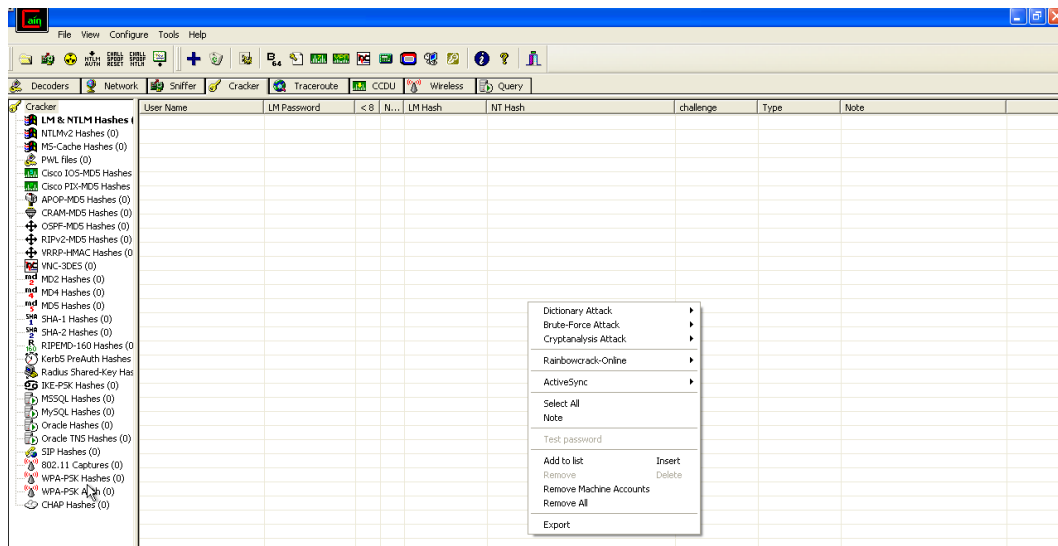
SISTEM KOMPUTER
FAKULTAS KOMPUTER
UNIVERSITAS SRIWIJAYA

INDRALAYA
TAHUN AJARAN 2015 / 2016

Pada tugas *password cracking* ini, saya menggunakan:

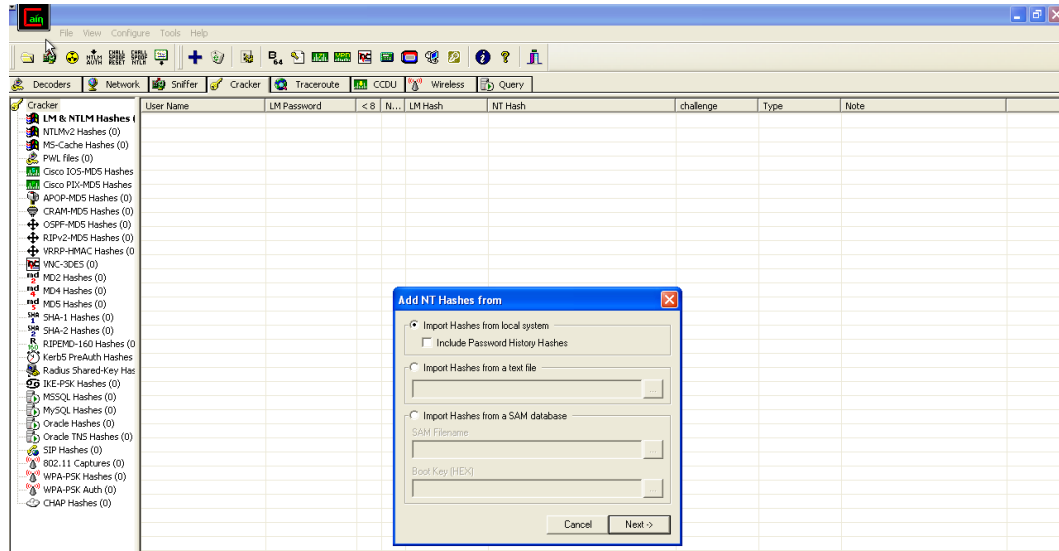
- Windows XP Service Pack 3 (yang di-*install* di Oracle Virtual Machine)
- Kali Linux 2.0
- Cain & Abel
- Hashcat

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.



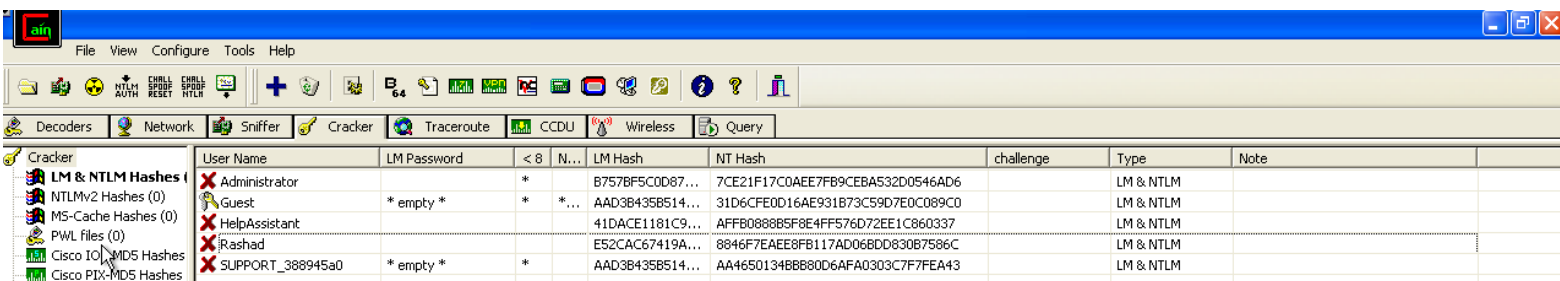
Gambar 1.

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



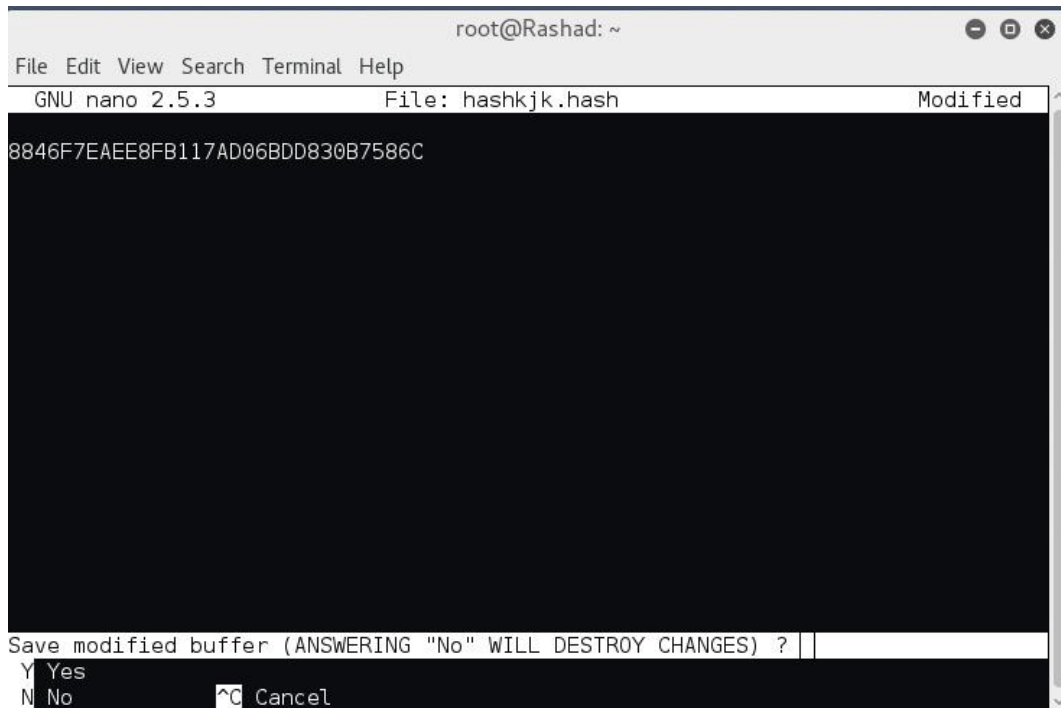
Gambar 2.

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).



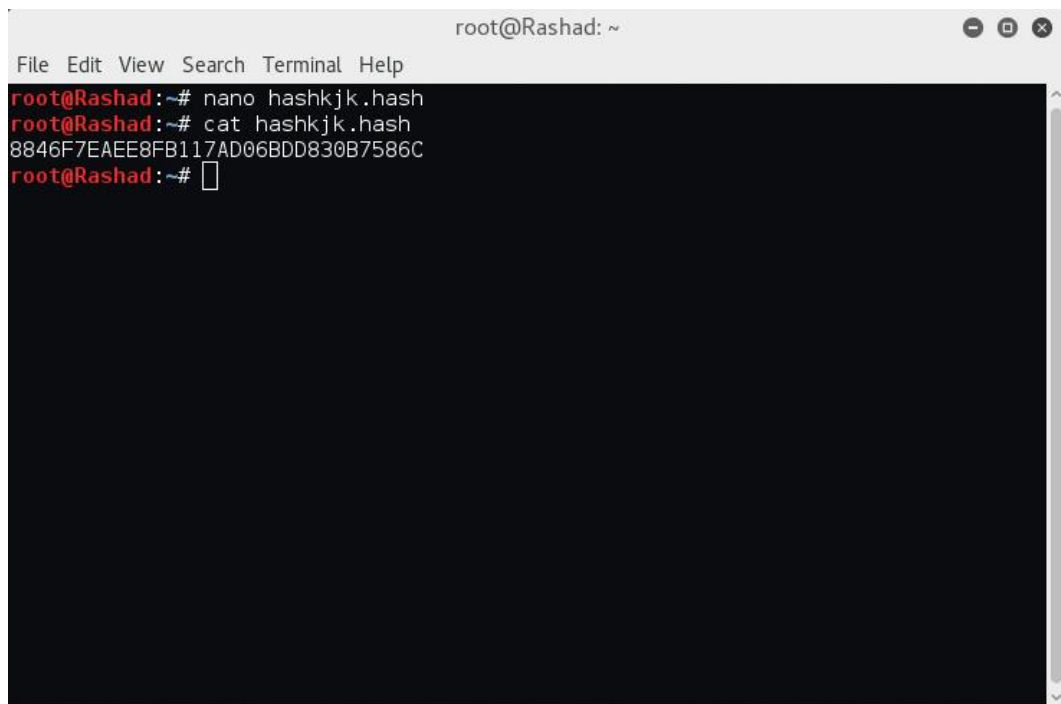
Gambar 3.

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.



```
root@Rashad: ~
File Edit View Search Terminal Help
GNU nano 2.5.3 File: hashkjk.hash Modified
8846F7EAAA8FB117AD06BDD830B7586C
Save modified buffer (ANSWERING "No" WILL DESTROY CHANGES) ?
Y Yes
N No ^C Cancel
```

Gambar 4.



```
root@Rashad: ~
File Edit View Search Terminal Help
root@Rashad:~# nano hashkjk.hash
root@Rashad:~# cat hashkjk.hash
8846F7EAAEE8FB117AD06BDD830B7586C
root@Rashad:~#
```

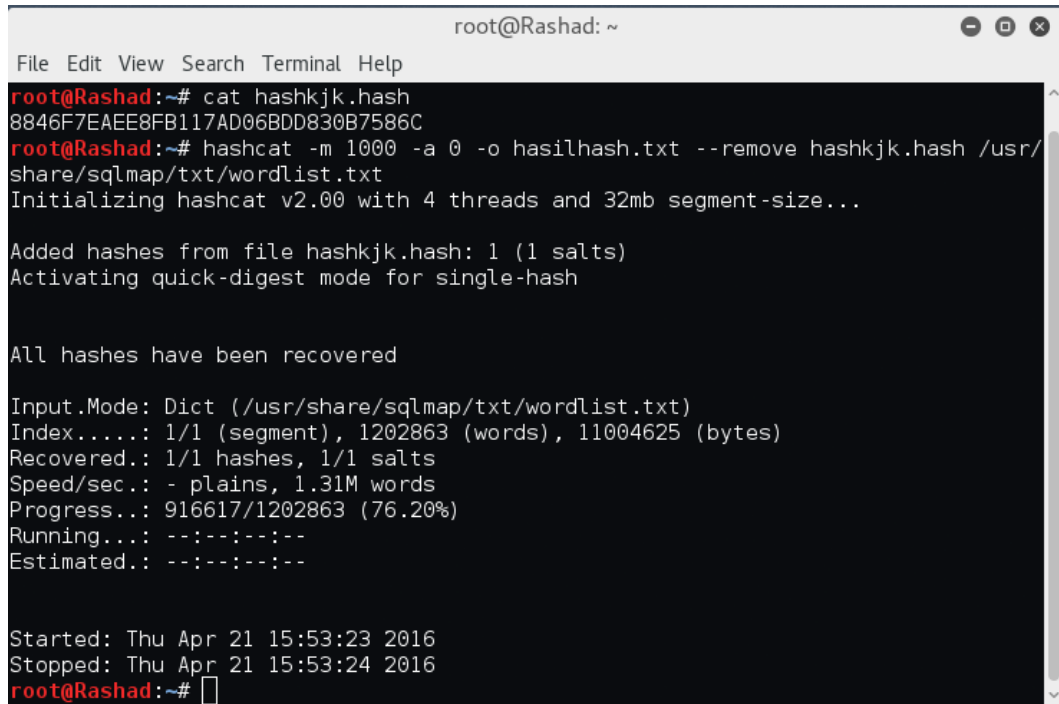
Gambar 5.

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.



```
root@Rashad: ~  
File Edit View Search Terminal Help  
root@Rashad:~# cat hashkjk.hash  
8846F7EAE8FB117AD06BDD830B7586C  
root@Rashad:~# hashcat -m 1000 -a 0 -o hasilhash.txt --remove hashkjk.hash /usr/  
share/sqlmap/txt/wordlist.txt  
Initializing hashcat v2.00 with 4 threads and 32mb segment-size...  
  
Added hashes from file hashkjk.hash: 1 (1 salts)  
Activating quick-digest mode for single-hash  
  
All hashes have been recovered  
  
Input.Mode: Dict (/usr/share/sqlmap/txt/wordlist.txt)  
Index.....: 1/1 (segment), 1202863 (words), 11004625 (bytes)  
Recovered.: 1/1 hashes, 1/1 salts  
Speed/sec.: - plains, 1.31M words  
Progress..: 916617/1202863 (76.20%)  
Running...: --:--:--:--  
Estimated.: --:--:--:--  
  
Started: Thu Apr 21 15:53:23 2016  
Stopped: Thu Apr 21 15:53:24 2016  
root@Rashad:~#
```

Gambar 6.

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

```
root@Rashad: ~
File Edit View Search Terminal Help
root@Rashad:~# hashcat -m 1000 -a 0 -o hasilhash.txt --remove hashkjk.hash /usr/
share/sqlmap/txt/wordlist.txt
Initializing hashcat v2.00 with 4 threads and 32mb segment-size...

Added hashes from file hashkjk.hash: 1 (1 salts)
Activating quick-digest mode for single-hash

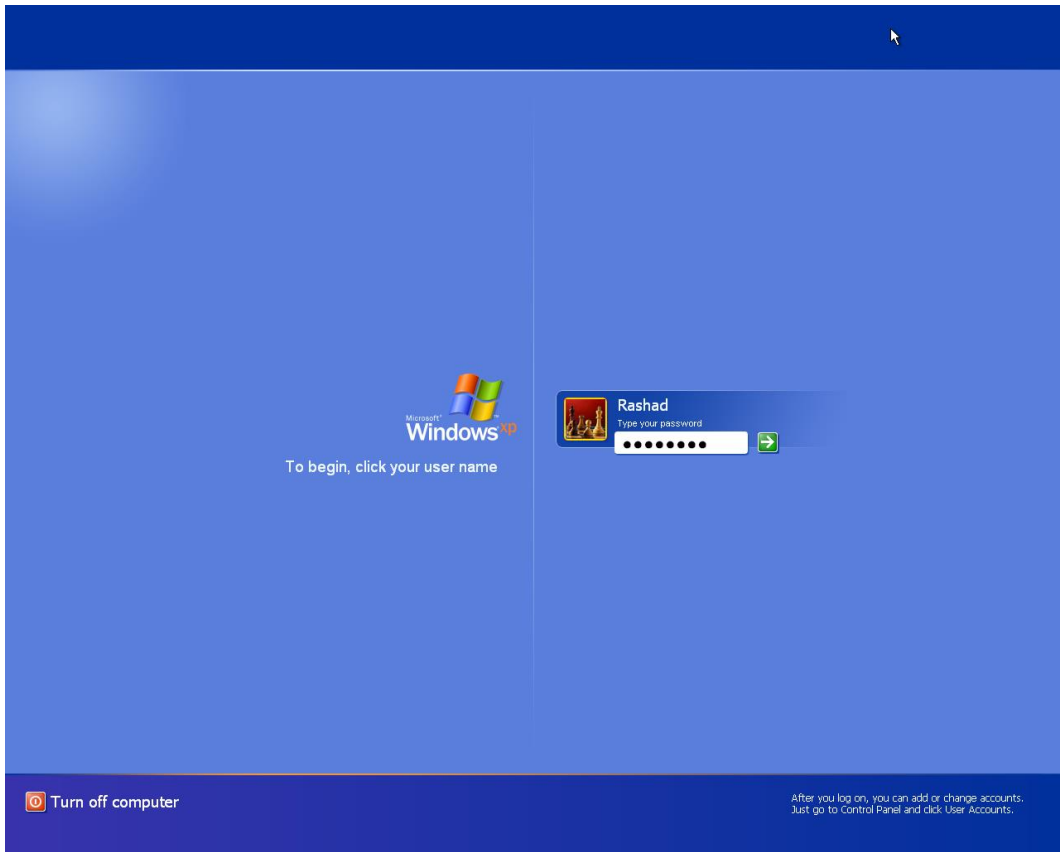
All hashes have been recovered

Input.Mode: Dict (/usr/share/sqlmap/txt/wordlist.txt)
Index.....: 1/1 (segment), 1202863 (words), 11004625 (bytes)
Recovered.: 1/1 hashes, 1/1 salts
Speed/sec.: - plains, 1.31M words
Progress..: 916617/1202863 (76.20%)
Running...: --:--:--:--
Estimated.: --:--:--:--

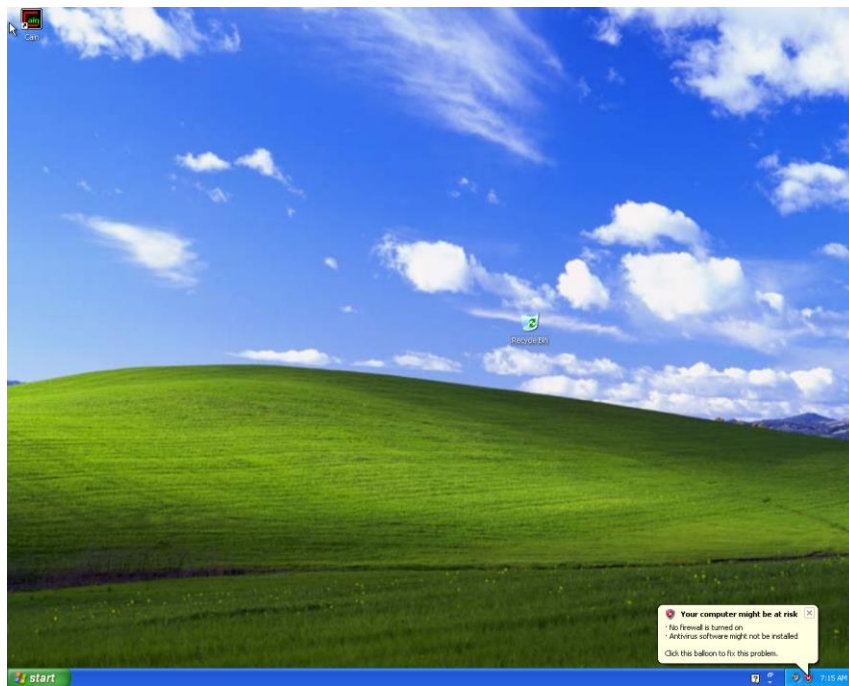
Started: Thu Apr 21 15:53:23 2016
Stopped: Thu Apr 21 15:53:24 2016
root@Rashad:~# cat hasilhash.txt
8846f7eaaa8fb117ad06bdd830b7586c:password
root@Rashad:~#
```

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.